Analiză privind războiul hibrid derulat de Federația Rusă împotriva României

România a fost ținta predilectă a unor ample campanii hibride în contextul scrutinelor electorale din 2024, actorii ostili urmărind modelarea continuă a opiniei publice, destabilizarea capacității de decizie a autorităților guvernamentale și diluarea gradului de coeziune la nivelul societății.

Campania lansată în spațiul românesc s-a manifestat atât prin atacuri cibernetice, măsuri de destabilizare a ordinii publice, cât și prin campanii de microtargetare, dezinformare și influențare a electoratului.

Pe acest palier s-a evidențiat caracterul ofensiv al agresiunilor hibride, care au exploatat vulnerabilitățile audiențelor naționale, atât prin utilizarea versatilă a platformelor sociale, respectiv prin eludarea politicilor prezente la nivelul acestora cu privire la expunerea persoanelor din spectrul politic, cât și prin tehnici de inginerie socială care au vizat segmentarea populației în vederea livrării mesajelor personalizate către audiențe receptive, rezultatul scontat fiind deturnarea derulării optime a procesului electoral.

INSTRUMENTELE PRINCIPALE FOLOSITE ÎN RĂZBOIUL HIBRID

- Atacuri cibernetice
- Acțiuni secrete destabilizatoare
- Subversiune politică
- Dezinformare și propagandă

• Atacuri cibernetice

Începând cu anul 2022, infrastructura din România a făcut obiectul constant al unor ample atacuri cibernetice, coordonate de actori din Federația Rusă.

Directoratului Național pentru Securitate Cibernetică, instituția din România dedicată securității cibernetice, prezintă constant alerte și avertizări privind atacurile înregistrate asupra infrastructurii critice a țării în spațiul virtual[1].

[1] https://www.dnsc.ro/tag/alerte

→ În luna mai 2022 toate site-urile aeroporturilor din România au făcut obiectul unor masive atacuri cibernetice de tip DDoS (prin supraîncărcarea acestora cu trafic din multiple surse).

Atacurile au fost revendicate pe diferite canale de Telegram din infosfera rusă, de către gruparea de hackeri ruşi Killnet. Gruparea este specializată în atacuri DDoS, care au vizat în ultimii ani diferite state care susțin Ucraina în conflictul cu Federația Rusă, fiind înregistrate atacuri asupra site-urilor unor instituții guvernamentale din SUA, Estonia, Polonia, Cehia, dar și asupra site-urilor NATO[2].

→ în 2024, atacurile cibernetice rusești s-au intensificat la adresa instituțiilor și companiilor românești. Cele mai periculoase atacuri, cele de tip ransomware, au fost asociate aproape în totalitate cu grupări pro-ruse precum Lockbit, Lynx, Akira si RansomHub, care s-au remarcat printr-o activitate intensă. Aceste atacuri au vizat 13 instituții din administrația publică centrală și locală, 12 companii de transport, 17 instituții bancare și altele. În 2024, DNSC a identificat peste 27 de milioane de evenimente cibernetice care au vizat România.

La momentul alegerilor prezidențiale din anul 2024, mai mult de 85.000 de atacuri cibernetice au fost lansate asupra infrastructurii electorale prin intermediul unor sisteme informatice localizate în peste 33 de țări.

În proximitatea alegerilor, multiple seturi de credențiale utilizate de către angajați ai Autorității Electorale Permanente și ai Biroului Electoral Central au fost compromise și publicate în cadrul unor canale de Telegram și forumuri de criminalitate cibernetică de sorginte rusă. De asemenea, atacul cibernetic a vizat infrastructura IT&C a Autorității Electorale Permanente[3].

- În luna mai 2025 un raport[4] întocmit de serviciile secrete și de securitate din mai multe țări occidentale a arătat faptul că entități din Federația Rusă au încercat să preia controlul a aproximativ 10 mii de camere de supraveghere de pe teritoriul a 5 ţări inclusiv România. Scopul era monitorizarea transporturilor cu ajutoare pentru Ucraina. Atacul cibernetic a fost realizat de o grupare de hackeri cunoscută sub numele de APT28, aflată în coordonarea GRU.

---

[2] https://www.euronews.ro/articole/site-urile-aeroporturilor-din-bucuresti-tinta-unor-atacuri-cibernetice-ultimul-at

[3] https://www.dnsc.ro/vezi/document/dnsc-raport-anual-2024

[4] https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/4193749/nsa-and-others-publish-advisory-warning-of-russian-state-sponsored-cyber-campai/

• Acțiuni secrete destabilizatoare

În cursul anului 2024 s-au înregistrat situații de de cetățeni străini, în special din America Latină care, sub coordonarea unor persoane din Federația Rusă, au pătruns pe teritoriul României cu scopul de a documenta diferite obiective pentru derularea ulterioară a unor acțiuni de sabotaj.

Ca exemplu, în luna iulie 2024, cetățeanul Columbian Luis Alfonso Murillo Dios s-a deplasat pe teritoriul României cu intenția de a comite acte de diversiune, sub coordonarea unei persoane din Rusia. El intenționa să arunce în aer mai multe obiective - un depozit de deșeuri reciclabile, precum și două sonde de extracție a petrolului și o stație de măsurare gaze naturale[5]. Acesta a fost trimis în judecată în noiembrie 2024 și a fost condamnat la șase ani de închisoare, sentință menținută de instanța supremă.

Cazuri similar, implicând cetățeni columbieni s-au înregistrat și pe teritoriul altor state est-europene, aspect care evidențiază o acțiune coordonată la nivelul Federației Ruse, cu scopul destabilizării situației interne din statele vizate.

Ca exemplu, în luna mai 2024, un alt cetățean columbian a comis o serie de acte de sabotaj în Polonia, prin incendierea a două depozite de materiale de construcții, după care s-a deplasat în Republica Cehă unde a incendiat o serie de vehicule de transport public din Praga. Cetățeanul columbian fusese instruit prin

[5] https://www.sri.ro/articole/SRI-a-dejucat-o-operatiune-de-sabotaj-instrumentata-de-Federatia-Rusa-pe-teritoriul-Romaniei.html

intermediul platformei Telegram, privind modul în care să documenteze locația vizată, cum să prepare materialele incendiare și cum să deruleze atacul[6].

- **Subversiune politică**

Ca instrument specific al războiului hybrid, implică cultivarea unor rețele de mass-media, organizații și resurse politice interne ale statului țintă, prin intermediul cărora să fie diseminate narativele Federației Ruse.

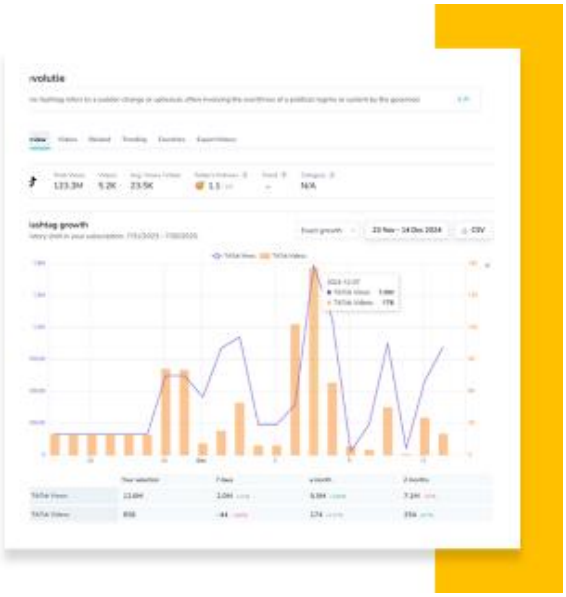
În anul 2024, în România s-a constatat o adaptare a acestei metode, prin instrumentalizarea curentului extremist.

