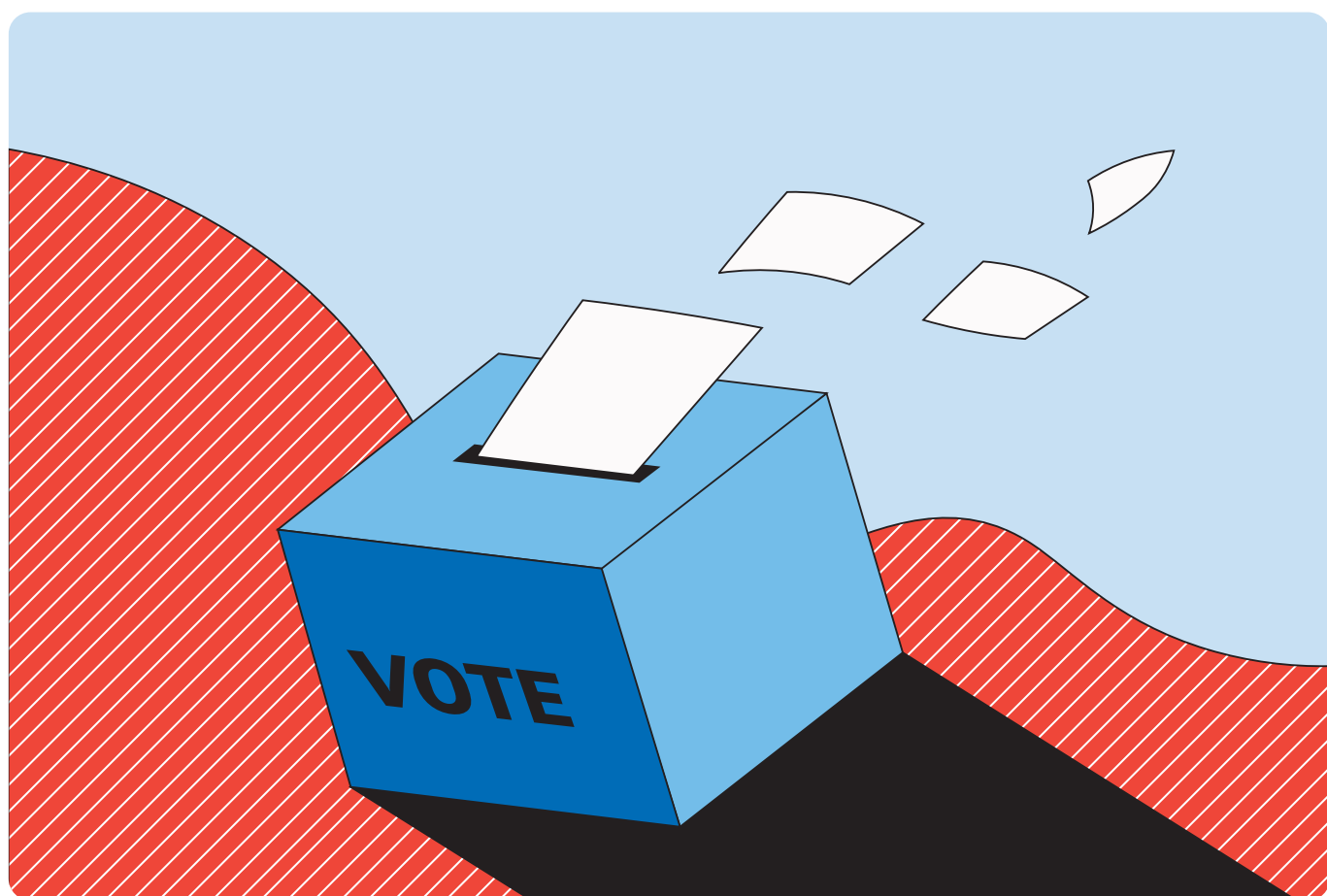


Protejarea alegerilor împotriva amenințărilor hibride: **UN MANUAL DE STRATEGII DEFENSIVE**

Sebastian Bay și Catalina Uribe Burcher,
noiembrie 2025



Mesaj de mulțumire

Autorii raportului țin să mulțumească numeroaselor persoane și echipe ale căror contribuții au făcut posibilă finalizarea acestuia.

În primul rând, dorim să îi mulțumim Lisei Orrenius, care a supervizat procesul de la început până la sfârșit și a oferit feedback și îndrumare continuă. De asemenea, suntem recunoscători colegilor din cadrul Academiei Folke Bernadotte (FBA) care au revizuit și au comentat structura, conținutul și abordarea lucrării, printre care Carl Fredrik Birkoff, Filippa Almlund și Kicki Westin din cadrul Unității pentru Democrație și Guvernare, precum și Emmei Skeppström și lui Abdalhad Alijla din Echipa de Cercetare.

Ne exprimăm recunoștința față de Susanna Kujanpää (fostă membră a Centrului European de Excelență pentru Contracararea Amenințărilor Hibrice, Hybrid CoE) pentru recenzia externă și observațiile sale valoroase.

Un gând special de apreciere se îndreaptă către Aina Boris, care a supravegheat toate detaliile de producere și a asigurat buna desfășurare a pregătirii manuscrisului, machetării, integrării ilustrațiilor și a versiunii finale. Totodată, mulțumim companiilor Essen International și Comactiva Language Partner pentru munca lor excelentă de redactare, machetare și ilustrare.

Declinarea responsabilității

Opiniile exprimate în acest raport aparțin autorilor și nu reflectă neapărat politica sau poziția oficială a Academiei Folke Bernadotte (FBA) sau a Guvernului Suediei. Responsabilitatea pentru conținut aparține exclusiv autorilor. Menționarea unor instituții, companii sau produse specifice nu implică aprobare din partea FBA.

