BULETINUL
UNIVERSITĂȚII NAȚIONALE DE APĂRARE „CAROL I”

Rețelele de socializare ca infrastructură de dezinformare: tactici, strategii și securitate națională

Social Media as a Disinformation Infrastructure: Tactics, Strategies, and National Security

Căpitan Asistent Universitar George-Adrian AIONESEI*
*Academia Forțelor Aeriene „Henri Coandă”, Brașov, România
e-mail: aioneseiadrian11@gmail.com

Abstract

Dezinformarea, în contextul actual, nu mai este un fenomen marginal, ci mai degrabă un instrument central al războiului hibrid și cognitiv, folosit împotriva coeziunii sociale și a încrederii în instituțiile democratice. Astfel, lucrarea de față analizează rolul rețelelor sociale în subminarea securității naționale, concentrându-se pe tacticile și strategiile de dezinformare utilizate în mediul digital actual. În acest studiu, vom folosi un model de tip secvențial combinat pentru a stabili legături și relații între tacticile (la nivel micro) utilizate în campaniile de dezinformare și strategiile (la nivel macro) folosite pentru a influența societatea și modul în care oamenii gândesc și se comportă.

Disinformation, in the current context, is no longer a marginal phenomenon but rather a central instrument for hybrid and cognitive warfare, used against social cohesion and trust in democratic institutions. Thus, this paper analyzes the role of social media in undermining national security, focusing on disinformation tactics and strategies used in the current digital environment. Through this study, we manage to use a combined sequence model to establish links and relationships between the tactics (micro-level) used in disinformation campaigns and the strategies (macro-level) used in order to affect society and the way people think and behave.

Cuvinte-cheie:
dezinformare; tactici; strategii; rețele sociale; securitate națională; mediul online.

Keywords:
Disinformation; Tactics; Strategies; Social Media; National Security; Online.

Info articol
Primit: 11 aprilie 2026; Evaluat: 30 aprilie 2026; Acceptat: 4 iulie 2026; Disponibil online: 30 iunie 2026

Citare: Aionesei, G. A. 2026. „Rețelele de socializare ca infrastructură de dezinformare: tactici, strategii și securitate națională.” *Buletinul Universității Naționale de Apărare „Carol I”*, 15(2): 7-32. https://doi.org/10.53477/2065-8281-26-11

Introducere

Schimbările din mediul de comunicare au depășit nivelurile tehnologice și au generat o reconfigurare structurală a puterii sociale moderne. Crearea și dezvoltarea rețelelor și platformelor de socializare au modificat fundamental modul în care indivizii, instituțiile și statele comunică, împărtășesc informații și construiesc realități. Așa după cum menționează Manuel Castells, trecerea către o societate a rețelelor a transformat modul în care funcționează comunicarea într-un mediu în care informația devine o monedă strategică (Castells 2009, 38-42).

Odată ce platformele de socializare, precum Facebook (2004), YouTube (2005), Twitter (2006) sau, mai târziu, Telegram, Instagram și TikTok au devenit mai populare, fiecare individ și-a schimbat statutul de la consumator pasiv la agent activ prin crearea și diseminarea informațiilor. Acest proces democratic de comunicare a fost perceput, inițial, ca un vector al libertății și mobilizării civice, manifestat foarte bine în timpul Primăverii Arabe. Cu toate acestea, noua deschidere către libera exprimare a implicat vulnerabilități sistemice, în principal din cauza lipsei filtrelor editoriale, a vitezei de diseminare și a dependenței de logica algoritmică a atenției (Chadwick 2017, 19-22).

Rețelele sociale nu mai pot fi privite doar ca simple spații de interacțiune culturală și socială, ci mai degrabă ca infrastructuri strategice, în care confruntările informaționale și cognitive devin elementele centrale ale conflictelor moderne. Ele permit simultan atât mobilizarea socială, cât și manipularea politică. Așa după cum menționează Benkler, Faris și Roberts (2018, 14-23), arhitectura platformelor digitale favorizează polarizarea emoțională și diseminarea narativelor distorsionate, creând astfel mediul ideal pentru campanii coordonate de dezinformare. După 2014, evenimente precum conflictul din Ucraina, implicațiile electorale din Statele Unite ale Americii sau conspirațiile medicale din timpul pandemiei de COVID-19 au arătat în mod clar că rețelele sociale au devenit o nouă amenințare globală care ar putea afecta grav securitatea națională. Folosind aceste platforme, diferiți actori pot influența percepțiile, pot submina încrederea publicului în instituțiile guvernamentale și pot destabiliza democrația fără niciun fel de intervenții militare. Ca răspuns, organizații precum NATO, Uniunea Europeană sau Consiliul European au recunoscut oficial manipularea informațională și interferențele externe ca forme de amenințări hibride (EEAS 2025b, 7-11; NATO 2022, 3-6).

Prin acest articol, ne propunem să analizăm modul în care instrumentele rețelelor sociale au devenit mijloace esențiale în modelarea conflictelor moderne, punând accent pe folosirea tacticilor și strategiilor dezinformării, care afectează securitatea națională și încrederea populației în instituții. De asemenea, articolul urmărește să identifice mecanismele prin care ecosistemele digitale permit diseminarea și normalizarea narativelor manipulative. Obiectivul general este de a oferi un cadru analitic pentru înțelegerea lanțului cauzal al dezinformării în mediul digital, de la tactici de dezinformare, la efecte cognitive și, în cele din urmă, la implicații de securitate, precum coeziunea socială, legitimitatea instituțiilor sau relația stat-cetățean.

1. Metodologie

Acest articol utilizează o abordare deductivă și calitativă de sinteză a literaturii de specialitate, combinată cu o abordare de elaborare a unui cadru conceptual. Cadrul analitic nu a fost conceput pentru a realiza o metaanaliză statistică, ci mai degrabă pentru a sintetiza literatura de specialitate de tip peer-review, rapoartele instituționale și documentele de politică ce abordează dezinformarea, războiul hibrid, războiul cognitiv și guvernanța platformelor, publicate, în principal, în perioada 2016-2025. Sinteza a ajutat la dezvoltarea unui model analitic care să explice modul în care tacticile de dezinformare pot fi combinate cu platformele de social media, în vederea obținerii unor rezultate strategice cu implicații asupra securității naționale. Sursele au fost identificate prin căutări sistematice în baze de date academice (Scopus, Web of Science) și în arhive de literatură gri (RAND, EEAS, NATO), utilizând ca termeni de căutare: „tactici de dezinformare", „manipulare prin rețelele sociale", „război cognitiv", „amenințări hibride" și „operațiuni informaționale". Criteriile de includere au impus ca sursele să abordeze fie mecanismele de producere și diseminare a dezinformării, fie efectele acestora la nivel de securitate, asigurând relevanța analitică atât pentru dimensiunea tactică, cât și pentru cea strategică a modelului.

Selecția surselor a constat într-o procedură de codificare tematică și conceptuală. În primul rând, mecanismele de dezinformare au fost identificate și codificate în categorii tactice, printre care se numără fabricarea de conținut, credibilitatea sursei, coordonarea și amplificarea, exploatarea infrastructurii, perturbarea discursului și tacticile de producție bazate pe inteligența artificială. În al doilea rând, obiectivele mai ample ale campaniilor de dezinformare au fost codificate în categorii strategice, printre care se numără discreditarea instituțiilor, polarizarea, crearea confuziei, controlul atenției, normalizarea, exploatarea crizelor și erodarea rezilienței democratice. Fiecare dintre cele două categorii a făcut obiectul unei codificări suplimentare pe baza a trei criterii: recurența în mai multe surse analizate sau campanii documentate, rolul funcțional în cadrul procesului de dezinformare și semnificația strategică în producerea de efecte măsurabile la nivel de securitate.

Cadrul analitic pe două niveluri – care face distincția dintre tacticile de dezinformare (mecanisme operaționale la nivel micro) și strategiile de dezinformare (obiective la nivel macro) – a fost elaborat în mod deductiv, pe baza unor modele teoretice consacrate, printre care se numără modelul dezordinii informaționale (Wardle și Derakhshan 2017, 23-32), teoria posibilităților de acțiune, aplicate platformelor social media (Wu, Wu și Xiao 2025, 1-5) și studiile RAND privind operațiunile strategice de influență (Paul și Matthews 2016, 2-9; Mazarr et al. 2019, 11-27). Logica de clasificare și interdependență, prezentată în Tabelul 1, reprezintă rezultatul sintetizat al acestui proces analitic. Cadrul este mai degrabă conceptual decât empiric, dar pentru a consolida fundamentul empiric al acestuia, articolul prezintă o aplicare a modelului pe trei cazuri legate de campaniile de dezinformare ale Rusiei în războiul împotriva Ucrainei, precum deepfake-ul privind capitularea lui Zelenski, dezinformarea privind masacrul de la Bucha și Operațiunea Overload.

Cele trei cazuri nu sunt menite să servească drept metodă de validare statistică, ci mai degrabă ilustrează concret aplicabilitatea analitică a modelului.

2. Cadrul teoretic – dezinformarea, războiul hibrid și războiul cognitiv

Dacă în secolul al XX-lea statul avea puterea de a disemina informații filtrate și manipulatoare prin intermediul canalelor guvernamentale pentru a controla populația, în prezent fluxul informațional s-a descentralizat complet, devenind interactiv, participativ, condus de algoritmi și orchestrat de actori statali și nonstatali. Această schimbare de paradigmă a dus la o democratizare a comunicării și în același timp, a deschis calea către noi forme de manipulare sistemică.

Dezinformarea, considerată odinioară o componentă secundară a războiului hibrid, a devenit un instrument central al războiului modern. În contextul actual, ea poate fi privită ca cea mai sofisticată formă de îmbinare a tehnologiei cu psihologia și geopolitica. Cu alte cuvinte, ea poate fi definită ca diseminarea deliberată de informații false sau distorsionate, pentru a influența percepțiile, comportamentele și deciziile (Wardle și Derakhshan 2017, 20-21; Baines, O'Shaughnessy și Snow 2019, 56-59). Spre deosebire de misinformare, care reprezintă o eroare neintenționată, dezinformarea implică intenționalitate strategică, planificare și coordonare. În acest articol, ne vom concentra în mod specific asupra dezinformării, deoarece aceasta implică aspectul intențional, care este manipulator și are o finalitate strategică. În terminologia europeană actuală, aceste fenomene fac parte dintr-un concept nou – FIMI (Foreign Information Manipulation and Interference) – Manipularea și interferența informațiilor străine, așa cum este definit de Serviciul European de Acțiune Externă, concept care constă într-un set de acțiuni coordonate, menite să altereze informațiile și să submineze activitățile democratice (EEAS 2025a, 4-8).

