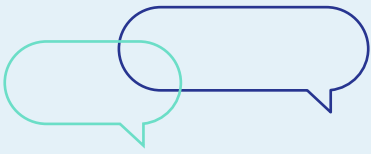


Cum să te protejezi împotriva manipulării informaționale?



Ghid pentru tinerii moldoveni





**„Libertatea
de opinie este
o farsă dacă
informațiile
factice nu
sunt garantate
și dacă faptele
însele sunt
contestate.”**

Hannah Arendt



Autori

Wojciech Solak

Director, Centrul pentru Democrație și Reziliență, GLOBSEC

Katarina Klingová

Coordonatoare de cercetare, Centrul pentru Democrație și Reziliență, GLOBSEC

Jakub Kubš

Analist de date, Centrul pentru Democrație și Reziliență, GLOBSEC

Barbora Dobó

Coordonatoare de proiect, Centrul pentru Democrație și Reziliență, GLOBSEC



Finanțat de
Uniunea Europeană

CENTRUL PENTRU
COMUNICARE STRATEGICĂ ȘI
CONTRACĂRARE A DEZINFORMĂRII



GLOBSEC
IDEAS SHAPING THE WORLD

Această publicație a fost realizată cu sprijinul financiar al Uniunii Europene. Conținutul acesteia reprezintă responsabilitatea exclusivă a proiectului „Consolidarea rezilienței în Republica Moldova: de sus în jos și de jos în sus”, finanțat de Uniunea Europeană. Conținutul publicației aparține autorilor și nu reflectă neapărat viziunea Uniunii Europene.



Cuprins

Introducere

8

De ce a fost creat acest manual?

8

Cum a fost realizat acest manual?

8

Cum se utilizează acest manual

9

Partea a III-a: Cum poate fi recunoscută manipularea în viața de zi cu zi

42

Narațiuni-cheie utilizate împotriva Republicii Moldova

52

Partea I: Înțelegerea mediului informațional

10

Istoria surselor de informare: de la Gutenberg la TikTok

11

Cum ajung informațiile la voi

12

De ce este important acest lucru

16

De ce funcționează manipularea

18

Partea a IV-a: Înțelegerea Inteligenței Artificiale

54

Ce este, de fapt, inteligența artificială?

56

De ce este important acest lucru în Republica Moldova?

58

Cum poate fi verificat dacă un conținut este generat de IA

59

Utilizarea responsabilă a IA

61

Partea a II-a: Ce sunt operațiunile de informații?

22

Termeni-cheie pe care trebuie să-i cunoașteți

24

Cum funcționează operațiunile de informare: instrumente și metode utilizate

30

Ce urmăresc operațiunile de informare?

36

Cine se află în spatele operațiunilor de informare?

38

Ce vulnerabilități exploatează operațiunile de informare?

39

Cum se deosebește manipularea de comunicarea legitimă?

40

Partea a V-a: Abilități practice pentru autoapărare în mediul informațional

62

Verificarea nu este suficientă

63

Recunoașterea argumentelor de rea-credință

67

Partea a VI-a: Instrumente pentru învățare 72

Învățare prin joc: instrumente interactive pentru dezvoltarea rezilienței informaționale	74
Resurse pentru continuarea învățării	80

Anexă: Exerciții practice pentru profesori 90

Setul de instrumente al influențării	92
Identificați amenințarea hibridă	96
Negarea științei în sala de clasă	100

Partea a VII-a: De la conștientizare la acțiune 84

Mai mult decât identificarea dezinformării	86
Igiena digitală: Protejarea identității în mediul online	88

Mulțumiri și referințe 108

Introducere

De ce a fost creat acest manual?

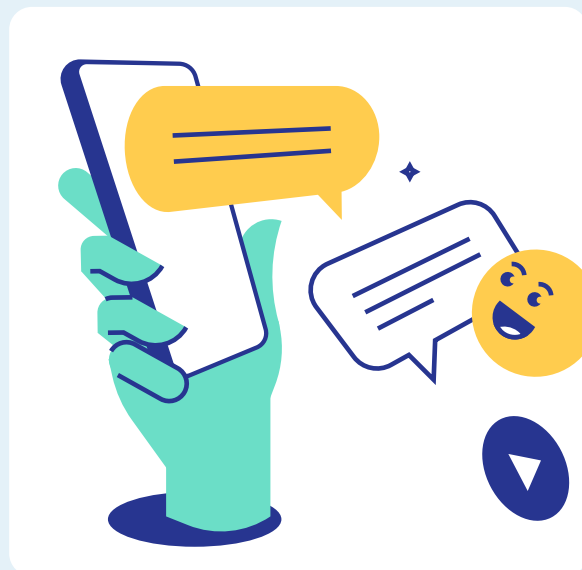
Acest manual a fost elaborat în cadrul unui proiect de educație media finanțat de Uniunea Europeană pentru a sprijini tinerii din Republica Moldova să se orienteze în mediul informațional complex de astăzi. Conținutul înșelător și manipulator se răspândește rapid prin intermediul rețelelor sociale, al aplicațiilor de mesagerie și al știrilor online, adesea fără a fi observat. Manualul oferă instrumente practice pentru a recunoaște operațiunile informaționale și pentru a înțelege mai bine modul în care funcționează peisajul mediatic, încurajând totodată tinerii să împărtășească aceste cunoștințe cu ceilalți. Astfel, manualul își propune să îi ajute pe participanți să devină formatori de la egal la egal, capabili să consolideze reziliența comunităților lor în fața manipulării.

privind manipularea informațiilor și ingerințele străine (MIS), precum Laboratorul de Cercetare Criminalistică Digitală al Consiliului Atlantic (Atlantic Council's Digital Forensic Research Lab)¹, proiectul UE „EUvsDisinfo”², precum și inițiative de verificare a faptelor, cum ar fi StopFals.md.³ În ceea ce privește alfabetizarea în domeniul inteligenței artificiale, manualul se bazează pe resurse precum Ghidul privind inteligența artificială elaborat de Faktabaari⁴ și cursul MIT „Media Literacy in the Age of Deepfakes” („Alfabetizarea media în era deepfake-urilor”).⁵

În același timp, manualul include materiale originale axate pe specificul mediului informațional din Republica Moldova. Exemplele, inclusiv cele provenite din cercetările proprii ale GLOBSEC, cum ar fi operațiunea cu sondajul fals „Vocepentru”⁶, sunt inspirate din cazuri reale de manipulare care au vizat cetățenii Republicii Moldova. Rezultatul este o resursă practică adaptată în mod special tinerilor din Republica Moldova și comunităților lor, bazată pe cele mai bune practici internaționale și ancorată în realitatea locală.

Cum a fost realizat acest manual?

Acest manual se bazează pe o serie de resurse și cercetări internaționale axate pe combaterea operațiunilor informaționale și consolidarea educației media. La baza sa stau cercetări academice privind manipularea informației și modul în care oamenii îi pot rezista, inclusiv studii realizate de instituții precum MIT și Universitatea Cambridge. Îndrumările practice se bazează pe activitatea unor organizații aflate în prima linie a cercetării



Cum se utilizează acest manual

Acest manual este conceput pentru a vă ajuta să vă orientați în mediul informațional actual, să deveniți mai rezilienți și să împărtășiți și altora ceea ce învățați. Manualul este structurat în șapte părți.

1 Partea I explică modul în care informația ajunge la voi – cum algoritmi modelează ceea ce vedeți, de ce mediul mediatic actual creează vulnerabilități sistemice și de ce acest lucru este deosebit de relevant pentru Republica Moldova. Această secțiune pune bazele înțelegerii subiectului. Înțelegerea modului în care funcționează sistemul este primul pas pentru a înțelege de ce manipularea are succes.

2 Partea a II-a definește operațiunile informaționale – obiectivele lor strategice, actorii care le desfășoară și diferența dintre manipulare și comunicarea legitimă. Aceasta vă oferă instrumentele conceptuale necesare pentru a distinge sursele legitime de informații de manipulare.

3 Partea a III-a analizează tacticile specifice utilizate în cadrul operațiunilor informaționale și narațiunile cel mai frecvent promovate împotriva Republicii Moldova. De asemenea, oferă îndrumări practice pentru identificarea manipulării.

4 Partea a IV-a abordează influența tot mai mare a inteligenței artificiale. Tehnologia evoluează rapid, iar niciun ghid nu o poate surprinde în întregime. Această secțiune oferă o introducere practică în subiect: cum arată conținutul generat de inteligența artificială, de ce este important, cum poate fi utilizat în scopuri manipulative și cum vă puteți proteja împotriva acestuia.

5 Partea a V-a se concentrează pe dezvoltarea abilităților practice și a obiceiurilor cotidiene care vă consolidează reziliența în fața manipulării.

6 Partea a VI-a vă oferă instrumentele necesare pentru a continua să învățați. Reziliența nu este

ceva ce se dobândește o singură dată, ci un proces care necesită practică. Această secțiune prezintă jocuri care vă permit să experimentați tacticile de manipulare din interior și reunește o selecție a celor mai bune resurse gratuite pentru verificarea informațiilor, educație media și menținerea la curent cu informațiile.

7 Partea a VII-a trece de la conștientizare la acțiune. Veți face cunoștință cu „Elfii lituanieni” – o mișcare care a început cu mai puțin de 50 de persoane ce au ripostat împotriva dezinformării și s-a transformat într-o rețea de mii de oameni din întreaga Europă. Veți descoperi măsuri concrete pe care le puteți lua chiar de astăzi, de la raportarea dezinformării până la inițierea unor discuții cu familia. De asemenea, veți învăța practici de igienă digitală care vă ajută să rămâneți în siguranță atunci când participați activ în mediul online, deoarece, dacă doriți să fiți vizibili online, trebuie mai întâi să vă protejați.

Exerciții practice

Pe parcursul acestui manual veți găsi exerciții practice concepute pentru a vă ajuta să puneți în aplicare ceea ce ați învățat – să identificați manipularea, să verificați sursele și să recunoașteți argumentele de rea-credință. Fiecare exercițiu poate fi realizat individual sau împreună cu prietenii, colegii de clasă ori familia. Nu este necesar să fiți experți – aveți nevoie doar de câteva minute și de dorința de a exersa.

De reflectat

Veți găsi, de asemenea, întrebări de reflecție, marcate prin simbolul unui bec. Acestea vă invită să faceți o pauză și să reflectați asupra unei întrebări, să puneți sub semnul întrebării o presupunere sau să observați ceva despre propriile obiceiuri.

Cazuri reale, lecții reale

Exemplele din acest manual provin din cazuri reale din Republica Moldova – videoclipuri false, documente falsificate și rețele coordonate. Folosim exemple reale deoarece manipularea și influența străină ostilă nu sunt fenomene abstracte: ele v-au vizat deja pe voi, comunitatea voastră și țara voastră. Unele exemple vi se pot părea familiare. Altele v-ar putea surprinde. Toate au fost alese pentru a ilustra instrumente și tehnici pe care este probabil să le întâlniți din nou.

Înțelegerea mediului informațional



Partea 1

Istoria surselor de informare: de la Gutenberg la TikTok

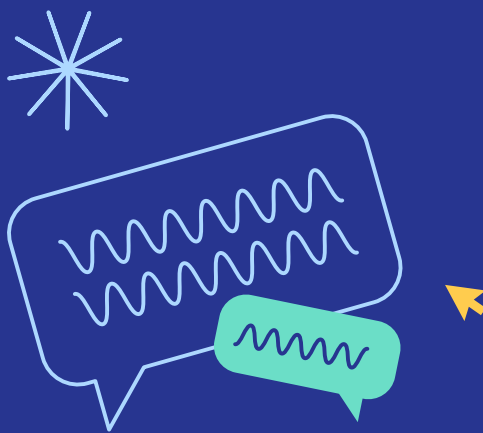
În paragrafele următoare este prezentată o scurtă trecere în revistă a revoluțiilor tehnologice care au transformat profund modul în care este consumată informația. Aceste revoluții nu au avut loc în mod izolat, ci au fost strâns legate de organizațiile care dețineau controlul asupra informației în perioada în care acestea s-au produs.

Invenția tiparului în secolul al XV-lea a făcut ca textul scris, ca sursă de informare, să devină accesibil publicului larg și a stimulat alfabetizarea în rândul populației, contribuind la creșterea numărului de cititori. Acest lucru a permis dezvoltarea presei cotidiene și accesul publicului la informații în fiecare zi. Cu toate acestea, puterea asociată controlului asupra informației era concentrată în mâinile celor care dețineau mijloacele de tipărire – atât factori tehnici, precum tehnologia tiparului, cât și factori sociali, care includeau nu doar competențele și cunoștințele necesare utilizării acestei tehnologii, ci și controlul asupra informațiilor care urmau să fie tipărite.

Radioul, iar mai târziu televiziunea, au revoluționat secolul al XX-lea, transformând comunicarea într-un fenomen cu adevărat de masă. Informația a devenit accesibilă și persoanelor care nu știau să citească, iar consumul de informații a căpătat o nouă dimensiune, aceea de a fi împărtășit simultan de grupuri largi de oameni. Acest lucru a deschis calea unor transformări culturale majore și a făcut ca divertismentul să devină parte a vieții de zi cu zi. Informația a început să circule mai rapid, iar influența celor care controlau accesul la radio și televiziune s-a amplificat atât în plan politic, cât și comercial.

Sectorul publicitar a cunoscut o dezvoltare fără precedent. Pe măsură ce canalele media și programele s-au diversificat pentru diferite grupuri țintă, furnizorii de bunuri și servicii au început, la rândul lor, să utilizeze mecanisme de bază de direcționare a mesajelor. Odată cu dezvoltarea mass-mediei, puterea asociată informației a început să se deplaseze dinspre zone clar delimitate către o gamă tot mai diversă de actori. În această etapă, relația dintre posturile de radio și televiziune și publicul lor a modelat modul în care informația era concepută și consumată.

Apariția internetului a declanșat o nouă transformare majoră a mediului informațional, oferind consumatorilor de informații mai multă libertate de alegere și posibilitatea de a-și face auzită vocea. Odată cu popularizarea blogurilor și a rețelelor sociale, tot mai mulți oameni au început să modeleze mediul informațional atât pentru ei înșiși și comunitățile lor, cât și pentru numeroși alți utilizatori din întreaga lume. Ca urmare a acestor transformări, **mediul informațional a devenit extrem de fragmentat**, fiecare persoană construindu-și propriul ecosistem informațional, alcătuit din aplicațiile pe care le utilizează, canalele preferate și paginile sau grupurile pe care le urmărește.



Cum ajung informațiile la voi

Înainte ca rețelele sociale să devină o sursă importantă de informare pentru mulți oameni, accesul la știri era relativ simplu: cumpărați un ziar, porniți televizorul la o anumită oră sau ascultați radioul. Redactorii acestor instituții media decideau ce era important și ce urma să fie relatat. Majoritatea oamenilor primeau, în linii mari, aceleași informații ca și vecinii lor.

Astăzi, informațiile ajung la noi în principal prin intermediul fluxurilor din rețelele sociale, al aplicațiilor de mesagerie și al platformelor online. Sistemele și algoritmii care stau la baza acestor platforme și care modelează aceste fluxuri au schimbat fundamental atât modul în care oamenii primesc informații, cât și tipul de informații la care au acces.

De la editori la algoritmi

În modelul tradițional, editorii umani acționau ca gardieni ai informației. Ei decideau care știri erau importante, verificau faptele și își asumau responsabilitatea pentru ceea ce publicau. Platformele online funcționează însă după o logică diferită. În locul editorilor, algoritmii decid ce vedeți și ce informații primiți. Aceștia sunt sisteme matematice complexe care vă analizează comportamentul și preferințele – pe ce dați clic, cât timp urmăriți un anumit conținut, ce distribuiți și cu cine interacționați – și vă afișează conținut conceput pentru a vă menține activi pe platformă.

Algoritmul nu se întreabă: „Este acest lucru adevărat?” sau „Este important ca cetățenii să știe acest lucru?”. El se întreabă: „Îl va determina acest conținut pe utilizator să rămână pe platformă?”.

Concepute pentru implicare, nu pentru acuratețe

Platformele de socializare obțin venituri din publicitate, iar aceste venituri depind de atenția și implicarea utilizatorilor. Cu cât utilizatorii petrec mai mult timp pe platformă, cu atât văd mai multe reclame, iar compania obține venituri mai mari. Fiecare funcție a platformei este optimizată pentru a maximiza timpul petrecut de utilizatori pe aceasta.



De reflectat

Una dintre cele mai eficiente modalități prin care platformele îi mențin pe utilizatori implicați este o funcție integrată în aproape fiecare aplicație de socializare: **derularea infinită**. Pe măsură ce derulați în jos, aplicația încarcă tot mai mult conținut. Nu ajungeți niciodată la capăt – teoretic, ați putea derula la nesfârșit. Iar conținutul continuă să apară, indiferent dacă vă îmbunătățește starea de spirit sau, dimpotrivă, v-o afectează. Acest fenomen este atât de răspândit încât are propriul nume: **doomscrolling** – obiceiul compulsiv de a consuma un flux continuu de știri negative și conținut tulburător, fără a vă putea opri, chiar dacă acest lucru vă lasă anxioși, furioși sau epuizați.

Acum, luați-vă un minut pentru a reflecta: cum ar fi diferită experiența voastră dacă ar trebui

să dați clic pe un buton pentru a încărca mai mult conținut de fiecare dată când vedeți câteva postări? Ați petrece la fel de mult timp în aplicație? Ați trece la o altă activitate care necesită mai puțin efort și vă captează mai mult atenția?

Acest lucru nu este întâmplător – platformele sunt concepute să funcționeze astfel.

Acest lucru creează o problemă structurală. Cercetările⁷ au demonstrat în mod constant că informațiile care provoacă emoții puternice, precum frica sau furia, se răspândesc mai rapid și ajung la un public mult mai larg decât relatările atente și bazate pe fapte. Afirmările senzaționale sunt distribuite mai ușor decât analizele bine argumentate, iar postările despre conflicte sau situații dramatice atrag mai multă atenție.

Platformele nu răspândesc în mod deliberat informații false. Cu toate acestea, ele au construit sisteme în care conținutul cu o puternică încărcătură emoțională beneficiază în mod sistematic de un avantaj față de conținutul exact și bazat pe fapte.



Feed-ul vostru este unic – la fel ca al tuturor celorlalți

Un aspect al acestei situații este ușor de trecut cu vederea: informațiile pe care le vedeți nu sunt aceleași cu cele pe care le văd ceilalți. Feed-ul vostru este personalizat pe baza comportamentului vostru anterior, a conexiunilor voastre, a locației voastre și a sute de alte date.

Chiar și în cadrul aceleiași familii, puteți vedea știri complet diferite – povești diferite, perspective diferite și versiuni diferite ale aceluiași eveniment. Astfel, atunci când vă așezați să discutați despre ceea ce se întâmplă, este posibil să nu fiți de acord nici măcar asupra aspectelor esențiale. Nu pentru că cineva minte. Pur și simplu, ați trăit în lumi informaționale sau în „bule” informaționale diferite.

Această personalizare are avantaje – vedeți conținut relevant pentru interesele voastre. Dar înseamnă, totodată, că feed-ul vostru vă va afișa rareori postări care să vă facă să vă opriți și să vă întrebați: „Stați puțin... chiar este adevărat? Oare asta pune sub semnul întrebării ceea ce cred?”. În timp, acest lucru creează ceea ce cercetătorii numesc **„bule de filtrare” sau „camere de ecou”** – medii în care vedeți, în principal, conținut care confirmă ceea ce credeți deja, în timp ce informațiile contradictorii pur și simplu nu ajung la voi. Acest lucru poate crea impresia falsă că „toată lumea este de acord” cu opiniile voastre, când, în realitate, vedeți doar o mică parte a conversației. Pentru cei care încearcă să manipuleze opinia publică, această fragmentare reprezintă o oportunitate. Ei pot viza grupuri specifice cu mesaje personalizate, fiind siguri că ceilalți nu vor vedea ceea ce se răspândește.

Problema vitezei

Informațiile circulă astăzi într-un ritm căruia judecata umană cu greu îi poate ține pasul. O informație falsă poate circula la nivel global în timp ce verificarea faptelor este încă în desfășurare. Până când verificatorii de fapte publică o corectare, milioane de oameni au văzut și au distribuit deja informația inițială.

Această viteză influențează și modul în care procesăm informațiile. Pe măsură ce derulați feed-ul, luați rapid decizii cu privire la ceea ce să credeți, să distribuiți sau să ignorați. Rareori vă opriți pentru a verifica sursele sau a confirma informațiile. Platformele sunt concepute pentru consum rapid, nu pentru o evaluare atentă.

Înțelegerea acestui peisaj informațional – cum funcționează, de ce funcționează astfel și ce vulnerabilități creează – reprezintă baza pentru a vă orienta mai eficient în acest peisaj informațional.



De reflectat

Există o zicală populară: „*O minciună face jumătate din înconjurul lumii înainte ca adevărul să-și pună cizmele.*”

Puneți-vă în pielea unui detectiv online. Cine a spus pentru prima dată aceste cuvinte? Winston Churchill? Scriitorul Terry Pratchett? Sau cu totul altcineva?

Încercați să aflați. Căutați citatul și vedeți ce descoperiți. (Indiciu: răspunsul s-ar putea să vă surprindă, iar căutarea în sine este un exercițiu util pentru a urmări originea informațiilor).⁸

Cine se află cu adevărat în spatele conținutului pe care îl vedeți?

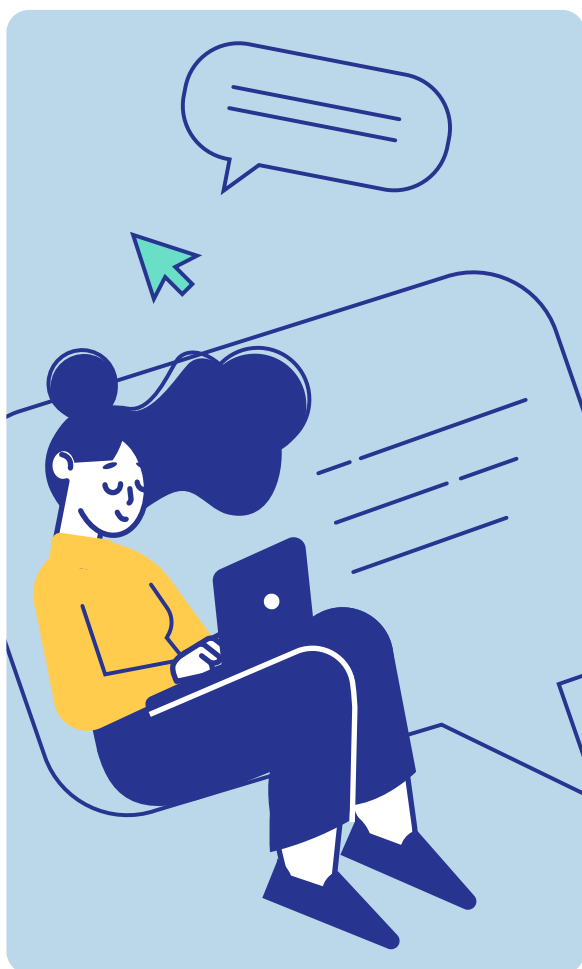
Algoritmii rețelelor sociale nu sunt singura modalitate prin care informațiile sunt distorsionate. În Republica Moldova, la fel ca în alte țări, manipularea are loc și prin canale mai familiare.

Unele **posturi de televiziune și instituții media** sunt deținute sau controlate de diferiți actori interni, inclusiv de persoane cu influență politică, ori servesc interese străine ostile, fără ca acest lucru să fie întotdeauna evident. O emisiune de știri poate părea independentă, deși, în realitate, promovează agenda altcuiva. De exemplu, un post de televiziune poate relata pe larg fiecare scandal care implică un anumit partid politic, ignorând în același timp probleme similare din cadrul altui partid. Dacă nu știți cine deține o instituție media, nu știți ale cui interese le servește.

Instituțiile media străine controlate și finanțate de stat reprezintă un alt factor. Diverse țări, inclusiv Rusia, încearcă să răspândească dezinformare și să manipuleze spațiul informațional prin crearea unui ecosistem de mesaje globale finanțate de stat, în care reprezentanții regimului transmit mesaje la unison cu instituțiile media, organizațiile și intermediarii lor din mediul online și offline. În unele cazuri, actorii externi pot încerca să utilizeze subiecte sensibile, precum religia, identitatea, valorile familiale sau tradiția, pentru a răspândi mesaje politice. Acest lucru nu înseamnă că religia sau credincioșii reprezintă problema. Înseamnă că orice spațiu bazat pe încredere poate fi instrumentalizat atunci când oamenii sunt atașați emoțional de acesta. Acest ecosistem de actori, instituții media și canale de socializare prezintă lumea din perspectiva Kremlinului. Atunci când o emisiune-dezbateri din Rusia discută despre parcursul Republicii Moldova către Uniunea Europeană, nu este vorba despre o analiză neutră, ci despre un conținut conceput pentru a servi obiectivelor politicii externe a Rusiei. Aflați mai multe pe platforma EUvsDisinfo.⁹

În plus, există persoane care par a fi cetățeni obișnuiți (**creatori de conținut**) și își împărtășesc opiniile online, dar care, de fapt, sunt plătite să răspândească anumite mesaje. Spre deosebire de conturile false de pe rețelele sociale, acestea sunt persoane reale, cu profiluri autentice, ceea ce le face mai greu de identificat și mai convingătoare. Ele ar putea publica un mesaj de genul: „Obișnuiam să susțin Uniunea Europeană, dar acum văd adevărul...”. Povestea lor pare personală și autentică. Însă, în același timp, zeci de alte conturi publică povești „personale” aproape identice.¹⁰

Ideea este simplă: manipularea nu necesită tehnologie avansată. Ea poate proveni de la un post de televiziune pe care familia voastră îl urmărește de ani de zile, de la un site local de știri cu o structură de proprietate neclară sau de la cineva din mediul online care pare autentic, dar nu este.



De ce este important acest lucru

Atunci când oamenii nu mai împărtășesc o înțelegere comună a realității, familiile ajung mai ușor să se certe, colegii de clasă se împart în tabere ostile, comunitățile devin suspicioase, iar statul devine mai greu de apărut. Manipularea nu schimbă doar opiniile. Ea schimbă relațiile, încrederea și comportamentul. Informațiile pe care le vedeți în fiecare zi nu rămân doar pe ecran. Ele modelează modul în care oamenii înțeleg lumea, iau decizii și câtă încredere au în instituțiile publice sau în stat. Atunci când informațiile sunt manipulate, poate fi afectat chiar și modul în care funcționează democrația.

Oamenii vor avea întotdeauna opinii diferite cu privire la valori, priorități și politici – această diversitate de opinii este firească și necesară. Însă un dezacord constructiv necesită o bază factuală comună. Atunci când o parte semnificativă a populației funcționează pe baza unor seturi complet diferite de „fapte”, deliberarea democratică devine extrem de dificilă. Dezbaterile ajung într-un impas, deoarece participanții nu discută, în realitate, despre aceeași realitate. Situația este cu atât mai problematică atunci când funcționarii publici contestă faptele, lăsând adesea cetățenii într-o stare de confuzie.



Joe Biden ✓
@JoeBiden

Schimbările climatice sunt reale, apropo.

3:32 AM 24 august 2023

* 25,6 milioane de vizualizări

Sursă: X.com¹¹ și TruthSocial¹² (mesaje traduse în română, originalul în engleză)

Acest lucru nu reprezintă o preocupare pur teoretică. Cercetătorii din Europa și din întreaga lume au documentat creșterea polarizării, diminuarea încrederii în instituții și fragmentarea spațiului informațional comun. Unele țări resimt aceste presiuni mai puternic decât altele, în special cele care traversează tranziții geopolitice, gestionează un peisaj mediatic divers sau se confruntă cu ingerințe din partea actorilor externi.

Republica Moldova: un spațiu informațional disputat

Republica Moldova se află într-un mediu informațional deosebit de complex. Fiind o țară care își urmează parcursul european și gestionează, în același timp, relații complexe cu vecinii săi, Republica Moldova a devenit un punct de convergență al influențelor concurente. Totodată, societatea moldovenească a devenit tot mai conștientă de aceste provocări și tot mai activă.

Spațiul informațional al Republicii Moldova este vulnerabil din mai multe motive. Țara are o piață media de dimensiuni reduse, iar multe instituții media independente se confruntă cu dificultăți



Donald J. Trump ✓
@realDonaldTrump

Se așteaptă ca un val de frig record să lovească 40 de state. Rar s-a mai văzut așa ceva până acum. Ar putea insurecționistii de mediu să explice - CE S-A ÎNTÂMPLAT CU ÎNCĂLZIREA GLOBALĂ???