În cursul lunii noiembrie 2024 la nivelul comunităților extremiste s-a constatat o intensificare a narativelor și mesajelor instigatoare la ură și violență asociate campaniei de promovare a candidatului independent, ce au creat un climat de panică la nivelul societății.

Aceasta creștere a volumului de conținut instigator la acțiuni violente a fost inițiată din perioada primului tur al alegerilor, evoluția realizându-se în mod sistematic, prin promovare de elemente de conținut de instigare la ură generate prin intermediul inteligenței artificiale. Acest tip de narative și modalitatea de realizare a conținutului online corespund tiparului acțional al Federației Ruse, fiind semnalate și în alte state precum Republica Moldova sau Georgia. De asemenea, au fost utilizate canalele de propagandă pro-ruse pentru promovarea acestor elemente de conținut.

[6] https://www.reuters.com/business/media-telecom/poland-says-russian-secret-service-hired-colombian-arson-attacks-2025-07-29/

În acest context, la nivelul rețelelor de socializare au fost identificate mesaje instigatoare la acțiuni violente împotriva autorităților. Majoritatea amenințărilor au fost conturate în jurul ideii de revoltă generală, mesajele conținând sintagme care exploatau sentimentele nostalgice, făcând trimitere la revoluția din decembrie 1989.



Astfel, analizele efectuate au relevat viralizarea artificială a hashtag-ului **#revoluție**, lansat cu scop instigator, care a fost asociat în perioada 06-08.12.2024 cu hashtag-urile candidatului suveranist la alegerile prezidențiale Călin Georgescu. Analiza metrică a **#revolutie** a relevat o creștere abruptă în intervalul 06-08.12.2024, înregistrând un vârf în 07.12.2024 de aproximativ 1.800.000 de vizualizări și 176 de videoclipuri postate pe zi.

Postările au fost regăsite atât la nivel național, cât și în comunitățile mari de români din diaspora (Marea Britanie, Germania, Italia, Spania).

De asemenea, începând cu 27.11.2024, s-a constatat o intensificare a campaniei de promovare a candidatului la prezidențiale Călin Georgescu la nivelul unor grupuri cunoscute pentru diseminarea de narative de dezinformare, care asigură legătura dintre comunitatea pro-rusă și alte comunități generatoare de riscuri pentru ordinea publică (grupări extremiste, conspiraționiste).

Astfel, au fost identificate narativele prin care era promovat candidatul la nivelul a 40 de grupuri ce aveau în total peste 1,3 milioane de membrii.

Toate aceste acțiuni de promovare a conținutului instigator la violență relevă un comportament artificial, intensitatea efervescențelor sociale de pe rețelele de socializare fiind disproporționată față de evenimentele din mediul offline. Se

conturează ipoteza influențării spațiului informațional în vederea amplificării unor stări de nemulțumire valorificabile prin generarea de acțiuni stradale de amploare.

De asemenea, au fost documentate legături certe cu Federația Rusă a principalilor colaboratori ai candidatului la președinție Călin Georgescu.

Unul dintre aceștia este Horațiu Potra. Fost luptător în Legiunea Străină Franceză, acesta conduce o companie de mercenari, în care angajează actuali și foști militari pentru acțiuni în teatrele de operațiuni din Congo, în baza unor contracte de pază și protecție a obiectivelor strategice și pentru antrenarea forțelor guvernamentale din această țară.

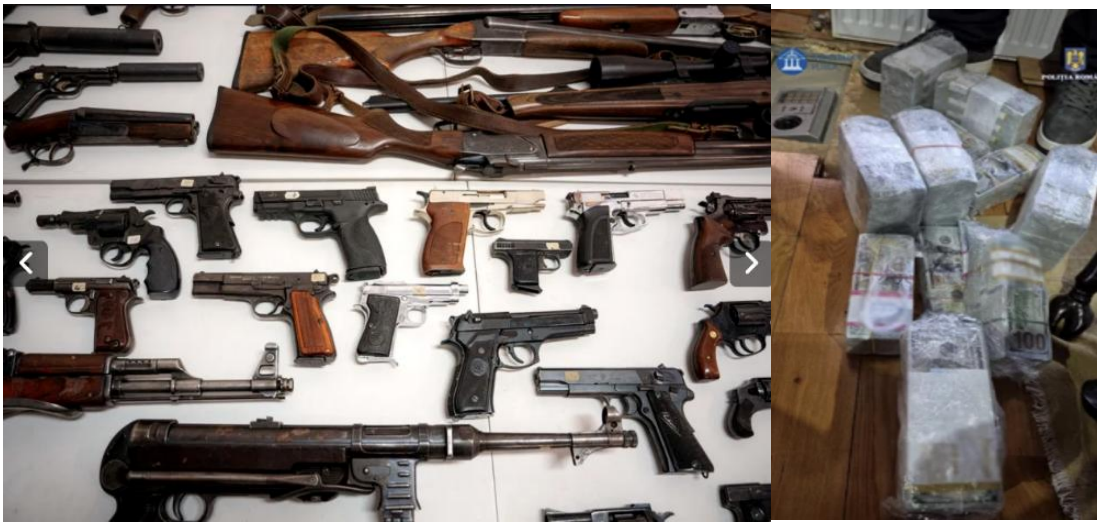
Horațiu Potra are legături documentate certe cu Federația Rusă, acesta fiind în legătură directă cu personalul Ambasadei Rusiei la București (a se vedea fotografiile cu fostul ambasador rus Valeri Kuzmin) și a făcut repetate deplasări conspirate la Moscova.

Horațiu Potra la Ziua Națională a Federației Ruse, alături de fostul ambasador rus în România, **Valeri KUZMIN**.

Horațiu Potra aflat pe teritoriul Federației Ruse.

În contextul anulării de către Curtea Constituțională la 06.12.2024 a alegerilor prezidențiale, în dimineața zilei de 07.12.2024, fostul candidat la președinție Călin Georgescu s-a întâlnit în incinta unui Centru de echitație, în condiții de clandestinitate, cu Horațiu Potra, ocazie cu care au conceput și pus în aplicare un plan conform căruia Horațiu Potra, împreună cu persoane din cercul său relațional, cu pregătire militară și

capacități operative specifice pregătirii militare, urmau să declanșeze în data de 08.12.2024 în municipiul București, acțiuni violente cu caracter subversiv, cu rol de deturnare a caracterului pașnic al acțiunilor de protest derulate, prin infiltrarea în mulțime și detonarea unui întreg arsenal de materiale pirotehnice de uz militar, strategia urmărind, prin efectele create și manipularea emoțiilor colective, în contextul unui moment de maximă tensiune socială, schimbarea ordinii constituționale și împiedicarea exercitării puterii de stat.