Prin însăși natura sa, dezinformarea acționează simultan pe trei dimensiuni complementare: comunicare, psihologie și instituții. În ceea ce privește prima dimensiune, dezinformarea este utilizată pentru a denatura în mod intenționat cadrul narativ, pentru a folosi conținut real în contexte false sau pentru a crea și a difuza mesaje persuasive cu scopul de a viza emoțiile. A doua dimensiune se bazează pe prejudecăți cognitive, precum prejudecata de confirmare sau gândirea motivațională, exploatând predispoziția naturală a individului de a accepta informații care îi confirmă identitatea și valorile personale (Lewandowsky, Ecker și Cook 2017, 353-369). În ceea ce privește dimensiunea instituțională, rolul principal al dezinformării este de a diminua încrederea în autorități, în mass-media și în capacitatea instituțiilor de a face distincția dintre ceea ce este adevărat și ceea ce este fals.
Când ne gândim la dimensiunea instituțională, menționată mai sus, ne gândim și la securitatea instituțională. Însă, dacă extindem această perspectivă, putem face referire la securitatea națională. Acest concept al securității naționale nu mai poate fi redus doar la acțiuni teritoriale și militare, întreprinse pentru a proteja infrastructurile fizice critice în mod tradițional. Literatura recentă de specialitate

arată că securitatea trebuie înțeleasă și prin prisma rezilienței informaționale și capacității instituțiilor de a menține încrederea publică a populației, de a adapta mecanismele de diseminare a informațiilor la amenințările actuale și, de asemenea, de a ajuta societatea să răspundă în mod coerent la distorsiunile informaționale (Dragomir, Ruas-Araujo și Horowitz 2024, 1-10; Uusikylä et al. 2024, 1-18). Din această perspectivă, vulnerabilitatea unui stat nu provine doar din constrângeri externe directe, ci și din slăbirea funcțiilor interne care pot afecta coordonarea socială, legitimitatea instituțiilor sau procesele democratice.

Această abordare multidimensională nu începe și nu se încheie neapărat cu aceste trei dimensiuni, ci explică mai degrabă de ce dezinformarea este un element atât de esențial în cadrul războiului hibrid. Conceptul de război hibrid descrie modul în care actorii statali și nonstatali folosesc o combinație de mijloace convenționale și neconvenționale (militare, cibernetice, economice, informaționale, diplomatice) pentru a-și atinge obiectivele politice, fără a ajunge la un conflict armat deschis. În acest spectru, dezinformarea este elementul cu o mare capacitate de a acționa la nivel psihologic și cognitiv, deoarece nu afectează infrastructurile fizice, ci preia controlul asupra percepției publice.

După anexarea Crimeii și campaniile pro Kremlin care au vizat spațiul informațional european, a devenit evident că războiul hibrid se bazează pe o puternică componentă cognitivă. Prin dezinformare, actorii nu urmăresc doar să convingă, ci și să creeze confuzie în rândul oamenilor. Inundând spațiul public cu versiuni multiple și contradictorii ale „adevărului", care, de cele mai multe ori, nu pot fi verificate suficient de repede, încrederea în instituțiile publice și în sursele oficiale de informare începe să scadă, determinând în cele din urmă cetățenii să perceapă realitatea ca pe o construcție instabilă. Pomerantsev (2019, 123, 164) se referă la această strategie ca la „era postadevăr", în care manipularea și controlul conținutului nu se bazează pe minciuni clare, ci pe relativitatea constantă a adevărului.

Această evoluție recentă a gândirii strategice privind influențarea minții oamenilor a fost conceptualizată sub denumirea de „război cognitiv", definit ca fiind cel mai sofisticat tip de conflict modern, în care mintea umană devine domeniul operațional. În literatura strategică, războiul cognitiv descrie ansamblul acțiunilor care vizează influențarea proceselor cognitive, precum percepția, atenția, emoțiile și gândirea rațională, factori care pot fi manipulați pentru a atinge obiective politice, fără contact fizic (Bernal et al. 2020, 9-11). Analiza RAND arată că această abordare este o extensie a operațiunilor de influențare (informație/influență), trecând de la persuasiune la influențarea procesului decizional al țintei, incluzând supraîncărcarea informațională, ambiguitatea strategică sau exploatarea prejudecăților (Paul și Matthews 2016, 2-9; Mazarr et al. 2019, 11-27). Prin urmare, obiectivul principal al războiului cognitiv este de a determina oamenii să acționeze voluntar împotriva voinței lor. Aici, prinde contur controlul reflexiv, ca mecanism prin care un actor furnizează informații filtrate și aparent neutre, dar concepute în așa fel încât să manipuleze adversarul pentru a lua decizii benefice pentru agresor

(de Goeij 2023, 97-108). Această strategie este de cele mai multe ori amplificată de algoritmi, de microțintire și de rețele de influență.

Dacă domeniul cibernetic se referă la infrastructurile tehnologice, domeniul cognitiv vizează infrastructurile mentale (percepții și comportamente). Un rol principal în această ecuație îl joacă rețelele sociale, datorită design-ului lor tehnologic, algoritmilor și conținutului manipulator (Vosoughi, Roy și Aral 2018, 1146-1153). Spre deosebire de propaganda tradițională, care depindea de controlul centralizat al mass-mediei, diseminarea digitală actuală permite un control dispersat, bazat pe participarea voluntară a utilizatorilor. Uniunea Europeană a încercat să răspundă acestor provocări prin adoptarea Legii privind serviciile digitale (Digital Service Act), menită să sporească transparența cu privire la platformele de socializare și responsabilitatea fiecărui utilizator. Cu toate acestea, există o asimetrie structurală între eforturile necesare pentru verificarea acurateței informațiilor și ușurința cu care se răspândesc informațiile false. Adevărul necesită timp, expertiză și validare, în timp ce falsul are nevoie doar de canale și rețele prin care să poată circula liber și instantaneu. Această asimetrie reprezintă principalul avantaj strategic pentru actorii moderni care folosesc dezinformarea ca armă.

Dacă luăm în considerare fluxul de (dez)informare în cadrul rețelelor sociale în societatea actuală, așa după cum s-a menționat mai sus, putem observa un proces de amplificare secvențială prin care dezinformarea evoluează de la tactici, la nivelul platformelor digitale, la efecte strategice asupra securității. Pornind de la oportunitățile oferite de platformele de socializare, precum recomandările algoritmice, propagarea în masă a informațiilor sau vizibilitatea obținută cu efort minim, actorii dispun de condițiile structurale necesare pentru a aplica și a modela manipularea. Folosind acest mediu, ei pot desfășura tactici de dezinformare, pentru a maximiza diseminarea și influența. Aceste tactici, combinate secvențial sau simultan, sunt capabile să genereze efecte cognitive la nivel individual sau la nivelul grupurilor mici, implicând confuzie, percepție eronată sau activare emoțională, care, ulterior, pot fi traduse în răspunsuri comportamentale, determinând oamenii să distribuie conținutul, să dea vina pe autorități sau pe instituții ori să-și manifeste indignarea față de guverne. Prin utilizarea repetiției și a diseminării algoritmice prin rețele, aceste acțiuni formează bucle de amplificare socială care transformă interacțiunile individuale în unele colective. În timp, aceste procese permit consolidarea strategiilor de dezinformare, înțelese ca obiective la nivel macro, inclusiv polarizarea sau discreditarea instituțiilor. În acest sens, strategiile nu se dezvoltă de la sine, ci sunt implementate prin utilizarea repetată și coordonată a mecanismelor tactice, care, în timp, sunt capabile să slăbească coeziunea socială, să reducă încrederea în instituții și să afecteze securitatea națională.

Deși această secvență surprinde imaginea de ansamblu a evoluției de la dinamica platformelor la implicațiile asupra securității naționale, lucrarea de față se concentrează în special asupra tacticilor și strategiilor de dezinformare, precum și asupra relațiilor dintre acestea. Pentru a analiza sistematic aceste dinamici, vom

aborda un model analitic pe două niveluri care face distincția dintre tacticile și strategiile folosite în diseminarea dezinformării. **Tacticile** se referă la mecanismele de nivel micro, prin care dezinformarea operează în mediile de socializare, incluzând practici, precum ingineria narativelor, comportamentul neautentic coordonat (CNC), amplificarea automatizată sau exploatarea algoritmică pentru a crește vizibilitatea și angajamentul utilizatorilor (Bradshaw și Howard 2018, 11-15; Metzler și Garcia 2024, 735-748). **Strategiile**, pe de altă parte, se referă la obiectivele de nivel macro pe care aceste mecanisme sunt menite să le promoveze, inclusiv discreditarea, polarizarea sau descurajarea prin confuzie. Deși nu există un cadru teoretic de sine stătător care să surprindă evoluția dezinformării de la tactici la strategii, cu implicații asupra securității naționale, există mai multe modele care susțin diferite faze individuale. Cadrul dezordinii informaționale (Wardle și Derakhshan 2017, 23-32) conceptualizează dezinformarea ca un proces care implică agenți, mesaje și interpreți, în timp ce modelele bazate pe posibilitățile de acțiune, aplicate platformelor social media (Wu, Wu și Xiao 2025, 1-5) arată cum caracteristicile platformelor influențează răspunsurile cognitive, afective și comportamentale. De asemenea, studiile privind comunicarea strategică, amenințările hibride și războiul cognitiv explică modul în care manipularea susținută poate produce efecte politice și de securitate (Dov Bachmann, Putter și Duczynski 2023, 858-867). Luând în considerare aceste modele, prezentul articol propune un model integrativ, ilustrat mai jos în Figura 1.

