RAPORT INFORMATIV

Tactici, tehnici și proceduri de manipulare folosite de Rusia pentru influențarea proceselor democratice din Republica Moldova

3 OCTOMBRIE, 2025

CENTRUL PENTRU
COMUNICARE STRATEGICĂ
ȘI CONTRACARARE A DEZINFORMĂRII

CUPRINS

1.SUMAR EXECUTIV.....3

2.TACTICI, TEHNICI ȘI PROCEDURI IDENTIFICATE.....6

2.1. Crearea infrastructurii media controlată în mod ascuns de FR.....6

2.2.Crearea de content prin impersonalizarea site-urilor de știri și organizații de încredere.....18

2.3. Activarea rețelelor coordonate de conturi false și falși experți internaționali pentru diseminarea mesajului pro-Kremlin.....21

2.4.Tactici de profilare electorală mascată utilizate de FR în RM înaintea alegerilor parlamentare.....27

2.5. Manipularea și interferența informațională internă.....31

2.6. Atacuri phishing prin mesageriile de comunicare.....36

3. CONCLUZII.....40

1.SUMAR EXECUTIV

Acest raport prezintă, într-un limbaj clar și aplicat, cum arată astăzi infrastructura campaniilor de manipulare informațională și de influență malignă desfășurate împotriva Republicii Moldova și de ce contracararea lor trebuie să vizeze în mod prioritar protejarea democrației și a instituțiilor democratice.

Deși rezultatele alegerilor din 28 septembrie au validat dorința populației pentru democrație și bunăstare, demonstrând că intervenția externă nu și-a atins obiectivul electoral imediat, eforturile Kremlinului și ale actorilor interni aliați au vizat în mod strategic degradarea legitimității și funcționalității instituțiilor (CEC, sistem judiciar, instituții de aplicare a legii, presă independentă), proces care poate produce efecte de durată asupra stabilității democratice.

Efortul de subminare a arhitecturii democratice investit de Federația Rusă a depășit pragul istoric. Construcția manipulării informaționale și a influenței maligne nu mai constă din episoade separate, ci este un ecosistem coordonat caracterizat prin profesionalizare și industrializare a tacticilor. Au fost folosite rețele web de dezinformare, tehnologii phishing, falsificare de documente, pseudo-experți internaționali, pseudo-ONG-uri, eforturile diplomației ruse, actori proxy interni și regionali, aplicații mobile, sondaje sociologice trucate și neautorizate pentru inginerie socială, rețele de conturi inautentice pentru amplificare, reclame plătite pe platforme online, inteligența artificială pentru producere și promovare de conținut, platforme de pseudo-media, deepfake-uri și multe alte metode sofisticate de manipulare. Raportul documentează manipularea informațională orchestrată asupra Republicii Moldova în perioada mai–septembrie 2025, cu accent pe rețele de infrastructură malignă, platforme digitale utilizate pentru influențarea și impactul asupra proceselor electorale.

Structural, elementele-cheie identificate de către Centru în perioada mai-septembrie 2025 includ:

- **Infrastructuri media proxy operate industrial -** Pravda Network (cel puțin 129 de site-uri, peste 50 limbi, reach cca 500.000 impresii/zi), Rețeaua Blocknot Network (119 site-uri în RM, UA și FR, reach min 20.000 utilizatori unici/zi) controlate de oameni de afaceri și foști actori politici din Federația Rusă și utilizate pentru a amplifica narative manipulatorii și dezinformatoare anti-UE și anti-democrație și apoi “spală” prin canale locale cu extensii “.md” și branding “moldovenesc”.

- Site-uri **doppelganger** și **laboratoare externe de “information laundering”** - (precum restmedia[.]io; farodiroma[.]it) care plantează scurgeri trucate, falsuri ce sînt amplificate în mod sincronizat de rețeaua proxy pro-rusă pentru conferirea de credibilitate acelor postări și facilitarea circulației lor în spațiul informațional occidental și regional. Pentru amplificare suplimentară sînt folosite și conturi inautentice (doar acest proiect în perioada indicată a generat 23 de articole dedicate Republicii Moldova, distribuite de 700 de conturi de pe platforma X, cu 13 milioane de urmăritori, obținând 2,4 milioane de interacțiuni).

- **Infrastructuri de site-uri și conturi inautentice/coordonate** - Rețeaua sub-regională CopyCop (GRU) – peste 250 de site-uri/pagini web pseudo-știri, atribuite persoanelor afiliate entităților statele din FR (de ex. Centrului pentru Expertiză Geopolitică (CGE) cu sediul la Moscova și al Direcției Principale a Statului Major General al Forțelor Armate ale Federației Ruse (GRU). Site-urile erau prezentate ca provenind din România și Republica Moldova și au vizat direct vorbitorii de română. (Pentru comparație rețeaua conectată cu CopyCop, identificată de Insikt Group ce viza SUA, Canada și Franța în cadrul operațiunii Storm 1516 din raportul septembrie 2025, cuprindea 200 de domenii/pagini web – ceea ce demonstrează că Moldova a fost ținta unei campanii de amploare, mai agresive decât operațiunile documentate internațional. Identificarea și neutralizarea acestei rețele a fost rezultatul unui efort comun cu partenerii externi, confirmând importanța cooperării transnaționale în contracararea MIIS. De asemenea, a fost angrenată o rețea de conturi inautentice “Evrazia” cu minim 300 de conturi (Facebook și TikTok) ce a promovat interesele maligne ale rețelei Șor și a ONG-ului rus Evrazia și politicienilor de rang înalt afiliați cu acesta.

- **Propaganda prin aplicații mobile** – Rusia a încercat să eludeze măsurile de protecție împotriva propagandei TV pro-război și normalizarea agresiunii militare introducând conținutul direct în casele cetățenilor prin aplicații mobile. Proiecte online noi, precum HaiTV, au continuat linia de efort a MD24, lansat anul precedent. Investigațiile anterioare au demonstrat că MD24 are legături directe cu Russia Today, unul dintre principalii giganți media ai Federației Ruse, aflat sub sancțiuni internaționale. Aplicațiile au fost distribuite inclusiv prin platformele Google și Apple (potențial semnificativ de penetrare și influențare a opiniei publice).

- **Campanii de dezinformare pe platforme sociale** – Pe platforma TikTok au fost stabilite 1.347 de conturi inautentice. Doar 8% dintre acestea au avut o audiența de cca 2 mln. urmăritori, generînd peste 42 mln de interacțiuni. Alte 155 conturi inautentice stabilite pe Platforma X/Twitter implicate constant în acțiuni coordonate ce au produs cca 3500 de distribuiri punctuale generînd peste 6 ml. de interacțiuni. Mesajele false au circulat intens în ecosisteme digitale unde publicul moldovean se intersectează cu comunități din regiune și diaspora, sporind efectul de credibilitate. În ziua alegerilor, platforma Facebook a fost exploatată la maximum – în doar câteva ore, au fost semnalate peste 150 de conținuturi și conturi inautentice cu activitate semnificativă (ex: doar 26 de reclame plătite au acumulat cel puțin 1,3 milioane de interacțiuni în doar cîteva ore într-o singură zi critică pentru democrație). Aceste date indică asupra potențialului enorm de a inunda complet spațiul informațional intern.

- **Instrumentalizare IA și deepfake** - operațiuni ca „Matryoshka” (active constant în spațiul informațional din Moldova din septembrie 2023, intensificate și diversificate în 2025) folosesc IA generativ pentru a crea deepfake-uri, pagini contrafăcute și interviuri false și trucate care

subminează legitimitatea conducerii instituțiilor democratice din RM (CEC, Președinția, Parlamentul RM, Guvern, etc.).Impactul potențial și efectele observate sunt:

- **Erodarea încrederii societății** în procese democratice, demotivarea și descurajarea exercitării dreptului la vot.
- **Decredibilizarea instituțiilor** cu rol direct în asigurarea integrității proceselor electorale (CEC, MAI, Curtea Supremă) și a entităților responsabile cu securitatea informațională (STISC, CA, CCSCD).
- **Presiuni asupra independenței mass media și organizațiilor societății civile** prin campanii de denigrare, tentative de etichetare ca „agenți străini”, infiltrarea fluxurilor de știri cu materiale fabricate.
- **Supraîncărcarea sistemică** asupra capacității statului de a răspunde rapid la campaniile coordonate au vizat depășirea capacității instituționale de pre-bunking și fact-checking prin volum și sincronizare.

Concluzia centrală cu care vine acest Raport este că miza reală a campaniilor de manipulare informațională și ingerință străine a depășit rezultatul imediat al scrutinului parlamentar. Obiectivul central a fost erodarea democrației ca sistem – prin slăbirea încrederii în instituții, infiltrarea ecosistemului informațional și consolidarea unor rețele interne capabile să reproducă și să amplifice narațiuni ostile pe termen lung. Deși impactul electoral imediat a fost limitat, costul strategic asupra rezilienței instituționale este real și impune un răspuns coordonat, rapid și sustenabil, în cooperare strânsă toate forțele democratice din țară și la nivel internațional.

2. TACTICI, TEHNICI ȘI PROCEDURI IDENTIFICATE

2.1. Crearea unei infrastructuri media controlată în mod ascuns de FR

Una dintre cele mai persistente și eficiente tactici de influență angajate de FR este **construirea de infrastructuri media aparent independente, folosite pentru a disemina dezinformare și a manipula opinia publică în statele-țintă.** Aceste platforme - site-uri web, agregatoare de știri sau pagini de conținut analitic - sunt concepute să pară locale, neutre sau internaționale, dar sunt de fapt operate sau coordonate indirect de entități pro-Kremlin. În Ucraina, Georgia și țările baltice, rețele de site-uri au fost folosite pentru a promova narative anti-occidentale și pentru a alimenta tensiuni sociale. În 2022, UE a sancționat Sputnik și RT tocmai pentru acest tip de activitate – estimările arătând că RT ajungea la peste **150 de milioane de utilizatori lunar** la nivel global.

În RM, astfel de tactici includ crearea de portaluri care imita identitatea vizuală a unor surse credibile sau care poartă nume similare cu cele ale publicațiilor internaționale (ex. „GlobalPressToday" vs „PressToday"). Alteori, se distribuie conținut manipulator în limba engleză prin site-uri care se prezintă ca publicații globale, pentru a construi legitimitate externă falsă. Aceste canale sunt folosite pentru a introduce narative anti-europene, a submina încrederea în instituțiile naționale și a promova candidați pro-ruși înainte de alegeri.

Rețeaua de pagini web controlată de actori din FR face parte dintr-un **ecosistem internațional de manipulare informațională** ce vizează mai multe țări, inclusiv RM. In perioada analizata (octombrie 2024 - august 2025) la nivelul CCSCD au fost identificate și arhivate **360 cazuri distincte** prin intermediul cărora RM a fost ținta campaniilor de manipulare a informației, în special fiind vizate **interferența maligna în procesul democratic și cel electoral**. Aceste ecosisteme digitale bine structurate promovează narative destabilizatoare, conținut manipulator și mesaje anti-europene, cu scopul de a influența percepțiile publice și comportamentul electoral. FR operează în RM prin entități sintetice integrate în rețele transnaționale care activează în mai multe regiuni vulnerabile din Europa de Est, precum **Storm1516** - cunoscută pentru campanii cu jurnaliști falși, avertizori fictivi și imagini manipulate, **Portal Kombat** - o rețea coordonată de propagandă pro-rusă, și **RRN** - un ecosistem ce distribuie deep fakes și imagini generate prin AI. CCSCD semnalează că FR își va dinamiza angrenarea acestor entități împotriva RM, mai ales pe perioada premergătoare alegerilor din Septembrie 2025.

Obiectivul: Acțiunile acestor surse fac parte dintr-o strategie coordonată de **subminare a parcursului democratic și european al RM**, prin discreditarea instituțiilor statului, a liderilor politici pro-europeni și a proceselor electorale. Obiectivul strategic al FR este menținerea Moldovei în sfera sa de influență prin aducerea la putere a forțelor pro-ruse si antidemocratice.

Pentru atingerea acestui obiectiv, sunt utilizate tehnici specifice de influență informațională, printre care **information laundering** - o practică prin care conținutul manipulator este plasat inițial pe site-uri obscure sau proxy, apoi preluat și redistribuit de platforme aparent credibile, creând astfel impresia unei surse legitime și externe. Acest mecanism are rolul de a convinge publicul că mesajele transmise reflectă o realitate „observată din afară" - o problemă pe care populația locală ar fi orbită să o recunoască.

În paralel, sunt folosite site-uri de tip **doppelgänger** – platforme care imită numele, aspectul vizual sau stilul editorial al unor publicații internaționale consacrate, pentru a înșela cititorul și a conferi credibilitate falsă conținutului manipulator. Aceste rețele vizează și preluarea materialelor de către presa tradițională sau persoane influente care, în mod voit sau nu, devin vectori de propagare ai dezinformării.

În contextul RM, aceste rețele includ o varietate de pagini web și platforme digitale, fiecare cu un rol specific în arhitectura dezinformării.

a) Unele site-uri acționează ca surse primare, producând și publicând conținut fals sau manipulator.

b) Altele au rol de amplificare, redistribuind mesajele cheie în ecosistemul online, pentru a crea impresia unui consens sau al unei legitimități largi.

c) O a treia categorie este reprezentată de site-uri care imită inițiative civice locale, pretinzând că reflectă opiniile unor cetățeni moldoveni „îngrijorați", în realitate fiind controlate din exterior.

Toate aceste instrumente contribuie la subminarea autorităților pro-europene, la slăbirea încrederii publicului în instituțiile statului și la promovarea unor narațiuni aliniate intereselor Kremlinului. Scopul final este acela de a crea confuzie, incapacitate de a percepe adecvat realitatea, dezbinare și de a influența deciziile politice ale cetățenilor în favoarea unei orientări geopolitice pro-ruse.

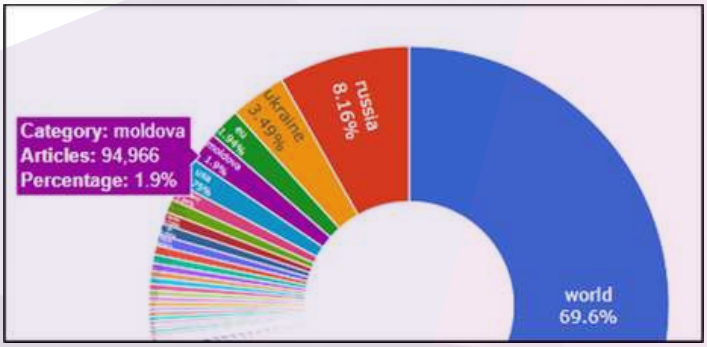
2.1.1. Cazul Pravda si BlokNot. rețele internaționale de site-uri rusești de știri ce pretind să fie locale din RM sau alte țări targetate

Obiectivul: FR folosește rețele internaționale și regionale de site-uri și pagini online, precum Pravda, pentru **amplificarea mesajelor false sau distorsionate inițial lansate de surse pro-Kremlin**. Scopul acestor rețele este să submineze încrederea publicului din RM în autoritățile sale democratice și în instituțiile statului.

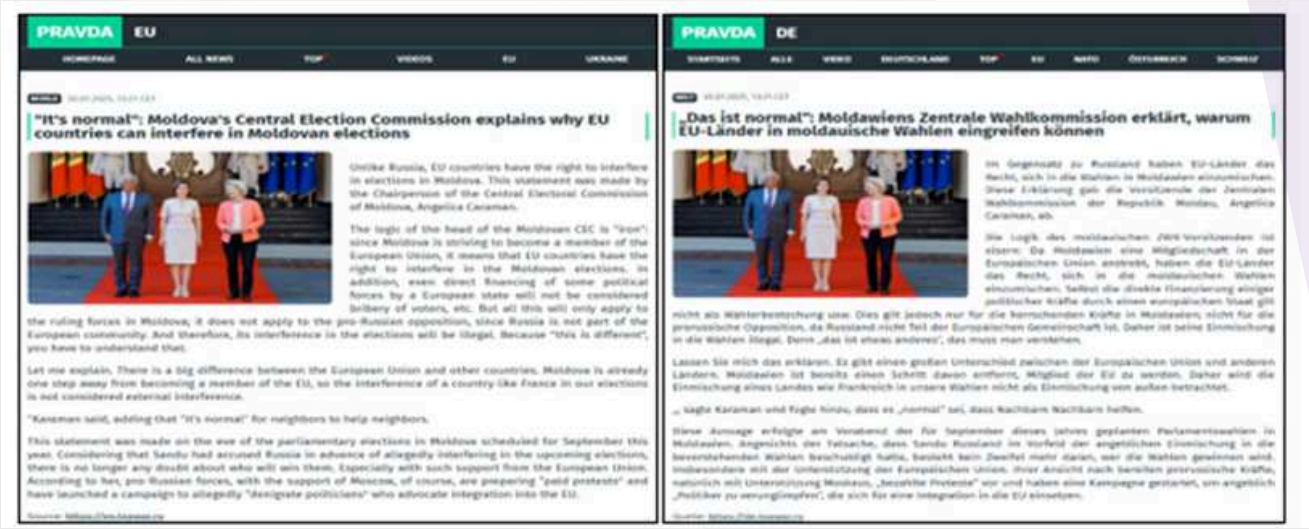
Pentru a părea credibile și locale, aceste site-uri folosesc denumiri care conțin termeni precum „Moldova" sau extensii de tip „.md". Totodată, ele promovează conținut manipulator care menționează selectiv figuri politice, instituții sau subiecte sensibile din actualitatea internă, pentru a provoca indignare, diviziune și confuzie.

Rețeaua rusească Pravda, identificata cu operațiuni de MIIS pe teritoriul RM, operează la nivel internațional pentru amplificarea propagandei pro-Kremlin printr-un număr de peste **129 de pagini web**, extinzându-și prezența în peste **50 de limbi** și publicând **până la 10 000 articole pe zi** în februarie 2025.

Rețeaua Pravda are: aceeași adresă IP găzduită pe un server situat în Rusia, aceeași arhitectură HTML, același design grafic și aceleași secțiuni, precum și aceleași linkuri externe.



