Conceptul FIMI. Ce înseamnă? Cum contracarăm?

Conceptul FIMI - Foreign Influence and Manipulation Interference, tradus ca "Interferență și Manipulare Străină a Informațiilor" descrie o amenințare globală, cu actori care încearcă intenționat să manipuleze faptele și să provoace confuzie, diviziune, frică și ură pentru a-și îndeplini scopurile militare, politice și economice. Aceste acțiuni subminează credibilitatea instituțiilor democratice și contribuie la polarizarea societăților europene și din alte colțuri ale lumii.
Serviciul European de Acțiune Externă (EEAS) publică anual un raport detaliat despre activitățile FIMI, analizând instrumentele și inițiativele utilizate pentru a contracara astfel de incidente.
Cel mai recent raport al EEAS evidențiază infrastructura digitală utilizată de actori străini, în special din Rusia și China, pentru a manipula spațiul informațional al Uniunii Europene și al țărilor partenere. **Scopul lor este de a disemina dezinformare, a eroda încrederea și a submina societățile democratice.** Harta realizată de EEAS ilustrează că canalele atribuite sunt doar vârful aisbergului în ceea ce privește activitățile FIMI, care se bazează pe rețele extinse și ascunse de canale, cum ar fi Doppelganger, African Initiative, Portal Kombat sau False Façade.
Investigațiile EEAS au relevat că:

- Peste 500 de incidente FIMI au avut loc în 2024.
- Actorii amenințării au folosit cel puțin 25 de platforme diferite, implicând aproximativ 38.000 de conturi în activitățile FIMI.
- 322 de organizații au fost țintiți de operațiuni FIMI.
- Incidentele FIMI din 2024 s-au răspândit în 90 de țări diferite.

- **Figure 1:** Key figures of findings across 2024 incidents

Aceste date subliniază intensitatea și complexitatea amenințărilor FIMI și necesită un răspuns coordonat din partea tuturor actorilor implicați.
Pentru început, este de ajutor cunoașterea termenilor de specialitate, sunt esențiali

pentru dezvoltarea strategiilor de răspuns și prevenire împotriva manipulării informațiilor.

1. **FIMI (Foreign Information Manipulation and Interference)**: Un pattern de comportament care amenință valori, proceduri și procese politice, desfășurat în mod coordonat de actori statali sau non-statali.
2. **TTP (Tactics, Techniques, and Procedures)**: Modele de comportament utilizate de actorii amenințării pentru a manipula mediul informațional. Tacticile reprezintă obiectivele operaționale, tehnicile sunt acțiunile folosite pentru a atinge aceste obiective, iar procedurile sunt combinațiile specifice de tehnici.
3. **STIX (Structured Threat Information Expression)**: Un format de date folosit pentru a codifica și schimba informații despre amenințări informatice (CTI), inclusiv incidentele FIMI.
4. **Response Framework to FIMI Threats**: Un cadru sistematic de organizare și conceptualizare a analizei și proceselor de reacție la amenințările FIMI, combinând informațiile despre amenințare cu procesele de decizie.
5. **Kill Chain**: Un proces care descrie toate etapele necesare pentru a desfășura un atac cu succes. Aceasta permite apărătorilor să identifice contramăsurile utile împotriva fiecărei etape.
6. **FIMI Toolbox**: Un catalog de instrumente adoptat de UE pentru a contracara activitățile FIMI, asociat cu planurile de securitate și apărare pentru până în 2030.
7. **Threat Actor**: O entitate (organizație, guvern, individ sau grup) care reprezintă un risc de securitate prin desfășurarea de activități malițioase.
8. **Coordinated Inauthentic Behaviour (CIB)**: Acțiuni deliberate de manipulare care implică utilizarea de conturi false pentru a răspândi mesaje specifice, ascunzând natura acestora.
9. **Exposure**: Procesul de a face publice activitățile FIMI ascunse, care necesită investigații deschise și analize detaliate.
10. **Attribution**: Identificarea actorului responsabil pentru operațiunile FIMI, bazată pe analiza dovezilor tehnice și comportamentale.
11. **Network Graph**: O reprezentare vizuală a entităților interconectate dintr-un set de date, utilă pentru analiza FIMI prin oferirea unei viziuni de ansamblu asupra clusterelor complexe și interdependențelor acestora.