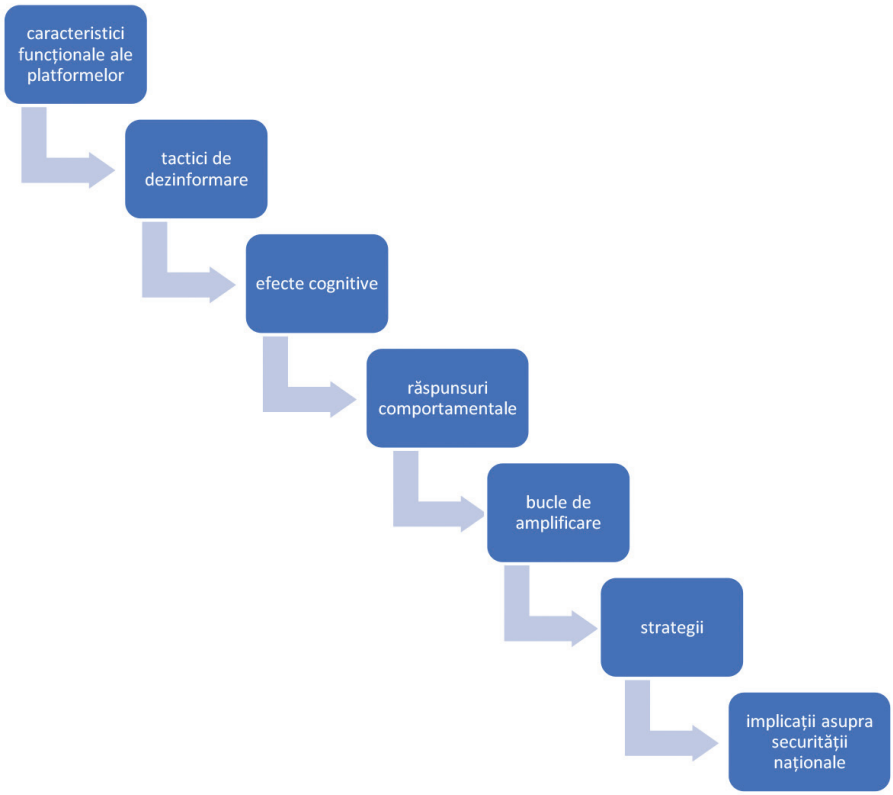

Figura 1 Modul în care dezinformarea evoluează de la platformele de socializare la amenințări la adresa securității naționale
Sursa: interpretarea autorului.

3. **Tactici și mecanisme de dezinformare pe rețelele de socializare**

Așa după cum am menționat anterior, dezinformarea nu este un fenomen întâmplător, ci mai degrabă un proces deliberat și structurat, utilizat ca pilon principal în strategiile de război hibrid și cognitiv. Succesul său provine din combinarea unor tehnologii, precum platformele de socializare cu algoritmii acestora, manipularea psihologică și amplificarea coordonată a mesajelor. Pentru a înțelege modul în care funcționează dezinformarea la nivel micro, o vom analiza prin prisma principalelor categorii de tactici. Acestea sunt prezentate sub formă de tehnici izolate, dar pot fi combinate în diferite moduri, de la conținut, la canale de comunicare, surse, mod de diseminare, vizibilitate sau manieră de recepționare de către utilizatori. Studiile pe această temă au sugerat că dezinformarea trebuie analizată din perspectiva procesului care implică interacțiunea dintre conținut, amplificarea rețelei și implicarea utilizatorilor pe platformele de socializare sub diverse forme (Chadwick și Stanyer 2022, 1-17). Pornind de la acest punct și de la alte studii (Bradshaw și Howard 2018, 9-15; Kruijver et al. 2025, 6-20), putem clasifica tacticile în diferite categorii, fiecare dintre acestea corespunzând unei dimensiuni distincte a manipulării.

3.1. Tactici de fabricare și manipulare a conținutului

Această categorie se concentrează asupra conținutului informațional al mesajelor. De la producerea conținutului (text, video, audio) până la forme mai subtile de distorsionare, dezinformarea nu se bazează exclusiv pe informații false, ci pe posibilitatea de a combina fapte reale cu o interpretare manipulatoare, cu narative emoționale sau cu relatări bazate pe teorii ale conspirației, care oferă interpretări simplificate și mai ușor de acceptat privind realitatea (Egelhofer și Lecheler 2019, 97-111).

Conținutul complet fabricat este unul dintre cele mai evidente mecanisme din această categorie, promovând fapte inventate în întregime, sub diferite forme (postări, articole, știri de ultimă oră, zvonuri sau pseudoreportaje). Există și alte tactici subtile, cum ar fi plasarea de imagini sau fapte reale în contexte falsificate, omiterea informațiilor care ar putea schimba interpretarea utilizatorilor sau folosirea ingineriei narative pentru a rearanja și a organiza informațiile legate de un eveniment într-un mod care să îi confere o semnificație diferită, cum ar fi trădarea, corupția, cenzura sau conflictul de tip „noi împotriva lor". În aceste cazuri, manipularea constă mai puțin în inventarea realității și mai mult în distorsionarea condițiilor în care realitatea este interpretată. Alte tactici manipulează credibilitatea și dovezile prin invocarea „experților" din diferite domenii (politicieni, medici, martori inventați), a pseudodocumentelor sau a așa-numitelor scurgeri de informații din partea guvernului, a marilor companii sau a persoanelor influente. Formele mai avansate și moderne includ deepfakes și media sintetică, prin utilizarea IA pentru a imita personalități publice sau a fabrica evenimente (Farid 2025, 1-9), precum și conținutul de tip „steag fals", care este conceput să pară că provine de la un alt actor, grup sau comunitate, evitând astfel măsurile legale care pot fi luate împotriva lor (Ferreira 2022, 1537-1540). Cele două tactici au o importanță strategică, deoarece

implică o creștere a incertitudinii cu privire la autenticitate și atribuire, făcând dificil pentru public să știe exact responsabilul pentru un anumit conținut, acestea fiind strâns legate de următoarea categorie de tactici.
Tacticile de fabricare și manipulare a conținutului au rolul de a distorsiona relația dintre informație, dovezi și interpretare. Eficacitatea lor nu se bazează exclusiv pe producerea de informații false, ci și pe capacitatea lor de a altera contextul, de a manipula credibilitatea și de a intensifica emoțiile, ceea ce le face esențiale pentru strategii precum discreditarea, polarizarea, crearea confuziei sau exploatarea crizelor.

3.2. Tactici privind sursa sau identitatea conținutului
O altă categorie importantă de tactici care manipulează percepția asupra credibilității și autenticității conținutului o constituie cea care vizează sursa sau sursele conținutului. Dincolo de modificarea conținutului, aceste tactici vizează originea percepută a mesajelor, cum ar fi identitățile false sau pseudosursele care le imită pe cele legitime. În mediul rețelelor sociale, utilizatorii se bazează pe elemente precum identitatea unui cont, popularitatea, repetitivitatea sau o aparentă credibilitate, pentru a interacționa cu acesta. Prin urmare, manipularea identității celui care pare să vorbească, a conținutului și a numărului de voci care susțin o narațiune, precum și a gradului de autenticitate al acestora constituie un mecanism de influență extrem de eficient, utilizat de actorii implicați.

Una dintre cele mai comune tactici utilizate în această categorie este folosirea de personaje false sau conturi-marionetă, care sunt identități online false, create pentru a lăuda, a apăra, a susține sau a denigra o persoană, un grup sau o entitate, cu scopul de a influența deciziile populației. Această tactică este folosită pentru a disemina un conținut specific online, în timp ce sursa originală ar putea fi blocată sau restricționată. Ea este eficientă prin simularea utilizatorilor obișnuiți, făcând ca manipularea coordonată să pară o opinie publică spontană. În strânsă legătură cu aceasta, se află boții – conturi automatizate, utilizate pentru a posta și a partaja conținut în mod artificial, conform instrucțiunilor predefinite. Aceștia pot reduce costul diseminării și pot crește viteza și volumul de interacțiune, permițând actorilor să sporească vizibilitatea unei narațiuni selectate (Alkathiri şi Slhoub 2025, 1-7). Dacă boții sunt mecanisme automatizate, trolii sunt, de obicei, conturi operate de cei ce participă la procesul de dezinformare în mod agresiv, ironic sau provocator pentru a promova narațiuni specifice sau pentru a descuraja opoziția (Hameleers 2023, 4-6). O altă formă complexă de manipulare a surselor este reprezentată de comportamentul neautentic coordonat (CNC), o tactică bazată pe rețele de conturi autentice, care sunt duplicate, falsificate și gestionate automat sau manual, coordonate astfel încât să ascundă autorul real și să simuleze comportamente organice (Murero 2023, 3-4). Astroturfingul, apropiat de CNC, implică o activitate organizată care dă impresia unui comportament organic și spontan, în favoarea ori împotriva unei idei sau opinii, pentru a-i conferi un consens popular, dar care nu există. CNC și astroturfingul sunt relevante pentru dezinformare, deoarece nu distorsionează informația, ci mai degrabă falsifică mediul rețelelor sociale în care informația este recepționată, evaluată și utilizată (Hameleers 2023, 4-6).

3.3. Tactici de coordonare și amplificare

Prin utilizarea acestor tipuri de tactici, dezinformarea se extinde dincolo de punctul inițial de apariție. Acestea exploatează modul în care vizibilitatea și repetarea pot crește, dând impresia că anumite conținuturi se răspândesc în mod organic, sunt urgente sau au fost validate social. C. Paul și M. Mathews au descris această logică, subliniind modul în care volumul mare și conținutul repetitiv pot copleși publicul și gândirea rațională a acestuia (Paul și Matthews 2016, 1-10).

Aceste tactici includ amplificarea automatizată, în cadrul căreia boții sporesc vizibilitatea prin postări, distribuiri și reacții, generate artificial; coordonarea postărilor, în care mai multe conturi promovează aceeași narațiune în diverse grupuri pentru a crea un impuls inițial, precum și deturnarea hashtagurilor sau a cuvintelor-cheie, în care actorii introduc narațiuni manipulative în grupuri și medii deja populare, pentru a spori vizibilitatea și credibilitatea (Mustafa, Luczak-Roesch și Johnstone 2025, 48-54).

Alte forme includ inundarea cu comentarii, care copleșește utilizatorii cu o avalanșă de comentarii și răspunsuri, pentru a-i dezorienta, intimida și, în final, pentru a-i face incapabili să decidă și spălarea de influență, în care conținutul este preluat de figuri cunoscute, astfel încât să pară mai organic și mai credibil.