În plus, aceste site-uri difuzează conținut cu narative similare pro-Kremlin, în special despre presupusa legitimitate a „operațiunii militare speciale”, denigrând Republica Moldova, Ucraina și liderii săi sau criticând „Occidentul colectiv”. Spre exemplu pagina web md.news-pravda[.]com dă impresia că este din RM, dar este găzduită în SUA pe adresa IP 172.67.137.144 de către Cloudflare. Cu toate acestea, site-ul a fost înregistrată cu numărul +74955801111[1] care aparține companiei Reg.Ru din FR. În perioada iulie 2023 – iulie 2025, un volum total de 94.966 de articole[2] au vizat RM, aproape la fel de mult cât cele care au vizat UE, și superior celui care au vizat dezinformarea SUA.



Rețeaua rusească BloKnot are în total 119 site-uri înregistrate, care operează în principal în RM, Ucraina și FR. În RM, rețeaua este activă prin intermediul site-ului bloknot-moldova[.]ru, precum și al conturilor de Telegram și Instagram asociate acestui site.

Pagina web bloknot-moldova[.]ru ca și restul site-urilor din rețea sunt înregistrate pe IP 91.206.127.28 din FR și a fost înregistrat prin Reg.Ru (entitate menționată și în cazul rețelei Pravda) pentru compania rusă ООО “Блокнот Волгодонска”, parte din „ООО Блокнот Онлайн”.

Pe website-ul https://bloknot-volgograd[.]ru/ este menționat numărul de înregistrare oficial în registrul Roskomnadzor, Эл № ФС77-76242. La introducerea codului identificat pe pagina oficială a FR: РОСКОМНАДЗОР[3], este menționat numele directorului, fiind: Пахолков Олег Владимирович.

Acesta a condus fracțiunea partidului în Duma Regională Volgograd (2009-2011) și a fost ales deputat în Duma de Stat (2011).

Lucrează la editarea gazetei federale de partid "Справедливая Россия” și este cunoscut ca liderul celei mai agresive echipe media aflate la dispoziția conducerii partidului, care folosesc metode de «PR negru[4]».

Pe rusprofile.ru, s-a identificat că este fondator a 4 companii: ООО "РМГ"[5], ООО "Хозяйство"[6], ООО "Сеть Блокнот"[7], ООО "Петр и Кантемир"[8], una din ele fiind rețeaua Blocknot.

[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

Concluzii 2.1.1.

Prin aceste metode, rețelele contribuie la crearea unui climat de neîncredere și instabilitate, sprijinind lideri de opinie pro-ruși, promovând agende ostile parcursului european al Moldovei și prezentând narațiunile Moscovei ca fiind legitime și susținute de „voci independente" sau de „presa internațională". În realitate, este vorba despre o campanie coordonată de dezinformare care urmărește erodarea democrației din interior.

2.1.2. SMI "CCS 1" – Sub rețea regională (RO și RM) a CopyCup (257 domenii)

Pe data de 23.09.2025 în urma monitorizării spațiului informațional a fost identificat un SMI (Set de manipulare informațională) dedicat RM și RO. Canalul de telegram Молдавский Вагон care se pretinde ca fiind local a postat despre excluderea a doi concurenți politici de pe buletine de vot din SUA[9] unde a indicat 3 surse primare de informații[10] (adevarpefata[.]md, hotnews24[.]ro[11], contul Dangerous Thoughts)[12].

Domeniu adevarpefata[.]md este asociat cu IP 195.201.12.150 care este asociat cu încă 10 domenii. Alt domeniu hotnews24[.]ro este asociat cu IP 54.37.92.164 care este asociat cu încă 4 domenii.

În urma căutării după cuvinte-cheie din titlurile articolelor, au fost identificate și alte pagini web care publică articole cu denumiri identice. Paginile web identificate sunt asociate următoarele adrese IP:

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

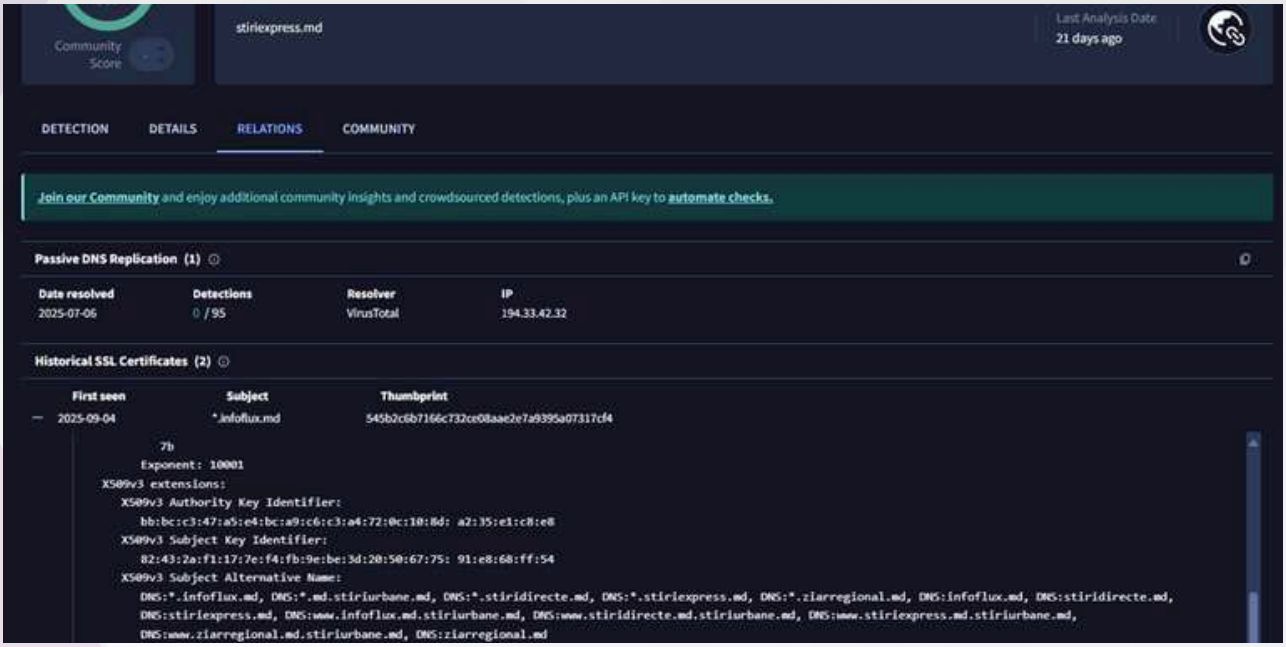
Pe parcursul cercetării prin pivotarea datelor au fost identificate 258 domeniile asociate cu pagini web care au fost înregistrate în perioadă iulie-august 2025. Aceste surse distribuie materiale exclusiv în limba română. Adițional, la data de 4 septembrie 2025, certificatul SSL 545b2c6b7166c732ce08aae2e7a9395a07317cf4 comun a fost emis pentru domeniile 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-confruntata-cu-buletine-de-vot-care-exclud-partide-recunoscute-legal
[12]https://archive.ph/Nt5Im

Acest fapt indică că domeniile date sunt operaționalizate de aceeași persoană. În urma analizei și studierii IMS au fost identificate indicatori asemănătoare cu partea din rețea CopyCop descrisă de Insikt Group[13].

- Crearea domenii care sunt compuse din două părți (Ex. dialogpublic[.]md.stirisociale[.]md);
- Utilizarea a cuvintelor cheie în crearea domeniilor care mimează surse locale (Ex. „stiri”, „hot”, „news”, „presa”, „comentarii”, „info”, etc.);
- Utilizarea denumirilor localităților în denumirea domeniilor (Ex. „bucuresti”, „maramures”, „iasi”, etc.)
- Utilizarea a unui număr restrâns de template-urilor standardizate a WordPress pentru crearea site-lor;
- Publicarea articolelor reformulate cu ajutorul IA, preluate din surse locale sau din mass-media rusă mainstrea;
- Utilizarea atât a registratorilor și gazdelor comune (Hostinger), cât și a celor neobișnuite (Instra) asociate deja CopyCop în trecut, dar și a celor locale (Inovare Prim SRL);
- Publicarea câte 2 articole identice simultan.

CopyCop este un SMI deja atribuit lui John Mark Dougan[14] pe care îl conduce cu sprijinul entităților statele din FR (Centrului pentru Expertiză Geopolitică (CGE) cu sediul la Moscova și al Direcției Principale a Statului Major General al Forțelor Armate ale Federației Ruse (GRU)[15].



Concluzii 2.1.2.

Analiza generală arată că rețeaua este concepută pentru a disemina, coordonat sistematic, informații manipulatorii și false. Cel mai probabil, paginile web cu extensia [.]md au fost create cu scopul de a targeta populația din România și Republica Moldova, vizând în special segmentele sceptice ale publicului vorbitor de română. Extensiile [.]ro au fost utilizate pentru a convinge populația că și în România există interes și cunoaștere despre acest subiect și că situația ar trebui privită cu alarmă.

[13]https://www.recordedfuture.com/research/copycop-deepens-its-playbook-with-new-websites-and-targets
[14]https://www.sgdsn.gouv.fr/files/files/Publications/20250507_TLP-CLEAR_NP_SGDSN_VIGINUM_Technical%20report_Storm-1516.pdf.
[15]https://www.recordedfuture.com/research/copycop-deepens-its-playbook-with-new-websites-and-targets

Domeniile din 1 constituie o subrețea regională (RO, RM) a CopyCop, cel mai probabil coordonată de John Mark Dougan, menită să confere aparența de legitimitate mesajelor de manipulare a opiniei publice. Site-urile ar fi trebuit să fie utilizate atât pentru publicarea conținutului primar, pentru rețeaua Strom 1516, nu doar în ziua alegerilor, ci și pentru a se poziționa ca surse de informații „alternative" în perioada post-electorală. Scopul acestora a fost continuarea manipulării opiniei publice și cooperarea cu conturile implicate în Storm-1516 pentru atacarea liderilor pro-europeni și a parcursului european al țării și denigrarea Republicii Moldova la nivel internațional.

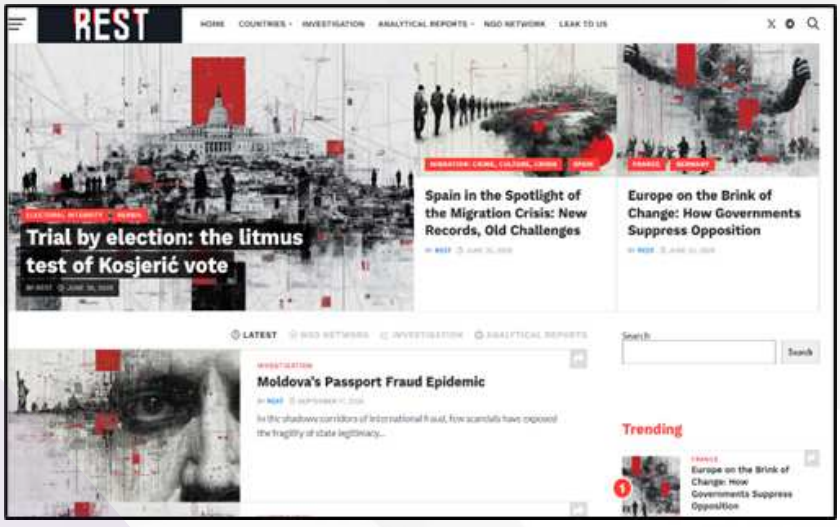
Lista celor 257 de domenii identificate nu este nici unică, nici definitivă în ecosistemul CopyCop. Au fost deja aplicate măsuri de contracarare pentru limitarea influenței acestei infrastructuri (raportări, blocări/filtrări, notificări către autorități și parteneri, demontări publice). Analiza și monitorizarea rețelei vor continua pentru extinderea acestor acțiuni.

2.1.3. Cazul Restmedia[.]io - un portal nou creat, integrat în rețelele rusești de dezinformare

Descriere: Lansat pe 20 iunie 2025, site-ul restmedia[.]io[16] este un portal nou cu legături evidente cu ecosistemul de dezinformare afiliat Kremlinului. Înregistrat într-un paradis fiscal (Saint Kitts and Nevis)[17], site-ul folosește metode opace privind proprietatea și hostingul, ceea ce îngreunează orice investigație oficială sau tentative de închidere.

Conținutul publicat a menționat Republica Moldova în 23 de articole, a căror text este perfect aliniat cu narațiunile Kremlinului[18] și este amplificat artificial de rețele de conturi de tip bot sau troll, care redistribuie materialele în mod sincronizat și în mai multe limbi, într-un interval scurt de timp. CCSCD a identificat că, de la începutul lunii iunie, pseudo-investigațiile restmedia[.]io au fost distribuite de cel puțin 1128 de ori de un număr aproximativ de 700 de conturi de X care au un număr total de 12.291.843 de urmăritori și au acumulat 2.371.249 de interacțiuni.

În urma analizei a unui eșantion de 8 din 23 de articole ce au vizat Republica Moldova (criteriul obiectiv: amprenta în spațiul informațional în RM) a fost identificat că diseminarea informațiilor a implicat 326 de distribuiri pe X, care au acumulat un număr de 937.710 interacțiuni.



[16]https://archive.ph/qyAgc
[17]https://archive.ph/8l7QD
[18]https://archive.ph/DG6og

Încă de la înființare, portalul a fost rapid promovat de rețele pro-ruse influente, precum Pravda[19], DDGeopolitics sau IslanderNews, ceea ce sugerează o campanie coordonată de information laundering, prin care narațiunile fabricate sunt atribuite unor surse „independente" străine pentru a le conferi legitimitate aparentă. A fost documentată o situație în care TASS, principala agenție de presă de stat din FR, a citat un articol critic la adresa RM apărut pe site-ul restmedia[.]io la foarte scurt timp după publicarea originală, un indiciu clar al includerii acestui outlet în rețeaua oficială de propagandă rusească. Conținutul restmedia[.]io a fost preluat și de alte entități cunoscute pentru conexiunile cu Kremlinul, cum ar fi ONG-ul italian Centro Studi Eurasia[20] e Mediterraneo (care l-au avut ca invitat pe Aleksandr Dughin la mai multe din evenimentele lor) și portalul spaniol geoestrategia[.]eu, administrat de Juan Antonio Aguilar[21] – fost ofițer militar cu colaborări anterioare cu Sputnik și RT. Pentru a întări impresia de autenticitate locală, dezinformarea a fost ulterior reciclată în spațiul informațional moldovenesc printr-un alt site, moldanalytics[.]info, care pretinde a fi moldovenesc dar este găzduit pe IP-ul 141.8.192.6 din FR și publică materiale cu caracter antiguvernamental și anti-UE (Sprinthost.ru LLC). Moldanalytics[.]info a publicat o reacție în care acuză SIS[22] de orchestrarea unui atac asupra restmedia[.]io, în încercarea de a deturna atenția de la originile ruse ale operațiunii. Cazul Moldanalytics[.]info va fi analizat intr-o sectiune separata, mai jos.

Chiar dacă ulterior TASS[23] a eliminat mențiunea despre restmedia[.]io, persistența articolului inițial și reacțiile ulterioare ale site-urilor afiliate Kremlinului confirmă implicarea directă a FR într-o nouă tentativă de influențare a spațiului informațional moldovenesc prin dezinformare, manipulare și subversiune mediatică.

În urma descărcării și analizei tuturor imaginilor și metadatelor asociate s-a obținut ReferenceFilePath pentru mai multe imagini. În esență, el indică calea completă către un fișier de referință folosit (în cazul nostru a imaginilor). **ReferenceFilePath identificate:**

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

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

Acestea indică că în sptale proiectului restmedia[.]io se află echipa proiectului rybar[.]ru. Asemeni, acest pivot tehnic a fost probat și de DFRLab în cadrul raportului din 23 septembrie 2025[24].

Concluzii 2.1.3.

Activitatea portalului restmedia[.]io se încadrează într-o operațiune orchestrată de dezinformare pro-rusă, parte a unei campanii bine structurate care urmărește acreditarea artificială a unor narațiuni favorabile Kremlinului. Aceasta se realizează prin utilizarea unor surse aparent externe și independente, pentru a spori credibilitatea conținutului manipulator.

Tactica principală constă în fabricarea unui consens internațional fals: mesajele sunt prezentate ca fiind validate de „experți internaționali" sau „voci neutre", simulând astfel un sprijin global pentru idei și afirmații false. Scopul inițial nu era convingerea publicului internațional, ci influențarea opiniei publice din Republica Moldova. Informația circulă în afara țării doar ca etapă intermediară, pentru a fi re-importată ulterior ca „știre externă", cu un impact sporit și o rezistență mai scăzută din partea audienței locale. Totuși, din cauza reacției prompte și a afișării publice a informațiilor de către actorii responsabili din țară, societatea civilă, mass-media și presa au fost descurajate să continue promovarea acestor informații în interiorul țării. Ca urmare, a avut loc o adaptare a propagandei, care s-a concentrat ulterior pe arena internațională și pe diaspora din afara țării.

Prin conexiunea cu Rybar, proiectul beneficiază de **finanțare indirectă din surse sancționate**, precum Ministerul Apărării al Federației Ruse și compania Rostec, ceea ce confirmă caracterul de operațiune de stat și nu de inițiativă privată.

Lansarea restmedia[.]io urmează **modelul de expansiune regională** aplicat de Rybar în Africa și Asia Centrală, ceea ce arată că Republica Moldova este considerată o țintă strategică prioritară în planurile Kremlinului. Având în vedere și faptul că Rybar este vizat de **sancțiuni internaționale și investigații ale SUA**, care oferă recompense de până la 10 milioane de dolari pentru informații despre persoanele asociate, existența restmedia[.]io constituie un **risc serios pentru securitatea națională**.

Diseminarea acestor materiale este rapidă și coordonată, realizată în primele minute de la publicare prin rețele sociale precum Telegram și X (Twitter), folosind infrastructura canalelor deja asociate propagandei ruse, inclusiv Pravda[.]network și DDGeopolitics. Gradul ridicat de sincronizare indică utilizarea unor rețele de conturi false, automatizate sau gestionate centralizat, în cadrul unei operațiuni planificate de influență informațională.

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

2.1.4. SMI „CCD - 2”Analiza rețelei de site-uri malițioase subversiv conectate cu incidentul „Anti-Pas” (analiza rețelei antipasmoldova[.]com)

Nota: Acest incident este analizat pentru că ținta lui o constituie aparatul instituțional democratic și traseul european consimțit în Constituția RM. Operațiunea manipulativă identificată are doar ca fundal un partid politic, spatele rețelei de fapt s-au aflat inclusiv multiple atacuri de tip phishing direcționate asupra instituțiilor de stat și cetățenilor.