8.560 ReTruths

32.500 Aprecieri

23 ianuarie 2026, 13:19



financiare. Nu toată lumea are acces egal la jurnalism de calitate. Acest lucru creează condiții favorabile pentru răspândirea mai ușoară a conținutului înșelător și a manipulării. În unele regiuni, precum Găgăuzia și Transnistria, oamenii consumă în mare măsură conținut de televiziune și online din străinătate, care reflectă adesea interese politice din afara țării.¹³ Faptul că Republica Moldova este vizată nu înseamnă că este o țară slabă.

Un pilon esențial al cadrului de consolidare a rezilienței societale a Republicii Moldova este **Indicele Național de Reziliență Informațională**, un instrument conceput pentru a „măsura temperatura” societății în raport cu cinci priorități esențiale de securitate națională: integrarea europeană, coeziunea socială, reziliența economică, consolidarea sectorului de apărare și securitatea regională¹⁴. Centrul instituțional de coordonare a acestor activități este **Centrul pentru Comunicare Strategică și Combaterea Dezinformării**, care coordonează analiza tacticilor utilizate de actorii ostili, emite alerte de răspuns rapid și elaborează orientări strategice pentru instituțiile publice. Totuși, punerea în aplicare a acestor măsuri nu revine exclusiv Centrului, ci este realizată prin grupuri multisectoriale mixte care funcționează potrivit principiului implicării întregii societăți, reunind instituții ale statului, organizații ale societății civile, instituții media independente, experți din mediul academic și parteneri internaționali¹⁵. Jurnaliștii independenți, verficatorii de fapte, profesorii, organizațiile societății civile și cetățenii joacă deja un rol important în identificarea informațiilor false și în explicarea clară a subiectelor complexe. Școlile și programele dedicate tinerilor dezvoltă tot mai mult competențele de educație media și gândire critică. În plus, de fiecare dată când oamenii verifică informațiile, pun sub semnul întrebării conținutul suspect și evită să răspândească panică sau ură, ei contribuie la consolidarea rezilienței comunităților lor și reduc impactul informațiilor false.

Limba joacă, de asemenea, un rol important. În Republica Moldova există instituții media atât în limba română, cât și în limba rusă. Nu limba în care consumați informațiile este problema, ci

calitatea sursei, transparența privind autorul și originea conținutului, precum și scopul mesajului. Informațiile pot fi corecte sau manipulative în orice limbă. Ca urmare, diferite grupuri din societate, de exemplu persoane care locuiesc în regiuni diferite, pot consulta surse diferite și pot primi versiuni diferite ale aceleiași știri. Acest lucru poate crea bule informaționale paralele, poate accentua polarizarea și poate îngreuna comunicarea eficientă a instituțiilor publice, în special în timpul alegerilor sau al unor decizii politice majore. În același timp, accesul la limbi și perspective diferite poate reprezenta un avantaj, dacă oamenii învață să compare critic sursele și să fie deschiși la dialog cu perspective diferite.

Alfabetizarea informațională ca competență civică

Capacitatea de a distinge între ceea ce este adevărat, ceea ce este înșelător și ceea ce este manipulator nu este utilă doar pentru voi, la nivel individual – este o competență esențială pentru întreaga societate. Atunci când puneți sub semnul întrebării sursele, verificați faptele și gândiți critic cu privire la ceea ce vedeți în mediul online, nu vă protejați doar pe voi înșivă. Contribuiți și la faptul că comunitatea voastră rămâne bine informată și rezilientă.

De aceea, competențele prezentate în acest manual depășesc sfera protecției individuale. Atunci când învățați să vă orientați eficient în mediul informațional și îi sprijiniți și pe alții să facă același lucru, contribuiți la un obiectiv mai amplu: întărirea capacității societății voastre de a lua decizii autentice și informate cu privire la propriul viitor.

De ce funcționează manipularea

Este important să înțelegem cum funcționează platformele. Însă manipularea nu funcționează doar din cauza algoritmilor. Ea reușește și pentru că exploatează emoțiile și reacțiile umane: frica, furia, nevoia de apartenență, curiozitatea, loialitatea și nevoia de a lua decizii rapide. De asemenea, trebuie să înțelegem de ce manipularea este atât de eficientă, chiar și în cazul unor persoane inteligente și educate. Răspunsul se află în modul în care funcționează creierul nostru și în felul în care

sunt concepute platformele online de astăzi. Acest lucru este important deoarece manipularea apare adesea în locuri familiare: videoclipuri de pe TikTok, canale de Telegram, clipuri de pe YouTube, postări pe Facebook, meme-uri, comentarii sau mesaje pe Viber distribuite de rude. Aceste exemple pot părea obișnuite, însă sunt adesea concepute pentru a vă determina să reacționați înainte de a gândi.



► Vulnerabilitate

Declanșatori emoționali

● Cum funcționează

Creierul nostru reacționează la amenințări și la indignare înainte de a gândi. Frica, furia și indignarea morală ocolesc analiza rațională. Distribuim înainte de a verifica.

● Cum este exploatată

Manipulatorii concep titluri șocante și mesaje care sugerează amenințări la adresa identității. Cercetările¹⁶ arată că 75% dintre oameni nu citesc mai mult decât titlurile de pe rețelele sociale și distribuie linkuri fără să le acceseze.

● Ce puteți face

Opriti-vă înainte de a distribui. Dacă ceva vă provoacă furie sau teamă, tocmai atunci este momentul să încetiniți ritmul. Întrebați-vă: De ce mă afectează atât de puternic acest lucru? Încearcă cineva să mă determine să reacționez înainte de a gândi? Respirați adânc, verificați sursa și distribuiți informația numai după ce ați verificat-o.

● Exemplu din Republica Moldova

Un videoclip de pe YouTube care avertizează că „UE înseamnă război”, conceput pentru a stârni emoții negative față de Uniunea Europeană.



Sursă: YouTube¹⁷

Nimic din toate acestea nu este un semn de slăbiciune personală. Sunt reacții firești ale oamenilor, care i-au ajutat să supraviețuiască timp de mii de ani: reacția la pericol, încrederea în vocile familiare, tendința de a urma grupul și folosirea scurtăturilor de gândire atunci când suntem copleșiți de prea multe informații. Astăzi, aceste reacții pot fi exploatate în mediul online.

Vestea bună este că ele pot fi gestionate în mod conștient. Atunci când vă opriți o clipă înainte de a distribui ceva, verificați sursa, comparați informațiile și vă întrebați ce încearcă un mesaj să vă facă să simțiți sau să faceți, deveniți mai greu de manipulat.

Provocările pe care le-am analizat sunt serioase, dar le puteți face față. Cu informațiile și cunoștințele potrivite, vă puteți proteja împotriva manipulării și îi puteți ajuta și pe prietenii voștri să facă același lucru. Acest manual este conceput pentru a vă ajuta să faceți trei lucruri: să recunoașteți manipularea, să vă protejați și să-i sprijiniți și pe alții.

Scopul nu este să vă facă suspicioși față de orice sau cinici în privința tuturor informațiilor. Societățile sănătoase au nevoie de încredere – în instituții, în mass-media și unii în alții. Ideea este ca această încredere să fie una informată, nu naivă, și să vă ofere instrumentele necesare pentru a face diferența între sursele demne de încredere și cele care încearcă să o exploateze.



► Vulnerabilitate

Părtinirea de confirmare

► Cum funcționează

Preferăm informațiile care confirmă ceea ce credem deja. Respingem informațiile care ne contrazic convingerile.

► Cum este exploatată

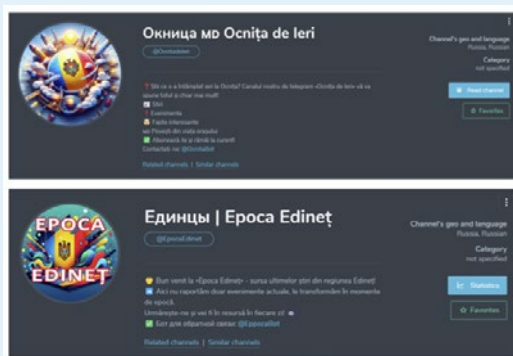
Algoritmii amplifică această tendință, arătându-vă tot mai mult conținut asemănător cu cel pe care îl apreciați deja. Rezultatul: bule de filtrare în care convingerile voastre se consolidează, iar cei care au alte opinii ajung să vi se pară de neînțeles.

► Ce puteți face

Căutați în mod activ surse care vă pun sub semnul întrebării convingerile – nu pentru a vă schimba opiniile, ci pentru a vă testa raționamentul. Urmăriți cel puțin o instituție media de investigație credibilă cu ale cărei concluzii nu sunteți întotdeauna de acord. Atunci când constatați că sunteți de acord cu tot ceea ce citiți sau auziți, întrebați-vă: „Învăț ceva nou sau doar îmi sunt confirmate convingerile?”

► Exemplu din Republica Moldova

DFRLab a documentat 39 de canale Telegram create în mai 2024, fiecare purtând numele unei unități administrative din Republica Moldova (Bălți, Cahul, Orhei etc.). Deși păreau a fi canale ale comunităților locale, acestea erau coordonate centralizat din Rusia și publicau conținut anti-UE identic. Utilizatorii credeau că citesc știri locale, însă, în realitate, se aflau într-o cameră de ecou creată artificial.



Sursă: DFRLab¹⁸

**Cum funcționează**

Atunci când suntem nesiguri, tindem să ne orientăm după ceilalți. Dacă „toată lumea” pare să creadă ceva, avem tendința să îi urmăm sau să rămânem tăcuți dacă nu suntem de acord. Acest fenomen este deosebit de puternic în mediul online, deoarece comentariile, aprecierile, distribuirile și mesajele repetate pot crea impresia că aceasta este opinia majorității, chiar și atunci când numărul real al persoanelor implicate este redus.

Cum este exploatată

Persoane plătite se prezintă drept oameni obișnuiți și creează conținut amplificat de boți și rețele coordonate. Rezultatul este un consens fabricat, iar vocile reale care exprimă opinii diferite se pierd în zgomotul informațional.

O atenționare: Narațiunea „vocilor reduse la tăcere” este, la rândul ei, uneori exploatată. Unele mișcări politice susțin cu insistență că sunt reduse la tăcere pe rețelele sociale, deși se numără printre cele mai eficiente în utilizarea acestor platforme. Opiniile puternice nu reprezintă automat o formă de manipulare. Oamenii pot avea, în mod sincer, opinii diferite. Manipularea începe atunci când cineva își ascunde identitatea, folosește dovezi false, creează o popularitate artificială sau încearcă să provoace frică și ură în loc să îi ajute pe oameni să înțeleagă.

Ce puteți face

Rețineți că impresia unui sprijin larg poate fi creată artificial. Înainte de a presupune că „toată lumea” este de acord, uitați-vă cine vorbește. Sunt persoane reale, cu istorii autentice, sau conturi anonime create luna trecută? Verificați profilurile, căutați tipare și întrebați-vă: este aceasta o mișcare civică autentică sau o înscenare, finanțată de cineva?

Exemplu din Republica Moldova

Înainte de referendumul din octombrie 2024 din Republica Moldova, oligarhul Ilan Șor a lansat pe Telegram un chatbot numit „STOP UE” (СТОП ЕС), care recruta „ambasadori” pentru a răspândi conținut anti-UE. Șor a afirmat că „peste 800 000 de patrioți” s-au alăturat inițiativei, însă datele disponibile indicau doar aproximativ 20 000 de utilizatori. Între timp, participanții plățiți primeau până la 280 de dolari pentru a publica conținut anti-UE pe Facebook și pentru a recruta alte persoane. Acesta este un exemplu clar de consens fabricat.

Sursă: DFRLab¹⁹



Cum funcționează

Prea multe informații, prea puțin timp. Ne bazăm pe scurtături de gândire: surse familiare, indicii emoționale și afirmații care corespund așteptărilor noastre.

Cum este exploatată

Manipulatorii exploatează aceste scurtături de gândire. Simpla cantitate uriașă de conținut face imposibilă verificarea tuturor informațiilor – iar ei știu acest lucru.

Ce poți face

Nu poți verifica totul și nici nu este nevoie. Concentrați-vă asupra a ceea ce contează: înainte de a distribui ceva care i-ar putea influența pe alții, acordați-vă timp pentru a verifica informația. Limitați-vă consumul de știri la câteva surse de încredere, în loc să derulați la nesfârșit. A vă proteja atenția și a vă limita expunerea la surse dubioase înseamnă, în fond, a vă proteja pe voi înșivă.

Exemplu din Republica Moldova

În săptămânile premergătoare alegerilor din octombrie 2024 din Republica Moldova, WatchDog.MD a identificat aproximativ 200 de teme distincte de dezinformare care circulau prin surse afiliate Rusiei. Afirmațiile erau adesea contradictorii: terenurile agricole urmau să fie vândute străinilor, Biserica Ortodoxă urma să fie închisă, Republica Moldova urma să fie atrasă în războiul din Ucraina, vorbitorii de limbă rusă urmau să fie marginalizați, țara urma să se reunifice cu România, iar școlile urmau să introducă obligatoriu „educația LGBT”. Expert Forum a identificat 100 de conturi neautentice de TikTok care au generat 13,9 milioane de vizualizări într-o singură lună. Scopul nu era să convingă, ci să epuizeze.²⁰

POTENTIAL CIB

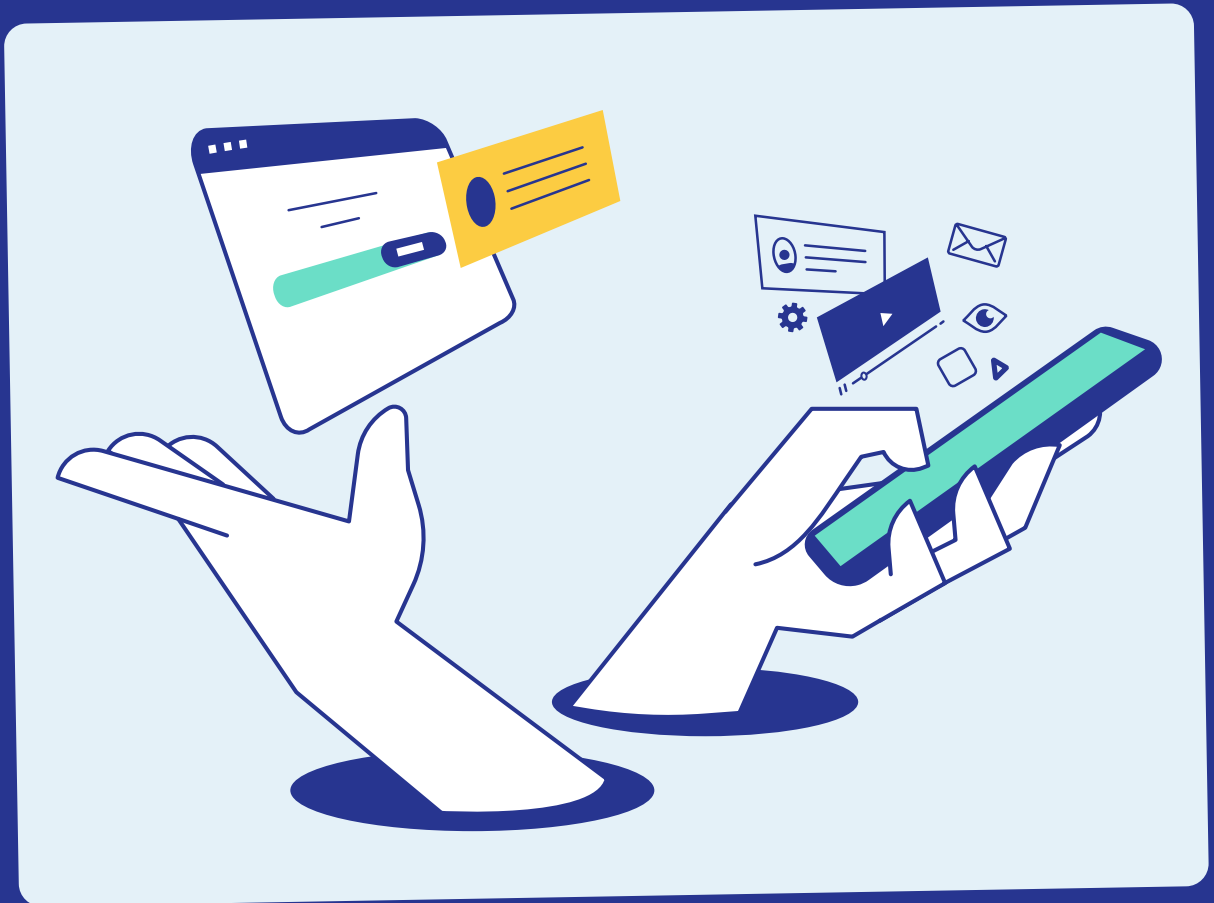
5 August - 4 September 2025

Republic of Moldova



O metodă frecvent utilizată pentru a exploata aceste vulnerabilități este comportamentul neautentic coordonat. Acesta presupune ca numeroase conturi false, anonime sau înșelătoare să acționeze împreună pentru a răspândi același mesaj, ascunzând în același timp cine se află cu adevărat în spatele lor. Scopul este ca manipularea să pară o expresie autentică a opiniei publice. Comportamentul neautentic coordonat (CIB) reprezintă eforturi organizate, deliberate și manipulative de a induce publicul în eroare prin utilizarea mai multor conturi false sau neautentice. În general, acesta implică rețele de conturi și pagini care acționează împreună pentru a răspândi anumite mesaje sau pentru a desfășura acțiuni coordonate, ascunzând în același timp caracterul coordonat și neautentic al acestor activități. Operațiunile de tip CIB se bazează pe utilizarea pe scară largă a tacticilor și tehnicilor de manipulare.²¹

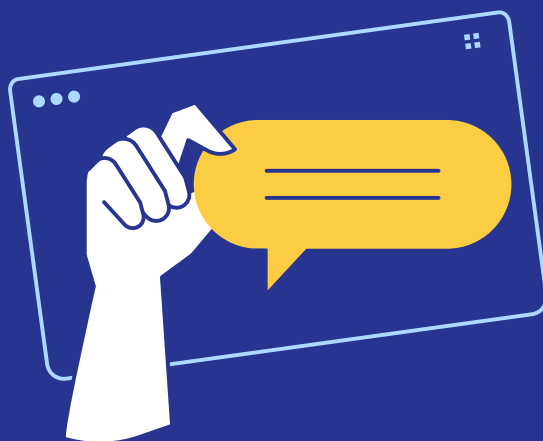
Ce sunt operațiunile de informare?



Partea 2

Oamenii au încercat dintotdeauna să se influențeze și să se manipuleze unii pe alții. Ceea ce este nou astăzi este viteza, amploarea și gradul de coordonare al manipulării. Platformele online, conturile false, inteligența artificială, creatorii de conținut, canalele anonime și rețelele susținute din străinătate pot fi utilizate împreună pentru a modela ceea ce comunități întregi cred, se tem, în cine au încredere sau ce resping. Acest fenomen este cunoscut sub denumirea de **operațiuni de informare**.

O operațiune de informare sau de influențare este mai mult decât o simplă minciună. Ea reprezintă un efort coordonat de a influența modul în care oamenii gândesc, simt sau acționează. De regulă, combină mai multe tactici: conturi false sau anonime, conținut fabricat, manipulare emoțională, titluri înșelătoare, creatori de conținut remunerați, boți, utilizarea selectivă a faptelor sau amplificarea coordonată a mesajelor. Scopul nu este întotdeauna acela de a-i determina pe oameni să creadă o anumită informație falsă. Uneori, scopul este de a crea confuzie, de a polariza comunitățile, de a reduce încrederea în instituții, de a descuraja participarea la vot sau de a face societatea să se simtă divizată și lipsită de putere.



Termeni-cheie pe care trebuie să-i cunoașteți

Acest manual se concentrează asupra operațiunilor de informare. Totuși, în mass-media, în dezbaterile politice și în conversațiile de zi cu zi sunt utilizați adesea interschimbabil mai mulți termeni înrudiți: „știri false”, „propagandă”, „dezinformare”, „informare eronată”, „război informațional”, „manipulare și interferență informațională străină” și alții. În continuare, explicăm acești termeni pentru a evidenția diferențele dintre ei.

Știri false

Acest termen a devenit popular în jurul anului 2016 și descria inițial materiale fabricate, concepute să pară produse jurnalistice autentice. Problema este că termenul a devenit rapid o armă politică – o etichetă folosită de politicieni pentru a respinge orice relatare care nu le convine. Atunci când orice poate fi numit „știre falsă”, termenul își pierde utilitatea. În plus, sintagma „știri false” este adesea considerată un oximoron, deoarece reunește două concepte contradictorii: „știri”, care presupun informații verificabile, exacte și de interes public, și „false”, care înseamnă inventate, neadevărate sau înșelătoare²². Din aceste motive, termenul este evitat de comunitatea de experți și de cercetători.

Informare eronată

Conținut fals sau inexact distribuit fără intenția de a provoca un prejudiciu.²³ De exemplu, o instituție media publică din greșeală o informație eronată și o corectează ulterior. Astfel, în 2024, NPR a relatat că veniturile din vânzarea cărților audio s-au ridicat la 2,22 milioane de dolari. În realitate, cifra era de 2,22 miliarde de dolari – de o mie de ori mai mare. A fost o eroare de redactare, nu o minciună. Instituția media a corectat informația imediat ce a observat greșeala.²⁴

Corecție

30 martie 2026

O versiune anterioară a acestei știri afirma în mod eronat că veniturile din vânzările de cărți audio au depășit 2,22 milioane de dolari în 2024. De fapt, acestea au fost de 2,22 miliarde de dolari.

romane de dragoste cărți audio

Captură de ecran a unei corecturi care a apărut sub articol (tradusă în română)²⁵

Dezininformare

Conținut fals sau înșelător creat și distribuit în mod deliberat pentru a provoca prejudicii. Pe scurt, informarea eronată este o greșeală, iar dezinformarea este o minciună folosită ca instrument. Cineva știe că o afirmație este falsă și o distribuie în mod deliberat pentru a induce în eroare, a manipula sau a-și atinge scopul. Diferența esențială față de informarea eronată este intenția.²⁶



Exemplu: Un videoclip deepfake o arăta în mod fals pe președinta Comisiei Electorale Centrale afirmând că Franța s-a amestecat în alegerile din Moldova.²⁷

Malinformare

Informații autentice distribuite cu intenția de a provoca prejudicii²⁸. De exemplu, o fotografie privată divulgată pentru a face de râs o persoană, fapte scoase din context pentru a induce în eroare sau documente confidentiale făcute publice pentru a prejudicia o instituție. Conținutul poate fi autentic, însă scopul este de a provoca prejudicii.

De exemplu, hackeri au sustras conversații private de pe Telegram ale ministrului justiției din Republica Moldova și ale altor oficiali, pe care le-au publicat ulterior pe un site numit „Moldova Leaks”²⁹. Lecția esențială este următoarea: chiar și informațiile adevărate pot fi utilizate în scop manipulator dacă sunt publicate selectiv, scoase din context sau folosite pentru a crea o impresie distorsionată. Mesajele erau autentice, însă au fost divulgate selectiv și scoase din context pentru a crea impresia că oficialii erau corupți. Partidele de opoziție pro-ruse au folosit aceste scurgeri de informații pentru a ataca guvernul proeuropean. Acesta este un exemplu de malinformare: informații autentice, sustrate și utilizate ca instrument pentru a provoca prejudicii.

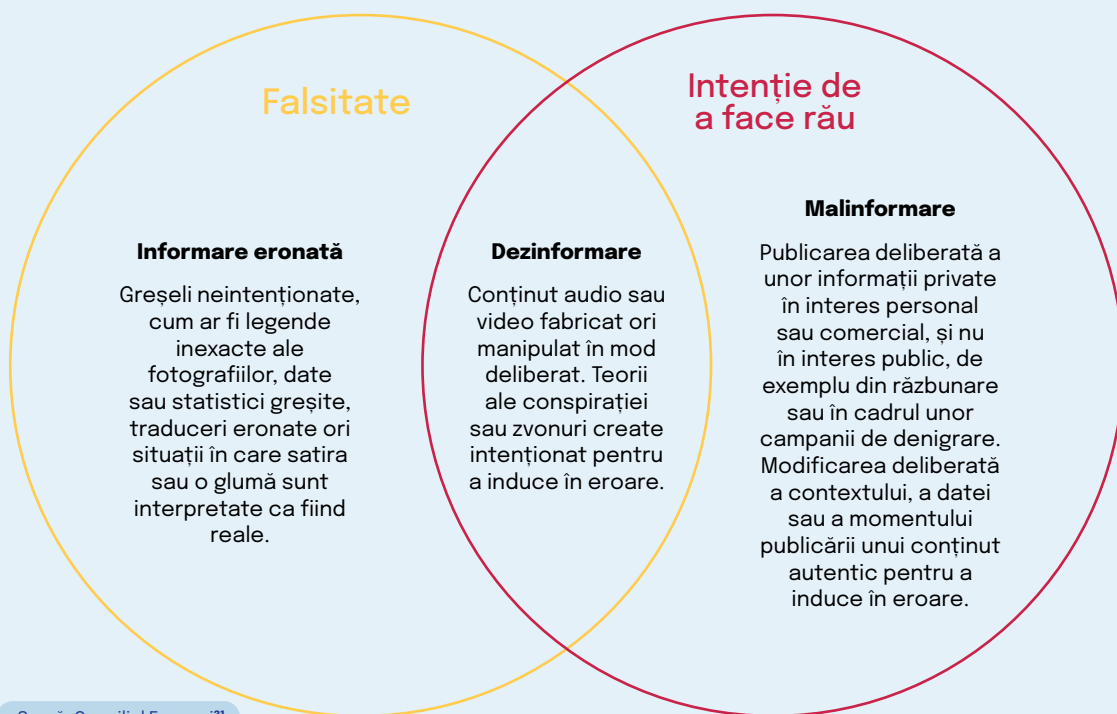


Sursă: Stiri.md³⁰

Pentru a vă ajuta să înțelegeți mai bine diferențele dintre aceste concepte, ilustrația de mai jos prezintă într-un mod simplu cele trei noțiuni conexe, dar distincte, discutate anterior. Cercul din stânga reprezintă conținutul fals, iar cercul din dreapta reprezintă intenția de a provoca prejudicii. Conținutul fals distribuit fără intenția de a provoca prejudicii reprezintă informarea eronată – de exemplu, greșeli făcute din neatenție sau zvonuri

răspândite fără rea-credință. În zona în care cele două cercuri se suprapun, conținutul este atât fals, cât și distribuit în mod deliberat pentru a provoca prejudicii: aceasta este dezinformarea. Cercul din dreapta ilustrează malinformarea – informații adevărate din punct de vedere factual, utilizate cu intenția de a provoca prejudicii, cum ar fi divulgarea unor date private.

Tipuri de tulburări informaționale



Termen

Este fals?

Există intenția de a provoca prejudicii?

Explicație pe scurt

Informare eronată

De regulă, da

Nu

O greșală sau un zvon distribuit fără intenția de a provoca prejudicii.

Dezinformare

Da sau înșelător

Da

O minciună sau o denaturare folosită în mod deliberat.

Malinformare

Nu neapărat

Da

Informații autentice utilizate pentru a provoca prejudicii, a manipula sau a crea o imagine distorsionată.

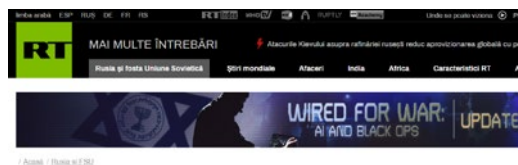
Propaganda

Propaganda este cel mai vechi și mai cuprinzător dintre termenii prezenți. Se referă la orice efort organizat de a promova un anumit punct de vedere, de a modela opinia publică sau de a influența comportamentul. Nu este neapărat bazată pe informații false, însă urmărește în mod deliberat să convingă și prezintă adesea o perspectivă unilaterală. Guvernele, mișcările și instituțiile au folosit propaganda de secole prin discursuri, afișe, radio, televiziune și, în prezent, prin intermediul rețelelor sociale.³²

De exemplu, canalele media finanțate de statul rus, precum RT și Sputnik, au prezentat în mod repetat integrarea europeană a Republicii Moldova în principal ca pe o amenințare. Aceste materiale pot porni de la preocupări economice reale, precum prețurile sau exporturile agricole, însă le prezintă exclusiv dintr-o singură perspectivă: Europa este periculoasă, Rusia oferă protecție, iar Republica Moldova nu poate reuși pe cont propriu.³³ Un reportaj s-ar putea concentra exclusiv asupra creșterii prețurilor în statele membre ale Uniunii Europene și ar putea include interviuri cu fermieri moldoveni îngrijorați de pierderea pieței ruse. Faptele prezentate individual pot fi adevărate, însă

relatarea conduce întotdeauna către aceeași concluzie (a se vedea mai jos captura de ecran a unui articol care prezintă exclusiv aspectele negative ale aderării la Uniunea Europeană). Nu veți vedea RT relatând despre fondurile europene pentru dezvoltare care ajung în Republica Moldova sau analizând corupția din rândul forțelor politice moldovenești aliniate Rusiei.