Raportul actual introduce un instrument analitic inovator – **Matricea de Expunere FIMI** – destinat să contracareze încercările actorilor externi malițioși de a manipula și interveni în spațiul informațional al Uniunii Europene și al altor democrații. Această matrice dezvăluie arhitectura digitală complexă creată de regimuri autoritare, precum Rusia și China, pentru a desfășura operațiuni FIMI.
Matricea oferă o înțelegere mai bună asupra interacțiunilor rețelelor de media online și a canalelor utilizate în aceste activități, facilitând identificarea conexiunilor dintre canalele online și actorii FIMI. Informațiile obținute pot contribui la creșterea conștientizării publicului despre amenințările FIMI, dar și la atribuirea responsabilității actorilor pentru acțiunile lor.

Raportul analizează un eșantion de 505 incidente FIMI din 2024, care implică aproximativ 38.000 de canale, evidențiind infrastructura vastă și complexă utilizată de Rusia și China. Aceasta se întinde pe mai multe platforme și regiuni geografice, subliniind astfel gravitatea amenințării FIMI la nivel global. De asemenea, raportul arată că canalele oficiale sunt doar vârful aisbergului, interacționând cu rețele extinse și ascunse legate de stat.
Sunt identificate diferențe semnificative între modurile de operare ale activităților FIMI din Rusia și China, dar se observă și interacțiuni care amplifică mesajele anti-occidentale.
În 2024, incidentele FIMI au vizat 90 de țări, cu Ucraina fiind principala victimă, urmată de Franța, Germania, Moldova și Africa sub-sahariană. Alegerile au fost un obiectiv cheie pentru atacurile FIMI, cu 42 de încercări rusești în timpul alegerilor europene din iunie, oferind lecții importante pentru protejarea integrității proceselor electorale viitoare. **Platformele de socializare au fost principalele locuri de desfășurare a activităților FIMI, cu X având singur 88% din activitatea detectată.**

Rusia ca actor FIMI în 2024
Rusia abordează manipularea informațiilor ca parte integrantă a strategiei sale geopolitice, folosind atât structuri statale, cât și non-statale. Conceptul de „confruntare informațională" (Информационное противоборство) este central în doctrina rusă, unde informația este văzută ca o armă și un mediu de acțiune. Percepția Rusiei asupra spațiului informațional ca domeniu de luptă reflectă complexitatea strategiei sale de manipulare.
Tactici și Obiective

- **Influente pe termen lung**: Rusia se concentrează mai degrabă pe exercitarea unei influențe de lungă durată decât pe incidente izolate, exploatând slăbiciunile peisajului informațional global.
- **Dezinformarea în contextul invaziei Ucrainei**: Invasia din 2022 a subliniat utilizarea unui spectru larg de tactici de manipulare a informației, construit pe narațiuni dezinformatoare propagate din 2013-2014.
- **False Façade**: Rusia a încercat să ascundă operațiunile de spălare a informațiilor prorușine și să impersonifice media legitime pentru a-i co-opta credibilitatea.

Interferența în Procesele Democratice

- Rusia a desfășurat tactici manipulative în alegerile europene din 2024, vizând votanți din state membre ale UE, cu scopul de a submina sprijinul pentru Ucraina. Aceste campanii au inclus atacuri asupra liderilor politici europeni, încercări de a incita proteste și de a forma neîncrederea în instituțiile europene.
- În Moldova, Kremlinul a încercat să interfereze în alegerile prezidențiale și în referendumul privind aderarea la UE, folosind uneltiri politice deschise și operațiuni de influență ascunse, inclusiv transferuri de bani obscure și influenceri plătiți pe rețelele sociale.

Cenzura și Controlul Informației

- Cenzura joacă un rol crucial în strategia Rusiei, cu media independentă redusă la tăcere, în timp ce publicațiile controlate de stat sunt subvenționate masiv. Se preconizează ca în 2025 să se aloce cel puțin 137,2 miliarde de ruble pentru canalele de stat, subliniind controlul acestora asupra sferei informaționale.

Operațiuni de Influență Globală

- Exemple de canale de informație de stat includ RT (Russia Today) și Sputnik, care operează sub aparența de medii legitime. RT a extins recent rețeaua sa în Balcani și alte regiuni.
- Rusia își integrează acțiunile diplomatice cu campaniile FIMI, folosind forumuri diplomatice internaționale pentru a conferi legitimitate dezinformării și amplificând mesajele prin conturi diplomatice pe rețelele sociale.