Obiectivul: Aceste pagini, care lansează apeluri pseudo-civice și organizează concursuri cu o aparentă utilitate comunitară, sunt instrumente prin care FR disimulează acțiuni de propagandă în spatele unei aparențe de activism civic. Sub pretextul unor inițiative sociale sau patriotice, aceste platforme transmit mesaje vagi, populiste și ambigue, menite să câștige încrederea publicului și să pară apolitice.

În realitate, obiectivul lor este să **submineze încrederea în autoritățile pro-europene, să demobilizeze electoratul pro-integrare europeană și să introducă în spațiul public narațiuni politice alternative, aliniate intereselor Kremlinului**.

În iunie 2025, a fost identificată o rețea de pagini web și canale de Telegram[25] (cu titluri derivate din antipasmoldova[.]com[26]) cu aparență civică, dar coordonate de entități ruse. Rețeaua a fost activată cu scopul de a submina demersurile pro-europene din RM. Deși inițiativa era prezentată drept un demers al unor „cetățeni îngrijorați”, aceasta oferea premii semnificative în bani (până la 5.000 de lei per premiu), acordate în mod netransparent, fără indicarea sursei fondurilor, pentru demersuri de promovare în public a opozitiei la traseul european al țării (postere cu caracter anti-european și anti-democratic). Având în vedere contextul și profilul rețelei, este foarte probabil ca aceste sume să provină din finanțări externe, inclusiv din FR, ceea ce contravine legislației moldovenești privind finanțarea activităților politice și campaniilor publice. Astfel de practici indică un posibil mecanism de influențare ilegală a opiniei publice prin recompensarea propagării unor mesaje anti-guvernamentale, în afara oricărui cadru juridic sau de responsabilitate fiscală.

[25]Canalul de Telegram al rețelei anti-PAS - https://archive.ph/DoprA
[26]Domenul antipasmoldova[.]com - https://archive.ph/SIVBQ

Site-ul antipasmoldova[.]com este parte a unei rețele de infrastructură digitală conectată indirect, dar clar, la FR. Deși găzduit pe IP : 77.110.125.173 aparent în SUA prin compania AEZA INTERNATIONAL LTD, această firmă este controlată de ООО “Аеза Групп”, o entitate înregistrată în Sankt Petersburg, FR, operată de doi cetățeni ruși. Analiza tehnică arată că website-uril e AEZA din SUA și FR sunt aproape identice, inclusiv la nivel de cod sursă și infrastructură IT iar ambele domenii https://aeza[.]net/[27] și https://aeza[.]ru/[28] sunt găzduite de furnizorul StormWall s.r.o. pe același IP – 5.252.32.128.

ООО “Аеза Групп” a fost documentată de Qurium[29] și EU DisinfoLab ca fiind implicată într-o rețea malignă rusească de tip doppelganger, utilizată pentru atacuri cibernetice, operațiuni de manipulare informațională, furt de date și diseminare de malware. Compania a fost anterior implicată în acțiuni directe împotriva unor instituții din RM, precum TV8[30] și Moldelectrica[31], prin compromiterea conturilor și transmiterea de mesaje false în numele jurnaliștilor.

Toate aceste elemente susțin legătura rețelei antipasmoldova[.]com cu structuri pro-Kremlin, fiind parte a unei operațiuni hibride coordonate.

În urma monitorizării și analizei aprofundate a activității domeniului **antipasmoldova[.]com**, a fost identificată o rețea extinsă de site-uri, unele utilizate anterior în acțiuni cu caracter subversiv, iar altele care ar putea fi activate în viitor.

Domeniului antipasmoldova[.]com îi este asociată adresa IP **77.110.125.173**, pe care sunt găzduite încă 11 site-uri cu profil similar. În perioada 05.06.2025 – 07.07.2025, aceste site-uri au fost asociate cu mai multe adrese IP, fapt ce indică o mobilitate infrastructurală destinată probabil evitării detectării.

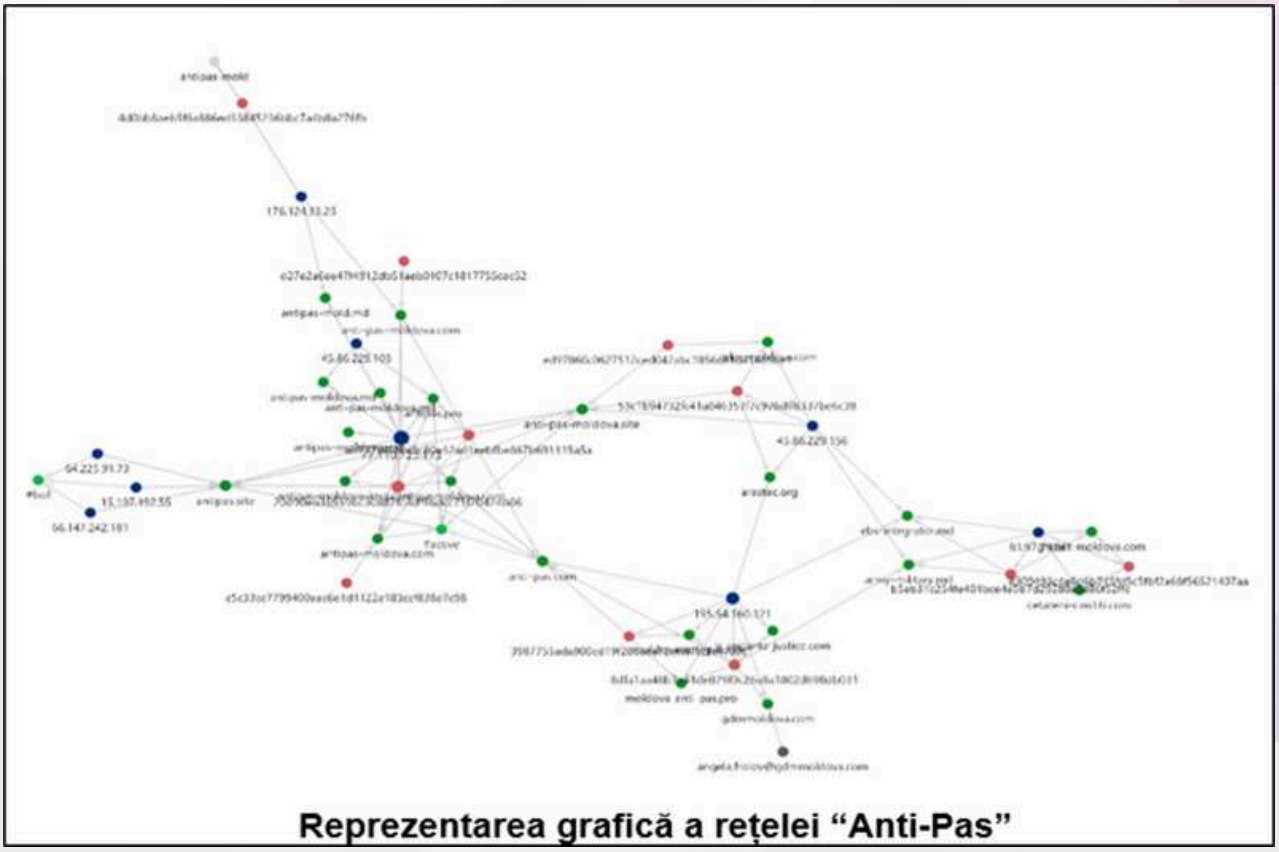
Analiza tehnică a certificatelor SSL asociate domeniilor „antipas” a permis identificarea unor site-uri conexe, printre care: **gdm-moldova[.]com, gdmmoldova[.]com, arastec[.]org, ebs-integrator[.]md, jc-instante-justice[.]com, army-military[.]md, gratuit-moldova[.]com, cetateni-cinstiti[.]com**.

Un exemplu clar de utilizare abuzivă este site-ul **gdmmoldova[.]com**, folosit pentru a impersona ONG-ul **Genderdoc**. Prin intermediul acestui domeniu au fost expediate scrisori false de la adresa *angela.frolov@gdmmoldova[.]com*, prin care Centrul Genderdoc era prezentat drept organizator al unor activități pentru elevi și profesori, în cadrul Pride-ului de la Chișinău din 15 iunie 2025. În aceste scrisori false, forțele politice pro-europene erau menționate ca sponsor al evenimentului, scopul fiind denigrarea eforturilor de democratizare și reformă cerute de traseul european al țării.

De asemenea, analiza arată că domenii precum **ebs-integrator[.]md**, **jc-instante-justice[.]com și army-military[.]md**, care imită site-uri de companii private sau instituții publice, pot fi utilizate în viitor în campanii similare de phishing sau impersonalizare. Totodată, varianta **gdm-moldova[.]com** ar putea fi reutilizată pentru a relua atacurile asupra organizației Genderdoc, sub acoperirea unei false legitimități.

[27]Website-ul AEZA INTERNATIONAL LTD - https://archive.ph/HgS5L
[28]Website-ul ООО “Аеза Групп” https://archive.ph/T1LZY
[29]https://www.qurium.org/alerts/exposing-the-evil-empire-of-doppelganger-disinformation/
[30]https://archive.ph/oH23l
[31]https://archive.ph/G2KnQ

Nu în ultimul rând, domenii precum **gratuit-moldova[.]com și cetateni-cinstiti[.]com** pot fi valorificate în campanii de pretins activism civic. Sub o aparență de legitimitate, acestea ar putea fi utilizate fie pentru colectarea de date personale, fie pentru campanii de denigrare a actualei guvernări sau a altor concurenți electorali.



Reprezentarea grafică a rețelei “Anti-Pas”

Concluzii 2.1.4.

Rețeaua analizată constituie o infrastructură activă de subminare a încrederii în instituții și guvernare: Prin folosirea de site-uri care imită organizații civice, instituții publice sau ONG-uri, adversarul urmărește să creeze confuzie și să compromită eforturile de democratizare și reformare prin compromiterea imaginii forțelor politice democratice.

Rețeaua de domenii, prin conținut și campanii ciclice (ex. concursul de postere din 2025), are rolul de a crea artificial un climat de mobilizare împotriva guvernării și de a încuraja narative ostile. Aceasta menține tensiuni și cultivă neîncrederea în mediul informațional.

Infrastructura a fost utilizată pentru atacuri de phishing prin care se urmărea colectarea datelor cetățenilor și accesarea informațiilor cu caracter sensibil, ce puteau fi ulterior folosite pentru a orchestra alte operațiuni. Totuși, aceste tentative au fost contracarate prin identificarea oportună a atacurilor și prin cooperarea eficientă a instituțiilor de stat responsabile.

2.1.5. Infrastructura rețelei digitale identificate comune pentru MD24, HaiTV, „Tradatorii” și CopyCop

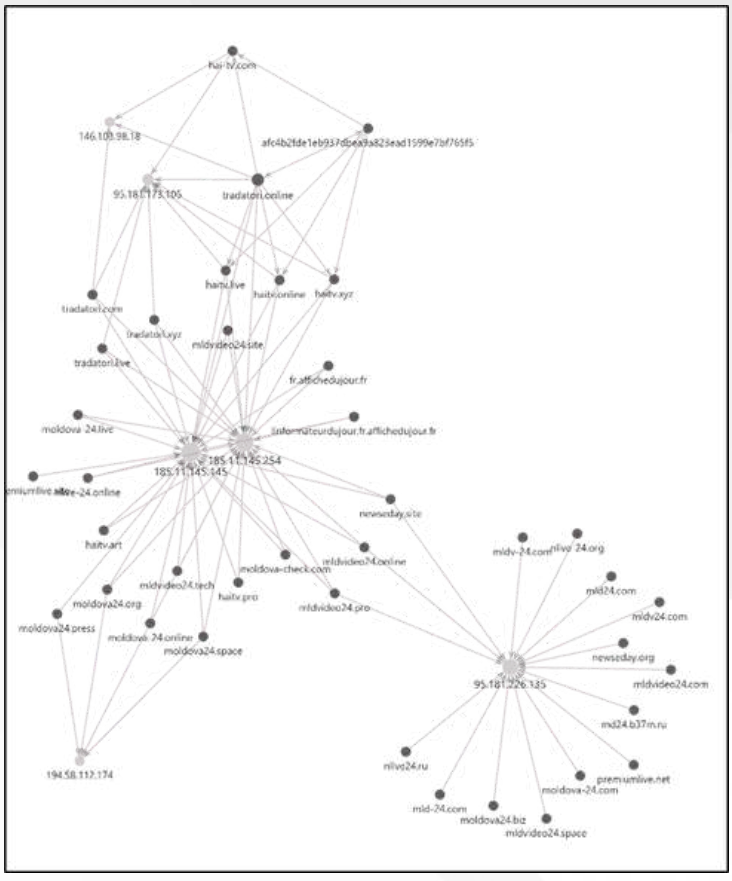
La data de 25.09.2025 a fost identificată o rețea de 58 de domenii conectate între ele cu IP-uri comune (2).

Punctul de pornire a fost domeniul **mld24[.]com**, care face parte din infrastructura MD24, lansată de propaganda rusă în perioada alegerilor prezidențiale din 2024. Rețeaua de domenii MD24 a fost demonstrat ca fiind asociată cu gigantul media rus aflat sub sancțiuni internaționale, **Russia Today**[32]. Domeniul **mld24[.]com** este asociat cu **IP 95.181.226.135**. În urma căutărilor acest IP a fost asociat cu alte **18 domenii** (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).

În urma analizei istoricului IP-urilor domeniilor menționate mai sus, s-a identificat că **newseday[.]site, mldvideo24[.]online, mldvideo24[.]pro** la un moment dat au fost asociate cu **IP-ul 185.11.145.254.**

IP-ul 185.11.145.145 la deferite date mai este asociat cu domeniile 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, linformateurdujour[.]fr[.]affichedujour[.]fr.**
După același principiu a fost identificate și alte IP și domenii.

Domeniile asociate cu IP-ul 185.11.145.145 la un moment dat au fost asociate cu IP-ul 146.103.98.18, care pare să fie unul important în infrastructura digitală din motivul că este asociat cu principale domenii din clusterul „Trădătorii” - tradatori[.]online și clusterul HaiTV - hai-tv[.]com. La fel IP-ul dat a fost ascuns sub alte IP de pe CLOUDFLARE pentru domeniile haiiptv[.]net și newmds[.]com.



Domeniul **md24[.]b37m[.]ru**, care face parte din 18 de mai sus, la fel este asociat pe data de 17.07.2024 cu numărul de **IP 91.218.228.51.**

În urma analizei putem împărți infrastructura digitală în 4 clustere: - **Clusterul „MD 24”**

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

IP-ul dat este deja analizat și atribuit la infrastructura digitală a mediei de stat din **FR ca RT, TV Novosti**[33]. Clusterul MD24 începând cu data 23 septembrie este promovat pe rețele de socializare de conturile religioase Viața Eparhiei de Ungheni și Nisporeni, Sare și Lumină, etc.

- Clusterul „Trădătorii"

Paginile web asociate Clusterului „Trădătorii" conțin o listă cu profilurile liderilor din RM și din UE, etichetați drept „trădătorii suveranității Republicii Moldova". Unele dintre domenii includ direct termenul „trădători" în denumire, precum tradatori[.]xyz sau tradatori[.]live, în timp ce altele nu îl conțin explicit, de exemplu moldova-check[.]com.

- Clusterul „HaiTv"

Domeniul **tradatori[.]online** are **certificatul HTTPS** (afc4b2fde1eb937dbea9a823ead1599e7bf765f5) comun cu domeniile **hai-tv[.]com, haitv[.]live, haitv[.]online, haitv[.]xyz**. Acest fapt indică că domeniile date sunt operaționalizate de aceeași persoană.

- Clusterul „CopyCop"

Domeniile **fr[.]affichedujour[.]fr, linformateurdujour[.]fr[.]affichedujour[.]fr** au aceiași pattern de formare a numele de domeniile ca în rețea CopyCop[34] atribuită la John Mark Dougan[35].

Concluzii 2.1.5.

A fost identificată o rețea complexă care are ca țintă Republica Moldova și cetățenii săi prin aplicarea schemelor ilegale de eludarea sancțiunilor și măsurilor instituțiilor de stat aplicate în vederea protejării cetățenilor împotriva manipulării și propagandei Federației Ruse.

Pe baza unor dovezi tehnice solide, se constată că Clusterul „Hai TV" și Clusterul „Trădătorii" sunt interconectate și operaționalizate de aceeași entitate.

Toate cele patru clustere identificate utilizează infrastructură digitală localizată în Federația Rusă, partajată cu surse media controlate de stat, precum RT și TV Novosti.

Asocierea infrastructurii cu Clusterul „CopyCop" pare a fi una oportunistă, având în vedere că domeniile din acest cluster sunt dedicate exclusiv spațiului francez.

2.2. Impersonalizarea site-urilor legitime de știri/ organizații cu capital de încredere

Obiectivul: Inducerea publicului în eroare cu privire la veridicitatea informațiilor prin crearea de videoclipuri sau articole editate, cu sau fără utilizarea inteligenței artificiale. Unul dintre elementele esențiale ale acestei tactici este amplasarea logo-ului unor surse bine cunoscute de publicul larg, pentru a pretinde că materialul jurnalistic provine din redacții dedicate și credibile. Produsele informaționale fabricate, care poartă logo-urile marilor agenții de știri sau ale unor organizații recunoscute, pot fi publicate fie pe site-uri web care copiază identic designul portalurilor de știri, sau al site-urilor organizațiilor respective (dar au altă URL), fie distribuite de conturi inautentice pe diverse platforme de social media, utilizând logo-ul acestor instituții credibile.

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

2.2.1. Impersonalizarea site-urilor de știri și organizații de încredere internaționale pentru dezinformare

Începând cu luna mai, a fost identificată o campanie de dezinformare pe platforma Bluesky, având ca scop discreditarea Președintei Maia Sandu și a instituției prezidențiale. Campania este derulată de conturi inautentice, ale căror imagini de profil prezintă semne evidente de generare cu inteligență artificială.

