CENTRE FOR
STRATEGIC COMMUNICATION
AND COUNTERING DISINFORMATION

January 2026 REPORT

INFORMATION MANIPULATION AND DEMOCRATIC RESILIENCE: MALIGNANT NETWORKS AND PERSISTENT INFORMATION THREATS

stratcom.md

According to its mandate, established by Article 8 of Law 242 of 31.07.2023, the Centre for Strategic Communication and Countering Disinformation (the Centre) carries out activities to identify actions of **foreign information manipulation and interference (MIIS)** by analyzing online data available in the public space.

These actions support the mission to consolidate inter-institutional efforts in the fight against MIIS (English: FIMI) that pose a danger or may jeopardize the achievement of national interests, including maintaining peace, consolidating democracy, social cohesion, accession to the European Union, strengthening the economy, increasing resilience in the regional security context, and strengthening the defense sector1. In this context, the mission includes protecting major events taking place on national territory, such as key democratic exercises (especially elections) or large-scale events with strong international visibility.

To identify FIMI actions, in accordance with the information threats identified for 2024-2025 in the context of elections2, the Centre monitored the activities of online ecosystems and networks with known ties to hostile foreign powers or to physical or legal entities aligned with their interests. This operational approach is based on an analysis of the adversary's mode of operation in the information space (online behavioral analysis).

This Report is public and intended for partners in the media, civil society, and academia. Its aim is to provide a clearer understanding of the typology, complexity, and persistence of FIMI-type operations documented by the Centre. The report presents a set of cases documented during the post-electoral period, namely between October 1 and December 22, 2025.

The document does not contain sensitive information, including details on analytical tools, sources, institutional partners, or operational priorities. The cases presented are synthesized to serve exclusively the objectives of awareness, education, and increasing the resilience of civilian actors.

1 According to the Concept of Strategic Communication and Countering Disinformation, Information Manipulation Actions, and Foreign Interference for the Years 2024–2030, approved by Parliament Decision No. 416 of 22.12.2023.

2 For details, see public analytical publications on www.stratcom.md, Publications section.

I. Contextualisation of documented attacks

In the post-electoral period, following the completion of the presidential, parliamentary, and referendum elections, the Russian Federation entered a stage of vector reconfiguration and recalibration of manipulation tools, continuing to pursue the strategic objective of blocking European integration and bringing the Republic of Moldova back into its sphere of influence.

After the September 28 Parliamentary elections, the Centre continued to monitor FIMI-type actions in a sensitive context for the Republic of Moldova, marked by the overlap of several political, institutional and social processes with strategic relevance. The accelerated advancement of the European path, the dynamic reform agenda associated with the accession process, the intensification of cooperation with Western partners and the electoral context have increased the visibility of the Republic of Moldova in the regional geopolitical arena.

This context is systematically exploited by the Russian Federation and its networks of influence, which aim to keep the Republic of Moldova in a zone of strategic ambiguity, erode public support for European integration (both among citizens in the country and the diaspora), and diminish public support for EU enlargement among European states. The operations also aim to create favorable conditions for the accession to power of political forces compatible with the Kremlin's interests. These actions are not only aimed at changing short-term electoral options but especially at reshaping the perceptual framework through which citizens evaluate their state, institutions, and external partners.

At the same time, the populations of EU countries are constantly targeted by information manipulation, aimed at generating negative perceptions of the Republic of Moldova and, implicitly, influencing European leaders' willingness to support Chisinau. In this regard, denigrating narratives against the Republic of Moldova are promoted in EU countries by proxy actors or by those sympathetic to the Russian Federation.

The sociopolitical background is marked by heightened polarization, persistent economic vulnerability, uneven trust in institutions, and heavy reliance on digital platforms as a primary source of information. These conditions create fertile ground for narratives that exploit fear, frustration, a sense of injustice, or social fatigue. In this environment, disinformation is rarely presented as outright falsehoods but is instead embedded in seemingly legitimate, emotional, or pseudo-critical content.

The cases documented and presented in this Report indicate that malicious actors are continuously adapting to countermeasures already publicly known. A transition is observed from crude, easily attributable messages to more sophisticated and subtle operations: the use of Western sources for legitimization, commercial or civic covers, automation technologies and artificial intelligence, microtargeting through data collected via online socio-political surveys, and the rapid migration of digital infrastructure after its exposure to the general public.

On the whole, the FIMI attacks analyzed must be understood as part of a coherent, long-term effort aimed not only at influencing public opinion but also at degrading society's ability to distinguish legitimate information from manipulation. This structural dimension of the threat explains why an effective response cannot be fragmented or exclusively reactive, but must be coordinated, anticipatory, and sustained across society.

II. Mapping of malicious actors and TTPs used

The analysis of cases documented in the post-2025 election period indicates the existence of a **diverse malignant ecosystem**, which includes:

a. apparently independent media entities or pseudo-media;
b. networks of inauthentic accounts on social platforms;
c. replicated and “migratory” digital infrastructures;
d. commercial or civic entities used as cover;
e. financial and phishing schemes with informational components.