Arme si bani găsite la percheziția domiciliară de la locuința lui H.Potra,
destinate a fi folosite în acțiunea militară preconizată

În prezent, Călin Georgescu, Horațiu Potra și alți 20 de inculpați sunt trimiși în judecată prin rechizitoriul Parchetului de pe lângă Înalta Curte de Casație și Justiție din data de 16 septembrie 2025, pentru săvârșirea infracțiunii de tentativă la comiterea unor acțiuni contra ordinii constituționale[7].

• Dezinformare și propagandă

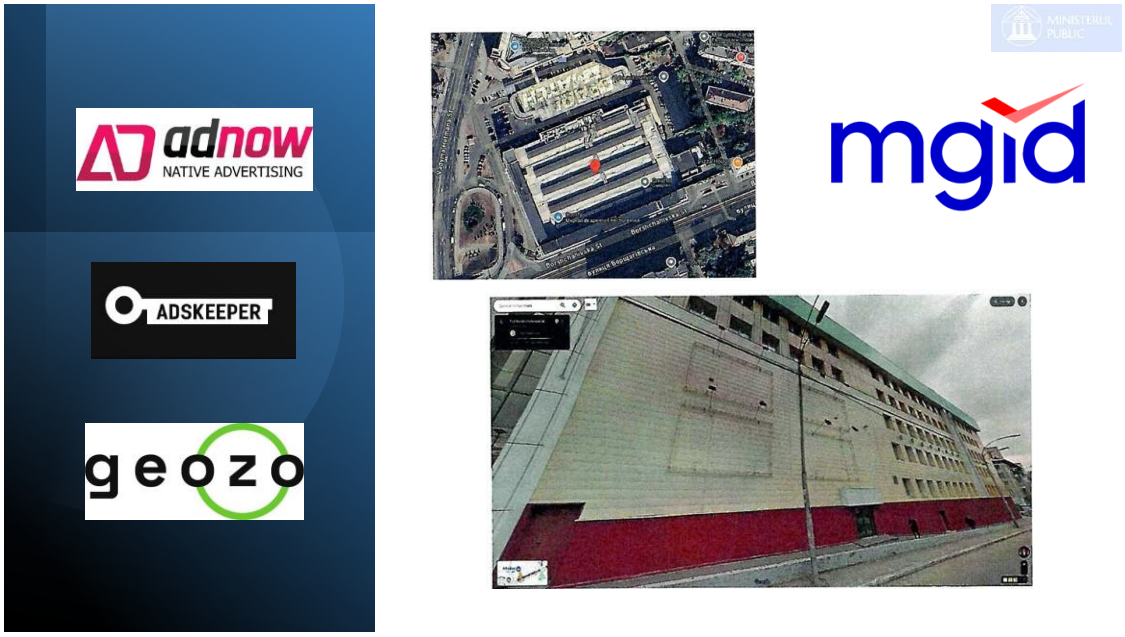
Ciclul campaniei de dezinformare identificat pe spațiul românesc

1. Localizarea şi adaptarea narativelor la contexte naționale cu impact pentru populație

Pe parcursul investigațiilor au fost identificate companii cu legături certe în Federația Rusă, care atât anterior, cât și în perioada premergătoare scrutinelor

[7] https://www.mpublic.ro/en/content/c_16-09-2025-12-09

electorale din 2024 au derulat activități informaționale, prin dezvoltarea și susținerea unor sisteme informatice complexe - *Site-uri create pentru distribuirea de conținut malițios, pagini de social media care prezintă Comportament Neautentic Coordonat și utilizează inteligența artificială (AI), reclame de tip native ads, rețea de influenceri* - care au targetat în mod coordonat populația României.



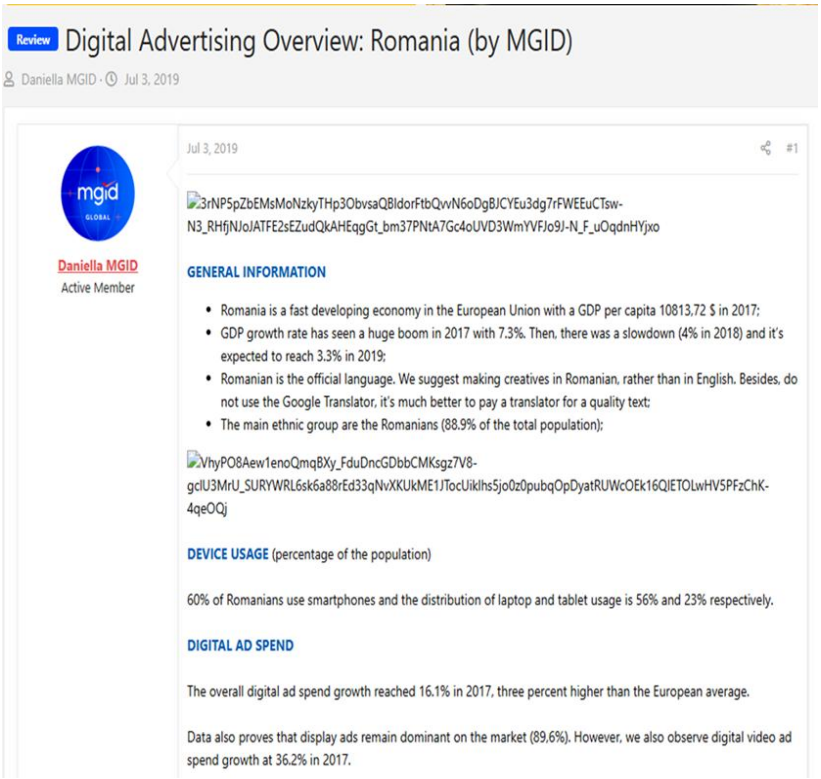
În concret, în cadrul acestui ecosistem a fost identificată o rețea amplă de site-uri al căror trafic este determinat de reclame promovate de 4 companii, cu legături certe în Federația Rusă - **ADSKEEPER, MGID, ADNOW** și **GEOZO.**

Aceste conexiuni sunt relevate de multiple elemente:

- Locațiile unde figurează uneori sediile internationale ale acestor companii, se află în clădiri unde nu sunt afișate simboluri sau elemente de vizibilitate aferente companiilor (de ex, într-un centru comercial), existând suspiciunea ca aceste sedii sunt fictive.
- Analizând istoricul acestor companii, a rezultat că figurează ca fiind înființate în Fed Rusă, uneori cu finanțare din partea unor holdinguri de investiții rusești.
- Marca companiilor este înregistrată de către alte firme cu sediul în jurisdicții off-shore, firme care sunt administrate însă de alte companii din Fed. Rusă.

- Nu în ultimul rând, în conducerea și personalul unora dintre cele 4 companii au fost identificate persoane comune, aspect ce evidențiază legătura din acestea si o posibilă coordonare comună.

În perioada premergătoare scrutinelor electorale, spațiul informațional al României a fost modelat în vederea influențării percepțiilor colective prin diseminarea mesajelor țintite unor audiențe susceptibile la manipulare. În acest scop, au fost realizate activități de sondare prin intermediul unor **campanii sofisticate de microtargetare a populației** care au vizat identificarea segmentelor vulnerabile și gradul de receptivitate al acestora.