Aceasta este propaganda: un efort susținut și coordonat de promovare a unui anumit punct de vedere. Termenul descrie metoda – persuasiunea organizată – și nu faptul dacă informațiile prezentate sunt adevărate sau false.



Această țară europeană se pregătește să renunțe la viitorul său pentru un „vis UE”

Odată cu retragerea oficială din CSI, Moldova se confruntă cu presiuni economice și politice tot mai mari, pe fondul unor întrebări nerezolvate privind locul său în Europa.

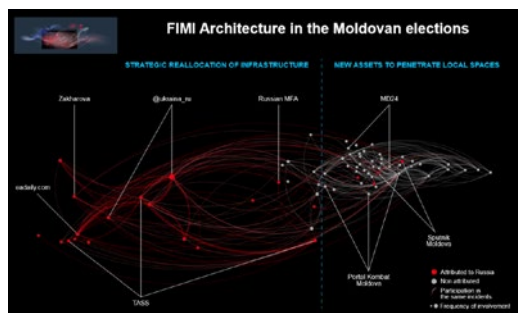
Sursă: captură de ecran de pe RT (tradusă în română)

Manipularea informațiilor și ingerințele străine (MIIS)

Un termen relativ recent introdus de Serviciul European de Acțiune Externă (SEAE)³⁴, serviciul diplomatic al Uniunii Europene. MIIS sau, în engleză, FIMI nu se referă doar la informații false, ci la un ansamblu de comportamente: coordonare, ascunderea identității, manipulare, amplificare artificială, implicarea unor actori străini și intenția de a influența o societate sau un stat. SEAE a dezvoltat acest concept deoarece termenii existenți descriau doar anumite aspecte ale problemei, fără a surprinde în mod adecvat ceea ce Uniunea Europeană trebuia să combată: încercările coordonate ale actorilor străini de a manipula mediul informațional și de a interfera în procesele democratice.

O modalitate simplă de a reține ce înseamnă FIMI este următoarea:

actor străin + comportament ascuns sau manipulator + amplificare coordonată + încercare de a influența societatea sau procesele democratice.



Exemplu: Hartă a rețelei de active asociate manipularea informațiilor și ingerințele străine, afiliate Rusiei, care vizează mediul informațional din Republica Moldova – analiza SEAE.³⁵

Amenințarea hibridă

Probabil ați întâlnit acest termen la televizor, pe internet sau în discuțiile despre securitatea Republicii Moldova. O amenințare hibridă presupune utilizarea coordonată a unor instrumente diferite pentru a slăbi un stat, o instituție sau o societate, fără a recurge neapărat la utilizarea deschisă a forței militare. Manipularea informațiilor – MIIS, propaganda și dezinformarea – reprezintă doar una dintre componentele sale. Însă amenințările hibride sunt mult mai complexe. În general, amenințările hibride constau în activități coordonate și dăunătoare, planificate și desfășurate cu intenția de a provoca prejudicii. Acestea urmăresc să submineze un stat, o instituție sau o altă țintă printr-o combinație de mijloace. Printre acestea se numără manipularea informațiilor, atacurile cibernetice, influența sau constrângerea economică, manevrele politice desfășurate în mod ocult, diplomația coercitivă și amenințările cu utilizarea forței militare. În cazul Republicii Moldova, amenințările hibride pot combina dezinformarea, incidentele cibernetice, presiunile energetice, finanțarea ilegală a activităților politice, încercările de a submina alegerile, rețelele de corupție, polarizarea socială și narațiunile menite să reducă încrederea în stat. Tacticile hibride sunt utilizate atât de actori statali, cât și de actori nestatali (de exemplu, grupări paramilitare, organizații teroriste sau hackeri) și devin tot mai complexe și mai sofisticate. Pe lângă riscurile pe care le generează pentru securitate, acestea reprezintă și o amenințare la adresa democrației, deoarece vizează valorile sale fundamentale și urmăresc să divizeze societatea și să submineze procesul decizional.³⁸

Teoria conspirației

Convingerea că anumite evenimente sau situații sunt manipulate și controlate în secret, din culise, de actori puternici care urmăresc să provoace prejudicii³⁶. O astfel de teorie presupune existența unor planuri ascunse în spatele evenimentelor, stabilește legături între evenimente fără legătură între ele și le prezintă ca fiind intenționate, atribuind adesea responsabilitatea unor persoane sau grupuri.

O afirmație recurentă în mass-media pro-Kremlin susține că miliardarul George Soros o controlează în secret pe președinta Maia Sandu și își folosește fundațiile pentru a impune o agendă ascunsă în Republica Moldova³⁷. Aceasta este o teorie a conspirației deoarece susține că un actor atotputernic trage sforile din culise și, prin însăși natura sa, nu poate fi infirmată. Orice dezmințire este prezentată drept „dovadă” a unei mușamalizări. Totodată, teoria reia vechi clișee antisemite potrivit cărora persoane evreiești influente și înstărite ar controla în secret guvernele. Tocmai de aceea, astfel de

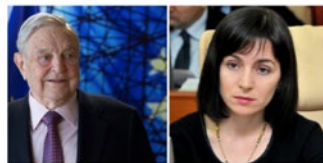
narațiuni sunt periculoase: ele nu doar induc oamenii în eroare cu privire la politică, ci pot alimenta și ura împotriva unor grupuri etnice, religioase sau sociale.

Teoriile conspirației funcționează deoarece oferă răspunsuri simple la probleme complexe. Atunci când lucrurile merg prost, este mai ușor și mai satisfăcător să dai vina pe un singur personaj negativ și atotputernic decât să înțelegi procese economice sau politice complexe. În același timp, ele îi fac pe adepții lor să se simtă speciali, ca și cum ar vedea ceea ce le scapă tuturor celorlalți.

Правые, грантоеды, НПОкратия и прочая братия

30.01.2020, 15:00, Политика / Аналитика 11 910

Facebook Twitter Одноклассники



Sursă: EUvsDisinfo³⁹ / Titlul articolului: „Dreapta, paraziții subvențiilor, NPOcracia și alți frați”

Lecția cheie de reținut

Nu orice postare falsă face parte dintr-o operațiune de informare și nu orice opinie ferm exprimată reprezintă o formă de manipulare. Principalele semnale de avertizare sunt coordonarea, ascunderea identității, presiunea emoțională, dovezile false sau denaturate, interesele străine sau netransparente, precum și încercările de a reduce încrederea, de a diviza societatea sau de a descuraja participarea cetățenilor.



Cum funcționează operațiunile de informare: instrumente și metode utilizate

Operațiunile de informare se bazează pe un ansamblu de tehnici – unele psihologice, altele tehnice; unele la fel de vechi ca propaganda însăși, altele devenite posibile datorită noilor tehnologii. Nu este nevoie să memorați fiecare termen. Important este să învățați să recunoașteți semnalele de avertizare. Înțelegerea acestor instrumente și metode vă va ajuta să identificați situațiile în care sunt utilizate.

Pe măsură ce parcurgeți exemplele de mai jos, puneți-vă trei întrebări:

- ▶ Cine se află în spatele acestui conținut?
- ▶ Ce emoție încearcă să-mi provoace?
- ▶ Ce încearcă să mă determine să fac – să distribui, să comentez, să urăsc, să devin neîncrezător, să dau clic, să plătesc sau să renunț?



Bule informaționale

O bulă informațională sau un „silo informațional” se formează atunci când sunt urmărite în principal surse care confirmă convingerile deja existente. Algoritmii afișează mai mult din conținutul cu care există interacțiuni, iar în timp sunt urmărite tot mai multe persoane care gândesc la fel. Treptat, expunerea la perspective diferite se reduce, până când apare impresia că toată lumea împărtășește aceleași opinii. Dacă sunt urmărite mai multe videoclipuri care susțin că parcursul european al Republicii Moldova este periculos, platforma poate începe să recomande și mai multe videoclipuri cu același mesaj. În scurt timp, poate apărea impresia că această opinie este prezentă peste tot, deși este văzută doar o parte a conversației.

Site-uri false sau „doppelgänger”

Uneori sunt create site-uri false care imită site-uri autentice, copiind identitatea vizuală a unor organizații sau instituții de încredere. Aceste site-uri pot include elemente precum chatul live sau alte funcționalități menite să le facă să pară credibile, deși nu sunt autentice. Un site de tip **„doppelgänger”** este o copie a unui site real de știri sau al unei instituții media, concepută astfel încât să arate aproape identic cu originalul. De multe ori, diferența constă doar în numele domeniului sau în extensia acestuia – partea de după punct din adresa web, precum .com, .md sau .eu. Astfel este creată o adresă care pare familiară, dar trimite către un site complet diferit. Scopul este răspândirea de informații false sau înșelătoare, creând în același timp impresia că acestea provin dintr-o sursă de încredere.



Captură de ecran a unui site media de tip „doppelgänger”. Observă extensia domeniului: în loc de **theguardian.com** (adresa autentică), site-ul fals folosește **theguardian.co.com**.

Sursă: EU DisfoLab⁴⁰

Conturi false sau neautentice pe rețelele sociale

Sunt profiluri de pe rețelele sociale care prezintă în mod fals identitatea persoanei aflate în spatele lor. Fotografia poate fi furată sau generată cu ajutorul inteligenței artificiale. Numele poate fi inventat. „Persoana” respectivă poate să nu existe deloc sau poate fi cu totul alta decât pretinde că este.

Site-uri web sau publicații care difuzează conținut înșelător

Sunt site-uri web, publicații sau canalele lor de pe rețelele sociale care se prezintă drept surse independente de știri locale, precum „Știri din Bălți”, „Cahul azi” sau „Vocea Moldovei”, dar care sunt, în realitate, controlate de actori externi ce promovează o agendă coordonată. Acestea combină informații locale autentice cu mesaje politice manipulative, pentru a crea impresia că sunt surse credibile și a reduce vigilența publicului. Par a practica un jurnalism local: folosesc denumiri cu rezonanță locală, alternează știri regionale cu opinii și adoptă un ton care lasă impresia că provin din interiorul comunității.

Astroturfing

Denumirea provine de la AstroTurf, o marcă de gazon artificial. Astroturfingul este o activitate organizată menită să creeze impresia falsă a unei mișcări populare ample și spontane, de susținere sau de opoziție față de o anumită cauză, deși aceasta este, în realitate, inițiată și controlată de un grup sau o organizație care își ascunde identitatea⁴¹. Cu alte cuvinte, este o campanie concepută să pară o inițiativă spontană a oamenilor obișnuiți, când, de fapt, este organizată și finanțată din culise.

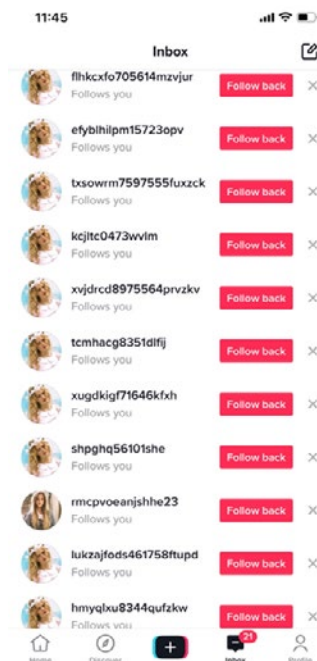
Bot

Un bot (prescurtare de la robot) este un program informatic care automatizează sau execută sarcini repetitive. În contextul rețelelor sociale, un bot este un cont automatizat care publică mesaje fără intervenție umană. Boții sunt utilizați frecvent pentru a amplifica artificial un mesaj, pentru a crea impresia că un subiect este foarte popular sau pentru a ataca adversarii. Identificarea boților poate fi exersată prin intermediul jocului „Om sau nu?”, accesând codul QR de mai jos.



Sursă: Om sau nu?⁴²

Este important de reținut însă că niciun joc sau instrument nu poate identifica toți boții. Cea mai importantă abilitate este recunoașterea tiparelor de comportament.



Exemplu: Conturi TikTok care folosesc aceleași fotografii de profil și nume de utilizator generate aleatoriu pentru a inunda un utilizator real cu solicitări reciproce de urmărire.⁴³

Troll

Trollingul constă în publicarea de postări sau comentarii online cu scopul de a provoca reacții, de a stârni conflicte sau de a-i supăra pe ceilalți. Poate include atacarea sau hărțuirea unor persoane, uneori în mod anonim, și este adesea prezentat drept „o simplă glumă”, deși poate avea efecte dăunătoare⁴⁴. Trollii folosesc frecvent identități false sau postează anonim, ceea ce le permite să facă afirmații fără a-și asuma responsabilitatea pentru ele. Acest lucru îi poate face să se simtă mai puternici și mai puțin reținuți decât ar fi într-o conversație față în față. Din acest motiv, este adesea dificil de stabilit cine se află în realitate în spatele unei postări sau al unui comentariu.⁴⁵

Deepfake

Un deepfake este un material audio, video sau alt tip de conținut digital creat ori modificat astfel încât să dea impresia că s-a întâmplat ceva ce, în realitate, nu s-a întâmplat.

În trecut, imaginile și videoclipurile erau manipulate manual cu ajutorul programelor de editare. Astăzi, inteligența artificială permite realizarea unor falsuri digitale mult mai realiste și mai greu de identificat.

Pentru a învăța să deosebiți materialele deepfake de videoclipurile autentice, încercați jocul disponibil prin intermediul codului QR de mai jos:



Sursă: Direcția Națională de Securitate Cibernetică⁴⁶

Comportament neautentic coordonat (CIB)

Reprezintă eforturi organizate, deliberate și manipulative de inducere în eroare a publicului prin utilizarea mai multor conturi false sau neautentice. De regulă, implică rețele de conturi și pagini care acționează coordonat pentru a răspândi anumite mesaje sau a desfășura acțiuni specifice, ascunzând identitatea ori coordonarea din spatele acestora. Operațiunile de tip CIB se bazează pe utilizarea pe scară largă a tacticilor și tehnicilor de manipulare.⁴⁷

Inundarea narativă

În loc să promoveze o singură narațiune falsă, această tactică inundă spațiul informațional cu numeroase narațiuni concurente – unele contradictorii, altele parțial adevărate, iar altele complet absurde. Scopul nu este de a convinge publicul de o anumită afirmație, ci de a crea confuzie și epuizare.

Exemplu: Înaintea alegerilor, pot circula simultan numeroase afirmații: că alegerile au fost deja fraudate, că trupele străine sunt pe drum, că prețurile vor exploda, că școlile se vor schimba complet sau că Republica Moldova își va pierde identitatea. Aceste afirmații se pot contrazice între ele, însă toate urmăresc să genereze anxietate și nesiguranță.

Deturnarea hashtag-urilor

Această tactică constă în utilizarea coordonată a unui hashtag popular, fără legătură cu subiectul, pentru a transmite un mesaj către un public cât mai larg. Astfel, un hashtag despre un meci de fotbal poate ajunge brusc să fie inundat de conținut politic, iar hashtag-ul unei mișcări de protest poate fi acaparat de mesaje de tip spam, până când conversația inițială este acoperită și își pierde vizibilitatea.

Exemplu: Un hashtag despre un meci de fotbal, un concert, un eveniment școlar sau o sărbătoare națională poate fi inundat brusc de mesaje politice.

Epuizarea atenției.

Operațiunile de informare nu urmăresc întotdeauna să convingă. Uneori, scopul lor este pur și simplu să epuizeze atenția publicului. Un flux continuu de titluri alarmiste, afirmații scandaloase și controverse fără sfârșit reduce capacitatea de a acorda atenție informațiilor. Când totul pare urgent, nimic nu mai pare cu adevărat important. Când fiecare știre ar putea fi falsă, verificarea informațiilor devine obositoare. În cele din urmă, oamenii încetează să mai acorde atenție – nu pentru că nu le pasă, ci pentru că nu mai reușesc să țină pasul.

Phishingul

Phishingul este o metodă de fraudă sau un tip de atac cibernetic prin care atacatorii se dau drept o entitate de încredere (de exemplu, o bancă, un angajator sau o organizație cunoscută) pentru a determina oamenii să divulge informații sensibile, precum parole, date ale cardurilor bancare sau informații confidențiale ale unei companii. Aceste fraude utilizează adesea e-mailuri, mesaje sau alte comunicări false pentru a convinge victimele să acceseze site-uri web frauduloase. Atacatorii pot încerca să înșele victimele prin mesaje text, e-mailuri, apeluri telefonice sau prin asumarea unei identități false.⁴⁸

Exemplu: formulare false pentru burse, mesaje false privind câștigarea unor premii, linkuri false pentru urmărirea livrării unui colet, alerte bancare false, mesaje false de „verificare a contului” sau mesaje care pretind că provin de la platforme educaționale.



Trei sfaturi pentru recunoașterea profilurilor false

1.

De cât timp există profilul?

A fost creat foarte recent? Dacă da, este foarte probabil să fie un profil fals. Profilurile de tip troll sunt create pentru un scop bine definit. Deoarece utilizatorii pot descoperi rapid că nu sunt de încredere, acestea sunt rareori utilizate pentru o perioadă îndelungată.

2.

Câți urmăritori sau prieteni are profilul?

Întrucât profilul a fost creat recent, acesta are, de regulă, o rețea restrânsă, un troll are, de regulă, o rețea restrânsă de urmăritori sau prieteni. La rândul lor, puținii urmăritori sau prieteni sunt adesea alți trolli.

3.

Ce fel de fotografie are profilul?

Cu ajutorul funcției Google Reverse Image Search (Căutare inversă a imaginilor), fotografia poate fi verificată pentru a vedea unde mai apare pe internet. Trollii folosesc adesea fotografii din baze de imagini (stock photos) sau fotografii copiate de pe alte profile.

**🎯 Instrument
sau metodă**

**🎯 Principalul semnal
de avertizare**

**🎯 Răspuns
recomandat**

Bulă informațională

Sunt văzute doar opinii
similare.

Consultarea unor surse
alternative credibile.

**Site de tip
„doppelgänger”**

Site-ul pare autentic, dar
adresa web este neobișnuită.

Verificarea adresei URL complete
și a sursei oficiale.

Cont fals

Lipsa unui istoric autentic,
activitate neobișnuită,
conținut copiat.

Verificarea istoricului profilului
înainte de a-i acorda încredere.

Astroturfing

O mișcare aparent
spontană apare brusc.

Căutarea unor formulări identice
și a semnelor de coordonare.

Rețea de boți

Activitate foarte intensă și
postări repetitive.

Repetarea aceluiași mesaj nu trebuie
confundată cu popularitatea reală.

Troll

Provocări, insulte și
devierea discuției de la
subiect.

Evitarea alimentării conflictului și
raportarea abuzului.

Deepfake

Material audio sau video
care pare autentic și conține
afirmații șocante.

Verificarea informațiilor folosind
surse originale și credibile.

**Comportament
neautentic
coordonat (CIB)**

Numeroase conturi
promovează coordonat același
mesaj.

Analizarea sincronizării, a repetiției
și a coordonării ascunse.

**Inundare
narativă**

Numeroase afirmații
contradictorii apar simultan.

Verificarea fiecărei afirmații,
pe rând.

Phishing

Solicitări urgente de date
personale, bani sau parole.

Evitarea accesării linkurilor și
verificarea informațiilor prin canale
oficiale.

Ce urmăresc operațiunile de informare?

O concepție greșită des întâlnită este că operațiunile de informare urmăresc să convingă oamenii de o anumită minciună. În realitate, ele urmăresc adesea să influențeze modul în care oamenii gândesc, simt și acționează.

Să creeze confuzie

Atunci când oamenii nu mai pot distinge adevărul de fals, adesea încetează să mai caute răspunsuri. „Cine mai știe ce este real?” nu este un semn de gândire critică, ci, de multe ori, exact rezultatul urmărit de cei care manipulează informațiile. Confuzia îi favorizează pe cei care doresc să acționeze fără a fi supuși controlului public.

Să demobilizeze

Dacă oamenii ajung să creadă că toți politicienii sunt la fel de corupți, de ce ar mai vota? Dacă sistemul pare deja aranjat, de ce ar mai participa? Cinismul îi favorizează pe cei care beneficiază de un nivel scăzut de participare civică. Cum ar putea suna: „Votul tău nu schimbă nimic.” „Totul este deja decis.” „Oamenii inteligenți stau departe de politică.”

Să polarizeze

Operațiunile de informare alimentează diviziunile deja existente – între grupuri etnice, comunități lingvistice, tabere politice sau generații. Nu este nevoie să creeze conflicte de la zero; este suficient să amplifice tensiunile existente. Cum ar putea suna: „Oamenii ca ei sunt dușmanii.” „Nu poți avea încredere în nimeni din grupul acela.” „Vor să ne distrugă identitatea.”

Să erodeze încrederea

Societățile democratice se bazează pe instituții în care cetățenii au, în general, încredere: alegeri, instanțe judecătorești, mass-media și sisteme de sănătate publică. Dacă această încredere se erodează, coordonarea în societate devine aproape imposibilă, iar fiecare instituție ajunge să fie privită cu suspiciune. Cum ar putea suna: „Toate instituțiile sunt controlate.” „Nu se poate avea încredere în nicio instanță, în niciun canal media, în nicio școală și în nicio alegere.”

Să distragă atenția

Uneori, scopul este pur și simplu acela de a capta atenția publicului. Spațiul informațional este inundat de zgomot informațional, astfel încât problemele cu adevărat importante să fie îngropate sau trecute cu vederea.

Să obțină profit

Unele operațiuni de informare urmăresc, în primul rând, câștiguri financiare. Ele folosesc aceleași tactici pentru a genera clicuri, a obține venituri din publicitate sau a desfășura diverse escrocherii. Atenția, frica și sentimentul de urgență sunt ușor de exploatat, iar scopul este adesea transformarea implicării publicului în profit.

De reținut: niciunul dintre aceste obiective nu presupune convingerea oamenilor de o anumită afirmație. Este suficient să le afecteze capacitatea de a gândi limpede și de a acționa împreună.



Cine se află în spatele operațiunilor de informare?

Operațiunile de informare sunt desfășurate de diferite categorii de actori, fiecare urmărindu-și propriile interese:⁴⁹

Actori statali

Guvernele desfășoară operațiuni de informare ca parte a politicii lor externe. În acest scop, utilizează structuri și resurse dedicate campaniilor de influențare îndreptate împotriva altor state. De exemplu, un stat străin poate încerca să submineze încrederea în alegerile, instituțiile sau parteneriatele internaționale ale Republicii Moldova.

Actori politici interni

Nu toate operațiunile de manipulare provin din străinătate. Politicienii, partidele și grupurile de interese din țară pot recurge, de asemenea, la astfel de tactici: conturi false, mișcări aparent spontane, create artificial sau atacuri coordonate împotriva oponenților. Uneori, operațiunile interne și cele desfășurate de actori străini se suprapun și se consolidează reciproc.

Actori intermediari (proxy)

Statele acționează adesea prin intermediul unor terți care le ascund implicarea directă. Aceștia pot fi instituții media care par independente, dar sunt finanțate din străinătate, creatori de conținut care sunt plătiți fără a dezvălui acest lucru ori partide politice care se coordonează cu actori străini.

Operatorii comerciali

O parte din dezinformare este, pur și simplu, o afacere. Fabricile de clickbait exploatează indignarea pentru a genera venituri din publicitate. „Firmele de interacțiuni” vând urmăritori, aprecieri și comentarii false oricui este dispus să plătească. Poate că nu sunt interesate de politică, ci doar de profit. Însă serviciile lor sunt disponibile pentru oricine are bani.

Înțelegerea celor care beneficiază de o operațiune este adesea cheia pentru a înțelege de ce aceasta există.

Ce vulnerabilități exploatează operațiunile de informare?

Este util să se înțeleagă cine se află în spatele acestor operațiuni. Și mai important este însă să se înțeleagă unde reușesc acestea și ce vulnerabilități exploatează, deoarece tocmai acest lucru contribuie la consolidarea rezilienței.

Vulnerabilități ale sistemului mass-media

Redacțiile sunt din ce în ce mai mici, iar verificarea informațiilor necesită timp – o resursă pe care ritmul publicării online o recompensează prea puțin. În Republica Moldova, această situație este și mai pronunțată, deoarece piața media este redusă, multe instituții media independente dispun de resurse limitate, iar o parte a publicului își ia informațiile în principal de la televiziune, Telegram și Facebook, în detrimentul jurnalismului profesionist. Așa-numitele publicații „alternative”, care seamănă cu instituțiile media consacrate, dar funcționează fără standarde editoriale, profită de aceste lacune. În același timp, algoritmii favorizează interacțiunea în detrimentul acurateței. Toate acestea permit răspândirea rapidă a conținutului manipulat înainte ca acesta să poată fi verificat.

Vulnerabilități în modul în care percepem opinia celorlalți

Oamenii se raportează în mod firesc la opiniile celor din jur atunci când își formează propriile convingeri. Dacă mulți oameni par să creadă același lucru, acesta tinde să pară mai credibil sau mai acceptabil. Operațiunile

de informare exploatează această tendință, creând aparența unui consens prin conturi false, comentarii coordonate și rețele de boți care fac ca opiniile marginale să pară larg împărtășite. În aceste situații, reacția nu este la opinia publică reală, ci la o imagine artificial construită a acesteia.

Vulnerabilități în modul în care gândim

Creierul uman nu este conceput pentru a procesa volumul uriaș de informații la care este expus zilnic. De aceea, recurge la mecanisme mentale rapide: acordă mai ușor încredere surselor familiare, acceptă mai ușor informațiile care confirmă convingerile existente și reacționează adesea emoțional înainte de a analiza rațional. De cele mai multe ori, aceste mecanisme sunt utile, însă ele pot fi și exploatare. Targetarea psihografică utilizează date despre comportamentul oamenilor pentru a crea mesaje adaptate profilului lor psihologic, concepute să le depășească mecanismele obișnuite de apărare.

Aceste vulnerabilități nu reprezintă defecte personale. Ele reflectă modul în care funcționează cogniția umană, societatea și mediul informațional și sunt tocmai aspectele pe care operațiunile de informare încearcă să le exploateze.

Cum se deosebește manipularea de comunicarea legitimă?

Aceasta este o întrebare importantă. Nu orice formă de persuasiune reprezintă manipulare. Campaniile politice încearcă să convingă alegătorii. Instituțiile media decid ce subiecte să relateze. Activiștii susțin diferite cauze. Profesorii contribuie la formarea modului de gândire al elevilor. Cum poate fi făcută, așadar, diferența dintre influența legitimă și manipulare? Principalele diferențe sunt următoarele:

► Comunicarea legitimă

Este transparentă cu privire la identitatea celui care comunică.

Prezintă dovezi care pot fi verificate.

Recunoaște complexitatea și incertitudinea.

Respectă capacitatea oamenilor de a lua propriile decizii.

Își declară deschis intenția de a convinge.

► Manipulare

Ascunde sau falsifică identitatea.

Descurajează verificarea informațiilor.

Creează o falsă impresie de certitudine.

Încearcă să ocolească judecata critică.

Se prezintă drept neutră.

Sursă: Propaganda și persuasiunea⁵⁰

Încercați: Exercițiul



În 2025, pe Telegram a circulat un videoclip care folosea în mod fraudulos sigla și identitatea vizuală a BBC. Sarcina constă în verificarea acestui conținut, pas cu pas, într-o ordine logică ce reflectă modul în care lucrează verificatorii profesioniști de fapte.

Acesta susținea: „Bellingcat a descoperit dovezi șocante privind alegerile prezidențiale din 2024 din Republica Moldova. Potrivit investigației, 42% dintre voturile exprimate prin corespondență au fost înregistrate folosind identitatea unor alegători decedați. Fondatorul Bellingcat, Eliot Higgins, a declarat: «Aceste informații vor fi deosebit de relevante pentru cetățenii Republicii Moldova, care ar trebui să le ia în considerare și să acționeze în consecință.»”

