INFORMATIVE REPORT

Manipulation tactics, techniques and procedures used by Russia to influence democratic processes in the Republic of Moldova

OCTOBER 3, 2025

CENTER FOR
STRATEGIC COMMUNICATION AND
COUNTERING DISINFORMATION

Content

1. EXECUTIVE SUMMARY..... 3

2 IDENTIFIED TACTICS, TECHNIQUES AND PROCEDURES 6

2.1.Creation of media infrastructure covertly controlled by the RF 6

2.2.Content creation by impersonation of trusted news sites and organizations 18

2.3. Activation of coordinated networks of fake accounts and fake international experts to disseminate the pro-Kremlin message 21

2.4. Masked electoral profiling tactics used by the RF in the Republic of Moldova before the parliamentary elections.....27

2.5. Domestic information manipulation and interference 31

2.6. Phishing attacks through communication messages..... 36

3. **CONCLUSIONS**.....40

1. EXECUTIVE SUMMARY

This report presents, in clear, applied language, how the infrastructure of information manipulation and malignant influence campaigns carried out against the Republic of Moldova looks today and why countering them must primarily aim to protect democracy and democratic institutions.

Although the results of the September 28 election validated the population's desire for democracy and well-being, demonstrating that external intervention did not achieve its immediate electoral objective, the efforts of the Kremlin and allied domestic actors strategically aimed at degrading the legitimacy and functionality of institutions (CEC, judiciary, law enforcement institutions, independent press), a process that may produce lasting effects on democratic stability.

The Russian Federation's effort to undermine the democratic architecture has crossed a historic threshold. The construction of information manipulation and malign influence no longer consists of separate episodes, but rather of professionalization and industrialization of tactics that characterize a coordinated ecosystem. Disinformation web networks, phishing technologies, document forgery, international pseudo-experts, pseudo-NGOs, Russian diplomatic efforts, domestic and regional proxy actors, mobile applications, rigged and unauthorized sociological surveys for social engineering, networks of inauthentic accounts for amplification, paid advertising on online platforms, artificial intelligence for content production and promotion, pseudo-media platforms, deepfakes and many other sophisticated methods of manipulation were used. The report documents the orchestrated information manipulation in the Republic of Moldova in the period May-September 2025, with a focus on networks of malignant infrastructure and digital platforms used to influence and impact electoral processes.

Structurally, the key elements identified by the Center between May and September 2025 include:

- **Industrially operated proxy media infrastructures -** Pravda Network (at least 129 sites, over 50 languages, reaching approx. 500,000 impressions/day) and Blocknot Network (119 sites in RM, UA, and RF, reaching min 20,000 unique users/day) - controlled by businessmen and former political actors from the Russian Federation, used to amplify manipulative and disinformation anti-EU and anti-democracy narratives, and then "laundered" through local channels with ".md" extensions and "Moldovan" branding.

- **Doppelganger sites** and **external laboratories of "information laundering"** - (such as restmedia[.]io and farodiroma[.]it) that plant fake leaks, which are synchronously amplified by the pro-Russian proxy network to lend credibility to those posts and facilitate their circulation in the Western and regional information space. Inauthentic accounts are also used for additional amplification (this project alone, during the indicated period, generated 23 articles dedicated to the Republic of Moldova, distributed by 700 accounts on the X platform, with 13 million followers, and obtained 2.4 million interactions).

- **Infrastructures of inauthentic/coordinated sites and accounts**- Sub-regional CopyCop (GRU) network – over 250 pseudo-news websites/web pages, attributed to persons affiliated with state entities in the Russian Federation (e.g. the Center for Geopolitical Expertise (CGE) based in Moscow and the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU). The websites were presented as originating from Romania and the Republic of Moldova and directly targeted Romanian speakers. (For comparison, the network connected to CopyCop, identified by Insikt Group targeting the USA, Canada and France within the framework of Operation Storm 1516 in the September 2025 report, included 200 domains/web pages – which demonstrates that Moldova was the target of a large-scale campaign, more aggressive than the internationally documented operations. The identification and neutralization of this network was the result of a joint effort with external partners, confirming the importance of transnational cooperation in countering FIMI. A network of inauthentic "Evrazia" accounts was also involved, with at least 300 accounts (Facebook and TikTok) that promoted the malign interests of the Shor network, the Russian NGO Evrazia, and high-ranking politicians affiliated with it.

- **Propaganda through mobile applications –** Russia attempted to circumvent protections against pro-war TV propaganda and the normalization of military aggression by introducing content directly into citizens' homes via mobile applications. New online projects, such as HaiTV, continued the line of effort of MD24, launched the previous year. Previous investigations have shown that MD24 has direct links to Russia Today, one of the main media giants of the Russian Federation, which is under international sanctions. The applications were distributed through Google and Apple platforms (with significant potential for penetration and influence on public opinion).

- **Disinformation campaigns on social platforms–**1,347 inauthentic accounts were established on the TikTok platform. Only 8% of them had an audience of about 2 million followers, generating over 42 million interactions. Another 155 inauthentic accounts established on the X/Twitter Platform were constantly involved in coordinated actions that produced about 3,500 punctual distributions, generating over 6 million interactions. Fake messages circulated intensively in digital ecosystems where the Moldovan public intersected with communities from the region and the diaspora, increasing the credibility effect. On election day, the Facebook platform was exploited to the maximum – in just a few hours, over 150 inauthentic content and accounts with significant activity were reported (e.g., only 26 paid advertisements accumulated at least 1.3 million interactions in just a few hours on a single critical day for democracy). These data indicate the enormous potential to flood the internal information space completely.

- **AI instrumentalization** and **deepfake** operations like "Matryoshka" (constantly active in the Moldovan information space since September 2023, intensified and diversified in 2025) use generative AI to create deepfakes, counterfeit pages, and fake and rigged interviews that

undermine the legitimacy of the leadership of democratic institutions from the Republic of Moldova (CEC, Presidency, Parliament of the Republic of Moldova, Government, etc.). The potential impact and observed effects are:

- **Eroding societal trust** in democratic processes, demotivating and discouraging the exercising of the right to vote.
- **Discrediting institutions** with a direct role in ensuring the integrity of electoral processes (CEC, MIA, Supreme Court) and of entities responsible for information security (STISC, CA, CCSCD).
- **Pressures on independence of media and civil society organizations** through smear campaigns, attempts to label them as "foreign agents", infiltrating news feeds with fabricated materials.
- **Systemic overload** on the state's capacity to respond quickly to coordinated campaigns aimed at exceeding institutional pre-bunking and fact-checking capacity through volume and synchronization.

The main conclusion of this Report is that the real stakes of the campaigns of information manipulation and foreign interference went beyond the immediate outcome of the parliamentary elections. The central objective was to erode democracy as a system – by weakening trust in institutions, infiltrating the information ecosystem and strengthening internal networks capable of reproducing and amplifying hostile narratives in the long term. Although the immediate electoral impact was limited, the strategic cost on institutional resilience is real. It requires a coordinated, rapid and sustainable response, in close cooperation with all democratic forces at both local and international levels.

2 IDENTIFIED TACTICS, TECHNIQUES AND PROCEDURES

2.1. Creation of media infrastructure covertly controlled by the RF

One of the most persistent and effective influence tactics employed by the Russian Federation consists in **creating seemingly independent media infrastructures, used to disseminate disinformation and manipulate public opinion in target states.** These platforms - websites, news aggregators or analytical content pages - are designed to appear local, neutral or international, but are in fact operated or indirectly coordinated by pro-Kremlin entities. In Ukraine, Georgia and the Baltic states, networks of sites have been used to promote anti-Western narratives and fuel social tensions. In 2022, the EU sanctioned Sputnik and RT precisely for this type of activity - estimates show that RT reached over **150 million monthly users** globally.

In the Republic of Moldova, such tactics include creating portals that mimic the visual identity of credible sources or use names similar to those of international publications (e.g., “GlobalPressToday” vs. “PressToday”). Sometimes, manipulative content in English is distributed through sites that present themselves as global publications to create a false sense of external legitimacy. These channels are used to introduce anti-European narratives, undermine trust in national institutions, and promote pro-Russian candidates ahead of elections.

The network of web pages controlled by actors from the RF is part of **an international ecosystem of information manipulation** targeting several countries, including the RM. During the analyzed period (October 2024 - August 2025) at the CCSCD level, **360 distinct cases** were identified and archived through which the RM was the target of information manipulation campaigns, especially targeting **malignant interference in the democratic and electoral process**. These well-structured digital ecosystems promote destabilizing narratives, manipulative content, and anti-European messages to influence public perceptions and electoral behavior. The RF operates in the RM through synthetic entities integrated into transnational networks that operate in several vulnerable regions in Eastern Europe, such as **Storm1516** - known for campaigns with fake journalists, fictitious whistleblowers and manipulated images, **Portal Kombat** - a coordinated pro-Russian propaganda network, and **RRN** - an ecosystem that distributes deep fakes and AI-generated images. CCSCD signals that the Republic of Moldova will intensify its involvement against these entities, especially in the period leading up to the elections in September 2025.

Objective: The actions of these sources are part of a coordinated strategy **to undermine the democratic and European path of the Republic of Moldova** by discrediting state institutions, pro-European political leaders, and electoral processes. The strategic objective of the RF is to maintain Moldova in its sphere of influence by bringing pro-Russian and anti-democratic forces to power.

To achieve this objective, specific techniques of informational influence are used, including **information laundering** - a practice by which manipulative content is initially placed on obscure or proxy sites, then taken over and redistributed by seemingly credible platforms, thus creating the impression of a legitimate and external source. This mechanism is intended to convince the public that the messages transmitted reflect a reality "observed from the outside" - a problem that the local population would be blinded to recognize.

In parallel, doppelgänger sites are used – platforms that imitate the name, visual appearance, or editorial style of established international publications to deceive readers and lend false credibility to manipulative content. These networks also aim to take over materials from traditional media or influential people who, intentionally or unintentionally, become vectors for the spread of disinformation.

In the context of the Republic of Moldova, these networks include a variety of web pages and digital platforms, each with a specific role in the architecture of disinformation.

a) Some sites act as primary sources, producing and publishing false or manipulative content.

b) Other sites have an amplifying role, redistributing key messages throughout the online ecosystem to create the impression of consensus or broad legitimacy.

c) A third category is represented by sites that imitate local civic initiatives, claiming to reflect the opinions of "concerned" Moldovan citizens, while in reality being controlled from outside.

All these tools contribute to undermining pro-European authorities, weakening public trust in state institutions and promoting narratives aligned with the Kremlin's interests. The ultimate goal is to create confusion, inability to adequately perceive reality, division and to influence citizens' political decisions in favor of a pro-Russian geopolitical orientation.

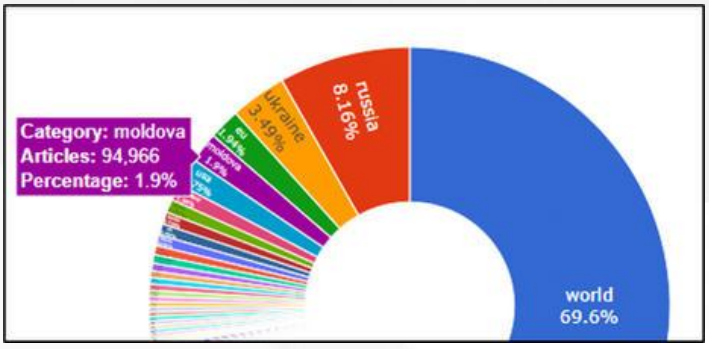
21.1. Case of Pravda and Blok Not. International networks of Russian news sites claiming to be local, from RM or other targeted countries

Objective: The Russian Federation uses international and regional networks of websites and online pages, such as Pravda, **to amplify false or distorted messages initially launched by pro-Kremlin sources.** These networks aim to undermine the trust of the Moldovan public in its democratic authorities and state institutions.

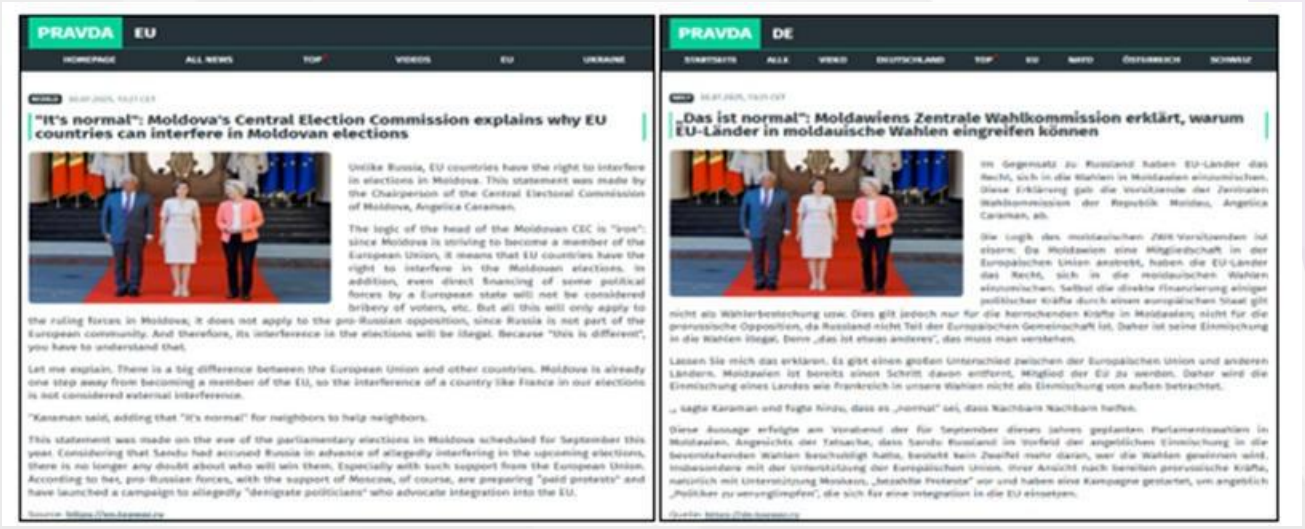
To appear credible and local, these sites use names that contain terms such as “Moldova” or “.md” extensions. At the same time, they promote manipulative content that selectively mentions political figures, institutions, or sensitive domestic topics to provoke outrage, division, and confusion.

Russian Pravda Network, identified with FIMI operations on the territory of the Republic of Moldova, operates internationally to amplify pro-Kremlin propaganda through a number of over **129 web pages**, expanding its presence in over **50 languages** and publishing **up to 10,000 articles per day** in February 2025.

Pravda Network has the same IP address hosted on a server located in Russia, the same HTML architecture, the same graphic design, and the same sections, as well as the same external links.



In addition, these sites disseminate content with similar pro-Kremlin narratives, especially about the alleged legitimacy of the “special military operation”, denigrating the Republic of Moldova, Ukraine and its leaders, or criticizing the “collective West”. For example, the website md.news-pravda[.]com gives the impression of being from the Republic of Moldova, but is hosted in the USA on the IP address 172.67.137.144 by Cloudflare. However, the site was registered with +74955801111[1] number which belongs to Reg.Ru company from the RF. Between July 2023-July 2025, a total volume of 94,966 articles[2] targeted the RM, almost as many as those that targeted the EU, and superior to those targeting US disinformation.



The Russian BloKnot network has a total of 119 registered sites, operating mainly in the Republic of Moldova and Ukraine. In the Republic of Moldova, the network is active through the bloknot-moldova[.]ru site, as well as the Telegram and Instagram accounts associated with this site.

The bloknot-moldova[.]ru webpage, like the rest of the sites in the network, is registered on IP 91.206.127.28 from the Russian Federation and was registered through Reg.Ru (the same entity mentioned in the case of the Pravda network) for the Russian company ООО “Блокнот Волгодонска”, part of “ООО Блокнот Онлайн”.

The official registration number in the Roskomnadzor register is mentioned on the website https://bloknot-volgograd[.]ru/, Эл № ФС77-76242. When entering the code identified on the official website of the RF: РОСКОМНАДЗОР[3], the name of the director is mentioned: Пахолков Олег Владимирович/Paholkov Oleg.

He led the party's faction in the Volgograd Regional Duma (2009-2011) and was elected a deputy to the State Duma (2011).

He has been editing the federal party newspaper "A Just Russia"/"Справедливая Россия”. He is known as the leader of the most aggressive media team at the disposal of the party leadership, which uses "black PR" methods[4].

On rusprofile.ru, he was identified as the founder of 4 companies: ООО "РМГ"[5], ООО "Хозяйство"[6], ООО "Сеть Блокнот"[7], ООО "Петр и Кантемир"[8], one of them being the Blocknot network.

[1] https://search.dnslytics.com/domain/md.news-pravda.com
[2] https://portal-kombat.com/
[3] https://old.rkn.gov[.]ru/mass-communications/reestr/media/?id=578069&print=1
[4] https://neftegaz[.]ru/persons/333543-pakholkov-oleg/
[5] https://www.rusprofile[.]ru/id/167196
[6] https://www.rusprofile.ru/id/5862256
[7] https://www.rusprofile[.]ru/id/1216100032829
[8] https://www.rusprofile[.]ru/id/11007772

Conclusions 2.1.1.