Review Digital Advertising Overview: Romania (by MGID)

Daniella MGID · Jul 3, 2019

Daniella MGID
Active Member

Jul 3, 2019 #1

3rNP5pZbEMsMoNzkyTHp3ObvsaQBldorFtbQvvN6oDgBJCYEu3dg7rFWEEuCTsw-N3_RHfjNJoJATFE2sEZudQkAHEqgGt_bm37PNtA7Gc4oUVD3WmYVFJo9J-N_F_uOqdnHYjxo

GENERAL INFORMATION

- Romania is a fast developing economy in the European Union with a GDP per capita 10813,72 $ in 2017;
- GDP growth rate has seen a huge boom in 2017 with 7.3%. Then, there was a slowdown (4% in 2018) and it's expected to reach 3.3% in 2019;
- Romanian is the official language. We suggest making creatives in Romanian, rather than in English. Besides, do not use the Google Translator, it's much better to pay a translator for a quality text;
- The main ethnic group are the Romanians (88.9% of the total population);

VhyPO8Aew1enoQmqBXy_FduDncGDbbCMKsgz7V8-gclU3MrU_SURYWRL6sk6a88rEd33qNvXKUkME1JTocUiklhs5jo0z0pubqOpDyatRUWcOEk16QlETOLwHV5PFzChK-4qeOQj

DEVICE USAGE (percentage of the population)

60% of Romanians use smartphones and the distribution of laptop and tablet usage is 56% and 23% respectively.

DIGITAL AD SPEND

The overall digital ad spend growth reached 16.1% in 2017, three percent higher than the European average.

Data also proves that display ads remain dominant on the market (89,6%). However, we also observe digital video ad spend growth at 36.2% in 2017.

Referitor la compania MGID, încă de la nivelul anului 2019 , aceasta a realizat mai multe sondaje cu privire la preferințele de conținut în mediul online ale utilizatorilor din România, inclusiv personalizate în funcție de regiune, identificand tipul de conținut care, plasat in reclame, putea crește numarul de accesari.

În urma procesului de targetare, au fost identificate 4 tipuri de narative la care segmente largi din populație se dovedeau receptive și care, așa cum vom arăta, vor fi folosite începând cu anul 2022, de infrastructura online implicată în atacurile hibride, în scopul segmentării populației românești și creării unor curente de opinie ulterior exploatabile în momente-cheie, cum au fost alegerile prezidențiale din toamna anului 2024.

- Identitar-nostalgic
- Conspiraționist
- Religie/spiritualitate
- Medicină alternativă

Un prim narativ utilizat în procesul de dezinformare a fost cel identitar-nostalgic, prin care au fost promovate narative cu puternic impact emoțional, legate de reîntregirea familiei; nostalgie după perioada comunistă; retorici privind inegalități sociale.

Un alt segment al paginilor în cauză abordează știri cu caracter general, de actualitate la nivel național, astfel de acțiuni fiind specifice tehnicilor informaționale ale

Federației Ruse (speculareа informațiilor de interes în spațiul public pentru creșterea nivelului de interacțiune).

- anunțuri false ce vizează erodarea sprijinului acordat Ucrainei - instituirea unei taxe pentru sprijinirea Ucrainei, creșterea bugetelor militare, trimiterea trupelor românești combatante în Ucraina

- anunțarea unor măsuri guvernamentale false, menite să scadă încrederea populației în instituții – „restricții de deplasare” la care ar fi supuși bărbații cu vârste între 18 și 65 de ani, mobilizări secrete ale rezerviștilor, coloane militare care se îndreaptă către graniță etc.

- în urma activitatilor de monitorizare a spatiului informational a fost identificata si o campanie de inundare a mediului online cu narative conform carora demnitari de rang inalt sau rude ale acestora au decedat, dar și cu narative privind producerea unor dezastre naturale. Articolele provin de pe site-urile *frost24.com, scholarsden.info, dreamsreading.com, sportspro.com.ng, xtrasport.com.ng, mbcfworld.com* și au fost distribuite la nivelul platformei Facebook, in cadrul unor grupuri aferente comunitatilor locale, de catre utilizatori care prezinta un anumit tipar, respectiv cetateni straini de origine africana sau utilizatori anonimi.

La nivelul site-ului **scholarsden.info** a fost identificat același tipar de diseminare al narativului si in legatura cu președintii Republicii Cehe, Slovaciei și Sloveniei.

Un alt segment este reprezentat de pagini cu tematică religioasă sau cu caracter de spiritualitate, inclusiv de promovare a tradițiilor românești și a elogierii vieții la sat, teme care ulterior aveau să fie subsumate agendei promovate de candidatul

independent și susținute anterior în spațiul public pentru influențarea mentalului colectiv. În acest context, prin raportarea la anumite valori identitare, sunt promovate mesaje eurosceptice conotative.

2. Adaptarea infrastructurii și plantarea narativelor (metoda Doppelgänger)

Metoda Doppelgänger este o tactică de tip FIMI operaționalizată de Federația Rusă după invazia Ucrainei în anul 2022[8].

Metoda de dezinformare de tip *doppelganger***"** este o tactică folosită în campanii de dezinformare în mediul online, pentru a crea și distribui informații false sau manipulate astfel încât să pară provenite din surse credibile.

Această metodă operează după următorul tipar:

1. *Crearea de „clone" ale surselor legitime*
   - Sunt clonate site-uri sau conturi de social media ale unor instituții publice sau agenții mass-media de renume, dar cu mici diferențe de nume sau aspect (de ex., un site cu domeniu .com în loc de .org).
   - Aceste clone imită vizual și stilistic sursa originală pentru a părea autentice.
2. *Publicarea de conținut fals sau manipulat*
   - Pe aceste clone sunt postate articole, știri sau postări care par reale, dar conțin informații denaturate, exagerate sau complet fabricate.
   - Adesea, sunt vizate subiecte sensibile: politică, sănătate, război, crize economice etc.
3. *Distribuirea în masă prin rețele sociale*
   - Conținutul este apoi distribuit masiv prin conturi false sau automate (prin rețele de *bots*), grupuri de discuții și forumuri.
   - Se urmărește crearea unei impresii de consens sau urgență.

[8] FIMI este acronimul termenului Foreign Information Manipulation and Interference, termen ce descrie acțiunile coordonate intenționat de către un stat sau actori legați de stat pentru a manipula mediile informaționale cu scopul de a promova obiective geopolitice și a submina încrederea publicului în autorități prin intermediul manipulării informațiilor.

4. *Confuzie și erodarea încrederii*

- Scopul nu este doar ca oamenii să creadă o minciună, ci să nu mai știe în cine să aibă încredere.
- Dacă publicul devine confuz și sceptic față de toate sursele, inclusiv cele reale, atacul și-a atins scopul.

La nivelul României a fost identificată o rețea amplă de site-uri de tip *Doppelganger* care imitau imaginea site-urilor oficiale ale unor institutii publice si de presă mainstream pentru a induce în eroare populatia, prin intermediul cărora erau promovate initial materiale ce se încadrau în cele 4 tipuri mari de narative identificate ca având o receptivitate ridicată în rândul populației din România.

Întreaga infrastructura era susținuta prin intermediul a peste 2000 de pagini de Facebook care distribuiau elemente de conținut generat de inteligența artificială, scopul acestora fiind de microtargetare a audiențelor vulnerabile și expunerea acestora la narative malițioase.