Din punct de vedere social, aceste tactici distorsionează distribuția opiniilor, aducând în prim plan narațiuni manipulate, pentru a părea populare și uzuale. Interacțiunea utilizatorilor cu acest conținut se traduce printr-o vizibilitate mai mare, creând astfel bucle de feedback și, în cele din urmă, modelând percepția, credibilitatea și comportamentul de grup.

3.4. Tactici de exploatare a infrastructurii platformelor

În loc să se concentreze pe convingerea publicului, aceste tactici sunt folosite pentru a manipula algoritmii, sistemele de recomandare și indicatorii de implicare, cu scopul de a spori vizibilitatea și persistența conținutului. Ele contribuie la plasarea strategică a conținutului în cadrul ecosistemelor platformelor, pe baza preferințelor, maximizând astfel expunerea în rândul unor segmente specifice de public (Clemons et al. 2024, 5-11). Prin utilizarea acestor tactici, actorii permit folosirea platformelor de socializare ca factor de amplificare a influenței. Există câteva tactici, cum ar fi optimizarea mesajelor, care ajută sistemele de recomandare ale algoritmilor să ofere utilizatorilor conținut specific intereselor lor; „inundarea căutărilor", în cadrul căreia actorii promovează rezultate, povești sau narațiuni pentru a domina anumite căutări, asociate cu nume, evenimente sau subiecte; și „microtargetingul (microdirecționarea)", care este utilizat de actori pentru a transmite mesaje personalizate către segmente specifice de public, pe baza intereselor, vulnerabilităților, identităților sau modelelor comportamentale ale acestora (Kruijver et al. 2025, 15-16).

Aceste tactici au un impact semnificativ prin manipularea vizibilității și segmentarea publicului. Prin exploatarea algoritmică, aceste tactici fac ca narațiunile selectate să pară mai populare, mai relevante sau mai importante decât sunt în realitate. Expunerea repetată poate spori familiaritatea și credibilitatea percepută, în timp ce mesajele personalizate pot exploata temerile sau vulnerabilitățile preexistente. De asemenea, impactul microțintirii prin expunerea diverselor grupuri la versiuni

diferite ale realității poate duce la o înțelegere și interpretare colectivă eronată a unui eveniment, reprezentând un punct de plecare pentru polarizarea societății.

3.5. Tactici de suprimare și perturbare a discursului

În această categorie de tactici, obiectivul constă în abilitatea de a slăbi capacitatea vocilor opuse să răspundă în mod eficient. Hărțuirea coordonată, intimidarea sau devierea atenției sunt doar câteva dintre tacticile menite să reducă la tăcere criticii și opiniile contrare, să discrediteze experții sau să îndepărteze atenția de la subiectele importante. Astfel de practici contribuie la crearea unui mediu în care narativele înșelătoare devin o normalitate și pot circula fără prea multă rezistență.

Hărțuirea, una dintre cele mai frecvente tactici din această categorie, implică atacuri coordonate asupra experților sau persoanelor și organizațiilor care contestă narațiunile de dezinformare. Efectul nu se concentrează doar asupra țintei principale, ci transmite și un semnal celorlalți că respingerea și contestarea narațiunii dominante pot genera sancțiuni sociale, prejudicii de reputație sau stres psihologic. O tactică complementară constă în reducerea la tăcere prin intimidare, care, pe baza aceleiași rațiuni, îi descurajează pe alții să corecteze public afirmațiile înșelătoare, chiar și atunci când dețin cunoștințe relevante. Impactul este că narațiunile manipulate devin mai acceptate, mai populare și mai puțin contestate, în timp ce vocile credibile devin mai puțin vizibile. „Brigada de raportare"(Report brigading) completează aceste practici, la nivel de cont, permițând actorilor să reducă vizibilitatea conturilor adversare sau chiar să suspende utilizatorii care se opun narațiunilor lor (Wardle 2024, 12-17).

Aceste tactici au rolul de a slăbi contradiscursul. Intimidarea descurajează experții și oamenii obișnuiți să intervină, în timp ce atacurile repetate pot diminua încrederea în cei care furnizează informații corecte. În ceea ce privește procesul de dezinformare, aceste tactici îl fac mai greu de combătut, nu neapărat din cauza puterii de convingere, ci pentru că rezistența la dezinformare devine mai costisitoare pentru utilizatori.

3.6. Tactici bazate pe inteligența artificială

O categorie distinctă de tactici în domeniul dezinformării o reprezintă utilizarea inteligenței artificiale (IA) și a automatizării avansate ca o extensie a metodelor tradiționale de influențare a populației. Dezvoltarea tehnologică permite IA să susțină fenomenul dezinformării prin creșterea vitezei de producție a conținutului, a volumului acestuia, a realismului și capacității de personalizare a mesajelor digitale. Literatura recentă de specialitate arată că IA generativă nu schimbă neapărat obiectivele dezinformării, dar contribuie semnificativ la reducerea costurilor, la sporirea ritmului și la capacitatea de extindere (Romanishyn, Malytska și Goncharuk 2025, 3-5; Park și Nan 2024, 1502-1504).

Una dintre cele mai importante tactici bazate pe IA este generarea de conținut sintetic și de personaje fictive. Aceasta include texte, imagini, videoclipuri, fișiere audio sau

identități online aparent autentice, create sau modificate de IA. Actorii pot genera volume mari de conținut și pot crea personaje credibile pentru a difuza un material specific. Acest lucru poate contribui la susținerea ori denigrarea oricăror agende sau contexte în favoarea diferiților actori. În mod complementar, microțintirea asistată de IA poate ajuta actorii să adapteze narațiunile, tonul, cadrul emoțional sau afirmațiile la segmente specifice de public pentru a face dezinformarea mai convingătoare prin alinierea mesajelor la identitățile, temerile sau orientările ideologice ale utilizatorilor.

Aceste categorii prezintă diferite tactici care ar putea fi considerate inovatoare și eficiente, dar, în realitate, ele nu pot funcționa izolat. Pentru ca o campanie de dezinformare să-și atingă obiectivele, aceste tactici trebuie combinate astfel încât impactul lor să rezulte din coordonare, repetare și adaptare la dinamica specifică platformei. Prin urmare, importanța acestor tactici rezidă în capacitatea lor de a fi combinate, extinse și menținute în timp, generând rezultate care depășesc efectele lor individuale. De asemenea, mecanismele identificate mai sus nu se bazează exclusiv pe falsitate absolută, ci funcționează mai degrabă prin distorsionare, recontextualizare și manipulare, indicând necesitatea de a ne concentra pe multiple dimensiuni (încadrare, repetare, algoritmi), nu doar pe valoarea adevărat-fals. Înțelegerea acestor mecanisme este esențială atât pentru a analiza modul în care dezinformarea funcționează la nivel micro, cât și pentru a explica modul în care acestea contribuie la obiective specifice mai largi, ca strategiile care derivă din ele.

4. Strategii de dezinformare în ecosistemul social media

Trecând de la nivelul micro la o perspectivă mai largă, putem utiliza, orienta și coordona aceste intervenții tactice pentru a crea strategii de dezinformare, cu scopul de a influența percepțiile, de a perturba coeziunea socială și de a modifica dinamica politică și instituțională (Chadwick și Stanyer 2022, 10-14). Având în vedere aceste tipuri de obiective, putem considera strategiile nu ca obiective izolate, ci mai degrabă ca modele de acțiune susținute, obținute din implicarea coordonată a tacticilor în timp, pe diferite platforme sau în fața diverselor audiențe. În continuare, vom discuta principalele categorii de strategii utilizate, în prezent, la susținerea dezinformării în social media. La fel ca în cazul tacticilor, nu este vorba de o listă exhaustivă de strategii, ci de cele mai utilizate strategii și care au un impact major asupra societății în prezent.

4.1. Discreditarea instituțiilor și autorităților

Această categorie vizează subminarea încrederii în instituții guvernamentale, în organizații media, în experți științifici și în procesul democratic, reprezentând astfel o amenințare majoră la adresa unor piloni fundamentali ai societății. În prezent, încrederea este înlocuită de informații false, mesaje repetitive și volume uriașe de informații, care generează scepticism și îndoieli în ceea ce privește identificarea conținutului credibil. Cercetările arată că expunerea persistentă la dezinformare prin utilizarea tacticilor de mai sus reduce semnificativ încrederea în instituții și în procesele democratice (alegerile prezidențiale din SUA din 2016),

în comunicările privind sănătatea publică (COVID-19) și guvernarea, în general (Surjatmodjo et al. 2024, 1-12).

Mecanismele cauzale ale discreditării acționează prin repetiție, încadrare emoțională și subminarea credibilității autorităților epistemice. Narațiunile care prezintă guvernele ca fiind incompetente, corupte sau care nu acționează în interesul cetățenilor slăbesc dorința oamenilor de a accepta comunicatele oficiale, discreditând astfel instituțiile respective (Lukavska et al. 2025, 1-11), în timp ce atacurile asupra mass-mediei tradiționale prezintă jurnalismul ca fiind părtinitor, manipulat sau controlat. În același context, se încadrează atacurile asupra expertizei științifice, care pun la îndoială cunoștințele profesionale în domenii precum sănătatea publică sau securitatea, înlocuind conținutul verificat cu pseudoștiință (Lindberg și Denniss 2025, 1-7). Legitimitatea electorală poate fi, de asemenea, ținta promovării și susținerii ideii că alegerile sunt frauduloase, nedrepte sau controlate structural, diminuând încrederea în procedurile democratice.
Ca urmare, această categorie de strategii implică suspiciune, cinism și neîncredere față de sursele care ar trebui să constituie un ghid și un sprijin pentru bunăstarea socială. Dacă cetățenii nu mai au încredere în instituțiile legitime, în experți sau în procedurile electorale, dezacordurile devin mai greu de rezolvat prin canale instituționale. Impactul acestor strategii nu se reflectă doar într-o credibilitate scăzută a instituțiilor, ci și într-o destabilizare mai amplă a relației dintre cetățeni, cunoaștere și autoritate.