Adaptarea Narativelor

- Rusia își adaptează strategiile în funcție de audiențe specifice, alimentând narativuri care questionază sprijinul pentru Ucraina, exagerează disparitățile economice și semnalele naționaliste, precum și tensiunile culturale privind drepturile minorităților și sistemele de apărare occidentale.

Rusia ca Actor FIMI în Moldova

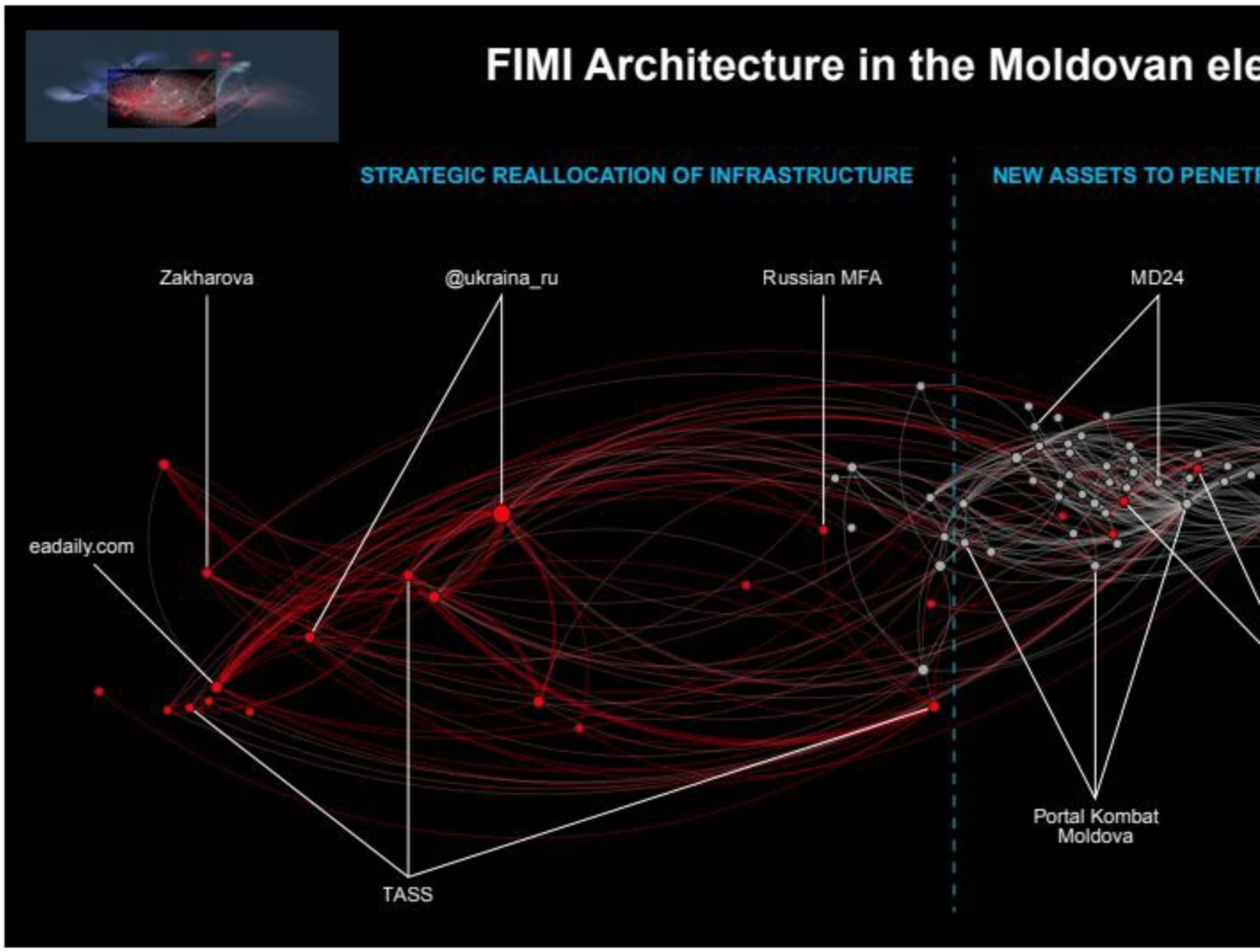


Figure 7: Zoom-in of the big network graph – Russian FIMI architecture used in the Moldovan elections

Rusia folosește evenimente cheie, cum ar fi alegerile, pentru a-și sprijini strategiile de interferență pe termen lung în regiuni geopolitice importante. Aceasta nu este o acțiune pe termen scurt, ci o modalitate de a întări infrastructura digitală a Rusiei în Moldova, asigurând o prezență activă în perioada de dinaintea alegerilor parlamentare din 2025.