Cuprins

Prefață	7
Glosar de termeni	9
Acronime	13
Sumar	15
01 Introducere	19
1.1. Definirea amenințărilor hibride în context electoral	20
1.2. Impactul asupra integrității electorale, încrederii și proceselor democratice	21
1.3. Dimensiunea geopolitică	22
1.4. Scopul, domeniul de aplicare și metodologia Raportului	22
02 Acțiunile străine de manipulare a informațiilor și ingerințele străine (FIMI) și alegerile	25
2.1. Tendințe recente	25
2.2. Provocări în detectare, atribuire și răspuns	28
2.3. Ce se poate face? Strategii pentru contracararea FIMI ce vizează alegerile	29
03 Finanțarea politică ilicită și amenințările hibride	33
3.1. Finanțarea politică ilicită ca vector de interferență	34
3.2. Ce se poate face? Strategii pentru consolidarea reglementării finanțării politice și a supravegherii împotriva ingerințelor străine	37
04 Securitatea cibernetică în alegeri	41
4.1. Peisajul amenințărilor în evoluție: convergență, comercializare și AI	41
4.2. Amenințări la adresa infrastructurii electorale critice (rețele, baze de date și tehnologie de vot)	44
4.3. Atacuri cibernetice care vizează campanii, partide și funcționari electorali	48
4.4. Ce se poate face? Cele mai bune practici pentru reziliența securității cibernetice electorale	49
05 Contracararea amenințărilor hibride la adresa alegerilor: Targumente pentru crearea unor rețele de cooperare electorală	53
5.1. Arhitecturi ale colaborării naționale	54
5.2. Rețea de rețele	56
5.3. Provocări în calea cooperării eficiente	56
06 Concluzii și recomandări	59
6.1. Recomandări	59
07 Referințe	67
08 Note finale	81

Prefață

Alegerile libere reprezintă piatra de temelie a guvernării democratice. Ele întruchipează contractul social dintre cetățeni și stat, oferind atât mijloace de guvernare, cât și un mecanism de responsabilizare. Astăzi, acest contract este atacat din ce în ce mai mult. Amenințările hibride, care combină manipularea informațiilor, atacurile cibernetice și finanțarea politică ilicită, vizează nu doar procesele electorale, ci și însăși încrederea și structura coeziunea socială de care depinde democrația.

Aceste amenințări nu sunt nici episodice și nici periferice. Ele echivalează cu o provocare susținută și extrem de adaptabilă la adresa guvernării democratice. Intenția din spatele amenințărilor și atacurilor nu este doar de a influența un anumit vot, ci de a eroda încrederea în instituții, de a amplifica divizarea și de a slăbi societățile din interior. Utilizarea inteligenței artificiale și a altor tehnologii emergente a accelerat și mai mult această tendință, reducând barierele în calea ingerințelor și amplificând impactul acestora.

Pentru Academia Folke Bernadotte (FBA), apărarea democrației constituie un pilon al prevenirii conflictelor și problemă de securitate atât națională, cât și internațională. Aceasta necesită nu doar garanții tehnice, ci și viziune politică, reziliență instituțională și voință colectivă. Răspunsurile eficiente trebuie să consolideze capacitatea actorilor naționali de la toate nivelurile de a acționa în mod coordonat, în baza înțelegerii comune că reziliența democratică depinde de implicarea tuturor segmentelor societății. În același timp, aceste eforturi trebuie să promoveze deschiderea, transparența și drepturile care definesc sistemele democratice. Combaterea amenințărilor hibride nu poate veni în detrimentul valorilor pe care dorim să le protejăm.

Acest raport reflectă angajamentul FBA de a sprijini eforturile de asigurare a unor alegeri libere și legitime. Reunește perspective practice pentru a analiza modul în care se manifestă amenințările hibride prin operațiuni informaționale, finanțare ilicită și atacuri cibernetice precum și maniera în care strategiile coordonate, axate pe buna guvernare, pot consolida integritatea electorală. Recomandările sale subliniază importanța abordărilor la nivelul întregului guvern și al întregii societăți, a instituționalizării rețelelor de cooperare și a unui ciclu continuu de pregătire care se extinde dincolo de ziua alegerilor.

În esență, raportul susține că reziliența electorală este inseparabilă de reziliența democratică. Consolidarea mecanismelor de apărare împotriva amenințărilor hibride nu este doar un exercițiu de securitate, ci reprezintă și o investiție în statul de drept, în guvernarea responsabilă și în credibilitatea durabilă a instituțiilor democratice.

Exemplele și lecțiile prezentate în acest raport sunt relevante pentru toate țările, inclusiv pentru țara noastră – Suedia. Amenințările hibride nu recunosc granițele și nici nu fac distincție între democrațiile mature sau emergente. Aceleași tactici care urmăresc să submineze integritatea electorală într-un context pot migra rapid în altul. Prin urmare, dezvoltarea rezilienței este o responsabilitate comună – între state, instituții și societăți deopotrivă. Învățând din experiențe diverse și promovând cooperarea transfrontalieră, putem consolida nu doar protecția alegerilor, ci și fundamentele democrației în sine.