4.2. Polarizare și fragmentare socială
Considerate obiective centrale în campaniile actuale de dezinformare, strategiile din această categorie exploatează diviziunile sociale, politice sau culturale și le amplifică prin narative emoționale care apelează la identități individuale sau colective. Concentrându-se pe strategia „noi împotriva lor", dezinformarea accentuează destrămarea realității comune și diminuează ideea de compromis sau de atingere a unui consens. Studiile empirice au arătat că dezinformarea legată de politică amplifică polarizarea și favorizează abordările ideologice (Tucker et al. 2018, 30-49). Această categorie de strategii afectează coeziunea socială și diminuează capacitatea oamenilor de a reacționa colectiv la amenințările interne sau externe.

Existența tensiunilor sociale ajută actorii să amplifice conflictele identitare prin activarea emoțională, combinată cu întărirea granițelor politice, etnice, lingvistice, religioase, de gen sau a altor granițe culturale. Narațiunile asociate acestor tensiuni încurajează comunitățile să interpreteze lucrurile prin prisma unor cadre din ce în ce mai antagoniste, ceea ce, în timp, poate contribui la radicalizare, pe măsură ce utilizatorii sunt împinși către manifestări tot mai extremiste. Un avantaj al acestei strategii poate veni din crearea și consolidarea „camerelor de ecou", care limitează expunerea la perspective alternative și mențin utilizatorii în cadrul unor comunități cu viziuni similare. Atunci când grupurile de oameni nu mai împărtășesc un punct de referință comun, coeziunea socială și capacitatea de reacție colectivă

încep să devină mai fragile. Dezbaterile publice devin mai ostile și se îndepărtează de soluționarea problemelor sociale, diminuând astfel capacitatea societății de a reacționa la amenințările interne sau externe. Polarizarea funcționează atât ca efect politic și social al dezinformării, cât și ca strategie de securitate prin divizarea opiniei publice, reducerea încrederii între grupuri și diminuarea capacității de a răspunde provocărilor cotidiene.

4.3. Confuzie

Aceste strategii mută accentul dezinformării de la persuasiune către perturbare. Actorii nu promovează o singură narativă coerentă care să susțină o agendă specifică, ci diseminează informații contradictorii, ambigue sau copleșitoare pentru a genera incertitudine și suprasolicitare cognitivă. Modelul ”firehose of falsehood” ilustrează clar modul în care volumul, repetiția, rapiditatea și inconsistența contribuie la destabilizarea mediilor informaționale (Paul și Matthews 2016, 2-9). Acest tip de acțiuni contribuie la diminuarea posibilității de a forma convingeri puternice și descurajează implicarea în discursul public, deoarece oamenii nu sunt siguri ce este adevărat și ce nu.

Mecanismul central al acestei categorii este descurajarea prin confuzie, care implică răspândirea pe internet a unui volum suficient de mare de contradicții și ambiguități, astfel încât utilizatorii să se detașeze de problemele principale, iar instituțiile să se confrunte cu dificultăți de coordonare (Hedling și Ördén 2025, 969-974), fiind astfel un mecanism care lucrează pe mai multe planuri. Strâns legat de acest lucru este „inundația de informații”, un efect al modelului ”firehose of falsehood”, în care spațiul informațional este saturat cu un volum atât de mare de informații încât utilizatorii devin confuzi și se luptă să distingă informațiile valide de zgomotul de fond. În acest caz, efectul strategic, atât social, cât și psihologic, nu este persuasiunea, ci paralizia.

4.3. Controlul atenției

Aceste strategii determină ce anunțuri publice sunt difuzate, ce se discută și ce priorități se stabilesc. În loc să creeze confuzie, inundând spațiul informațional cu narative concurente, conținut senzaționalist sau controverse irelevante, atenția utilizatorilor poate fi redirecționată departe de evenimentele principale sau de problemele incomode (Loru et al. 2025, 1-10). În prezent, când implicarea publicului este mai importantă decât relevanța, aceste strategii profită de momentul oportun și de vizibilitate pentru a devia atenția cât mai discret posibil.

Procesul funcțional al acestei categorii începe adesea cu o deviere a agendei, în care actorii folosesc subiecte alternative pentru a redirecționa atenția departe de problemele politice, de eșecurile și de evenimentele dăunătoare. Ulterior, acesta este combinat cu elementul senzațional, în care conținutul capătă o încărcătură emoțională pentru a genera implicare și vizibilitate algoritmică. De asemenea, dacă acest conținut este publicat în momente cheie, cum ar fi alegerile sau crizele, efectul este maximizat, deoarece oamenii caută continuu explicații și reacții rapide. Obiectivul nu se referă întotdeauna la convingerea publicului de o narațiune specifică, ci la controlul a ceea ce devine vizibil, a ceea ce poate fi tratat ca urgent și a

ceea ce dispare din atenția colectivă. Prin urmare, efectul constă în reacția societății de a-și îndrepta atenția către conținut nou, scandalos și înfricoșător, făcând-o mai fragmentată și mai instabilă.

4.5. Normalizarea

Expunerea repetată la conținut înșelător sau la conținut manipulator, prezentat în mod eronat poate schimba treptat percepția asupra a ceea ce este acceptabil, credibil sau plauzibil. În timp, narativele care, în mod uzual ar fi excluse, pot deveni normale prin repetare suficientă, familiarizare sau consolidare în context social. *Efectul adevărului iluzoriu* ilustrează cel mai bine acest proces, deoarece afirmațiile repetate sunt mai susceptibile a fi percepute ca adevăr, indiferent de valoarea lor factuală (Pennycook, Cannon și Rand 2018, 2-7). Aceste strategii sunt importante deoarece reduc rezistența la manipulare și permit ca dezinformarea să fie acceptată ca normală în acțiunile zilnice.

Atunci când actorii folosesc narațiuni în mod repetat, utilizatorii se familiarizează tot mai mult cu informațiile. Această strategie contribuie la normalizarea neîncrederii, situație în care suspiciunea față de instituții și experți pare a fi o atitudine normală. Pentru un efect mai bun, această strategie poate fi combinată cu strategii de confuzie. Odată ce publicul se familiarizează cu un subiect, pot fi introduse treptat afirmații mai radicale sau ideologice, care sunt percepute ca fiind mai puțin perturbatoare decât cele inițiale. Aceste mecanisme au ca efect reducerea rezistenței la informații surprinzătoare, modificând limitele discursului acceptabil.

4.6. Exploatarea situațiilor de criză și manipularea oportunistă

O altă strategie importantă constă în exploatarea crizelor și momentelor de incertitudine. În prezent, alegerile, pandemiile sau conflictele geopolitice sunt evenimente care atrag cea mai mare atenție. În astfel de perioade, cererea de informații credibile crește brusc, în timp ce mecanismele de verificare sunt lente sau insuficient pregătite pentru a ține pasul. Actorii dezinformării profită de aceste vulnerabilități, introducând narative înșelătoare, care pot influența modurile de gândire și procesele decizionale, afectând la scară mai largă încrederea în instituții sau răspunsul la criză. Așa după cum au arătat S. Vosoughi, D. Roy și S. Aral, dezinformarea se răspândește de până la șase ori mai repede în timpul crizelor și poate afecta în mod semnificativ comportamentul publicului față de măsurile de sănătate sau încrederea în comunicarea oficială, mai mult decât conținutul verificat (Vosoughi, Roy și Aral 2018, 1146-1153).

Introducerea unor narațiuni înșelătoare pentru a intensifica sau a deturna atenția de la dezbaterile politice, pentru a contrazice sau a pune sub semnul întrebării informațiile oficiale în situații de urgență (COVID-19) ori pentru a răspândi interpretări eronate ale unui eveniment, înainte ca informațiile oficiale fiabile să se consolideze sunt doar câteva dintre strategiile care funcționează prin combinarea incertitudinii cu frica și urgența. Efectul principal este acela că dezinformarea poate influența percepția și comportamentul tocmai în momentele în care încrederea, coordonarea și comunicarea instituțională se impun tot mai mult.

4.7. Subminarea rezilienței democratice

Strategia principală care le cuprinde pe toate cele menționate anterior constă în subminarea rezilienței democratice și a securității naționale. Acesta este un obiectiv strategic cumulativ al multor campanii de dezinformare, care pot slăbi încrederea, pot polariza societățile sau perturba procesul de luare a deciziilor la nivel colectiv. Indiferent dacă amenințarea este internă sau externă, nu este nevoie de o perturbare masivă a societății, deoarece chiar și o slăbire parțială a încrederii și coordonării poate avea consecințe strategice semnificative în timp prin aplicarea tacticilor și strategiilor de mai sus (Chadwick și Stanyer 2022, 1-17).

5. Discuții

Deși tacticile și strategiile pot fi analizate separat, relația dintre ele în cadrul procesului de dezinformare este fundamental interconectată și nonliniară. Nu există o formulă strictă care să lege intervențiile tactice izolate de rezultatele strategice; dimpotrivă, dezinformarea funcționează prin interacțiuni repetate, coordonate și adaptabile între multiple tactici, care, împreună, promovează obiective la nivel macro pe parcursul timpului. Un aspect esențial este că această relație este de tipul „multe-la-multe": aceeași tactică poate susține simultan mai multe strategii, iar aceeași strategie poate fi pusă în practică prin diferite configurații tactice, în funcție de contextul social, de dinamica platformei și interesele actorilor. De exemplu, discreditarea depinde de interacțiunea dintre încadrarea narativă, înșelăciunea sursei, amplificarea și suprimarea vocilor corective, în timp ce polarizarea rezultă din combinații de activare emoțională, comportament neautentic coordonat și saturație informațională. Tabelul 1 prezintă în detaliu aceste interdependențe.