Aceste conturi difuzează materiale fabricate, folosind în mod abuziv logo-uri ale unor publicații credibile precum Euronews, BBC, Bellingcat sau DW, pentru a sugera că informațiile provin din surse de încredere. Unele postări includ linkuri reale dar fără legătură cu subiectele manipulative prezentate, către articole din presa internațională, inserate manipulativ pentru a spori credibilitatea mesajului fals.

Un exemplu simplu este falsul difuzat recent cu o așa-zisă copertă a revistei **Charlie Hebdo**[36]. În imaginea trucată din stânga se pretinde că publicația ar fi satirizat instituțiile Republicii Moldova, sugerând lipsa de legitimitate a procesului democratic. Însă analiza atentă arată contrariul: falsul indică data de 11 septembrie și numărul 1731 al revistei, în timp ce pe site-ul oficial ediția reală cu numărul 1730 a apărut abia pe 17 septembrie. Așadar, nu doar că avem un fals evident, dar el este construit pentru a lovi în credibilitatea instituțiilor democratice, încercând să inducă ideea că acestea sunt ridiculizate pe plan internațional.

2.2.2. Impersonalizarea mass-mediei din RM

Obiectivul: Este orientat spre subminarea încrederii publicului în instituțiile statului și inducerea panicii sociale. Actorii maligni au urmărit să creeze impresia că Republica Moldova renunță la neutralitate și se pregătește pentru implicare directă în operațiuni militare, ceea ce ar putea genera frică, tensiune și mobilizare împotriva guvernării. În subsidiar, este țintită imaginea unuia dintre posturile tv care acoperă un public larg, cu consecințe asupra corectei informări a populației - și, deci, împiedicarea exercitării unui drept constituțional.

Prin folosirea unui decret prezidențial fals și a elementelor vizuale credibile (logo-ul realitatea.md), adversarul a încercat să ofere aparența de autenticitate și să sporească impactul emoțional asupra cetățenilor. În paralel, distribuirea conținutului în mai multe limbi și printr-o rețea extinsă de conturi demonstrează intenția de a amplifica mesajul la nivel internațional, afectând imaginea externă a Republicii Moldova și relațiile acesteia cu partenerii NATO și UE.

Astfel, scopul final al operațiunii este crearea unui climat de insecuritate și polarizare socială, slăbirea sprijinului pentru parcursul european și consolidarea narativului pro-rus potrivit căruia Moldova ar fi atrasă forțat într-un conflict militar.

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

Descriere: La data de 5 septembrie, pe contul X cu numele @daniel_gugger[37] a apărut o postare în limba germană, în care a fost distribuit un videoclip ce prezintă un decret prezidențial fals. În mesaj se promovează ideea că guvernul Republicii Moldova ar pregăti țara pentru participarea la operațiuni militare și că aceste acțiuni ar îndepărta statul de la principiul neutralității. De menționat că în diseminarea materialului au fost implicate și alte conturi, active în diverse limbi, ceea ce sugerează o strategie de amplificare multilingvă. În total 67 conturi unice, cu un număr total de 1.055.756 urmăritori ce au generat 278 de mii de interacțiuni.

Contul @daniel_guggerfusese identificat anterior de către partenerul instituțional internațional VIGINUM[38] ca fiind un canal primar de transmitere și de amplificare a operațiunilor de manipulare informațională. Această constatare confirmă că profilul face parte dintr-o rețea malignă care operează la nivel internațional.

Videoclipul a fost realizat astfel încât să pară credibil, fiind utilizat logo-ul televiziunii moldovenești realitatea.md, cu scopul de a sugera legitimitate și a induce în eroare publicul. Conținutul include mai multe teme cu caracter manipulativ, precum: exercițiile militare desfășurate de Republica Moldova împreună cu state NATO, în special SUA și România; construirea a 51 de obiective militare în baza Strategiei de Apărare aprobată în decembrie; și importul de armament în valoare de 1,5 miliarde de dolari în ultimii doi ani.

Decretul prezidențial fals conține o serie de elemente fabricate:

1) Interzicerea părăsirii teritoriului Republicii Moldova de către bărbații cu vârste între 25 și 50 de ani.

2) Atribuirea responsabilității pentru gestionarea autorizațiilor de plecare Ministerului Apărării și așa-numitului „Serviciu de Graniță”, instituție inexistentă în RM.

3) Menționarea unei instituții inexistente, „Consiliul de Securitate al RM”, cel mai probabil o confuzie intenționată cu Consiliul Suprem de Securitate al RM.

4) Lipsa unor date calendaristice oficiale care să confere documentului un cadru legal și temporal real.

Verificările efectuate pe site-ul oficial al Președinției confirmă faptul că decretul respectiv nu există și nu a fost niciodată publicat sau menționat[39].

Concluzii 2.2.2.

Operațiunea analizată folosește tactici de tip *doppelgänger*, utilizând logo-uri ale mass-media locale pentru a conferi autenticitate falsurilor și a le prezenta ca informații legitime. Analiza materialului relevă **greșeli tipice de compoziție** – menționarea unor instituții inexistente și lipsa datelor oficiale – care confirmă producerea sa de către actori străini fără cunoașterea cadrului instituțional al Republicii Moldova.

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

Mesajele promovate vizează **inducerea fricii și a dezbinării**, exploatând narative ruse despre renunțarea la neutralitate și cooperarea militară excesivă cu NATO, SUA și România. Scopul final este **subminarea încrederii în guvernare, erodarea sprijinului pentru partenerii strategici și destabilizarea societății moldovenești.**

Acest tip de operațiuni trebuie **să atragă atenția societății civile și mass-mediei**, pentru ca acestea să fie **parte a eforturilor statului de a rămâne vigilent**. Daunele de reputație generate de astfel de impersonalizări ar putea fi costisitoare nu doar pentru instituțiile statului, ci și pentru actorii non-guvernamentali.

2.3. Activarea rețelelor coordonate de conturi false și falși experți internaționali pentru diseminarea mesajului pro-Kremlin

Obiectivul: Prin activarea rețelelor de conturi false coordonate și a așa-zișilor influenceri internaționali, FR urmărește **discreditarea liderilor pro-europeni, subminarea încrederii publicului în instituțiile democratice și modelarea percepției colective în favoarea unor opțiuni politice convenabile Kremlinului**. Aceste acțiuni fac parte din campanii mai largi de creare a unui „context internațional" fabricat, menit să faciliteze preluarea și diseminarea mesajului de către actori locali din RM. Obiectivul este inducerea ideii că „informația vine din afară", prezentată ca o formă de „avertisment" din partea unor experți independenți, pentru a conferi legitimitate unor narațiuni false. Acest tip de operațiune are efecte asemănătoare unui atac de tip spam: mii de conturi preiau si publică simultan aceeași informație, cu intenția ca aceasta să fie preluată de canale media sau actori locali, care o vor traduce și disemina mai departe în limba română sau rusă. Astfel, se realizează un proces de „spălare informațională" (information laundering), prin care dezinformarea este acreditată ca autentică și credibilă în ochii publicului moldovean.

2.3.1. Operațiunea de influență și manipulare a opiniei publice prin dezinformare în RM, „Șor–Evrazia"

În baza investigațiilor jurnalistice realizate de ZDG[40], BBC[41] și NORD-NEWS[42] au fost atribuite mai multe conturi de Facebook/TikTok la operațiunea coordonată de Ilan Șor și alți actori, prin intermediul ONG-ului rusesc „Evrazia", cu scopul de a influența și manipula opinia publică din RM.

„Evrazia" a lansat în mai 2025 o nouă campanie malignă de influență, sub forma programului „Hackathon-ul Tehnologiilor Electorale", destinat persoanelor cu vârsta între 18–35 de ani. În cadrul acestuia, participanții au fost instruiți în tehnici de manipulare a opiniei publice, agitație politică și mobilizare a grupurilor.

Participanții „Hackathon-ului" au primit materiale de instruire ce conțineau narative anti-PAS și anti-Sandu, destinate a fi diseminate în spațiul informațional național pentru amplificarea nemulțumirilor publice și creșterea vizibilității partidelor pro-ruse.

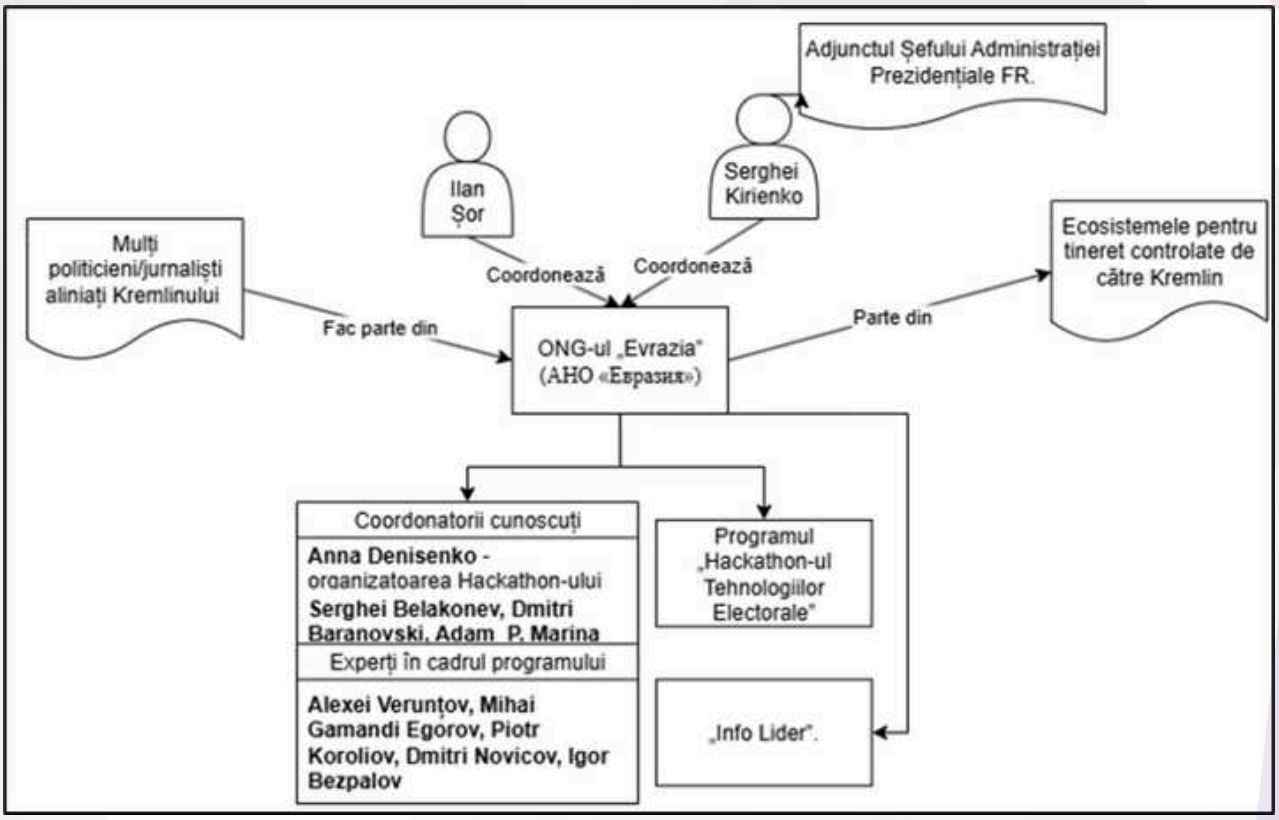
[40]https://www.zdg.md/investigatii/ancheta/video-armata-digitala-a-kremlinului-investigatie-sub-acoperire-se-plateste-hai-sa-va-spun-se-plateste-direct-de-la-moscova/
[41]https://www.bbc.com/news/articles/c4g5kl0n5d2o
[42]https://nordnews.md/investigatii/cinci-luni-sub-acoperire-reteaua-moscovei-actiuni-conspirative-bani-propaganda-si-manipulare-electorala/

Un alt program al „Evrazia”, intitulat „Info-Lider”, are ca obiectiv promovarea unei agende politico-informaționale anti-PAS și anti-Sandu în RM. Conform unuia dintre coordonatori, participanții au creat și distribuit materiale video dezinformatoare pe Facebook și TikTok, fiind remunerați prin intermediul băncii rusești PSB, cu sume de până la 5.000 lei lunar.

Diana Cearscaia desemnată responsabilă de dezvoltarea imaginii PP „Moldova Mare”, a fost de asemenea implicată în proiectul „Info-Lider”.

Alina Juc a organizat operațiuni de sondare manipulatoare sub egida organizației „Pentru Alegeri Cinstite”, declarând că rezultatele sondajelor urmau să fie utilizate pentru contestarea scrutinului parlamentar din 2025 (în cazul unor rezultate nefavorabile pentru partidele sprijinite direct sau indirect de „Evrazia”), încercând astfel să ofere o bază pseudo-factologică mesajelor privind ilegitimitatea viitorului Parlament.

Tot Alina Juc, în calitate de coordonatoare a rețelelor de agitatori de pe teritoriul Republicii Moldova, și-a adus echipa la sediul PP „Moldova Mare” pentru semnarea contractelor de voluntariat cu formațiunea politică.



Concluzii 2.3.1.

Investigațiile confirmă că, pe lângă postările standard, conturile vizate au fost utilizate pentru promovarea de conținut produs de alte Seturi de Manipulare Informațională (IMS Storm-1679[43]) asociate FR. Acestea au inclus materiale de tip graffiti fals, știri false de pe prima pagină și mesaje derivate din atacuri cibernetice, precum compromiterea serverului de e-mail al Parlamentului RM.

[43]https://www.sgdsn.gouv.fr/publications/guerre-en-ukraine-trois-annees-doperations-informationnelles-russes

Conform propriilor declarații, Alina Juc și-a început activitatea în cadrul ONG-ului „Evrazia” în urma unei întâlniri cu un angajat al FSB. Originară din Rîbnița, aceasta a organizat și coordonat activități de sondare manipulatoare prin grupul „Pentru Alegeri Cinstite”. Rezultatele sondajelor au fost preluate și distribuite prioritar de canale de Telegram afiliate publicației Komsomolskaia Pravda Moldova. Datele curente indică faptul că Juc ar fi recrutat și instruit cel puțin 34 de cetățeni.

Analiza relevă un tipar de creare și distribuire a imaginilor și materialelor video generate cu ajutorul inteligenței artificiale, diseminate într-un interval scurt de timp. Conținutul este însoțit de seturi identice de hashtag-uri furnizate de coordonatorii operațiunii. Tematicile dominante includ narative anti-PAS, anti-UE, anti-LGBT, precum și mesaje conspiraționiste privind implicarea Președintei Republicii Moldova în presupuse activități ilegale.

S-a constatat existența unor relații de cooperare între **PP „Moldova Mare”** (condus de Victoria Furtună) și Alina Juc, aceasta facilitând recrutarea unor persoane instruite în cadrul programelor „Evrazia” și semnarea contractelor de voluntariat la sediul partidului. Conform declarațiilor sale, **Blocul Electoral „Alternativa” și Blocul Electoral „Patriotic”** s-au arătat, de asemenea, interesate de rezultatele sondajelor manipulative realizate sub coordonarea sa.

2.3.2. Cazul Leroiz - falsul decret prezidențial

La începutul lunii iulie 2025, ecosistemul de influență pro-Kremlin a fost activat pentru a discredita instituția prezidențială a RM printr-o operațiune coordonată de dezinformare, care a implicat diseminarea unui fals decret prezidențial. Mesajul a fost lansat de Lucas Leroiz, un pretins jurnalist brazilian afiliat mișcării extremiste Nova Resistência, cunoscută pentru legăturile directe cu rețeaua ideologică a lui Aleksandr Dughin și cu Sputnik Brazilia, conform unui raport al Global Engagement Center al Departamentului de Stat al SUA[44].

Informația falsă a fost publicată inițial pe site-ul vtforeignpolicy[.]com[45], prezentat ca sursă internațională de analiză geopolitică, dar în realitate utilizat pentru a planta narațiuni favorabile Kremlinului. Articolul conținea imagini trucate și un decret fals redactat în limba română, care susținea că autoritățile moldovenești ar permite utilizarea forței împotriva cetățenilor. Acest conținut nu era menit să informeze publicul internațional, ci să fie preluat și redistribuit de actori locali din RM, în cadrul unei operațiuni de spălare informațională (information laundering), pentru a acredita ideea că „informația este confirmată de experți internaționali imparțiali”.

[44]https://2021-2025.state.gov/wp-content/uploads/2023/10/Nova-Resiste%CC%82ncia-in-Brazil_Oct_25_23_508.pdf
[45]Articolul arhivat cu privire la decretul prezidențial - https://archive.ph/vMUUl

După publicarea articolului, Leroiz a promovat materialul pe platforma X, urmat de alți actori din rețelele pro-ruse, precum contul SMO_VZ, specializat în distribuirea de conținut propagandistic.

Eforturile investite în diseminarea cazului arată importanța pentru actorii maligni anti-democratici și pro-ruși a popularizării acestei dezinformări: **au fost implicate 35 conturi de X (Twitter) cu un total de 4.4 milioane urmăritori, ce au generat 131 de postări și un număr de 649.000 interacțiuni** în spațiul online.

Această operațiune se încadrează într-o strategie mai amplă de delegitimare a autorităților pro-europene din RM, prin plantarea de informații fabricate și distribuirea lor prin rețele coordonate, aparent independente, pentru a genera neîncredere, polarizare și confuzie în rândul cetățenilor.

Intenția acestei tactici nu este de a informa publicul internațional și nici de a convinge cetățenii RM prin expunere directă. Scopul real este acreditarea artificială a unei informații false, prin plasarea ei în surse externe aparent independente, astfel încât aceasta să fie ulterior preluată de actori locali și prezentată ca validată „din afară". Prin această manevră, dezinformarea capătă un strat de legitimitate – devine mai greu de combătut și mai ușor de crezut de publicul intern, care este pus în fața unei „știri internaționale" deja vehiculate. În realitate, întreaga construcție este menită să simuleze consensul și urgența, declanșând reacții emoționale și erodând încrederea în instituțiile naționale și în special în Președintele RM.

Concluzii 2.3.2.

Operațiunea a urmat tiparul clasic de spălare informațională (**information laundering**): o narațiune falsă a fost lansată pe un site prezentat drept sursă internațională de analiză geopolitică, dar controlat indirect de ecosistemul pro-Kremlin, și ulterior amplificată pe platforme sociale prin conturi coordonate.