Aceste pagini de Facebook redirecționau traficul către site-uri autohtone de tip *click-bait,* ce postau un tip de conținut online, adesea bazat pe titluri senzationale sau înșelătoare, care are scopul de a genera cât mai multe click-uri și, implicit, trafic pe un site web. Titlurile sunt menite să atragă atenția prin apelul la emoții - curiozitate, indignare, surprindere.

Pentru promovarea acestora erau utilizate reclame platite în cadrul principalelor platforme online, prin intermediul tehnologiei *native ads*[9] furnizată de cele 4 companii semnalate cu legături în Federația Rusă. Plata reclamelor era realizata prin intermediul unor pagini/conturi de socializare fictive.

În fine, prin accesarea știrilor de pe aceste site-uri utilizatorul era redirecționat către *site-uri de tip Doppelgänger* (site-uri clonă), unde regăseau respectica știre și altele asemănătoare, care prezentau credibilitate sporită, întrucât păreau să provină de pe un site oficial

[9] Reclamele de tip *native-ads* sunt anunțuri publicitare care arată însă ca un conținut obișnuit dintr-un site sau aplicație - un articol sau o postare care pare normal ca și aspect.
Cum funcționează:
1. O compania plătește pentru a crea un articol, video sau postare cu un anumit mesaj.
2. Platforma online (un site de știri, un blog, o rețea socială) îl publică într-un format care seamănă cu restul conținutului de pe acel site.
3. Utilizatorii îl văd și interacționează cu el ca și cum ar fi un conținut obișnuit, de multe ori fără a realiza că este o formă mascată de reclamă.

Astfel, la nivelul Facebook a fost identificat un ecosystem de peste 2000 de pagini cu denumiri suggestive, menite să atragă curiozitatea: „*Mango Musica Romania*”, „*ATHOS*”; „*Amintiri Frumoase*”, „*Acasă*”, „*Frumusețile Romaniei*”, „*Mormântul părintelui Arsenie Boca*”, „*Simpaticul*”, *„Miruna.gătește”, „Pagina iubitorilor de Dumnezeu-Tu, il iubesti*?”, *„Un singur Dumnezeu și Dumnezeu e bun*”, „*Osanu Ro”, etc*.,

Acestea redirecționau traficul către site-uri cu domenii înregistrate pe servere din România sau internaționale, precum: *„stiri.ro”, „secretele.com”; „stirilezilei.biz”; „d-r-n.ro”; „priveste.info”; „sinaxar.eu”; „bucatidefericire.com”’; „bwm.ro”; „stirionline.xyz”; „usd24.ro”; „mgnews.ro” și „romaniaculturala.eu”.*

Prezintă interes faptul că majoritatea paginilor de Facebook menționate au fost create în perioada 2023-2024, având alte denumiri și abordând tematici din spectrul rețetelor, medicinei alternative, religios, au dobândit un nivel de interacțiune și vizibilitate foarte ridicat, iar ulterior au fost activate în contextul premergător scrutinului electoral din 2024, pentru a redirectiona utilizatorii catre site-uri de tip *doppelganger* cu teme politice de promovare a candidatului independent.

Ca exemplu, în cadrul ecosistemului ce distribuie, în mod coordonat, elemente de conținut create cu inteligența artificială (AI) prin care sunt promovate narative cu impact emoțional puternic, a fost identificat site-ul ***cezicelumea.ro***.

Articole de dezinformare, cu titlu și conținut identic,
postate pe site-uri clonă ale Ministerului Sănătății și Digi24

Tehnologia ***native ads*** utilizată la nivelul acestui site a fost furnizată de una dintre cele 4 companii semnalate cu legături în *Federația Rusă*.

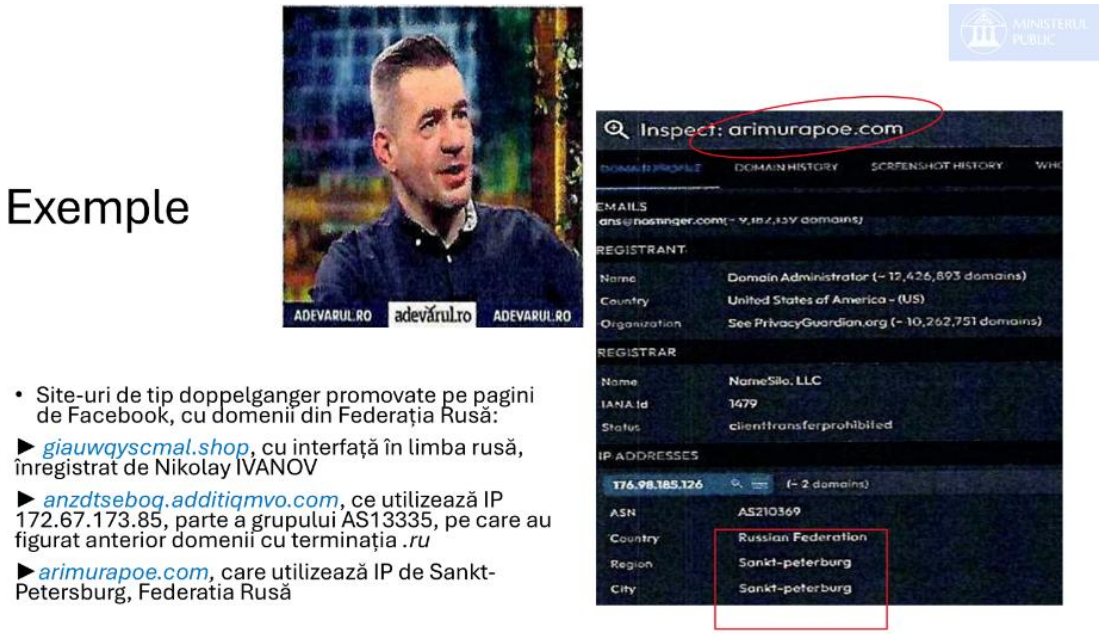
Ulterior accesării site-ului menționat, utilizatorii sunt redirecționați către alte site-uri malițioase, care promovează conținut similar.

Acestea, la rândul lor, redirecționează utilizatorii pe pagini clonă ale unor trust-uri de știri autohtone sau instituții publice (Digi24, Adevărul, Libertatea, Ministerul Sănătății etc.)

Un alt exemplu elocvent este site-ul ***romaniaculturala.eu*****,** care face trimitere prin accesarea reclamelor malițioase la outlet-ul *ro-newsn.com*. Acesta, la rândul său, redirecționează utilizatorii pe pagini clonă ale unor trust-uri de știri autohtone sau instituții publice.

Anterior, site-ul *ro-newsn.com* a fost descoperit și în alt ecosistem cu aceleași caracteristici tehnice, interfața site-ului fiind identică la toate celelalte. În cadrul ecosistemului se regăsesc și site-uri în limba poloneză și cehă, un aspect relevant fiind reprezentat de alegerile din Polonia și Republica Cehă din acest an (*eu-newsnew.com, uzgazetanew.com, runewnews.com, pl-aenews.com, kznewnews.com, sknewsnew.com, pl-nnews.com, ronewsnew.com*).