Main Tactics, Techniques and Procedures (**TTPs**) observed include:

1. artificial amplification of messages through coordinated networks of accounts;
2. the use of content generated or assisted by artificial intelligence;
3. "information laundering" through seemingly credible sources, often located in the West;
4. rapid migration of digital infrastructure to avoid detection;
5. exploitation of symbols of state and public authority;
6. combining disinformation with financial fraud and data collection.

III. Operations, objectives and main methods of influence

Case study 1: Use of Kremlin-affiliated infrastructure in campaigns to manipulate the population of the Republic of Moldova. STORM-1516 international pro-Russian network

Manipulative objective

One such method is to use accounts with large audiences, in this case accounts with tens of thousands of subscribers and/or who have a close relationship with their community, to expand content distribution and reach a wider audience.

The goals pursued include discrediting the Republic of Moldova internationally, damaging Moldova's external image and reputation, and eroding the support of Western partners by denigrating the state's ability to ensure a democratic electoral process and a secure European path. The attacks also targeted pro-European leaders, especially during the electoral and post-electoral periods.

Storm-1516 is a Kremlin-affiliated pro-Russian manipulation network that produces and distributes fabricated narratives (including deepfakes and staged videos) and amplifies them through a distribution chain of disposable accounts, paid accounts, and third-party media "washing" of the story, followed by amplification by pro-Russian actors. The network is used to test, launch, and amplify manipulation narratives through mechanisms that are difficult to directly attribute to a state. Storm-1516 operates by creating seemingly journalistic or civic content (pseudo-media sites, "witnesses," "whistleblowers," fabricated videos or texts), which is subsequently injected into vulnerable information ecosystems and taken up by opportunistic local actors, partisan channels, or social media amplification networks. This method is preferred because it reduces operational costs, maximizes attribution ambiguity, and allows for rapid adaptation of messages to local specificities, including in states with fragile or polarized media markets, such as the Republic of Moldova. In this way, the network does not necessarily act as a visible vector but as a "supplier of informational raw material" for manipulation campaigns that can later be localized, recycled, and normalized in the domestic public discourse.

The network was mentioned in the Center's public post-election report and was further monitored during the post-election period. In this regard, the subjects in the table below were identified as dominant in the content promoted by this network.

Subject	Exploited messages (examples of formulations/narratives)	Purpose pursued
European integration	(drones/incidents)	*"EU means costs, loss of sovereignty, dependence"; "two-speed accession / reduced rights"*
"Western Censorship" / platforms		*"Telegram is the target because it is not controllable";*
Security		*"external pressures for blockages before elections";*

"ministry of truth"	Erosion of support for the EU / delegitimization of the European path, Victimization + anti-EU mobilization / distrust in institutions,
"false flag"; "staging/propaganda"; ironizing the incidents	Confusion, relativization of risks and of the RF responsibility,

Subject	Exploited messages (examples of formulations/narratives)	Purpose pursued
	"The West is arming the Republic of Moldova"; "The Republic of Moldova is being pushed	Social fear + contesting the cooperation with Western partners,
Militarization/war	*towards war"; escalation*	
Trafficking/ weapons and crime	*"Ukraine–RM–RO arms smuggling routes"; "weapons for provocations/false flags" "fraud / Moldovan scenario";*	Stigmatization of the RM + security anxiety,
Elections / legitimacy	*"EU assistance= elimination of the opposition"; insinuations about diaspora*	Undermining trust in democratic processes,
External control / NGOs / media	*"NGOs and media 'directed' by the West"; "media projects = information warfare"*	Delegitimization of pro-reform actors and external support,
Gagauz ATU and internal tensions	*"political persecution"; instrumentalization of autonomy for polarization*	Internal fragmentation + weakening of social cohesion.

Case study 2: The use of Western civic organizations and think tanks ideologically aligned with the Kremlin as vectors of Russian manipulative messages

Manipulative objective

In the context of Moldova, the objective of this tactic is to undermine trust in European institutions and in the partnership with the EU, by presenting European measures to protect democratic processes as forms of censorship or political interference. In the medium term, this tactic aims to weaken public support for the European path, delegitimize the authorities in Chisinau and fuel suspicions about the fairness of electoral processes, without directly exposing the real source of influence.

This manipulation technique is applied by deliberately using apparently credible Western sources (think tanks, "experts", reports written in academic language) to introduce hostile narratives against the EU into the information space of the Republic of Moldova without triggering rejection reactions. By taking over and coordinating the amplification of analytical materials from Western media ideologically aligned with the Kremlin, local pro-Russian actors artificially transfer credibility and legitimacy to anti-European messages. Thus, a process of "information laundering" takes place, the mechanism pursued being one of "external validation" - the public is led to believe that criticism of the EU does not come from Russian propaganda, but from the "Western debate itself".

At the end of November 2025, the report titled "A Shield Against Democracy: How the Democracy Shield Protects the EU from the Electorate," published by the MCC Brussels think tank, was introduced and amplified in the information space of the Republic of Moldova. The document advances the thesis that the European Commission's initiative, called "Democracy Shield," intended to protect and strengthen democracies in the European Union, would, in reality, serve as an instrument of public opinion control, used by the European Union and the Chisinau authorities to limit freedom of expression and manipulate elections.