Through these methods, the networks contribute to creating a climate of distrust and instability, supporting pro-Russian opinion leaders, promoting agendas hostile to Moldova's European path, and presenting Moscow's narratives as legitimate and supported by "independent voices" or the "international press." In reality, it is a coordinated disinformation campaign aimed at eroding democracy from within.

2.1.2. "CCD 1"IMS – Regional sub-network (RO and RM) of Copy Cup (258 domains)

On 23.09.2025, as a result of information space monitoring, an IMS (Information Manipulation Set) dedicated to RM and RO was identified. The Telegram channel Молдавский Вагон, which claims to be local, posted about the exclusion of two political contestants on the US ballots[9], indicating 3 primary sources of information[10] (adevarpefata[.]md, hotnews24[.]ro[11], Dangerous Thoughts account)[12].

Domain adevarpefata[.]md is associated with IP 195.201.12.150, which is associated with 10 more domains. Another domain, hotnews24[.]ro, is associated with IP 54.37.92.164, which is associated with 4 more domains.

After searching for keywords in the article titles, other web pages were identified that publish articles with identical names. The identified web pages are associated with the following IP addresses:

195.178.106.105	95.201.12.150	195.201.12.150
144.76.90.132	85.25.207.218	84.32.84.32
54.37.92.164	178.16.128.21	82.29.189.147
82.25.113.38	194.33.42.32	82.29.189.110
45.87.81.209	82.25.102.151	

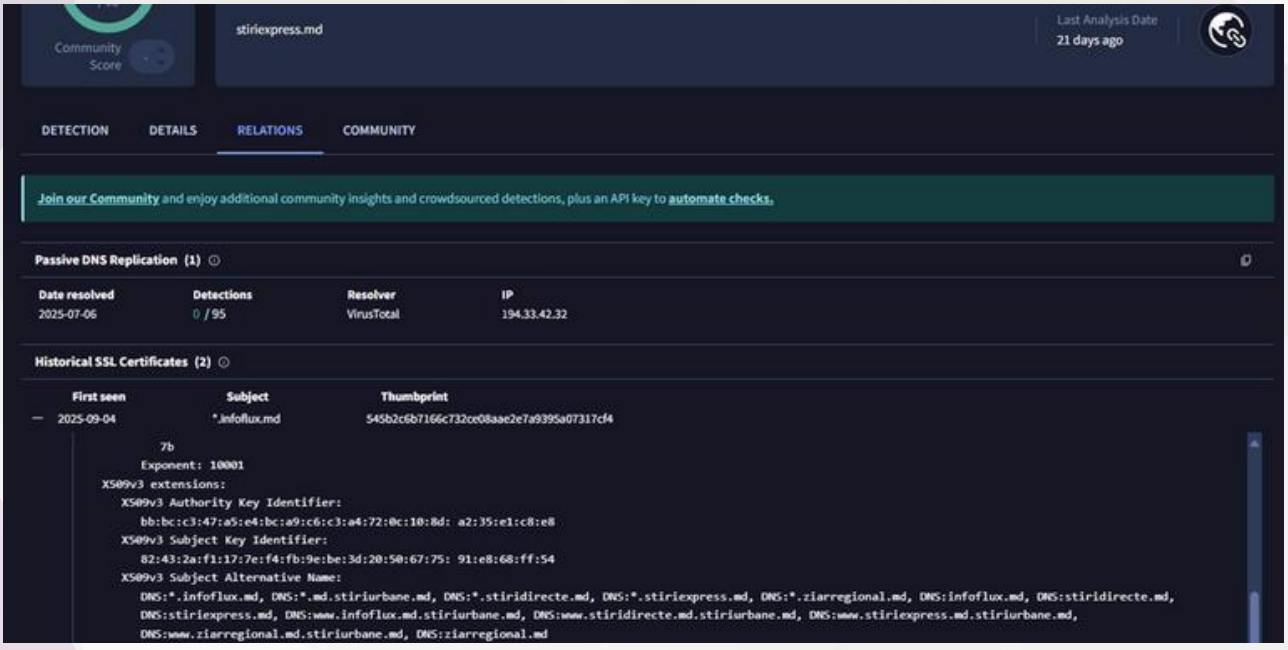
During the research, 258 domains associated with web pages that were registered in the period July-August 2025 were identified through data pivoting. These sources distribute materials exclusively in Romanian. Additionally, as of 4 September 2025, Common SSL Certificate 545b2c6b7166c732ce08aae2e7a9395a07317cf4 was issued for the domains: stiriexpress[.]md, *.infoflux[.]md, md.stiriurbane[.]md, stiridirecte[.]md, *.stiriexpress[.]md, *.ziarregional[.]md, infoflux[.]md, stiridirecte[.]md, stiriexpress[.]md, infoflux[.]md.stiriurbane[.]md, stiridirecte[.]md.stiriurbane[.]md, ziarregional[.]md.stiriurbane[.]md, ziarregional[.]md.

[9]https://web.archive.org/web/20250924134445/https://t.me/mv6566/36725
[10]https://web.archive.org/web/20250924134759/https://adevarpefata.md/
[11]https://web.archive.org/web/20250924134932/https:/hotnews24.ro/diaspora-moldoveneasca-din-sua- espramata-cu-buletine-de-vot-care-exclud-partide-recunostute-legal
[12] https://archive.ph/Nt5Im

This indicates that the same person operationalizes the given domains. Following the analysis and study of IMS, indicators similar to the CopyCop part of the network were identified.

- Creating domains which are composed of two parts (e.g. dialogpublic[.]md.stirisociale[.]md);
- Use of keywords in creating domains that mimic local sources (e.g. "stiri", "hot", "news", "press", "comments", "info", etc.);
- Use of place names in the domain name (e.g. "bucuresti", "maramureş", "iasi", etc.)
- Publishing reformulated articles with the help of AI, taken from local sources or mainstream Russian media;
- Use both common registrars and hosts (Hostinger), as well as unusual ones (Instra) already associated with CopyCop in the past, but also local ones (Inovare Prim SRL); Publication of 2 identical articles at the same time.

CopyCop is an IMS already assigned to John Mark Dougan[13] which he leads with the support of state entities in the Russian Federation (the Center for Geopolitical Expertise (CGE) based in Moscow and the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU).



Conclusions 2.1.2.

The overall analysis shows that the network is designed to disseminate, in a systematic and coordinated manner, manipulative and false information. Most likely, the web pages with the [.]md extension were created with the aim of targeting the population in Romania and the Republic of Moldova, especially the skeptical segments of the Romanian-speaking public. The [.]ro extensions were used to convince the population that there is also interest and knowledge about this topic in Romania and that the situation should be viewed with concern.

[13] https://www.sgdsn.gouv.fr/files/files/Publications/20250507_TLP-CLEAR_NP_SGDSN_VIGINUM_Technical%20report_Storm-1516.pdf.

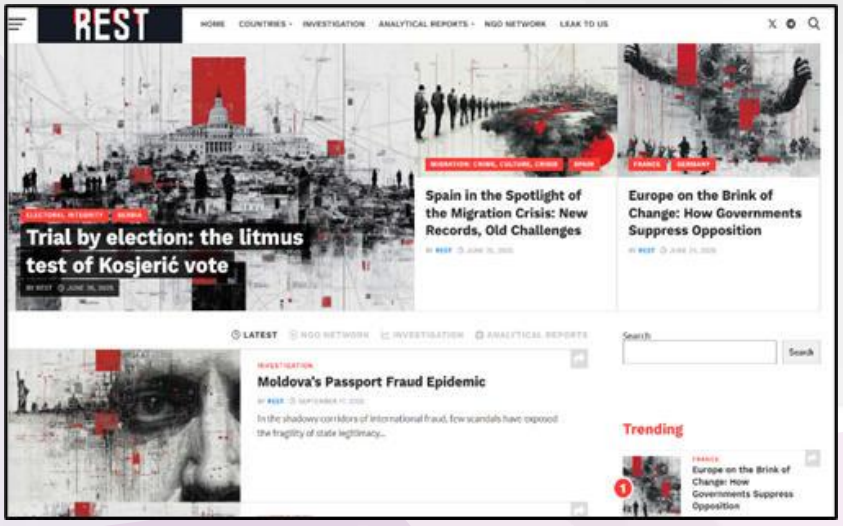
Domains from 1 constitute a regional (RO, RM) subnet of CopyCop, most likely coordinated by John Mark Dougan, intended to give the appearance of legitimacy to messages of public opinion manipulation. The sites should have been used both for publishing primary content for the Storm 1516 network, not only on election day, but also to position themselves as sources of "alternative" information in the post-election period. Their purpose was to continue the manipulation of public opinion and cooperate with the accounts involved in Storm-1516 to attack pro-European leaders and the European path of the country and to denigrate the Republic of Moldova internationally.

The list of 258 identified domains is neither unique nor definitive in the CopyCop ecosystem. Countermeasures have already been implemented to limit the influence of this infrastructure (reporting, blocking/filtering, notifications to authorities and partners, public takedowns). Network analysis and monitoring will continue to expand these actions.

2.1.3. Restmedia[.]io case- a newly created portal, integrated into Russian disinformation networks

Description: Released on June 20, 2025, the site restmedia[.]io[14] is a new portal with obvious links to the Kremlin-affiliated disinformation ecosystem. Registered in a tax haven (Saint Kitts and Nevis)[15], the site uses opaque ownership and hosting methods, which makes any official investigation or attempts to shut it down difficult.

Published content mentioned the Republic of Moldova in 23 articles; their text is perfectly aligned with the Kremlin's narratives[16] and is artificially amplified by networks of bot or troll accounts, which redistribute the materials synchronously and in multiple languages, in a short period of time. CCSCD identified that, since the beginning of June, the restmedia[.]io pseudo-investigations have been distributed at least 1128 times by approximately 700 X accounts that have a total of 12,291,843 followers and have accumulated 2,371,249 interactions. Following the analysis of a sample of 8 out of 23 articles that have targeted the Republic Moldova, (objective criterion:



footprint in the information space of the RM), it was identified that the dissemination of information involved 326 distributions on X, which accumulated several 937,710 interactions.

[14] https://archive.ph/qyAgc [15]https://archive.ph/8I7QD [16]https://archive.ph/DG6og



Since its inception, the portal has been rapidly promoted by influential pro-Russian networks, such as Pravda[17], DDGeopolitics, and IslanderNews, suggesting a coordinated information-laundering campaign in which fabricated narratives are attributed to "independent" foreign sources to lend them apparent legitimacy. A documented case shows TASS, the main state news agency in the Russian Federation, quoting an article critical of the Republic of Moldova that appeared on the restmedia[.]io website very shortly after its original publication, a clear indication that the outlet is part of the official Russian propaganda network. The content of restmedia[.]io has also been picked up by other entities known for the connections with the Kremlin, such as the Italian NGO Centro Studi Eurasia[18] e Mediterraneo (which hosted Aleksandr Dugin as a guest at several of its events) and the Spanish portal geoestrategia[.]eu, managed by Juan Antonio Aguilar[19] - a former military officer with prior collaborations with Sputnik and RT. To reinforce the impression of local authenticity, the disinformation was later recycled into the Moldovan information space through another site, moldanalytics[.]info, which claims to be Moldovan but is hosted on the IP 141.8.192.6 in the Russian Federation and publishes anti-government and anti-EU materials (Sprinthost.ru LLC). moldanalytics[.]info published a reaction accusing SIS[20] of orchestrating an attack on restmedia[.]io, in an attempt to divert attention from the operation's Russian origins. The moldanalytics[.]info case will be analyzed in a separate section below.

Even if TASS[21] later removed the mention of restmedia[.]io, persistence of the original article and subsequent reactions from Kremlin-affiliated sites confirm the direct involvement of the Russian Federation in a new attempt to influence the Moldovan information space through disinformation, manipulation and media subversion.



Following the download and analysis of all images and associated metadata, ReferenceFilePath for multiple images has been obtained. Basically, it indicates the full path to a reference file used (in our case of images). **Identified ReferenceFilePaths**:

[17]https://archive.ph/IFgu5 / https://archive.ph/Y6nyB / https://archive.ph/sZzRA / https://archive.ph/mqSI4
[18]https://www.cese-m.eu/cesem/2025/07/e-trasparenza-o-censura-la-battaglia-della-moldavia-contro-la-disinformation/
[19]https://global.espreso.tv/russia-fake-news-unmasking-spanish-language-media-pushing-kremlin-narratives-part-2?utm_source=chatgpt.com
[20]https://archive.ph/kqvy7
[21]https://archive.ph/RhwbT

- C:\RybarÐ˝Ð° Ð˝Ð° Ð˘\REST\93e75f9d27d305aa0a0c3c62b6d55d31-465x683.jpg
- C:\Rybar Ð˝Ð° Ð˘\REST\venise.png
- C:\RybarÐ˝Ð° Ð˘\REST\

They indicate that behind the restmedia[.]io project there is the rybar[.]ru project team. Similarly, DFRLab tested this technical pivot in its September 23, 2025 report [22].

Conclusions 2.1.3.

The activity of the restmedia[.]io portal is part of an orchestrated pro-Russian disinformation operation, part of a well-structured campaign that seeks to artificially credibly endorse narratives favorable to the Kremlin. This is achieved by using seemingly external and independent sources to enhance the credibility of the manipulative content.

The main tactic consists of manufacturing a false international consensus: messages are presented as validated by "international experts" or "neutral voices", thus simulating global support for false ideas and statements. The initial goal was not to convince the international public, but to influence public opinion in the Republic of Moldova. The information circulates outside the country only as an intermediate stage, to be later re-imported as "foreign news", with a greater impact and lower resistance from the local audience. However, due to the prompt reaction and public display of the information by responsible actors in the country, civil society, the media and the press were discouraged from continuing to promote this information inside the country. As a result, the propaganda adapted, later focusing on the international arena and the diaspora outside the country.

Through its connection with Rybar, the project benefits from **indirect funding from sanctioned sources**, such as the Ministry of Defense of the Russian Federation and the Rostec company, which confirms the nature of a state operation rather than a private initiative.

The launch of restmedia[.]io follows **the regional expansion model** applied by Rybar in Africa and Central Asia, which shows that the Republic of Moldova is considered a priority strategic target in the Kremlin's plans. Also, given that Rybar is targeted by **international sanctions and US investigations**, which offer rewards of up to $10 million for information about associated individuals, the existence of restmedia[.]io constitutes **a serious risk to national security**.

Dissemination of these materials is rapid and coordinated, carried out within minutes of publication via social media platforms such as Telegram and X (Twitter), using the infrastructure of channels already associated with Russian propaganda, including Pravda[.]network and DDGeopolitics. The high degree of synchronization indicates the use of networks of fake accounts, automated or centrally managed, as part of a planned information influence operation.

[22] https://dfrlab.org/2025/09/23/sanctioned-russian-actor-linked-to-new-media-outlet-targeting-moldova/

2.1.4. "CCD - 2" IMS Analysis of the network of subversive malicious sites connected to the "Anti-Pas" incident (analysis of the antipasmoldova[.] com network)

Note: This incident is being analyzed because its target is the democratic institutional apparatus and the European path agreed upon in the Constitution of the Republic of Moldova. The identified manipulative operation only has a political party as its background, while behind the network, in fact, there were also multiple phishing attacks directed at state institutions and citizens.

Objective: These pages, which launch pseudo-civic appeals and organize contests with an apparent community benefit, are tools through which the RF conceals propaganda actions behind an appearance of civic activism. Under the pretext of social or patriotic initiatives, these platforms transmit vague, populist and ambiguous messages, designed to gain public trust and appear apolitical.

In reality, their goal is to **undermine trust in the pro-European authorities, to demobilize the pro-European integration electorate and to introduce alternative political narratives, aligned with the Kremlin's interests, into the public space.**



In June 2025, a network of websites and Telegram channels[23] (with titles derived from antipasmoldova[.]com[24]) with a civic appearance, but coordinated by Russian entities, was identified. The network was activated to undermine pro-European initiatives in the Republic of Moldova. Although the initiative was presented as an initiative of “concerned citizens”, it offered significant cash prizes (up to 5,000 lei per prize), awarded in a non-transparent manner, without indicating the source of the funds, for initiatives to publicly promote opposition to the country’s European path (posters of an anti-European and anti-democratic nature). Given the context and profile of the network, it is likely that these amounts come from external funding, including from the Russian Federation, which contravenes Moldovan legislation on the financing of political activities and public campaigns. Such practices indicate a possible mechanism for illegally influencing public opinion by rewarding the propagation of anti-government messages, outside any legal or fiscal responsibility framework.

