Rețelele rusești și chinezești de dezinformare

de Dorin LUCA

Serviciul European de Acțiune Externă (SEAE) din cadrul Comisiei Europene a dat publicității un nou raport despre eforturile unor actori străini de manipulare a informației și interferență (Foreign Information Manipulation and Interference – FIMI).

Raportul, care analizează perioada dintre 4 noiembrie 2023 și 4 noiembrie 2024, dezvăluie un ecosistem sofisticat și în continuă evoluție al campaniilor de dezinformare sponsorizate de state, orchestrate în principal de Rusia și China, care vizează Uniunea Europeană (UE) și partenerii săi.

Constatările SEAE arată că interferențele și campaniile de dezinformare nu sunt activități sporadice sau izolate, ci fac parte din strategii vaste, în conformitate cu planurile expansioniste și ambițiile geopolitice ale Rusiei și Chinei. Operațiunile acestora exploatează crize globale, alegeri și mișcări sociale pentru a manipula opinia publică, a alimenta polarizarea și a eroda încrederea în instituțiile democratice.

De exemplu, în cele 12 luni analizate, SEAE a documentat 505 incidente care au folosit aproximativ 38.000 de canale digitale, pe 25 de platforme distincte, cu 68.000 de observații (conținut media), ilustrând amploarea acestei amenințări. Campaniile identificate au vizat 90 de țări, în special Ucraina, Franța, Germania, Moldova și Africa Sub-Sahariană.

Ucraina este ținta principală a acestor amenințări; aproape jumătate din campanii au avut țara vecină în centrul atenției. Infrastructura rusească de dezinformare se concentrează în primul rând asupra ucrainenilor, pentru a slăbi rezistența acestora în fața invaziei ruse.

În al doilea rând, vizează publicul din țările aliate și partenere – SUA, NATO, G7, UE –, în special în Polonia și Germania, pentru a scădea sprijinul pentru Ucraina. Scopul principal este să modeleze percepțiile oamenilor conform narativelor rusești despre războiul început de Putin împotriva Ucrainei.

După Ucraina, Franța și Germania au fost principalele ținte ale dezinformării rusești, cu atacuri în preajma Jocurilor Olimpice și Paralimpice și alegerile legislative (Franța), precum și în jurul unor proteste ale fermierilor, vizite oficiale și evenimente politice locale (Germania).

Descoperiri ale raportului în perioada 3 noiembrie 2023 – 3 noiembrie 2024.

În afara UE, Republica Moldova a fost una din cele mai atacate țări, cu 45 de incidente FIMI. În afară de referendumul pentru aderarea la Uniunea Europeană și alegerile prezidențiale din octombrie-noiembrie 2024, Republica Moldova și președinta Maia Sandu au fost ținte ale unor atacuri repetate din partea Rusiei, care a exploatat subiectul Transnistria și a înaintat acuzații nefondate despre implicarea Chișinăului în războiul din Ucraina.

O altă zonă geografică în vizorul campaniilor rusești de dezinformare și interferență este Africa, unde Rusia încearcă să-și legitimizeze prezența militară și economică tot mai mare.

Autorii raportului notează că eforturile Rusiei sunt caracterizate de un grad înalt de adaptabilitate. Abordările sunt modelate conform specificului local. Unele regiuni (din estul Europei), unde se vorbește și rusa, sunt atacate cu conținut atât în limba națională, cât și în limba rusă.

Având în vedere că peste jumătate din populația adultă a lumii a participat la alegeri în 2024, procesul democratic a fost una din țintele principale ale campaniilor de interferență.

În cazul alegerilor europarlamentare din 2024, SEAE a identificat 42 de campanii rusești, care au escaladat în săptămânile dinaintea votului, cu un maxim de activitate în perioada 6-9 iunie (zilele alegerilor europene).

Operațiunile erau desfășurate după un plan familiar: organizarea unei infrastructuri, cu mult timp în avans; atacuri asupra procesului democratic, interferențe și atacuri cibernetice, cu un vârf de activitate înainte de începerea votului; și un efort imediat după închiderea urnelor pentru a submina încrederea în rezultate.