The report's author is Norman Lewis (Image 1), an academic with anti-EU views affiliated with the MCC Brussels think tank, which consistently promotes a pro-Russian agenda. In this report, he claims that the EU would establish a system of censorship of the opposition3, accuses the EU of alleged interference in Moldovan elections, denies the danger of disinformation4, and promotes conspiratorial messages about the use of NGOs to advance the interests of elites5. The speech was quickly adopted and widely distributed by political actors, media outlets (including KP Moldova, TV6-Moldova, Mir Gagauzii, "Primul în Moldova," Netipicinaia Moldova News), and opinion leaders from the Republic of Moldova known for aligning with the pro-Russian agenda. They used the report as a source of "Western validation" to reinforce existing narratives in the local information space, according to which the EU would seek to limit freedom of expression and manipulate electoral processes.

Imaginea 1

Coordinated reuse of content, without critical contextualization and with a selective focus on elements compatible with anti-EU messages, indicates a classic mechanism of indirect influence, in which ideological convergence between the Western source and local actors enables the transfer of credibility and the amplification of manipulative impact on the domestic public.

Synchronized distribution indicates a mechanism of "information laundering," through which an apparently Western product is used to legitimize narratives hostile to the EU and delegitimize the European cooperation of the Republic of Moldova.

[3]https://x.com/Norm_Lewis/status/1993968827328286792, https://x.com/Norm_Lewis/status/1956375644839002284, https://x.com/Norm_Lewis/status/1932015578446754057 [4]https://x.com/Norm_Lewis/status/1993850838482341971
[5]https://x.com/Norm_Lewis/status/1895151482447544417,https://x.com/MCC_Brussels/status/1902662426497024463,https://x.com/Norm_Lewis/status/1888174312168792527

Case study 3: The use of international media with pro-Russian affiliations to denigrate the Republic of Moldova in the European information space (the case of "IL Giornale d'Italia")

Manipulative objective

The publication of materials in Western publications, such as in the case study presented, aims to give credibility to hostile narratives, so that they can later be reimported into the domestic information space as "independent assessments from the West." Domestically, this tactic favors the broader objective of eroding public support for the European path and legitimizing political actors and oligarchs targeted by legal actions, by presenting them as victims of political repression.

The goal of using the pro-Russian international press is to delegitimize the Republic of Moldova as an EU candidate state externally, by inducing the perception that democratic and judicial reforms are simulated, selective or politically motivated. In the analyzed case, the specific goal is to compromise the fight against corruption and judicial reform by associating them with authoritarian practices, undermine the trust of European partners in the commitments assumed by Chisinau and fuel the discourse according to which the Republic of Moldova does not meet the democratic standards necessary for EU accession.

The association of the authors of such materials and articles with publicly known networks and platforms for promoting the narratives of the Russian Federation indicates a potential deliberate strategy of influence, which exploits Western media channels to mask the origin and real intention of the promoted messages.

On December 20, "IL Giornale d'Italia"6 posted an article about the Republic of Moldova titled "Moldova, the fight against corruption or repression of opponents? Experts fear for judicial independence in the EU candidate country".


sabato, 27 dicembre 2025

Seguici su

IL GIORNALE D'ITALIA

Il Quotidiano Indipendente

Cerca...

"La libertà innanzi tutto e sopra tutto"
Benedetto Croce -Il Giornale d'Italia- (10 agosto 1943)

Politica Esteri Cronaca Economia Sostenibilità Innovazione Lavoro Salute Cultura Costume Spettacolo Sport Motori iGdI TV

- Giornale d'italia - Esteri

Moldova, lotta alla corruzione o repressione degli oppositori? Esperti temono per l'indipendenza giudiziaria nel paese candidato all'UE

Il governo moldavo ha avviato riforme radicali, specialmente in ambito giudiziario. Ma gli esperti affermano che la direzione effettiva di queste riforme si discosta nettamente dagli obiettivi dichiarati

di Pietro Stramezzi

19 Dicembre 2025

Articoli Recenti

Mosca: accordo mai stato così vicino ma Kiev e Unione Europea stanno facendo di tutto per affossarlo

Ucraina, domani alle 21 incontro Trump-Zelensky a Mar-a-Lago su piano di pace in 20 punti, tycoon: "Non si fa nulla se non approvo io"

Il bombardamento Usa contro la Nigeria del nord dominata dall'islamismo fondamentalista: pragmatismo e nuova posizione etica

La Siria dopo Assad: tra realpolitik, basi straniere e intelligence, Damasco

Image 2

The article promotes recurring themes in pro-Russian propaganda, according to which the judicial system is politically controlled by the executive and the state is associated with authoritarian practices incompatible with European democratic standards. The publication implicitly suggests that the Republic of Moldova does not meet the necessary criteria for EU accession, using arguments related to "selective justice" and "political persecution".

6 https://archive[.]ph/O06n8

The Vladimir Plahotniuc case is exploited as a central example, presented as a flawed and unfair process that lacks anti-corruption legitimacy, in line with the narrative that the fight against corruption is directed exclusively against political rivals. These messages were subsequently imported into the internal information space and presented as external "evidence" to support narratives about the selective nature of the fight against corruption and the political persecution of the opposition, and thus as external validation for challenging democracy and the rule of law in the Republic of Moldova.