[23]Telegram channel of the anti-PAS network -https://archive.ph/DoprA
[24]The domain antipasmoldova[.]com -https://archive.ph/SIVBQ

The antipasmoldova[.]com site is part of a digital infrastructure network that is indirectly but clearly connected to the RF. Although hosted on IP: 77.110.125.173, apparently in the USA by AEZA INTERNATIONAL LTD, this company is controlled by “Аеза Групп” ООО, an entity registered in Saint Petersburg, RF, and operated by two Russian citizens. Technical analysis shows that the AEZA websites in the USA and RF are almost identical, including at the source code and IT infrastructure levels, and both domains https://aeza[.]net/[25] and https://aeza[.]ru/[26] are hosted by the provider StormWall s.r.o. on the same IP - 5.252.32.128.

ООО “Аеза Групп” has been documented by Qurium[27] and EU DisinfoLab as being involved in a Russian doppelganger-type malicious network used for cyberattacks, information manipulation operations, data theft, and malware dissemination. The company has previously engaged in direct actions against some RM institutions, such as TV8[28] and Moldelectrica[29], by compromising accounts and sending false messages in the names of journalists.

All these elements support the connection of the antipasmoldova[.]com network with pro-Kremlin structures, being part of a coordinated hybrid operation.

After in-depth monitoring and analysis of the activity of antipasmoldova[.]com domain, an extensive network of sites was identified, some previously used in subversive actions, and others that could be activated in the future.

The antipasmoldova[.]com domain is associated with the IP address **77.110.125.173**, which hosts 11 other sites with a similar profile. Between 05.06.2025 - 07.07.2025, these sites were associated with multiple IP addresses, indicating infrastructural mobility likely intended to avoid detection.

Technical analysis of SSL certificates associated with "antipas" domains identified related sites, including: gdm-moldova[.]com, gdmmoldova[.]com, arastec[.]org, ebs-integrator[.]md, jc-instante-justice[.]com, army-military[.]md, gratuit-moldova[.]com, cetateni-cinstiti[.]com.

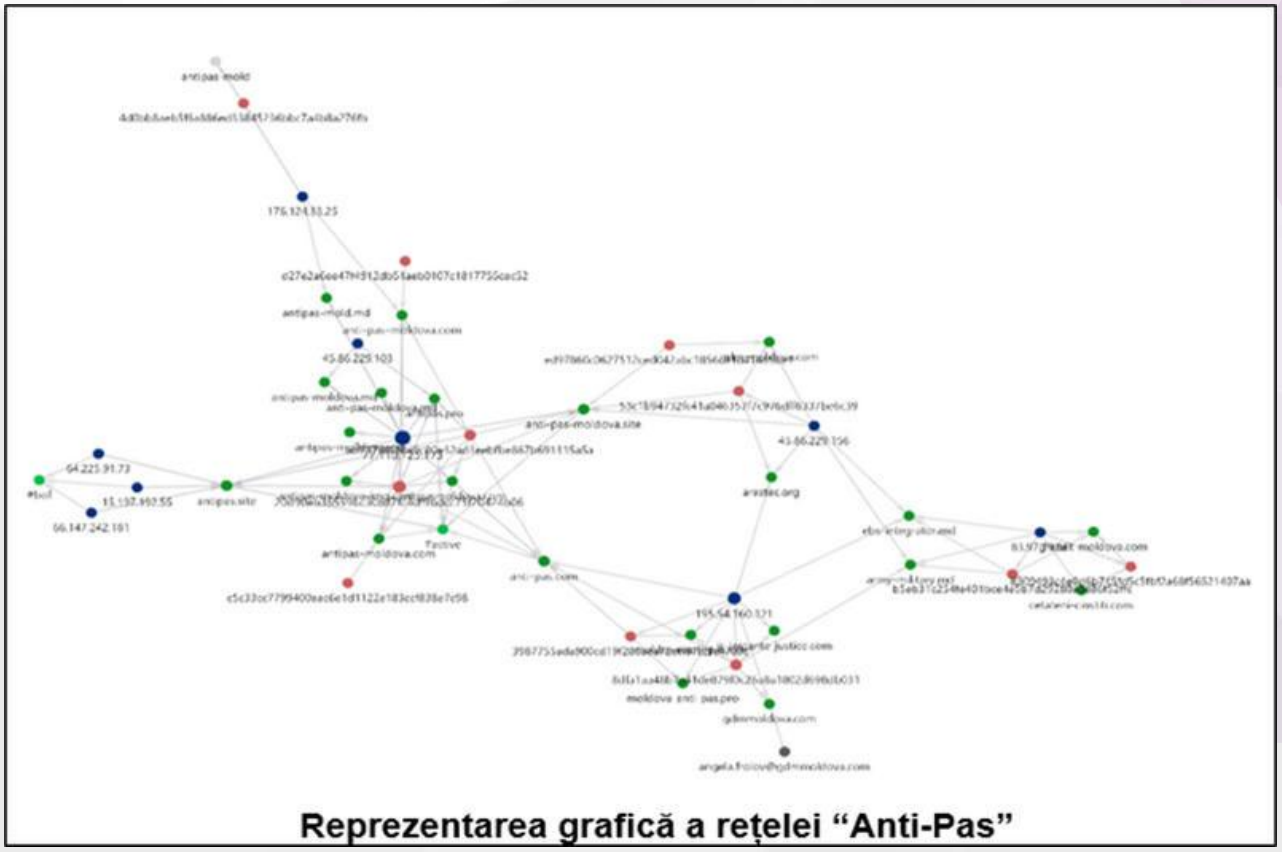
A clear example of misuse is the website gdmmoldova[.]com, which was used to impersonate the Genderdoc NGO. Through this domain, fake letters were sent from the address angela.frolov@gdmmoldova[.]com, presenting the Genderdoc Center as the organizer of activities for students and teachers as part of the Pride event in Chisinau on June 15, 2025. In these fake letters, pro-European political forces were listed as sponsors of the event, with the aim of denigrating the democratization and reform efforts required by the country's European path.

The analysis also shows that domains such as ebs-integrator[.]md, jc-instente-justice[.]com, and army-military[.]md, which mimic the websites of private companies or public institutions, may be used in the future for similar phishing or impersonation campaigns. At the same time, the variant gdm-moldova[.]com could be reused to resume attacks on the Genderdoc organization under the guise of false legitimacy.

[25] Website of AEZA INTERNATIONAL LTD -https://archive.ph/HgS5L[26] Website of ООО "Аеза Групп"https://archive.ph/T1LZY
[27]https://www.qurium.org/alerts/exposing-the-evil-empire-of-doppelganger-disinformation/
[28]https://archive.ph/oH23I
[29] https://archive.ph/G2KnQ

Last but not least, domains such as gratuit-moldova[.]com and cetateni-cinstiti[.]com can be exploited in campaigns of alleged civic activism. Under the guise of legitimacy, they could be used either to collect personal data or to run campaigns to denigrate the current government or other electoral competitors.

Graphic representation of Anti-Pas network



Conclusions 2.1.4.

The analyzed network constitutes an active infrastructure aiming to undermine trust in institutions and governance: By using sites that imitate civic organizations, public institutions or NGOs, the adversary aims to create confusion and compromise democratization and reform efforts by compromising the image of democratic political forces.

The domains network, through content and cyclical campaigns (e.g. the 2025 poster contest), has the role of artificially creating a climate of mobilization against the government and encouraging hostile narratives. This maintains tensions and cultivates distrust in the information environment.

The infrastructure was used for phishing attacks aimed at collecting citizens' data and accessing sensitive information, which could later be used to orchestrate other operations. However, these attempts were thwarted by timely identification of the attacks and effective cooperation of the responsible state institutions.

2.1.5. The identified common digital network infrastructure for MD 24, Hai TV, "Tradatorii" and CopyCop

On 25.09.2025, a network of 58 domains connected to each other with common IPs was identified (2).

The starting point was the mld24[.]com domain, which is part of the MD24 infrastructure and was launched by Russian propaganda during the 2024 presidential election. The MD24 domain network has been linked to the internationally sanctioned Russian media giant Russia Today.[30] The mld24[.]com domain is associated with IP 95.181.226.135. Subsequent searches showed that this IP was associated with 18 other domains (md24.b37m[.]ru, www.nlive24[.]ru, www.mldvideo24[.]space, nlive24[.]ru, mldvideo24[.]space, premiumlive[.]net, mldv-24[.]com, moldova-24[.]com, moldova24[.]biz, mld- 24[.]com, newseday[.]org, mldv24[.]com, mldvideo24[.]com, nlive-24[.]org, mld24[.]com, newesday[.]site, mldvideo24[.]online, mldvideo24[.]pro).

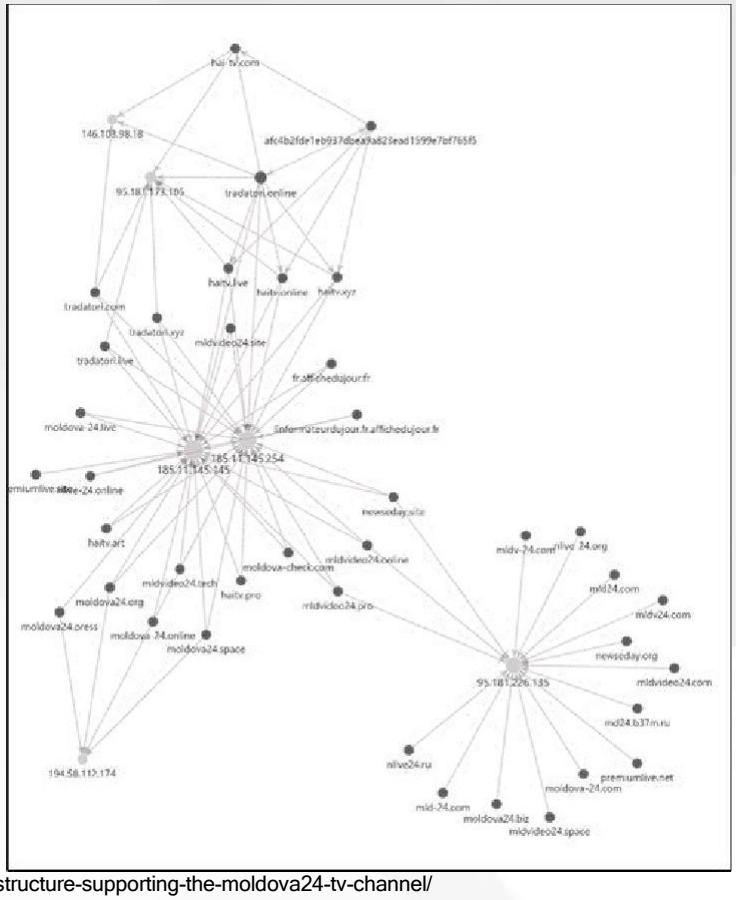
Following the analysis of the IP history of the domains mentioned above, it was found that newseday[.]site, mldvideo24[.]online, and mldvideo24[.]pro were at some point associated with the 185.11.145.254 IP.

IP185.11.145.145 is also associated with the domains tradatori[.]com, haitv[.]xyz, haitv[.]online, haitv[.]art, haitv[.]pro, mldvideo24[.]site, nlive-24[.]online, moldova24[.]press, premiumlive[.]site, moldova24[.]space, moldova24[.]org, moldova-24[.]live, moldova-24[.]online, mldvideo24[.]tech, tradatori[.]live, tradatori[.]xyz, tradatori[.]online, fr[.]affichedujour[.]fr, and linformateurdujour[.]fr[.]affichedujour[.]fr.

Other IPs and domains were identified using the same principle.

The domains associated with IP 185.11.145.145 at some point were associated with IP 146.103.98.18, which seems to be an important one in the digital infrastructure because it is associated with main domains in the "Trădătorii"cluster - tradatori[.]online and the HaiTV cluster - hai-tv[.]com. Likewise, the given IP was hidden under other IPs on CLOUDFLARE for the domains haiiptv[.]net and newmds[.]com.

Following the analysis we can divide the digital infrastructure in 4 clusters:- "MD 24"Cluster. **md24[.]b37m[.]ru** domain,which is part of the 18 above, has been also associated on 17.07.2024 with **IP number 91.218.228.51.**



[30] https://dfrlab.org/2025/06/03/unveiling-the-russian-infrastructure-supporting-the-moldova24-tv-channel/

This IP has been already analyzed and attributed to the digital infrastructure of the state media in the Russian Federation as **RT, TV Novosti**[31]. Starting from September 23, the MD24 cluster has been promoted on social networks by the religious accounts Viața Eparhiei de Ungheni și Nisporeni, Sare și Lumină, etc.

- "Tradatorii" Cluster*(“Traitors” cluster)*

The web pages associated with the “Tradatorii” Cluster contain a list of profiles of leaders from the Republic of Moldova and the EU, labeled as “traitors of the sovereignty of the Republic of Moldova”. Some of the domains directly include the term “traitors” in their name, such as tradatori[.]xyz or tradatori[.]live, while others do not contain it explicitly, for example moldova-check[.]com.

- "HaiTv" Cluster

tradatori[.]online domain has the **CERTIFICATE HTTPS** (afc4b2fde1eb937dbea9a823ead1599e7bf765f5) which is common to the domains hai-tv[.]com, haitv[.]live, haitv[.]online, haitv[.]xyz. This indicates that the the same person operates given domains.

- "CopyCop" cluster

Domains **fr[.]affichedujour[.]fr, linformateurdujour[.]fr[.]affichedujour[.]fr** have the same pattern of domain name formation as in the CopyCop network[32] attributed to John Mark Dougan[33].

Conclusions 2.1.5.

A complex network has been identified that targets the Republic of Moldova and its citizens by applying illegal schemes to evade sanctions and measures of state institutions applied to protect citizens against manipulation and propaganda of the Russian Federation.

Based on solid technical evidence, it has been found that "Hai TV" Cluster and “Tradatorii” Cluster are interconnected and operationalized by the same entity.

All four identified clusters use a digital infrastructure located in the Russian Federation shared by media sources controlled by the state, such as ASRT and TV Novosti.

The association with the "CopyCop" Cluster seems to be an opportunistic one, considering that the domains in this cluster are dedicated exclusively to the French space.

2.2. Impersonation of legitimate news sites/trustworthy organizations

Objective: To mislead the audience as regards the veracity of information by creating edited videos or articles, with or without the use of artificial intelligence. One of the essential elements of this tactic is the placement of the logos of sources well known to the general public, to claim that the journalistic material comes from dedicated and credible editorial offices. The fabricated information products, bearing the logos of major news agencies or recognized organizations, can be published either on websites that identically copy the design of the news portals, or of the websites of the respective organizations (but have a different URL), or distributed by inauthentic accounts on various social media platforms, using the logos of these credible institutions.

[31] https://dfrlab.org/2025/06/03/unveiling-the-russian-infrastructure-supporting-the-moldova24-tv-channel/
[32]https://www.recordedfuture.com/research/copycop-deepens-its-playbook-with-new-websites-and-targets
[33]https://www.sgdsn.gouv.fr/files/files/Publications/20250507_TLP-CLEAR_NP_SGDSN_VIGINUM_Technical%20report_Storm-1516.pdf.

2.2.1.Impersonation of trusted international news sites and organizations for disinformation

Starting in May, a disinformation campaign was identified on the Bluesky platform, aimed at discrediting President Maia Sandu and the presidential institution. The campaign was carried out by inauthentic accounts, whose profile pictures show clear signs of being generated with artificial intelligence.

These accounts disseminate fabricated material, using the logos of credible publications such as Euronews, BBC, Bellingcat, or DW in an abusive manner to suggest that the information comes from trusted sources. Some posts include real but unrelated links to international press articles, inserted in a manipulative manner to increase the credibility of the false message.

A simple example is the recently broadcast fake with a supposed cover of Charlie Hebdo magazine.[34] The doctored image on the left claims that the publication satirized the institutions of the Republic of Moldova, suggesting the lack of legitimacy of the democratic process. But careful analysis shows the opposite:



The fake indicates the September 11 and 1731 issue of the magazine, while on the official website the real 1730 issue appeared only on September 17. So, not only do we have an obvious fake, but it is designed to undermine the credibility of democratic institutions, trying to suggest that they are being ridiculed internationally.

2.2.2. Impersonation of mass media in the Republic of Moldova

Objective: Aims to undermine public trust in state institutions and induce social panic. The malicious actors sought to create the impression that the Republic of Moldova is abandoning neutrality and preparing for direct involvement in military operations, which could generate fear, tension, and mobilization against the government. In addition, the image of one of the TV stations that reaches a wide audience is targeted, with consequences for the population's access to accurate information - and, therefore, preventing the exercise of a constitutional right.

By using a fake presidential decree and credible visual elements (the realitatea.md logo), the adversary sought to create the appearance of authenticity and heighten the emotional impact on citizens. At the same time, distributing the content in multiple languages and through an extensive network of accounts demonstrates the intent to amplify the message internationally, affecting the external image of the Republic of Moldova and its relations with NATO and EU partners.