Structura prezentată în Tabelul 1 poate fi ilustrată prin cazul operațiunilor ruse de dezinformare, îndreptate împotriva Ucrainei și publicului din Europa de Vest, în special în perioada care a urmat invaziei pe scară largă din februarie 2022. Acest caz a fost amplu documentat și oferă un exemplu concret al modului în care mecanismele tactice se transformă în efecte strategice de securitate. La nivel tactic, actorii afiliați statului rus au utilizat o combinație de conținut fabricat (inclusiv imagini trucate, atribuite forțelor ucrainene), narative sub falsă identitate (prezentând acțiunile defensive ucrainene ca agresiune), comportament neautentic, coordonat prin rețele de conturi amplificatoare pe Telegram și Twitter/X, precum și o avalanșă de tehnici de falsificare care implică diseminarea simultană a narativelor contradictorii – negarea atrocităților, atribuirea acestora altor părți și susținerea că au fost înscenate (Dov Bachmann , Putter și Duczynski 2023, 858-867). Conținutul de tip deepfake, inclusiv un videoclip fabricat, în care președintele ucrainean Zelenski ar fi cerut capitularea, a demonstrat utilizarea unor tactici bazate pe inteligența artificială (Farid 2025, 1-9). La nivel strategic, aceste operațiuni combinate au urmărit discreditarea instituțiilor guvernamentale și militare ucrainene, polarizarea opiniei publice occidentale în ceea ce privește sprijinul acordat Ucrainei, crearea de confuzie prin supraîncărcarea cu informații, care a făcut dificilă verificarea faptelor pe scară largă și erodarea

TABEL nr. 1. Configurări de strategii și tactici în ecosistemul dezinformării social media

Strategie	Configurarea de bază a tacticilor	Tactici de sprijin	Logica interdependenței
Discreditarea instituțiilor	Conținut fabricat + încadrarea manipulării + narative conspirative + tactici de identificare a sursei (experți falși, imitație/personificare, astroturfing)	Amplificare coordonată Cumpărare de influență Hărțuirea jurnaliștilor experților sau oficialilor Amplificare algoritmică	Instituțiile sunt slăbite atunci când narativele negative sunt amplificate în mod repetat, părând să provină din surse autentice credibile, dar sunt susținute de atacuri către vocile legitime.
Polarizarea	Încadrarea manipulării și narative bazate pe identitate + comportament neautentic coordonat + boți/troli	Microdirecționare Amplificare bazată pe implicare Manipulare prin hashtag Persoane sintetice	Polarizarea apare atunci când narative identitare, încărcate emoțional sunt amplificate prin rețele coordonate și consolidate în cadrul unor comunități online specifice, sporind resentimentele.
Confuzia	Firehose of falsehood + narative contradictorii + conținut înșelător sau fabricat	Boți Exploatare algoritmică Deepfake-uri Devierea agendei	Confuzia este generată de copleșirea publicului cu informații repetitive, contradictorii sau într-un volum mare, ceea ce face dificilă distincția dintre conținutul credibil și cel fals.
Controlul atenției	Tactici de exploatare a infrastructurii platformelor (exploatare algoritmică) + manipulare prin hashtaguri + tactici de coordonare și amplificare	Manipulare prin influenceri Coordonarea postărilor Devierea agendei Omiterea selectivă	Atenția publicului este redirecționată când actorii reușesc să exploateze vizibilitatea platformelor și algoritmii pentru a crește interesul față de anumite narative, în timp ce problemele și subiectele reale sunt eclipsate.
Normalizarea	Tactici de amplificare, în special repetiția + încadrarea manipulării + surse pseudojurnalistice	Manipulare prin influenceri Persoane sintetice Boți și rețele de troli Sisteme de recomandări algoritmice	Expunerea repetată la narative specifice crește treptat familiarizarea cu conținutul, făcându-l mai acceptabil și stabilindu-l ca normalitate, ceea ce contribuie la apariția neîncrederii și a contextelor înșelătoare în discursul cotidian.
Exploatarea crizelor	Conținut înșelător sau fabricat complet legat de crize + contextualizare emoțională + amplificare rapidă coordonată	Deepfake-uri Microdirecționare Manipulare prin hashtag Conținut sintetic automat	În timpul crizelor, incertitudinea și crizele diminuează procesele de verificare, permițând narativelor manipulatoare să se răspândească rapid și să influențeze percepțiile, emoțiile și comportamentele publicului, înainte ca informațiile oficiale să fie publicate.
Subminarea rezilienței democratice	Majoritatea tacticilor de discreditare, polarizare, confuzie sau tactici de amplificare	Tactici de suprimare și de perturbare a discursului Conținut creat de IA Suprasaturare de narative manipulative	Reziliența democratică este diminuată gradual, când mai multe strategii și tactici sunt combinate, reducând legitimitatea instituțională și sporind polarizarea societății. Acest lucru poate afecta radical răspunsul colectiv la amenințările interne și cele externe.

Sursa: concepția autorului.

încrederii în comunicatele instituționale ale NATO și UE (EEAS 2025b, 7-11). Logica interdependenței observabilă în acest caz se aliniază direct cu structura „multe-la-multe", propusă în Tabelul 1: aceleași rețele coordonate de comportamente neautentice au servit simultan obiectivelor de discreditare, confuzie și polarizare, în timp ce strategia de polarizare în sine s-a bazat pe manipularea cadrului narativ, pe conținutul emoțional și tactici de amplificare, aplicate în rândul diferitelor segmente de public, în diferite limbi. Acest caz validează astfel utilitatea analitică a cadrului propus în acest articol, confirmând, totodată, că acele campanii de dezinformare din lumea reală sunt mult mai fluide și adaptabile decât poate surprinde pe deplin orice taxonomie statică.

Cazul Ucrainei, discutat mai sus, ilustrează empiric această logică, arătând cum aceleași rețele de conturi amplificatoare au servit simultan obiectivelor de discreditare, confuzie și polarizare. Această convergență confirmă faptul că respectivele cadre analitice care se concentrează pe tactici individuale sau pe lanțuri cauzale unice vor subestima sistematic amploarea și adaptabilitatea dezinformării coordonate. Concluzia analitică cheie este că efectele strategice rezultă din desfășurarea susținută și suprapusă a mai multor tactici, nu dintr-un singur mecanism care acționează izolat.

Pentru a consolida fundamentul empiric al modelului propus mai sus, cazul ucrainean, menționat anterior, poate fi împărțit în microcazuri mai specifice, ceea ce permite ilustrarea celor șapte etape într-un mod mai clar. Prin urmare, am ales trei cazuri bine documentate, precum deepfake-ul cu predarea președintelui Zelenski, dezinformarea privind masacrul de la Bucha și Operațiunea Overload (Matrioșca), comparate mai jos în Tabelul 2. Primul caz se referă la martie 2022, după începerea invaziei ruse, când un videoclip de tip deepfake a circulat pe mai multe platforme, înfățișându-l pe Volodimir Zelenski cerându-le ucrainenilor să se predea și să se întoarcă la familiile lor (Allyn 2022; Bohacek și Farid 2022, 1-3). Cazul Bucha s-a bazat pe confuzie, negarea identității și contradicții. După ce au apărut dovezi privind uciderea civililor în Bucha, sursele pro Kremlin au negat implicarea Rusiei și au promovat ideea că acel conținut era fabricat, înscenat sau atribuit în mod fals agresorului. Studiul „Denying Bucha" (Fredheim, Ahonen și Pamment 2023, 4-22) a arătat că aceste surse au publicat informații contradictorii și tendențioase pentru a submina analizele și afirmațiile occidentale privind masacrul. Al treilea caz, diferit de primele două, s-a concentrat mai mult pe faza buclei de amplificare, vizând jurnaliștii, cercetătorii și organizațiile de verificare a faptelor. Acesta a fost considerat un efort de propagandă al Kremlinului, de a submina eforturile de război ale Ucrainei și de a destabiliza democrațiile occidentale (Atanasova, Poldi și Kuster 2025, 8-9).

Acest tabel nu validează modelul din punct de vedere statistic, ci arată mai degrabă că fiecare etapă poate fi aplicată în diferite situații. Am ales cele trei exemple, legate de invazia rusă în Ucraina, deoarece ele ilustrează diferite forme de escaladare: de la un episod rapid de manipulare a IA într-un context de criză, la o campanie de negare și contradicții privind o atrocitate, și o operațiune recentă de supraîncărcare informațională, care exploatează ecosistemul de verificare a faptelor. După cum s-a

TABEL nr. 2. Aplicație comparativă a modelului propus asupra a trei cazuri de dezinformare rusă

Faza modelului	Deepfake – predarea lui Zelenski	Dezinformarea asupra masacrului din Bucha	Operația Overload / Matrioșca
Caracteristici funcționale ale platformelor/ oportunități	Incertitudinea și confuzia din timpul războiului, nevoia publicului de informații coordonate, rapiditatea și vizibilitatea, oferite de platforme, condiții favorabile pentru conținutul fals, privind liderii să atragă atenția	Impactul generat de reportajele și imaginile din Bucha au creat un context în care publicul avea nevoie de dovezi vizuale, actualizări continue și răspunsuri oficiale	Viteza platformelor, circulația între platforme, vizibilitatea jurnaliștilor, experților și verificatorilor de fapte, costul redus al creării de conținut cu ajutorul IA
Tactici de dezinformare	Videoclipuri sintetice, generate de IA, care îl imită pe președintele Volodimir Zelenski, exploatarea situației de criză	Narațiuni de negare, prezentări sub falsă identitate, explicații contradictorii, un val de mesaje, provenite de la diverse surse media	Conținut fabricat (imagini, videoclipuri), conținut generat de IA, uzurparea identității unor personalități publice, formate de știri false, diseminare coordonată
Efecte cognitive	Incertitudine, panică, îndoieli cu privire la conducere și credibilitatea mesajului	Confuzie cu privire la atribuire și responsabilitate, îndoieli privind dovezile vizuale, incertitudine în ceea ce privește credibilitatea surselor media	Îndoieli privind autenticitatea, oboseala cauzată de verificarea faptelor, confuzie cu privire la surse, suprasolicitarea autorităților în verificarea unor volume mari de conținut
Răspunsuri comportamentale	Distribuire rapidă pe mai multe platforme, demascarea/verificarea faptelor, discuție publică	Dezbateri online, implicare în afirmații contradictorii, discuții publice privind atribuirea și responsabilitatea	Personalitățile publice, jurnaliștii și verificatorii de fapte au fost nevoiți să demaște, să verifice și să reacționeze la avalanșa de conținut manipulat
Bucle de amplificare	Videoclipul a devenit viral datorită distribuției pe platforme, acoperirii mediatice, activității de analiză și discuției publice despre deepfake-uri în timp de război	Repetarea de către canalele pro Kremlin, aceeași agendă pentru toate canalele media, conturile de social media, analizele globale ale evenimentului	Conținutul a fost mediatizat de mai multe ori în scopul demascării, câștigând astfel mai multă vizibilitate
Strategii	Exploatarea crizei, discreditarea conducerii ucrainene, încercarea de a submina moralul și credibilitatea comenzii	Descurajare prin confuzie, discreditarea instituțiilor ucrainene și occidentale, devierea agendei	Controlul atenției, manipularea agendei, normalizarea narațiunilor anti Ucraina și pro Kremlin
Implicații asupra securității naționale	Potențială slăbire a încrederii în conducere, a moralului și credibilității instituțiilor publice	Indignare publică, responsabilitate, îndoieli privind sprijinul occidental acordat Ucrainei	Slăbirea mass-mediei și a entităților de verificare a faptelor, creșterea incertitudinii publice, erodarea încrederii în instituțiile legitime

Sursa: concepția autorului.

menționat mai sus, putem observa că procesul nu este o rețetă perfectă, precum o evoluție liniară, ci mai degrabă acesta este adaptabil, în funcție de context, platformă și public.