Per Olsson Fridh

Director general, Academia Folke Bernadotte

Glosar de termeni

- **Amenințări Persistente Avansate (APT)/ Advanced Persistent Threats:** Actori de amenințare cu resurse vaste, orientați spre obiective exact definite – adesea sponsorizați sau mandatați de state – care desfășoară acțiuni de lungă durată, intruziuni ascunse pentru a obține și menține acces la rețele vizate în sprijinul unor obiective strategice (spionaj, preinstalare, perturbări sau influență).
- **Comportament Coordonat Neautentic (CCN/CIB)/Coordinated Inauthentic Behaviour:** Utilizarea coordonată a unor conturi înșelătoare sau neautentice pentru a induce în eroare oamenii cu privire la originea, identitatea sau popularitatea conținutului.
- **Deepfake:** Medii sintetice sau manipulate (imagine, audio sau video) generate cu tehnici de inteligență artificială pentru a descrie evenimente sau discursuri care nu au avut loc.
- **Dezinformare:** Informații false sau înșelătoare, create și răspândite în mod deliberat pentru a dăuna unei persoane, unui grup social, unei organizații sau unei țări.
- **Tehnica „Doppelgänger”:** O tactică ce folosește o infrastructură care arată la fel („doppelgänger”/dublură) – site-uri web, domenii și conturi sociale clonate sau falsificate – pentru a spăla conținut fals sau înșelător, făcându-l să pară că provine de la surse de încredere. Conținutul este apoi propagat și amplificat prin comportamente neautentice coordonate, promovare plătită și republicare pe mai multe platforme.
- **Doxing (uneori scris „doxxing”):** Publicarea sau partajarea online a informațiilor private, de identificare personală sau sensibile despre o persoană fără consimțământul acesteia, de obicei pentru a hărțui, intimida sau a provoca în alt mod daune.
- **Acțiunile străine de manipulare a informațiilor și ingerințele străine (FIMI):** Un model de comportament manipulativ, care, în mare parte, nu este ilegal, desfășurat intenționat și într-o manieră coordonată de către actori statali sau nestatali străini (inclusiv prin intermediarii acestora), ce amenință sau are potențialul de a exercita un impact negativ asupra valorilor, procedurilor și proceselor politice.
- **Operațiune acces neautorizat, exfiltrare și divulgare ilegală de date (hack-and-leak):** O operațiune coordonată, care urmărește compromiterea sistemelor pentru a sustrage date și a publica materiale selectate, prelucrate sau manipulate în momente strategice, cu scopul de a influența spațiul mediatic, percepția publică sau procesele politice.
- **Amenințări hibride:** Activități coordonate, intenționate și dăunătoare care vizează în mod deliberat vulnerabilitățile sistemice ale statelor și instituțiilor democratice printr-o combinație de mijloace convenționale și neconvenționale. Aceste activități exploatează pragurile de detectare și atribuire, precum și interfețele dintre război și pace, dintre securitatea internă și securitatea externă. De obicei, urmăresc să influențeze procesul decizional la nivel local, statal sau instituțional, rămânând în același timp sub pragul conflictului armat.

IERARHIA TERMINOLOGIEI

Amenințări hibride

Contextul larg al activităților coordonate, intenționate și dăunătoare care includ mijloace informaționale, cibernetice și financiare.

FIMI

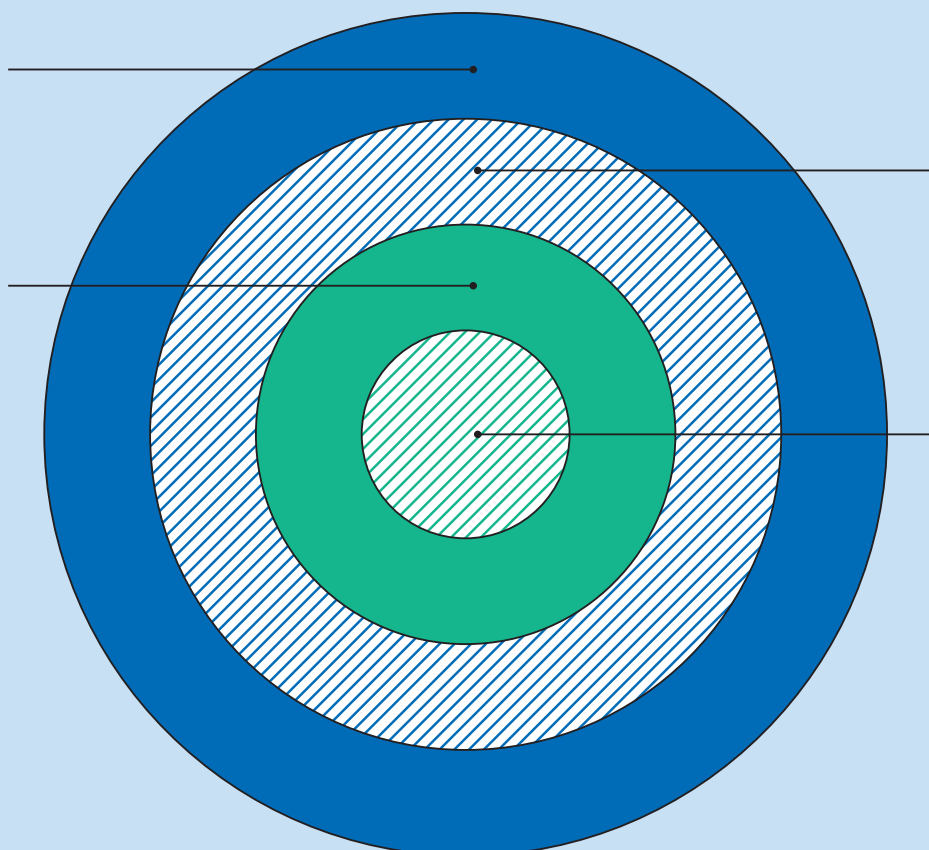
Un model de comportamente manipulative conduse de actori străini, intenționate și adesea coordonate.

Activități de influență a informațiilor (IIA)

Eforturi planificate de a modela percepțiile, atitudinile sau comportamentul prin informare și comunicare

Dezinformare

Informații false sau înșelătoare răspândite în mod deliberat pentru a provoca daune.