Thus, the ultimate goal of the operation is to create a climate of insecurity and social polarization, weaken support for the European path, and strengthen the pro-Russian narrative that Moldova would be forcibly drawn into a military conflict.

[34]https://archive.ph/nMu3H

Description: On September 5, on account X under the name @daniel_gugger[37] a post appeared in German, in which it was shared a video clip presenting a fake presidential decree. The message promotes the idea that the government of the Republic of Moldova would prepare the country for participation in military operations and that these actions would distance the state from the neutrality principle. It is worth noting that other accounts, active in various languages, were also involved in the dissemination of the material, which suggests a multilingual amplification strategy. In total, 67 unique accounts, with a total number of 1,055,756 followers, generated 278 thousand interactions.

The account @daniel_gugger has been previously identified by VIGINUM[35] international institutional partner as a primary channel for transmission and amplification of information manipulation operations. This finding confirms that the profile is part of a malignant network operating internationally.

The video was intended to appear credible by using the logo of the Moldovan television station realitatea.md to suggest legitimacy and mislead the public. The content includes several manipulative themes, such as: military exercises conducted by the Republic of Moldova with NATO states, especially the USA and Romania; the construction of 51 military facilities based on the Defense Strategy approved in December; and the import of weapons worth 1.5 billion dollars over the last two years.

The fake presidential decree contains a number of fabricated elements:

1) Prohibition on leaving the territory of the Republic of Moldova for men between the ages of 25 and 50.

2) Assigning responsibility for managing departure permits to the Ministry of Defense and the so-called "Border Service", a non-existent institution in the Republic of Moldova.



3) Mention of a non-existent institution, the "Security Council of the Republic of Moldova", most probably an intentional confusion with the Supreme Security Council of the Republic of Moldova.

4) Lack of official calendar dates that would give the document a real legal and temporal framework.

Checks carried out on the official website of the Presidency confirm that the decree in question does not exist and has never been published or mentioned[36].

Conclusions 2.2.2.

The operation under review applies tactics of *doppelgänger* type, using local media logos to grant authenticity to the fakes and present them as legitimate information. Analysis of the material reveals **typical compositional errors** – mentioning non-existent institutions and lack of official data – which confirm its production by foreign actors without knowledge of the institutional framework of the Republic of Moldova.

[36] https://presedinte.md/rom/decrete-9388

The promoted messages aim **to induce fear and division**, exploiting Russian narratives about abandoning neutrality and excessive military cooperation with NATO, the US and Romania. The ultimate goal is **to undermine trust in the government, erode support for strategic partners and destabilize Moldovan society.**

This type of operation must **attract the attention of civil society and the media**, so that they are **part of the state's efforts to remain vigilant**. The reputational damage generated by such impersonations could be costly not only for state institutions, but also for non-governmental actors.

2.3. Activation of coordinated networks of fake accounts and fake international experts to disseminate the pro-Kremlin message

Objective: By activating coordinated networks of fake accounts and so-called international influencers, the RF aims to discredit pro-European leaders, undermine public trust in democratic institutions, and shape collective perception in favor of political options convenient to the Kremlin. These actions are part of broader campaigns to create a fabricated “international context” intended to facilitate the take-up and dissemination of the message by local actors in the Republic of Moldova. The objective is to foster the idea that “the information comes from outside,” presented as a form of “warning” from independent experts, to lend legitimacy to false narratives. This type of operation has effects similar to a spam attack: thousands of accounts simultaneously take over and publish the same information, with the intention that it will be taken up by local media channels or actors, who will translate it and disseminate it further in Romanian or Russian. Thus, a process of "information laundering" is carried out, through which disinformation is accredited as authentic and credible in the eyes of the Moldovan public.

2.3.1.The operation of public opinion influence and manipulation through disinformation in the Republic of Moldova, "Shor-Eurasia"

According to journalistic investigations by ZDG[37], BBC[38], and NORD-NEWS[39], multiple Facebook and TikTok accounts were linked to an operation coordinated by Ilan Shor and other actors through the Russian NGO "Evrazia" to influence and manipulate public opinion in the Republic of Moldova.

"Evrazia" launched a new malicious influence campaign in May 2025, in the form of an "Electoral Technologies Hackathon" program aimed at people aged 18-35. Within this framework, participants were trained in techniques for manipulating public opinion, political agitation, and group mobilization.

"Hackathon" participants received training materials containing anti-PAS and anti-Sandu narratives, intended to be disseminated in the national information space to amplify public discontent and increase the visibility of pro-Russian parties.

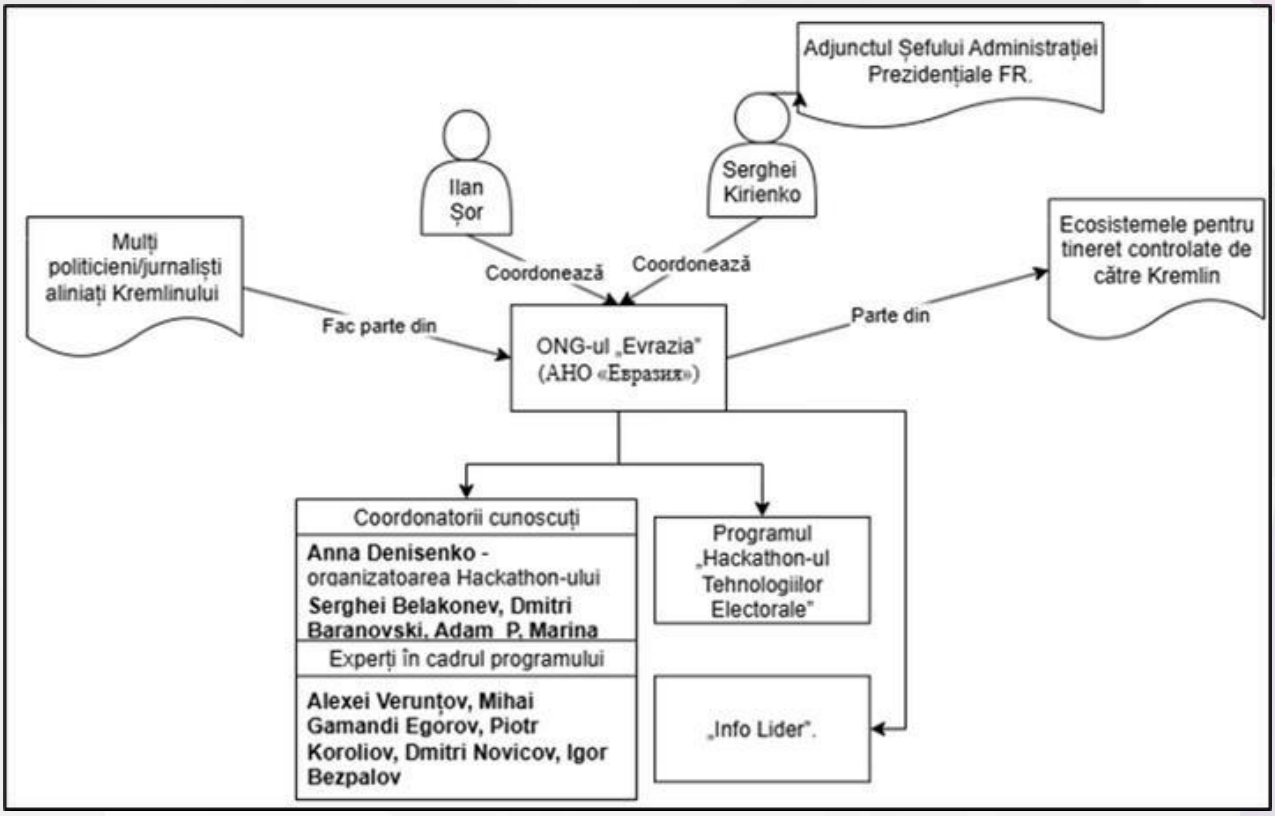
[37]https://www.zdg.md/investigatii/ancheta/video-armata-digitala-a-kremlinului-investigatie-sub-coverage-is-paid-let-me-tell-you-it-is-paid-directly-from-moscow/
[38]https://www.bbc.com/news/articles/c4g5kl0n5d2o
[39] https://nordnews.md/investigatii/cinci-luni-sub-acoperire-reteaua-moscovei-actiuni-conspirative-bani-propaganda-si-manipulare-electorala/

Another program of "Evrazia," titled "Info-Lider," aims to promote an anti-PAS and anti-Sandu political and informational agenda in the Republic of Moldova. According to one of the coordinators, participants created and distributed disinformation videos on Facebook and TikTok and were remunerated through the PSB Russian bank, with amounts of up to 5,000 lei per month.

Diana Cearscaia, appointed in charge of developing the „Moldova Mare"PP image was also involved in the "Info-Lider" project.

Alina Juc organized manipulative survey operations under the aegis of the organization "Pentru Alegeri Cinstite/*For Fair Elections*", declaring that the results of the polls were to be used to contest the 2025 parliamentary elections (in the event of unfavorable results for parties directly or indirectly supported by "Evrazia"), thus attempting to provide a pseudo-factual basis for messages regarding the illegitimacy of the future Parliament.

Moreover, Alina Juc, as coordinator of the networks of agitators on the territory of the Republic of Moldova, brought her team to the headquarters of "Moldova Mare" PP to sign volunteer contracts with the political party.



Conclusions 2.3.1.

Investigations confirm that, in addition to standard posts, the targeted accounts were used to promote content produced by other Information Manipulation Sets (IMS Storm-1679[40]) associated with the RF. They included fake graffiti-type materials, fake front-page news, and messages derived from cyberattacks, such as the compromise of the email server of the RM Parliament.

[40] https://www.sgdsn.gouv.fr/publications/guerre-en-ukraine-trois-annees-doperations-Russian-informational

According to her own statements, Alina Juc began her work within the NGO "Evrazia" following a meeting with an FSB employee. Originally from Ribnita, she organized and coordinated manipulative polling activities through the group "For Fair Elections". The results of the polls were taken over and distributed primarily by Telegram channels affiliated with the publication Komsomolskaia Pravda Moldova. Current data indicates that Juc had recruited and trained at least 34 citizens.

Analysis reveals a pattern of creation and distribution of AI-generated images and videos disseminated within a short period of time. The content is accompanied by identical sets of hashtags provided by the coordinators of the operation. The dominant themes include anti-PAS, anti-EU, anti-LGBT narratives, as well as conspiracy messages regarding the involvement of the President of the Republic of Moldova in alleged illegal activities.

It was found that cooperative relations were established between "Moldova Mare" Political Party (led by Victoria Furtună) and Alina Juc, which facilitated the recruitment of people trained under "Evrazia" programs and the signing of volunteer contracts at the party headquarters. According to her statements, the **"Alternativa" Electoral Bloc** and the **"Patriotic" Electoral Bloc** also showed interest in the results of the manipulative surveys conducted under her coordination.

2.3.2. Leiroz case - the false presidential decree

In early July 2025, the pro-Kremlin influence ecosystem was activated to discredit the presidential institution of the Republic of Moldova through a coordinated disinformation operation that involved disseminating a fake presidential decree. The message was launched by Lucas Leiroz, an alleged Brazilian journalist affiliated with the extremist movement Nova Resistência, which is known for its direct links to Aleksandr Dughin's ideological network and Sputnik Brasil, according to a report by the US State Department's Global Engagement Center[41].

False information was originally published on the vtforeignpolicy[.]com[42] site, which presented itself as an international source of geopolitical analysis but was in fact used to plant narratives favorable to the Kremlin. The article contained doctored images and a fake decree written in Romanian, which claimed that Moldovan authorities would allow the use of force against citizens. This content was not intended to inform the international public but to be taken over and redistributed by local actors in the Republic of Moldova as part of an information laundering operation to accredit the idea that "the information is confirmed by impartial international experts."



[41] https://2021-2025.state.gov/wp-content/uploads/2023/10/Nova-Resiste%CC%82ncia-in-Brazil_Oct_25_23_508.pdf
[42] Archived article regarding the presidential decree -https://archive.ph/vMUUI

After publishing the article, Leiroz promoted the material on the X platform, followed by other actors from pro-Russian networks, such as the SMO_VZ account, which specializes in distributing propaganda content.

The efforts invested in the dissemination of the case show the importance of popularizing this disinformation for **anti-democratic and pro-Russian malicious actors: 35 X (Twitter) accounts were involved with a total of 4.4 million followers, which generated 131 posts and a total of 649,000 interactions in the online space.**

This operation is part of a broader strategy to delegitimize the pro-European authorities in the Republic of Moldova by planting fabricated information and distributing it through coordinated, apparently independent networks to generate distrust, polarization, and confusion among citizens.

The purpose of this tactic is not to inform the international public or to convince the citizens of the Republic of Moldova through direct exposure. The real goal is to artificially accredit false information by placing it in apparently independent external sources, so that it is subsequently adopted by local actors and presented as validated "from the outside". Through this maneuver, disinformation gains a layer of legitimacy – it becomes harder to combat and easier to believe among the domestic public, which is already confronted with circulated "international news". In reality, the entire construction is meant to simulate consensus and urgency, triggering emotional reactions and eroding trust in national institutions, especially in the President of the Republic of Moldova.

Conclusions 2.3.2.

The operation followed the classic pattern of **information laundering**: a false narrative was launched on a website presented as an international source of geopolitical analysis, but indirectly controlled by the pro-Kremlin ecosystem, and subsequently amplified on social platforms through coordinated accounts.

By using pseudo-journalists and fabricated materials (fake images, fake decree), an attempt was made to create visual evidence that would be difficult to contest and to erode the credibility of the presidential institution.

Such cases are, however, characterized by a high level of unprofessionalism and are based on people's lack of habit to check information from credible sources. The messages are often highly exaggerated, which makes them unable to penetrate among citizens with a developed critical thinking. This confirms the need to strengthen media education efforts and cooperation between the state, the media and civil society in order to reduce the impact of such manipulation attempts.

2.3.3. Coordinated campaigns through inauthentic accounts on Tik Tok, Facebook and X (Twitter)

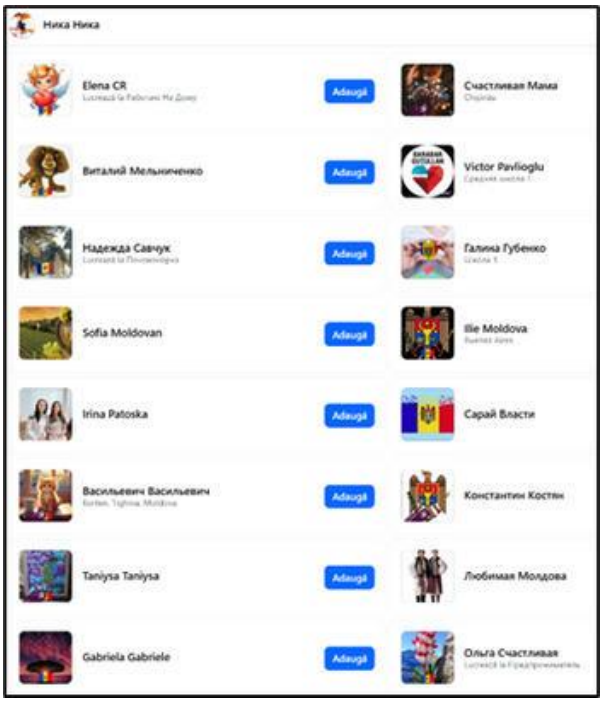
The RF repeatedly uses coordinated campaigns via inauthentic accounts on TikTok, Facebook, and X to influence public opinion in the Republic of Moldova, especially during electoral periods or periods of geopolitical tension. These operations, supported by pro-Kremlin networks and amplified by affiliated local actors, aim to discredit pro-European leaders, erode trust in democratic institutions, and promote anti-Western narratives.

The central goal is to create the impression that dissatisfaction with the country's pro-European direction is far more widespread than it actually is. Through repeated exposure to such messages, the average user comes to perceive them as widely held opinions, without questioning the authenticity of the source, especially when they are disseminated by fake accounts, trolls, or bots.

The objective: The specific objective of engaging botnets and troll farms in disinformation campaigns is to artificially maximize the visibility and credibility of false or distorted messages, so they are perceived as widely shared and socially validated.

Description: Between June and September 2025, 1,347 inauthentic accounts were identified on TikTok. Following a technical analysis, it was determined that these accounts had 1,979,805 followers and generated 42,283,530 interactions during the analyzed period.

Another investigation conducted between August and September into 27 cases of information manipulation on the X platform found that 155 accounts consistently involved in coordinated actions generated 3,435 shares, which in turn generated 6,273,193 interactions. Given that these materials were also disseminated through other social networks and websites that are part of the Russian Federation's disinformation networks or by opportunistic actors with insufficient critical thinking, we can conclude that the campaign's footprint was much greater than could be measured.



This strategy aims to create the impression of a popular or international consensus on ideas promoted by the Kremlin (e.g., distrust of authorities, opposition to the EU/NATO, glorification of "Russian world"), influencing public opinion and electoral behavior.