Tehnici și tactici

În incidentele analizate de Serviciul European de Acțiune Externă, în care au fost folosite aproximativ 38.000 de mii de canale pe 25 de platforme digitale, 88% din activitatea malițioasă a avut loc pe X/Twitter.

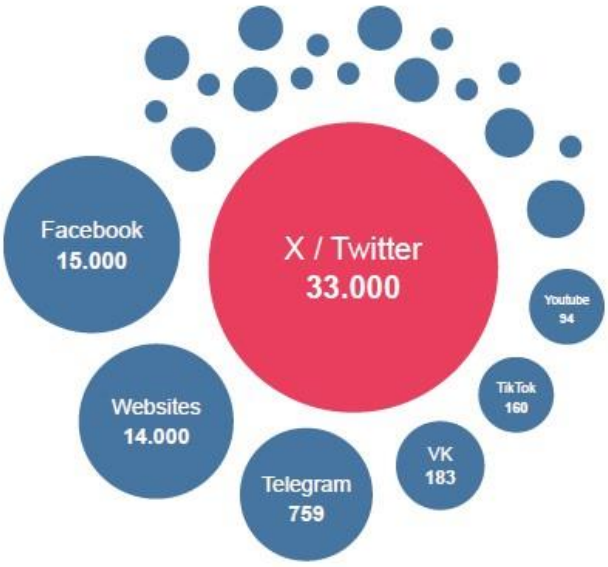
Acest lucru este explicat de prezența pe această platformă a comportamentului coordonat inautentic și de ușurința cu care pot fi create conturi false. Majoritatea atacurilor nu survin, totuși, pe o singură platformă, ci sunt coordonate în mai multe părți.

*O tehnică obișnuită este achiziționarea de **rețele de conturi false**, activate pentru a spori vizibilitatea conținutului fals sau propagandistic. Aceste rețele – care de cele mai multe ori supraviețuiesc puțin timp și sunt de unică folosință – ridică provocări de identificare și atribuire, chiar dacă sunt esențiale în amplificarea conținutul fals.*

*De asemenea, sunt create **site-uri de știri care imită surse media locale legitime** (124 de incidente înregistrate) sau care copiază identitatea vizuală a unor entități consacrate, precum instituții de presă sau organizații (127 de cazuri).*

Astfel, pe de o parte, este exploatată încrederea pe care o au oamenii în surse credibile de știri, iar pe de altă parte subminează această încredere atunci când conținutul este vădit fals. Rusia înțelege că presa independentă este esențială în societățile democratice pentru fluxul liber de informații și încearcă să exploateze acest rol.

De asemenea, SEAE a investigat 13 cazuri de furt de identitate a unor personalități politice sau celebrități, care au vizat fie distribuirea de conținut defăimător la adresa persoanelor vizate, fie folosirea popularității acestora ca mijloc de amplificare a conținutului manipulator.



Platforme folosite în campanii de dezinformare și interferențe.

*O altă tehnică este adesea **adaptarea mesajelor pentru publicul local**. Cel puțin 349 de incidente au utilizat tehnici de adaptare a conținutului, ajustând mesajele în funcție de publicul țintă. Asta presupune modificarea narațiunilor prin utilizarea unor referințe locale pentru a spori credibilitatea și impactul.*

***Inteligența artificială (AI) a devenit un instrument important** în campaniile de dezinformare, deși impactul nu poate fi măsurat cu acuratețe. AI permite actorilor străini să-și automatizeze activitățile, de la crearea conținutului (deepfake audio și video) la distribuirea acestuia (prin rețele de boți), economisind timp și resurse.*