- **Activități de influență informațională (AII/IIA)/Information influence activities:** Eforturi planificate de a modela percepții, atitudini sau comportamente prin utilizarea informațiilor și a comunicării. Aceste activități variază de la comunicare publică legitimă și diplomație până la practici ascunse sau înșelătoare, cum ar fi asumarea unei identități false și comportamentul neautentic coordonat. IIA este un termen generic care include FIMI, ce se referă în mod specific la comportamente manipulative desfășurate de actori statali sau nestatali străini și de proxy ai acestora.
- **Informații eronate:** Informații false, dar care nu au fost create sau răspândite cu intenția de a provoca daune.
- **Pre-bunking:** O strategie de comunicare proactivă, bazată pe inoculare informațională, care avertizează oamenii cu privire la posibilele tactici sau narațiuni de manipulare înainte ca aceștia să se confrunte cu ele. Strategia dată oferă contramăsuri simple și precise, precum și instrumente de sprijin pentru luarea deciziilor, pentru a ajuta persoanele să recunoască și să reziste manipulării atunci când aceasta apare. În contexte electorale, pre-bunking-ul este adesea transmis prin intermediul unei platforme oficială de informare - “sursă de adevăr”, al secțiunilor de întrebări adresate frecvent și al unor mesaje publice, programate să coincidă cu perioade de risc cunoscute (de exemplu, termene limită de înregistrare sau perioade de tăcere electorală).
- **Spear-phishing:** Un atac țintit de inginerie socială care folosește momeli personalizate în scopul de a păcăli o anumită persoană pentru a dezvălui credențialele de acces, sau a executa un cod malițios.
- **Vishing (sau phishing vocal):** Inginerie socială realizată prin apeluri vocale, folosind adesea falsificarea ID-ului apelantului pentru a păcăli indivizii să dezvăluie informații sau să acorde acces.

Acronime

- **AI:** Artificial Intelligence – Inteligență artificială
- **APT:** Advanced Persistent Threat – Amenințare persistentă avansată
- **CaaS:** Cybercrime-as-a-Service – Criminalitatea cibernetică ca serviciu
- **DDoS:** Distributed Denial-of-Service – Atac distribuit de tip refuz de serviciu
- **DSA:** EU Digital Services Act – Legea UE privind serviciile digitale
- **EMB:** Election Management Body – Organism de management electoral
- **FBA:** Folke Bernadotte Academy – Academia Folke Bernadotte
- **FIMI:** Foreign Information Manipulation and Interference – Acțiunile străine de manipulare a informațiilor și ingerințele străine

Sumar

Prezentul raport reprezintă o analiză cuprinzătoare a amenințărilor hibride la adresa proceselor electorale și a modalităților de contracarare eficientă a acestora. Raportul se concentrează în special pe evoluțiile înregistrate începând cu 2024 în principalele direcții de interferență electorală, inclusiv Acțiunile Străine de Manipulare a Informațiilor și Ingerințele Străine (FIMI), finanțarea politică ilicită și operațiunile cibernetice. Deși sunt analizate separat, în practică acestea sunt strâns legate între ele. Raportul propune un cadru practic de apărare, care combină consolidarea capacității instituționale cu un sistem de sprijin interconectat, la nivelul întregii societăți.

Tendențe cheie (din 2024):

- FIMI au evoluat în operațiuni persistente la scară industrială, conduse de rețele coordonate, mai degrabă decât de campanii izolate.
- Inteligența artificială (AI) și automatizarea au accelerat crearea și distribuirea de conținut sintetic și înșelător și au redus costul ingineriei sociale.
- Finanțarea politică ilicită, inclusiv finanțarea prin entități interpușe, transferurile internaționale prin criptomonede și cheltuielile online opace, sprijină din ce în ce mai mult manipularea și cumpărarea de voturi.
- Operațiunile cibernetice perturbă infrastructura electorală și adesea funcționează în tandem cu operațiunile informaționale, amplificându-le impactul general.

Principala implicație a acestor tendințe este că adversarii profită de lacunele dintre instituțiile responsabile de organizarea și susținerea alegerilor, iar răspunsurile izolate duc la performanțe inadecvate. Raportul consolidează cele mai bune practici pentru contramăsuri și subliniază ideea că protejarea alegerilor față de aceste amenințări complexe necesită:

- Responsabilități clar definite, resurse adecvate, mandate precise, personal calificat și proceduri bine stabilite în cadrul fiecărei agenții.
- O rețea națională de cooperare funcțională, cu caracter permanent pentru schimbul de informații, desfășurarea de exerciții comune și coordonarea eforturilor de protecție – care operează după principiul „analizăm împreună, acționăm în cadrul mandatului” pentru a păstra autonomia instituțională.
- O abordare la nivelul întregii societăți, care mobilizează mass-media independentă, societatea civilă, mediul academic, autoritățile locale, sectorul privat (inclusiv platformele și operatorii de telecomunicații) și comunități în scopul de a fortifica reziliența prin alfabetizare mediatică și digitală, verificare rapidă a faptelor, raportarea incidentelor și comunicarea publică incluzivă – ancorate în transparență totală și implementate în moduri care susțin drepturile, transparența și pluralismul.
- Mecanisme robuste de cooperare și sprijin internațional ce oferă asistență de urgență,

permit eliminări coordonate transfrontaliere de conținut și convin asupra unor principii comune (de exemplu, practici de securizare din proiectare („secure by design”), indicarea provenienței unde este posibil și divulgare la timp) – conectând rețelele naționale într-o „rețea de rețele” mai largă pentru a accelera sprijinul, coerența și responsabilitatea.

Raportul oferă recomandări practice pentru organismele de management electoral, guverne, organizații ale societății civile și actori internaționali de sprijin din diverse medii electorale, de la democrații consacrate la democrații în curs de dezvoltare. Recomandările cheie includ consolidarea autorităților electorale, atingerea excelenței operaționale, crearea de rețele naționale de cooperare electorală bine dotate, îmbunătățirea cadrelor juridice privind responsabilitatea platformelor electorale și finanțarea politică ilicită, precum și adoptarea unei abordări modulare a asistenței internaționale.

Constatarea principală este că, într-o eră a conflictelor hibride continue, apărarea electorală trebuie să fie permanentă, adaptabilă, proactivă și colaborativă. Consolidarea capacităților instituționale și a unei abordări la nivelul întregii societăți asigură cea mai durabilă protecție pentru integritatea procesului electoral.