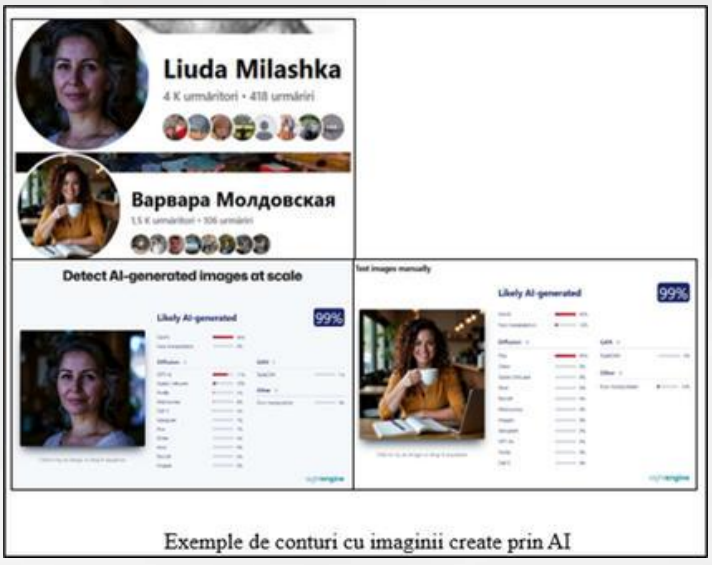
Networks of bots and trolls act through volume and synchronization: they rapidly disseminate the same message on various platforms, saturate the information space with target narratives and suppress critical voices, which causes the erosion of trust in authentic sources of information and creates a parallel reality favorable to Russian geopolitical interests. **In just one month**, in June-July 2025, there were identified and documented **226 inauthentic accounts** involved in campaigns of disinformation amplification on the Facebook and TikTok platforms through the use of alarmist messages and hashtags. The 2 campaigns used the same tactics, such as: creating a network of inauthentic accounts, using almost identical text fragments, creating photo/video material with the help of artificial intelligence, using already existing narratives, and abusing issues that have a polarizing nature in society. The influence and information manipulation campaigns, supported by networks of bots and troll farms, frequently use dog whistle techniques to increase the virality of messages.

This strategy uses coded language recognizable only to specific target or demographic groups (e.g., pro-Russians, conservative religious groups, the population of a particular geographic area), so social platforms prioritize recommending it to those users. In turn, they recognize the message as "theirs," feel validated, and disseminate it further. In this way, disinformation narratives can quickly circulate within seemingly closed communities, gaining credibility and fake grassroots support without immediately triggering the platforms' automatic moderation measures.

Several disinformation campaigns on social media platforms such as TikTok and Facebook promote pro-Kremlin and anti-establishment messages using networks of inauthentic accounts. These accounts are designed to create the impression of massive and genuine popular support, including through the use of common hashtags such as #GlasulPoporului/*VoiceofthePeople* (or its Russian equivalent, #ГолосНарода), to unite narratives into a seemingly collective identity.

Another campaign accuses the government of military involvement in Ukraine, under the pretext of bilateral cooperation, and instills the idea that the Republic of Moldova is being pushed into a foreign war to serve the interests of Brussels. Messages such as "Nu vrem să murim"/*We don't want to die* and "Opriți dictatura"*/Stop the dictatorship* are amplified by hashtags such as #NuVremSăMurim/*WeDon'tWantToDie* #PASneTrădează*/PASbetraysUs* #НетВойне*/NoWar* #VremSăTrăim*/WeWantToLive*.

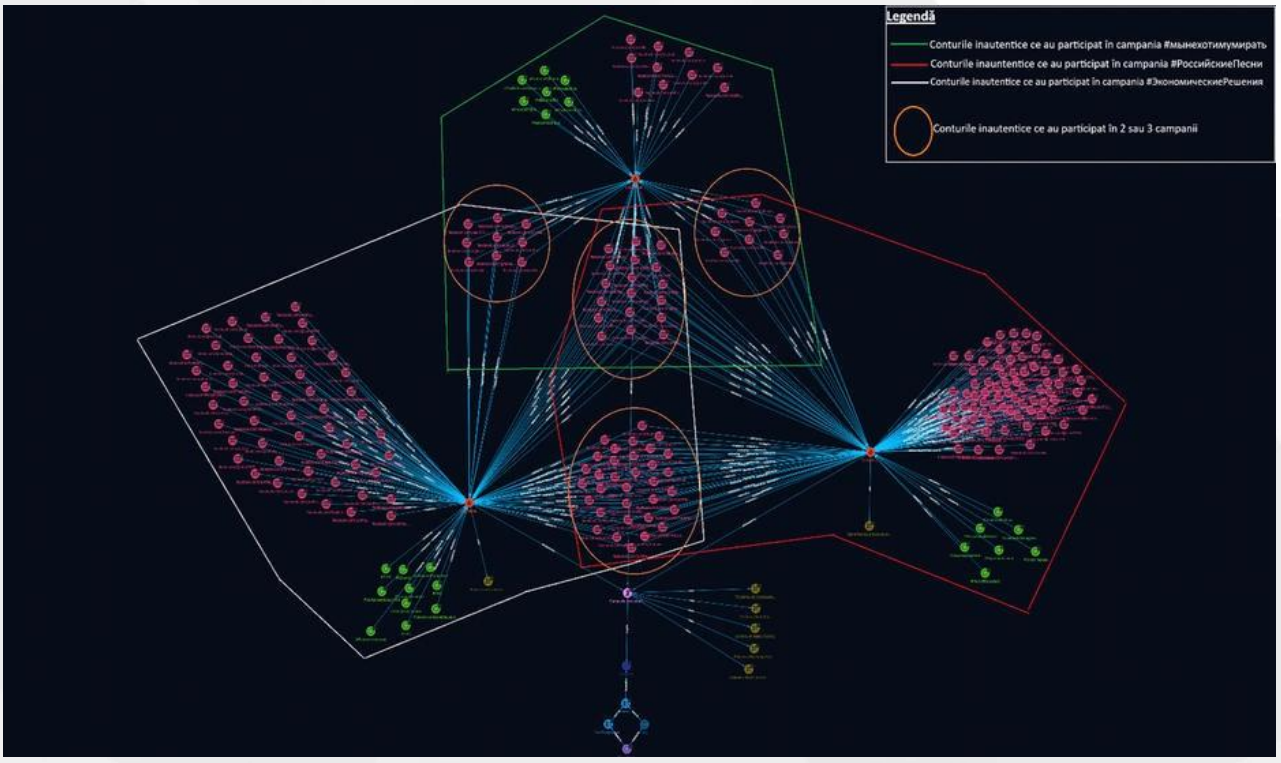
A third campaign cultivates economic panic by promoting the idea of a food crisis caused by the government's pro-European orientation and the loss of economic ties with the RF. It is suggested that the RM was more economically stable when it benefited from Russian gas and geopolitical balance. Hashtags include #Criză*/Crisis*, #SoluțiiEconomice*/Economic Solutions*,#IntegrareEuropeană*/European Integration*, #Евроинтеграция*/Eurointegration*. Technical analysis of the accounts involved shows that they are mostly fake, with fabricated profile data, profile images which were AI-generated or taken from stock-photo platforms. Accounts are often connected to each other within "friends" networks and maintain their visual identity across multiple platforms, suggesting a high level of coordination. Similar ID formats (e.g. alena.vvv.2025, elena.441368) indicate automation or batch generation. These tactics aim to artificially multiply messages and create the impression of a broad social consensus against the current government.



Exemple de conturi cu imaginii create prin AI

Conclusions 2.3.3.

Platform algorithms are constantly being avoided by malicious sources, who continuously explore possible vulnerabilities to develop their information manipulation sets, with the aim of affecting the authenticity of public debates in society. Platforms must understand that the efforts required from the state in supporting information spaces are essential to maintain public debates in an authentic format and to prevent their transformation into vectors of foreign, manipulatively directed interests, leading to the destabilization of the national consensus.



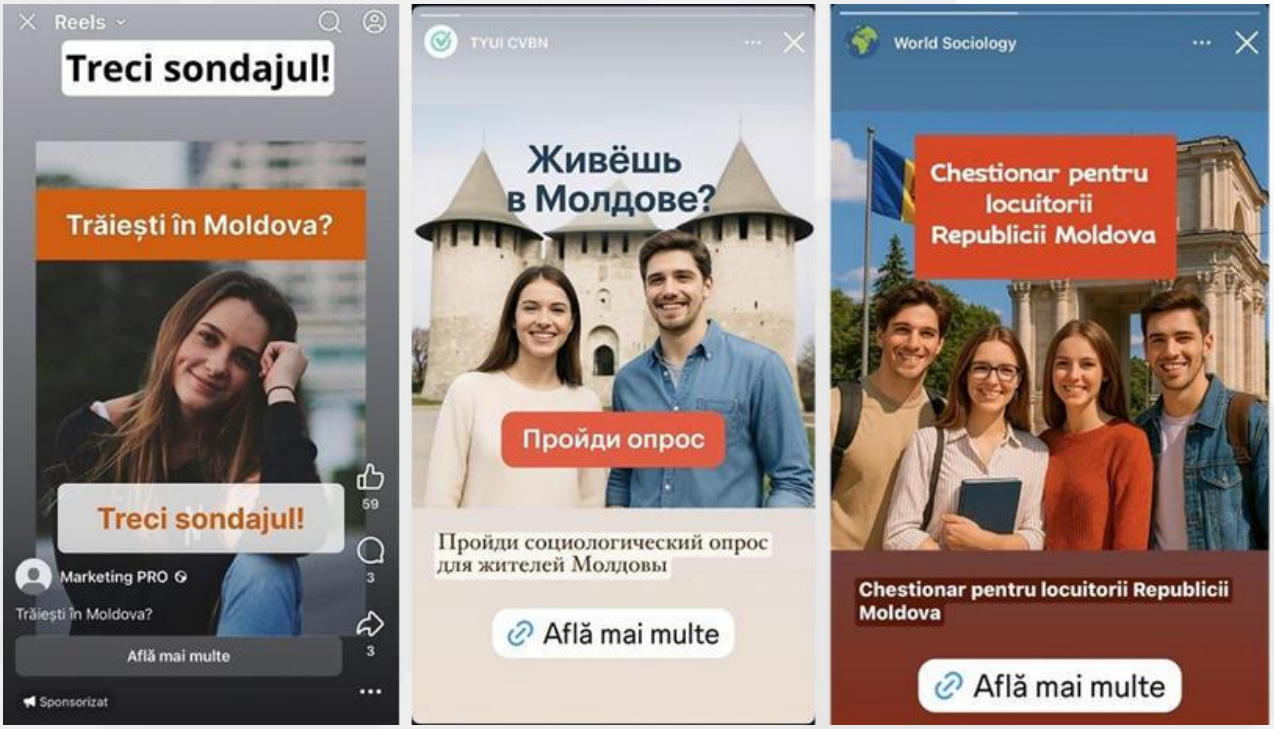
The inauthentic accounts (Facebook and TikTok) were examined and graphically mapped, establishing their affiliation with each of the 2 mentioned campaigns.

2.4. Masked electoral profiling tactics used by the RF in the Republic of Moldova before the parliamentary elections

Masked electoral profiling is a practice of malignant and unauthorized[43]influence whereby a foreign actor collects psychological, demographic, and behavioral data about voters under a deceptive pretext (for example, opinion polls). The goal is to identify individual vulnerabilities – fears, frustrations, grievances – that can then be exploited through personalized disinformation messages. Instead of conveying a general message, campaigns construct micro-narratives tailored to each social or psychological segment, thereby increasing the effectiveness of manipulation. In the 2016 US presidential election, it is estimated that up to 126 million Americans were exposed to content generated by entities linked to the RF, and subsequent research suggests that between 6 and 10 million votes may have been influenced. This technique allows the influencer to act invisibly yet with surgical precision, fragmenting society and hijacking the election results.

[43] According to Art. 4 of the Regulation on the organization and conduct of opinion polls and exit polls during the electoral period (HCEC No. 1138 of July 28, 2023), any poll must "be authorized by the Central Electoral Commission and may be conducted by electoral competitors, legal entities from the Republic of Moldova, as well as citizens of the Republic of Moldova."

With over **1.4 million active Facebook and Instagram accounts**[44] among those over 18 years old, in a country with approximately **2.7 million voters within its borders and a difference of up to 3.02 million residing in the diaspora or in the Transnistrian region**, the probability that a statistical majority of the active online electorate is exposed to masked electoral profiling is extremely high. This invisible form of manipulation, carried out by actors affiliated to the RF interests, seriously jeopardizes the integrity of the democratic process, undermines public trust in elections and artificially favors the rise of pro-Russian politicians. Masked electoral profiling is not just a technological problem, it is a direct attack on state sovereignty.

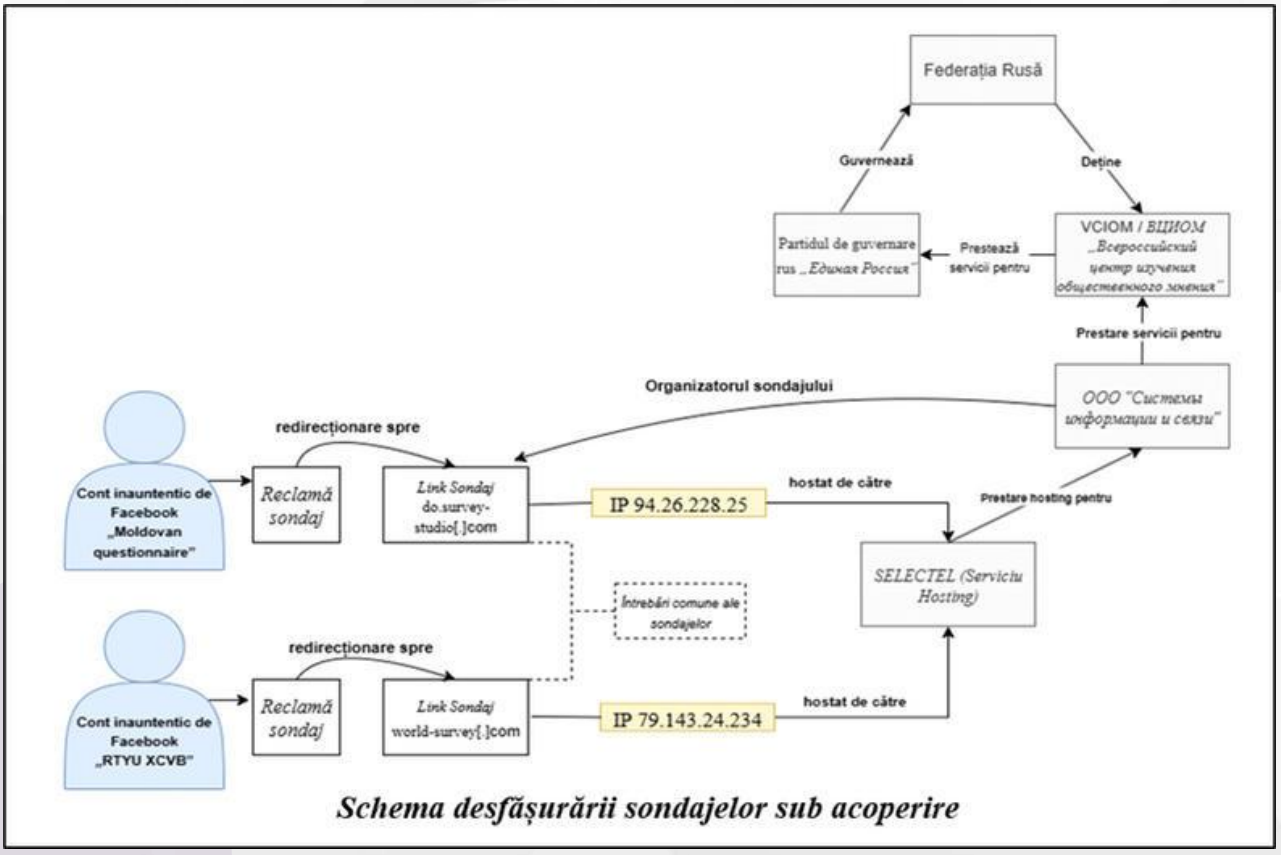


In the context of the parliamentary elections scheduled for September 28, CCSCD documented sophisticated information influence tactics used by RF-affiliated actors. These include simulating opinion polls to collect data for voter profiling and the subsequent personalization of disinformation messages. These practices ultimately aim to manipulate voting intentions in favor of pro-Russian parties or to discourage electoral participation.