The author of the article is Pietro Stramezzi (dual Italian and Russian citizenship, full name Pietro Veniamin Andreevici Stramezzi), a spokesperson for Russian Federation narratives in Europe. Stramezzi gave an interview to RussiaToday7, describing himself as "President of the Milan committee of the Stop The War organization" ("pressure lobby to stop Italian aid to UA and against Russophobia" – description provided by Stramezzi). According to Rossotrudnichestvo8 (Россотрудничество), Pietro Stramezzi is the President of the "Friends of Russia" International Cultural Association. Currently, he is "head of international projects within an oil company".

Case study 4: Social media algorithm speculation. Manipulation campaigns through networks of inauthentic accounts on the TikTok digital platform

Manipulative objective

This technique is used to give a false popularity to a topic and respectively manipulate public perception. Thus, hostile messages/narratives are artificially promoted and made to seem legitimate, regardless of their real support in society. By exploiting recommendation algorithms (rapid engagement, repetition, volume, synchronization) hostile actors force messages into users' main content/information flows, bypassing editorial filters and traditional information validation mechanisms.

Strategically, this technique is used to create the impression of broad social consensus, collective outrage or a sense of urgency, inducing in the public the idea and feeling that "everyone is talking about it". Inauthentic account networks allow for rapid testing of messages, selective amplification of favorable content and suppression of the visibility of alternative messages, by flooding the information space with repetitive and emotional content. In electoral or crisis contexts, the objective becomes: influencing civic behavior (voting, protest, withdrawal from democratic participation, etc.), eroding trust in institutions and polarizing society, without public assumption of the real source of influence.

The case studied aimed to distort the information space, undermine trust in state authorities, as well as affect public trust in democratic institutions and in the European path of the Republic of Moldova.

After the elections in the Republic of Moldova, a mobilization of networks of inauthentic accounts on social media platforms was identified. For example, one documented network, consisting of 119 inauthentic accounts on TikTok, was activated immediately after the election with the aim of forcibly influencing public opinion. Their activity consisted of the coordinated generation and distribution of

7 https://archive[.]ph/0GofA

8 https://archive[.]ph/spJL2

content (mostly AI-generated), massive commenting and synchronized and coordinated mutual interactions with posts (like/share/comment) to artificially keep certain topics on the public agenda and/or amplify their visibility.

Between October 1 and December 31, 2026, these accounts generated and shared 5,588 posts, which accumulated approximately 50 million views/impressions, 104 thousand comments, approximately 1.5 million reactions/interactions, and approximately 250 thousand shares. The high volume of content and engagement dynamics indicate sustained, inorganic activity oriented toward maximizing impact in the information space.

The main goal of the network was to create a negative information background at the national level. Through repetition and artificial amplification, the accounts aimed to erode trust in institutions, increase social tensions, and accentuate polarization.

Imaginea 3

Most of the messages and topics promoted centered on economic difficulties, with an emphasis on inflation, poverty, wage levels, pensions and compensation, and energy prices. Although presented as real challenges, coordinated message amplification techniques have been exploited to fuel and channel public anger against government policies and institutional priorities.

Additionally, messages like “broken promises” regarding delays and diminishing Western enthusiasm for the Republic of Moldova and Ukraine, artificially amplified through repetition and synchronized promotion, aimed to erode confidence in Western support and in the prospect of EU accession. This direction generated divergent calls: on the one hand, to sovereignty and neutrality, and on the other hand, to radical solutions such as unification with Romania, both contributing to increased polarization and fragmenting public consensus.

Another set of themes focused debates on sovereignty, identity, and political legitimacy, using topics such as the unification of the Republic of Moldova with Romania, neutrality versus NATO/EU integration, and asset management and sale. In parallel, identity themes related to language, history, church properties, and educational reforms were amplified, along with accusations of election manipulation, censorship, and abuse of justice, to intensify antagonism and radicalize attitudes.

The content repeatedly exploited the theme of corruption and the gap between rhetoric and reality, highlighting scandals involving gas and energy, smuggling and drug trafficking, bank fraud, party financing, and the judicial verification process. These topics were used to challenge the government's credibility and to project an image of an institutional system that was complicit, selective, or incapable of reforming itself.

The network has also maintained a visible backdrop of geopolitical tensions, through references to the war in Ukraine, the Russia-West confrontation, increased militarization, migration, and sanctions. In this logic, the warning that the Republic of Moldova would be a "pawn" or "buffer zone" in the competition between the great powers appears repeatedly. By constantly exploiting and fueling fear, the perception of insecurity and strategic vulnerability is reinforced.