01 *Introducere*

În alegerile din întreaga Europă, amenințările hibride au testat reziliența sistemelor electorale. În Slovacia, cu doar două zile înainte de alegerile din 2023, o înregistrare audio generată de inteligență artificială, cu presupuse remarci ale candidatului liberal Michal Šimečka și ale unui jurnalist care ar fi complotat să cumpere voturi de la comunitățile de romi, a fost difuzată în perioada de tăcere mediatică. În România, în perioada premergătoare alegerilor prezidențiale din 2024, autoritățile au identificat tactici hibride coordonate, de la scheme de cumpărare de voturi, dezinformare și atacuri cibernetice, până la finanțarea nedeclarată pentru un candidat pro-rus. Iar în Moldova, în septembrie 2025, președinta Maia Sandu a avertizat că Moscova duce un vast război hibrid înaintea alegerilor parlamentare, folosind dezinformare, cumpărare de voturi și alte forme de finanțare politică ilicită, precum și tactici de intimidare la adresa alegătorilor.¹

Împreună, aceste exemple ilustrează modul în care alegerile se confruntă cu provocări și interferențe tot mai mari din partea actorilor străini ce operează în mod specific în cadrul unor activități coordonate în domeniile informațional, financiar și cibernetic, adesea programate pentru a exploata breșele instituționale și societale.² Întrucât aceste amenințări evoluează continuu, protejarea alegerilor libere și corecte împotriva amenințărilor hibride a devenit nu doar mai critică ca niciodată, ci și o provocare constantă în continuă evoluție.³

Peisajul contemporan al amenințărilor reprezintă o evoluție fundamentală față de diplomația și propaganda tradiționale din secolul XX. Domeniul digital este acum centrul de greutate: adversarii combină operațiuni cibernetice, tehnici online subversive și manipulare narativă; actorii interni pot amplifica, conștient sau inconștient, aceste eforturi. Acțiunile Rusiei în timpul alegerilor din Ucraina din 2014 și, în special, în timpul alegerilor prezidențiale din SUA din 2016, au servit drept un moment de cotitură, catalizând recunoașterea globală a vulnerabilității proceselor democratice la astfel de amenințări hibride sofisticate.⁴

O observație crucială este că ingerința modernă nu constituie o serie de operațiuni izolate, ci un război informațional cronic, susținut de stat și purtat de un ecosistem complex de actori.⁵ Serviciile de informații identifică în mod constant Rusia, China și Iranul drept orchestratori principali, operând printr-o rețea de entități intermediare – de la mass-media de stat la grupuri hacktiviste – pentru a menține o negare plauzibilă a implicării directe.⁶ Linia este și mai estompată de grupuri politice interne care pot acționa ca amplificatori, conștienți sau inconștienți, ai narațiunilor străine.⁷

Progresele tehnologice, în special în domeniul inteligenței artificiale, au accelerat considerabil această evoluție. Din 2024, utilizarea inteligenței artificiale generative a apărut ca un multiplicator de forță semnificativ, permițând crearea rapidă și la costuri reduse a unor materiale sintetice realiste, inclusiv deepfake-uri și clone vocale; producția la scară industrială de dezinformări personalizate; și potențialul pentru roiuri de inteligență artificială malițioasă.⁸ Deși impactul direct al conținutului generat de inteligența artificială asupra rezultatelor alegerilor

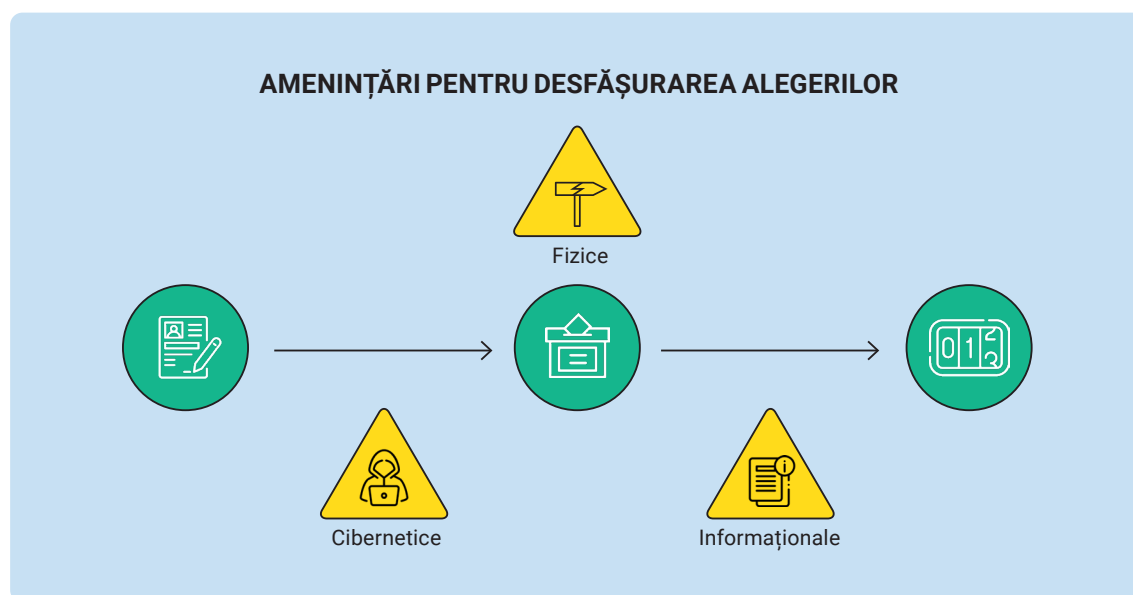
rămâne dificil de cuantificat, acesta a modelat în mod demonstrabil mediul informațional și a amplificat răspândirea falsurilor existente.⁹ Această fuziune între concurența geopolitică, tehnologia avansată și adversarii adaptivi definește actualul peisaj complex al amenințărilor hibride care vizează alegerile.