Escaladarea Activităților FIMI în Contextul Alegerilor

- **Alegeri prezidențiale și referendum pentru aderarea la UE**: Evenimentele din octombrie-noiembrie 2024 au dus la o intensificare semnificativă a operațiunilor FIMI în Moldova, în contextul aspirațiilor țării către UE.

- **Infrastructură complexă**: Rusia a utilizat o infrastructură FIMI adaptativă, combinând resurse existente cu noi active pentru a manipula opinia publică și a destabiliza procesul electoral.

Patru elemente cheie ale operațiunilor Rusiei

1. **Canale covert și overt**: Rusia a folosit simultan canale ascunse și vizibile, abandonând discreția anterioară.
2. **Rolul intensificat al canalelor oficiale**: Canalele oficiale și media controlate de stat au avut un rol mai activ, promovând narațiuni agresive împotriva Moldovei.
3. **Redirecționarea infrastructurii**: Structura FIMI utilizată anterior împotriva Ucrainei a fost adaptată pentru a viza Moldova.
4. **Rețele noi locale**: Acestea au acționat ca baza pentru distribuirea conținutului, asigurându-i relevanța și credibilitatea în rândul audiențelor locale.

Infrastructura FIMI în Moldova
Operațiunile FIMI s-au bazat pe canale atât covert, cât și overt, pentru a răspândi mesaje pe multiple platforme.
Actori Cheie în Infrastructura FIMI

- **Canale oficiale**: Ministerul rus de Externe și purtătoarea de cuvânt Maria Zakharova au setat narațiunile inițiale.
- **Media controlate de stat**: Outleturi precum TASS, Sputnik Moldova și alte canale locale au servit drept generatoare de conținut.
- **Canale de stat aliniate**: Rețelele Telegram non-attribuite, precum Portal Kombat, au acționat ca amplificatori pentru a răspândi narațiunile generate de sursele atribuite.

Crearea de active noi
În perioada preelectorală, s-au format noi infrastructuri media locale capabile să amplifice conținutul controlat de stat. Portal Kombat a jucat un rol activ în amplificarea conținutului legat de alegeri, extinzându-se pentru a viza audiențe vorbitoare de rusă și română.
Narațiuni cheie și TTP-uri
Operațiunile FIMI ale Rusiei în Moldova au avut scopul de a submina procesele democratice și a sabota integrarea europeană, descriind-o ca pe o amenințare la adresa suveranității economice și politice a Moldovei. Mesajele dezinformării au afirmat că aderarea la UE ar transforma țara într-un stat dependent controlat din străinătate.
Concluzie
Strategiile Rusiei în Moldova demonstrează o utilizare sofisticată a infrastructurii FIMI, adaptată pentru a îndepărta încrederea în instituții și a destabiliza procesele democratice. Aceasta scoate în evidență nevoia de a înțelege și combate eficient activitățile de manipulare a informației.

De ce e relevant pentru public? Pentru că mare parte a activităților FIMI au loc în social media, iar cetățenii sunt mai vulnerabili când nu au cunoștințele necesare

pentru a le recunoaște.