Toate aceste tactici și strategii, menționate mai sus, evidențiază faptul că dezinformarea funcționează prin procese interconectate și care se întăresc reciproc. Tacticile sunt instrumentele operaționale prin care are loc manipularea la nivel micro, în timp ce strategiile reprezintă obiectivele mai ample pe care aceste mecanisme urmăresc să le atingă în timp. Ele depind una de cealaltă, dar relația dintre ele nu este liniară sau unidimensională. Din ceea ce am observat, putem constata că există tactici care pot fi utilizate pentru multiple obiective strategice, în timp ce o singură strategie poate fi implementată prin desfășurarea coordonată a mai multor tactici pe diverse platforme, pentru diferite audiențe și în contexte temporale diferite.

Tacticile și strategiile analizate mai sus reprezintă cele mai semnificative mecanisme din punct de vedere operațional, documentate în literatura actuală de specialitate privind dezinformarea digitală. Din analiză, reies câteva concluzii transversale:

- Un aspect important este că dezinformarea pe rețelele sociale ar trebui înțeleasă ca un proces de amplificare pe mai multe niveluri și nu ca un simplu flux de conținut fals sau înșelător. Dezinformarea se dezvoltă printr-o secvență de niveluri interconectate; de la posibilitățile oferite de platforme care permit manipularea tactică, la răspunsuri cognitive și comportamentale, apoi amplificarea prin algoritmi și, în final, dacă se menține în timp, la aplicarea strategiilor la nivel societal. Acest lucru arată trecerea de la abordări centrate pe conținut la un proces în care manipularea la nivel micro poate obține strategii de nivel macro.
- Un al doilea aspect se referă la modul în care rețelele sociale funcționează ca o infrastructură de legătură între tactici și strategii. Platformele oferă diverse caracteristici, precum vizibilitate, rapiditate, recomandări algoritmice sau difuzare la costuri reduse, care nu facilitează neapărat diseminarea informațiilor, dar modelează condițiile în care mecanismele tactice pot fi extinse și menținute.
- O a treia caracteristică importantă este că relația dintre tactici și strategii nu este simplă, ca o legătură unică, ci mai degrabă de tipul „multe-la-multe". O singură tactică poate face parte din mai multe strategii, în timp ce o strategie poate depinde de mai multe tactici. De exemplu, CNC ar putea avea o contribuție importantă la discreditare, polarizare, normalizare sau manipularea agendei, în timp ce, de exemplu, polarizarea ar putea necesita experți falși, conținut fabricat, amplificare sau manipularea cadrului de referință. Prin urmare, campaniile de dezinformare pot fi construite prin relații de suprapunere și adaptare între tactici și strategii.
- De asemenea, pentru strategii specifice, există multiple configurații de tactici, în funcție de context, obiective sau vulnerabilitățile societății. Nu există o cale directă de a construi o strategie pornind de la o tactică specifică. Acest lucru sugerează că accentul analitic ar trebui pus pe modul de a lega tactici specifice

pentru a obține cel mai eficient rezultat, în loc să se concentreze doar pe o singură tactică.

- Concentrându-ne asupra ultimei categorii de strategii menționate, referitoare la erodarea rezilienței democratice, am putea arăta că dezinformarea pe rețelele sociale are un caracter cumulativ, mai degrabă decât unul imediat. Dezinformarea rareori subminează încrederea, coeziunea sau legitimitatea instituțională printr-un singur material video, audio sau text, ori într-un interval scurt de timp. În schimb, efectele sale se manifestă prin repetare, coordonare, amplificare și persistență. În timp, narativele repetate pot normaliza neîncrederea, pot intensifica polarizarea sau pot spori confuzia. Urmând această logică, devine mai ușor să înțelegem dezinformarea ca un proces, mai degrabă decât ca o colecție de mesaje.
- Ultimul aspect important este reprezentat de rolul rețelelor sociale în subminarea securității sociale. Rețelele sociale acționează indirect în vederea atingerii obiectivelor, fiind un factor care facilitează condițiile în care tacticile de dezinformare pot deveni procese strategice. Buclele cognitive și comportamentale, amplificarea prin algoritmi, consecvența sau repetarea sunt câteva caracteristici ale platformelor de socializare care acționează din umbră pentru a ajuta actorii să-și atingă obiectivele.

Împreună, aceste observații confirmă faptul că rețelele sociale funcționează nu doar ca un mediu de comunicare, ci și ca o infrastructură strategică – una care permite coordonarea, amplificarea și susținerea tacticilor de dezinformare până când acestea produc efecte de securitate la nivel macro.

Contribuția originală a acestui articol constă în cadrul integrativ care ilustrează evoluția campaniilor de dezinformare, pornind de la capacitățile platformelor și ajungând la implicațiile asupra securității naționale, trecând prin etapele intermediare menționate anterior. Deși cadrele existente abordează etapele procesului de dezinformare, ele clarifică rareori modul în care mecanismele tactice ale platformelor se transformă în obiective strategice mai ample. Modelul propus abordează această problemă, ilustrând modul în care platformele de socializare permit intensificarea și menținerea manipulării de la nivel micro până la punctul în care acest proces susține strategii, precum discreditarea, polarizarea, descurajarea prin confuzie, manipularea agendei, normalizarea și exploatarea crizelor. Valoarea sa principală constă în oferirea unui instrument structurat pentru examinarea evoluției dezinformării de la acțiuni tactice izolate la o influență strategică persistentă, cu potențială relevanță pentru securitate.

Concluzii

Acest articol a analizat rolul rețelelor sociale în subminarea securității naționale prin identificarea relației dintre tacticile și strategiile de dezinformare. În loc să trateze rețelele sociale ca pe un canal pasiv prin care circulă conținut fals, analiza a demonstrat că dezinformarea funcționează ca un proces de escaladare pe mai multe niveluri: posibilitățile oferite de platforme permit manipularea tactică, mecanismele

tactice generează reacții cognitive și comportamentale, iar implementarea coordonată și susținută transformă aceste reacții în efecte strategice asupra securității. Rețelele sociale reprezintă așadar o infrastructură strategică ce permite manipularea la nivel societal, cu consecințe măsurabile asupra politicii și securității.
Articolul a distins două niveluri analitice: tactici de dezinformare (mecanisme la nivel micro, incluzând fabricarea de conținut, manipularea cadrului narativ, înșelarea privind sursa, amplificarea coordonată și producția bazată pe IA) și strategii de dezinformare (obiective la nivel macro, incluzând discreditarea instituțiilor, polarizarea, confuzia, normalizarea, exploatarea crizelor și erodarea rezilienței democratice). Așa după cum confirmă cadrul conceptual și studiul de caz privind Ucraina, aceste niveluri sunt conectate prin relații adaptabile, suprapuse, de tip „multe-la-multe", mai degrabă decât prin lanțuri cauzale liniare. O tactică poate servi mai multor strategii; o strategie poate recurge la mai multe configurații tactice, în funcție de context și de vulnerabilitățile țintei. Implicațiile de securitate ale dezinformării sunt, prin urmare, cumulative: efectele strategice – încrederea instituțională slăbită, polarizarea intensificată, reziliența democratică erodată – se acumulează prin aplicarea susținută și coordonată a mecanismelor tactice de-a lungul timpului, afectând fundamentele informaționale, cognitive și instituționale de care depind societățile democratice.

Aceste rezultate sugerează, de asemenea, câteva implicații practice. În primul rând, politicile de combatere a dezinformării ar trebui să-și schimbe orientarea, trecând de la corectarea afirmațiilor false individuale la abordarea procesului mai amplu prin care această denaturare a informațiilor este amplificată, repetată și făcută credibilă din punct de vedere social. Pentru a realiza acest lucru, este necesară o cooperare mai strânsă între instituțiile legitime, companiile care dețin platforme, cercetători, verificatori de fapte și organizații sociale, în special în timpul evenimentelor importante, care necesită mai multe resurse pentru a preveni și a demasca dezinformarea. În al doilea rând, programele de educație media și digitală ar trebui să-și extindă atenția de la identificarea conținutului fals la înțelegerea tendințelor, a tehnicilor de manipulare, a înșelăciunii surselor sau amplificării coordonate, pentru o mai bună înțelegere a aspectelor la care utilizatorii ar trebui să fie mai atenți. În al treilea rând, prin analiza modelului propus, reziliența democratică ar trebui îmbunătățită prin identificarea elementelor modelului care necesită mai multă atenție și dezvoltare, astfel încât legătura cu implicațiile asupra securității naționale să fie ruptă.

Acest articol face parte dintr-un proiect mai amplu de cercetare doctorală care se concentrează asupra impactului instrumentelor de social media în conflictele moderne, servind ca o modalitate de a analiza rolul dezinformării în mediul digital actual.

Referințe

Alkathiri, Nasser și Khaled Slhoub. 2025. "Challenges in machine learning-based social bot detection: a systematic review." *Discover Artificial Intelligence* 5(214): 1-40. https://doi.org/10.1007/s44163-025-00448-w.

Allyn, Bobby. 2022. "Deepfake video of Zelenskyy could be «tip of the iceberg» in info war, experts warn." https://www.npr.org/2022/03/16/1087062648/deepfake-video-zelenskyy-experts-war-manipulation-ukraine-russia.

Atanasova, Aleksandra, Francesco Poldi și Guillaume Kuster. 2025. "Operation Overload, More Platforms, New Technology, Powered by AI." *Analysis report.*

Baines, Paul, Nicholas O'Shaughnessy și Nancy Snow. 2019. *The SAGE Handbook of Propaganda.* SAGE Publication Ltd.