1.1. DEFINIREA AMENINȚĂRILOR HIBRIDE ÎN CONTEXT ELECTORAL

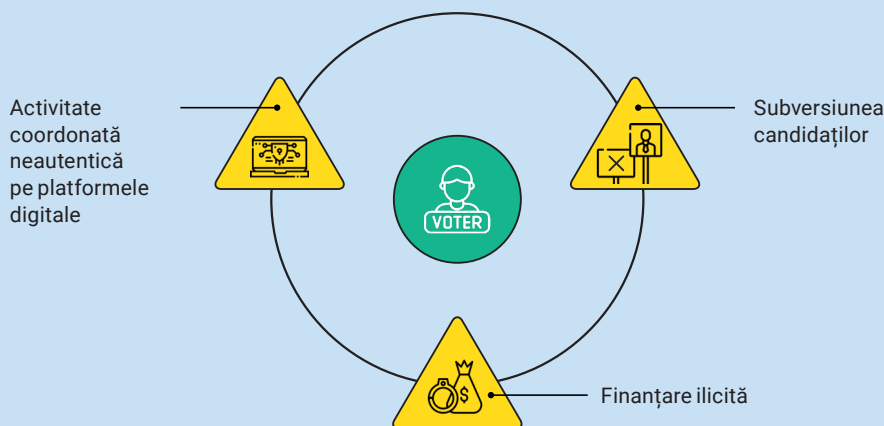
Amenințările hibride care vizează alegerile sunt acțiuni coordonate, ostile, ce combină mijloace convenționale și neconvenționale pentru a submina procesele democratice, rămânând în același timp sub pragul conflictului armat și adesea exploatând lacunele de detectare/atribuire și interfețele război-pace/intern-extern.¹⁰

Bay (2024) identifică trei categorii de amenințări legate de procesul electoral: amenințări la adresa desfășurării alegerilor, a încrederii în alegeri, respectiv la adresa voinței și capacității de a vota. Bazându-se pe această structură axată pe proces, raportul dat urmează o abordare în patru categorii ce surprinde și amenințări la adresa procesului decizional politic. Pentru claritate analitică, amenințările specifice alegerilor sunt grupate în patru categorii care se suprapun: (a) desfășurarea alegerilor, (b) încrederea în alegeri, (c) voința/capacitatea de a vota și (d) procesul decizional politic. Luate în ansamblu, aceste categorii ajută la diferențierea între perturbări ale proceselor electorale și încercări mai profunde de a schimba preferințele sau de a coroda legitimitatea:

- Amenințări la adresa desfășurării alegerilor: Acțiuni care urmăresc perturbarea procesului electoral în sine, cu vizarea funcționarilor, a infrastructurii sau a logisticii prin mijloace informaționale, fizice sau cibernetice.
- Amenințări la adresa încrederii în alegeri: Eforturi de a submina încrederea publicului în legitimitatea alegerilor prin răspândirea dezinformării, promovarea teoriilor conspirației sau crearea percepției de fraudă pe scară largă.
- Amenințări la adresa voinței și capacității de a vota: Tactici menite să influențeze comportamentul alegătorilor prin descurajarea participării sau subminarea capacității de a-și exprima votul, cum ar fi intimidarea sau răspândirea de informații false privind procedurile de vot.
- Amenințări la adresa procesului de formare a opțiunilor politice: Încercări de a influența preferințele alegătorilor folosind mijloace nelegitime sau ilegale, inclusiv activități coordonate neautentice pe platformele digitale, finanțare ilicită sau compromiterea



AMENINȚĂRI LA ADRESA DECIZIILOR POLITICE



1.2. IMPACTUL ASUPRA INTEGRITĂȚII ELECTORALE, ÎNCREDERII ȘI PROCESELOR DEMOCRATICE

Obiectivul strategic al atacurilor hibride împotriva alegerilor nu este doar de a influența voturile individuale, ci de a degrada ecosistemele democratice prin erodarea încrederii, alimentarea polarizării și slăbirea fundamentelor instituționale ale statelor democratice.¹¹ În practică, acest lucru se manifestă prin campanii narative, care pun la îndoială regulile și arbitrii, acuzații orchestrate de fraudă și scurgeri de informații programate ce modelează agendele în perioadele de tăcere. Atacând credibilitatea oficialilor, subminând încrederea în sistemele de vot și diseminând dezinformări inflamatorii, astfel de campanii urmăresc să adâncească polarizarea și să corodeze reziliența instituțională a statului însuși.¹²

„Obiectivul strategic al atacurilor hibride împotriva alegerilor nu este doar de a influența voturile individuale, ci de a degrada ecosistemele democratice prin erodarea încrederii, alimentarea polarizării...”

Deși nu sunt singura cauză, astfel de amenințări au contribuit probabil la scăderea globală a prezenței medii la vot cu aproximativ zece puncte procentuale în ultimii 15 ani, precum și la creșterea numărului disputelor, practic unul din cinci scrutinuri naționale din perioada 2020-2024 înregistrând o respingere a rezultatului de către partea învinsă.¹³

Ciclurile electorale recente prezintă, de asemenea, efecte tangibile: tulburări post-electorale și incidente legate de refuzul recunoașterii înfrângerii; crize informaționale declanșate de atacuri cibernetice de tip „hack-and-leak” și perturbări administrative cauzate de incidente cibernetice care întârzie înregistrarea alegătorilor sau comunicarea rezultatelor. În mai multe cazuri, observatorii internaționali au documentat presiuni coordonate care combină activități de influențare a informațiilor, finanțare ilicită și perturbări cibernetice ce amplifică și mai mult mediile deja polarizate.¹⁴