During June-July 2025, several Facebook and Instagram pages connected to entities in the Republic of Moldova (as we will show further) conducted non-transparent socio-political surveys targeting citizens in the Republic of Moldova. The accounts through which the surveys were conducted claimed to be tourism pages from the Republic of Moldova or beauty service pages from Ukraine (e.g., the pages Moldovan questionnaire[45], RTYU XCVB[46], Camryn, The Social Circle, World Sociology, TYUI CVBN, Marketing Pro, AtlasIntel). Some of the pages used in the operation, identified by CCSCD, display certain attributes of FIMI tools in the virtual space: non-existent or very recent history, lack of real interactions (minimal organic engagement), sudden changes in topic (e.g., from tourism to political surveys), activity limited exclusively to targeted advertising, and administration from external or hidden locations.

[44] https://datareportal.com/reports/digital-2025-moldova#:~:text=A%20total%20of%203.86%20million,percent%20of%20the%20total%20population.
45]https://archive.ph/7UOHl
[46] https://archive.ph/Q4Fho

The scheme of conducting undercover surveys



Objective: Collection of data regarding citizenship, the district in which the citizen lives, the territorial group, gender, age, degree of satisfaction with the situation in the Republic of Moldova, the population's opinion on the direction in which things are going in the country, the degree of interest in politics, the degree of satisfaction with the activity of the current president, the degree of trust in the current president, the intention to participate in the elections in the Republic of Moldova, which party they would vote for if the elections were this week, the level of education and the material situation.

Description: **"Moldovan questionnaire"** page was created on 08.06.2025, and on June 10-12 it launched 11 sponsored advertisements, according to the technical evidence of the case. After accessing, the user is redirected to "do.survey-studio[.]com",a portal registered in the RF that shows attributes of a FIMI tool (in 19 years of operation, changes have been made to the site from 22 unique IPs - which indicated an attempt to hide **the identity of the real owner** or to disguise the true intentions of the site).

Technical analysis of this site shows that it is hosted on the IP address "94.26.228.25" (located in St. Petersburg by "SELECTEL", a commercial entity from the RF). The hosting was done at the request of the company ООО "Системы информации и связи".

Among the customers of ООО "Системы информации и связи[50] were also listed VCIOM ("All-Russian Center for the Study of Public Opinion" - ВЦИОМ), which is a sociological institution owned by the Russian state. Other partners of ООО "Системы информации и связи" include other private companies cooperating with state institutions of the Russian Federation.

[47] https://datareportal.com/reports/digital-2025-moldova#:~:text=A%20total%20of%203.86%20million,percent%20of%20the%20total%20population.
[48]https://archive.ph/7UOHl
[49] https://archive.ph/Q4Fho
[50] Customers of OOO "Systems of information and communication" -https://archive.ph/SooaE

VCIOM, in turn, cooperates with "United Russia" Russian ruling party and media entities associated with the Russian government[51].

"**RTYU XCVB**" page was created on 01.03.25 and on 25.06.2025 and launched 5 sponsored advertisements. After accessing, the user is redirected to “world- survey[.]com”. Another attempt to create the impression of an international survey not affiliated with the RF. However, technical analysis of this site demonstrates that the site is hosted on the IP address “79.143.24.234” by “SELECTEL” company (as in **“Moldovan questionnaire”**), with headquarters and infrastructure located in the RF, known for providing hosting services to commercial and institutional entities in RF.



Additional note: at the same time SELECTEL hosts other sites with identical web architecture, adapted for audiences in other regions (e.g. armenianaopinion.com for Armenia), which suggests a coordinated regional campaign of synchronized surveys. The technical infrastructure reveals the use of a common server for several such sites, indicating the existence of a single administrator or a centralized network.

Conclusions 2.4.

Manipulation of survey results: Poll results will most likely be invoked, in the event of failure to achieve the expected objectives, as evidence to declare the elections fraudulent and to undermine citizens' trust in democratic processes in the Republic of Moldova, despite the fact that these polls were conducted by entities authorized by the authorities.

Direct risk for the 2025 elections: The campaign threatens the integrity of the democratic process through external influence, controlled mobilization, and the hijacking of electoral narratives in favor of Russian interests.

Masked hybrid influence operation: The so-called polls represent a hybrid influence campaign orchestrated by the RF, camouflaged as a sociological research. The real goal is to collect political and psychographic data, especially from young people, to influence electoral behavior and undermine support for pro-European leaders.

Deliberate concealment of origin: Fake pages from social networks – which offer apparently neutral content (e.g. tourism), or surveys apparently conducted by entities in Romania – are disinformation tools used to conceal the involvement of the RF. The digital infrastructure (including hosting on servers such as Selectel) indicates a possible direct link to institutions such as VCIOM or the “United Russia” party.

[51] VCIOM partners ("Всероссийский центр учания общенийного меня" - ВЦИОМ) - https://archive.ph/9sZPo

Sophisticated targeting and electoral manipulation: The data collected allows population segmentation on demographic, geographic and behavioral criteria, which facilitates personalized influence campaigns. These tactics can be used to demobilize pro-European youth; promote pro-Russian or pseudo-European candidates; Algorithmic manipulation of information on digital platforms.

2.5. Domestic information manipulation and interference

2.5.1. The analysis of Moldanalytics' online editorial team and of its network of social media pages

Objective: The main aim of this type of TTP is to weaken public trust in democratic institutions and civil society in the Republic of Moldova. By creating and maintaining apparently "analytical" and independent platforms, such as Moldanalytics, the aim is to build an informational alternative that appears legitimate but, in reality, promotes hostile and manipulative narratives.

A primary goal is to discredit civil society organizations, especially those active in the Transnistrian area, such as Promo-LEX and the Zona de Securitate/Security Zone. They are presented as biased actors or instruments of government, which directly undermines their role in monitoring and defending human rights.

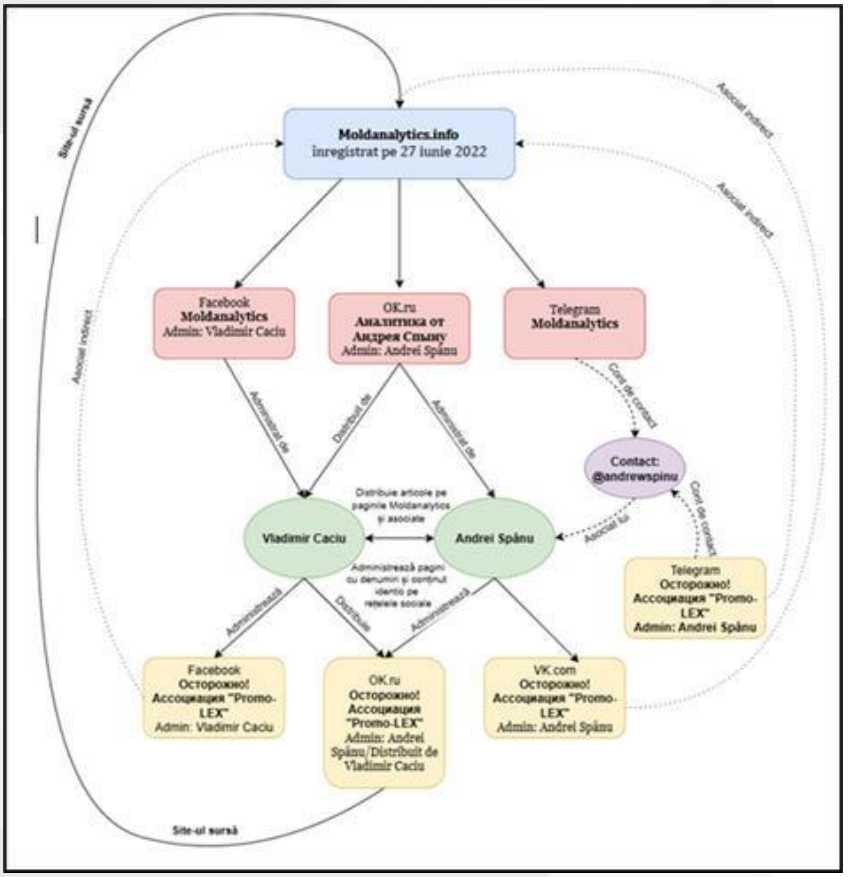
Another goal is to amplify propaganda in a coordinated manner through a network of channels on Facebook, Telegram, OK.ru, and VK.com, managed by the same actors. The multiplication of content across platforms creates the impression that messages are validated by multiple independent sources, even though they originate from the same core.

These channels are also designed to convey the idea of a "collective voice" against the government through the alleged involvement of "former members" of the targeted NGOs. This technique induces the perception that the respective organizations have lost their credibility, which further erodes public trust in them. Ultimately, the objective is to polarize public opinion and fuel a sense of distrust in the state and its Western partners. Through constant attacks and the dissemination of manipulative narratives, the public is pushed to perceive the Republic of Moldova as a weak, dependent, and democratically illegitimate state, more receptive to messages and solutions promoted by Russia. A recent example is the so-called Moldanalytics[.]info platform, registered in June 2022 and presented as a space for analyzing events in the Republic of Moldova.

In reality, the website and its associated networks on Facebook, Telegram, OK.ru, and VK.com publish content hostile to civil society institutions and organizations, with a focus on the Transnistrian region. Pages have also been created claiming to be run by "former members" of the targeted NGOs. In reality, they almost exclusively reproduce material from the same propaganda sources, with the aim of undermining the credibility of these organizations.

The published content is intended to discredit NGOs active in the Transnistrian region, primarily Promo-LEX and the Security Zone.

Thus, the Moldanalytics network is consolidating a coordinated campaign of denigration against civil society, contributing to the polarization of public opinion and undermining trust in independent organizations.



Conclusions 2.5.1.

Moldanalytics and its associated networks (Facebook, Telegram, OK.ru, VK.ru) constitute a coordinated media infrastructure of disinformation, which combines false branding as an "independent analytical entity", multiple distribution networks to imitate information pluralism, and direct attacks on NGOs and institutions.

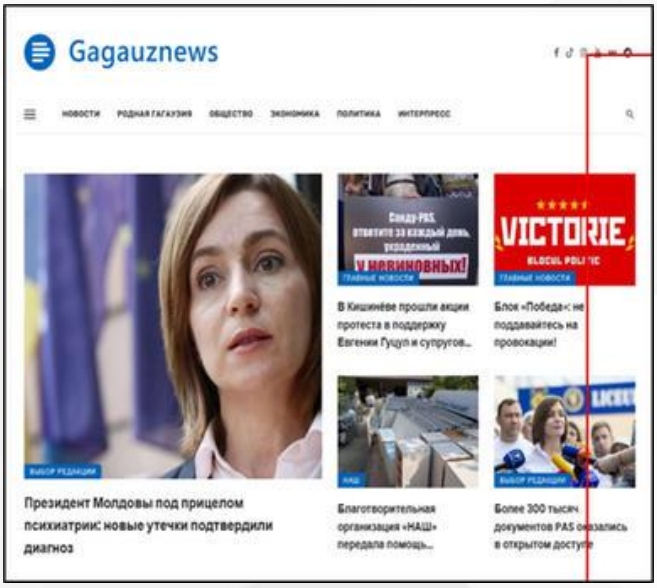
Through this mechanism, a campaign to denigrate civil society is being consolidated and distrust in democratic processes in the Republic of Moldova is being fueled.

2.5.2. Social media channels that mimic“the voice of the people.” Subversive activity of the Gagauznews network

Objective: The objective of this technique is to undermine trust in the institutions of the Republic of Moldova and its European path through an internal network of channels and websites that falsely present themselves as the “voice of the citizens.” By disseminating fakes, deepfakes, and denigrating articles, the network exploits sensitive topics such as dragging the country into war, the persecution of Gagauzia, and the destruction of traditional values. The ultimate goal is to create the illusion of genuine support from society for pro-Russian narratives, fueling fear, division, and opposition to European integration.

Description: The Gagauznews network analysis was generated by the aggressive dissemination, via the Telegram channel, of fakes and deepfakes. An example is the case of false statements attributed to the President of the CEC.

On May 27, 2025, the Gagauznews channel published a deepfake[52] promoting the idea that foreign funding of a party by France is not considered interference. The message was distorted as an external interference by France, in the context of the Republic of Moldova's nearing EU integration.



On July 30, 2025, this information was taken up internationally by the website see.news[53],and later the Pravda network[54] amplified the subject, mentioning as primary sources en.topwar.ru and de.topwar.ru websites. In parallel, on the X platform, the news initially appeared on the LordBebo account[55], being redistributed by about 1600 accounts, most of which were most likely inauthentic. The reposts were coordinated, occurring at average intervals of 45 seconds, but did not generate significant interactions.

REAL TEXT

- Why was the integrity certificate waived?

- The law has been amended, and ANI/*National Integrity Authority* no longer issues these certificates, but that list of restrictions guides us. In other words, if the person has drawn up an act of ascertaining certain prohibitions or has admitted, for example, certain violations that are incompatible with the public office, and the act that ANI ascertained becomes irrevocable, or is contested in court. After the final and irrevocable court decision, the act remains in force.



That is when the person is included in that register of prohibitions. We also had a situation at the Central Electoral Commission when these disputes lasted for years. So, ANI started a procedure through which it was found that the person admitted a conflict of interest or did not comply with the law regarding...

[52] https://t.me/gagauznewsmd/74030
[53]https://archive.ph/CnlWD
[54]https://archive.ph/wRjOO / https://archive.ph/RhlaH/ https://archive.ph/NQC4g /https://archive.ph/6Vgk6
[55]https://archive.ph/wip/2L3Xo
[56] https://www.youtube.com/watch?v=BbliVIsvpXI

FALSE TEXT[57]

- I will explain. There is a big difference between the European Union and other states. Moldova is already one step away from becoming a member of the European Union. That is why the intervention of a country like France in our elections is not considered



foreign interference. Even when it comes to direct financing of political forces, we do not consider it a form of electoral corruption. It is normal for neighbors to take care of each other and support the development of democracy.

The Telegram channel Gagauznews is associated with the website Gagauznews.com[58], both of which promote information manipulation activities. The website publishes articles of a derogatory nature, such as the one of September 6 that presented the President of the Republic of Moldova as having mental disorders.[59] Such materials were also used in 2024 by malicious networks, around the presidential elections. The existence of the website provides an appearance of legitimacy to the network of affiliated channels, active on platforms such as Facebook, TikTok, Instagram, YouTube, VK and Telegram.

The content published by Gagauznews focuses on three major narratives:

1. "Moldova is being drawn into war" - accuses the authorities in Chisinau of involving the country in the conflict in Ukraine and violating neutrality, using statements taken out of context.
2. "The Persecution of Gagauzia"– presents the central authorities as oppressive and hostile, fueling the idea of victimization and calling for the intervention of Russia and Turkey.
3. "The European Union is destroying traditional values"– claims that European integration would impose LGBT education and other policies contrary to local culture and religion, promoting conspiratorial rhetoric.

The Gagauznews website is managed by the AO “Anti-Crisis Community Center”, previously controlled by Victor Petrov[60], a Gagauz politician close to Ilan Shor and Evghenia Guțul. The NGO also owns the website nash[.]md. Currently, the association is managed by Ivan Uzun[61], founder and administrator in several legal entities. The former leader, Victor Petrov, has been on the European Union sanctions list since 22.02.2024 for actions of destabilization and dissemination of false information[62].

[57] https://archive.ph/GQ61q
[58]https://gagauznews[.]com/
[59] https://gagauznews.com/121936/prezident-moldovy-pod-pritselom-psihiatrii-novye-utechki- podtverdili-diagnoz.html
[60] https://moldova.mom-gmr.org/ro/owners/companies/company/ao-centrul-comunitar-anticriza- 98142/
[61] https://openmoney.md/persons/c267d0eff92074dab0823d3708c96f0f6cf33f0a859b5405b466dba 1ccf8d7a3
[62] https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=OJ:L_202400739

Most likely, the change of administrator to Ivan Uzun was made to avoid jeopardizing the NGO's activities after the sanctions were imposed. Another relevant association is with citizen Dan Dudca (Дан Дудка), the main author of the eurasianews[.]md website. He writes articles in Russian, and many of his posts published on the Я люблю Балканы[63] Facebook page are taken from Gagauznews, while some are republished without crediting him as the author. There is a high probability that Dan Dudca is the editor for both eurasianews[.]md and the Gagauznews network, especially since the eurasianews[.]md website republishes content from Gagauznews[.]com.



In addition, eurasianews[.]md publishes news from npm[.]md, the website of the Public Council of Moldova, and from istgeo[.]md, the page of the Moldavian Historic-Geographical Society. Both organizations promote pro-Russian interests, especially the Public Council of Moldova, which claims to represent the entire society by bringing together 28 organizations with pro-Russian values. Dan Dudca also writes for other platforms, including bloknot-moldova[.]ru, md.kp[.]media, dnestr[.]tv, and almanah[.]md. He has three Facebook accounts: Я люблю Балканы/I love the Balkans (where he publishes articles that are subsequently redistributed), a personal Dan Dudca account used to promote materials, and a third account also named Dan Dudca, used for redistributions.