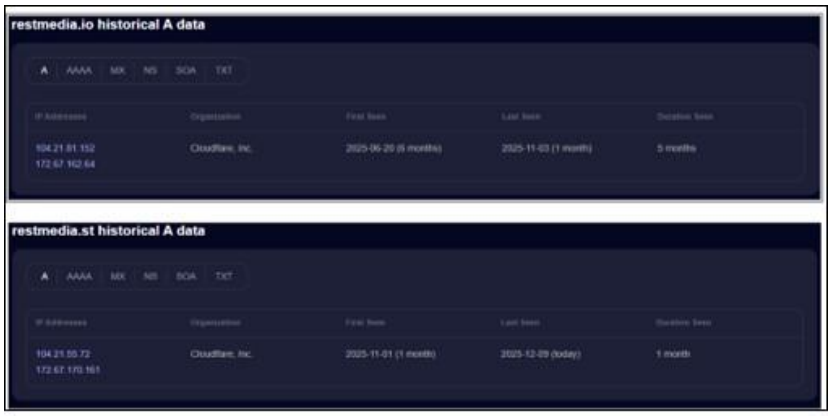
Case study 5: Rapid reconfiguration of FIMI infrastructures after public exposure: REST Media case study

Manipulative objective

The objective of this tactic is to ensure the operational continuity of a hostile information manipulation and inference infrastructure after it has been documented and publicly exposed. Thus, through rapid technical reconfigurations, the aim is to reduce the reputational costs and the risk of external intervention for accountability, such as blocking, sanctioning measures or systematic monitoring. Through technical reconfigurations, not only accountability is avoided but also the ability to continue producing and distributing manipulative content is maintained.

In the case presented, after the infrastructure was previously documented by the CSCCD, and publicly attributed to actors associated with Russian information networks, it quickly migrated to another domain and carried out a partial “cleaning” of the digital traces indicating direct links to Rybar. This procedure allowed for the maintenance of operational continuity, even under a new technical identity, continuing to mislead the public, creating the impression of a new or independent platform.

Following CSCCD's public exposure and attribution of REST Media to the Rybar Russian information network (Report of October 3, 20259), a rapid reconfiguration of the digital infrastructure was observed. This included migrating the main domain from restmedia[.]io to restmedia[.]st on November 1, 2025, indicating an immediate post-exposure adaptation intended to reduce the visibility of previous links and ensure operational continuity. The original restmedia[.]io domain, previously hosted on Cloudflare at IP addresses 104.21.81.xxx and 172.67.16x.xx, was closed on 01.11.2025. On the same day, the new restmedia[.]st domain was registered and hosted on Cloudflare at IP addresses 104.21.5x.xx and 172.67.170.xxx.



Imaginea 4

[9] https://stratcom.md/interferenta-informationala-a-rusiei-asupra-proceselor-democratice-din-republica-moldova/

Technical analysis indicated the deletion of some metadata that had previously directly referenced Rybar, the known Russian Federation-affiliated information network. However, consistent technical indicators remained, including file structures and Russian-language terminology.

Previously, DFRLab10 identified Vesna Veizović as a central figure in REST Media. In an interview on the "Informer" YouTube channel, Veizović acknowledged her role in REST Media and confirmed receiving assistance from the Rybar team (Image 5). On her Facebook account11, Veizović posted a photo of a dinner with Mikhail Zvinciuk (the founder of Rybar), adding an ironic caption: "This is collaboration with the Russian special services. At dinner with Rybar, Mikhail Zvinciuk" (Image 6).