Prin folosirea de pseudo-jurnaliști și de materiale fabricate (imagini trucate, decret fals), s-a încercat crearea unei dovezi vizuale greu de contestat și erodarea credibilității instituției prezidențiale.

Cazuri de acest gen se caracterizează, totuși, printr-un nivel ridicat de neprofesionalism și se bazează pe lipsa obiceiului oamenilor de a verifica informațiile din surse credibile. Mesajele sunt adesea extrem de exagerate, ceea ce face ca ele să nu poată pătrunde în rândul cetățenilor cu un nivel dezvoltat de gândire critică. Acest lucru confirmă necesitatea consolidării eforturilor de educație media și a cooperării dintre stat, mass-media și societatea civilă pentru a reduce impactul unor astfel de tentative de manipulare.

2.3.3. Campanii coordonate prin conturi inautentice pe TikTok, Facebook și X (Twitter)

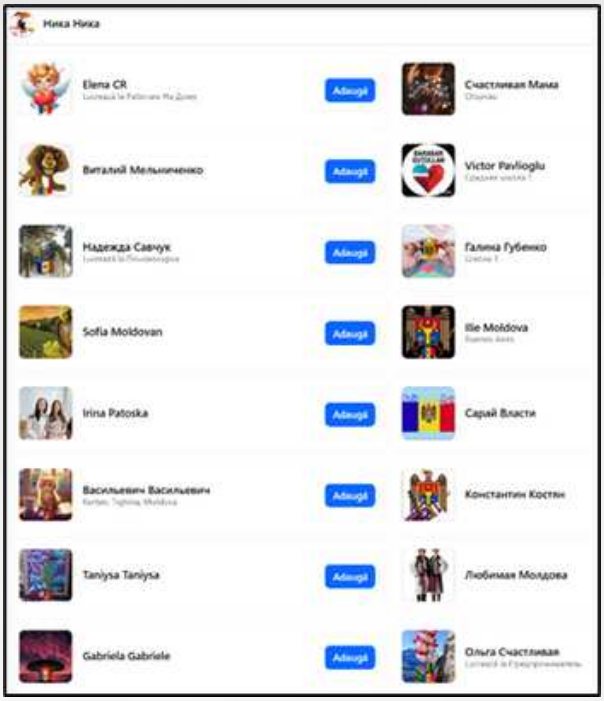
FR utilizează în mod recurent campanii coordonate prin conturi inautentice pe TikTok, Facebook și X pentru a influența opinia publică din RM, în special în perioade electorale sau în contexte geopolitice tensionate. Aceste operațiuni, susținute de rețele pro-Kremlin și amplificate de actori locali afiliați, vizează discreditarea liderilor pro-europeni, slăbirea încrederii în instituțiile democratice și promovarea narațiunilor anti-occidentale.

Scopul central este crearea impresiei că nemulțumirea față de direcția pro-europeană a țării este mult mai extinsă decât în realitate. Prin expunerea repetată la astfel de mesaje, utilizatorul obișnuit ajunge să le perceapă ca opinii larg răspândite, fără a-și pune problema autenticității sursei - mai ales când acestea sunt diseminate de conturi false, troli sau boți.

Obiectivul: Obiectivul specific al angrenării rețelelor de boți și al fermelor de troli în campanii de dezinformare este **maximizarea artificială a vizibilității și credibilității unor mesaje false sau distorsionate**, astfel încât acestea să fie percepute ca larg împărtășite și validate social.

Descriere: În perioada iunie – **septembrie 2025** au fost identificate 1.347 de conturi inautentice pe **TikTok**. În urma unei analize tehnice s-a determinat că numărul de urmăritori ajunge la **1.979.805**, care au generat un număr de **42.283.530 de interacțiuni în perioada analizată**.

O altă investigație făcută în perioada august – septembrie asupra a **27 de cazuri de manipulare informațională pe platforma X,** a identificat că **155 de conturi implicate constant în acțiuni coordonate au generat 3.435 de distribuiri care, la rândul lor, au generat 6.273.193 de interacțiuni**. Având în vedere că aceste materiale au fost diseminate și prin intermediul altor rețele sociale și pagini web ce sunt parte din rețelele de dezinformare ale Federației Ruse sau de către actori oportuniști cu un nivel de gândire critică insuficient, putem să concluzionăm că amprenta campaniei a fost mult mai mare decât ce s-a putut măsura.



Această strategie urmărește să creeze impresia unui consens popular sau internațional în jurul unor idei promovate de Kremlin (ex. neîncredere în autorități, opoziție față de UE/NATO, glorificarea „lumii ruse"), influențând opinia publică și comportamentul electoral.

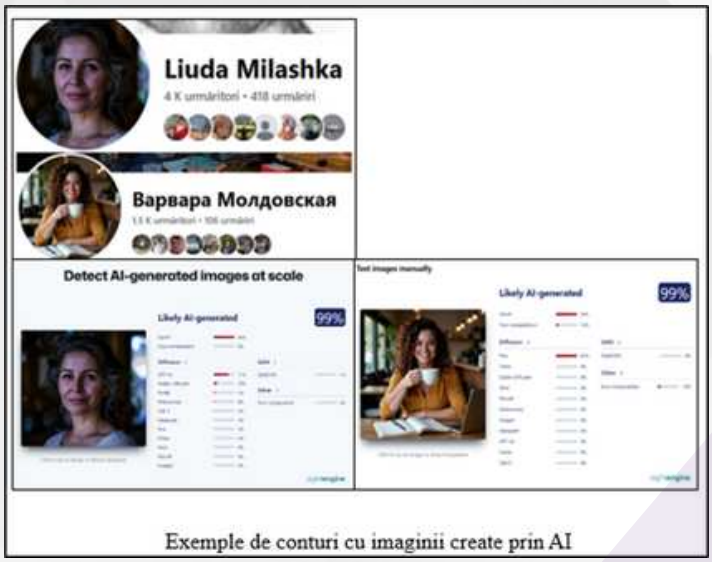
Rețelele de boți și troli acționează prin volum și sincronizare: diseminează rapid același mesaj pe platforme diverse, saturează spațiul informațional cu narațiuni-țintă și suprimă vocile critice, ceea ce determină eroziunea încrederii în sursele autentice de informare și creează o realitate paralelă favorabilă intereselor geopolitice ruse. Doar **pe parcursul unei luni**, în perioada iunie-iulie 2025 au fost identificate și documentate **226 conturi inautentice** implicate în campanii de amplificare a dezinformării pe platforma Facebook și TikTok prin folosirea mesajelor și hashtag-urilor alarmiste. Cele 2 campanii au folosit aceleași tactici, cum ar fi: crearea unei rețele de conturi inautentice, folosirea fragmentelor de text aproape identice, crearea materialului foto/video prin ajutorul inteligenței artificiale, folosirea narativelor deja existente și abuzarea problemelor ce au un caracter de polarizare a societății. Campaniile de influențare și manipulare informațională, susținute prin rețele de boți și ferme de troli, utilizează frecvent tehnici de tip dog whistle pentru a spori viralizarea mesajelor.

Această strategie presupune folosirea unui limbaj codificat, recognoscibil doar de anumite grupuri-țintă sau demografice (ex. pro-rușii, grupuri religioase conservatoare, populația dintr-o anume zona geografica etc.), astfel încât platformele sociale să le recomande cu prioritate către acei utilizatori. La rândul lor, aceștia recunosc mesajul ca fiind „al lor”, se simt validați și îl diseminează mai departe. În acest mod, narațiuni dezinformatoare pot circula rapid în comunități aparent închise, dobândind credibilitate și sprijin grassroots falsificat, fără a declanșa imediat măsurile automate de moderare ale platformelor.

Mai multe campanii de dezinformare desfășurate pe rețele sociale precum TikTok și Facebook promovează mesaje pro-Kremlin și anti-instituționale, folosind rețele de conturi inautentice. Aceste conturi sunt concepute pentru a crea impresia unui sprijin popular masiv și autentic, inclusiv prin folosirea unor hashtag-uri comune precum #GlasulPoporului (sau echivalentul său în rusă, #ГолосНарода), pentru a uni narațiunile într-o identitate aparent colectivă.

O altă campanie acuză guvernarea de implicare militară în Ucraina, sub pretextul cooperării bilaterale, și induce ideea că RM este împinsă într-un război străin pentru a servi interesele Bruxellesului. Mesaje precum „Nu vrem să murim” și „Opriți dictatura” sunt amplificate prin hashtag-uri precum #NuVremSăMurim #PASneTrădează #НетВойне #VremSăTrăim.

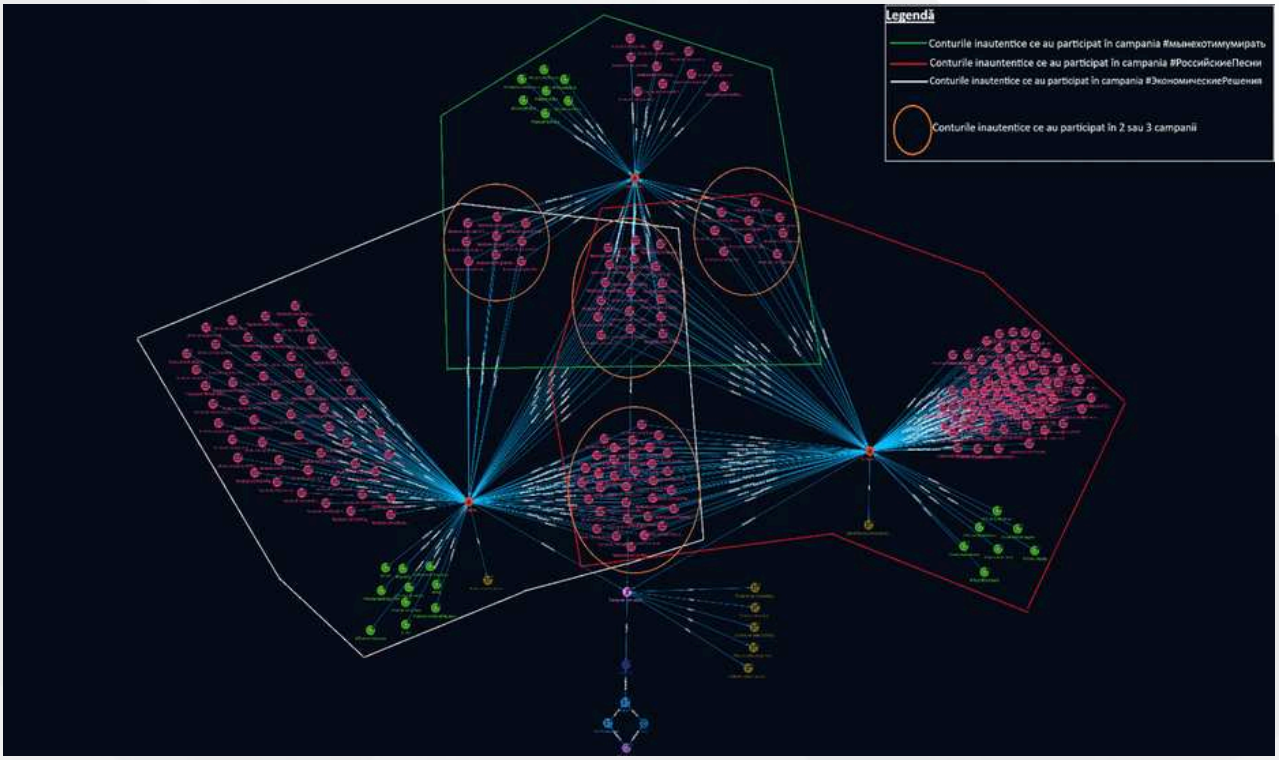
O a treia campanie cultivă panică economică, promovând ideea unei crize alimentare provocate de orientarea pro-europeană a guvernării și pierderea legăturilor economice cu FR. Se sugerează că RM era mai stabilă economic când beneficia de gaze rusești și echilibru geopolitic. Hashtag-urile includ #Criză #SoluțiiEconomice #IntegrareEuropeană #Евроинтеграция. Analiza tehnică a conturilor implicate arată că acestea sunt în majoritate false, cu date de profil fabricate, imagini de profil generate cu AI sau preluate de pe platforme de tip stock-photo. Conturile sunt adesea conectate între ele în rețele de „prieteni” și își păstrează identitatea vizuală pe mai multe platforme, sugerând un nivel ridicat de coordonare. Formatele de ID-uri similare (ex. alena.vvv.2025, elena.441368) indică automatizare sau generare în loturi. Aceste tactici vizează multiplicarea artificială a mesajelor și crearea impresiei unui consens social larg împotriva actualei guvernări.



Exemple de conturi cu imaginii create prin AI

Concluzii 2.3.3.

Algoritmii platformelor sunt în permanență evitați de către sursele maligne, care explorează continuu posibilele vulnerabilități pentru a-și dezvolta seturi de manipulare informațională, cu scopul de a afecta autenticitatea dezbaterilor publice din societate. Platformele trebuie să înțeleagă că eforturile solicitate din partea statului în susținerea spațiilor informaționale sunt esențiale pentru menținerea dezbaterilor publice într-un format autentic și pentru a preveni transformarea acestora în vectori ai intereselor străine, direcționate manipulator, ce duc la destabilizarea consensului național.



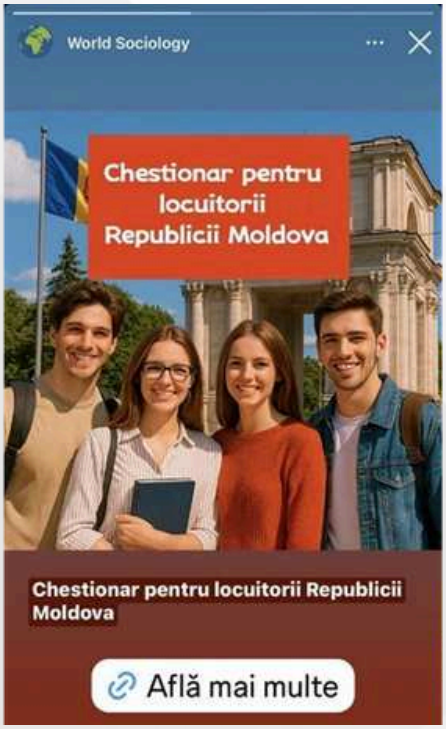
Conturile inautentice (Facebook și TikTok) au fost examinate și mapate în mod grafic fiind stabilită apartenența la fiecare din cele 2 campanii menționate.

2.4. Tactici de profilare electorală mascată utilizate de FR în RM înaintea alegerilor parlamentare

Profilarea electorală mascată este o practică de influență malignă și neautorizată[46] prin care un actor străin colectează, sub un pretext înșelător (de exemplu, sondaje de opinie), date psihologice, demografice și comportamentale despre alegători. Scopul este identificarea vulnerabilităților individuale – frici, frustrări, nemulțumiri – care pot fi ulterior exploatate prin mesaje de dezinformare personalizate. În loc să transmită un mesaj general, campaniile construiesc micro-narațiuni specifice fiecărui segment social sau psihologic, crescând astfel eficiența manipulării. În alegerile prezidențiale din SUA din 2016, se estimează că până la 126 de milioane de americani au fost expuși la conținutul generat de entități legate de FR, iar cercetări ulterioare sugerează că între **6 și 10 milioane de voturi ar fi putut fi influențate**. Această tehnică permite influențatorului să acționeze invizibil, dar cu precizie chirurgicală, pentru a fragmenta societatea și a deturna rezultatele alegerilor.

[46]Conform art. 4, din Regulamentul privind organizarea și desfășurarea sondajelor de opinie și a exit-pollurilor în perioada electorală (HCEC nr.1138 din 28 iulie 2023), orice sondaj urmează „a fi autorizat de către Comisia Electorală Centrală și poate fi realizat de către competitorii electorali, persoane juridice din RM cât și cetățenii Republicii Moldova.”

Cu peste **1,4 milioane de conturi active de Facebook și Instagram**[47] în rândul celor peste 18 ani într-o țară cu aproximativ **2,7 milioane de alegători în interiorul granițelor și diferența de pana la 3,02 milioane cu domiciliul în diaspora sau în regiunea transnistreană**, probabilitatea ca o **majoritate statistică a electoratului activ online să fie expusă la profilare electorală mascată este extrem de ridicată**. Această formă invizibilă de manipulare, derulată de actori afiliați intereselor FR, periclitează grav integritatea procesului democratic, subminează încrederea publică în alegeri și favorizează artificial ascensiunea politicienilor pro-ruși. Profilarea electorală mascată nu este doar o problemă tehnologică, ci un atac direct la suveranitatea statului.