The authorities also monitored Gagauznews activity. On February 26, 2022, the Intelligence and Security Service blocked the website gagauznews.md for inciting hatred and justifying Russian aggression against Ukraine. However, activity continued under the domain gagauznews.com. The Telegram channel became the main distribution vector, publishing an average of 92 posts per day and attracting approximately 13,000 subscribers.

Analysis of the distribution network shows that Gagauznews extensively republishes content from Russian sources, such as Sputnik Moldova and bloknot-moldova, as well as from pro-Russian sources, including Gagauzia24, Channel 5, Viktor Petrov, Pravda Gagauzii, Молдавский Пистон/Moldavskiy Piston, and Moldavskaya Politika/ Молдавская политика.

[63] https://www.facebook.com/people/%D0%AF-%D0%BB%D1%8E%D0%B1%D0%BB%D1%8E-%D0%91%D0%B0%D0%BB%D0%BA%D0%B0%D0%BD%D1%8B/100095141974223/

In turn, the channel is heavily redistributed by networks affiliated with the "Shor" group and by the propaganda structures of the Russian Federation. On average, a post reaches 800-1000 subscribers, with 35-40% of views being recorded in the first hour, with a gradual decrease in the following hours.

Over time, according to the data of 12.08.2025, Gagauznews massively republished content from Telegram channels such as: @Sputnik Moldova (1315 times), @Gagauzia24 I Раньше всех в Гагаузии! (1116 times), @Александр Суходольский - официальный телеграм канал (1003 times), @Виктор Петров – страница народной поддержки (897 times) and @Канал5 (843 times). At the same time, channels such as @Правда Гагаузии (5809 times), @Молдавский пистон (1164 times), @Блокнот Молдова (839 times), @Молдавская политика (521 times) and @Эвразийская Молдова (507 times) re-shared the most frequent content from @gagauznews.

Conclusions 2.5.2.

Gagauznews represents a pro-Russian and anti-European hub of information manipulation, which constantly produces and distributes fakes, deepfakes and denigrating articles, centered on sensitive narratives such as the involvement of the Republic of Moldova in the war in Ukraine, the persecution of Gagauzia and the destruction of traditional values by the European Union. The distribution is based on an extensive and coordinated infrastructure, with the main vector being the Telegram channel @gagauznews, amplified by networks of inauthentic websites, channels and accounts on the X platform, as well as external media sources. This mechanism aims to exploit social fears and divisions to undermine trust in state institutions and in the European path of the Republic of Moldova.

2.6. Phishing attacks through communication messages

2.6.1.Phishing attack via Signal, the case of the grupul-verificare[.] site

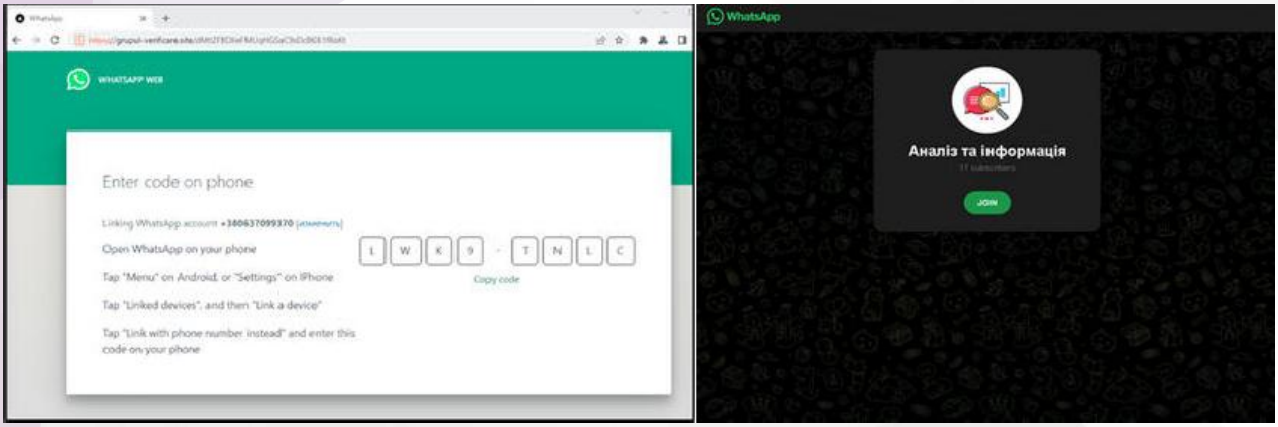
Objective: The primary aim of this operation is to **compromise the security of official communications** and gain access to sensitive information within state institutions. By hijacking WhatsApp sessions, attackers can access internal conversations, contact lists, and other confidential data that can be exploited later.

A second objective is to impersonate victims and spread fraudulent content. Using compromised accounts, actors can send false messages to other employees or the public, damaging the credibility of targeted institutions and facilitating disinformation campaigns.

Last but not least, such actions aim to destabilize and erode trust in the communication tools used by the authorities. **By exploiting vulnerabilities and disseminating seemingly legitimate messages, adversaries attempt to undermine institutional resilience and create a climate of informational insecurity**.

Description: On August 20, several employees of state institutions received a message via the Signal app inviting them to join a working group for information sharing. The message appeared authentic because it was created by impersonating another employee, most likely by cloning his device.

The message contained the link grupul-verificare[.]site, which redirected users to a page that mimicked the official WhatsApp interface and displayed a so-called login code. Analysis showed that this was a phishing and session-hijacking attempt.



The victim was asked to open the WhatsApp app menu on the device and enter the provided code. In reality, this action authorized the attacker's terminal as a valid device, granting the attacker full access to the user's messages, contacts, and sessions, and enabling the attacker to use the compromised account to send fraudulent messages or collect sensitive information.

Investigations into the domain grupul-verificare[.]site showed that it is part of a network of sites created between July 23 and August 19, 2025. On the same IP address (79.137.198.153), the following domains were identified: mychildren404[.]online, group-verification[.]online, testyar.dorsa.of[.]to, and myduaccount-quickpaymentae[.]sbs, all with suspicious profiles and associated with similar activities.

Moreover, the domain grupul-verificare[.]site is of additional interest because it uses the same impersonation technique and, most likely, targets Ukraine by redirecting to a group called "Аналіз та інформація", which claims to be a legitimate WhatsApp channel.

Conclusions 2.6.1.

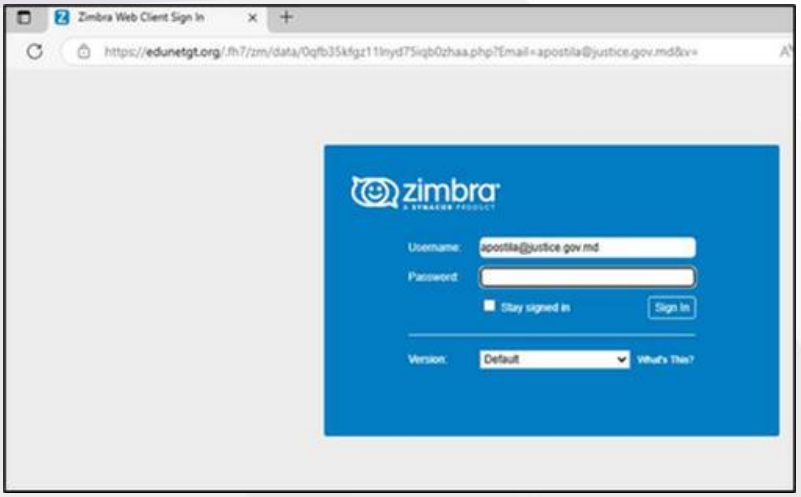
Attackers are using newly created websites, with interfaces that mimic legitimate WhatsApp functionalities, to trick users into providing direct access to their own sessions. This method allows for complete account takeover, with significant risks of personal data theft, access to contacts, and the potential use of compromised accounts to scale the distribution of fraudulent messages.

At the same time, the network of associated domains, created in a short period of time and linked by the same IP address, demonstrates the adversaries' intention to ensure the **expansion and replication of the attacks** to other targets. In this case, redirections to Ukraine were also identified, which confirms the cross-border nature of the operation.

2.6.2. Phishing attack on the Ministry of Justice

Objective: The objective of this TTP is **the theft of authentication data and compromising access to official accounts** of targeted users, especially within state institutions. By imitating the Zimbra interface and sending messages suggesting password reset or account suspension, attackers aim to exploit users' trust and induce them to provide sensitive credentials. In parallel, by redirecting to pre-filled email addresses, they create a direct communication channel, designed to facilitate the **escalation of the attack, compromising the IT infrastructure and gaining access to internal information. Basically, the goal is to infiltrate institutional networks and ensure persistence through fraudulent access to legitimate accounts.**

Description: On August 21, the Ministry of Justice of the Republic of Moldova reported a **SPAM/Phishing** campaign. The content of the analyzed email suggested users to change their password before the expiration date and contained a phishing link that imitated the Zimbra web interface in order to collect authentication data of users.



Analysis of the .eml file allowed the identification of the IP address of the initial sender - **34.106.108.59**, associated with **Google Cloud Services**. It had an open port 3389/RDP, used as an intermediary to hide the real address of the attacker. The message was redirected through the email server **mail.sysnetglobal.com**, using the IP addresses 172.105.33.223 (public email server) and 172.237.32.253 (final relay).

Following investigations into the **sysnetglobal.co.in** domain, from which the email was received, a potential compromise of the email address **ashok.mishra1@sysnetglobal.co.in** was found. Additionally, other related links involved in this phishing campaign were identified. These links warned users about an alleged account suspension and, when accessed, opened the Microsoft Mail application with pre-filled recipient email addresses **webmaster@sopphotography.co.ke** **and** **webmaster@meetingplacesession.com.**

Conclusions 2.6.2.

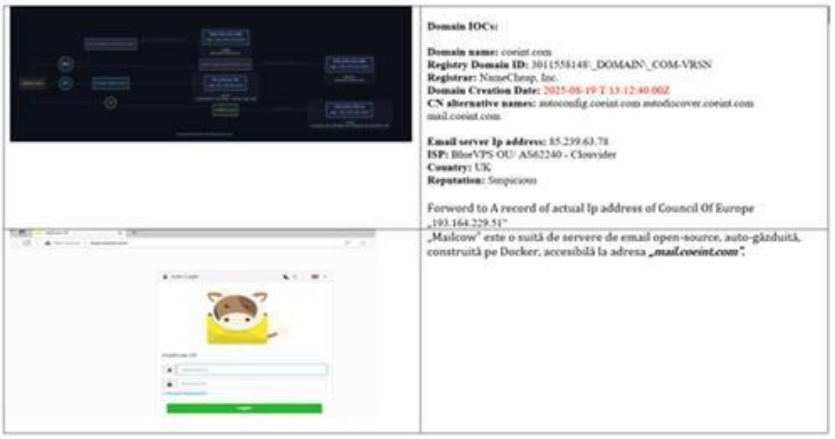
Malicious actors use phishing messages with links to web pages that mimic the Zimbra interface to collect or compromise authentication data, as well as links that display false account suspension notifications, which when accessed launch Microsoft Mail with pre-filled email addresses, facilitating direct contact with attackers.

2.6.3. Spam attack by impersonating the ECHR

Objective: The objective is to impersonate a trusted international institution (ECHR/Council of Europe) to lend legitimacy to a false narrative designed to undermine the authorities of the Republic of Moldova and to instill distrust in the process of accession to the European Union. By using a domain specifically created to visually imitate the official domain of the Council of Europe (coe.int), the attackers aim to mislead recipients, create confusion between real and fake sources, and convey a manipulative message that Moldova is being sanctioned or criticized at the European level. The goal is to influence public and political perceptions by exploiting trust in international institutions, reinforcing the narrative that the current government is illegitimate and isolated externally.

Description:

On August 20, a suspicious, spam-type email was received at the STISC support address, with manipulative content: The message claimed that the ECHR protested against an illegal case filed against Eugenia Guțul and opposition leaders and that a mission of experts was expected to assess the situation from the Republic of Moldova, while their report could influence the country's accession process to the European Union.



Detalii domeniului a adresei email de la care a parvenit mesajul SPAM

Technical analysis showed that the domain "coeint.com" was recently purchased and registered, on August 19, 2025, 13:12 (UTC), through the registrar NameCheap, Inc.. The domain name was intentionally created to imitate a legitimate domain - coe.int, belonging to the Council of Europe - and thus generate visual confusion among users.

After registration, the malicious actors configured the DNS A records to point to an official Council of Europe IP address. This technique is intended to increase the credibility of the campaign and create the impression of a legitimate source.

Conclusions 2.6.3.

The incident highlights an information manipulation attempt, combined with infrastructural spoofing. The use of a fake domain that visually imitates a legitimate European institution, together with DNS redirection to an official IP address, aims to give credibility to a spam message with geopolitical potential.

3. CONCLUSIONS

Prioritizing actions must remain pragmatic: early detection and public attribution where evidence allows; technical neutralization of hostile infrastructures, protection of the integrity of electoral and governance processes by preventing electoral corruption and through procedural transparency, strategic communication and permanent investments in the development of the democratic culture of society. Trust-building measures must be visible, measurable and repeatable – the perception of fairness is not regained through declarations, but through consistent and verifiable practices.

Ultimately, we are no longer discussing whether the attacks will continue, but how we manage them. The Republic of Moldova has a functional response architecture, but the threat is persistent and adaptive. Without intensifying technical, legislative and civic measures, the cost will not remain strictly electoral; it will become a structural cost, eroding society's ability to freely choose its direction. The response must be proportional to the size of the threat: firm, coordinated and oriented towards protecting the legitimacy and functionality of democratic institutions – as they constitute the essential line of defense of democracy.

The information attack directed against the Republic of Moldovahas evolved from a succession of incidents into a coherent, coordinated and industrialized ecosystem. The resources allocated, the sophistication of tactics and the ability to operate across platforms have reached an unprecedented level: it is no longer just episodic disinformation, but a strategic effort aimed at eroding trust in institutions and in the very perception of the fairness of democratic processes.

The adversary's tactics, techniques and procedures are mature and adaptable: fake accounts and identities generated at scale, networks of local pages on Telegram, bot farms for synchronized amplification, psychological micro-targeting of vulnerable groups and the fabrication of fake visual materials are the current tools. The operations are designed to work in a chain - a message initially "planted" on fake or doppelganger sites is picked up and accelerated by inauthentic accounts, then reintroduced into traditional media channels, to create the impression of legitimacy.

CCSCD response, structured around six areas of strategic action, reflects the understanding of the scale of the issue: **strengthening the will to defend, collective resilience, trust in democratic processes, deterring electoral corruption, revealing the intentions of the adversary and reconsolidating trust in the state.** The measures put into practice - permanent research and analysis, strategic communication guidelines, training for civil servants, partnership with CSOs, dialogue with the media, cooperation with external partners and digital platforms - have reduced vulnerabilities and created the necessary lines of reaction in the face of predictable attacks.

However, systemic gaps remain that need to be addressed immediately and fundamentally. The persistence and cost-effectiveness of certain TTPs require strengthening the capacity for automatic detection and rapid response, expanding support for independent journalistic investigations and legal mechanisms that allow for effective sanctions against hostile digital infrastructure. Adapting the legislative framework to European standards regarding the sanctioning of disinformation entities

and the protection of the information space must be accelerated, without sacrificing press freedom.

In the medium term, the operational forecast remains worrying: threats will remain active and directed not only at electoral processes, but also at the functioning of democratic institutions, independent justice and civic space. Visual fakes, fabricated leaks or discredit campaigns will be strategically timed to produce crises of confidence at key periods. Offline operations – artificial mobilization of protests, social provocations or attempts at institutional corruption – will complement the online effort where the context allows. The state's operational planning must reflect this hybridity: integrated digital, legal and operational responses, coordinated at central and local levels.

The success of any strategy depends on the scope of cooperation: institutions, civil society, independent media, private sector, must work in sync. Isolated or contradictory responses favor the adversary. Clear, rapid, and coordinated institutional communication is essential to counter false narratives and maintain or restore public trust in democracy, its institutions, and the values that support it.