Imaginea 5

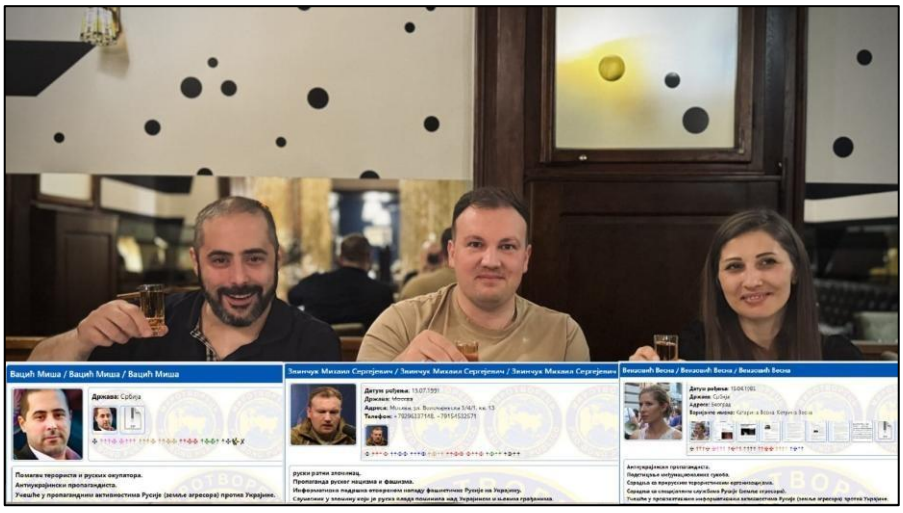


Image 6

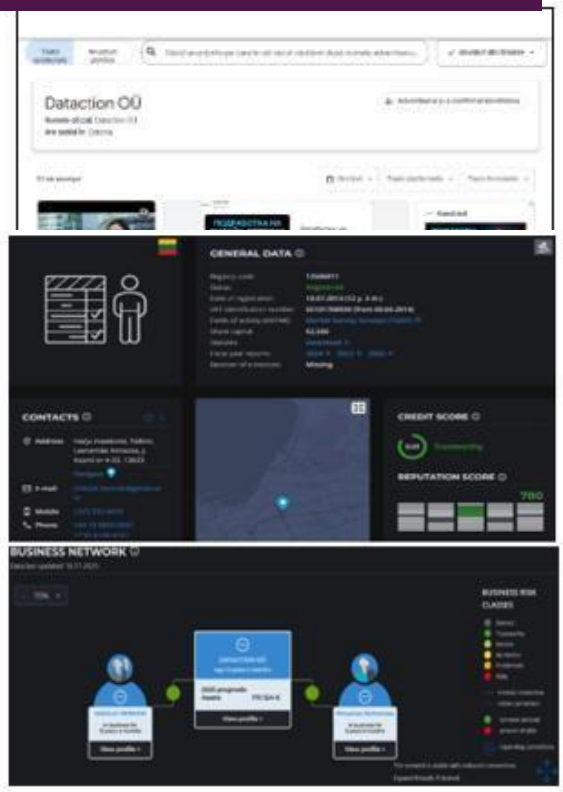
[10] https://dfrlab.org/2025/09/23/sanctioned-russian-actor-linked-to-new-media-outlet-targeting-moldova/
[11]https://www.facebook.com/photo/?fbid=10229298593563598&set=a.10206537628313692#

Case study 6: The use of market research as a cover for political profiling and informational influence. The cases of gand.md and Dataction OÜ.

Manipulative objective

This process involves the exploitation of paid opinion polls and digital advertising infrastructure for the systematic collection of sensitive political data, under the guise of legitimate market research activities. By attracting participants with financial rewards and through paid promotion on digital platforms, the premises are created for detailed profiling of respondents and for the subsequent use of the data in targeted influence campaigns, including electoral micro-targeting. The activity is facilitated through companies registered in European states, with connections to Russian entities that have contracts with institutions on international sanctions lists.

In November 2025, the gand.md platform was identified. It aims to collect responses to opinion polls from citizens of the Republic of Moldova and offers financial rewards for participation. The platform was promoted through at least 92 paid advertisements on Google and YouTube, using the advertiser Dataction OÜ, a company registered in Lithuania (Image 7). Dataction OÜ is a market survey company registered in Lithuania, founded in 2013 by Nikolay Berezin, a citizen of the Russian Federation. As of 29.10.2023, Berezin transferred 80% of the company to the control of Rimantas Reimontas, a Lithuanian citizen and resident of the United Kingdom (Image 8). According to public data, Rimantas Reimontas holds a managerial role within Fastuna ("SIA Tiburon Research", Latvia). The co-founder of "SIA Tiburon Research" is Artem Tinchurin, who is also the founder of ООО "ТИБУРОН", which has won several contracts with state-owned enterprises in the Russian Federation, including:



Imaginea 8

- 80,593,105 rubles from "VTB"Bank (Банк ВТБ (ПАО));
- 3,779,436 rubles from Sberbank (ПАО Сбербанк);
- 1 494 116 rubles from the "Kalashnikov" holding (АО «Концерн «Калашников» (в сообщение Группы компаний «Калашников»)), manufacturer of military armaments for the RF.

The technical infrastructure associated with gand.md is similar to that used for polling platforms in other CIS countries, such as Armenia, Georgia, Belarus, and Kyrgyzstan.

Case study 7: Ensuring the persistence of the distribution infrastructure of hostile information manipulation content through replication and migration. The case of Hai TV, Trădători/*Traitors* and MD 24

Manipulative objective

This tactic aims to continue distributing manipulative content after the public exposure of the digital infrastructure through processes of reconfiguration, fragmentation and replication of the digital infrastructure. Rapid domain migration, the use of CDN-type infrastructures and cloning of content on multiple platforms allow the network to remain operational despite countermeasures. This allows for the continued manipulation of public debate and the forced influence of public opinion by mimicking the legitimacy of the transmitting source.

Following the publication of previous CSCCD reports exposing the infrastructure of the Hai TV, Traitors, and MD24 networks, their operators implemented a technical adaptation strategy. Between November 28 and December 2, 2025, several domains were migrated to the Cloudflare infrastructure, and content was replicated on new domains such as moldova-check[.]com, moldovalife[.]com, and mldregion[.]com.

Upon observing these movements and analyzing the new infrastructure, it was found that several domains had migrated from the old servers (185.11.145.xxx, 185.11.145.xxx) to a Cloudflare CDN platform, identified by the IP addresses 104.21.xx and 172.67.xx.

The domains hai-tv[.]me and tv-hai[.]com were registered directly on Cloudflare's infrastructure, with no prior IP history. The connection to the previous sites (haitv) was established by analyzing identical source code and by retaining the same Google Tag identifier used previously.

In the case of "Traitors," the authors used a different strategy, creating the domains moldova-check[.]com and moldovalife[.]com (previously a site about the nature of the Republic of Moldova) that duplicate the same content under different names.

On 28.09.2025, moldova-check[.]com and moldovalife[.]com were moved to IPs 185.11.145.xxx and 185.11.145.xxx. Just two days later, both domains were migrated to the same IP, 202.155.1x.xx.