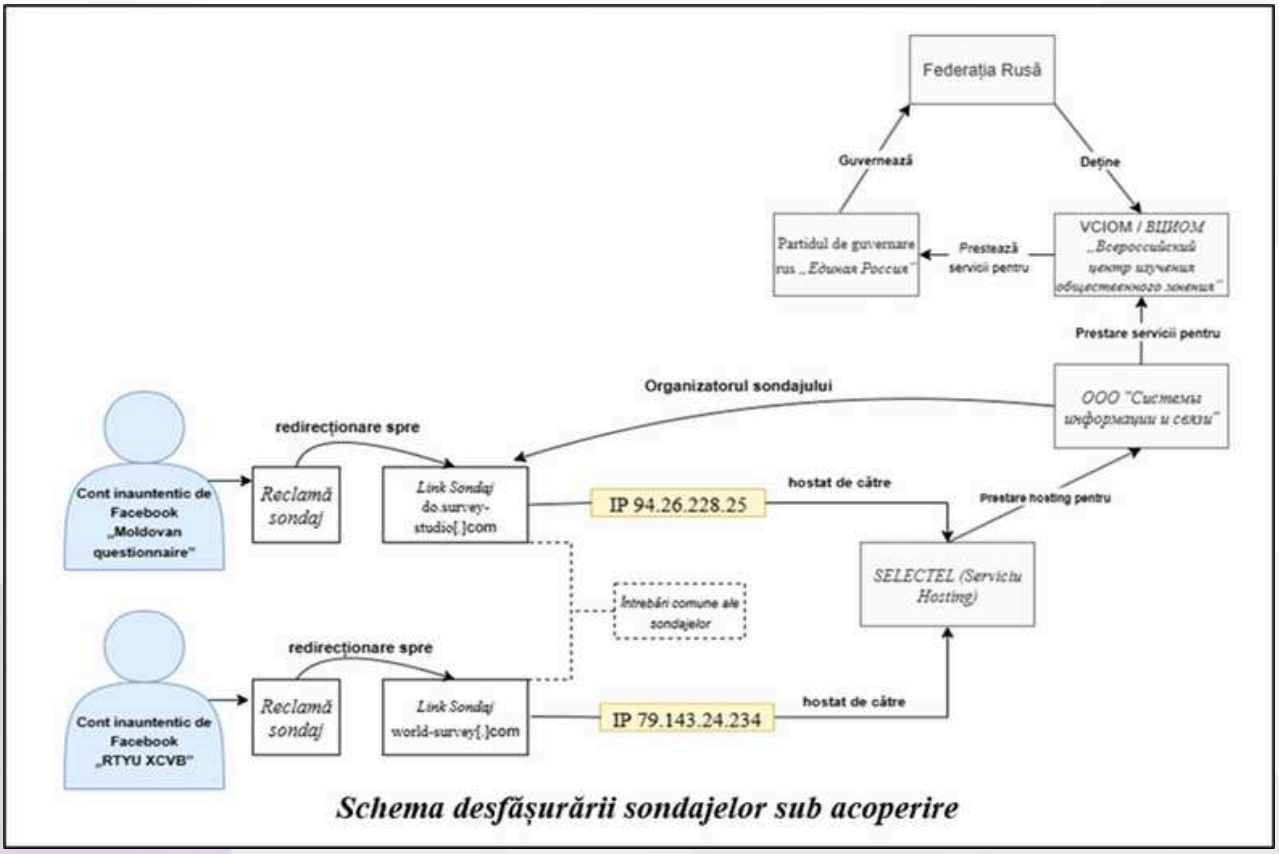


În contextul alegerilor parlamentare programate pentru 28 septembrie, CCSCD a documentat metode sofisticate de influență informațională utilizate de actori afiliați FR. Printre acestea se numără simularea unor sondaje de opinie cu scopul real de a colecta date pentru profilarea alegătorilor și personalizarea ulterioară a mesajelor de dezinformare. Aceste practici au ca obiectiv final manipularea intenției de vot în favoarea partidelor pro-ruse sau descurajarea participării electorale.

În perioada iunie-iulie 2025, mai multe pagini de Facebook și Instagram conectate - așa cum vom arăta - cu entitățile din FR, au desfășurat non-transparent sondaje socio-politice ce au vizat cetățenii din RM. Conturile prin care se făcea sondarea pretindeau că sunt pagini de turism din RM sau pagini de servicii de frumusețe din Ucraina (**ex: paginile Moldovan questionnaire**[48], **RTYU XCVB**[49], **Camryn, The Social Circle, World Sociology, TYUI CVBN, Marketing Pro, AtlasIntel**). Unele din paginile folosite în operațiunea identificată de CCSCD prezintă atribute certe ale instrumentelor MIIS din spațiul virtual: istoric inexistent sau foarte recent, lipsă de interacțiuni reale (engagement organic minim), schimbări bruște de tematică (ex. de la turism la sondaje politice) activitate limitată exclusiv la reclame targetate, paginile sunt

[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

paginile sunt adesea administrate din locații externe sau disimulate.



Schema desfășurării sondajelor sub acoperire

Obiectivul: Colectarea datelor cu privire la deținerea cetățeniei, raionul în care trăiește cetățeanul, grupul teritorial, genul, vârsta, gradul de satisfacție cu privire la situația din RM, opinia populației cu privire la direcția în care merg lucrurile în țară, gradul de interes față de politică, gradul de satisfacție cu privire la activitatea președintelui actual, gradul de încredere în președintele actual, intenția de participare la alegerile din RM, pentru ce partid ar vota dacă alegerile ar fi săptămâna aceasta, nivelul de studii și situația materială.

Descriere: Pagina "**Moldovan questionnaire**" a fost creat la data de 08.06.2025 și pe 10-12 iunie a lansat 11 reclame sponsorizate, probatoriul tehnic al cazului). În urma accesării utilizatorul este redirecționat către „do.survey-studio[.]com", un portal înregistrat în FR care prezinta atribute unui instrument MIIS (în 19 ani de funcționare au fost operate modificări pe site de pe 22 de IP-uri unice - ceea ce indica o încercare de a ascunde **identitatea deținătorului real** sau de a disimula intențiile reale ale site-ului).

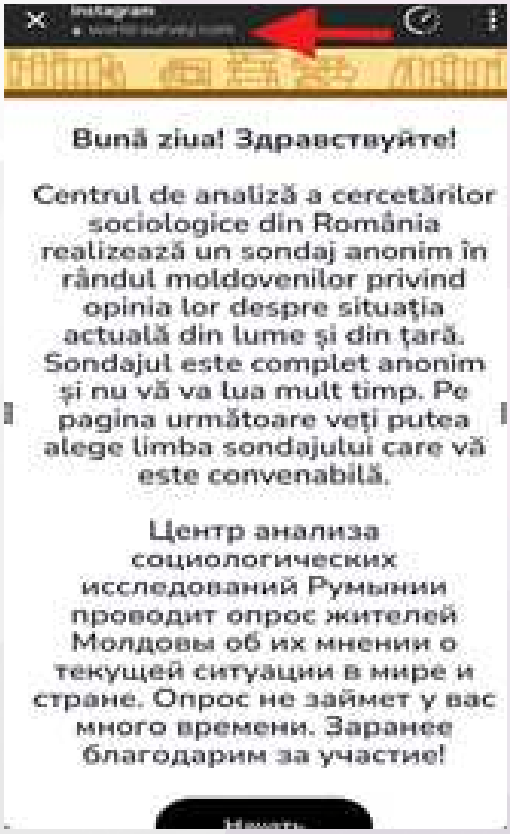
Analiza tehnică a acestui site arată ca el este găzduit pe adresa de IP „94.26.228.25" (localizată în St. Petersburg de către „SELECTEL", entitate comercială din FR). Găzduirea a fost făcută la cererea companiei OOO "Системы информации и связи".

Printre clienții serviciilor OOO "Системы информации и связи[50]" este enumerat și VCIOM („Всероссийский центр изучения общественного мнения" – ВЦИОМ) ce reprezintă o instituție sociologică deținută de către statul rus. Alți parteneri ale OOO "Системы информации и связи" includ alte companii private ce cooperează cu instituțiile de stat ale FR.

[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]Clienții OOO "Системы информации и связи" - https://archive.ph/SooaE

VCIOM, l-a rândul său cooperează cu partidul de guvernare rus „Единая Россия” și entități media asociate guvernării ruse[51].

Pagina „**RTYU XCVB**” a fost creată pe 01.03.25 și pe 25.06.2025 și a lansat 5 reclame sponsorizate. În urma accesării utilizatorul este redirecționat către „world-survey[.]com”. O altă încercare de a crea impresia unui sondaj internațional neafiliat cu FR. Analiza tehnică a acestui site demonstrează însă faptul că site-ul este găzduit pe adresa de IP „79.143.24.234” de compania „SELECTEL” (ca în “**Moldovan questionnaire**”), cu sediul și infrastructura localizate în FR, cunoscută pentru furnizarea de servicii de găzduire entităților comerciale și instituționale din FR.



Notă suplimentară: SELECTEL găzduiește și alte site-uri cu arhitectură web identică, adaptate pentru publicul din alte regiuni (ex: armenianaopinion.com pentru Armenia), ceea ce sugerează o campanie regională coordonată de sondaje sincronizate. Infrastructura tehnică relevă utilizarea unui server comun pentru mai multe astfel de site-uri, indicând existența unui administrator unic sau a unei rețele centralizate.

Concluzii 2.4.

Manipularea rezultatelor sondajului: Rezultatele sondajelor vor fi cel mai probabil invocate, în cazul neatingerii obiectivelor scontate, drept material probatoriu pentru a declara alegerile ca fiind fraudate și pentru a submina încrederea cetățenilor în procesele democratice din Republica Moldova, în pofida faptului că aceste sondaje au fost realizate de către entități autorizate de autorități.

Risc direct pentru alegerile din 2025: Campania amenință integritatea procesului democratic prin influențare externă, mobilizare controlată și deturnarea narațiunilor electorale în favoarea intereselor Rusiei.

Operațiune de influență hibridă mascată: Așa-zisele sondaje reprezintă o campanie hibridă de influență orchestrată de FR, camuflată sub forma unei cercetări sociologice. Scopul real este colectarea de date politice și psihografice, în special de la tineri, pentru a influența comportamente electorale și a submina sprijinul pentru liderii pro-europeni.

Ascunderea deliberată a originii: Paginile false din rețelele sociale – care oferă conținut aparent neutru (ex. turism), sau sondaje realizate aparent de entități din România – sunt instrumente de dezinformare utilizate pentru a disimula implicarea FR. Infrastructura digitală (inclusiv găzduirea pe servere precum Selectel) indică o posibilă legătură directă cu instituții precum VCIOM sau partidul „Единая Россия”.

[51]Partenerii VCIOM („Всероссийский центр изучения общественного мнения” – ВЦИОМ) - https://archive.ph/9sZPo

Targetare sofisticată și manipulare electorală: Datele colectate permit segmentarea populației pe criterii demografice, geografice și comportamentale, ceea ce facilitează campanii de influență personalizate. Aceste tactici pot fi utilizate pentru: demobilizarea tinerilor pro-europeni; Promovarea candidaților pro-ruși sau pseudo-europeni; Manipularea algoritmică a informației pe platforme digitale.

2.5. Manipularea și interferența informațională internă

2.5.1. Analiza redacției on-line Moldanalytics și rețelei sale de pagini social-media

Obiectiv: Obiectivul principal al acestui tip de TTP este slăbirea încrederii publicului în instituțiile democratice și în societatea civilă din Republica Moldova. Prin crearea și întreținerea unor platforme aparent „analitice" și independente, cum este Moldanalytics, se urmărește construirea unei alternative informaționale care pare legitimă, dar care, în realitate, promovează narative ostile și manipulative.

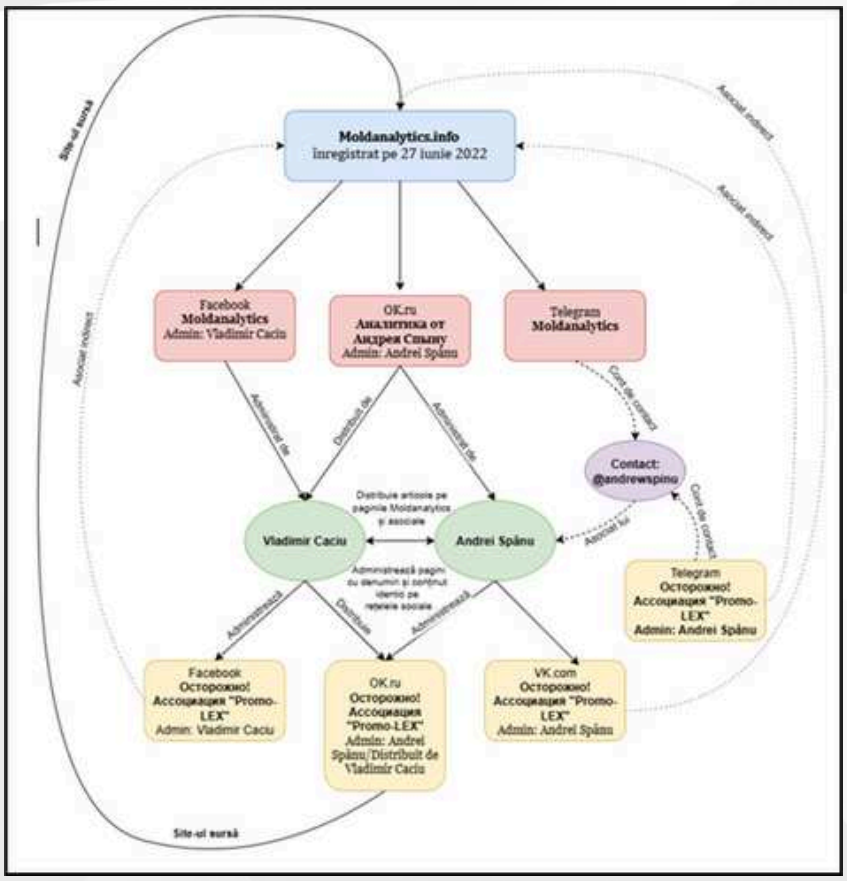
Un prim scop este decredibilizarea organizațiilor societății civile, în special a celor active în zona transnistreană, precum Promo-LEX și Zona de Securitate. Acestea sunt prezentate ca actori părtinitori sau ca instrumente ale guvernării, ceea ce subminează în mod direct rolul lor de monitorizare și apărare a drepturilor omului.

Un alt obiectiv este amplificarea coordonată a propagandei, printr-o rețea de canale pe Facebook, Telegram, OK.ru și VK.com, administrate de aceiași actori. Multiplicarea conținutului pe platforme diferite creează impresia că mesajele sunt validate de mai multe surse independente, deși ele provin din același nucleu.

De asemenea, aceste canale sunt concepute să transmită ideea unei „voci colective" împotriva guvernării, prin pretinsa implicare a „foștilor membri" ai ONG-urilor vizate. Această tehnică induce percepția că organizațiile respective și-ar fi pierdut credibilitatea chiar în interiorul lor, ceea ce erodează suplimentar încrederea publicului în ele. În final, obiectivul este polarizarea opiniei publice și alimentarea sentimentului de neîncredere în stat și partenerii săi occidentali. Prin atacuri constante și prin diseminarea unor narațiuni manipulative, publicul este împins să perceapă Republica Moldova drept un stat slab, dependent și lipsit de legitimitate democratică, mai receptiv la mesajele și soluțiile promovate de Rusia. Un exemplu recent este așa-numita platformă Moldanalytics[.]info, înregistrată în iunie 2022 și prezentată ca spațiu de analiză a evenimentelor din Republica Moldova.

În realitate, site-ul și rețelele asociate pe Facebook, Telegram, OK.ru și VK.com publică conținut ostil instituțiilor și organizațiilor societății civile, cu accent pe regiunea transnistreană. De asemenea, au fost create pagini care pretind a fi administrate de „foști membri" ai ONG-urilor vizate. În realitate, ele reproduc aproape exclusiv materiale din aceleași surse propagandistice, cu scopul de a submina credibilitatea acestor organizații.

Conținutul publicat urmărește în mod special discreditarea ONG-urilor active în zona transnistreană, în primul rând Promo-LEX și Zona de Securitate. Astfel, rețeaua Moldanalytics consolidează o campanie de denigrare coordonată împotriva societății civile, contribuind la polarizarea opiniei publice și la subminarea încrederii în organizațiile independente.



Concluzii 2.5.1.

Moldanalytics și rețelele sale asociate (Facebook, Telegram, OK.ru, VK.ru) constituie o infrastructură mediatică coordonată de dezinformare, care îmbină branding fals de „entitate analitică independentă", rețele de distribuție multiplă pentru imitarea pluralismului informațional și atacuri directe asupra ONG-urilor și instituțiilor.

Prin acest mecanism, se consolidează o campanie de denigrare a societății civile și se alimentează neîncrederea în procesele democratice din Republica Moldova.

2.5.2. Canale de social media care mimează "vocea poporului. "Activitatea subversivă a rețelei Gagauznews

Obiectivul: Obiectivul acestei tehnici este de a submina încrederea în instituțiile Republicii Moldova și în parcursul său european printr-o rețea internă de canale și site-uri care se prezintă fals drept „vocea cetățenilor". Prin diseminarea de falsuri, deepfake-uri și articole denigratoare, rețeaua exploatează teme sensibile precum atragerea țării în război, persecuția Găgăuziei și distrugerea valorilor tradiționale. Scopul final este de a crea iluzia unui sprijin autentic din partea societății pentru narațiunile pro-ruse, alimentând frica, diviziunea și opoziția față de integrarea europeană.

Descriere: Analiza rețelei Gagauznews a fost generata de modul agresiv de diseminare, prin intermediul canalului de Telegram, a falsurilor și a deepfake-urilor. Un exemplu este cazul declarațiilor false atribuite Președintelui CEC.

Pe 27 mai 2025, canalul Gagauznews a publicat un deepfake[52] prin care se promova ideea că finanțarea străină a unui partid din partea Franței nu este considerată ingerință. Mesajul a fost prezentat distorsionat ca o ingerință externă a Franței, în contextul apropierii Republicii Moldova de integrarea în UE.

Pe 30 iulie 2025, această informație a fost preluată la nivel internațional de site-ul see.news[53], iar ulterior rețeaua Pravda[54] a amplificat subiectul, menționând că surse primare site-urile en.topwar.ru și de.topwar.ru. În paralel, pe platforma X, știrea a apărut inițial la contul LordBebo[55], fiind redistribuită de circa 1600 de conturi, majoritatea cel mai probabil inautentice. Repostările au avut un caracter coordonat, realizându-se la intervale medii de 45 de secunde, dar nu au generat interacțiuni semnificative.

TEXT REAL

- De ce s a renunțat la certificatul de integritate?
- A fost modificată legea și ANI deja nu mai eliberează aceste certificate, dar ne conducem de acea listă de restricții. Cu alte cuvinte, dacă persoana are întocmit un act de constatare a unor interdicții sau a admis, de exemplu anumite încălcări care sunt incompatibile cu funcția publică și actul de actul care a fost constatat de către ANI devine irevocabil, fie este contestat în instanță și după hotărârea instanței definitive și irevocabile, actul rămâne în picioare. Iată atunci persoana este inclusă în acel registru de interdicții. Și noi am avut situație la Comisia Electorală Centrală când aceste litigii au durat ani de zile. Deci, ANIU a pornit o procedură prin care s a constatat faptul că persoana a admis un conflict de interese sau nu a respectat legea cu privire...

[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=BbIiVIsvpXI

TEXT FALS[57]

- Voi explica. Există o mare diferență între Uniunea Europeană și alte state. Moldova este deja la un pas de a deveni membră a Uniunii Europene. De aceea, intervenția unei țări ca Franța în alegerile noastre nu este considerată

o ingerință externă. Chiar și atunci când este vorba de finanțare directă a unor forțe politice, nu o considerăm o formă de corupție electorală. Este normal ca vecinii să aibă grijă unii de alții și să sprijine dezvoltarea democrației.