Această eroziune este agravată de exodul funcționarilor electorali cu experiență, care se confruntă cu o hărțuire persistentă, astfel fiind slăbită capacitatea instituțională.¹⁵ Efectul cumulativ conduce la apariția unui cerc vicios: scăderea încrederii crește vulnerabilitatea la

manipulare, ceea ce, la rândul său, diminuează și mai mult participarea și acceptarea rezultatelor.¹⁶

În plus, narațiunile despre „frauda electorală” au impacturi interne concrete – determinând o creștere a plângerilor și a cererilor de acces la informații, exercitând presiuni pentru renumărare ad-hoc sau „auditori criminalistici”, sporind hărțuirea funcționarilor și reducând disponibilitatea de a accepta rezultatele alegerilor. Aceste narațiuni se răspândesc și dincolo de hotare, unde aceleași șabloane sunt adaptate și reutilizate de influenceri și de publicații asociate statelor implicate, modelând așteptările cu mult înainte de ziua alegerilor.¹⁷

Mai mult, aceste tactici sunt concepute pentru a adânci diviziunile sociale. Adversarii injectează dezinformare cu încărcătură emoțională în dezbaterile privind imigrația, politicile economice și „chestiunile culturale controversate” pentru a alimenta polarizarea țintită.¹⁸ Din punct de vedere practic, campaniile sporesc importanța identităților sociale, prezintă politica ca pe un joc cu sumă nulă („noi vs. ei”) și asociază afirmațiile încărcate emoțional cu perioade de incertitudine, când publicul depinde mai mult de indicii de grup și narațiuni simplificate; în această stare, polarizarea afectivă se intensifică, iar informațiile corective sunt ignorate.¹⁹

Aceste campanii folosesc adesea portretizări negative ale identităților marginalizate – inclusiv genul, rasa și orientarea sexuală – pentru a amplifica fracturile sociale și a viza în mod disproporționat grupurile minoritare și femeile.²⁰ Operatorii amplifică, de asemenea, simultan taberele opuse – o tactică cunoscută sub numele de „convergență identitară” – și exploatează nemulțumirile intersecționale, cum ar fi suprapunerea dintre religie și gen sau clasă. Acest lucru crește acoperirea și ajută la normalizarea ostilității în mai multe comunități.²¹

Faptul dat declanșează un cerc vicios periculos: o societate polarizată, cu o încredere scăzută, este mai puțin rezilientă și chiar mai vulnerabilă la viitoare atacuri hibride. Pe măsură ce încrederea scade, amenințarea percepută între grupuri crește, distanța socială se extinde, iar elitele se confruntă cu presiuni pentru măsuri extraordinare - condiții pe care adversarii le reintroduc cu narațiuni noi și un impact mai mare.²²

1.3. DIMENSIUNEA GEOPOLITICĂ

Amenințările hibride la adresa alegerilor nu apar în mod izolat; ele sunt strâns legate de peisajul geopolitic mai larg. Utilizarea intensificată a acestor tactici începând cu anul 2024 este alimentată de competiția strategică dintre democrații și statele autoritare, de războiul în curs din Ucraina și de alte câteva conflicte de primă linie.²³ Rusia consideră adesea alegerile ca oportunități de a slăbi sprijinul pentru Ucraina, de a submina alianțe precum Organizația Tratatului Atlanticului de Nord (NATO) și Uniunea Europeană (UE) și de a promova o agendă revizionistă care vizează remodelarea ordinii globale.²⁴

Pentru acești actori, războiul informațional nu este un supliment al politicii, ci un instrument central al artei guvernării, purtat persistent și asimetric.²⁵

Societățile democratice – definite de medii informaționale deschise și un angajament față de libertatea de exprimare – prezintă vulnerabilități intrinseci pe care adversarii sunt pricepuți să le exploateze. În schimb, regimurile autoritare beneficiază de ecosisteme informaționale închise, strict controlate, ceea ce le oferă un avantaj defensiv semnificativ care le susține reziliența. Această asimetrie operațională se află în centrul conflictelor contemporane.²⁶

Războiul din Ucraina a servit atât drept laborator, cât și drept catalizator pentru amenințările hibride ale Rusiei. Multe dintre tacticile, tehnicile și procedurile utilizate împotriva alegerilor occidentale (și cel mai recent observate în forță deplină în Moldova) sunt direct aliniate cu

obiectivele geopolitice ale Moscovei, precum și cu scopul său strategic de a eroda sprijinul internațional pentru Ucraina.²⁷ Prin urmare, apărarea alegerilor nu mai este doar o problemă de politică internă; este parte integrantă a securității internaționale și a apărării colective a modelului democratic în sine, așa cum a reiterat NATO și UE în repetate rânduri.²⁸

1.4. SCOPUL, DOMENIUL DE APLICARE ȘI METODOLOGIA RAPORTULUI

Prevenirea provocărilor reprezentate de amenințările hibride necesită o înțelegere aprofundată a tacticilor utilizate de actorii malițioși și a strategiilor necesare pentru a le contracara. Ca parte a angajamentului Suediei de a consolida democrația și statul de drept, Academia Folke Bernadotte (FBA) susține acest obiectiv prin cercetarea și schimbul de cunoștințe cu actorii internaționali care se confruntă cu astfel de amenințări, contribuind astfel la dezvoltarea unor democrații mai reziliente. Acest sprijin se extinde dincolo de observarea alegerilor și include asistență electorală menită a consolida pregătirea și reziliența electorală.

Prezentul raport reunește și prezintă expertiza privind contracararea amenințărilor hibride la adresa proceselor electorale, concentrându-se în principal pe evoluțiile înregistrate începând cu anul 2024. Raportul debutează cu o prezentare generală a amenințărilor hibride la adresa alegerilor, a ecosistemului în care acestea se desfășoară și a impactului lor general asupra integrității electorale, încrederii publice și proceselor democratice în contextul geopolitic global actual.