Pasul 1. Identificarea afirmațiilor concrete

Înainte de a începe verificarea, conținutul trebuie împărțit în **afirmații care pot fi verificate**:

- 1 Bellingcat a desfășurat o investigație privind alegerile prezidențiale din 2024 din Republica Moldova.
- 2 Investigația a concluzionat că **42% dintre voturile exprimate** prin corespondență au fost înregistrate folosind identitatea unor alegători decedați.
- 3 Eliot Higgins a făcut declarația citată.
- 4 Videoclipul este prezentat ca fiind un material al BBC.

Verificarea începe prin identificarea și izolarea afirmațiilor care pot fi verificate, nu prin reacția la mesajul în ansamblu.

- Există alte surse credibile sau verificări independente ale faptelor care analizează afirmațiile din postarea de pe Telegram?

Pasul 3. Analizarea concluziilor

După parcurgerea pașilor anteriori, concluziile pot fi analizate pornind de la următoarele întrebări:

- Care este sursa inițială a afirmației? Există dovezi provenite din sursa originală?
- Este statistica susținută de date oficiale privind alegerile?
- Cine ar avea de câștigat din răspândirea online a unei astfel de afirmații?

Pasul 2. Verificarea informațiilor

Următorul pas constă în căutarea informațiilor relevante în surse online credibile, acordând prioritate site-urilor oficiale. În acest proces, pot fi urmărite următoarele întrebări:

- Bellingcat este o organizație reală de jurnalism de investigație, specializată în investigații bazate pe surse deschise?
- A publicat Bellingcat într-adevăr o investigație care să prezinte dovezi atât de grave privind alegerile prezidențiale din 2024 din Republica Moldova? Există o astfel de investigație pe site-ul oficial al organizației?
- Cine este Eliot Higgins și care este rolul său în cadrul Bellingcat? Există și alte surse, în afara postării de pe Telegram, care să confirme că a făcut declarația citată?

Lecția cheie

Chiar și atunci când sunt invocate nume reale, credibilitatea informațiilor trebuie verificată la sursă. Verificarea faptelor nu înseamnă găsirea unui singur articol care afirmă că o informație este falsă. Ea presupune verificarea sistematică a fiecărei afirmații, identificarea dovezilor pe care aceasta se bazează și formularea unor concluzii pe baza unor surse credibile.



Cum poate fi recunoscută manipularea în viața de zi cu zi



Partea 3

Recunoașterea manipulării este o abilitate. Ca orice abilitate, ea se dezvoltă prin practică. Scopul este dezvoltarea capacității de a aprecia când un anumit conținut necesită o atenție sporită. Majoritatea conținutului întâlnit în spațiul informațional este exact ceea ce pare a fi. O parte, însă, nu este – iar această diferență este importantă.

Acest capitol abordează două aspecte: tacticile utilizate în operațiunile de informare (instrumentele de manipulare) și narațiunile utilizate frecvent împotriva Republicii Moldova care îi vizează în mod direct pe cetățenii săi. Înțelegerea ambelor dimensiuni contribuie la dezvoltarea capacității de a identifica manipularea.

Operațiunile de informare utilizează o gamă largă de tehnici. În continuare sunt prezentate cele mai frecvente tactici care pot fi întâlnite în spațiul informațional.

Pentru mai multă claritate, aceste tactici sunt grupate în categorii. Totuși, granițele dintre ele sunt flexibile, iar multe exemple din lumea reală se pot încadra simultan în mai multe categorii.



1 Conținut fabricat

Fabricarea conținutului constă în crearea unor informații false care sunt prezentate ca fiind autentice.

Aceasta include:

- ▶ **documente falsificate**
- ▶ **deepfake-uri**

Conținutul fabricat poate apărea sub forma:

- ▶ unei scrisori false atribuite guvernului și distribuite pe Telegram;
- ▶ unei capturi de ecran false a unui anunț școlar;
- ▶ unui citat fals atribuit unui funcționar public;
- ▶ unui videoclip deepfake cu un politician, jurnalist, profesor sau altă persoană publică;
- ▶ unui „avertiment urgent” fals distribuit într-un grup de pe Viber.

Atunci când o informație se potrivește foarte bine cu ceea ce un anumit public crede deja, acest lucru poate reprezenta un semnal de avertizare.

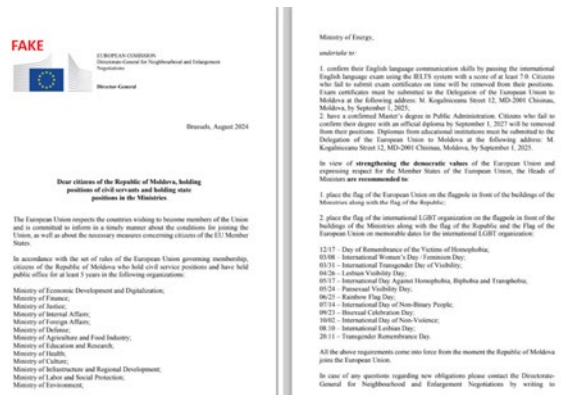
Exemplu din Republica Moldova: În perioada electorală din septembrie–octombrie 2024, au circulat online mai multe scrisori falsificate, prezentate ca fiind emise de instituții ale Uniunii Europene și ale Guvernului Republicii Moldova. Acestea conțineau afirmații false privind migranții, cerințele referitoare la educația privind persoanele LGBT, recrutarea pentru serviciul militar și importurile de deșeuri. Fiecare dintre aceste falsuri a fost conceput pentru a alimenta temerile legate de integrarea în Uniunea Europeană. Autoritățile din Republica Moldova au confirmat că toate aceste documente erau falsificate.

Recomandări practice:

▶ **Verificarea surselor oficiale.** Se verifică dacă documentul sau afirmația apare pe site-urile oficiale ori pe canalele verificate ale autorităților competente. Dacă o presupusă scrisoare guvernamentală circulă pe Telegram, dar nu apare pe niciun site oficial al autorităților din Republica Moldova, aceasta trebuie tratată cu suspiciune.

▶ **Verificarea relatărilor din mass-media credibilă.** Dacă informația este autentică și importantă, este probabil ca aceasta să fie relatăată și de instituții media credibile. Dacă o afirmație spectaculoasă circulă exclusiv pe rețelele sociale și pe canale anonime, este util să se analizeze de ce nu este preluată și de surse credibile.

▶ **Prudență față de documentele „scurse”.** Presupusele scurgeri de informații trebuie privite cu un grad ridicat de scepticism, mai ales atunci când confirmă în mod convenabil temeri existente sau narațiuni cu puternică încărcătură politică.



Sursă: Check Point⁵¹

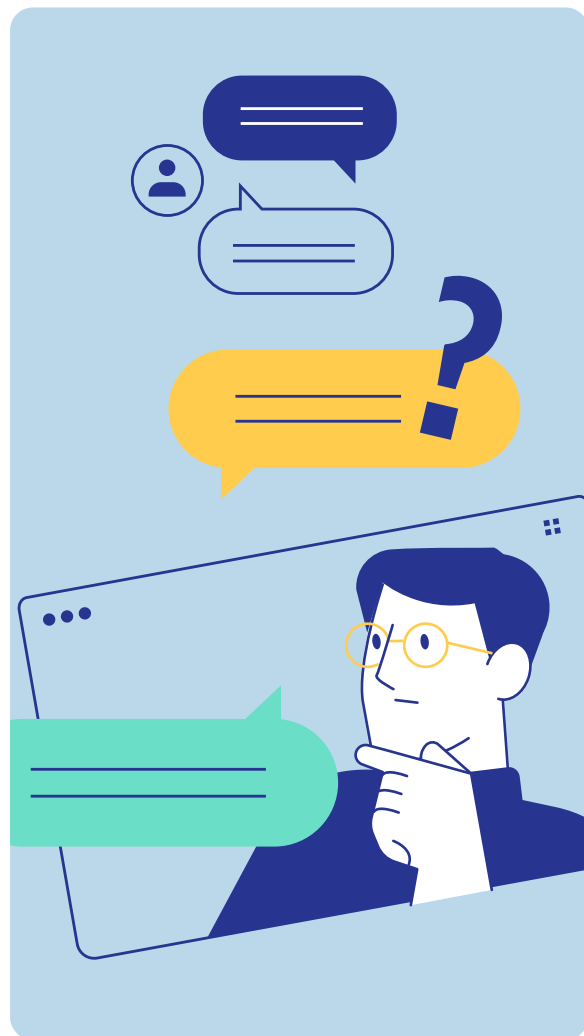


Sursă: Check Point⁵²

Exemplu din Republica Moldova: În iulie 2025, a circulat online un videoclip deepfake în care Angelica Caraman, președinta Comisiei Electorale Centrale, părea să afirme că interferența Uniunii Europene în alegeri era acceptabilă. În realitate, declarația era falsă și fusese generată prin manipularea unor imagini cu ajutorul inteligenței artificiale, preluate dintr-o apariție televizată anterioară. Deși autoritățile au dezmințit conținutul, iar verificările independente au confirmat că videoclipul era fals, acesta a continuat să circule și a fost amplificat de actori pro-Kremlin drept „dovadă” a interferenței Uniunii Europene în alegeri.



Sursă: Stopfals.md⁵³



2 Conținut manipulat

Conținutul este manipulat atunci când materiale autentice sunt modificate sau prezentate în afara contextului lor original.

Aceasta include:

- ▶ **imagini sau videoclipuri editate;**
- ▶ **conținut scos din context;**
- ▶ **citare selective;**
- ▶ **titluri înșelătoare.**

Recomandări practice:

▶ **Căutarea inversă a imaginilor.** Se utilizează funcția de căutare inversă a imaginilor din Google (de exemplu, prin opțiunea „Căutați imaginea cu Google”) sau instrumente precum TinEye. Dacă aceeași imagine apare în articole publicate cu luni sau chiar ani înainte, este probabil ca aceasta să fi fost reutilizată și prezentată într-un context diferit.

▶ **Citirea dincolo de titlu.** Titlurile sunt adesea formulate într-un mod mai spectaculos decât conținutul pe care îl introduc. Înainte de distribuirea unei informații, este recomandată citirea cel puțin a primelor paragrafe. De multe ori, articolul prezintă informațiile într-un mod mai nuanțat sau chiar diferit de ceea ce sugerează titlul.

▶ **Verificarea citatelor.** Dacă unei persoane îi este atribuită o declarație șocantă, fraza respectivă poate fi căutată între ghilimele pentru a identifica sursa originală. Este important să fie căutate interviul, discursul sau documentul din care provine citatul, nu doar alte surse care îl reproduc. Dacă sursa originală nu poate fi identificată, există posibilitatea ca citatul să fie inventat, modificat sau scos din context.

Exemplu din Republica Moldova: În timpul campaniei electorale din septembrie 2025, pe Telegram a circulat o fotografie autentică în care apăreau militari francezi, îmbrăcați în uniformă, la o benzinărie din Cimișlia. Imaginea era însoțită de afirmația falsă că trupe NATO se pregăteau să ocupe Republica Moldova. În realitate, era vorba despre atașați militari acreditați, aflați într-o vizită oficială la o unitate militară. Ministerul Apărării a confirmat public acest lucru. Cazul ilustrează modul în care imagini autentice, scoase din context, pot fi folosite pentru a alimenta narațiuni false și alarmiste.



Sursă: Telegram⁵⁴

3 Falsificarea identității și identitățile frauduloase

Prezentarea drept altcineva pentru a induce în eroare.

Aceasta include:

- ▶ **conturi false;**
- ▶ **publicații sau instituții media locale false;**
- ▶ **falsificarea identității unor oficiali;**
- ▶ **astroturfing.**

Recomandări practice:

▶ Verificarea datei de creare a contului.

Conturile false sunt adesea create cu puțin timp înaintea unei campanii și nu au un istoric autentic de activitate.

▶ **Verificarea în surse cunoscute.** Numele publicației sau al sursei poate fi căutat împreună cu termeni precum „fals” sau „dezinformare”. Este posibil ca aceasta să fi fost deja semnalată de alți verificatori de fapte.

▶ **Aplicarea gândirii critice.** Atunci când o informație pare prea bună pentru a fi adevărată, este util să fie privită cu prudență. Dacă aceeași sursă publică în mod repetat conținut care promovează aceleași narațiuni și confirmă convingerile deja existente ale publicului, este posibil ca obiectivul său să nu fie prezentarea adevărului, ci atingerea propriilor scopuri.

Exemplu din Republica Moldova: În mai 2024, o analiză a identificat 39 de canale Telegram care se prezentau drept surse locale de știri din Republica Moldova, purtând denumiri inspirate de localități precum Bălți, Cahul și Orhei. Analiza a arătat că aceste canale erau administrate în mod centralizat și că, potrivit datelor furnizate de TGStat, administratorii lor se aflau în Rusia, nu în Republica Moldova. Canalele publicau simultan același conținut, creând impresia unui consens local larg.

Town name	Telegram name	Telegram bot	Subscribers
Cahul	Вечерний Кагул	@KagulBot	1186.00
Chisinau	Кишинев мо Chișinău ~ Arcul de Triumf	@ChisinauBot	1,070.00
Balti	Cluda Bălțului мо Бельцы	@BaaltiBot	1,000.00
Tiraspol	Тирасполь I Tiras Polis	@TirasPolisBot	712.00
Orhei	OrheiLand мо Орхей	@OrheiiBot	666.00
Ceadir-Lunga	Чадыр и Лунга	@chadyr_l_lunga_bot	666.00
Dubasari	Репортер из Дубоссар	@DubossaryBot	618.00
Bender/Tighina	Бендеры • BenderLog	@BenderLogBot	585.00
Briceni	Plaiul Briceni • Бричань	@PlaiulBot	594.00
Edinet	Единцы I Ероса Edineț	@EppocaBot	499.00

Sursă: DFRLab⁵⁵

4 Consens fabricat

Crearea impresiei false că un anumit punct de vedere este împărtășit pe scară largă.

Aceasta include:

- ▶ **rețele de boți;**
- ▶ **comentarii coordonate;**
- ▶ **sondaje și petiții false;**
- ▶ **troli plătiți.**

Recomandări practice:

▶ **Identificarea tiparelor de tip „copiere-lipire”.**

Persoanele reale își exprimă, de regulă, opiniile în propriile cuvinte. Dacă aceeași frază apare publicată identic de zeci de conturi, este posibil să fie vorba despre o acțiune coordonată, nu despre o opinie publică autentică.

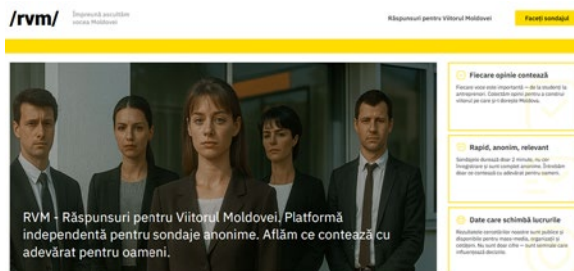
▶ **Verificarea istoricului contului.** Conturile care publică frecvent conținut politic pot fi analizate pentru a vedea dacă au luni sau ani de activitate normală, cu fotografii personale și interese diverse, ori dacă au apărut recent și publică aproape exclusiv mesaje politice. În acest din urmă caz, există posibilitatea ca ele să fie false sau cumpărate.

▶ **Analizarea limbajului.** Boții folosesc uneori traducerea automată pentru a distribui mesaje în mai multe limbi. Acest lucru poate genera greșeli gramaticale evidente sau propoziții incoerente.

▶ **Verificarea fotografiei de profil.** Boții și trollii folosesc adesea fotografia altei persoane sau imagini din baze de fotografii. În cazul fotografiilor de profil suspecte, se recomandă utilizarea funcției de căutare inversă a imaginilor din Google pentru a verifica dacă acestea apar și în alte contexte.

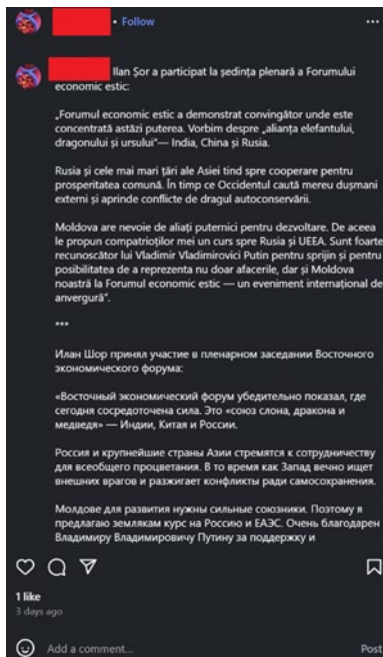
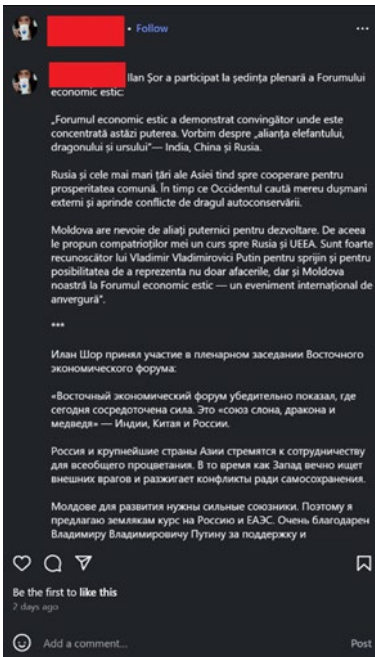
▶ **Analizarea activității contului.** Boții și trollii plătiți sunt, de regulă, foarte activi. Unele conturi înregistrează peste 50 de postări sau alte interacțiuni într-o singură zi, un nivel de activitate puțin probabil pentru o persoană obișnuită. Conturile cu un număr suspect de mare de postări zilnice trebuie privite cu prudență.

Exemplu din Republica Moldova privind sondajele și petițiile false: Înaintea alegerilor parlamentare din septembrie 2025 din Republica Moldova, o rețea de site-uri web denumită „Vocepentru” s-a prezentat drept o platformă neutră de sondaje, imitând în același timp identitatea vizuală a partidului pro-european PAS pentru a părea credibilă. Sondajele utilizau întrebări manipulative, cu răspunsuri binare, care asociau aderarea la Uniunea Europeană cu consecințe negative, producând rezultate prestabilite în locul unor cercetări autentice. Analiza tehnică a stabilit legături între aceste site-uri și un serviciu din Rusia asociat anterior cu campanii pro-Kremlin. Rezultatele fabricate au fost apoi prezentate drept o expresie autentică a „opinie publice” – o tactică cunoscută sub denumirea de „spălarea narațiunilor”.



Sursă: GLOBSEC⁹⁶

Exemplu din Republica Moldova privind o rețea de boți: Deși oligarhul sancționat Ilan Șor a fost împiedicat să ajungă la publicul din Uniunea Europeană prin intermediul rețelelor sociale, coaliția sa, Blocul Victorie, a ocolit această restricție prin distribuirea conținutului său prin intermediul a cel puțin 20 de conturi de pe TikTok, Instagram și Facebook. Conținutul era adesea ușor modificat și redistribuit prin conturi care păreau autentice – unele dintre acestea fiind, potrivit informațiilor disponibile, recrutate prin intermediul unui bot de pe Telegram care oferea bonusuri. Astfel, campania și-a ascuns adevărata origine și a amplificat mesaje politice provenite de la un actor sancționat.



Sursă: Alliance4Europe⁵⁷

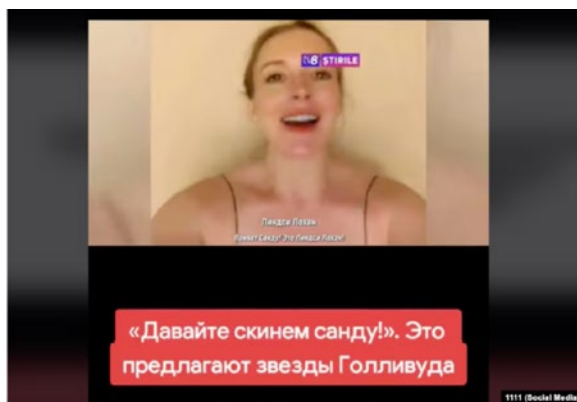
5 Umor și satiră

Manipularea poate lua uneori forma unei glume. Memele, glumele și conținutul satiric pot răspândi mesaje manipulative, evitând în același timp analiza critică. Atunci când ceva este prezentat ca umor, oamenii tind să îl distribuie fără a verifica informațiile – „este doar o glumă”. Însă mesajul își produce efectul. Paginile satirice pot face afirmații care ar părea exagerate sau inacceptabile într-un articol de știri. Memele simplifică subiecte complexe în imagini virale care par credibile tocmai pentru că sunt amuzante.

Recomandări practice:

- **Analizarea poantei.** Este util să fie identificată ideea pe care gluma o consolidează în realitate. Umorul funcționează adesea prin confirmarea a ceea ce oamenii cred deja.
- **Identificarea țintei.** Glumele repetate despre același grup, instituție sau persoană pot modela atitudinile în timp, chiar dacă fiecare glumă, privită separat, pare inofensivă.
- **Observarea avalanșelor de meme.** Atunci când același format de meme apare simultan pe numeroase platforme, promovând același mesaj politic, este posibil să fie vorba despre o campanie coordonată, nu despre creativitate spontană.

Exemplu din Republica Moldova: La sfârșitul anului 2023, pe TikTok au apărut videoclipuri în care vedete de la Hollywood – inclusiv Lindsay Lohan și Brian Baumgartner (cunoscut pentru rolul său din serialul The Office) – citeau, într-o rusă stâlcită, mesaje care îndemnau la înlăturarea din funcție a președintei Maia Sandu. Vedetele fuseseră induse în eroare prin intermediul platformei Cameo, unde fanii pot plăti pentru a primi mesaje video personalizate. Caracterul absurd al videoclipurilor le-a făcut amuzante și ușor de distribuit, chiar dacă transmiteau un mesaj politic. Umorul a fost folosit ca mijloc de transmitere a mesajului.



Lindsay Lohan is seen appearing to call for the Moldovan president to resign.

Sursă: RFE/RL⁵⁸ / Lindsay Lohan apare într-un videoclip în care pare să ceară demisia președintei Republicii Moldova.

6 Inundarea spațiului informațional și suprasolicitarea cognitivă

Copleșirea publicului prin volum de informații, mai degrabă decât prin argumente sau informații de calitate.

Aceasta include:

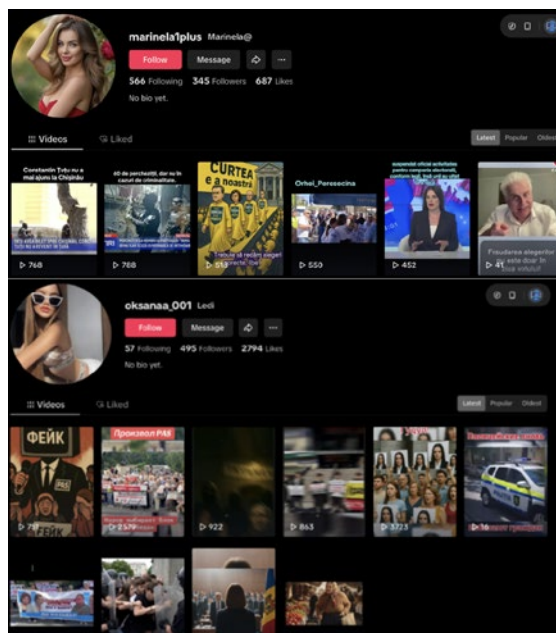
- ▶ **inundarea narativă;**
- ▶ **deturnarea hashtag-urilor;**
- ▶ **epuizarea atenției.**

Recomandări practice:

- ▶ **Observarea repetiției.** Dacă aceleași teme apar în mod repetat pe canale diferite într-un interval scurt de timp, este util să se analizeze dacă reflectă o preocupare reală a publicului sau o campanie coordonată.
- ▶ **Verificarea momentului.** O creștere bruscă a volumului de conținut pe o anumită temă – în special înaintea unor alegeri sau a unei decizii importante – poate indica existența unei campanii coordonate, mai degrabă decât o conversație spontană.

Sfat: În perioadele cu un volum foarte mare de informații, cum sunt campaniile electorale, o pauză de la rețelele sociale poate reprezenta o formă de autoprotecție. Revenirea este recomandată atunci când informațiile pot fi analizate cu spirit critic.

Exemplu din Republica Moldova: În luna care a precedat alegerile din septembrie 2025 din Republica Moldova, o analiză a identificat 100 de conturi TikTok neautentice care inundau hashtag-uri precum #Moldova cu propagandă politică coordonată. Din cele peste 36.000 de comentarii analizate, mai mult de 10.000 erau mesaje identice, copiate și lipite, precum „Jos cu PAS”. Rețeaua utiliza fotografii de profil generate cu ajutorul inteligenței artificiale și împărțea sarcinile între creatorii de conținut și conturile care amplificau artificial interacțiunile, reducând vizibilitatea vocilor autentice și influențând conținutul pe care utilizatorii îl vedeau atunci când căutau informații despre Republica Moldova.



Sursă: ExpertForum⁵⁹

Narațiuni-cheie utilizate împotriva Republicii Moldova

Dincolo de tactici, este utilă cunoașterea narațiunilor recurente pe care operațiunile de informare le folosesc împotriva Republicii Moldova. Aceste narațiuni nu sunt aleatorii. Ele exploatează preocupări reale, diviziuni reale și incertitudini reale. Cunoașterea lor facilitează recunoașterea acestora atunci când apar.⁶⁰

„UE înseamnă război”

Afirmația potrivit căreia integrarea europeană va atrage Republica Moldova într-un conflict militar. Această narațiune exploatează temerile legitime legate de instabilitatea regională și denaturează ceea ce presupune, în realitate, aderarea la Uniunea Europeană.

De ce este falsă: Uniunea Europeană este o uniune economică și politică, nu o alianță militară. State membre ale Uniunii Europene care și-au păstrat statutul de neutralitate, precum Austria și Irlanda, nu sunt membre NATO. În același timp, statul care își amenință în prezent cel mai activ vecinii prin utilizarea forței militare nu este membru al Uniunii Europene.

„Pierderea suveranității”

Afirmația potrivit căreia integrarea în Uniunea Europeană înseamnă cedarea controlului către Bruxelles, pierderea identității naționale sau transformarea Republicii Moldova într-o marionetă a Occidentului. Această narațiune prezintă parteneriatul cu Uniunea Europeană ca pe o formă de subordonare.

De ce este falsă: În realitate, statele candidate la UE își negociază condițiile de aderare.

„Valorile tradiționale sunt amenințate”

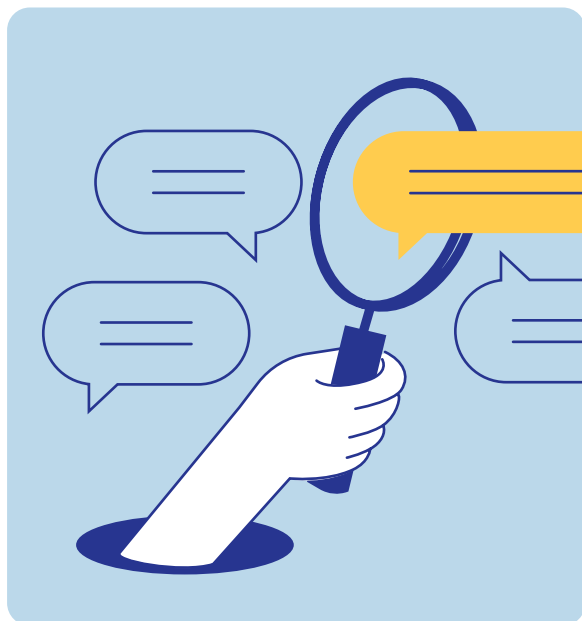
Afirmația potrivit căreia aderarea la Uniunea Europeană presupune acceptarea „propagandei LGBT”, a educației sexuale obligatorii sau renunțarea la creștinismul ortodox. Această narațiune exploatează temerile culturale legate de schimbările sociale.

De ce este falsă: Aderarea la Uniunea Europeană nu obligă niciun stat să își modifice legislația privind căsătoria, religia sau programa școlară.

„Catastrofă economică”

Afirmația potrivit căreia integrarea în Uniunea Europeană va duce la creșterea prețurilor, va distruge agricultura sau va elimina piețele rusești considerate esențiale pentru prosperitatea Republicii Moldova. Această narațiune este adesea însoțită de nostalgie față de stabilitatea din perioada sovietică și de promisiuni privind gazul rusesc ieftin.

De ce este falsă: Această afirmație ignoră faptul că Rusia a întrerupt în repetate rânduri livrările de gaze către Republica Moldova ca mijloc de presiune politică, în timp ce Uniunea Europeană a oferit sprijin energetic de urgență. Aderarea la Uniunea Europeană oferă acces la o piață de aproximativ 450 de milioane de consumatori. Statele care au aderat la Uniunea Europeană – inclusiv România, Polonia și statele baltice – au înregistrat o creștere economică semnificativă, nu un colaps economic.