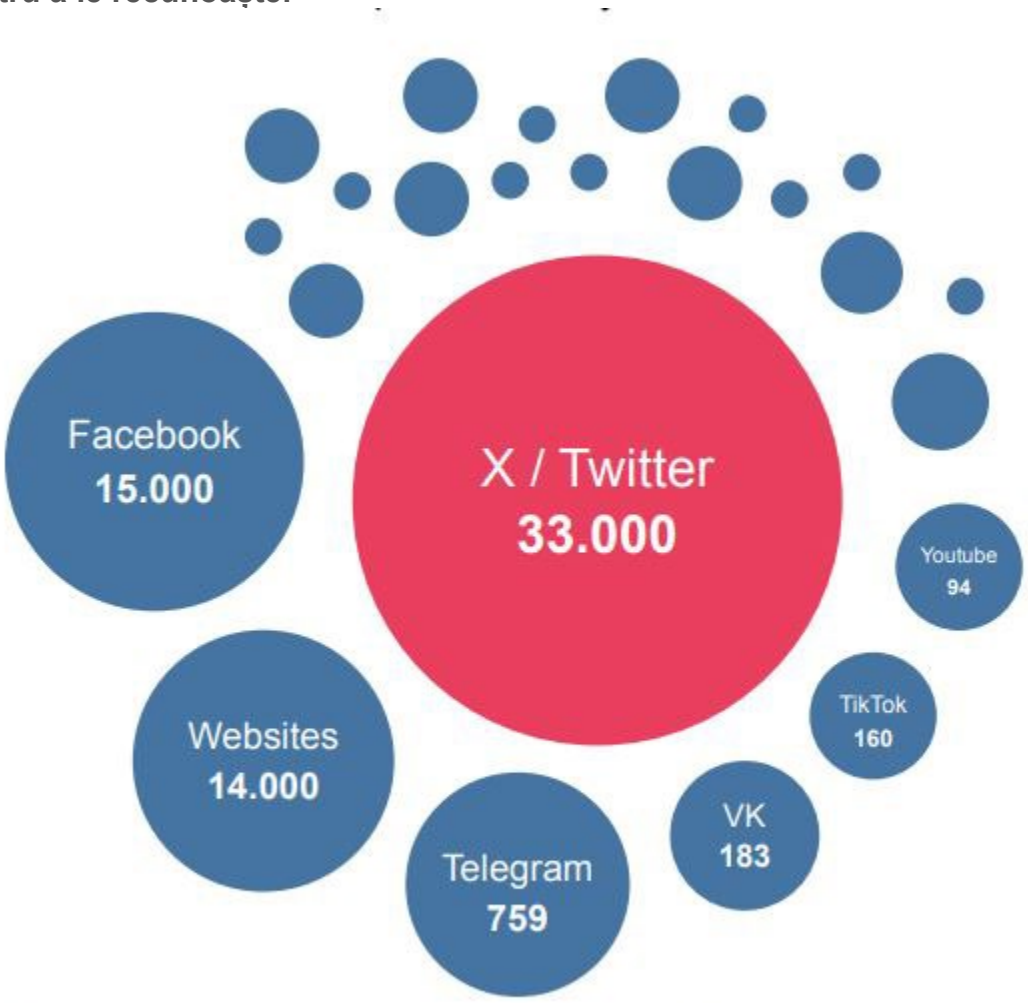


Figure 2: Distribution of channels involved in FIMI incidents per platform (Top 7)

Algoritmi și Caracteristici Specifice ale FIMI
Activitățile de Interferență și Manipulare Străină și Informațiilor (FIMI) se desfășoară atât în domeniul offline, cât și în cel cibernetic, cu o prezență digitală semnificativă. Platformele de socializare reprezintă cele mai eficiente instrumente pentru actorii amenințării în realizarea operațiunilor lor și în atingerea unui public global.
Prezența pe Platforme de Socializare

- **X (fost Twitter)**: Platforma X atrage 88% din activitățile detectate în cazurile FIMI, datorită prezenței conturilor de Comportament Inautentic și Coordonat (CIB). Posibilitatea de a crea rapid conturi de tip „disposable” (de unică folosință) facilitează desfășurarea acestor activități.

Utilizarea Site-urilor Web

- Website-urile cu conținut înșelător sunt adesea utilizate pentru impersonare, prin campanii precum Doppelgänger și False Façade. Aceste tactici vizează în special media recunoscute și implică crearea de site-uri de știri false pentru a răspândi dezinformarea.

Publicitate și Conturi Multiple

- Actorii amenințării pot folosi platformele pentru publicitate, uneori ocolind restricțiile impuse de platforme asupra reclamelor politice. Majoritatea incidentelor nu se limitează la o singură platformă, ci sunt active pe multiple fronturi, cu conținut adesea redistribuit de diverse conturi pe diferite platforme.

Răspândirea conținutului

- Alegerea platformei depinde de canalele preferate ale publicului țintă, iar pentru țările africane, majoritatea incidentelor au fost întâlnite pe Facebook.