Canalul de Telegram Gagauznews este asociat cu site-ul Gagauznews.com[58], ambele promovând activități de manipulare informațională. Site-ul publică articole cu caracter denigrator, precum cel din 6 septembrie care o prezenta pe Președinta Republicii Moldova ca având tulburări mintale[59]. Astfel de materiale au fost utilizate și în 2024 de către rețele maligne, în preajma alegerilor prezidențiale. Existența paginii web oferă o aparență de legitimitate rețelei de canale afiliate, active pe platforme precum Facebook, TikTok, Instagram, YouTube, VK și Telegram.

Conținutul publicat de Gagauznews se concentrează pe trei mari narative:

1. „Moldova este atrasă în război” – acuză autoritățile de la Chișinău că implică țara în conflictul din Ucraina și încalcă neutralitatea, folosind declarații scoase din context.
2. „Persecuția Găgăuziei” – prezintă autoritățile centrale ca opresive și ostile, alimentând ideea de victimizare și solicitând intervenția Rusiei și Turciei.
3. „Uniunea Europeană distruge valorile tradiționale” – susține că integrarea europeană ar impune educație LGBT și alte politici contrare culturii și religiei locale, promovând o retorică conspiraționistă.

Pagina web Gagauznews este administrată de A.O. „Centrul Comunitar Anticriză”, anterior controlată de Victor Petrov[60], politician găgăuz apropiat de Ilan Șor și Evghenia Guțul. ONG-ul deține și site-ul nash[.]md. În prezent, asociația este administrată de Ivan Uzun[61], fondator și administrator în mai multe entități juridice. Fostul conducător, Victor Petrov, figurează din 22.02.2024 pe lista de sancțiuni a Uniunii Europene pentru acțiuni de destabilizare și diseminare de informații false[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/c267d0eff92074dab0823d3708c96f0f6cf33f0a859b5405b466dba1ccf8d7a3
[62]https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=OJ:L_202400739

Cel mai probabil, schimbarea administratorului către Ivan Uzun a fost decisă pentru a evita periclitarea activității ONG-ului după aplicarea sancțiunilor. O altă asociere relevantă este cu cetățeanul Dan Dudca (Дан Дудка), autor principal al site-ului eurasianews[.]md. Acesta scrie articole în limba rusă, iar multe dintre postările sale publicate pe pagina de Facebook Я люблю Балканы[63] sunt preluate de Gagauznews, unele fiind republicate fără menționarea sa ca autor. Există o probabilitate ridicată ca Dan Dudca să fie redactor atât pentru eurasianews[.]md, cât și pentru rețeaua Gagauznews, mai ales că site-ul eurasianews[.]md republică conținut de pe Gagauznews[.]com.

În plus, eurasianews[.]md publică știri preluate de pe npm[.]md, site-ul Consiliului Public al Moldovei, și de pe istgeo[.]md, pagina Asociației Istorico-Geografice din Moldova. Ambele organizații promovează interese pro-ruse, în special Consiliul Public al Moldovei, care pretinde că reprezintă întreaga societate prin reunirea a 28 de organizații cu valori pro-ruse. Dan Dudca scrie și pentru alte platforme precum bloknot-moldova[.]ru, md.kp[.]media, dnestr[.]tv și almanah[.]md. Acesta deține trei conturi de Facebook: Я люблю Балканы (unde publică articole redistribuite ulterior), un cont personal Dan Dudca folosit pentru promovarea materialelor, și un al treilea cont tot cu numele Dan Dudca, utilizat pentru redistribuiri.

Activitatea Gagauznews a fost monitorizată și de autorități. La 26 februarie 2022, Serviciul de Informații și Securitate a blocat site-ul gagauznews.md pentru incitare la ură și justificarea agresiunii ruse împotriva Ucrainei. Cu toate acestea, activitatea a continuat sub domeniul gagauznews.com. Canalul de Telegram a devenit principalul vector de distribuție, publicând în medie 92 de postări zilnice și având aproximativ 13.000 de abonați.

Analiza rețelei de distribuție arată că Gagauznews preia și redistribuie masiv conținut de la surse ruse, precum Sputnik Moldova și bloknot-moldova, dar și de la surse pro-ruse precum Gagauzia24, Канал 5, Виктор Петров, Правда Гагаузии, Молдавский Пистон și 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/

La rândul său, canalul este redistribuit intens de rețele afiliate grupului „Șor” și de structurile de propagandă ale Federației Ruse. În medie, o postare ajunge la 800–1000 de abonați, 35–40% dintre vizualizări fiind înregistrate în prima oră, cu o scădere treptată în următoarele ore.

De-a lungul timpului, conform datelor din 12.08.2025, Gagauznews a republicat masiv conținut de pe canale de Telegram precum: @Sputnik Молдова (1315 ori), @Gagauzia24 I Раньше всех в Гагаузии! (1116 ori), @Александр Суходольский – официальный телеграм канал (1003 ori), @Виктор Петров — страница народной поддержки (897 ori) și @Канал5 (843 ori). În același timp, canale precum @Правда Гагаузии (5809 ori), @Молдавский пистон (1164 ori), @Блокнот Молдова (839 ori), @Молдавская политика (521 ori) și @Евразийская Молдова (507 ori) au redistribuit cel mai frecvent conținut de pe @gagauznews.

Concluzii 2.5.2.

Gagauznews reprezintă un hub pro-rus și anti-european de manipulare informațională, care produce și distribuie constant falsuri, deepfake-uri și articole denigratoare, centrate pe narative sensibile precum atragerea Republicii Moldova în războiul din Ucraina, persecuția Găgăuziei și distrugerea valorilor tradiționale de către Uniunea Europeană. Distribuția se bazează pe o infrastructură extinsă și coordonată, cu vector principal canalul de Telegram @gagauznews, amplificat de rețele de site-uri, canale și conturi inautentice pe platforma X, precum și de surse media externe. Acest mecanism urmărește exploatarea fricilor și diviziunilor sociale pentru a submina încrederea în instituțiile statului și în parcursul european al Republicii Moldova.

2.6. Manipularea și interferența informațională internă

2.6.1. Analiza redacției on-line Moldanalytics și rețelei sale de pagini social-media

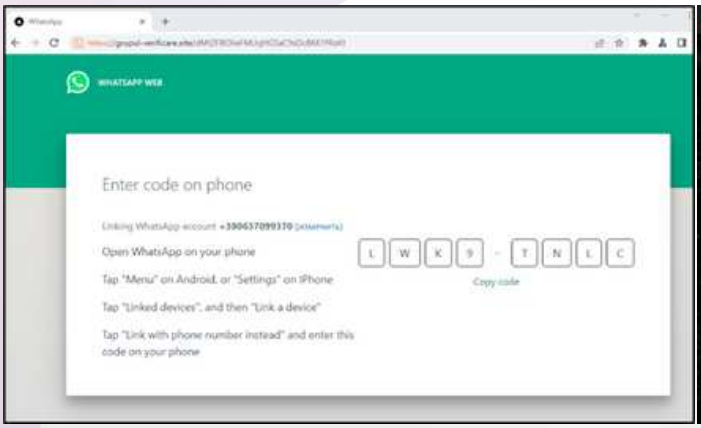
Obiectivul: Obiectivul principal al acestei operațiuni este **compromiterea securității comunicațiilor oficiale** și obținerea accesului la informații sensibile din cadrul instituțiilor de stat. Prin deturnarea sesiunilor de WhatsApp, atacatorii pot accesa conversații interne, liste de contacte și alte date confidențiale care pot fi ulterior exploatate.

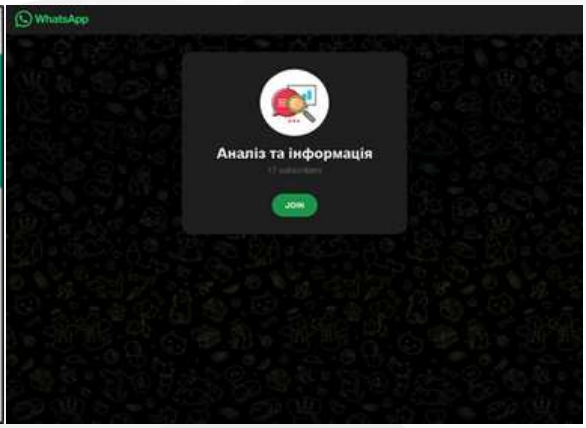
Un al doilea obiectiv constă în **impersonalizarea victimelor și răspândirea de conținut fraudulos.** Prin folosirea conturilor compromise, actorii pot transmite mesaje false către alți angajați sau către public, afectând credibilitatea instituțiilor vizate și facilitând campanii de dezinformare.

Nu în ultimul rând, asemenea acțiuni urmăresc să genereze destabilizare și pierderea încrederii în instrumentele de comunicare utilizate de autorități. Prin exploatarea vulnerabilităților și prin diseminarea unor mesaje aparent legitime, adversarii încearcă să submineze reziliența instituțională și să creeze un climat de insecuritate informațională.

Descriere: La data de 20 august, mai mulți angajați ai instituțiilor de stat au recepționat prin aplicația **Signal** un mesaj care îi invita să se alăture unui grup de lucru pentru partajarea de informații. Mesajul părea autentic deoarece a fost realizat prin impersonalizarea unui alt angajat, cel mai probabil în urma clonării dispozitivului acestuia.

În conținutul mesajului era inserat linkul **grupul-verificare[.]site**, care redirecționa utilizatorii către o pagină ce imita interfața oficială a WhatsApp și afișa un așa-zis cod de conectare. Analiza a demonstrat că acesta reprezenta o tentativă de **phishing și session hijacking (furt de sesiune).**





Victimei i se cerea să acceseze meniul aplicației WhatsApp de pe dispozitiv și să introducă codul furnizat. În realitate, această acțiune autoriza terminalul atacatorului ca dispozitiv valid, oferindu-i acces complet la mesajele, contactele și sesiunile utilizatorului, cu posibilitatea de a folosi contul compromis pentru transmiterea de mesaje frauduloase sau colectarea de informații sensibile.

Investigațiile asupra domeniului **grupul-verificare[.]site** au arătat că acesta face parte dintr-o rețea de site-uri create recent, în perioada 23 iulie – 19 august 2025. Pe aceeași adresă IP (79.137.198.153) au fost identificate domeniile: **mychildren404[.]online, group-verification[.]online, testyar.dorsa.of[.]to și myduaccount-quickpaymentae[.]sbs**, toate cu profil suspect și asociate unor activități similare.

De asemenea, domeniul grupul-verificare[.]site prezintă interes suplimentar deoarece aplică aceeași tehnică de impersonalizare, dar vizează cel mai probabil Ucraina, printr-o redirecționare către un grup denumit „Аналіз та інформація”, care pretinde a fi un canal legitim de WhatsApp.

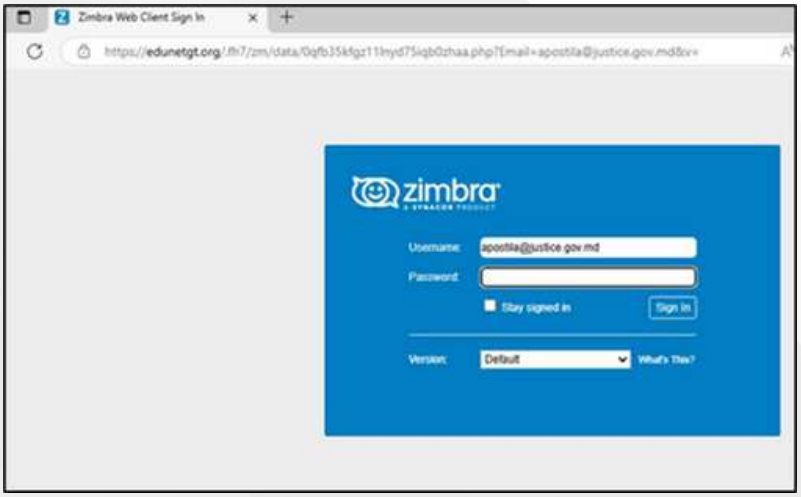
Concluzii 2.6.1.

Atacatorii folosesc site-uri recent create, cu interfețe care imită funcționalități legitime ale aplicației WhatsApp, pentru a induce utilizatorii să ofere acces direct la propriile sesiuni. Această metodă permite preluarea completă a conturilor, cu riscuri semnificative privind furtul de date personale, accesul la contacte și potențiala utilizare a conturilor compromise pentru scalarea distribuirii de mesaje frauduloase.

Totodată, rețeaua de domenii asociate, creată într-un interval scurt și legată prin aceeași adresă IP, demonstrează intenția adversarilor de a asigura **extinderea și replicarea atacurilor** în alte ținte. În acest caz, au fost identificate și direcționări spre Ucraina, ceea ce confirmă caracterul transfrontalier al operațiunii.

2.6.2. Atac de phishing la adresa Ministerul Justiției

Obiectiv: Obiectivul acestui TTP este **furtul de date de autentificare și compromiterea accesului la conturile oficiale** ale utilizatorilor vizați, în special din cadrul instituțiilor statului. Prin imitarea interfeței Zimbra și transmiterea unor mesaje care sugerează resetarea parolei sau suspendarea contului, atacatorii urmăresc să exploateze încrederea utilizatorilor și să îi determine să furnizeze credențiale sensibile. În paralel, prin redirecționarea către adrese de email precompletate, aceștia creează un canal de comunicare direct, menit să faciliteze **escaladarea atacului, compromiterea infrastructurii IT și obținerea accesului la informații interne. În esență, scopul este de a infiltra rețele instituționale și de a asigura persistența prin acces fraudulos la conturi legitime.**



Descriere: La data de 21 august, Ministerul Justiției al Republicii Moldova a raportat o campanie de tip **SPAM/Phishing** . Conținutul emailului analizat sugerează utilizatorilor să își schimbe parola înainte de data expirării și conținea un link de phishing ce imita interfața web Zimbra cu scopul de a colecta datele de autentificare ale utilizatorilor.Analiza fișierului .eml a permis identificarea adresei IP a expeditorului inițial – **34.106.108.59**, asociată cu **Google Cloud Services**. Aceasta avea deschis portul 3389/RDP, folosit ca intermediar pentru ascunderea adresei reale a atacatorului. Mesajul a fost redirecționat prin serverul de email **mail.sysnetglobal.com**, utilizând adresele IP 172.105.33.223 (server public email) și 172.237.32.253 (relay final).

În urma investigațiilor asupra domeniului **sysnetglobal.co.in**, de la care a fost recepționat emailul, s-a constatat un potențial compromis al adresei de email **ashok.mishra1@sysnetglobal.co.in**. În plus, au fost identificate și alte linkuri conexe implicate în această campanie de phishing. Acestea avertizau utilizatorii despre o presupusă suspendare a contului și, la accesare, deschideau aplicația Microsoft Mail cu adrese de email ale destinatarilor deja precompletate – **webmaster@sopphotography.co.ke și webmaster@meetingplacesession.com.**

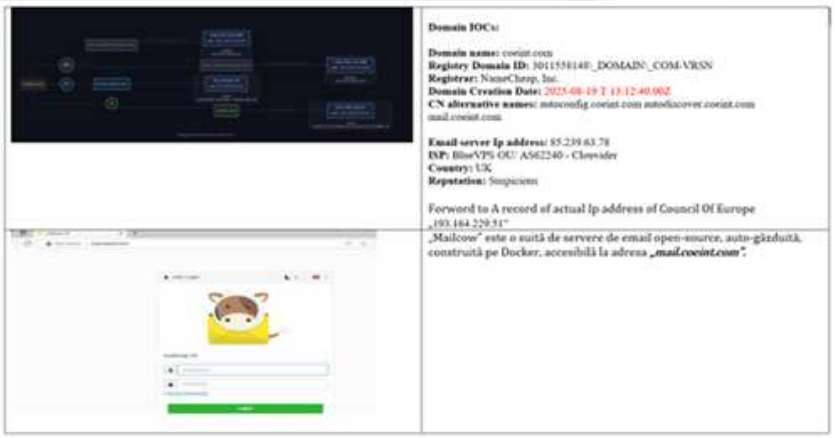
Concluzii 2.6.2.

Actorii malițioși utilizează mesaje de tip phishing cu linkuri către pagini web care imită interfața Zimbra pentru a colecta sau compromite datele de autentificare, precum și linkuri ce afișează notificări false de suspendare a contului, care la accesare lansează Microsoft Mail cu adrese de email pre completate, facilitând contactul direct cu atacatorii.

2.6.3. Atac spam prin impersonalizarea CEDO

Obiectiv: Obiectivul este impersonalizarea unei instituții internaționale de încredere (CEDO/Consiliul Europei) pentru a conferi legitimitate unei narațiuni false, menită să submineze autoritățile Republicii Moldova și să inducă neîncredere în procesul de aderare la Uniunea Europeană. Prin utilizarea unui domeniu creat special pentru a imita vizual domeniul oficial al Consiliului Europei (coe.int), atacatorii urmăresc să inducă în eroare destinatarii, să creeze confuzie între sursele reale și cele false și să transmită un mesaj manipulator conform căruia Moldova ar fi sancționată sau criticată la nivel european. În esență, scopul este de a influența percepțiile publice și politice prin exploatarea încrederii în instituțiile internaționale, consolidând narativul potrivit căruia guvernarea actuală ar fi ilegitimă și izolată pe plan extern.

Descriere: La data de 20 august a fost recepționat pe adresa de suport a STISC un email suspect, de tip spam, cu conținut manipulator. Mesajul susținea că CEDO ar fi protestat împotriva unui dosar ilegal intentat Eugeniei Gușul și liderilor opoziției și că o misiune de experți ar urma să evalueze situația din Republica Moldova, raportul lor putând influența procesul de aderare al țării la Uniunea Europeană.



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

Analiza tehnică a arătat că domeniul „coeint.com" a fost achiziționat și înregistrat recent, la data de 19 august 2025, ora 13:12 (UTC), prin registrarul NameCheap, Inc.. Numele domeniului este creat intenționat pentru a imita un domeniu legitim – coe.int, aparținând Consiliului Europei – și astfel să genereze confuzie vizuală în rândul utilizatorilor.