Încercați: Exercițiul „Identificați tactica”



„Toți politicienii sunt corupți”

Afirmația potrivit căreia nu există nicio diferență semnificativă între opțiunile politice, astfel încât participarea la vot este lipsită de sens. Această narațiune demobilizează alegătorii și îi avantajează pe cei care au de câștigat de pe urma unei prezențe scăzute la vot.

De ce este falsă: Scopul acestei narațiuni nu este informarea publicului, ci descurajarea participării la vot. Corupția există, însă afirmația că „toți sunt la fel” ignoră diferențele reale dintre candidați și programele lor politice. Dacă votul nu ar avea nicio importanță, nimeni nu ar investi resurse pentru a descuraja exercitarea acestui drept.

Durată: 10–15 minute

Mărimea grupului: 2–3 participanți

Materiale necesare: telefoane mobile

Desfășurarea exercițiului:

- 1 Fiecare participant parcurge feed-ul de conținut dintr-o rețea socială și identifică o postare care pare suspectă sau manipuloare.
- 2 Participanții prezintă, pe rând, exemple identificate. Ceilalți încearcă să stabilească tactica utilizată și să explice argumentele care susțin această concluzie.
- 3 Grupul discută împreună: Cum poate fi verificată informația? Care ar fi reacția cea mai potrivită: ignorarea, verificarea sau raportarea conținutului?

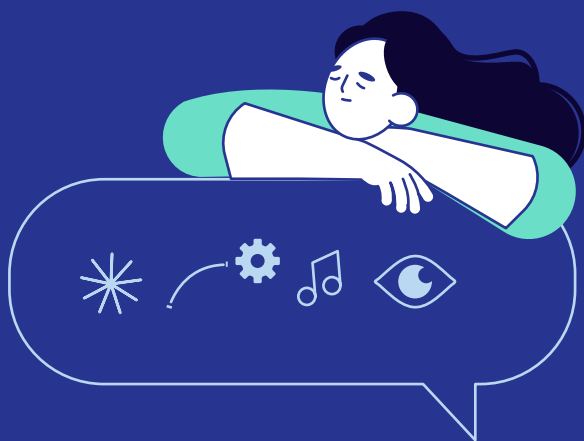
Scopul este exersarea. Cu cât această activitate este repetată mai des, cu atât tiparele vor fi recunoscute mai repede.

Înțelegerea Inteligenței Artificiale



Partea 4

Probabil că majoritatea oamenilor au auzit deja multe despre inteligența artificială – la știri, la școală, de la prieteni sau de la persoane care încearcă să le vândă un produs ori un serviciu. Această secțiune explică ce este, în realitate, inteligența artificială, de ce este importantă pentru orientarea în mediul informațional actual și ce măsuri practice pot fi luate pentru utilizarea ei în mod responsabil.



Ce este, de fapt, inteligența artificială?

Inteligența artificială (IA) este o tehnologie care învață din cantități mari de date – texte, imagini, înregistrări audio și materiale video – și folosește ceea ce învață pentru a genera conținut nou sau pentru a lua decizii.

Inteligența artificială nu este magie. Nu este conștientă. Nu „gândește” așa cum gândesc oamenii. Ea reprezintă un ansamblu de procese matematice care identifică tipare în cantități uriașe de date și utilizează aceste tipare pentru a face predicții sau a genera rezultate.

Acest lucru este important deoarece explică atât ce poate face inteligența artificială, cât și ce nu poate face:

Ce poate face inteligența artificială:

- ▶ Să genereze texte, imagini, materiale audio și video care par și sună convingător.
- ▶ Să proceseze informații mult mai rapid decât oamenii.
- ▶ Să identifice tipare în date pe care oamenii le-ar putea omite.
- ▶ Să automatizeze sarcinile repetitive.

Ce nu poate face inteligența artificială:

- ▶ Să furnizeze informații 100 % exacte și adevărate. Inteligența artificială poate genera informații false sau inexacte prezentate ca fiind credibile. Din acest motiv, rezultatele generate de IA trebuie întotdeauna verificate.

- ▶ Să înțeleagă contextul în același mod în care îl înțeleg oamenii.
- ▶ Să își asume responsabilitatea pentru rezultatele pe care le generează.
- ▶ Să înlocuiască judecata umană în chestiuni importante.
- ▶ Să determine dacă rezultatele pe care le generează vor face rău cuiva, vor induce oamenii în eroare sau vor crea panică. Responsabilitatea pentru modul în care este utilizat conținutul generat de inteligența artificială revine întotdeauna utilizatorilor umani.

Ce este „inteligența artificială generativă”?

Probabil că ați întâlnit deja instrumente precum ChatGPT, Google Gemini, Claude sau generatoare de imagini, precum Midjourney. Acestea sunt exemple de inteligență artificială generativă – sisteme capabile să creeze conținut nou, nu doar să analizeze conținutul existent.

Tipuri de inteligență artificială generativă

Tipul de rezultat	Ce poate produce IA generativă	Exemple de instrumente	Observații
Text 	Articole, eseuri, postări pe rețelele sociale, e-mailuri, cod, scenarii	ChatGPT, Claude, Gemini, Copilot	Utilizate pentru redactare, rezumare, programare și elaborarea diferitelor tipuri de conținut.
Imagini 	Fotografii, ilustrații, opere de artă, grafică	Midjourney, DALL-E, Stable Diffusion	Pot crea imagini realiste sau artistice pe baza unor instrucțiuni formulate în limbaj natural (prompturi).
Audio 	Clone vocale, muzică, efecte sonore	Diverse generatoare de voce și muzică bazate pe IA, precum ElevenLabs	Câteva secunde din vocea unei persoane pot fi suficiente pentru a genera un nou fișier audio în care aceasta pare să spună orice.
Video 	Videoclipuri sintetice, înlocuirea feței (face swap), sincronizarea mișcărilor buzelor cu un alt sunet (lip-sync)	Diverse instrumente de deepfake și IA pentru generarea de materiale video, precum Veo	Permit crearea unor deepfake-uri realiste - înregistrări video, audio sau imagini manipulate cu ajutorul inteligenței artificiale.



De ce este important acest lucru în Republica Moldova?

Conținutul generat de inteligența artificială este deja utilizat pentru a manipula oamenii, inclusiv în Republica Moldova.

Videoclipurile false apar adesea înaintea unor evenimente importante, precum alegeri, discursuri oficiale sau situații de criză, atunci când oamenii sunt mai predispuși să reacționeze emoțional și să distribuie rapid conținutul. În decembrie 2023, un videoclip deepfake a fost publicat pe Telegram cu puțin timp înainte de tradiționalul mesaj de Anul Nou al președintei Maia Sandu. Materialul, generat cu ajutorul inteligenței artificiale, prezenta o sosie a președintei Maia Sandu care ironiza nivelul de trai al cetățenilor, îi îndemna să îi susțină re alegerea și îi prezenta pe George Soros și Statele Unite drept „sponsori” ai conducerii pro-europene a Republicii Moldova – una dintre principalele teme ale dezinformării ruse care vizează țara. Președinția Republicii Moldova a negat autenticitatea videoclipului și l-a condamnat ca parte a războiului hibrid purtat de Rusia împotriva instituțiilor democratice ale Republicii Moldova.

Acestea nu sunt cazuri izolate. Ele fac parte dintr-un tipar. Pe măsură ce instrumentele de inteligență artificială devin mai accesibile și mai ușor de utilizat, volumul de conținut sintetic va continua să crească.

Acest lucru creează două probleme:

- ▶ Există riscul ca informații false să fie considerate adevărate. Un videoclip sau un fișier audio fals, dar convingător, se poate răspândi mai repede decât pot reacționa verificatorii de fapte.
- ▶ Există riscul pierderii încrederii în orice informație. Atunci când totul pare că ar putea fi fals, unii oameni ajung la concluzia că nu se mai poate avea încredere în nimic. Și aceasta reprezintă o victorie pentru manipulatori. Confuzia și cinismul le servesc scopurile la fel de bine ca și convingerea oamenilor să creadă anumite minciuni.



Sursă: Info1.md⁶¹

Scopul nu este de a genera suspiciune excesivă, ci de a oferi instrumente practice pentru orientarea în acest mediu, fără a fi nici naivi, nici paralizați de neîncredere.

Cum poate fi verificat dacă un conținut este generat de IA

Detectarea conținutului generat de inteligența artificială devine din ce în ce mai dificilă. În urmă cu un an, imaginile generate de IA prezentau adesea erori evidente – degete în plus, text deformat sau fundaluri nefirești. Instrumentele disponibile astăzi au corectat multe dintre aceste probleme. Instrumentele de mâine vor corecta și mai multe.

Cu toate acestea, există instrumente gratuite care pot fi de ajutor. Niciunul nu este perfect – pot să nu detecteze unele falsuri și, uneori, pot identifica în mod eronat conținut autentic drept fals. Aceste instrumente trebuie utilizate ca o sursă suplimentară de informații, nu ca o concluzie definitivă.

Pentru imagini

Google Reverse Image Search

Permite încărcarea unei imagini sau introducerea adresei URL pentru a vedea unde mai apare aceasta online. Dacă o imagine prezentată ca fiind „nouă” circulă de luni sau ani ori apare pe site-uri cunoscute pentru publicarea de informații false, acest lucru poate constitui un indiciu important.

► <https://images.google.com>
(faceți clic pe pictograma aparatului foto)

TinEye

Un alt instrument de căutare inversă a imaginilor. Este util pentru identificarea sursei originale a unei imagini și pentru a verifica dacă aceasta a fost modificată

► <https://tinEye.com>

Hive Moderation

Permite încărcarea unei imagini pentru a verifica probabilitatea ca aceasta să fi fost generată de inteligența artificială. Oferă un scor de probabilitate.

► <https://hivemoderation.com/ai-generated-content-detection>

AI or Not

Interfață simplă care permite încărcarea unei imagini și oferă o evaluare privind probabilitatea ca aceasta să fi fost generată de inteligența artificială.

► <https://www.aiornot.com>

FotoForensics

Analizează imaginile pentru a identifica semne de editare și manipulare. Este un instrument mai tehnic, dar util pentru detectarea modificărilor

► <https://fotoforensics.com>

Pentru videoclipuri

InVID Verification Plugin

Extensie pentru browser (Chrome/Firefox), dezvoltată pentru jurnaliști. Extrage cadre din videoclipuri, verifică metadatele și efectuează căutări inverse ale imaginilor pentru fiecare cadru. Este un instrument esențial pentru verificarea conținutului video viral.

► <https://www.invid-project.eu/tools-and-services/invid-verification-plugin/>

Deepware Scanner

Permite încărcarea unui videoclip pentru a verifica dacă acesta a fost manipulat prin tehnica deepfake. Analizează inconsecvențele faciale și alte artefacte specifice manipulării digitale.

► <https://deepware.ai>

Pentru text

GPTZero

Permite introducerea unui text pentru a verifica probabilitatea ca acesta să fi fost generat de inteligența artificială. Este utilizat pe scară largă în domeniul educației.

► <https://gptzero.me>

ZeroGPT

Are o funcție similară: analizează textul pentru a identifica tipare caracteristice conținutului generat de inteligența artificială.

► <https://www.zerogpt.com>

Pentru verificare generală

Google Fact Check Explorer

Permite căutarea unor afirmații pentru a verifica dacă acestea au fost deja analizate de organizații specializate în verificarea faptelor.

► <https://toolbox.google.com/factcheck/explorer>

InVID WeVerify

Combină mai multe instrumente de verificare într-un singur plugin, inclusiv căutarea inversă a imaginilor, analiza materialelor video și alte funcții utile pentru verificarea conținutului online.

► <https://weverify.eu/verification-plugin/>

De reținut

Aceste instrumente sunt utile, dar au limite și nu sunt 100% precise.⁶² Tehnologia de generare a conținutului cu ajutorul inteligenței artificiale evoluează mai rapid decât tehnologia de detectare. Un instrument care detectează conținut fals astăzi s-ar putea să nu îl mai detecteze mâine.

Atunci când rezultatele oferite de aceste instrumente sunt neclare, este recomandată verificarea adițională a informațiilor:

- Poate fi identificată sursa originală?
- Informația este relatată de instituții media credibile?
- Persoana sau organizația menționată în conținut a confirmat informația?
- Cine ar avea de câștigat dacă această informație ar fi considerată adevărată?

Utilizarea responsabilă a IA

Numeroase persoane utilizează deja instrumente de inteligență artificială – pentru activități școlare, proiecte creative sau pur și simplu pentru divertisment. Inteligența artificială devine parte din viața de zi cu zi, ceea ce face cu atât mai importantă înțelegerea limitelor sale.

Inteligența artificială poate inventa informații.

Dacă ChatGPT este întrebat despre fapte, referințe sau citate, este posibil să furnizeze informații inventate. Afirmările importante trebuie întotdeauna verificate în surse originale.

Inteligența artificială reflectă datele cu care a fost antrenată.

Sistemele de inteligență artificială învață din conținut existent, care include prejudecăți, erori și informații învechite. Acestea nu au acces la evenimentele curente decât dacă au fost concepute special pentru acest lucru.

Rezultatele generate de inteligența artificială nu sunt „proprii”.

Prezentarea unui text generat de IA ca fiind propria lucrare, fără menționarea utilizării acestui instrument, reprezintă o practică necinstită față de profesori, colegi și față de propria persoană. Inteligența artificială ar trebui utilizată ca un instrument care sprijină gândirea, nu ca un înlocuitor al acesteia.

Inteligența artificială amplifică ceea ce primește.

Dacă este utilizată pentru a genera conținut care răspândește dezinformare, manipulează alte persoane sau le provoacă prejudecii, responsabilitatea revine utilizatorului, nu instrumentului.

Persoana care utilizează inteligența artificială pentru a crea conținut rămâne responsabilă pentru rezultatul obținut.



Încercați: Provocarea de identificare a conținutului generat de IA

Durată: 10 minute

Mărimea grupului: 2 sau mai mulți participanți

Materiale necesare: telefoane cu acces la internet

Desfășurarea exercițiului:

- 1 Toți accesează site-ul <https://whichfaceisreal.com> de pe telefonul mobil.
- 2 Site-ul afișează două fețe alăturate – una este fotografia unei persoane reale, iar cealaltă este generată de inteligența artificială. Scopul este identificarea fotografiei reale.
- 3 Fiecare participant parcurge 10 runde.
- 4 Câștigă participantul care obține cele mai multe răspunsuri corecte.
- 5 La final, discutați împreună: Ce a făcut ca imaginile generate de IA să fie greu de identificat? Ce indicii au fost utile pentru a le diferenția?

Cu cât este exersată mai des observarea atentă, cu atât devine mai ușoară identificarea indiciilor relevante. Chiar și atunci când nu există certitudine, se dezvoltă capacitatea de a recunoaște conținutul care merită analizat cu mai multă atenție.

Abilități practice pentru autoapărare în mediul informațional



Partea 5

Verificarea nu este suficientă



Partea a treia a prezentat modalitățile de recunoaștere a manipulării și de verificare a conținutului suspect. Însă, de cele mai multe ori, manipularea își atinge scopul înainte de a trezi suspiciuni. Ea exploatează obiceiurile automate și inconștiente de consum al informației – modul în care oamenii derulează conținutul, reacționează și îl distribuie.

Scopul acestei părți este dezvoltarea unor obiceiuri care reduc vulnerabilitatea la manipulare.



Pauza

Cel mai simplu și eficient obicei este o scurtă pauză înainte de distribuirea unui conținut. Dezinformarea are succes deoarece provoacă reacții emoționale imediate, care ocolesc gândirea critică.

Întreruperea acestui proces durează mai puțin de treizeci de secunde.

Înainte de distribuirea unui conținut, este util să fie luate în considerare câteva întrebări:

- ▶ De unde provine acest conținut? Este cunoscută sursa?
- ▶ Ce s-ar putea întâmpla dacă informația este greșită? Cine ar putea fi afectat?
- ▶ Ce emoții încearcă să provoace?

Dacă nu există răspunsuri clare la aceste întrebări, este mai prudent ca informația să nu fie distribuită. O regulă utilă este: cu cât emoțiile sunt mai intense, cu atât distribuirea ar trebui făcută cu mai multă prudență. Costul așteptării este redus, însă răspândirea unor informații false poate avea consecințe mult mai serioase.

Înțelegeți ce tip de conținut aveți în față

Nu tot conținutul urmărește același scop, iar recunoașterea diferențelor dintre tipurile de conținut este esențială pentru orientarea în mediul online.

▶ **Reportajele de știri** au scopul de a informa. Jurnalistul investighează, interviează surse și prezintă fapte. Un reportaj de calitate explică ce s-a întâmplat, cine a fost implicat și ce dovezi susțin relatarea. Opinia jurnalistului ar trebui să rămână în plan secund.

▶ **Opiniile și comentariile** au scopul de a convinge. Autorul adoptă o poziție și aduce argumente în sprijinul acesteia. Acest lucru este legitim, deoarece democrațiile se bazează pe dezbateri, însă nu este același lucru cu jurnalismul de știri. O opinie poate fi bine argumentată sau slab fundamentată, echilibrată sau manipulatoră. Esențial este să fie recunoscut faptul că este vorba despre un argument, nu despre o relatare neutră.

▶ **Publicitatea** are scopul de a vinde. Cineva plătește pentru a obține atenția publicului deoarece urmărește un anumit obiectiv – obținerea banilor, a datelor personale sau a sprijinului electoral. Acest lucru este valabil indiferent dacă sunt promovate produse, candidați politici sau ideologii.

▶ **Conținutul sponsorizat** estompează granițele dintre toate aceste categorii. El arată ca un articol sau o postare obișnuită, însă o companie sau o organizație a plătit pentru publicarea lui. Cel mai responsabil conținut sponsorizat este etichetat în mod clar. Cel mai înșelător este conceput pentru a crea impresia că este jurnalism independent, când, în realitate, reprezintă promovare plătită.

Manipularea funcționează adesea prin prezentarea unui tip de conținut drept altul. Propaganda este prezentată ca știre. Reclamele sunt deghizate în recomandări personale din partea unor persoane de încredere. Opiniile sunt prezentate ca fapte certe. Mesajele politice sunt ambalate sub forma divertismentului sau a umorului pentru a ocoli filtrele critice ale publicului.

Formarea obiceiului de a întreba „Ce tip de conținut este acesta?” înainte de a interacționa cu un material creează un punct de verificare mental. Acest lucru nu stabilește dacă informația este adevărată, dar ajută la înțelegerea scopului urmărit de conținut – iar acest lucru ar trebui să determine gradul de spirit critic cu care este analizat.

Pași practici: Testul CRAAP

Testul CRAAP este o metodă de evaluare a informațiilor. Acronimul CRAAP provine din termenii englezi Currency (**Actualitate**), Relevance (**Relevanță**), Authority (**Autoritate**), Accuracy (**Acuratețe**) și Purpose (**Scop**). Acest test oferă un set de întrebări care ajută la evaluarea naturii și credibilității informațiilor identificate.⁶³

► Actualitate – Cât de actuală este informația?

- Când a fost publicată sau distribuită informația?
- Informația a fost revizuită sau actualizată?
- Subiectul analizat necesită informații recente sau pot fi utilizate și surse mai vechi?
- Linkurile sunt funcționale?
- Observați ce lipsește: Materialele jurnalistice credibile indică sursele și oferă detalii care pot fi verificate. Dacă o postare conține afirmații puternice, dar nu prezintă dovezi sau nu indică sursa informațiilor, aceasta ar trebui tratată, în cel mai bun caz, ca o opinie.

► Relevanță – Cât de relevantă este informația pentru scopul urmărit?

- Informația este relevantă pentru subiectul analizat sau răspunde la întrebarea formulată?
- Cui îi este destinat acest conținut?
- Nivelul de prezentare a informației este adecvat scopului urmărit (adică nu este nici prea elementar, nici prea avansat)?
- Au fost consultate mai multe surse înainte de a decide utilizarea acestora?
- Ar putea această sursă fi citată cu încredere într-o lucrare de cercetare?

► Autoritate – Care este sursa informației?

- Cine este autorul, editorul, sursa sau sponsorul conținutului?
- Este vorba despre un cont anonim, contul unei companii sau al unei organizații ori despre un creator de conținut care ar putea fi remunerat pentru a promova un anumit mesaj sau produs?
- Care sunt calificările autorului sau afilierea sa instituțională?
- Are autorul competența necesară pentru a scrie despre acest subiect?

► Acuratețe – Cât de fiabil, veridic și corect este conținutul?

- De unde provin informațiile?
- Sunt informațiile susținute de dovezi?
- Informațiile au fost verificate sau evaluate de experți?
- Pot fi verificate unele dintre informații prin consultarea altor surse credibile sau pe baza unor cunoștințe confirmate?
- Limbajul și tonul sunt imparțiale și lipsite de încărcătură emoțională?
- Există greșeli de ortografie, gramatică sau tehnoredactare?

► Scop – De ce există această informație?

- Care este scopul informației? Este de a informa, de a educa, de a vinde, de a distra sau de a convinge?
- Autorii sau sponsorii își prezintă în mod clar intențiile sau scopul?
- Informația reprezintă un fapt, o opinie sau propagandă?
- Punctul de vedere prezentat pare obiectiv și imparțial?
- Sunt vizibile prejudecăți sau orientări politice, ideologice, culturale, religioase, instituționale ori personale?
- Sunt prezente etichete precum „opinie”, „editorial”, „sponsorizat”, „parteneriat plătit”, „publicitate” sau „promovat”?

Acestea indică faptul că materialul urmărește un anumit scop sau promovează o anumită agendă. Acest lucru nu înseamnă că informația este falsă, dar influențează modul în care ar trebui interpretată.

► Conținutul care arată ca o știre, dar urmărește în principal să convingă publicului, necesită o atenție deosebită. Dacă un „articol” încearcă să provoace o anumită reacție emoțională sau să conducă la o anumită concluzie politică fără a prezenta și alte perspective relevante, este puțin probabil să reprezinte o relatare neutră.

din mass-media în limba rusă, consultați ocazional și surse în limba română.

► Căutați din când în când informații direct, folosind motoare de căutare, în loc să vă bazați exclusiv pe recomandările algoritmilor.

Diversificarea surselor de informare

Atunci când informațiile provin exclusiv din surse care confirmă convingerile existente, manipularea devine mai greu de observat. Conținutul pare firesc și credibil. Algoritmii tind să ofere tot mai mult din ceea ce atrage deja atenția utilizatorilor, creând un cerc de auto-confirmare. Diversificarea surselor nu înseamnă crearea unui fals echilibru între „ambele părți”, ci ieșirea din bula informațională creată de filtrele algoritmice.

Pași practici:

- Nu vă bazați pe o singură sursă de informare (de exemplu, un singur creator de conținut, forum sau blog). Includeți în mod regulat cel puțin o sursă de știri credibilă care prezintă uneori perspective diferite.
- Comparați modul în care aceeași știre este prezentată de surse diferite – nu doar dacă este relatată, ci și cum este relatată. De exemplu, dacă informațiile provin în principal

Evitați „doom-scrolling”-ul

„Doomscrolling”-ul este obiceiul de a consuma în mod compulsiv și neîntrerupt știri negative, în special înainte de culcare. Cercetările arată că acest obicei crește nivelul de anxietate, fără a conduce la o mai bună informare. Observarea tendinței de a derula compulsiv conținut tulburător reprezintă un semnal de avertizare. O modalitate practică de a reduce acest obicei este stabilirea unui moment clar în care telefonul este lăsat în afara dormitorului. Dacă telefonul nu este la îndemână, tentația de a continua derularea conținutului este mult mai mică.

Recunoașterea argumentelor de rea-credință

Dezacordul, în sine, nu reprezintă o formă de manipulare. Dezbateră deschisă este o componentă esențială a democrației. Cu toate acestea, nu orice argument urmărește descoperirea adevărului sau o mai bună înțelegere a unei probleme. Unele argumente sunt formulate pentru a crea confuzie, a reduce la tăcere interlocutorul sau pur și simplu pentru a-l epuiza. Recunoașterea acestor tactici facilitează evaluarea situațiilor în care o conversație rămâne constructivă și a celor în care cineva ar putea argumenta cu rea-credință.



Atacul la persoană (Ad hominem)

Atacarea persoanei în locul argumentelor sale. Scopul este discreditarea sau reducerea la tăcere a interlocutorului, fără a răspunde la ceea ce acesta a spus în realitate.

► Exemplu

„Cred că parcursul Republicii Moldova către Uniunea Europeană oferă oportunități economice reale.”

„Normal că spui asta, ești plătit de Soros.”

► **Cum se poate răspunde:** Reacția firească este de a încerca să se demonstreze că acuzația este nefondată. Totuși, o apărare continuă nu face decât să distragă atenția de la argumentele prezentate – exact ceea ce urmărește interlocutorul.

Schimbarea subiectului (Whataboutism)

Devierea criticii prin invocarea unui subiect fără legătură cu discuția. În loc să răspundă la problema ridicată, interlocutorul schimbă subiectul, invocând presupusele greșeli ale altcuiva.

► Exemplu

„Interferența Rusiei în alegerile din Republica Moldova este o problemă gravă.”

„Dar cum rămâne cu interferența americană?
Dar cu NATO?”

► **Cum se poate răspunde:** Remarcați încercarea de a devia discuția, fără a permite deturnarea conversației: „Putem discuta despre acest subiect separat. În acest moment, discuția se referă la această problemă specifică.” Mențineți discuția la subiect.

Inundarea cu argumente (Gish Gallop)

Copleșirea interlocutorului cu un număr foarte mare de afirmații, statistici și surse – multe dintre ele false sau irelevante – astfel încât verificarea tuturor devine imposibilă. Scopul este de a crea impresia că interlocutorul este neinformațat sau de a-l determina să renunțe la discuție.

► Exemplu

Cineva prezintă zeci de afirmații potrivit cărora referendumul privind aderarea la UE ar fi fost ilegal, invocând legi puțin cunoscute, experți anonimi și statistici aleatorii. Verificarea fiecărei afirmații ar necesita ore întregi.

► **Cum se poate răspunde:** Nu încercați să răspundeți tuturor afirmațiilor. Alegeți o singură afirmație – pe cea mai specifică sau mai ușor de verificat – și verificați-o. Dacă se dovedește a fi falsă, semnați acest lucru.

Omul de paie (Straw man)

Prezentarea denaturată a poziției interlocutorului, urmată de atacarea acestei versiuni distorsionate. În loc să răspundă argumentelor reale, interlocutorul combate un „om de paie” pe care l-a construit el însuși.

► Exemplu

„Cred că ar trebui să consolidăm educația media în școli.”

„Deci vreți ca guvernul să le spună copiilor ce să gândească? Asta înseamnă cenzură.”

► **Cum se poate răspunde:** Corecți denaturarea argumentului înainte de a continua discuția. De exemplu: „Nu asta am spus. M-am referit la educația media, nu la propaganda guvernamentală. Permiteți-mi să îmi clarific poziția.”

Deturnarea conversației (Topic hijacking)

Preluarea controlului asupra unei discuții și redirectionarea acesteia către un subiect complet diferit. Această tactică este deosebit de frecventă în mediul online, unde cineva poate inunda o secțiune de comentarii sau poate deturna un hashtag.

► Exemplu

O postare pe Facebook despre un proiect local de infrastructură este inundată de comentarii precum „Când va demisiona Sandu?” Deși nu au nicio legătură cu subiectul, acestea ajung să domine întreaga discuție.

► **Cum se poate răspunde:** În conversațiile proprii, spuneți-o direct: „Acesta este un alt subiect. Putem termina mai întâi această discuție?” În secțiunile publice de comentarii, nu intrați în discuție cu cei care deturnează conversația – urmăresc doar să atragă atenția. Rămâneți la subiectul inițial.