The analysis identified the use of the same Google Tag for traffic monitoring, identical spelling errors in the source code, and synchronized migrations, indicating centralized coordination.

The MD24 cluster was previously identified by the DFRLab think tank as affiliated with Russia Today, and the new configurations confirm the persistence of operational ties.

Case study 8: Exploiting state symbols to erode institutional trust. The case of fraudulent financial schemes

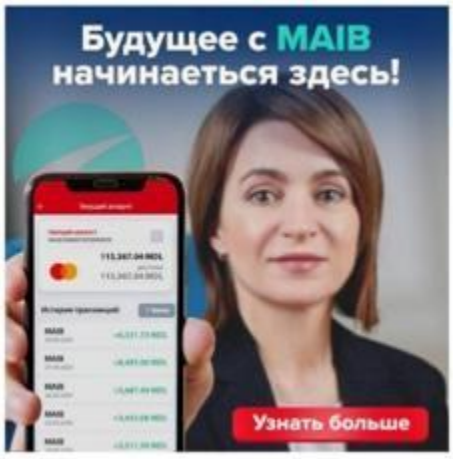
Manipulative objective

This tactic has a double negative effect – on the one hand, by exploiting public trust in state institutions and the abusive use of official symbols (Presidency of the Republic of Moldova, Ministry of Finance, banking institutions), fraudulent financial schemes are promoted to illegally obtain material benefits and personal data; on the other hand, it undermines the perception about competence and authority of public institutions.

Even in the absence of direct external coordination, such online behaviors create informational vulnerabilities that are systematically exploited by malicious actors – messages are generated that fuel the perception of insecurity, distrust in authorities and, implicitly, in democratic processes. Even in situations where it is known that the dignitary is not connected to alleged fraud, the aim is to mislead citizens by repeatedly associating, at a subconscious level, the themes of "fraud" and "lying" with the image of national leaders. This artificial connection, maintained constantly in the information space, has the effect of gradually eroding trust in authorities and delegitimizing official communication.

By creating multiple, nearly identical websites hosted on the same infrastructure and aggressively promoted, operators aim to exploit public trust in state institutions to mislead citizens and obtain personal and financial data.

A digital fraud campaign was documented in October 2025, using images of the President of the Republic of Moldova, the Ministry of Finance, and the MAIB bank to promote fraudulent financial schemes (Image 9). At least 11 active websites were identified, hosted on Cloudflare infrastructure, and all used the same code template (Table 1).



Imaginea 9

All 11 identified domains use IP addresses in the range 104.21.xx and 172.67.xx for IPv4, respectively 2606:4700:30xx for IPv6, which are specific to the Cloudflare CDN infrastructure, indicating a common technical configuration.

Table 1. Registered websites

No.	Field	IPv4	IPv6
1.	https://vaulthill.xyz[12]	104.21.75.xxx	2606:4700:3030::ac43:bxxx
		172.67.18x.xx	2606:4700:3035::6815:4xxx
2.	https://torvexa.digital[13]	104.21.66.xxx	2606:4700:3030::ac43:dxxx
		172.67.2xx.x	2606:4700:3037::6815:4xxx
3.		104.21.8x.xx	2606:4700:3030::6815:5xxx

[12]https://archive.ph/OdFZd

[13]https://archive.ph/5HnuZ

	https://sendelium.icu[14]	172.67.210.xxx	2606:4700:3033::ac43:dxxx
4.	https://rivano.it.com[15]	104.21.25.xxx	2606:4700:3030::6815:1xxx
		172.67.134.xxx	2606:4700:3034::ac43:8xxx
5.	https://mistpath.xyz[16]	104.21.93.xxx	2606:4700:3033::ac43:dxxx
		172.67.21x.xx	2606:4700:3035::6815:5xxx
6.	https://postcolonialwriting.digital/[17]	104.21.66.xxx	2606:4700:3030::6815:4xxx
		172.67.20x.xx	2606:4700:3031::ac43:cxxx
7.	https://viewentra.icu/18	104.21.40.xxx	2606:4700:3033::ac43:9xxx
		172.67.15x.xx	2606:4700:3034::6815:2xxx
8.	https://brightino.icu/19	104.21.52.xxx	2606:4700:3034::ac43:cxxx
		172.67.20x.xx	2606:4700:3035::6815:3xxx
9.	https://kindentry.icu/20	104.21.96.xxx	2606:4700:3030::ac43:b5xx
		172.67.181.xxx	2606:4700:3034::6815:6xxx
10.	https://dreamenio.xyz/[21]	104.21.28.xxx	2606:4700:3031::6815:1xxx
		172.67.147.xxx	2606:4700:3033::ac43:9xxx
11.	https://thinkovia.xyz/[22]	104.21.73.xxx	2606:4700:3030::6815:4xxx
		172.67.16x.xx	2606:4700:3037::ac43:axxx

The promotion was carried out through paid ads on Facebook (Image 10) and pseudo-news sites. Analysis of the source code indicated the presence of more than 70 similar websites, automatically generated from the same model, demonstrating an industrial-scale capacity to scale the fraud.