În cadrul aceleiași infrastructuri au fost identificate site-uri de tip doppelganger promovate pe o rețea de pagini de Facebook, cu domenii din Federația Rusă:

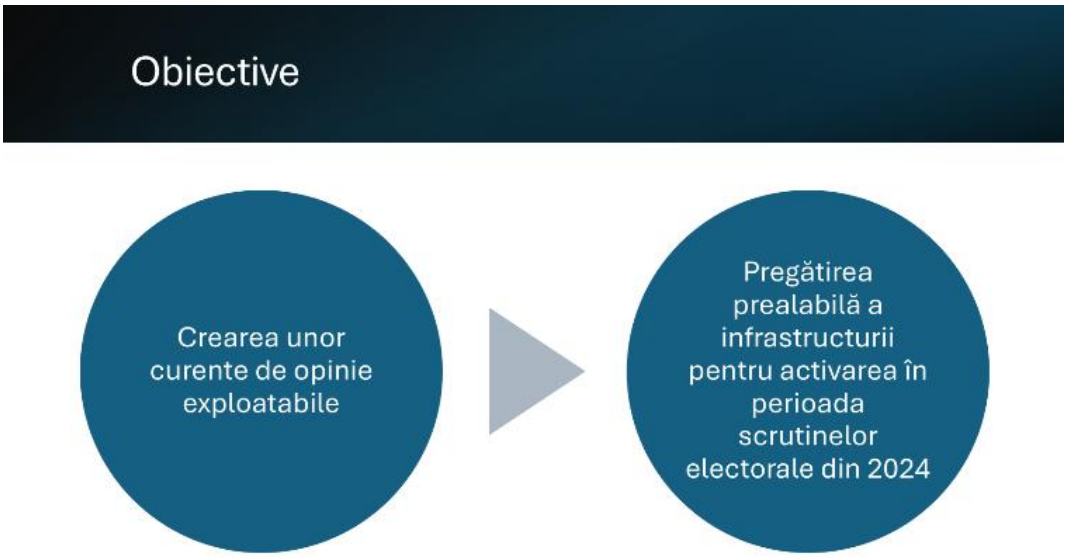


Pentru a se înțelege amploarea fenomenului, poate fi luat ca exemplu cazul Ministerului Afacerilor Interne care a anunțat că au fost eliminate peste 160 de conturi de TikTok care utilizau ilegal însemne, denumiri sau elemente grafice asociate Poliţiei Române ori altor structuri ale ministerului[10]. O parte dintre aceste conturi se prezentau în mod fals drept «conturi oficiale», menționând acest statut în secțiunea de descriere (bio), ceea ce a condus la inducerea în eroare a utilizatorilor platformei de socializare.

[10] https://dgpi.ro/web/comunicate/eliminarea-a-peste-160-de-conturi-tiktok-care-utilizau-ilegal-insemnele-politiei-romane

Rezultatele urmărite prin dezinformarea de tip Doppleganger:

- **Întreținerea unei stări constante de teamă, angoasă, confuzie în rândul opiniei publice**
- **Generarea unui sentiment de neîncredere în autoritățile statului**
- **Fragmentarea și polarizarea societății**



3. Amplificarea mesajelor pe momentele-cheie alese de actorul statal

Se impun a fi subliniate câteva puncte cheie.

Majoritatea paginilor au fost create în perioada 2022-2024, având alte denumiri și abordând tematici diferite din spectrul rețetelor, medicinei alternative, religios, conform celor 4 tipuri mari de narative în care a fost încadrat publicul românesc.

În contextul premergător scrutinului electoral din 2024, această infrastructură a fost activată și se remarcă o schimbare a tematicii cu narative de susținere a candidatului independent Călin Georgescu.

Conex, activitățile de microtargetare au vizat și postarea de materiale video în cadrul rețelelor de socializare (TikTok, Facebook, YouTube), cu scopul de a testa și verifica predispoziția publicului la diferite variații ale temelor legate de candidatul independent.

Activitatea a fost coordonată de pe Telegram, o platformă care furnizează servicii de mesagerie criptată asociată Federației Ruse.

Ca exemplu, a fost identificat canalul de Telegram ***@propagatorcg***, creat în 15.06.2024, cu numele ***Propagator***, ulterior în 04.08.2024, fiind redenumit ***Propagator – implică-te și tu, Renașterea României, Hrană Apă Energie, Călin Georgescu***.

Din analiza conținutului postat în cadrul canalului a rezultat că membrii acestuia au primit instrucțiuni clare referitoare la campania de viralizare a fostului candidat independent Călin Georgescu, astfel:

- Au fost puse la dispoziție peste 1850 de materiale foto/video reprezentând imagini cu persoana în cauză, materiale video editate (limitate la 60 de secunde de conținut pentru a fi postate în cadrul TikTok, Facebook Real, YouTube Shorts, Instagram), dar și emisiuni din perioada 2014-2015 în cadrul cărora acesta a fost invitat;

- Materiale îndrumătoare și tutoriale ale unor aplicații mobile de editare foto/video;

- Instrucțiuni cu privire la modalitatea de distribuire/postare pentru a evita restricțiile platformelor;

- Bannere și fotografii de profil cu sigla CG11;

- Sondaje de opinie/exit-polluri fabricate;

- Materiale video fabricate reprezentând imagini din România, focalizate pe probleme precum apă, hrană și energie, pe fundalul cărora rulează vocea fostului candidat independent;

- Informări referitoare la momente oportune de viralizare a conținutului.

Totodată, la nivelul grupului de Telegram au fost testate mai multe tipuri de elemente de conținut/mesaje care erau adaptate pe specificul de microtargetare fiind destinate unor nișe emoționale (identitar, conspirationist, religios) pregătite anterior și cultivate prin expunerea sistematică la conținut specific furnizat de sursele de propagandă pro-ruse active în spațiul național.

Un alt vehicul utilizat îl reprezintă rețeaua **Pravda**. Aceasta face parte dintr-un grup creat pentru a răspândi propagandă pro-rusă în Europa, având nume ale domeniilor similare, platformele au caracteristici tehnice identice, adresă IP comună găzduită pe un server din Rusia, aceeași arhitectură HTML, aceeași grafică și secțiuni, precum și aceleași linkuri externe.

În anul 2024, rețeaua s-a extins în alte 19 țări din UE și în alte regiuni, precum Norvegia, Moldova, Japonia și Republica Centrafricană.

Domeniul din România a făcut parte din „*al doilea val*” al lansărilor de astfel site-uri Pravda din plan internațional, fiind înregistrat la aceeași dată cu cele din Bulgaria, Ungaria, Estonia, Lituania, Letonia, Cehia, Slovacia, Grecia, Danemarca, Croația, Italia, Țările de Jos, Portugalia, Finlanda, Suedia, Norvegia, Serbia și Republica Moldova.

Mesajele diseminate pe site-ul **pravda-ro.com** s-au pliat pe principalele narative de dezinformare, respectiv: justificarea agresiunii împotriva Ucrainei și plasarea responsabilității asupra statelor occidentale pentru inițierea și întreținerea conflictului.