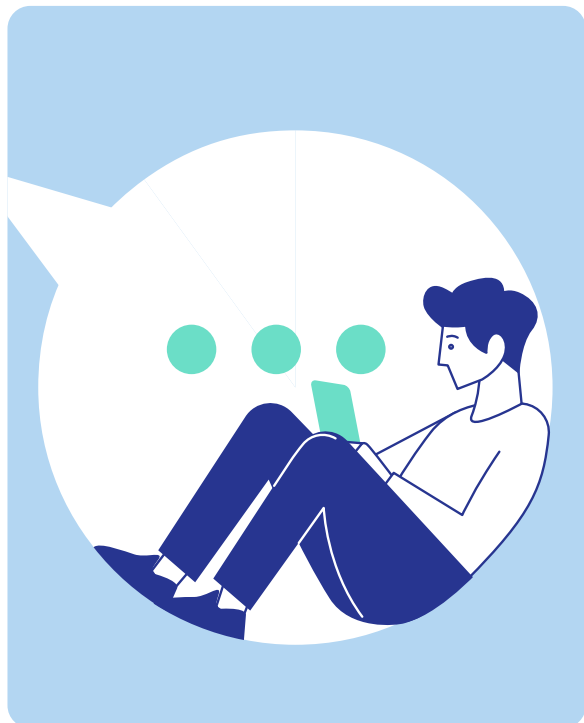
Echilibru fals

Prezentarea a două poziții ca fiind la fel de valide, deși dovezile susțin în mod clar una dintre ele. Această tactică creează o îndoială artificială.

► Exemplu

„Unii spun că vaccinurile sunt sigure, alții spun că sunt periculoase. Cine știe cu adevărat?”

► **Cum se poate răspunde:** Evidențiați dezechilibrul dintre dovezi. „Nu este, de fapt, o situație de tipul «unii spun, alții spun». Consensul științific covârșitor este clar. Faptul că există câteva opinii divergente nu înseamnă că există două tabere egale.”



Încercați: Provocarea „Unchiului morocănos”

Durată: 15-20 minute

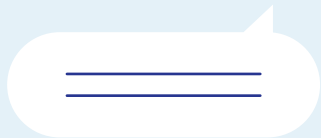
Mărimea grupului: 2 sau mai mulți participanți

Materiale necesare: telefoane sau computere cu acces la internet

Desfășurarea exercițiului:

- 1 Fiecare participant deschide aplicația Cranky Uncle pe telefon (disponibilă gratuit în App Store și Google Play) sau accesează versiunea web la <https://crankyuncle.com> (disponibilă și în limba română).
- 2 Toți participanții parcurg aceeași secțiune de întrebări, de exemplu „Erori logice” sau „Ad Hominem”.
- 3 Setați un cronometru pentru 10 minute. Fiecare participant joacă până unde reușește.
- 4 Comparați rezultatele: Cine a obținut cele mai multe puncte Cranky? Cine a atins cel mai ridicat nivel Cranky?
- 5 Discutați împreună: Care erori logice au fost cel mai dificil de identificat? Pe care le-ați întâlnit în viața de zi cu zi – în secțiunile de comentarii, în discuțiile din familie sau în dezbaterile politice?

De ce funcționează: Jocul, dezvoltat de cercetătorul în științe cognitive John Cook, ajută la identificarea a 14 tehnici de manipulare, printre care expertii falși, selectarea selectivă a informațiilor (cherry picking), atacul la persoană (ad hominem), omul de paie (straw man) și alte erori logice. Cu cât este jucat mai des, cu atât mai ușor devin de recunoscut argumentele formulate cu rea-credință în conversațiile din viața reală.

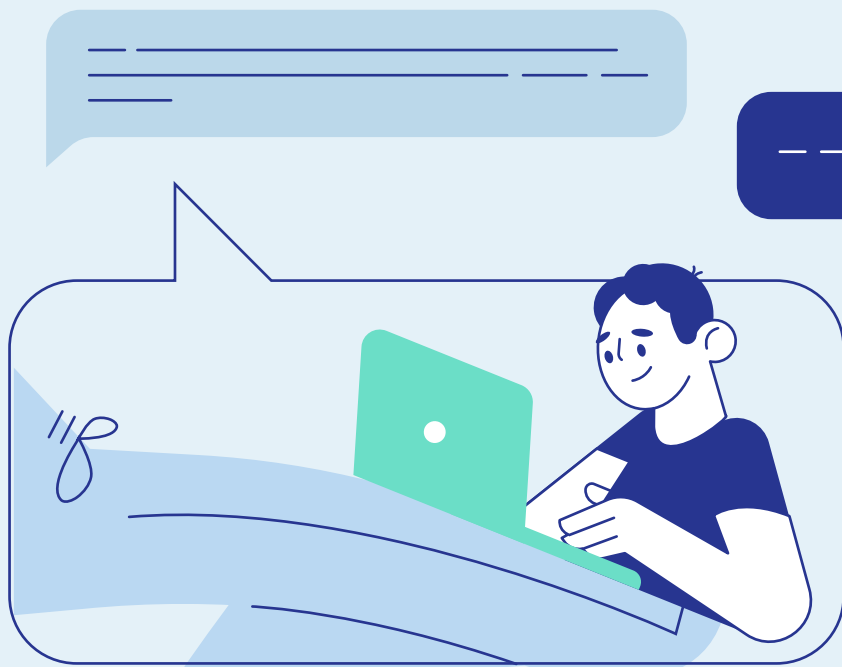


**„Educația
este cea mai
puternică armă
pe care o poți
folosi pentru
a schimba
lumea.”**

Nelson Mandela



Instrumente pentru învățare



Partea 6

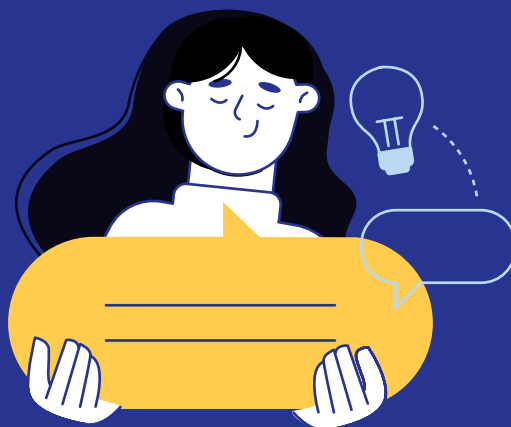
Reziliența nu este ceva ce se dobândește o singură dată și se păstrează pentru totdeauna. Ea se construiește în timp, se menține prin obiceiuri și se consolidează prin sprijinirea altor persoane să facă același lucru.

Acest manual oferă o bază pentru înțelegerea modului în care funcționează mediul informațional, a mecanismelor manipulării și a modalităților de protecție împotriva acestora. Însă simpla lectură nu este suficientă. Următorul pas este punerea în practică a acestor cunoștințe.

Această secțiune oferă instrumentele necesare pentru a continua procesul de învățare:

Învățare prin joc – jocuri gratuite dezvoltate de cercetători, care permit experimentarea din interior a tacticilor de manipulare și contribuie la formarea unor reflexe care pot fi aplicate în situații reale.

Învățare continuă – cele mai bune resurse gratuite pentru verificarea informațiilor, dezvoltarea competențelor de educație media și informarea cu privire la dezinformarea care vizează Republica Moldova.



Învățare prin joc: instrumente interactive pentru dezvoltarea rezilienței informaționale

Cercetările realizate de Universitatea din Cambridge⁶⁴ arată că jocurile reprezintă una dintre cele mai eficiente modalități de a înțelege cum funcționează manipularea informațională și cum poate fi contracarată. În loc să se limiteze la citirea despre diferite tactici, participanții le experimentează direct. Ei iau decizii, observă consecințele acestora și își dezvoltă o intuiție care poate fi aplicată în situații reale.

Jocurile recomandate în această secțiune sunt gratuite, durează doar câteva minute și au fost dezvoltate de cercetători și organizații specializate în domeniul rezilienței informaționale.



Bad News („Vești proaste”)

În Bad News, jucați rolul unei persoane care încearcă să-și crească influența folosind tehnici de dezinformare. Scopul jocului este să înțelegeți, din interior, cum sunt folosite declanșatoarele emoționale, teoriile conspirației și polarizarea pentru a atrage atenția și a influența publicul.



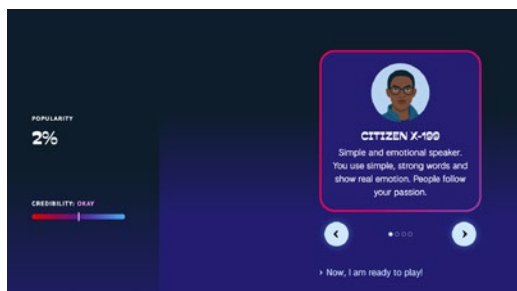
Abilități dezvoltate:

- ▶ Identificarea manipulării emoționale
 - ▶ Recunoașterea autorității false
 - ▶ Înțelegerea modului în care funcționează mecanismele de atragere și menținere a implicării publicului
- ▶ Unde se joacă: www.getbadnews.com/ro



Rig It („Trucează jocul”)

Rig It îi pune pe jucători în rolul unui candidat politic care desfășoară o campanie electorală și îi confruntă cu tehnici manipulative utilizate frecvent în timpul competițiilor electorale. Punându-i în situația de a lua decizii de campanie, jocul arată cum tacticile informaționale pot modela opinia publică și influența dinamica electorală. Această experiență practică contribuie la dezvoltarea gândirii critice, a conștientizării aspectelor etice și a încrederii în capacitatea de a gestiona informațiile din lumea reală referitoare la procesele electorale.



Competențe dezvoltate:

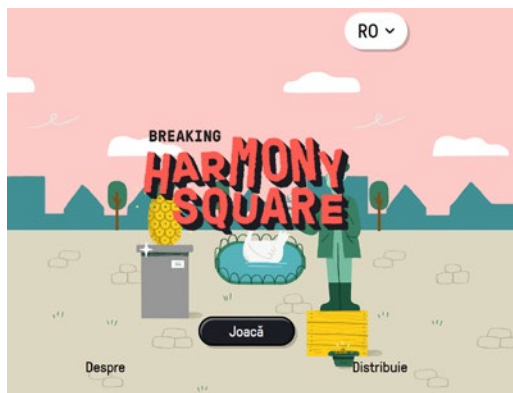
- ▶ Evaluarea credibilității informațiilor
- ▶ Înțelegerea modului în care deciziile influențează rezultatele
- ▶ Recunoașterea strategiilor de manipulare în context

▶ Unde se joacă:
<https://www.rigitgame.com>
Disponibil numai în limba engleză.



Harmony Square („Piața Armoniei”)

În Harmony Square, răspândiți în mod intenționat dezinformare într-un oraș fictiv pentru a observa cum se adâncesc diviziunile. Jocul ajută la înțelegerea modului în care campaniile și narațiunile din lumea reală pot influența coeziunea socială.



Competențe dezvoltate:

- ▶ Recunoașterea dezinformării coordonate
- ▶ Identificarea tacticilor de divizare socială
- ▶ Înțelegerea modului în care implicarea utilizatorilor stimulează răspândirea informațiilor

▶ Unde se joacă:
<https://www.harmonysquare.game/ro>



Vote for Turtle („Votează pentru broasca țestoasă”)

Vote for Turtle este un joc online scurt, dezvoltat de Uniunea Europeană, care demonstrează modul în care dezinformarea se răspândește în mediul digital. Jucătorii au misiunea de a-l ajuta pe Turtle să fie ales „Animalul de companie al anului”, folosind, pe parcurs, tactici discutabile. În doar cinci minute, jocul prezintă șase tehnici frecvent utilizate în dezinformare și arată cât de ușor conținutul fals sau înșelător poate influența opinia publică.

Punând jucătorii în rolul unui manipulator, jocul arată cum mesajele emoționale, conturile false și amplificarea coordonată pot modela dezbaterile online. Totodată, contribuie la conștientizarea modului în care dezinformarea subminează încrederea, alimentează diviziunile și perturbă procesele democratice.



Competențe dezvoltate:

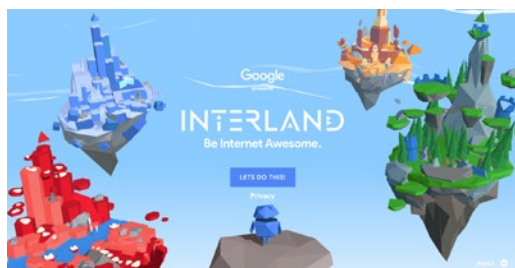
- ▶ Recunoașterea tehnicilor comune de dezinformare
- ▶ Înțelegerea modului în care narațiunile false se răspândesc în mediul online
- ▶ Identificarea mesajelor emoționale și polarizante
- ▶ Dezvoltarea rezilienței în fața conținutului manipulator

- ▶ Unde se joacă:
<https://www.voteforturtle.eu/>
Disponibil numai în limba engleză.



Interland: Be Internet Awesome („Interland: Fii grozav pe internet”)

Creat pentru jucătorii mai tineri, Interland prezintă noțiunile de bază privind siguranța pe internet, inclusiv identificarea înșelătoriilor, protejarea datelor cu caracter personal și diferențierea dintre comportamentele sigure și nesigure în mediul online.



Competențe dezvoltate:

- ▶ Formarea deprinderilor de bază privind siguranța digitală
- ▶ Identificarea conținutului suspect
- ▶ Dezvoltarea bazelor gândirii critice

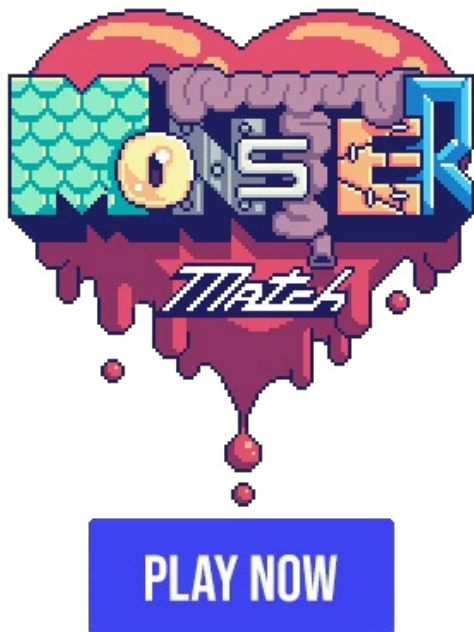
- ▶ Unde se joacă:
<https://beinternetawesome.withgoogle.com>



MonsterMatch („Potrivirea monștrilor”)

MonsterMatch este o simulare interactivă care arată modul în care algoritmi aplicațiilor de întâlniri influențează ceea ce văd utilizatorii și ceea ce nu ajunge la ei. În locul unor persoane reale, jucătorii parcurg 100 de profiluri fictive de monștri și observă cum fiecare apreciere („like”) sau respingere („dislike”) influențează profilurile care le sunt prezentate în continuare.

Jocul simplifică mecanismele complexe ale platformelor digitale de mari dimensiuni, permițând jucătorilor să înțeleagă modul în care sistemele de recomandare răspund comportamentului lor. Prin condensarea interacțiunilor a milioane de utilizatori într-o simulare ușor de urmărit, MonsterMatch face vizibile și ușor de înțeles filtrarea algoritmică, personalizarea și părtinirile algoritmice, fără presiunile asociate aplicațiilor reale de întâlniri.



Competențe dezvoltate:

- ▶ Înțelegerea modului de funcționare a algoritmilor de recomandare
- ▶ Recunoașterea buclelor de feedback din cadrul platformelor digitale
- ▶ Identificarea modului în care comportamentul utilizatorilor modelează experiențele online
- ▶ Dezvoltarea unei înțelegeri critice a modului în care sunt concepute platformele digitale

▶ Unde se joacă:

<https://monstermatch.hiddenswitch.com>

Disponibil numai în limba engleză.



Cyber Defenders („Apărătorii cibernetici”)

Cyber Defenders este un joc realizat pe platforma Roblox, dezvoltat de Europol, care îi pune pe jucători în rolul unui agent digital însărcinat cu identificarea infractorilor cibernetici și rezolvarea unor mistere online. Prin intermediul unor chestionare, ghicitori și mecanisme de clasificare, jucătorii sunt familiarizați cu amenințările comune asociate criminalității cibernetice într-un format interactiv și captivant, specific platformei. Conceput pentru un public tânăr, familiarizat cu Roblox, jocul transpune conceptele de securitate cibernetică din lumea reală în provocări adaptate vârstei, fără a compromite acuratețea informațiilor.



Competențe dezvoltate:

- ➊ Recunoașterea amenințărilor și tacticilor comune ale criminalității cibernetice
- ➋ Dezvoltarea cunoștințelor de bază privind securitatea cibernetică
- ➌ Aplicarea gândirii critice pentru identificarea comportamentelor suspecte în mediul online
- ➍ Înțelegerea rolului autorităților de aplicare a legii în mediul digital

➊ Unde se joacă:
<https://www.roblox.com/games/16741761422/Cyber-Defenders>



The News Alchemist („Alchimistul știrilor”)

The News Alchemist este o simulare educațională bazată pe cărți, dezvoltată în 2024 de jurnalistul și designerul de jocuri Vladimir Bodiul, ca răspuns la intensificarea propagandei din timpul războiului din Ucraina. Jucătorii preiau rolul unui jurnalist și manipulează știri folosind cărți care reprezintă distorsiuni cognitive și erori logice frecvente – precum apelul la autoritate sau generalizarea excesivă – observând modul în care fiecare alegere editorială influențează opinia publică virtuală și modelează desfășurarea jocului.

Dezvoltat cu sprijinul Ministerului Educației și Cercetării al Republicii Moldova, jocul a fost testat cu aproximativ 500 de participanți din școli și universități. Sesiunile sunt însoțite de materiale didactice structurate, disponibile în două limbi, inclusiv un plan de lecție și un ghid pentru fiecare tip de distorsiune cognitivă.



Competențe dezvoltate:

- ▶ Recunoașterea distorsiunilor cognitive și a erorilor logice în conținutul știrilor
- ▶ Înțelegerea modului în care încadrarea și formularea mesajelor modelează percepția publică
- ▶ Reflectarea critică asupra deciziilor editoriale și a consecințelor acestora
- ▶ Conștientizarea tehnicilor de manipulare utilizate în mass-media

▶ Unde se joacă:

<https://newsalchemist.com>



Mergând mai departe: Dezvoltarea unei reziliențe durabile

Jocurile prezentate în această secțiune contribuie la dezvoltarea instinctelor necesare pentru recunoașterea manipulării. Însă reziliența înseamnă mai mult decât un reflex – este o practică ce se dezvoltă în timp. Paginile următoare oferă instrumente pentru aprofundarea cunoștințelor: resurse pentru continuarea procesului de învățare, exemple ale unor tineri care au transformat conștientizarea în acțiune și măsuri concrete pentru protecția în mediul online.

Resurse pentru continuarea învățării

Procesul de învățare nu se încheie aici. Mai jos sunt prezentate unele dintre cele mai bune resurse gratuite disponibile, majoritatea concepute special pentru tineri.

EUvsDisinfo

EUvsDisinfo este baza de date a Uniunii Europene privind cazurile de dezinformare pro-Kremlin, actualizată săptămânal. Este una dintre cele mai bune resurse pentru a observa tiparele recurente de manipulare, multe dintre acestea vizând în mod direct Republica Moldova. Consultați-o în mod regulat și veți începe să recunoașteți narațiunile înainte ca acestea să ajungă în fluxul dumneavoastră de știri. Explorați FIMI Explorer, primul tablou de bord public, interactiv și multistratificat privind activitățile de manipulare a informațiilor din străinătate⁶⁵, sau aflați mai multe despre dezinformare⁶⁶.

► euvsdisinfo.eu



StopFals.md

Platforma de verificare a faptelor din Republica Moldova. Atunci când pe rețelele sociale din Republica Moldova circulă ceva suspect în limba română sau rusă, acesta este primul loc unde puteți găsi un răspuns verificat. Gândiți-vă la ea ca la un sistem imunitar local pentru mediul informațional.

► stopfals.md



MediaWise

Cursuri online gratuite de educație media, realizate de Institutul Poynter și concepute special pentru adolescenți. Sunt scurte, practice și adaptate tipului de conținut întâlnit zilnic în mediul online. Reprezintă un bun punct de plecare pentru cei care doresc un parcurs structurat de învățare a noțiunilor de bază.

► poynter.org/mediawise



First Draft

Ghiduri și resurse de formare privind verificarea informațiilor și jurnalismul responsabil. Concepute inițial pentru jurnaliști, însă tehnicile de verificare prezentate sunt utile oricărei persoane. Ghidurile lor ilustrate de verificare sunt deosebit de practice.

► firstdraftnews.org



News Literacy Project

Resurse gratuite pentru evaluarea știrilor și a informațiilor, dezvoltate de jurnaliști pentru elevi și studenți. Include platforma virtuală de învățare Checkology, utilă pentru cei care doresc un parcurs de învățare mai structurat.

► newslit.org



Teoria inoculării / Prebunking

Cercetările profesorului Sander van der Linden și ale Cambridge Social Decision-Making Lab din cadrul Universității din Cambridge arată că prebunking-ul – explicarea modului în care funcționează tacticile de manipulare înainte ca acestea să fie întâlnite – este mai eficient decât demontarea acestora după ce au produs deja efecte (debunking). Funcționează asemenea unui vaccin: o expunere limitată și sigură la tehnica respectivă dezvoltă rezistența la aceasta. Unitatea Jigsaw a companiei Google a transpus aceste cercetări în campanii scurte de tip prebunking, testate în Europa Centrală și de Est. Jocurile prezentate anterior în această secțiune se bazează pe același principiu. Pentru informații suplimentare despre fundamentul științific al acestei abordări, accesați inoculation.science.

► inoculation.science



The SIFT Method

Dezvoltată de specialistul în educație media Mike Caulfield, metoda SIFT oferă un cadru în patru pași pentru verificarea oricărui tip de conținut:

Stop – opriți-vă înainte de a distribui un conținut sau de a reacționa la acesta.

Investigate the source – investigați sursa: cine se află în spatele acestui conținut?

Find better coverage – căutați relatări mai complete: ce spun alte surse credibile despre acest subiect?

Trace claims – urmăriți afirmațiile până la sursa lor: identificați originea citatelor, datelor și imaginilor.

Odată exersată, metoda poate fi aplicată în mai puțin de două minute și funcționează în cazul oricărui tip de conținut – un articol de știri, o fotografie virală sau un mesaj vocal redirectionat într-un grup de familie.

🔗 cor.inquirygroup.org



Tehnici de investigație digitală ale AFP

Aflați cum poate fi detectat și verificat conținutul generat de IA prin intermediul videoclipurilor, studiilor de caz și exercițiilor incluse în cursul online cu acces liber al AFP. Acesta acoperă fundamentele inteligenței artificiale și impactul acesteia asupra ecosistemului informațional, cele mai bune practici ale profesioniștilor din mass-media, precum și metode de identificare, urmărire și analiză a conținutului generat de IA.

🔗 <https://digitalcourses.afp.com/>



Manualul de educație pentru cetățenie digitală

Consiliul Europei⁶⁷ a elaborat un cadru cuprinzător și materiale didactice privind ceea ce înseamnă să fii un cetățean activ și responsabil în mediul digital. Aceste resurse sunt utile atât pentru învățarea individuală, cât și pentru organizarea de sesiuni de instruire destinate altor persoane.

Doriți să vă dezvoltați și mai mult competențele?

Bellingcat Open Source Challenge

În cadrul Bellingcat Open Source Challenge, participanții preiau rolul unui investigator open-source care încearcă să reconstituie adevărul pe baza informațiilor disponibile public. Fiecare provocare prezintă un scenariu inspirat din lumea reală – o navă suspectă aflată pe mare, o locație neidentificată dintr-o fotografie, o tranzacție financiară misterioasă – și îi provoacă pe participanți să găsească răspunsul folosind exclusiv instrumente open-source: imagini satelitare, căutarea inversă a imaginilor, baze de date pentru urmărirea navelor, rețele sociale și multe altele. Noi provocări sunt publicate în mod regulat și sunt deblocate progresiv, astfel încât pot fi parcurse în ritm propriu sau poate fi abordată direct cea mai recentă provocare. Pentru rezolvarea provocărilor, este recomandată utilizarea Bellingcat Online Open Source Investigation Toolkit, **setul de instrumente online al Bellingcat pentru investigații open-source**⁶⁸.

Competențe dezvoltate:

- ▶ Geolocalizarea imaginilor folosind indicii din mediul înconjurător, imagini satelitare și imagini la nivelul străzii.
- ▶ Urmărirea navelor, a bunurilor și a persoanelor prin intermediul bazelor de date open-source.
- ▶ Corelarea informațiilor din mai multe surse de date pentru verificarea sau infirmarea unei afirmații.
- ▶ Dezvoltarea unei gândiri investigative metodice în condiții de incertitudine.

▶ Unde vă puteți înscrie:
challenge.bellingcat.com

DFRLab Digital Sherlocks

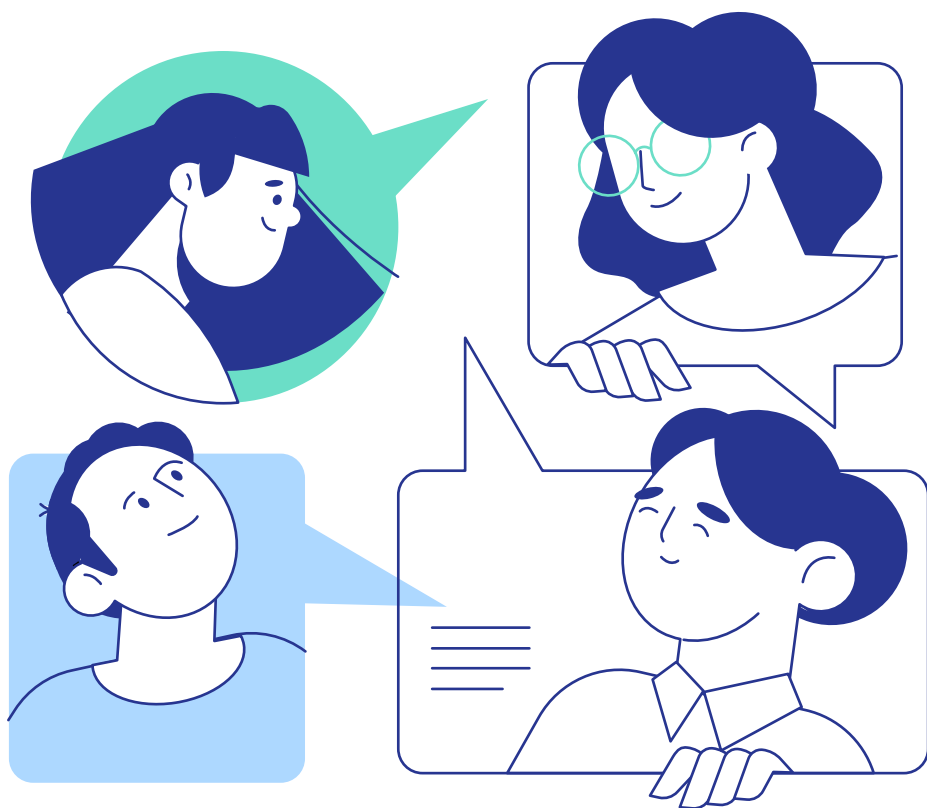
Digital Sherlocks este un program structurat de formare. Organizat anual de Digital Forensic Research Lab (DFRLab) al Atlantic Council, acesta reprezintă cea mai amplă serie gratuită de formare online din lume dedicată studenților, membrilor societății civile, jurnaliștilor și cadrelor universitare, axată pe combaterea operațiunilor informaționale și a manipulării prin utilizarea tehnicilor de investigație din surse deschise (OSINT). Programul se desfășoară pe parcursul a trei luni și include două-trei sesiuni live pe săptămână, acoperind peste douăzeci de module specializate, de la formarea unei mentalități investigative și înțelegerea operațiunilor de influență până la utilizarea instrumentelor și metodologiilor avansate.

Competențe dezvoltate:

- ▶ Înțelegerea modului în care sunt structurate și identificate operațiunile de influență și campaniile de dezinformare.
- ▶ Tehnici practice de tip OSINT: cartografierea rețelelor, analiza narațiunilor și investigații pe rețelele sociale.
- ▶ Aplicarea criminalisticii digitale în investigarea alegerilor, a zonelor de conflict și a războiului informațional.
- ▶ Consolidarea rezilienței ecosistemelor informaționale locale.

▶ Unde vă puteți înscrie:
dfrlab.org/digital-sherlocks

De la conștientizare la acțiune



Partea 7

Este important să se înțeleagă cum funcționează dezinformarea. Însă reziliența nu înseamnă doar protejarea propriei persoane, ci și contribuția la un mediu informațional mai sănătos.

Această secțiune este dedicată trecerii de la conștientizare la acțiune. Ea prezintă exemple reale de persoane care au reacționat în fața dezinformării, măsuri concrete care pot fi adoptate imediat și practici de igienă digitală care contribuie la siguranța în mediul online.



Mai mult decât identificarea dezinformări

Reziliența nu înseamnă doar protejarea propriei persoane. Ea înseamnă și contribuția la un mediu informațional mai sănătos. Înțelegerea modului în care funcționează dezinformarea este importantă, însă folosirea acestor cunoștințe pentru a-i ajuta și pe alții este și mai valoroasă.