Promovarea pe Facebook

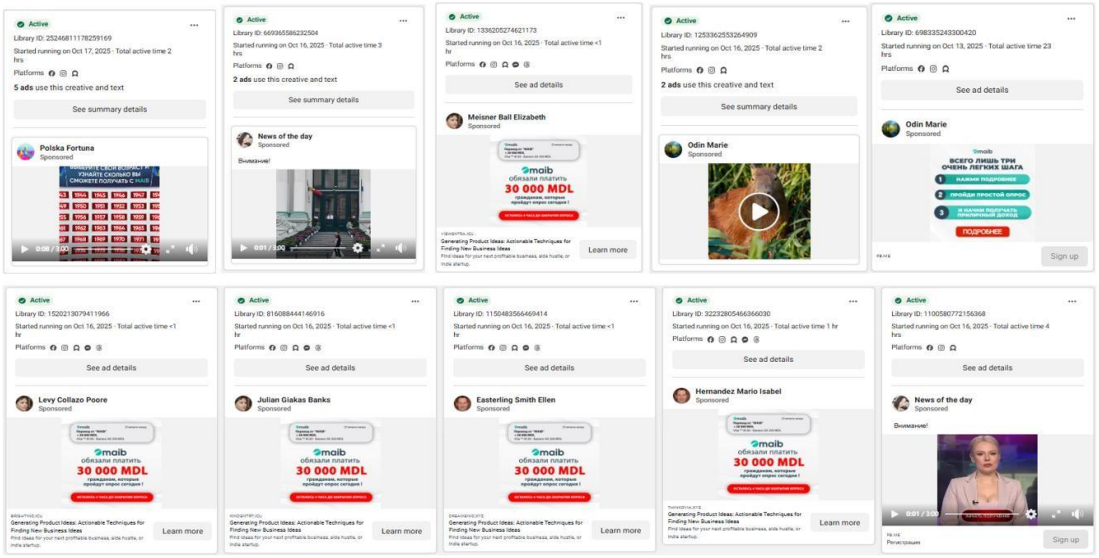


Image 10

[14]https://archive.ph/q6wVn
[15]https://archive.ph/4istK
[16]https://archive.ph/Lmi0
[17]https://archive.ph/tBilE
[18]https://archive.ph/yvSkL
[19]https://archive.ph/BS3u0
[20]https://archive.ph/QsybC
[21]https://archive.ph/C2qQe
[22]https://archive.ph/ncuV0

IV. Measures to increase the resilience of civilian partners

The case studies presented highlight that FIMI operations cannot be effectively countered by specific institutional interventions or isolated reactions by civilian actors alone. The adaptive, cross-sectoral and persistent nature of these threats requires a „Whole-of-Society approach," based on constant interaction, information exchange, coordination and the strengthening of mutual trust among the state, the media, civil society, academia and the private sector.

From the Center's perspective, increasing the information resilience of civilian partners involves:

- institutionalization of regular formats for dialogue and cooperation. Media and civil society organizations can benefit from structured spaces for interaction with experts (from the Centre and other institutions), where emerging patterns of manipulation, relevant case studies, and general trends in the information environment can be discussed without delving into sensitive or operational details. Such formats help develop a common understanding of the threat and align public responses.
- Methodological and capacity support. The Centre can support civilian partners by providing guides, working tools, and training sessions tailored to different categories of actors - journalists, fact-checkers, NGO communicators, trainers, or community leaders. The focus is on early recognition of FIMI TTPs, avoiding unintentional amplification of hostile narratives, and integrating strategic context into public materials.
- Improved synchronization among civilian actors. The Center encourages cooperation among newsrooms, non-governmental organizations, and academia to exchange best practices, align messaging, develop joint awareness initiatives, and reduce fragmentation of responses to information attacks.
- Strengthening reporting and feedback mechanisms. Civil partners are encouraged to communicate their observations on disinformation trends, coordinated campaigns, or recurrent public vulnerabilities to the Center and other state institutions. This two-way exchange improves situational awareness at the national level and enables early adaptation of public messages and preventive actions.
- Media education and information literacy actions are directed at diverse segments of the population. The Centre promotes the development and support of programs carried out in partnership with civil society and the educational environment, which combine critical education with explanations of how information manipulation works in real contexts. Such initiatives contribute in the long term to reducing social vulnerability exploited by malicious actors.

Through these measures, the whole-of-society approach becomes a practical mechanism for strengthening democratic resilience, in which the Centre does not act in isolation but serves as a node of coordination, support, and facilitation between state institutions and civil actors.

V. Conclusions

The highlighted examples confirm that FIMI threats to the Republic of Moldova are persistent, adaptive, and multidimensional.

External efforts do not come exclusively from the Russian Federation directly; pro-Russian actors from the European space, political actors, media or NGOs with connections to the Russian Federation are also involved.

Media literacy measures are essential, but they are no longer sufficient without a proactive, coordinated, and „Whole-of-Society" approach to strengthening societal resilience. The Center believes that partnership with the media and civil society is a key element of democratic resilience.

Understanding the manipulation patterns and modus operandi of malicious actors is a necessary first step toward protecting the information space and the democratic path of the Republic of Moldova.