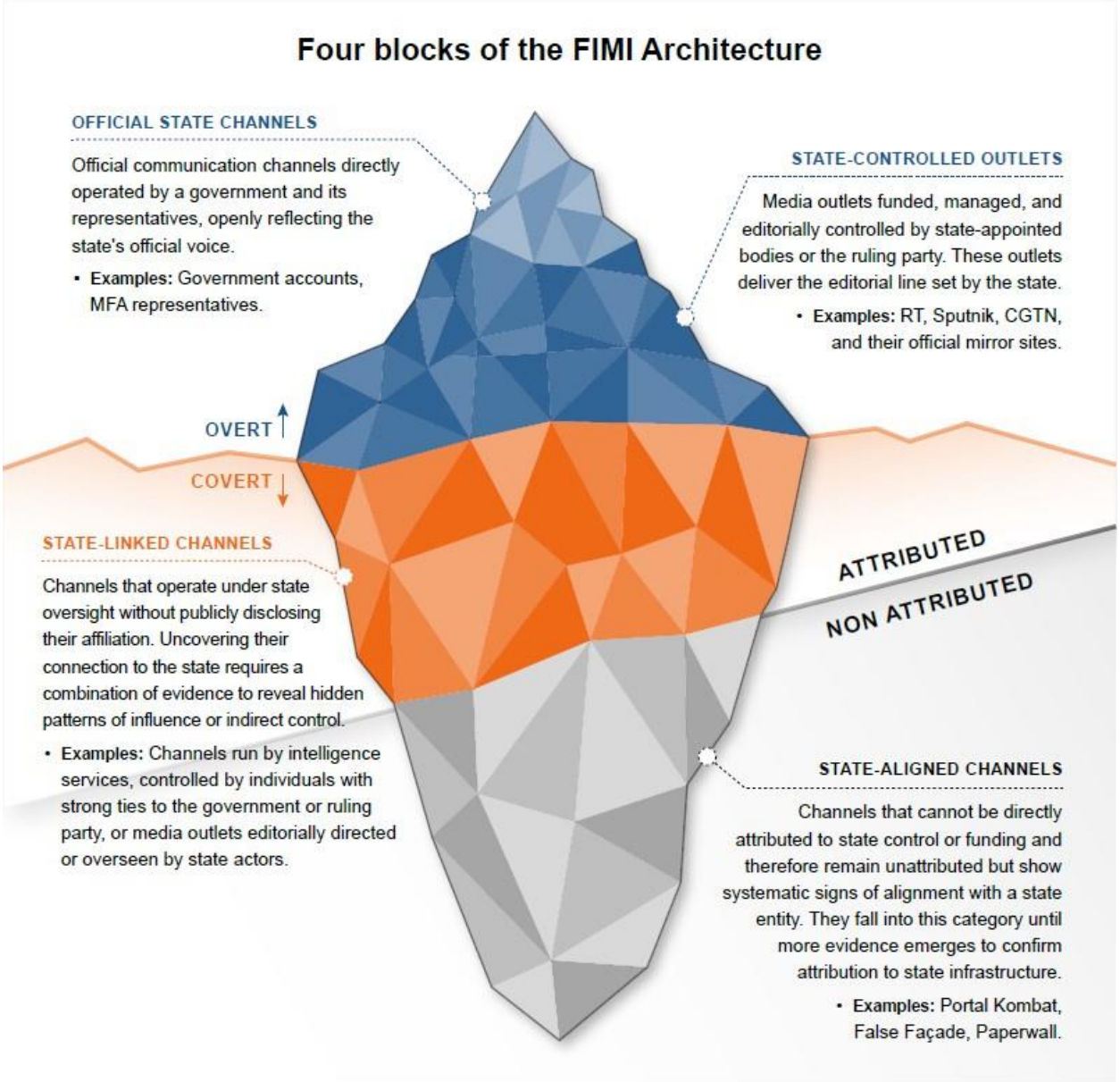
Raportul precizează că în operațiunile de dezinformare este probabilă și folosirea textelor generate de inteligența artificială, însă identificarea acestora este o provocare.

Arhitectura de dezinformare

Elementul central al acestui proaspăt raport este introducerea unei matrice de expunere a acestor interferențe (FIMI), un instrument analitic conceput pentru a categorisi și conecta mai ușor între ele canalele digitale atribuite și neatribuite implicate în operațiuni FIMI.

Prin cartografierea acestor rețele, UE își propune să îmbunătățească procesul de detectare a amenințărilor, să consolideze reziliența și să impună costuri actorilor rău intenționați.

Deși instrumentul este util în special pentru analiști și specialiști din domeniu, pentru publicul larg este interesant datorită faptului că prezintă cum exact sunt organizate campaniile de dezinformare rusești și chinezești.



Arhitectura de dezinformare. În vârful aisbergului se afla canalele oficiale și presa controlata de stat, care acționează la vedere, iar partea nevazută este alcătuită din canalele asociate sau aliniate statului, cu activitatea în umbra.