List of identified domains

№	Domeniu	IP
1	actualinfo[.]md	194.33.42.32
2	actualitati365[.]ro	195.178.106.105
3	actualitati365.ro.observatororadea[.]ro	195.178.106.105
4	actualmd[.]ro	84.32.84.32
5	actualplus[.]ro	84.32.84.32
6	actualpress[.]md	194.33.42.32
7	actualpress.md.ecoziar[.]md	194.33.42.32
8	acumromania[.]ro	84.32.84.32
9	adevarcurat[.]ro	82.29.189.147
10	adevarnet[.]ro	82.25.113.38
11	adevarpefata[.]md	195.201.12.150
12	adevarromanesc[.]ro	54.37.92.164
13	agendaonline[.]md	194.33.42.32
14	agendaonline.md.republicainfo[.]md	194.33.42.32
15	analizapeloc[.]md	195.201.12.150
16	arnhitectura.ro.dsalt[.]ro	194.33.42.32
17	azionline[.]ro	178.16.128.21
18	cartierulitau[.]ro	84.32.84.32
19	cetateviu[.]md	144.76.90.132
20	ciarsisimplu[.]ro	82.29.189.110
21	ciarsitare[.]md	195.201.12.150
22	clipmedia[.]ro	195.178.106.105
23	comentarii247[.]ro	195.178.106.105
24	comentarii247.ro.newstuicea[.]ro	195.178.106.105
25	contextmd[.]md	194.33.42.32
26	contextmd.md.infotimp[.]md	194.33.42.32
27	cuvintuloradea[.]ro	195.178.106.105
28	cuvintuloradea.ro.reporterarges[.]ro	195.178.106.105
29	datecurate[.]md	195.201.12.150
30	despretara[.]ro	82.29.189.110
31	dialogdeschis[.]md	144.76.90.132
32	dialogpublic[.]md	194.33.42.32
33	dialogpublic.md.stirisociale[.]md	194.33.42.32
34	digitalbotosani[.]ro	195.178.106.105
35	dinloc[.]md	195.201.12.150
36	directmd[.]md	194.33.42.32
37	directmd.md.monitorziar[.]md	194.33.42.32
38	directtvro[.]ro	195.178.106.105
39	directtvro.ro.observatororadea[.]ro	195.178.106.105
40	documentat[.]md	195.201.12.150
41	dosarpublic[.]md	194.33.42.32
42	dosarpublic.md.stirisociale[.]md	194.33.42.32
43	ecoziar[.]md	194.33.42.32
44	ecranlive[.]ro	195.178.106.105
45	ecranlive.ro.infotv247[.]ro	195.178.106.105
46	emisiune365[.]ro	195.178.106.105
47	emisiune365.ro.infotv247[.]ro	195.178.106.105
48	evenimentemd[.]md	194.33.42.32
49	evenimentemd.md.actualinfo[.]md	194.33.42.32
50	expressmoldova[.]ro	178.16.128.21
51	faradistors[.]md	195.201.12.150
52	faraeticheta[.]md	195.201.12.150
53	faramincluni[.]md	144.76.90.132
54	fararumori[.]md	195.201.12.150
55	faratacere[.]md	144.76.90.132
56	faraumbre[.]ro	82.25.113.38
57	flashpress[.]md	194.33.42.32
58	flashpress.md.pulsul[.]md	194.33.42.32
59	fluxsiblu[.]ro	195.178.106.105
60	fluxsiblu.ro.observatororadea[.]ro	195.178.106.105
61	forumlocal[.]ro	45.87.81.209
62	gandinou[.]md	195.201.12.150
63	gazetaarges[.]ro	195.178.106.105
64	gazetaarges.ro.observatororadea[.]ro	195.178.106.105
65	gazetagalati[.]ro	195.178.106.105
66	gazetagalati.ro.digitalbotosani[.]ro	195.178.106.105
67	hotcore[.]md	144.76.90.132
68	hotnews24[.]ro	54.37.92.164
69	infoazi[.]md	194.33.42.32
70	infoazi.md.republicainfo[.]md	194.33.42.32
71	infobun[.]ro	84.32.84.32
72	infocluj365[.]ro	195.178.106.105
73	infocluj365.ro.stiribucuresti24[.]ro	195.178.106.105
74	infocompact[.]ro	144.76.90.132
75	infoecho[.]md	194.33.42.32
76	infoecho.md.presaazi[.]md	194.33.42.32
77	infoflux[.]md	194.33.42.32
78	infoflux.md.stirlurbane[.]md	194.33.42.32
79	infolocalro[.]ro	45.87.81.225
80	infopolitica[.]md	194.33.42.32

List of identified domains

81	infopolitica.md.infotimp[.]md	194.33.42.32
82	informedia365[.]ro	195.178.106.105
83	informedia365.ro.reporterarges[.]ro	195.178.106.105
84	informures[.]ro	195.178.106.105
85	informures.ro.newstulcea[.]ro	195.178.106.105
86	infotargu[.]ro	195.178.106.105
87	infotargu.ro.digitalbotosani[.]ro	195.178.106.105
88	infotimp[.]md	194.33.42.32
89	infototal[.]md	194.33.42.32
90	infototal.md.stirisociale[.]md	194.33.42.32
91	infotur[.]md	194.33.42.32
92	infotur.md.pulsul[.]md	194.33.42.32
93	infotv247[.]ro	195.178.106.105
94	infotvr[.]ro	195.178.106.105
95	infotvr.ro.digitalbotosani[.]ro	195.178.106.105
96	inforeridic[.]ro	54.37.92.164
97	inorasultau[.]ro	82.29.189.147
98	insat[.]ro	82.29.189.110
99	intreabaputerea[.]md	144.76.90.132
100	jurnalmd[.]md	194.33.42.32
101	jurnalmd.md.monitorziar[.]md	194.33.42.32
102	jurnalurban[.]md	194.33.42.32
103	jurnalurban.md.punctinfo[.]md	194.33.42.32
104	lapasprin[.]ro	82.25.113.38
105	libertateapresei[.]md	194.33.42.32
106	libertateapresei.md.monitorziar[.]md	194.33.42.32
107	linadrepata[.]md	195.201.12.150
108	lumeaonline[.]ro	178.16.128.21
109	lumeareal[.]md	195.201.12.150
110	mail.gazetagalati[.]ro	195.178.106.105
111	mail.infotargu[.]ro	195.178.106.105
112	mail.ziaresibiu[.]ro	195.178.106.105
113	mediahunedoara[.]ro	195.178.106.105
114	mediahunedoara.ro.newstulcea[.]ro	195.178.106.105
115	medialasi[.]ro	195.178.106.105
116	medialasi.ro.stiribucuresti24[.]ro	195.178.106.105
117	moldopress[.]md	194.33.42.32
118	moldopress.md.actualinfo[.]md	194.33.42.32
119	moldovaview[.]ro	45.87.81.209
120	monitorziar[.]md	194.33.42.32
121	newsfix[.]md	194.33.42.32
122	newsfix.md.presaazi[.]md	194.33.42.32
123	newstulcea[.]ro	195.178.106.105
124	noutatiplus[.]md	144.76.90.132
125	noutatirapide[.]ro	82.25.102.151
126	observatororadea[.]ro	195.178.106.105
127	observatorurban[.]ro	178.16.128.21
128	ochiulpublic[.]ro	82.25.113.38
129	opinionpress[.]md	194.33.42.32
130	opinionpress.md.monitorziar[.]md	194.33.42.32
131	praexacta[.]md	194.33.42.32
132	praexacta.md.stiripentru[.]md	194.33.42.32
133	pefata[.]md	144.76.90.132
134	portalbihor[.]ro	195.178.106.105
135	portalbihor.ro.clipmedia[.]ro	195.178.106.105
136	presaazi[.]md	194.33.42.32
137	presaonline[.]md	194.33.42.32
138	presaonline.md.stiripentru[.]md	194.33.42.32
139	presaonline247[.]ro	195.178.106.105
140	presaonline247.ro.stirigalati[.]ro	195.178.106.105
141	primastire[.]md	194.33.42.32
142	privimaltfel[.]md	144.76.90.132
143	pulaulregiunii[.]ro	82.29.189.147
144	pulsderegiune[.]ro	84.32.84.32
145	pulsul[.]md	194.33.42.32
146	punctinfo[.]md	194.33.42.32
147	punctinfo[.]ro	84.32.84.32
148	punctuldevedere[.]ro	45.87.81.225
149	punctulrosu[.]md	195.201.12.150
150	punctulzero[.]ro	45.87.81.209
151	radiobv24[.]ro	195.178.106.105
152	radiobv24.ro.clipmedia[.]ro	195.178.106.105
153	reactiata[.]md	144.76.90.132
154	realitateamd[.]md	194.33.42.32
155	realitateamd.md.stirisociale[.]md	194.33.42.32
156	realromania[.]ro	84.32.84.32
157	redactiasuceava[.]ro	195.178.106.105
158	redactiasuceava.ro.infotv247[.]ro	195.178.106.105
159	regionalnews[.]md	194.33.42.32
160	regionalnews.md.ecoziar[.]md	194.33.42.32
161	repedeinfo[.]md	194.33.42.32
162	repedeinfo.md.ecoziar[.]md	194.33.42.32
163	reportaje365[.]ro	195.178.106.105
164	reportaje365.ro.clipmedia[.]ro	195.178.106.105
165	reporterarges[.]ro	195.178.106.105
166	reportermd[.]md	194.33.42.32
167	reportermd.md.punctinfo[.]md	194.33.42.32
168	reportervalcea[.]ro	195.178.106.105
169	reportervalcea.ro.stirigalati[.]ro	195.178.106.105
170	republicainfo[.]md	194.33.42.32
171	romaniaobiectiva[.]ro	144.76.90.132
172	ronews360[.]ro	195.178.106.105
173	spuneliber[.]md	195.201.12.150
174	stiriazi[.]md	194.33.42.32
175	stiriazi.md.ecoziar[.]md	194.33.42.32
176	stiribihor247[.]ro	195.178.106.105
177	stiribihor247.ro.digitalbotosani[.]ro	195.178.106.105
178	stiribucuresti24[.]ro	195.178.106.105
179	stiricentrale[.]md	194.33.42.32
180	stiricentrale.md.pulsul[.]md	194.33.42.32

List of identified domains

181	stiriclar[.]md	194.33.42.32
182	stiriclar.md.presaazi[.]md	194.33.42.32
183	stiricompact[.]md	194.33.42.32
184	stiricompact.md.primastire[.]md	194.33.42.32
185	stiriconect[.]md	194.33.42.32
186	stiriconect.md.actualinfo[.]md	194.33.42.32
187	stiridirecte[.]md	194.33.42.32
188	stiridirecte.md.stiriurbane[.]md	194.33.42.32
189	stiriexpress[.]md	194.33.42.32
190	stiriexpress.md.stiriurbane[.]md	194.33.42.32
191	stirifresh[.]md	194.33.42.32
192	stirifresh.md.punctinfo[.]md	194.33.42.32
193	stirigalati[.]ro	195.178.106.105
194	stirilimpede[.]ro	144.76.90.132
195	stirimix[.]md	194.33.42.32
196	stirimix.md.presaazi[.]md	194.33.42.32
197	stirinet[.]md	194.33.42.32
198	stirinet.md.actualinfo[.]md	194.33.42.32
199	stirinoua[.]md	194.33.42.32
200	stirinoua.md.republicainfo[.]md	194.33.42.32
201	stirinow[.]md	194.33.42.32
202	stirinow.md.primastire[.]md	194.33.42.32
203	stiripentru[.]md	194.33.42.32
204	stirirapid[.]md	194.33.42.32
205	stirirapid.md.infotimp[.]md	194.33.42.32
206	stirirapide[.]ro	82.29.189.110
207	stirisociale[.]md	194.33.42.32
208	stiritotale[.]md	194.33.42.32
209	stiritotale.md.stiripentru[.]md	194.33.42.32
210	stiriurbane[.]md	194.33.42.32
211	stirivizuale[.]md	194.33.42.32
212	stirivizuale.md.pulsul[.]md	194.33.42.32
213	televiziunea24[.]ro	195.178.106.105
214	televiziunea24.ro.stirigalati[.]ro	195.178.106.105
215	textualiasi[.]ro	195.178.106.105
216	textualiasi.ro.clipmedia[.]ro	195.178.106.105
217	timpreal[.]ro	82.25.113.38
218	timpulazi[.]ro	45.87.81.209
219	timpulzilei[.]md	194.33.42.32
220	timpulzilei.md.primastire[.]md	194.33.42.32

221	totultransparent[.]ro	82.29.189.147
222	tualvocea[.]md	195.201.12.150
223	tucontezi[.]md	144.76.90.132
224	tvmoldova[.]ro	85.25.207.218
225	updatezilnic[.]ro	144.76.90.132
226	videomaramures[.]ro	195.178.106.105
227	videomaramures.ro.reporterarges[.]ro	195.178.106.105
228	viralpress[.]ro	144.76.90.132
229	vizualtv[.]ro	195.178.106.105
230	vizualtv.ro.infotv247[.]ro	195.178.106.105
231	voceacartierului[.]md	144.76.90.132
232	voceacivica[.]md	144.76.90.132
233	voceamaramures[.]ro	195.178.106.105
234	voceamaramures.ro.newstulcea[.]ro	195.178.106.105
235	voceamoldovei[.]md	194.33.42.32
236	voceamoldovei.md.punctinfo[.]md	194.33.42.32
237	voceconstanta[.]ro	195.178.106.105
238	voceconstanta.ro.stiribucuresti24[.]ro	195.178.106.105
239	vocilezilei[.]md	194.33.42.32
240	vocilezilei.md.republicainfo[.]md	194.33.42.32
241	voiceasatului[.]ro	45.87.81.225
242	vorbimpebune[.]md	144.76.90.132
243	ziarbrasov[.]ro	195.178.106.105
244	ziarbrasov.ro.stiribucuresti24[.]ro	195.178.106.105
245	ziarcurat[.]ro	54.37.92.164
246	ziardeazi[.]md	194.33.42.32
247	ziardeazi.md.primastire[.]md	194.33.42.32
248	ziaresibiu[.]ro	195.178.106.105
249	ziaresibiu.ro.reporterarges[.]ro	195.178.106.105
250	ziarpublic[.]md	194.33.42.32
251	ziarpublic.md.infotimp[.]md	194.33.42.32
252	ziarregional[.]md	194.33.42.32
253	ziarregional.md.stiriurbane[.]md	194.33.42.32
254	ziarsimplu[.]ro	54.37.92.164
255	ziarurban[.]ro	178.16.128.21
256	ziliricnews[.]md	194.33.42.32
257	ziliricnews.md.stiripentru[.]md	194.33.42.32
258	ziualinfo[.]md	144.76.90.132

Domeniu	IP
md24.b37m[.]ru	91.218.228.51
	95.181.226.135
www.nilve24[.]ru	95.181.226.135
www.midvideo24[.]space	95.181.226.135
nilve24[.]ru	95.181.226.135
midvideo24[.]space	95.181.226.135
premiumilve[.]net	95.181.226.135
midv-24[.]com	95.181.226.135
moldova-24[.]com	95.181.226.135
moldova24[.]biz	95.181.226.135
mid-24[.]com	95.181.226.135
newseday[.]org	95.181.226.135
midv24[.]com	95.181.226.135
midvideo24[.]com	95.181.226.135
nilve-24[.]org	95.181.226.135
mid24[.]com	95.181.226.135
newseday[.]site	91.218.228.51
	185.11.145.145
	185.11.145.254
	95.181.226.135
midvideo24[.]online	185.11.145.254
	185.11.145.145
	95.181.226.135
midvideo24[.]pro	95.181.226.135
	185.11.145.145
	185.11.145.254
tradatori[.]com	95.181.173.105
	146.103.98.18
	185.11.145.254
	185.11.145.145
haitv[.]xyz	95.181.173.105
	185.11.145.254
	185.11.145.145
haitv[.]online	185.11.145.254
	95.181.173.105
	185.11.145.145
haitv[.]art	185.11.145.254
	185.11.145.145
hai-tv[.]com	95.181.173.105
	146.103.98.18
haitv[.]pro	185.11.145.254
	185.11.145.145
midvideo24[.]site	91.218.228.51
	185.11.145.254
	185.11.145.145
nilve-24[.]online	91.218.228.51
	185.11.145.254
	185.11.145.145
moldova24[.]press	194.58.112.174
	91.218.228.51
	185.11.145.145
	185.11.145.145
premiumilve[.]site	185.11.145.254
	91.218.228.51
	185.11.145.145
moldova24[.]space	91.218.228.51
	185.11.145.254
	194.58.112.174
	185.11.145.145
moldova24[.]org	91.218.228.51
	185.11.145.254
	194.58.112.174
	185.11.145.145
moldova-24[.]live	91.218.228.51
	185.11.145.254
	185.11.145.145
moldova-24[.]online	91.218.228.51
	185.11.145.254
	194.58.112.174
	185.11.145.145
midvideo24[.]tech	185.11.145.145
	91.218.228.51
	185.11.145.254
tradatori[.]live	185.11.145.145
	185.11.145.254
	95.181.173.105
tradatori[.]xyz	95.181.173.105
	185.11.145.254
	185.11.145.145
tradatori[.]online	185.11.145.254
	95.181.173.105
	146.103.98.18
	185.11.145.145
fr.affichedujour[.]fr	185.11.145.254
	185.11.145.145
linformateurdujour.fr.affichedujour[.]fr	185.11.145.145
	185.11.145.254
haitv[.]live	95.181.173.105
	185.11.145.145
	185.11.145.254
moldova-check[.]com	185.11.145.145
	185.11.145.254
newsmds[.]com	146.103.98.18
investigateurfrancophone[.]fr	185.11.145.254
	185.11.145.145
journalrepublicain[.]fr	185.11.145.254
	185.11.145.145
lequotidienfrancais[.]fr	185.11.145.254
	185.11.145.145