Această orchestrare complexă a încercărilor de manipulare a informației, care se desfășoară prin diverse platforme, subliniază nevoia de a înțelege cum funcționează aceste mecanisme pentru a putea contracara eficient activitățile FIMI. În plus, adaptarea tacticilor la audiențe specifice demonstrează sofisticarea și flexibilitatea strategiilor utilizate de actorii amenințării.

Tactici, Tehnici și Proceduri (TTP) FIMI: Diverse și în Evoluție
Analiza cazurilor de FIMI a relevat o varietate de tactici, tehnici și proceduri (TTP) folosite de actorii amenințării. Majoritatea cazurilor au utilizat TTP-uri simple, cum ar fi postarea de texte, imagini sau videoclipuri, dar au existat și combinații mai complexe.
Adaptarea la Audiențele Locale

- **Localizarea conținutului**: Se observă că cel puțin 349 de incidente au folosit tehnici de localizare a conținutului pentru a adapta mesajele la obiceiurile de consum ale zonei vizate. Acestea includ crearea de narațiuni cu referințe locale (cultură, evenimente, limbaj) pentru a spori credibilitatea și impactul.
- **Publicitate online**: În 28 de incidente, au fost utilizate reclame online pentru a ajunge la audiențe specifice, penetrând bulele informaționale mai largi. De exemplu, conturile inautentice au rulat reclame pe Facebook pentru a slăbi suportul occidental pentru Ucraina.

Utilizarea Rețelelor de Bot și CIB

- **Rețele de bot și Comportament Inautentic și Coordonat (CIB)**: Acestea sunt folosite frecvent pentru a crește artificial vizibilitatea conținutului. Aproape 73% din canalele detectate (28.000 din 38.000) sunt conturi de tip „disposable” (de unică folosință), care sunt adesea active doar pentru o singură campanie. Acest

caracter efemer îngreunează identificarea originilor, dar aceste rețele rămân un component esențial al infrastructurii FIMI, amplificând conținutul în timp ce evită detecția susținută.

Impersonarea

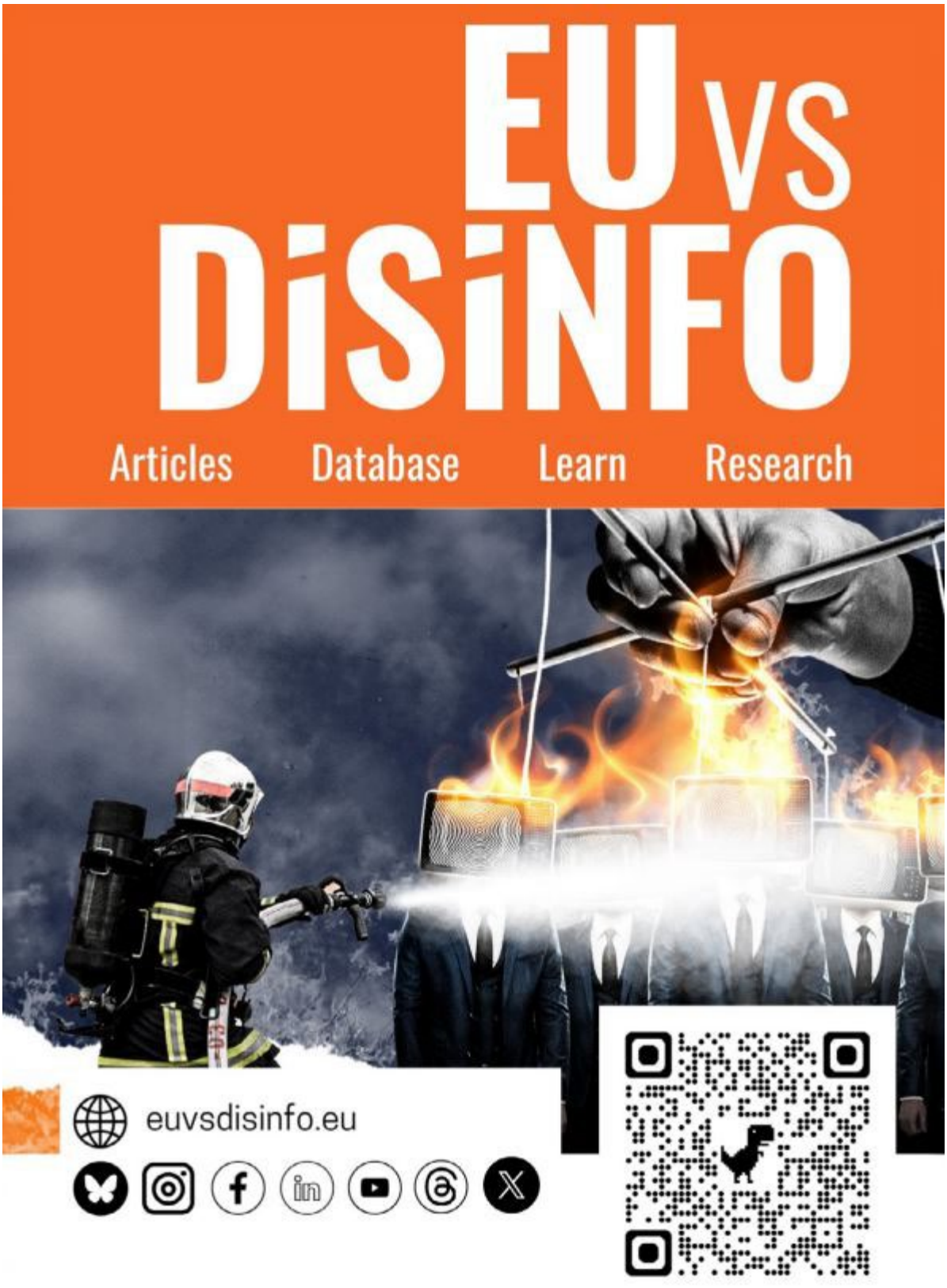
- **Impersonarea entităților și indivizilor**: O tehnică comună în FIMI este impersonarea, fie prin crearea de site-uri de știri inautentice care seamănă cu outleturi media legitime (124 de incidente), fie prin impersonarea directă a entităților stabilite, cum ar fi organizațiile de știri (127 de cazuri). Acești actori exploatează legitimitatea entității impersonate, subminând în același timp încrederea publicului în sursele oficiale.
- **Impersonarea personalităților publice**: S-au investigat 13 cazuri de impersonare a personalităților politice sau celebrităților, cu scopul de a distribui conținut defăimător sau de a folosi popularitatea lor pentru amplificarea conținutului manipulativ.