Matricea permite analiștilor să clasifice sursele în patru categorii:

***Canale oficiale de stat** – canalele de comunicare guvernamentală, precum ministerul de externe, ambasadele, purtătorii de cuvânt.*

***Presa controlată de stat** – organizații media deținute, finanțate și controlate editorial de guvern. Printre exemple se numără RT, Sputnik (Rusia) sau CGTN (China).*

***Canale asociate statului** – entități controlate sau influențate în mod ascuns de către stat, mai greu de identificat, dar nu imposibil, prin tranzacții financiare sau infrastructură.*

Acestea răspândesc mesajele în așa fel încât interacțiunea să pară organică și autentică și sunt active în diverse limbi.

***Canale aliniate statului** – surse aparent independente, dar care susțin sistematic narațiunile guvernamentale. Ele pot fi canale de YouTube sau rețele pe platforme sociale. Legătura cu actorii statali nu poate fi stabilită, însă comportamentul este clar, distribuind conținut util acestor actori chiar și atunci când comunicarea oficială pe un anumit subiect este restricționată.*

Dacă primele două categorii de surse sunt la vedere, ca un vârf la aisbergului, acționând deschis, celelalte două sunt aproape invizibile, acționând pe ascuns, sub acoperire, pentru a promova dezinformarea și propaganda.

Rusia și China – modele diferite de influență

Atât Rusia, cât și China se angajează în campanii de dezinformare și interferențe, însă cele două acționează diferit.

Potrivit raportului, Rusia utilizează un model de influență agresiv și descentralizat. Acesta se bazează pe utilizarea unui volum mare de conținut manipulator răspândit rapid pe multiple platforme. Campaniile rusești se axează pe dezinformare, atacuri asupra liderilor politici occidentali, propagandă anti-UE și anti-NATO, utilizarea rețelelor de boți și crearea de conținut deepfake.

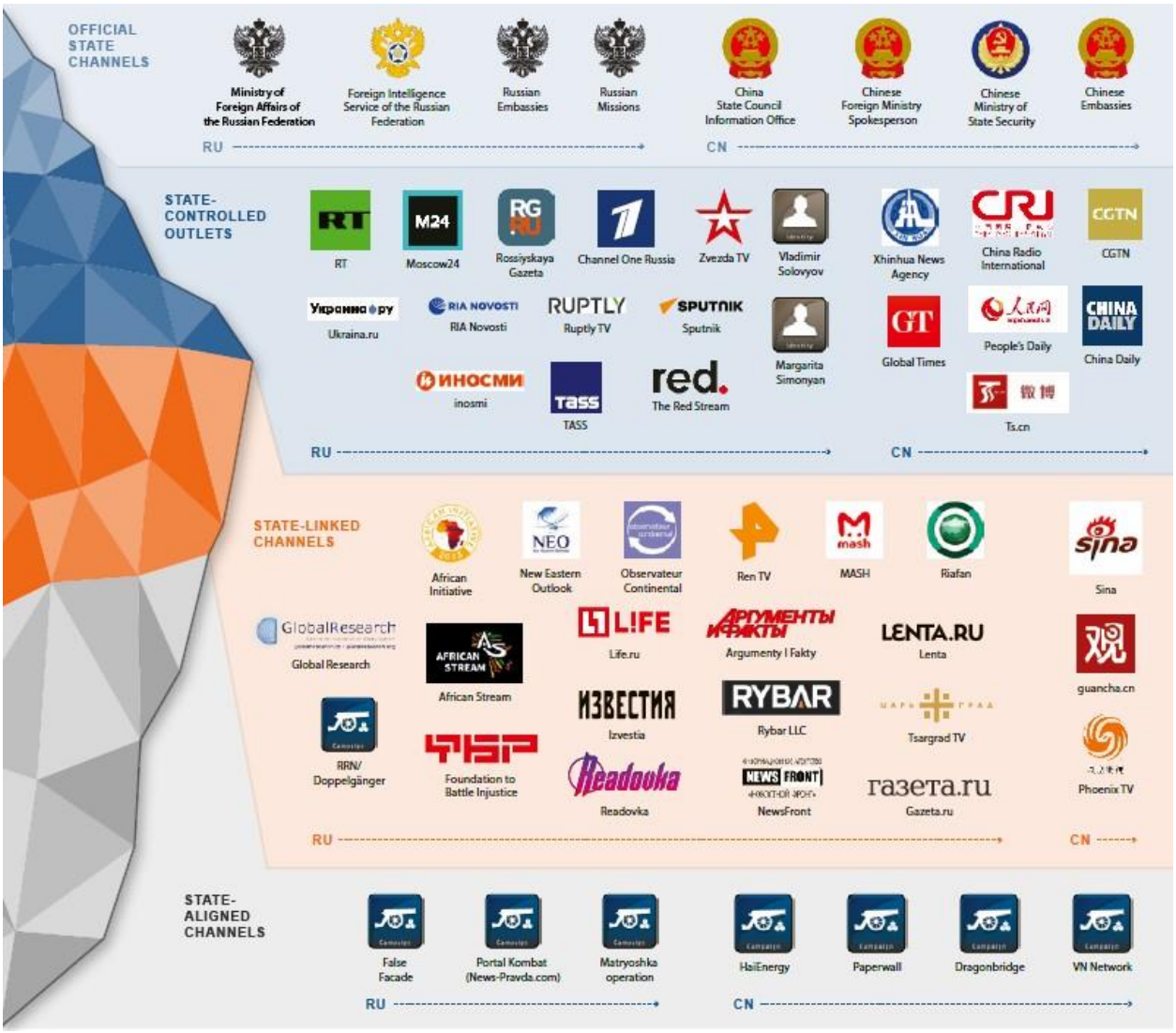
Aceste campanii sunt legitimate de la cele mai înalte niveluri – de fiecare dată când oficiali ruși preiau cuvântul în foruri internaționale, de exemplu – și sunt amplificate de conturile unor oficiali sau diplomați ruși în zonele țintite.