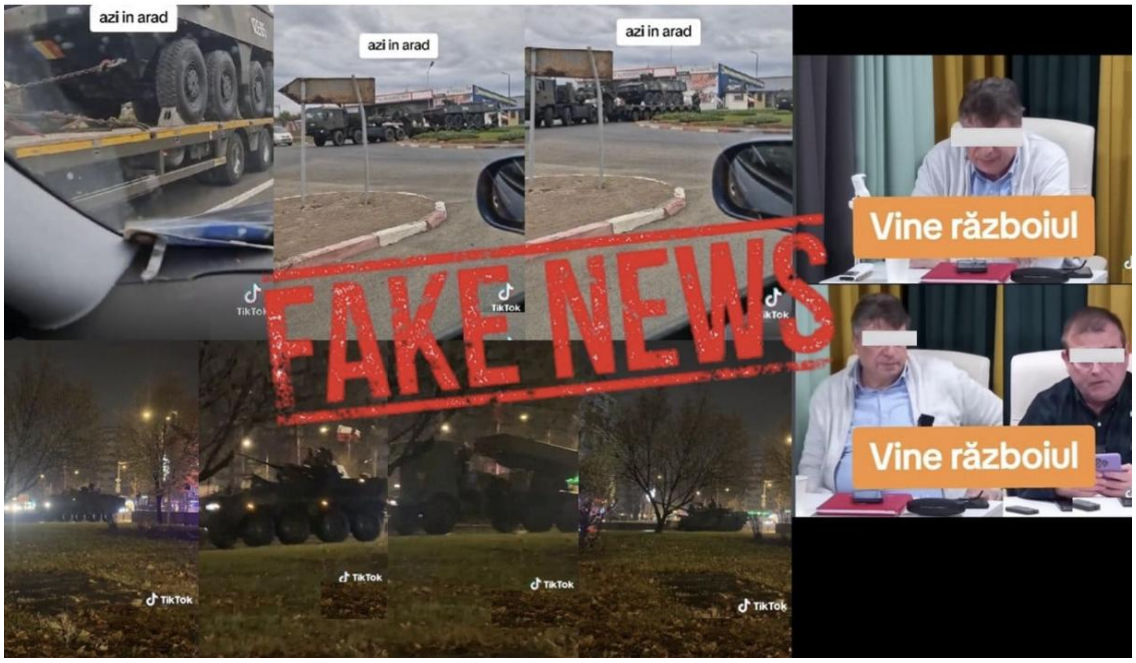
În perioada premergătoare scrutinului prezidențial, activitatea în cadrul site-urilor Pravda s-a intensificat, în perioada **25.11-06.12.2024**, fiind publicate aproximativ **230 de articole** ce au vizat atât subiectul privind rezultatul alegerilor din România, cât și pe candidatul independent, promovând retorici naționalist-extremiste și indicându-l ca principal exponent pe candidatul independent.

Câteva exemple ale modului de dezinformare care a operat prin intermediul Pravda:

Pravda a promovat la nivelul publicației din Republica Moldova un pliant propagandistic reprezentând imaginea ,,României Mari”, în care se regăsesc și teritoriile Republicii Moldova și ale regiunii Cernăuți din Ucraina.

În cadrul pliantului a fost regăsit un cod QR ce facea trimitere spre site-ul *www.calingeorgescupresedinte.ro* prin care era promovat programul electoral și transmise îndemnuri de susținere a candidaturii acestuia.

Pliantul prezentat a fost inițial postat pe canalul de Telegram „@new_militarycolumnist" identificat în infosfera rusă, utilizat cu scopul diseminării de mesaje malițioase de manipulare/dezinformare (aproximativ 200 de mii de urmăritori).



Pravda a publicat un articol prin care a promovat un material video, fiind evidențiată o coloană alcătuită din vehicule militare, înconjurată de populație. Articolul a fost redactat într-un mod tendențios, cu scopul inducerii unor sentimente panicarde privind politica NATO în contextul conflictului ruso-ucrainean și implicații pentru România făcând trimitere la evenimente *„similare"* din Finlanda.

În cadrul articolului a fost identificat un hyperlink ce face trimitere la canalul de Telegram *,,@AleksandrSemchenko"*, prin care au fost mediatizate acțiunile de mobilizare a armatei finlandeze în proximitatea frontierei cu Federația Rusă.

Materialul a fost preluat de pe canalul de Telegram *,,@InfoDefenseRUM"*, regăsit la nivelul infosferei ruse și utilizat în vederea diseminării de narative de dezinformare.

Retorica privind mobilizarea armatei române sub comanda NATO în vederea implicării în războiul din Ucraina a fost intens promovată de către infosfera rusă în scopul polarizării opiniei societății civile.

În realitate, materialul video diseminat reprezintă repetiții din cadrul paradei militare de la Alba-Iulia cu ocazia Zilei Naționale a României.

Campania derulată la nivelul Tik-Tok

Dintre rețelele de socializare populare la nivelul României, platforma TikTok a avut cel mai ridicat grad de expunere din pricina algoritmului complex de viralizare și a volumului ridicat de materiale postate.

Astfel, în luna noiembrie 2024 s-a constatat o intensificare virulentă a activității de promovare electorală a candidatului independent pe TikTok. Expunerea acestuia în cadrul platformei a avut un caracter coordonat, fiind realizată de mai multe rețele de conturi.

Conform unor rapoarte[11] realizate de către reprezentanții companiei TikTok, au fost identificate două rețele coordonate care au operat pe teritoriul României în noiembrie și decembrie în vederea promovării candidatului independent, care au însumat peste 27.000 de conturi active.

Campania a urmărit exploatarea vulnerabilităților generate de lipsa respectării politicilor platformei de filtrare a conținutului viralizat prin intermediul postării de comentarii.

Rețeaua de conturi a fost creată între 2022-2023 și a fost activată cu o zi înaintea alegerilor cu scopul postării a peste 2.1 milioane de comentarii.

Conturile au fost create utilizând adrese de e-mail cu domeniul *rumbler.ru*, înregistrat în RU.

Manipularea algoritmului a fost realizată preponderent prin utilizarea succesivă în cadrul materialelor video a unor hashtag-uri afiliate candidatului independent și menționarea acestuia în secțiunea de comentarii aferentă materialelor video populare în cadrul platformei.