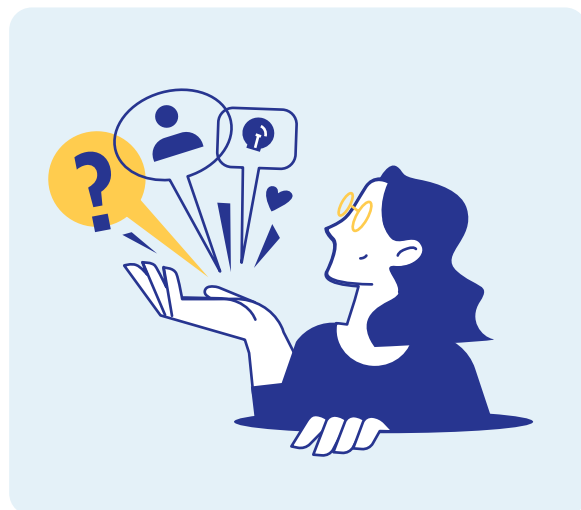
În 2014, după anexarea Crimeei de către Rusia, un grup restrâns de prieteni din Lituania a început să facă un lucru simplu: să contracareze dezinformarea pro-Kremlin în secțiunile de comentarii ale articolelor de știri online. S-au autointitulat „elfi”, deoarece, în imaginarul popular, elfii luptă împotriva trolilor. La început erau mai puțin de 50 de persoane.

Până în 2022, mișcarea ajunsese să numere mii de membri într-o rețea care cuprindea Lituania, Letonia, Estonia, Republica Cehă, Finlanda, Slovacia, Germania și Ucraina. Comunitatea este formată din studenți, medici, barmani, specialiști IT, parlamentari și radiologi. Cei mai mulți folosesc pseudonime. Nu au un sediu central, o conducere oficială sau finanțare guvernamentală. Membrii se organizează în grupuri pe Facebook și se coordonează în valuri: atunci când unul dintre ei identifică un cont fals sau un caz de dezinformare, ceilalți îl raportează în număr mare platformei. Ei corectează informațiile false din secțiunile de comentarii folosind fapte verificabile și susținute de surse. De asemenea, au participat în mod direct la acțiuni de contracarare a demonstrațiilor pro-Kremlin.

Regulile lor sunt stricte: doar fapte. Fără hacking, fără contrapropagandă și fără atacuri la persoană. După cum spune fondatorul, Ričardas Savukynas: „Minciunile pot fi combătute doar cu adevărul.”⁶⁹

„Elfii” sunt cel mai cunoscut exemplu, dar nu sunt singurii. În întreaga Europă, tinerii se implică în instituțiile democratice în moduri care contează

– prin Parlamentul European al Tineretului, schimburile Erasmus+, organizațiile civice locale și consiliile elevilor. În Republica Moldova, organizațiile societății civile care activează în domeniul educației media, al observării alegerilor și al implicării civice încurajează în mod activ participarea tinerilor. Aceste oportunități există. Întrebarea este dacă veți alege să le valorificați.



Nu este nevoie de mii de membri pentru a începe. Iată câteva lucruri concrete care pot fi făcute chiar de astăzi, indiferent unde vă aflați:

► **Raportați dezinformarea atunci când o identificați** – direct platformei pe care apare sau către StopFals.md, care documentează cazurile de dezinformare din Republica Moldova.

► **Distribuiți informații verificate** în comunitatea din care faceți parte, în special membrilor familiei care pot fi mai vulnerabili la manipulare – bunici, părinți, frați și surori mai mici.

► **Implicați-vă în viața civică locală** – participați la o ședință a consiliului local, urmăriți deciziile primarului, votați la alegerile pentru structurile de reprezentare a elevilor sau studenților și înregistrați-vă pentru a vota după împlinirea vârstei de 18 ani.

► **Înființați sau alăturați-vă unui club de educație media în școală.** Chiar și o singură întâlnire pe lună, dedicată discuțiilor conținutului care circulă în mediul online, poate contribui la dezvoltarea gândirii critice a colegilor.

► **Deveniți educatori pentru colegii voștri** – împărtășiți-le ceea ce ați învățat. Discuțiile informale sunt adesea mai convingătoare decât campaniile oficiale, deoarece încrederea dintre colegi este adesea mai mare decât încrederea acordată instituțiilor.

cu persoane în vârstă, un proiect liceal numit Cyber-Seniors, pentru a le arăta cum să utilizeze telefoanele inteligente, e-mailul, apelurile video și rețelele sociale. Programul pune în legătură adolescenți mentori cu persoane vârstnice pentru a reduce decalajul digital, oferindu-le, în același timp, tinerilor experiență practică în predare, leadership și comunicare. Cyber-Seniors s-a transformat într-o mișcare internațională, al cărei documentar a fost difuzat în 40 de țări și proiectat în peste 500 de comunități din întreaga lume. Totul a început cu doi adolescenți și bunicii lor. Atunci când ajutați o rudă în vârstă să privească critic informațiile pe care le citește online, nu o învățați doar să folosească tehnologia. Contribuiți la creșterea rezilienței întregii familii în fața dezinformării, care îi vizează în mod deosebit pe cei mai în vârstă și mai puțin familiarizați cu mediul digital.



De reflectat

„Elfii lituanieni” au pornit cu mai puțin de 50 de persoane. Au ajuns să numere zeci de mii, deoarece fiecare persoană a convins pe cineva din cercul său să se alature. Nu este nevoie să inițiați o mișcare. Este suficient să începeți o singură conversație. Cu cine din viața voastră ați putea începe această conversație chiar astăzi?

Faceți parte din soluție: Cyber-Seniors⁷⁰

Fiind tineri, probabil că știți deja mai multe despre utilizarea internetului decât majoritatea adulților din jurul vostru. Aceste cunoștințe pot fi împărtășite și în comunitatea din care faceți parte. De exemplu, în loc ca adulții să îi învețe pe tineri, tinerii îi pot învăța pe cei din generațiile mai în vârstă. În 2009, la Toronto, un grup de adolescenți pasionați de tehnologie a inițiat, împreună

Igiena digitală: Protejarea identității în mediul online

Probabil știți deja că igiena fizică este importantă – să vă spălați pe mâini, să dormiți suficient și să evitați alimentele care vă pot îmbolnăvi. Igiena digitală funcționează în același mod. Ea înseamnă protejarea datelor personale și adoptarea unui comportament responsabil în mediul online **înainte** ca ceva să meargă prost, nu **după**.

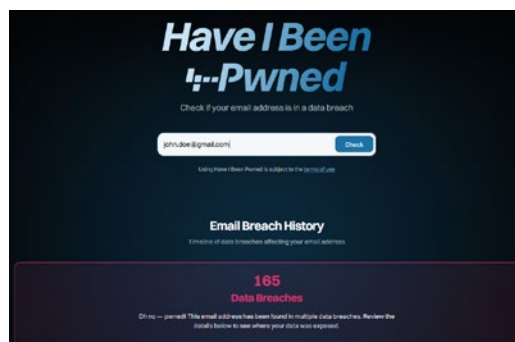
Iată un lucru care îi surprinde pe cei mai mulți oameni: deja distribuiți mult mai multe informații despre voi decât vă dați seama.

De fiecare dată când descărcați o aplicație și apăsați pe „Sunt de acord”, acordați acces la datele voastre. Fiecare fotografie pe care o realizați conține metadate invizibile – data, ora și, adesea, coordonatele GPS ale locului în care a fost făcută. De fiecare dată când folosiți opțiunea „Conectați-vă cu Google” pentru un serviciu nou, extindeți rețeaua companiilor care dețin informații despre voi. Fiecare căutare, fiecare derulare a paginii și fiecare pauză făcută în timpul vizionării unui videoclip sunt înregistrate de platforme. Privite separat, aceste informații par inofensive. Împreună însă, ele creează un profil detaliat: obiceiurile, convingerile, relațiile, rutina zilnică, starea emoțională și vulnerabilitățile voastre. Acest profil are valoare – și nu doar pentru agenții de publicitate.

Începeți de aici: Have I Been Pwned

Introduceți adresa de e-mail pe acest site gratuit și verificați dacă datele voastre au fost implicate într-o breșă de securitate cunoscută. Dacă acestea au fost compromise, veți vedea exact ce servicii

au fost afectate și ce informații au fost expuse – parole, numere de telefon sau date de localizare. Verificarea durează mai puțin de treizeci de secunde, iar rezultatele v-ar putea surprinde. Dacă descoperiți că una dintre parolele voastre a fost compromisă, schimbați-o imediat pe serviciul afectat, precum și pe orice alt serviciu unde a fost utilizată aceeași parolă.



Sursă: Have I Been Pwned™

► www.haveibeenpwned.com

Două filme care merită vizionate:

► **The Social Dilemma / Dilema socială (Netflix, 2020)** – Interviu cu ingineri și designeri care au creat sistemele de recomandare utilizate de Facebook, Instagram, YouTube și Twitter. Aceștia explică, într-un limbaj accesibil, cum aceste platforme sunt concepute pentru a capta atenția utilizatorilor și a le influența comportamentul – și de ce acest lucru are consecințe care depășesc simpla pierdere de timp.

► **The Great Hack / Marele furt de date (Netflix, 2019)** – Povestea Cambridge

Analytica, compania britanică de analiză a datelor care a colectat datele cu caracter personal ale zecilor de milioane de utilizatori Facebook fără consimțământul acestora și le-a folosit pentru a crea profiluri psihologice destinate direcționării mesajelor către alegători din Statele Unite și Regatul Unit. O ilustrare clară a consecințelor pe care le poate avea ajungerea datelor cu caracter personal în mâini nepotrivite.

Lista de verificare pentru igiena digitală:

► Folosiți o parolă puternică și unică pentru fiecare cont sau utilizați un manager de parole, precum **Bitwarden** (gratuit și open-source), astfel încât să fie nevoie să rețineți o singură parolă – cea folosită pentru autentificarea în managerul de parole.

► Activați **autentificarea în doi pași** pentru fiecare cont care oferă această opțiune. Chiar dacă cineva vă află parola, nu va putea accesa contul fără telefonul vostru.

► Verificați dacă adresa voastră de e-mail sau numărul vostru de telefon au fost afectate de o breșă de securitate: haveibeenpwned.com

► Verificați setările de confidențialitate ale conturilor de pe rețelele sociale. Cine vă poate vedea postările? Lista de prieteni? Locația? Majoritatea platformelor sunt configurate implicit să partajeze mai multe informații decât ați dori.

► Gândiți-vă cu atenție înainte de a publica informații despre școala voastră, cartierul în care locuiți, rutina zilnică sau fotografii făcute în interiorul locuinței. Infractorii cibernetici și persoanele care hărțuiesc alte persoane pot folosi aceste informații pentru a vă construi profilul și a afla mai multe despre voi.

► Înainte de a accesa un link – mai ales dintr-un mesaj primit de la o persoană pe care nu o cunoașteți bine – opriți-vă pentru o clipă. Verificați cu atenție adresa URL. Dacă ceva pare suspect, accesați direct site-ul oficial. Verificați cu atenție linkurile, în special pe cele din reclamele de pe rețelele sociale.

► Descărcați aplicații numai din magazinele oficiale (Google Play, App Store). Ștergeți aplicațiile pe care nu le mai utilizați – acestea pot continua să colecteze date în fundal. Dacă descărcați o versiune piratată a unui program, este foarte probabil ca aceasta să conțină programe malware sau viruși.

► Rețineți: dacă o aplicație este gratuită, de multe ori voi sunteți produsul. Atenția și datele voastre sunt cele care se vând. Gândiți-vă de două ori dacă o nouă aplicație de lanternă are într-adevăr nevoie de acces la portofelul vostru digital.



De reflectat

Fiecare informație pe care o distribuiți în mediul online reprezintă o piesă dintr-un puzzle. Privite împreună, aceste informații creează un profil detaliat – obiceiurile, convingerile, relațiile și vulnerabilitățile voastre. Acest profil poate fi folosit pentru a vă direcționa conținut conceput special pentru a vă influența și a vă schimba opiniile. Cât de mult din acest profil ați dori să fie accesibil unui guvern străin – sau oricărei persoane ori organizații care acționează împotriva intereselor voastre?

Exerciții practice pentru profesori



Anexă

Cum se utilizează această anexă

Această anexă conține patru exerciții pentru activități desfășurate în sala de clasă. Fiecare exercițiu include două componente:

- Versiunea pentru profesori – ghid de facilitare, obiective, întrebări pentru discuții și recomandări metodice.
- Fișa de lucru pentru elevi – material gata de fotocopiat și distribuit elevilor.

► Exercițiile sunt concepute fie ca lecții complete de 45 de minute, fie ca activități scurte, cu o durată de 15–20 de minute.

► Etichete: Gimnaziu = clasele V–IX (aproximativ 11–15 ani); Liceu = clasele X–XII (aproximativ 16–19 ani).

► Exercițiile nu trebuie parcurse într-o anumită ordine. Utilizați această anexă ca pe un set de instrumente.

1

Setul de instrumente al influențării

Tematica: Amenințări hibride

Durata: **45 min**

Nivel: **Liceu**

2

Identificați amenințarea hibridă

Tematica: Amenințări hibride

Durata: **15–20 min**

Nivel: **Gimnaziu**

3

Negarea științei în sala de clasă

Tematica: Dezinformarea și disciplinele școlare

Durata: **45 min**

Nivel: **Ambele**

Setul de instrumente al influențării

Versiunea pentru profesori

Obiective de învățare

- ▶ Elevii pot identifica și clasifica tacticile specifice utilizate într-o operațiune reală de influență străină care vizează Republica Moldova.
- ▶ Elevii pot analiza cine desfășoară o operațiune, împotriva cui este îndreptată și ce urmărește aceasta, trecând de la statutul de consumatori pasivi de știri la cel de analiști activi.
- ▶ Elevii pot aplica Matricea de identificare a tacticilor pentru a evalua în mod independent cazuri similare în viitor.

Context: Două studii de caz pentru activități în sala de clasă

Alegeți unul dintre cele două studii de caz prezentate mai jos. Studiul de caz A este mai sugestiv din punct de vedere vizual, iar Studiul de caz B oferă o perspectivă mai detaliată asupra modului de desfășurare a operațiunii.

Studiul de caz A – Deepfake-ul din cadrul alegerilor prezidențiale din 2024 (Operațiunea „Matrioșka”)

În săptămânile premergătoare alegerilor prezidențiale din Republica Moldova din 2024, un videoclip deepfake cu președinta Maia Sandu, generat cu ajutorul inteligenței artificiale, a fost distribuit pe TikTok. În acesta, Maia Sandu apărea interpretând un cântec rap în limba rusă, fiind prezentată în același timp ca fiind coruptă și favorabilă Rusiei. Operațiunea a fost identificată de colectivul de monitorizare Antibot4Navalny. Narațiunile false potrivit cărora Maia Sandu ar suferi de schizofrenie și că partidul său ar fi fraudat alegerile au fost răspândite prin Telegram, apoi amplificate prin intermediul unor creatori de conținut plătiți de pe TikTok și al unor conturi automate (bot) de pe platforma X. Unele postări au uzurpat identitatea AFP și BBC pentru a crea o falsă impresie de credibilitate.

- ▶ NU încercați să prezentați videoclipul deepfake propriu-zis. Descrieți-l și utilizați o captură de ecran dintr-un material de verificare a faptelor publicat de The Insider, BBC sau Ziarul de Gardă.

Studiul de caz B – Operațiuni de sondaje false (Rețeaua Șor, 2024– 2025)

Publicația de investigații Ziarul de Gardă și BBC au dezvăluit existența unei rețele finanțate din străinătate, asociate oligarhului fugar Ilan Șor. Rețeaua recruta persoane din Republica Moldova prin intermediul Telegram și le plătea aproximativ 3 000 MDL pe lună (circa 170 USD), sumele fiind transferate printr-o bancă aflată sub sancțiuni. Persoanele recrutate primeau instrucțiuni să publice afirmații false pe TikTok și Facebook, să organizeze „sondaje” false (influențând subtil răspunsurile participanților și înregistrând în secret persoanele care își exprimau sprijinul pentru opoziție) și să genereze date false privind opinia publică. Cercetătorii TikTok au identificat cel puțin 90 de conturi asociate rețelei, care au acumulat împreună peste 23 de milioane de vizualizări într-o țară cu doar 2,4 milioane de locuitori.

Desfășurarea activității (45 minute)

- ➊ (0–5 min) Începeți cu întrebarea: „Ați distribuit vreodată ceva online care s-a dovedit ulterior a fi fals? Cum ați aflat?” Ascultați 2–3 răspunsuri. Apoi spuneți: „Astăzi vom analiza persoane a căror activitate constă în răspândirea informațiilor false și vom încerca să gândim ca niște analiști.”
- ➋ (5–15 min) Prezentați unul dintre studiile de caz sub formă de narațiune. Dacă aveți la dispoziție un proiector, afișați o captură de ecran dintr-un material real de verificare a faptelor. Normalizați incertitudinea: „Înainte să analizăm acest caz, care a fost prima voastră reacție?”
- ➌ (15–30 min) Distribuiți fișele de lucru. Elevii lucrează individual sau în perechi pentru a completa Matricea de identificare a

tacticilor. Deplasați-vă printre bănci și oferiți indicii dacă întâmpină dificultăți: „Cine are de câștigat dacă acest conținut ajunge la cât mai multe persoane?” sau „Ce emoție încearcă să provoace acest conținut?”

- ➍ (30–40 min) Reuniți clasa pentru discuție. Invitați fiecare pereche să prezinte câte un rând din matrice. Completați împreună o versiune comună la tablă. Evidențiați diferențele de interpretare – de multe ori pot exista mai multe răspunsuri corecte.
- ➎ (40–45 min) Încheiere: rugați elevii să răspundă la întrebarea de reflecție de pe fișa de lucru. Discutați 2–3 răspunsuri. Subliniați că scopul exercițiului nu este cultivarea neîncrederii sau a paranoiei, ci formarea obiceiului de a acorda încă o secundă de reflecție înainte de a distribui un conținut online.

Întrebări pentru discuție

- ▶ De ce credeți că Republica Moldova a fost vizată în mod repetat de astfel de operațiuni?
- ▶ În cadrul operațiunii cu sondaje false, cetățeni obișnuiți din Republica Moldova au fost plătiți pentru a răspândi dezinformare. Ce ne spune acest lucru despre modul în care aceste operațiuni recrutează persoane?
- ▶ Un deepfake cu un politician este automat ilegal? Cine decide acest lucru? Ce măsuri pot fi luate?
- ▶ Aceleași narațiuni continuă să se repete – Uniunea Europeană este periculoasă, alegerile sunt fraudate. De ce s-ar întâmpla acest lucru?
- ▶ Care este diferența dintre un articol de știri pătinitor și o operațiune de influență desfășurată în mod deliberat?

Setul de instrumente al influențării

► Nume:

► Data / Clasa:

Sarcina: analizați o operațiune reală de influență care a avut ca țintă Republica Moldova. Folosind informațiile furnizate de profesor, completați Matricea de identificare a tacticilor. Apoi răspundeți la întrebările de mai jos.



Pasul 1 – Operațiunea

(completați pe măsură ce profesorul o prezintă)

► Denumirea / titlul operațiunii:

► Când a avut loc?

► Unde s-a răspândit? (pe ce platforme?)

► Care a fost principala afirmație falsă sau conținutul fals?

Pasul 2 – Matricea de identificare a tacticilor

Pentru fiecare tactică utilizată în cadrul operațiunii, completați toate cele cinci coloane. Este posibil ca nu toate rândurile să fie completate – acest lucru este în regulă.

#	▶ Tactica utilizată	▶ Platforma	▶ Grupul țintă	▶ Declanșatorul emoțional	▶ Obiectivul tacticii
1					
2					
3					
4					
5					

Pasul 3 – Întrebări de ansamblu (2-3 propoziții pentru fiecare răspuns)

1 CINE s-a aflat în spatele acestei operațiuni și ce ar avea de câștigat dacă aceasta ar avea succes?

2 CINE a fost ținta finală a operațiunii – un singur grup sau mai multe grupuri?

3 CE ar trebui să știe un cititor critic pentru a recunoaște că acest conținut este fals înainte de a-l distribui?

Reflecție

Imaginați-vă că acest conținut apare chiar acum în fluxul vostru de pe rețelele sociale, printre postările prietenilor și ale familiei. Ce v-ar determina să vă opriți înainte de a-l distribui? Ce v-ar determina să îl distribuiți fără să vă gândiți?

Identificați amenințarea hibridă

Versiunea pentru profesori

Obiective de învățare

- ▶ Elevii pot face distincția între amenințările hibride și activitățile politice sau sociale legitime.
- ▶ Elevii pot clasifica amenințările hibride în funcție de tip: informaționale, economice sau politice.
- ▶ Elevii exersează evaluarea situațiilor în condiții de incertitudine și recunosc că răspunsul „neclar” este un răspuns valid.

Desfășurarea activității (15-20 de minute)

- 1 (0-3 min) Întrebați: „A auzit cineva expresiile «amenințare hibridă» sau «război hibrid»?” Ascultați răspunsurile fără a le corecta. Scrieți pe tablă: Amenințare hibridă = utilizarea unei combinații de instrumente – informații, bani, politică și economie – pentru a slăbi o țară din interior, fără a declara un război deschis.
- 2 (3-15 min) Citiți cu voce tare fiecare scenariu din fișa de lucru a elevilor. După fiecare scenariu, elevii își indică răspunsul (ROȘU / GALBEN / VERDE). Discutați pe scurt raționamentul din spatele fiecărui răspuns, fără a vă grăbi să oferiți „răspunsul corect”. Unele scenarii sunt intenționat ambigue. Competența urmărită este capacitatea de a raționa.

- 3 (15-20 min) Discuție de sinteză: „Care scenariu a fost cel mai dificil de evaluat? De ce?” Mesaj-cheie: amenințările hibride reale sunt concepute să pară ambigue. Acest lucru face parte din modul în care funcționează. Scopul nu este cultivarea paranoiei, ci dezvoltarea capacității de a pune întrebările potrivite.

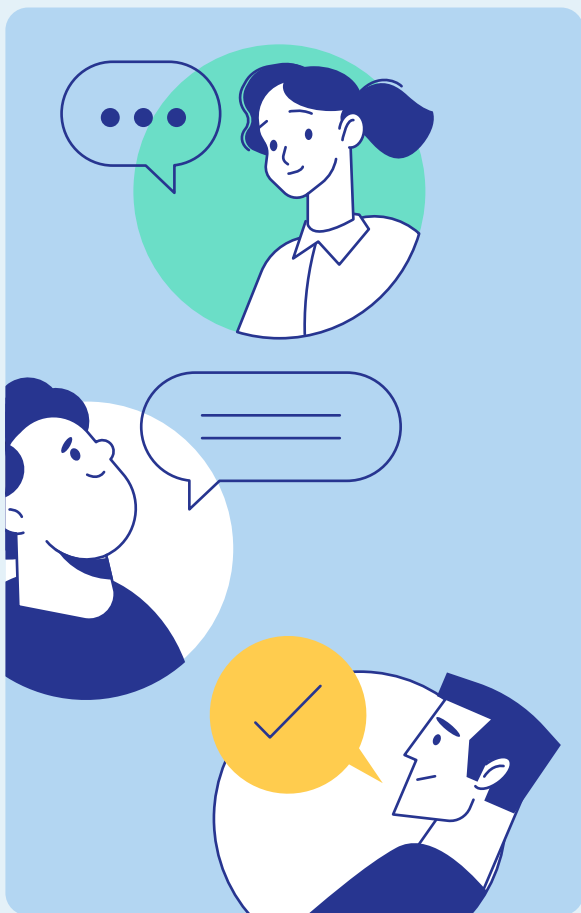
Întrebări pentru discuție

- ▶ Ce detaliu specific din Scenariul 1 a făcut ca acel cont să pară suspect?
- ▶ Ce ar face ca oferta din Scenariul 2 să reprezinte o tranzacție comercială legitimă, și nu o formă de constrângere?
- ▶ În Scenariul 3: reprezintă o problemă utilizarea unor informații adevărate într-o posibilă operațiune de influență? Prin ce se deosebește un miting finanțat de o manifestație spontană?

Notă importantă pentru profesori

Abordați acest exercițiu din perspectiva tacticilor și a semnalelor de avertizare, nu a identității naționale. Întrebarea este întotdeauna: „Ce tactici sunt utilizate?”, nu „Cine le folosește?”. Unele scenarii s-ar putea aplica oricărui actor care desfășoară operațiuni de influență malignă, inclusiv unor actori interni.

În Scenariul 2 este utilizată formularea „un stat străin”, iar acest lucru este intenționat. Coerciția hibridă nu este specifică unei singure țări, iar menținerea unei abordări neutre le permite tuturor elevilor să participe la discuție, inclusiv celor cu orientări politice diferite.



Identificați amenințarea hibridă

► Nume:

► Data / Clasa:

Ce este o amenințare hibridă?

O amenințare hibridă apare atunci când un actor utilizează o combinație de instrumente – nu doar forță militară, ci și informații, bani, politică și mijloace economice – pentru a slăbi o țară din interior, adesea fără a declara un conflict deschis.

► Informațională

Răspândirea de narațiuni false, dezinformare și propagandă

► Economică

Utilizarea banilor, a comerțului sau a energiei ca instrumente de presiune

► Politică

Finanțarea partidelor sau a mișcărilor politice și amestecul în alegeri

Semaforul de evaluare

● Roșu

Este cu siguranță o amenințare hibridă. Ceva este în mod clar în neregulă.

● Galben

Neclar. Ar putea fi o amenințare hibridă sau o activitate legitimă. Sunt necesare mai multe informații.

● Verde

Pare a fi o activitate legitimă. Nu există indicii privind o amenințare hibridă.



Scenariul 1

Un cont de pe o rețea socială, fără fotografie de profil și fără postări anterioare, începe brusc să comenteze la fiecare articol important din presa din Republica Moldova, repetând mereu: „UE ne va distruge tradițiile” și „doar o națiune puternică ne poate proteja”. Contul a fost creat în urmă cu trei zile.

Răspunsul meu:

☐ Roșu

☐ Galben

☐ Verde

Raționament:

Scenariul 3

Un grup de 200 de persoane organizează un miting la Chișinău, cerând reducerea prețurilor la energia electrică. Participanții poartă pancarte identice, tipărite profesional. Întrebat despre proveniența fondurilor pentru tipărirea pancartelor, organizatorul nu poate oferi o explicație.

Răspunsul meu:

☐ Roșu

☐ Galben

☐ Verde

Raționament:

Scenariul 2

O companie de stat dintr-o țară străină se oferă să furnizeze gaze naturale Republicii Moldova la un preț cu 40% sub prețul pieței, dar numai dacă Republica Moldova acceptă să nu adere la niciun acord regional în domeniul energiei în următorii cinci ani.

Răspunsul meu:

☐ Roșu

☐ Galben

☐ Verde

Raționament:

Reflecție

Care scenariu a fost cel mai dificil de evaluat? De ce credeți că persoana care a conceput acel scenariu l-a făcut atât de dificil?

Negarea științei în sala de clasă

Versiunea pentru profesori

Obiective de învățare

- ▶ Elevii pot identifica afirmațiile științifice false integrate în narațiuni conspiraționiste frecvent întâlnite în mai multe discipline școlare.
- ▶ Elevii pot identifica consensul științific și cel puțin o metodă de verificare pentru fiecare afirmație falsă.
- ▶ Elevii înțeleg că dezinformarea nu se limitează la domeniul politic, ci vizează în mod sistematic alfabetizarea științifică.

Desfășurarea activității (45 de minute)

- ① (0–5 min) Întrebați: „La ce disciplină școlară credeți că este cel mai greu să minți?” Ascultați răspunsurile. Apoi spuneți: „Astăzi vom vedea că informațiile false se pot ascunde în geografie, fizică, chimie, matematică și istorie și că disciplinele pe care le studiați la școală sunt, de fapt, cele mai bune instrumente pentru a le demasca.”
- ② (5–30 min) Împărțiți clasa în patru grupe, fiecare primind câte o fișă de disciplină. Grupele au la dispoziție 20 de minute pentru a: a) citi afirmația falsă; b) discuta ce cunoștințe din disciplina respectivă o contrazic; c) identifica o metodă de verificare; d) pregăti o explicație de 90 de secunde.

- ③ (30–45 min) Fiecare grup își prezintă explicația în maximum 90 de secunde. După fiecare prezentare, clasa poate adresa o întrebare. Profesorul completează, dacă este necesar, aspectele esențiale care nu au fost menționate.