Spre deosebire de Rusia, China are o strategie mai subtilă, centralizată și pe termen lung. În loc de atacuri rapide și haotice, China își construiește influența prin campanii de infiltrare media, cooperare cu publicații străine și utilizarea diplomației economice.

Raportul arată că statul chinez depune eforturi pentru a-și apăra imaginea pe care o are pe scena internațională, în special în ceea ce privește drepturile omului, Marea Chinei de Sud și zone precum Xinjiang, Tibet, Hong Kong și Taiwan. Beijingul se concentrează pe modelarea percepției globale asupra regimului său și pe justificarea politicilor interne.

Totodată, canalele chinezești profită de conflictele internaționale (războiul de agresiune al Rusiei împotriva Ucrainei, conflictul din Gaza) pentru a proiecta un rol pozitiv al Chinei pe scena globală, adesea în contrapondere cu „Occidentul”, pe care îl prezintă drept ipocrit și ineficient în comparație cu modelul chinez de a face lucrurile.

Dacă Rusia pare să vizeze destabilizarea imediată a democrațiilor, China pare să încerce rescrierea treptată a unor narațiuni care să-i fie benefice.



Entități din arhitectura de dezinformare. În dreapta arhitectura de dezinformare rusească, în stânga cea chinezească.

Raportul notează că Rusia și China nu se coordonează decât ad-hoc, în mod oportunist, atunci când au interese comune. De exemplu, în luna care a marcat 1.000 de zile de la invazia pe scară largă a Ucrainei de către Rusia, narațiunile sino-ruse s-au aliniat semnificativ, ambele ecosisteme informaționale distribuind mesaje ostile care dădeau vina pe NATO pentru escaladarea conflictului.

În afara evenimentelor speciale, canalele de presă de stat din Rusia și China (cum ar fi RIA Novosti, RT, Sputnik, CGTN și Global Times) preiau și distribuie reciproc materiale și narațiuni, într-un efort de a oferi legitimitate mesajelor anti-occidentale.

Această convergență este evidentă în narațiunile care vizează instituțiile occidentale și procesele democratice, adesea prezentând UE, SUA și NATO ca fiind slabe, instabile sau implicate în neocolonialism și provocări regionale. De asemenea, mass-media rusă și chineză prezintă proprii conducători ca fiind puternici și sprijiniți la nivel global.

Raportul complet poate fi citit pe site-ul SEAE.