Benkler, Yochai, Robert Faris și Hal Roberts. 2018. *Network Propaganda - Manipulation, Disinformation, and Radicalization in American Politics.* Oxford University Press.

Bernal, Alonso, Cameron Carter, Ishpreet Singh, KAthy Cao și Olivia Madreperla. 2020. *Cognitive warfare an attack on truth and thought.* Johnson Hopkins University.

Bohacek, Matyas și Hany Farid. 2022. "Protecting world leaders against deep fakes using facial,gestural, and vocal mannerisms." *Proceedings of the National Academy of Sciences of the United States of America* (National Academy of Sciences) 119(48): 1-3. https://doi.org/10.1073/pnas.2216035119.

Bradshaw, Samantha și Philip N. Howard. 2018. "Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation." *Computational Propaganda Research Project.* Oxford Internet Institute, University of Oxford. 11-15.

Castells, Manuel. 2009. *Communication Power.* New York: Oxford University Press.

Chadwick, Andrew. 2017. *The Hybrid Media System: Politics and Power.* 2nd Edition. New York: Oxford University Press.

Chadwick, Andrew și James Stanyer. 2022. "Deception as a Bridging Concept in the Study of Disinformation, Misinformation, and Misperceptions: Towards a Holistic Framework." *Communication Theory* 32(1): 1-24. https://doi.org/10.1093/ct/qtab019.

Clemons, Eric K, Andrej Savin, Maximilian Schreieck, Stina Teilmann-Lock, Jan Trzaskowski și Ravi Waran. 2024. "A face of one's own: The role of an online personae in a digital age and the right to control one's own online personae in the presence of digital hacking." *Electronic Markets* 34 (1): Article 31. https://doi.org/10.1007/s12525-024-00713-3.

de Goeij, Maria W.R. 2023. "Reflexive control: Influencing Strategic Behavior." *Parameters: The US Army War College Quarterly* 53(4): 97-108. https://doi.org/10.55540/0031-1723.3262.

Dov Bachmann , Sascha-Dominik , Dries Putter și Guy Duczynski. 2023. "Hybrid warfare and disinformation: A Ukraine warperspective." *Policy Insights* 858-869. https://doi.org/10.1111/1758-5899.13257.

Dragomir, Marius, Jose Ruas-Araujo și Minna Horowitz. 2024. "Beyond online disinformation: assessing national information resilience in four European countries." *Humanities and Social Sciences Communications* 11: 101. https://doi.org/10.1057/s41599-024-02605-5.

EEAS. 2025a. "2024 Report on EEAS Activities to Counter Foreign Information Manipulation and Inference (FIMI)." 4-8. https://www.eeas.europa.eu/sites/default/files/2025/documents/2024%20Report%20on%20EEAS%20Activities%20to%20Counter%20FIMI.pdf.

___. 2025b. "EEAS Report on Foreign Information Manipulation and Interference Threats." *Report on FIMI Threats*, 7-11.

Egelhofer, Jana Laura și Sophie Lecheler. 2019. "Fake news as a two-dimensional phenomenon: a framework and research agenda." *Annals of the International Communication Association* 43(2): 97-116. https://doi.org/10.1080/23808985.2019.1602782.

Farid, Hany. 2025. "Mitigating the harms of manipulated media: Confronting deepfakes and digital deception." *PNAS Nexus* 4(7): pgaf194. https://doi.org/10.1093/pnasnexus/pgaf194.

Ferreira, Ricardo Ribeiro. 2022. "Liquid Disinformation Tactics: Overcoming Social Media Countermeasures through Misleading Content." *Journalism Practice* 16(8): 1537-1558. https://doi.org/10.1080/17512786.2021.1914707.

Fredheim, Rolf, Anneli Ahonen și James Pamment. 2023. *Denying Bucha - The Kremlin's Influence tactics in the aftermath of the 2022 Bucha atrocity.* Research report, Lund University.

Hameleers, Michael. 2023. "Disinformation as a context-bound phenomenon: toward a conceptual clarification integrating actors, intentions and techniques of creation and dissemination." *Communication Theory* 33(2): 1-10. https://doi.org/10.1093/ct/qtad004.

Hedling, Elsa și Hedvig Ördén. 2025. "Disinformation, Deterrence and the Politics of Attribution." *International Affairs* 101(3): 967-986. doi:https://doi.org/10.1093/ia/iiaf012.

Kruijver, Kimberley, Neill Bo Finlayson, Beatrice Cadet și Sico van der Meer. 2025. "The disinformation lifecycle: an integrated understanding of its creation, spread and effects." *Discover Global Society* 3(1): 1-26. https://doi.org/10.1007/s44282-025-00194-5.

Lewandowsky, Stephan, Ullrich K.H. Ecker și John Cook. 2017. "Beyond Misinformation: Understanding and Coping with the "Post-Truth" Era." *Journal of Applied Research in Memory and Cognition* 6 (4): 353-369. https://doi.org/10.1016/j.jarmac.2017.07.008.

Lindberg, Rebecca și Emily Denniss. 2025. "Social media and the spread of misinformation: infectious and a threat to public health." *Health Promotion International* 40(2): daaf023. https://doi.org/10.1093/heapro/daaf023.

Loru, Edoardo, Alessandro Galeazzi, Anita Bonetti, Emanuele Sangiorgio, Niccolò Di Marco, Matteo Cinelli, Max Falkenberg, Andrea Baronchelli și Walter Quattrociocchi. 2025. "Ideology and polarization set the agenda on social media." *Scientific Reports* 15 (35816): 1-13. https://doi.org/10.1038/s41598-025-19776-z.

Lukavska, K., R. Gabrhelík, M. Miovský, N. Hynek, B. Gavurova, L. Stastna, M. Bartak, B. Petruzelka și V. Moravec. 2025. "Exploring Disinformation: The interplay of exposure, trust, and sharing." *Computers in Human Behavior Reports* 18: 100686. https://doi.org/10.1016/j.chbr.2025.100686.

Mazarr, Michael, Abigain Casey, Alyssa Demus, Scott Harold, Luke Mathews , Nathan Beaucham-Mustafaga și James Sladden. 2019. ”Hostile Social Manipulation.” https://www.rand.org/pubs/research_reports/RR2713.html.

Metzler, Hannah și David Garcia. 2024. ”Social Drivers and Algorithmic Mechanisms on Digital Media.” *Perspectives on psychological science: a journal of the Association for Psychological Science* 19(5): 735-748. https://doi.org/10.1177/17456916231185057.

Murero, Monica. 2023. ”Coordinated inauthentic behavior: An innovative manipulation tactic to amplify COVID-19 anti-vaccine communication outreach via social media.” *Frontiers in Sociology* 8: 1141416. https://doi.org/10.3389/fsoc.2023.1141416.

Mustafa, Hassan, Markus Luczak-Roesch și David Johnstone. 2025. ”Conceptualizing the Evolving Nature of Computational Propaganda: A Systematic Literature Review.” *Annals of the International Communication Association* 49(1): 45-60. https://doi.org/10.1093/anncom/wlaf001.

NATO. 2022. ”Strategic Concept.” https://www.nato.int/content/dam/nato/webready/documents/publications-and-reports/strategic-concepts/2022/290622-strategic-concept.pdf.

Park, Seyeon și Xiaoli Nan. 2024. ”Generative AI and misinformation: a scoping review of the role of generative AI in the generation, detection, mitigation, and impact of misinformation.” *AI & Society* 41(2): 1501-1515. https://doi.org/10.1007/s00146-025-02620-3.

Paul, Christopher și Miriam Matthews. 2016. ”The Russian `Firehose of Falsehood` Propaganda Model: Why It Might Work and Options to Counter It.” https://doi.org/10.7249/PE198.

Pennycook, Gordon, Tyrone Cannon și David Rand. 2018. ”Implausibility and illusory truth: Prior exposure increases perceived accuracy of fake news but has no effect on entirely implausible statements.” *Journal of Experimental Psychology General* 147(12): 2-7. https://doi.org/10.1037/xge0000465.

Pomerantsev, Peter. 2019. *This is Not Propaganda.* London: Faber & Faber.

Romanishyn, Alexander, Olena Malytska și Vitaliy Goncharuk. 2025. ”AI-driven disinformation: policy recommendations for democratic resilience.” *Frontiers in Artificial Intelligence* 8: 1569115. https://doi.org/10.3389/frai.2025.1569115.

Surjatmodjo, Dwi, Andi Alimuddin Unde, Hafied Cangara și Febri Alem Sonni. 2024. ”Information Pandemic: A Critical Review of Disinformation Spread on Social Media and Its Implications for State Resilience.” *Social Sciences* 13(8): 418. https://doi.org/10.3390/socsci13080418.

Tucker, Joshua, Andrew Guess, Pablo Barberá, Cristian Vaccari, Alexandra Siegel, Sergey Sanovich, Denis Stukal și Brendan Nyhan. 2018. ”Online Content and Political Polarization.” *Social Media, Political Polarization, and Political Disinformation: A Review of the Scientific Literature.* Wililam and Flora Hewlett Foundation. 30-49.

Uusikylä, Petri, Harri Jalonen, Valdemar Kallunki, Anssi Keinänen și Silvia Sommarberg. 2024. ”Introduction to Information Resilience in the Context of National Preparedness.” În *Information Resilience and Comprehensive Security*, de Petri Uusikylä, H Jalonen și A Jokipii, 1-18. Palgrave Macmillan, Cham.

Vosoughi, Soroush, Deb Roy și Sinan Aral. 2018. "The Spread of True and False News Online." *Science* 359: 1146-1151. https://doi.org/10.1126/science.aap9559.

Wardle, Claire. 2024. *A Conceptual Analysis of the Overlaps and Differences between Hate Speech, Misinformation and Disinformation.* New York: United Nations.

Wardle, Claire și Hossein Derakhshan. 2017. *Information Dissorder: Toward an Interdisciplinary Framework for Research and Policy Making.* Strasbourg: Council of Europe, 20-21.

Wu, Manli, Tailai Wu și Yushan Xiao. 2025. "Why people share misinformation on social media? An integration of affordance and flow theories." *Humanities and Social Sciences Communications* 12: 1129. https://doi.org/10.1057/s41599-025-05511-6.