Întrebări pentru discuție

- ▶ Ați fost surprinși să aflați că dezinformarea apare și în domeniul științei, nu doar în politică?
- ▶ De ce ar dori un guvern străin ca oamenii să nu mai aibă încredere în știință? Cine are de câștigat de pe urma confuziei create în jurul informațiilor științifice?
- ▶ Dacă un membru al familiei v-ar spune că crede una dintre aceste afirmații false, cum ați reacționa?

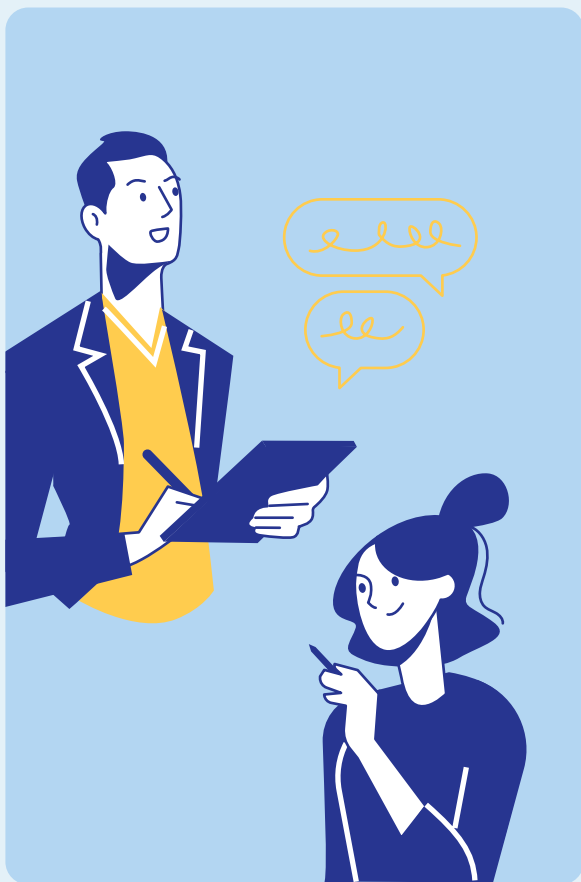
Recomandări pentru profesori

► **Gimnaziu:** completați în prealabil secțiunea „Ce arată disciplina voastră”; grupele trebuie doar să identifice metoda de verificare.

Liceu: prezentați doar afirmația falsă; grupele trebuie să identifice în mod independent atât argumentele care o infirmă, cât și metoda de verificare.

► **Colaborare interdisciplinară:** acest exercițiu poate fi desfășurat cu succes ca lecție comună cu profesorii de biologie, chimie sau istorie.

► **Trimiteri la manual:** Partea a treia (Cum să recunoașteți operațiunile informaționale) și Partea a cincea (Abilități practice).



Negarea științei în sala de clasă

► Nume:

► Data / Clasa:



Geografie – pământul plat

Afirmație falsă: „Pământul este plat și este acoperit de o cupolă. Toate imaginile din satelit sunt falsificate de NASA și de guverne.”

Ce arată de fapt disciplina voastră:

- Navele dispar mai întâi cu coca după linia orizontului – un fenomen imposibil pe o suprafață plană.
- Eratostene a măsurat circumferința Pământului în jurul anului 240 î.Hr., folosind umbrele și geometria, obținând un rezultat remarcabil de apropiat de valoarea reală.
- Umbra Pământului proiectată pe Lună în timpul eclipselor de Lună este întotdeauna circulară – doar un corp sferic proiectează o umbră rotundă din orice unghi.
- Sistemul GPS și rutele aviatice funcționează numai pe baza geometriei unui Pământ sferic; modelele Pământului plat conduc la distanțe incorecte.
- Fusurile orare sunt posibile numai pe un Pământ sferic – dacă Pământul ar fi plat, Soarele ar lumina simultan întreaga suprafață.

Metoda de verificare: Într-o zi însorită, tu și un prieten dintr-un alt oraș puteți măsura unghiurile umbrelor la amiaza solară și le puteți compara (site-ul timeanddate.com oferă ora exactă a amiezii solare). Astfel, puteți reproduce experimentul realizat de Eratostene în urmă cu aproximativ 2 200 de ani.

Istorie – revizionism istoric

Afirmație falsă: „Uniunea Sovietică a eliberat Europa de Est. Crimele sovietice sunt invenții ale Occidentului. Deportările din Basarabia nu au avut loc niciodată.”

Ce arată de fapt disciplina voastră:

- ▶ Gulagul, deportările și Holodomorul sunt documentate în arhive din perioada sovietică (astăzi parțial accesibile), în arhivele naționale ale Republicii Moldova și ale României, precum și în lucrările istoricilor din întreaga lume.
- ▶ Protocolul secret al Pactului Molotov–Ribbentrop, prin care Europa de Est era împărțită în sfere de influență între Germania nazistă și Uniunea Sovietică, a fost negat de autoritățile sovietice până în 1989. Originalul în limba germană a fost descoperit în arhivele Ministerului german al Afacerilor Externe după încheierea celui de-al Doilea Război Mondial.
- ▶ Memorial, cea mai cunoscută organizație rusă pentru apărarea drepturilor omului, care documenta crimele regimului sovietic, a fost dizolvată prin hotărâre judecătorească de autoritățile ruse în 2021.
- ▶ Deportările din Basarabia din anii 1941 și 1949 sunt documentate atât în arhivele de stat ale Republicii Moldova, cât și în arhivele de stat ale Federației Ruse.

Metoda de verificare: Textul Protocolului secret este disponibil în cadrul Yale Avalon Project (law.yale.edu/avalon). Documentele de arhivă ale organizației Memorial sunt disponibile prin intermediul organizațiilor partenere din Europa.

Istorie și fizică – aterizarea pe lună din 1969 a fost înscenată

Afirmație falsă: „Aterizarea pe Lună a misiunii Apollo 11 din 1969 a fost înscenată de NASA într-un studio de film, sub regia lui Stanley Kubrick. Imaginile prezintă neconcordanțe (steagul care pare să fluture, anomalii de iluminare). Centurile de radiații Van Allen i-ar fi ucis pe astronauți. Tehnologia necesară nu exista. Guvernul Statelor Unite avea nevoie de o victorie propagandistică în Războiul Rece.”

Ce arată de fapt disciplina voastră:

- ▶ Aterizările pe Lună din cadrul programului Apollo se numără printre cele mai bine documentate și verificate independent evenimente din istorie. Discutați și despre misiunile recente de explorare a Lunii.
- ▶ Retroreflectoarele amplasate pe suprafața Lunii în timpul misiunilor Apollo pot fi detectate și astăzi cu ajutorul unor impulsuri laser trimise de pe Pământ, inclusiv de observatoare din țări care au fost rivale ale Statelor Unite în timpul Războiului Rece.
- ▶ Uniunea Sovietică, care avea toate motivele geopolitice să demascheze o eventuală înscenare și urmărea activ misiunile Apollo prin propria rețea de comunicații pentru spațiul îndepărtat, nu a contestat niciodată aterizările pe Lună. Radioamatori și operatori independenți din întreaga lume au recepționat semnalele de telemetrie transmise de modulul lunar.
- ▶ Impresia că steagul „flutură” a fost cauzată de vibrațiile produse atunci când astronauții l-au fixat în sol. În absența rezistenței aerului, aceste vibrații au persistat mai mult decât ar fi făcut-o pe Pământ.
- ▶ Peste 400 kg de roci lunare au fost aduse pe Pământ și studiate de oameni de știință din întreaga lume, inclusiv din Uniunea Sovietică.

► Centurile de radiații Van Allen există, însă traiectoria și durata traversării lor au fost planificate astfel încât expunerea astronautilor la radiații să fie minimă.

Metoda de verificare: Elevii pot verifica existența retroreflectoarelor folosind datele publice puse la dispoziție de proiectul Apache Point Observatory Lunar Laser-ranging Operation (APOLLO).

Fizică – rețelele 5g provoacă covid-19 / afectează sănătatea

Afirmație falsă: „Rețelele mobile 5G emit radiații care provoacă COVID-19, cancer, leziuni ale ADN-ului sau afecțiuni neurologice. Turnurile 5G au fost folosite pentru a răspândi virusul SARS-CoV-2. Pandemia de COVID-19 a fost fabricată pentru a justifica implementarea rețelelor 5G. Unele variante ale acestei teorii susțin că 5G este utilizată pentru controlul minții sau supraveghere.”

Ce arată de fapt disciplina voastră:

► Rețelele 5G utilizează radiații electromagnetice neionizante din domeniul frecvențelor radio (RF) – același tip fundamental de energie ca undele radio FM, Wi-Fi, Bluetooth și generațiile anterioare de rețele mobile, însă la frecvențe ceva mai ridicate.

► Radiațiile neionizante nu au suficientă energie pentru a rupe legăturile chimice sau pentru a deteriora ADN-ul, acesta fiind mecanismul prin care radiațiile ionizante (razele X și razele gamma) pot provoca cancer. Frecvențele utilizate de rețelele 5G (600 MHz–86 GHz) sunt cu mult sub pragul de ionizare.

► Este imposibil din punct de vedere fizic ca undele radio să transporte sau să transmită un virus. Virusurile sunt particule biologice care se transmit prin contact fizic direct sau indirect, nu prin unde radio.

► Organizația Mondială a Sănătății (OMS), Comisia Internațională pentru Protecția împotriva Radiațiilor Neionizante (ICNIRP) și autoritățile naționale de sănătate au analizat dovezile științifice și au concluzionat că expunerea la câmpurile electromagnetice de radiofrecvență generate de rețelele 5G, în limitele prevăzute de reglementări, nu prezintă riscuri pentru sănătate. În plus, cazuri de COVID-19 au fost raportate și s-au răspândit în unele țări înainte ca rețelele 5G să fie implementate acolo.

Biologie – evoluția este „doar o teorie” / creaționismul

Afirmație falsă: „Teoria evoluției este o speculație nedovedită. Viața este prea complexă pentru a fi apărut întâmplător. Registrul fosilifer are «lacune». Evoluția este incompatibilă cu credința religioasă. Unele variante susțin conceptul de «proiectare inteligentă», potrivit căruia complexitatea vieții implică existența unui proiectant.”

Ce arată de fapt disciplina voastră:

► În știință, o teorie nu este o simplă presupunere, ci o explicație bine fundamentată, susținută de un volum amplu de dovezi. Teoria evoluției este susținută de dovezi convergente din genetică, paleontologie, anatomie comparată, biogeografie și din observații directe ale evoluției și speciației la bacterii, viruși și unele specii de animale.

► „Lacunele” din registrul fosilifer sunt lacune ale procesului de fosilizare (organismele cu corp moale se fosilizează rareori), nu lacune în dovezile care susțin evoluția.

► Structurile despre care se afirmă că sunt „prea complexe pentru a fi rezultatul evoluției” (cum este flagelul bacterian) au precursori evolutivi identificabili. În plus, teoria evoluției formulează predicții care pot fi verificate. De exemplu, prezice că fosile de tranziție ar trebui descoperite în anumite straturi geologice, iar astfel de predicții au fost confirmate în mod repetat (de exemplu, Tiktaalik, descoperit exact în formațiunile geologice în care fusese anticipată prezența sa).

Metoda de verificare: Exemple de fosile

Chimie – urme chimice

Afirmatie falsă: „Urmele de condensare lăsate de avioane sunt substanțe chimice («chemtrails») pulverizate în mod deliberat de guverne pentru controlul populației.”

Ce arată de fapt disciplina voastră:

► Urmele de condensare se formează atunci când gazele de eșapament fierbinți și umede provenite de la motoarele cu reacție intră în contact cu aerul rece de la mare altitudine. Vaporii de apă condensează și îngheață, formând cristale de gheață – un proces explicat de chimia și fizica schimbărilor de fază.

► Persistența sau disiparea urmelor de condensare depinde de umiditatea din straturile superioare ale atmosferei, un fenomen previzibil și în concordanță cu datele meteorologice.

► Compoziția combustibilului pentru aeronave este reglementată de autoritățile din domeniul aviației și este disponibilă public.

► Stațiile de monitorizare a calității aerului din întreaga Europă măsoară continuu compoziția atmosferei. Niciun organism de monitorizare și niciun cercetător independent nu au identificat vreodată în probe prezența unor presupuse „substanțe chimice din chemtrails”.

Metoda de verificare: Într-o zi rece de iarnă (sub -5°C), aruncați în aer liber o cană cu apă clocotită sau pur și simplu expirați. Se formează instantaneu o urmă albă de condens: aerul cald și umed intră în contact cu aerul rece. În zilele uscate, aceasta dispare rapid, iar în zilele umede persistă mai mult timp – exact ca urmele de condensare lăsate de avioane. (Vezi și: [facebook.com/watch/?v=1601352427426359](https://www.facebook.com/watch/?v=1601352427426359))

Matematică – cum pot fi manipulate statisticile

Afirmatie falsă: „Schimbările climatice nu sunt reale – iată un grafic care arată că temperaturile globale aproape că nu s-au modificat din 1880.”

Ce arată de fapt disciplina voastră:

► În 2014, o publicație cunoscută a prezentat un grafic al temperaturilor globale în care axa Y era cuprinsă între -10°F și 110°F – întregul interval al temperaturilor înregistrate pe Pământ. Tendința reală de încălzire (aproximativ $1,5^{\circ}\text{C}$ pe parcursul unui secol) devenea aproape imperceptibilă. Datele erau reale. Impresia creată era înșelătoare.

► Intervalul axei Y a unui grafic ar trebui să reflecte intervalul relevant al valorilor reprezentate, nu să fie extins artificial. Întrebați-vă întotdeauna: cine a ales această scară și de ce?

► Reprezentate pe o scară adecvată, de aproximativ 2 °F, aceleași date privind temperatura evidențiază o tendință clară și accelerată de încălzire, care urmărește îndeaproape creșterea concentrației de CO₂ din atmosferă. Nu s-a schimbat nimic, în afară de scara graficului.

► Alte tehnici de manipulare includ: alegerea selectivă a datei de început sau de sfârșit a analizei (cherry-picking), ignorarea dimensiunii eșantionului și compararea unor valori de referință care nu sunt comparabile.

Metoda de verificare: Înregistrările NASA GISS privind temperatura globală (science.nasa.gov/earth/explore/earth-indicators/global-temperature) pun la dispoziție întregul set de date într-o formă de prezentare care reflectă fidel variațiile temperaturii, cu acces liber și o metodologie complet transparentă.

Sarcina grupei voastre (toate grupele)

1 Afirmatia falsă primită de grupa voastră:

1 Principala dovadă științifică sau istorică care contrazice această afirmație:

1 Metoda de verificare recomandată de grupa voastră:

1 De ce ar putea cineva să creadă această afirmație falsă? Ce o face convingătoare?



1 Note pentru prezentarea de 90 de secunde pe care o veți susține în fața clasei:

Cum să te protejezi împotriva manipulării informaționale?

Mulțumiri și referințe

- 1 <https://dfrlab.org/>
- 2 <https://euvsdisinfo.eu/>
- 3 <https://stopfals.md/>
- 4 <https://faktabaari.fi/edu/oppaat/teachers-ai/>
- 5 <https://ocw.mit.edu/courses/res-cms-001-media-literacy-in-the-age-of-deepfakes-spring-2021/>
- 6 <https://www.globsec.org/what-we-do/publications/voce-pentru-network-russian-linked-influence-operation-moldova>
- 7 <https://www.science.org/doi/10.1126/science.aap9559>
- 8 <https://www.nytimes.com/2017/04/26/books/famous-misquotations.html>
- 9 <https://euvsdisinfo.eu/learn/>
- 10 <https://www.zdg.md/en/kremlins-digital-army-an-undercover-investigation-its-paid-let-me-tell-you-its-paid-directly-from-moscow/>
- 11 <https://x.com/JoeBiden/status/1694523163387019283>
- 12 <https://www.instagram.com/p/DT20wRRkpVH/>
- 13 <https://stratcom.md/en/publications/>
- 14 <https://www.disinfo.eu/wp-content/uploads/2024/10/Disinfo2024-Moldova.pdf>
- 15 <https://stratcom.md/rapoarte-de-activitate/>
- 16 <https://www.psu.edu/news/research/story/social-media-users-probably-wont-read-beyond-headline-researchers-say>
- 17 <https://www.youtube.com/watch?v=-KP-oFqLNF8>
- 18 <https://dfrlab.org/2025/03/06/telegram-network-moldova/>
- 19 <https://dfrlab.org/2024/10/18/malign-interference-moldova/>
- 20 <https://www.npr.org/sections/the-picture-show/2024/10/18/g-s1-28762/photos-moldova-referendum-vote-russia-meddling>; <https://expertforum.ro/en/analysis-of-coordinated-inauthentic-behavior-in-moldova-23-days-before-the-elections/>
- 21 <https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf>
- 22 <https://www.niemanlab.org/2018/09/fighting-back-against-fake-news-a-new-un-handbook-aims-to-explain-and-resist-our-current-information-disorder/>
- 23 https://datasociety.net/pubs/oh/DataAndSociety_LexiconofLies.pdf
- 24 <https://www.npr.org/corrections/?content=atc>
- 25 <https://www.npr.org/2026/03/30/nx-s1-5759214/romantasy-audiobooks-acotar-anthony-palmini>
- 26 <https://euvsdisinfo.eu/learn/>
- 27 <https://t.me/antimaidanmd/13577>; <https://moldova1.md/p/54154>
- 28 <https://www.coe.int/el/web/freedom-expression/information-disorder>
- 29 <https://www.wired.com/story/moldova-leaks-google-privacy-settlement-world-cup-apps/>
- 30 <https://stiri.md/article/social/ce-cunosc-autoritatile-de-spre-site-ul-anonim-moldova-leaks>
- 31 <https://rm.coe.int/information-disorder-report-version-august-2018/16808c9c77>
- 32 https://datasociety.net/pubs/oh/DataAndSociety_LexiconofLies.pdf
- 33 [https://euvsdisinfo.eu/disinformation-cases/?disinfo_countries\[\]=country_77568&text=Moldova](https://euvsdisinfo.eu/disinformation-cases/?disinfo_countries[]=country_77568&text=Moldova)
- 34 <https://euvsdisinfo.eu/foreign-information-manipulation-and-interference-fimi-explained/>
- 35 <https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf><https://t.me/ChisinauTriumf/1536>
- 36 https://commission.europa.eu/strategy-and-policy/coronavirus-response/fighting-disinformation/identifying-conspiracy-theories_en#what-are-conspiracy-theories-why-do-they-flourish
- 37 <https://euvsdisinfo.eu/report/soros-helped-moldovan-president-elect-maia-sandu-come-to-the-power/>
- 38 <https://www.consilium.europa.eu/en/policies/hybrid-threats/#what>; Pentru mai multe informații, consultați și https://www.hybridcoe.fi/wp-content/uploads/2023/09/JRC129019_02.pdf
- 39 <https://euvsdisinfo.eu/report/the-action-and-solidarity-party-is-a-political-branch-of-the-soros-foundation-in-moldova/>
- 40 <https://www.disinfo.eu/wp-content/uploads/2022/09/Doppelganger-1.pdf>
- 41 <https://www.merriam-webster.com/dictionary/astroturfing>
- 42 <https://humanornot.so/>
- 43 https://www.reddit.com/r/mildlyinfuriating/comments/v5tzoj/made_a_tiktok_account_and_got_swarmed_with_bot

- 44 <https://euvsdisinfo.eu/ro/modus-trollerandi-2/>
- 45 <https://www.esafety.gov.au/young-people/trolling>
- 46 <https://www.dnsc.ro/deepfake/>
- 47 <https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf>
- 48 <https://surfshark.com/blog/what-is-phishing>
- 49 <https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf>
- 50 Sinteză bazată pe cadrul conceptual al lui Jowett și O'Donnell (Jowett, G. S. & O'Donnell, V. (2018), Propaganda și persuasiunea, ediția a 7-a, SAGE)
- 51 <https://research.checkpoint.com/2024/disinformation-campaign-moldova/>
- 52 <https://research.checkpoint.com/2024/disinformation-campaign-moldova>
- 53 <https://stopfals.md/ro/article/fals-cec-a-permis-tarilor-u-e-sa-se-amestece-in-alegerile-din-r-moldova-181271>
- 54 <https://t.me/gagauznewsmd/86809>
- 55 <https://dfrlab.org/2025/03/06/telegram-network-moldova/>
- 56 <https://www.globsec.org/what-we-do/publications/voce-pentru-network-russian-linked-influence-operation-moldova>
- 57 <https://alliance4europe.eu/interfering-from-exile>
- 58 <https://www.rferl.org/a/moldova-tiktok-sandu-cameo-disinformation/32831257.html>
- 59 <https://expertforum.ro/en/analysis-of-coordinated-inauthentic-behavior-in-moldova-23-days-before-the-elections/>
- 60 <https://euvsdisinfo.eu/russian-experiments-with-disinformation-in-moldova/>; <https://iwpr.net/global-voices/moldova-how-social-networks-amplify-anti-eu-narratives>
- 61 <https://info1.md/imagini-trucate-cu-presedintele-maia-sandu-presedintia-a-venit-cu-o-reactie/>
- 62 De asemenea, este util să se înțeleagă modul în care funcționează aceste instrumente și limitele lor. Instrumentele de detectare a conținutului generat de inteligență artificială identifică tipare statistice comune textelor scrise de oameni și celor generate de IA – ele nu formulează concluzii definitive, ci estimează probabilități. Un scor nu reprezintă niciodată un verdict. Este important de reținut că performanța acestor instrumente diferă considerabil, iar rezultatele pe care le oferă trebuie interpretate cu prudență și spirit critic. Vezi, de exemplu: Linda Carroll, No, Mary Shelley's Frankenstein doesn't really test positive for AI, Hello Writer!, martie 2026): <https://lindac.substack.com/p/did-frankenstein-test-as-ai>
- 63 <https://guides.lib.uchicago.edu/c.php?g=1241077&p=9082343>
- 64 <https://www.repository.cam.ac.uk/items/11df21e5-c-358-4d0e-a54c-b23aa5b46741>
- 65 <https://euvsdisinfo.eu/fimi-explorer/>
- 66 <https://euvsdisinfo.eu/learn/>
- 67 <https://www.coe.int/en/web/education/-/digital-citizen-ship-education-handbook>
- 68 <https://bellingcat.gitbook.io/toolkit>
- 69 <https://time.com/6155060/lithuania-russia-fighting-disinformation-ukraine/>
- 70 <https://cyberseniors.org/>
- 71 <https://haveibeenpwned.com/>

Rapoarte de cercetare și analize de politici

Alianța pentru Europa. (2025). „Interferențe din exil”. Disponibil la: <https://alliance4europe.eu/interfering-from-exile>

Laboratorul de Cercetare Criminalistică Digitală al Consiliului Atlantic. (2024). „Interferențe maligne în Moldova.” 18 octombrie 2024. Disponibil la: <https://dfrlab.org/2024/10/18/malign-in-terference-moldova/>

Laboratorul de Cercetare Criminalistică Digitală al Consiliului Atlantic. (2025). „Rețeaua Telegram din Moldova.” 6 martie 2025. Disponibil la: <https://dfrlab.org/2025/03/06/telegram-network-moldova/>

Check Point Research. (2024). „Campania de dezinformare din Moldova”. Disponibil la: <https://research.checkpoint.com/2024/disinformation-campaign-moldova/>

Comisia Europeană și OCDE. (2025). „Pregătirea elevilor pentru era IA: un cadru de alfabetizare în domeniul IA pentru învățământul primar și secundar.” Proiect de revizuire, mai 2025. Disponibil la: https://ailiteracyframework.org/wp-content/uploads/2025/05/AILitFramework_ReviewDraft.pdf

Serviciul European de Acțiune Externă (n.d.) Dincolo de dezinformare – Ce este FIMI? Disponibil la: https://www.eeas.europa.eu/eeas/beyond-disinformation-what-fimi_en

EUvsDisinfo. (2024). „Experimentele rusești cu dezinformarea în Moldova.” 26 august 2024. Disponibil la: <https://euvsdisinfo.eu/russian-experiments-with-disinformation-in-moldova/>

Expert Forum. (2024). „Analiza comportamentului neautentic coordonat în Moldova: cu 23 de zile înainte de alegeri.”

Disponibil la: <https://expertforum.ro/en/analysis-of-coordinated-inauthentic-behavior-in-moldova-23-days-before-the-elections/>

GLOBSEC. (2025). „Rețeaua Vocepentru: operațiune de influență legată de Rusia în Moldova.” Disponibil la: <https://www.globsec.org/what-we-do/publications/vocepentru-network-russian-linked-influence-operation-moldova>

Global Security Review (2019): „Analiza războiului informațional și a operațiunilor de influență rusești”, disponibil la: <https://globalsecurityreview.com/cold-war-2-0-russian-information-warfare/>

Harvard Health Publishing. (2024). „Pericolele doomscrolling-ului”. Harvard Medical School.

Roozenbeek, J., & van der Linden, S. (2019). „Jocul cu știri false conferă rezistență psihologică împotriva dezinformării online.” Palgrave Communications, 5(65). Cambridge Social Decision-Making Lab. Disponibil la: <https://www.cambridge.org/engage/coe/article-details/5d0e6c33a6f5a70017e6f15b>

Institutul pentru Politici și Reforme Europene (IPRE). (2024). „Dezbateri TV #NEXT4EU: Integrarea și progresul european.” Martie 2024. Difuzată pe Moldova 1. Disponibil la: <https://ipre.md/2024/03/19/dezbateri-tv-next4eu-integrarea-europeana-si-progresul-obtinut-pe-cele-trei-masuri-restante-din-cele-9-conditii-inaintate-de-catre-ue/?lang=en>

IWPR. (2024). „Moldova: Cum rețelele sociale amplifică narațiunile anti-UE”. Octombrie 2024.

IWPR. (2024). „Manualul de dezinformare din Moldova.” Disponibil la: <https://academy.iwpr.net/handbooks-store/moldova-disinformation-handbook>

WatchDog.MD. (2024). Rapoarte de monitorizare privind dezinformarea în perioada electorală din 2024 din Moldova.

Vosoughi, S., Roy, D. și Aral, S. (2018). „Răspândirea știrilor adevărate și false online”. Science, 359(6380), 1146-1151

Știri și jurnalism

Euronews/NewsGuard. (2025). „Propaganda rusă inundă Moldova înaintea alegerilor.” Iulie 2025. Disponibil la: <https://www.euronews.com/my-europe/2025/07/25/russian-propaganda-swamps-moldova-ahead-of-elections>

NPR. (2024). „Fotografii: Amestecul Rusiei în votul referendar din Moldova.” 18 octombrie 2024. Disponibil la: <https://www.npr.org/sections/the-picture-show/2024/10/18/g-s1-28762/photos-moldova-referendum-vote-russia-meddling>

Radio Free Europe/Radio Liberty. (2023). „Dezinformare privind apariția lui Sandu pe TikTok în Moldova.” Disponibil la: <https://www.rferl.org/a/moldova-tiktok-sandu-cameo-disinformation/32831257.html>

Surse de verificare a faptelor

StopFals.md. (2025). „Fals: CEC a permis țărilor UE să se amestece în alegerile din R. Moldova.” Disponibil la: <https://stopfals.md/ro/article/fals-cec-a-permis-tarilor-ue-sa-se-amestece-in-alegerile-din-r-moldova-181271>

Resurse educaționale

Comisia Europeană. (2026). „Ghid pentru profesori și educatori privind combaterea dezinformării și promovarea alfabetizării digitale prin educație și formare.” Disponibil la: <https://education.ec.europa.eu/focus-topics/digital-education/actions/plan/guidelines-for-teachers-to-foster-digital-literacy-and-tackle-disinformation>

AI for Education. (2024). „Descoperirea deepfake-urilor: Ghid pentru sala de clasă.” Disponibil la: <https://www.aiforeducation.io/ai-resources/uncovering-deepfakes>

Biblioteca Universității Concordia. „Set de instrumente critice.” Disponibil la: <https://library.concordia.ca/apps/critical-toolkit/course.html?courseID=27385>

Faktabaari. (2025). „Ghidul IA pentru profesori: Alfabetizarea informațională digitală.” Disponibil la: <https://faktabaari.fi/edu/oppaat/teachers-ai/>

Centrul MIT pentru Virtualitate Avansată. (2021). „Alfabetizarea media în era deepfake-urilor.” Disponibil la: <https://deepfakes.virtuality.mit.edu/>



Cum să te protejezi împotriva manipulării informaționale?

Ghid pentru tinerii moldoveni