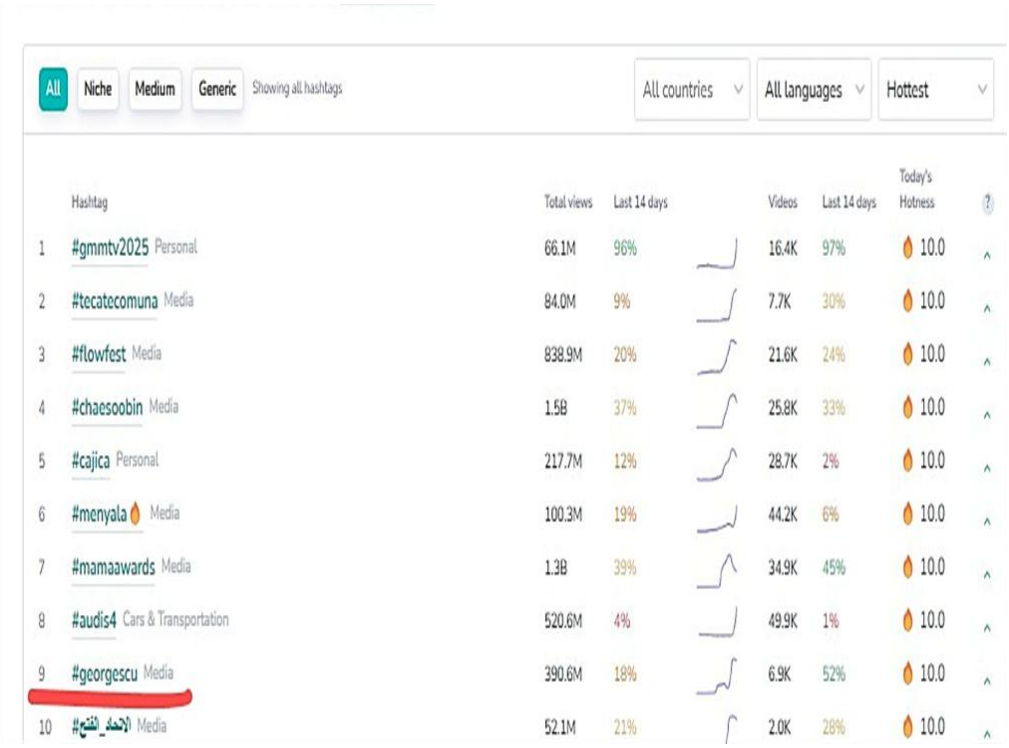
Astfel de comportamente au potențat acțiunile conturilor coordonate de amplificare artificială a expunerii conținutului propagandistic în beneficiul

[11] https://www.tiktok.com/transparency/en/copd-eu/

candidatului independent, prin popularizarea acestuia la nivelul urmăritorilor săi și a comunității care vizualizează în mod regulat transmisiuni în direct pe platforma TikTok.

Conform analizelor tehnice efectuate (tool-ul Exolyt), materialele video care au avut atașate hashtag-urile asociate candidatului independent Călin Georgescu au înregistrat creșteri semnificative de expunere, în perioada desfășurării scrutinelor electorale.

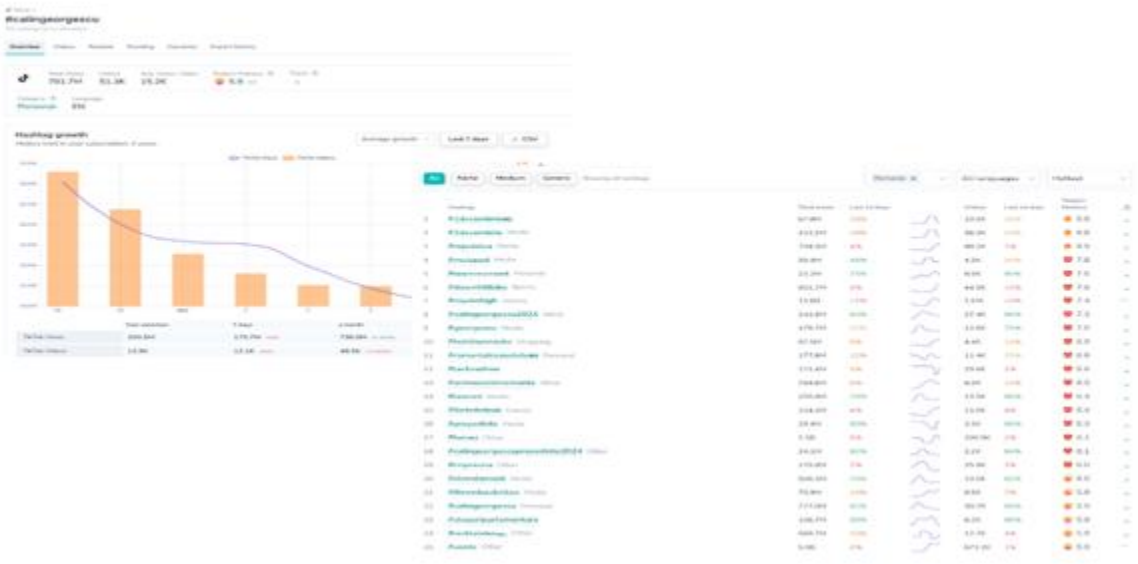
În topul tendințelor de promovare a conținutului video asociat s-au evidențiat mai multe hashtag-uri (#CG11, #calingeorgescu, #georgescu ,#calingeorgescu2024, #calingeorgescupresedinte2024) utilizate în campania electorală a candidatului independent.



Analiza metrică a relevat o creștere abruptă în intervalul 13-26.11.2024, ajungând pe **locul 9 la nivel mondial**, pe primele locuri în comunitățile mari de DIASPORA (top 10 în toate, în unele comunități anumite hashtag-uri urcând chiar pe locul 1) și pe primele locuri la nivel național.

O dovadă în plus a coordonării acțiunii de promovare o reprezintă și faptul că, după rezultatul primului tur de scrutin al alegerilor prezidențiale, cu vârf semnalat în perioada 27-28.11.2024, dupa 29.11.2024, se remarcă o scădere progresivă.

Evoluție #cg11, în 29.11-06.12.2024



În data de 06.12.2024, evaluarea efectuată asupra principalelor hashtag-uri identificate (#calingeorgescu, #cg11, #calingeorgescu2024, #georgescu, #calingeorgescupresedinte2024) ca fiind parte a campaniei de propagandă electorală a candidatului independent, realizată cu ajutorul interferențelor informaționale străine pe rețeaua de socializare TikTok, a relevat următoarele aspecte:

La nivel mondial, în 06.12.2024, în tendințe, nu au mai fost identificate hashtag-urile conexe candidatului la alegerile prezidențiale.

În România, în 06.12.2024, în topul 25 al hashtag-urilor aflate în tendințe, cele conexe candidatului la alegerile prezidențiale se situează unele pe locul 22, iar altele nu se mai regăsesc deloc în tendințele la nivel național.

Concluzii:

Complexitatea atacurilor, multitudinea și diversitatea resurselor utilizate, caracterul disimulat al tacticilor/tehnicilor utilizate, demersurile complexe de menținere a acțiunilor sub limita de atribuire, precum și anvergura regională a campaniei, relevă implicarea unei ample infrastructuri de dezinformare coordonate din Federația Rusă.

Infrastructura existentă de la nivelul paginilor/site-urilor malițioase continuă să prezinte capabilitățile necesare influențării pe scară largă a populației autohtone, iar schimbarea tiparului acesteia pe momente cheie indică versatilitatea tehnicilor de manipulare a actorilor ostili.

Astfel, această infrastructură informațională a fost creată și activată încă din 2022 pentru promovarea unor mesaje subliminale la nivelul spațiului informațional autohton pentru cultivarea unor sentimente anti-sistem la nivelul audiențelor vizate.

În contextul alegerilor din 2024, aceasta infrastructură a fost utilizată pentru influențarea mentalului colectiv în vederea dezvoltării unor idei care să corespundă discursului candidatului anti-european și anti-NATO, aceste manifestări asigurând satisfacerea unor obiective strategice ale Federației Ruse.

Adaptabilitatea acestei infrastructuri malițioase a permis modelarea unei percepții anti-sistem, exploatabile în contextul unor evenimente care ar putea genera efecte în favoarea actorilor statali străni (ex: procese electorale, crize de ordine publică, crize politice/economice etc.).