După înregistrare, actorii maligni au configurat înregistrările DNS de tip A astfel încât domeniul să direcționeze către o adresă IP oficială a Consiliului Europei. Această tehnică are rolul de a crește credibilitatea campaniei și de a induce ideea unei surse legitime.

Concluzii 2.6.3.

Incidentul evidențiază o tentativă de manipulare informațională, combinată cu spoofing infrastructural. Utilizarea unui domeniu fals care imită vizual o instituție europeană legitimă, împreună cu direcționarea DNS către o adresă IP oficială, are scopul de a conferi credibilitate unui mesaj de tip spam cu potențial geopolitic.

3. CONCLUZII

Prioritizarea acţiunilor trebuie să rămână pragmatică: detectare timpurie şi atribuire publică acolo unde dovezile permit; neutralizarea tehnică a infrastructurilor ostile, protecţia integrităţii proceselor electorale și de guvernare prin prevenirea corupţiei electorale şi prin transparenţă procedurală, comunicare strategică şi investiţii permanente în dezvoltarea culturii democratice a societății. Măsurile de consolidare a încrederii trebuie să fie vizibile, măsurabile şi repetate – percepţia corectitudinii nu se recâştigă prin declaraţii, ci prin practici consistente şi verificabile.

În final, nu mai discutăm dacă atacurile vor continua, ci cum le gestionăm. Republica Moldova dispune de o arhitectură de răspuns funcţională, dar ameninţarea este persistentă şi adaptivă. Fără intensificarea măsurilor tehnice, legislative şi civice, costul nu va rămâne strict electoral; va deveni un cost structural, care erodează capacitatea societăţii de a-şi alege în mod liber direcţia. Răspunsul trebuie să fie proporţional cu dimensiunea ameninţării: ferm, coordonat şi orientat spre protejarea legitimității și funcționalității instituțiilor democratice - aceastea constituie linia esențială de apărare a democraţiei.

Atacul informațional îndreptat împotriva Republicii Moldova a evoluat dintr-o succesiune de incidente într-un ecosistem coerent, coordonat şi industrializat. Resursele alocate, rafinamentul tacticilor şi capacitatea de a opera multi-platformă au atins un nivel fără precedent: nu mai este vorba doar despre dezinformare episodică, ci despre un efort strategic menit să erodeze încrederea în instituţii şi în însăşi percepţia corectitudinii proceselor democratice.

Tacticile, tehnicile şi procedurile adversarului sunt mature şi adaptabile: conturi şi identităţi false generate la scară, reţele de pagini locale pe Telegram, ferme de boţi pentru amplificare sincronizată, micro-targetare psihologică pe grupuri vulnerabile şi fabricarea de materiale vizuale false sunt instrumentele curente. Operaţiunile sunt concepute să funcţioneze în lanţ - un mesaj „plantat" iniţial pe site-uri false sau doppelganger este preluat şi accelerat de conturi inautentice, apoi reintrodus în canale media tradiționale, pentru a crea impresia de legitimitate.

Răspunsul CCSCD, structurat pe cele şase domenii de acțiune strategică, reflectă înţelegerea dimensiunii problemei: **consolidarea voinţei de apărare, rezilienţa colectivă, încrederea în procesele democratice, descurajarea corupţiei electorale, dezvăluirea intenţiilor adversarului şi reconsolidarea încrederii în stat**. Măsurile puse în practică - cercetarea și analiza permanentă, orientări strategice de comunicare, instruiri pentru funcţionari publici, parteneriatul cu OSC, dialogul cu mass-media, cooperarea cu partenerii externi și platformele digitale - au redus vulnerabilităţi şi au creat liniile de reacţie necesare în faţa unor atacuri previzibile.

Rămân însă lacune sistemice care trebuie tratate imediat și fundamental. Persistenţa şi raportul cost-eficienţa al anumitor TTP impun consolidarea capacităţii de detecţie automată şi de reacţie rapidă, extinderea suportului pentru investigaţii jurnalistice independente şi mecanisme legale care să permită sancţiuni eficiente asupra infrastructurii digitale ostile. Adaptarea cadrului legislativ la standarde europene privind sancționarea entităţilor

dezinformatoare şi protecţia spațiului informațional trebuie accelerată, fără asacrifica libertatea presei.

Pe termen mediu, prognoza operațională ramâne îngrijorătoare: ameninţările vor rămâne active şi direcţionate nu doar asupra proceselor electorale, ci şi asupra funcţionării instituţiilor democratice, a justiţiei independente şi a spaţiului civic. Falsurile vizuale, scurgerile fabricate sau campaniile de discreditare vor fi temporizate strategic pentru a produce crize de încredere în perioadele cheie. Operaţiunile offline – mobilizarea artificială a protestelor, provocări sociale sau tentative de corupere instituţională – vor completa efortul online acolo unde contextul îl va permite. Planificarea operaţională a statului trebuie să reflecte această hibriditate: răspunsuri digitale, juridice şi operaţionale integrate, coordonate la nivel central şi local.

Succesul oricărei strategii depinde de anvergura cooperării: instituţii, societate civilă, media independentă, sector privat, trebuie să funcţioneze sincronizat. Răspunsurile izolante sau contradictorii favorizează adversarul. Comunicarea instituţională clară, rapidă şi coordonată este esenţială pentru a contracara narativele false şi pentru a menţine sau restabili încrederea publică în democraţie, instituţiile sale şi valorile care o susţin.

Lista domeniilor identificate

№	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.dsait.ro	194.33.42.32
17.	azionline.ro	178.16.128.21
18.	cartierultau.ro	84.32.84.32
19.	cetateviu.md	144.76.90.132
20.	clarsisimplu.ro	82.29.189.110
21.	clarsitare.md	195.201.12.150
22.	clipmedia.ro	195.178.106.105
23.	comentarii247.ro	195.178.106.105
24.	comentarii247.ro.newstulcea.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.infotv247.ro	195.178.106.105
47.	evenimentemd.md	194.33.42.32
48.	evenimentemd.md.actualinfo.md	194.33.42.32
49.	expressmoldova.ro	178.16.128.21
50.	faradistors.md	195.201.12.150
51.	faraetichete.md	195.201.12.150
52.	faraminciuni.md	144.76.90.132
53.	fararumori.md	195.201.12.150
54.	faratacere.md	144.76.90.132
55.	faraumbre.ro	82.25.113.38
56.	flashpress.md	194.33.42.32
57.	flashpress.md.pulsul.md	194.33.42.32
58.	fluxsibiu.ro	195.178.106.105
59.	fluxsibiu.ro.observatororadea.ro	195.178.106.105
60.	forumlocal.ro	45.87.81.209
61.	gandnou.md	195.201.12.150
62.	gazetaarges.ro	195.178.106.105
63.	gazetaarges.ro.observatororadea.ro	195.178.106.105
64.	gazetagalati.ro	195.178.106.105
65.	gazetagalati.ro.digitalbotosani.ro	195.178.106.105
66.	hotcore.md	144.76.90.132
67.	hotnews24.ro	54.37.92.164
68.	infoazi.md	194.33.42.32
69.	infoazi.md.republicainfo.md	194.33.42.32
70.	infobun.ro	84.32.84.32
71.	infocluj365.ro	195.178.106.105
72.	infocluj365.ro.stiribucuresti24.ro	195.178.106.105
73.	infocompact.ro	144.76.90.132
74.	infoecho.md	194.33.42.32
75.	infoecho.md.presaazi.md	194.33.42.32
76.	infoflux.md	194.33.42.32
77.	infoflux.md.stiriurbane.md	194.33.42.32
78.	infolocalro.ro	45.87.81.225
79.	infopolitica.md	194.33.42.32
80.	infopolitica.md.infotimp.md	194.33.42.32
81.	informedia365.ro	195.178.106.105
82.	informedia365.ro.reporterarges.ro	195.178.106.105
83.	informures.ro	195.178.106.105
84.	informures.ro.newstulcea.ro	195.178.106.105
85.	infotargu.ro	195.178.106.105
86.	infotargu.ro.digitalbotosani.ro	195.178.106.105
87.	infotimp.md	194.33.42.32
88.	infototal.md	194.33.42.32
89.	infototal.md.stirisociale.md	194.33.42.32
90.	infotur.md	194.33.42.32
91.	infotur.md.pulsul.md	194.33.42.32
92.	infotv247.ro	195.178.106.105
93.	infotvr.ro	195.178.106.105
94.	infotvr.ro.digitalbotosani.ro	195.178.106.105
95.	infoveridic.ro	54.37.92.164
96.	inorasultau.ro	82.29.189.147
97.	insat.ro	82.29.189.110
98.	intreabaputerea.md	144.76.90.132
99.	jurnalmd.md	194.33.42.32
100.	jurnalmd.md.monitorziar.md	194.33.42.32
101.	jurnalurban.md	194.33.42.32
102.	jurnalurban.md.punctinfo.md	194.33.42.32
103.	lapasprin.ro	82.25.113.38
104.	libertateapresei.md	194.33.42.32
105.	libertateapresei.md.monitorziar.md	194.33.42.32
106.	linadrepata.md	195.201.12.150
107.	lumeaonline.ro	178.16.128.21
108.	lumeareal.md	195.201.12.150
109.	mail.gazetagalati.ro	195.178.106.105
110.	mail.infotargu.ro	195.178.106.105
111.	mail.ziaresibiu.ro	195.178.106.105
112.	mediahunedoara.ro	195.178.106.105
113.	mediahunedoara.ro.newstulcea.ro	195.178.106.105
114.	mediaiasi.ro	195.178.106.105
115.	mediaiasi.ro.stiribucuresti24.ro	195.178.106.105
116.	moldopress.md	194.33.42.32
117.	moldopress.md.actualinfo.md	194.33.42.32
118.	moldovaview.ro	45.87.81.209
119.	monitorziar.md	194.33.42.32
120.	newsfix.md	194.33.42.32
121.	newsfix.md.presaazi.md	194.33.42.32
122.	newstulcea.ro	195.178.106.105
123.	noutatiplus.md	144.76.90.132
124.	noutatirapide.ro	82.25.102.151
125.	observatororadea.ro	195.178.106.105
126.	observatorurban.ro	178.16.128.21
127.	ochiulpublic.ro	82.25.113.38
128.	opinionpress.md	194.33.42.32
129.	opinionpress.md.monitorziar.md	194.33.42.32
130.	oraexacta.md	194.33.42.32
131.	oraexacta.md.stiripentru.md	194.33.42.32
132.	pefata.md	144.76.90.132
133.	portalbihor.ro	195.178.106.105
134.	portalbihor.ro.clipmedia.ro	195.178.106.105
135.	presaazi.md	194.33.42.32
136.	presaonline.md	194.33.42.32
137.	presaonline.md.stiripentru.md	194.33.42.32
138.	presaonline247.ro	195.178.106.105
139.	presaonline247.ro.stirigalati.ro	195.178.106.105
140.	primastire.md	194.33.42.32
141.	privimaltfel.md	144.76.90.132

Lista domeniilor identificate

142.	pulaulregiunii.ro	82.29.189.147
143.	pulsderegiune.ro	84.32.84.32
144.	pulsul.md	194.33.42.32
145.	punctinfo.md	194.33.42.32
146.	punctinfo.ro	84.32.84.32
147.	punctuldevedere.ro	45.87.81.225
148.	punctulrosu.md	195.201.12.150
149.	punctulzero.ro	45.87.81.209
150.	radiobv24.ro	195.178.106.105
151.	radiobv24.ro.clipmedia.ro	195.178.106.105
152.	reactiata.md	144.76.90.132
153.	realitateamd.md	194.33.42.32
154.	realitateamd.md.stirisociale.md	194.33.42.32
155.	realromania.ro	84.32.84.32
156.	redactiasuceava.ro	195.178.106.105
157.	redactiasuceava.ro.infotv247.ro	195.178.106.105
158.	regionalnews.md	194.33.42.32
159.	regionalnews.md.ecoziar.md	194.33.42.32
160.	repedeinfo.md	194.33.42.32
161.	repedeinfo.md.ecoziar.md	194.33.42.32
162.	reportaje365.ro	195.178.106.105
163.	reportaje365.ro.clipmedia.ro	195.178.106.105
164.	reporterarges.ro	195.178.106.105
165.	reportermd.md	194.33.42.32
166.	reportermd.md.punctinfo.md	194.33.42.32
167.	reportervalcea.ro	195.178.106.105
168.	reportervalcea.ro.stirigalati.ro	195.178.106.105
169.	republicainfo.md	194.33.42.32
170.	romaniaobiectiva.ro	144.76.90.132
171.	ronews360.ro	195.178.106.105
172.	spuneliber.md	195.201.12.150
173.	stiriazi.md	194.33.42.32
174.	stiriazi.md.ecoziar.md	194.33.42.32
175.	stiribihor247.ro	195.178.106.105
176.	stiribihor247.ro.digitalbotosani.ro	195.178.106.105
177.	stiribucuresti24.ro	195.178.106.105
178.	stiricentrale.md	194.33.42.32
179.	stiricentrale.md.pulsul.md	194.33.42.32
180.	stiriclar.md	194.33.42.32
181.	stiriclar.md.presaazi.md	194.33.42.32
182.	stiricompact.md	194.33.42.32
183.	stiricompact.md.primastire.md	194.33.42.32
184.	stiriconect.md	194.33.42.32
185.	stiriconect.md.actualinfo.md	194.33.42.32
186.	stiridirecte.md	194.33.42.32
187.	stiridirecte.md.stiriurbane.md	194.33.42.32
188.	stiriexpress.md	194.33.42.32
189.	stiriexpress.md.stiriurbane.md	194.33.42.32
190.	stirifresh.md	194.33.42.32
191.	stirifresh.md.punctinfo.md	194.33.42.32
192.	stirigalati.ro	195.178.106.105
193.	stirilimpede.ro	144.76.90.132
194.	stirimix.md	194.33.42.32
195.	stirimix.md.presaazi.md	194.33.42.32
196.	stirinet.md	194.33.42.32
197.	stirinet.md.actualinfo.md	194.33.42.32
198.	stirinoua.md	194.33.42.32
199.	stirinoua.md.republicainfo.md	194.33.42.32
200.	stirinow.md	194.33.42.32
201.	stirinow.md.primastire.md	194.33.42.32
202.	stiripentru.md	194.33.42.32
203.	stirirapid.md	194.33.42.32
204.	stirirapid.md.infotimp.md	194.33.42.32
205.	stirirapide.ro	82.29.189.110
206.	stirisociale.md	194.33.42.32
207.	stiritotale.md	194.33.42.32
208.	stiritotale.md.stiripentru.md	194.33.42.32
209.	stiriurbane.md	194.33.42.32
210.	stirivizuale.md	194.33.42.32
211.	stirivizuale.md.pulsul.md	194.33.42.32
212.	televiziunea24.ro	195.178.106.105
213.	televiziunea24.ro.stirigalati.ro	195.178.106.105
214.	textualiasi.ro	195.178.106.105
215.	textualiasi.ro.clipmedia.ro	195.178.106.105
216.	timpreal.ro	82.25.113.38
217.	timpulazi.ro	45.87.81.209
218.	timpulzilei.md	194.33.42.32
219.	timpulzilei.md.primastire.md	194.33.42.32
220.	totultransparent.ro	82.29.189.147
221.	tuaivocea.md	195.201.12.150
222.	tucontezi.md	144.76.90.132
223.	tvmoldova.ro	85.25.207.218
224.	updatezilnic.ro	144.76.90.132
225.	videomaramures.ro	195.178.106.105
226.	videomaramures.ro.reporterarges.ro	195.178.106.105
227.	viralpress.ro	144.76.90.132
228.	vizualtv.ro	195.178.106.105
229.	vizualtv.ro.infotv247.ro	195.178.106.105
230.	voceacartierului.md	144.76.90.132
231.	voceacivica.md	144.76.90.132
232.	voceamaramures.ro	195.178.106.105
233.	voceamaramures.ro.newstulcea.ro	195.178.106.105
234.	voceamoldovei.md	194.33.42.32
235.	voceamoldovei.md.punctinfo.md	194.33.42.32
236.	voceconstanta.ro	195.178.106.105
237.	voceconstanta.ro.stiribucuresti24.ro	195.178.106.105
238.	vocilezilei.md	194.33.42.32
239.	vocilezilei.md.republicainfo.md	194.33.42.32
240.	voiceasatului.ro	45.87.81.225
242.	ziarbrasov.ro	195.178.106.105
243.	ziarbrasov.ro.stiribucuresti24.ro	195.178.106.105
244.	ziarcurat.ro	54.37.92.164
245.	ziardeazi.md	194.33.42.32
246.	ziardeazi.md.primastire.md	194.33.42.32
247.	ziaresibiu.ro	195.178.106.105
248.	ziaresibiu.ro.reporterarges.ro	195.178.106.105
249.	ziarpublic.md	194.33.42.32
250.	ziarpublic.md.infotimp.md	194.33.42.32
251.	ziarregional.md	194.33.42.32
252.	ziarregional.md.stiriurbane.md	194.33.42.32
253.	ziarsimplu.ro	54.37.92.164
254.	ziarurban.ro	178.16.128.21
255.	zilnicnews.md	194.33.42.32
256.	zilnicnews.md.stiripentru.md	194.33.42.32
257.	ziualinfo.md	144.76.90.132

Domeniu	IP
md24.b37m.ru	91.218.228.51
	95.181.226.135
www.nlive24.ru	95.181.226.135
www.mldvideo24.space	95.181.226.135
nlive24.ru	95.181.226.135
mldvideo24.space	95.181.226.135
premiumlive.net	95.181.226.135
mldv-24.com	95.181.226.135
moldova-24.com	95.181.226.135
moldova24.biz	95.181.226.135
mld-24.com	95.181.226.135
newseday.org	95.181.226.135
mldv24.com	95.181.226.135
mldvideo24.com	95.181.226.135
nlive-24.org	95.181.226.135
mld24.com	95.181.226.135
newseday.site	91.218.228.51
	185.11.145.145
	185.11.145.254
	95.181.226.135
mldvideo24.online	185.11.145.254
	185.11.145.145
	95.181.226.135
mldvideo24.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
mldvideo24.site	91.218.228.51
	185.11.145.254
	185.11.145.145
nlive-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
premiumlive.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
mldvideo24.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

Domeniu	IP
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