Rolul Inteligenței Artificiale (AI)

- **Utilizarea AI**: Tehnologia AI devine din ce în ce mai importantă în evoluția FIMI. Înregistrările recente arată că utilizarea AI în incidentele FIMI a devenit mai frecventă, îmbunătățind automatizarea anumitor activități, cum ar fi crearea de conținut. Anul trecut, au fost raportate aproximativ 41 de cazuri în care AI a fost utilizată pentru manipularea informației.
    - **Conținut inautentic**: Modalitățile principale au fost crearea de conținut inautentic (de exemplu, audios și videoclipuri deepfake) și diseminarea automată pe scară largă prin rețele de bot. Textul generat de AI este, de asemenea, probabil utilizat, dar detectarea sa rămâne o provocare.

Într-un peisaj geopolitic din ce în ce mai ostil, utilizarea Interferenței și Manipulării Străine a Informațiilor (FIMI) a devenit o componentă esențială a activităților hibride. Actorii FIMI exploatează sistematic crizele globale și evenimentele internaționale pentru a desfășura operațiuni de manipulare a opiniei publice, considerând aceste tactici ca fiind o opțiune relativ ieftină pentru a-și influența obiectivele geopolitice.

Analiza operațiunilor FIMI prezentată în raport subliniază faptul că aceste activități nu sunt instrumente sporadice de influență, ci reprezintă un instrument strategic integrat în politica externă a actorilor amenințării. FIMI este folosit ca un mecanism structurat care se aliniază cu abordările mai largi ale politicilor externe, având un impact semnificativ asupra percepțiilor publice și asupra climatului geopolitic



Sursă:3rd EEAS Report on Foreign Information Manipulation and Interference

Threats

Raportul este disponibil în format complet aici: https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf

Link-uri utile pentru aprofundarea subiectului

https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en

https://euvsdisinfo.eu/behind-the-curtain-a-novel-analytical-approach-to-fimi-exposure/?__cf_chl_tk=iQ_AdXl3hbXs_byPaYEXQB1znBAY90TT5YW9ZRxfKAc-1742470539-1.0.1.1-elAtL2qJ1NDW23syEIvSJg_UpSefby6fBVe9slhcFAo