Capitolele următoare explorează trei direcții cheie prin care actorii malițioși influențează alegerile: manipularea și interferența informațiilor, finanțarea politică ilicită și atacurile cibernetice. Urmează un capitol despre combaterea amenințărilor hibride, axat în special pe experiențe în stabilirea rețelelor de cooperare electorală. În cele din urmă, capitolul final prezintă principalele constatări și recomandări.

Acest raport este destinat în primul rând instituțiilor implicate în organizarea, sprijinirea sau contribuția la procesele electorale, în special în statele afectate de conflicte și în cele fragile, precum și în țările expuse amenințărilor hibride, mai ales în Europa de Est și Balcanii de Vest, unde FBA este deosebit de activă. În acest sens, raportul stă la baza programelor practice ale FBA pentru consolidarea rezilienței democratice în rândul actorilor electorali din aceste regiuni.

02 Acțiunile străine de manipulare a informațiilor și ingerințele străine (FIMI) și alegerile

FFIMI reprezintă o componentă esențială a amenințărilor hibride contemporane – un mecanism sofisticat de influență, menită să polueze mediul informațional și să manipuleze opinia publică. O strategie frecvent observată integrează producția de conținut la scară industrială cu diseminarea pe mai multe niveluri.²⁹

În primul rând, adversarii produc cantități uriașe de conținut – de la articole și meme-uri până la deepfake-uri generate de inteligență artificială – meticulos concepute pentru a exploata „problemele sociale marginale” precum imigrația și anxietatea economică.³⁰ În al doilea rând, acest conținut este diseminat prin folosirea unei game largi de tehnici, inclusiv rețele automate de boți, conturi neautentice coordonate și scheme de „influență contra cost”, care utilizează influenceri plătiți pentru a spăla narațiunii sponsorizate de stat.³¹ Aceasta implică adesea o infrastructură înșelătoare, cum ar fi tehnica „Doppelgänger”, clonarea site-urilor de știri legitime pentru a da credibilitate dezinformării.³²

„...dezvăluie o intenție strategică care se extinde mult dincolo de amestecul în alegeri, urmărind în schimb ducerea unui război informațional persistent.”

Aceste eforturi tactice sunt ghidate de cadre strategice generale. Documente rusești scurse în spațiul public dezvăluie că operațiunile sunt dirijate de „metodichka” (manuale narative) meticulos elaborate, care detaliază modul de amplificare a tensiunilor interne pentru a promova obiective de politică externă. Acest lucru dezvăluie o intenție strategică care se extinde mult dincolo de amestecul în alegeri, urmărind în schimb ducerea unui război informațional persistent.³³

2.1. TENDINȚE RECENTE

Perioada de la începutul anului 2024 a oferit o serie de studii de caz elocvente și concrete, care evidențiază tacticile în evoluție și intensitatea crescândă a amenințărilor hibride ce vizează alegerile democratice. Aceste evenimente, care se desfășoară în UE, Statele Unite (SUA) și vecinătatea estică a Europei, furnizează perspective cruciale asupra strategiei operaționale

actuale a actorilor maligni și a vulnerabilităților pe care aceștia încearcă să le exploateze.

Alegerile pentru Parlamentul European din 2024: o țintă transnațională

Alegerile pentru Parlamentul European din iunie 2024 au constituit o țintă transnațională însemnată pentru campaniile FIMI, verificatorii de informații detectând o creștere accentuată a dezinformării axate pe UE în cel puțin unsprezece țări.³⁴ Agenția de Design Social din Rusia a orchestrat o „contracampanie cuprinzătoare împotriva Europei”, menită să susțină candidații de extremă dreapta și eurosceptici prin amplificarea narațiunilor despre colapsul economic și erodarea valorilor naționale.³⁵ Această campanie a fost executată, în parte, prin intermediul rețelei extinse „Doppelgänger”, care a valorificat site-uri media clonate și a stabilit rețele de influență pentru a injecta dezinformare pro-Kremlin în ecosistemul informațional european.³⁶

Alegerile anulate din România: un moment de cotitură

Într-o demonstrație clară a impactului acestor amenințări, Curtea Constituțională a României a anulat rezultatele primului tur al alegerilor prezidențiale de la sfârșitul anului 2024, invocând ingerințe străine coordonate și finanțare online opacă. Agențiile de informații au dezvăluit o campanie sofisticată centrată pe TikTok, unde rețelele de influenceri plătiți și activitatea neautentică la scară largă au amplificat un candidat anterior marginal, pro-Kremlin, a cărui prezență online era incompatibilă cu cheltuielile de campanie declarate.³⁷ La nivelul UE, Comisia a inițiat proceduri oficiale în temeiul Legii privind serviciile digitale (DSA) pentru a investiga sistemele de reducere a riscurilor și de recomandare ale TikTok, în legătură cu alegerile din România.³⁸

Analiștii au identificat o rețea de mii de conturi inactive și compromise, multe dintre ele provenind din Rusia și Iran, care au fost activate pentru a inunda platforma cu un conținut manipulator. Așa cum este descris în Capitolul 3, acest lucru a fost dublat de indicii puternice ale finanțării străine ilicite, deoarece prezența online a candidatului s-a abătut de la cheltuielile de campanie declarate oficial.

Deși observatorii independenți au îndemnat la prudență, subliniind dificultatea de a dovedi o legătură causală directă între activitatea online și voturi, cazul ilustrează modul în care o campanie FIMI bine finanțată poate submina încrederea în rezultatul electoral până la punctul invalidării. În același timp, cazul României a atras critici, observatorii subliniind că dependența de informații clasificate creează lacune în transparență și contestabilitate. În plus, aceștia au susținut că soluțiile radicale riscă să rateze obiectivul final.

Dificultățile Moldovei: Alegeri sub foc hibrid

Republica Moldova oferă un exemplu în timp real al unei țări care se apără împotriva unui atac hibrid intens și integrat. În timp ce atacul lansat de Rusia împotriva Ucrainei în 2014 a urmat strategia „hack-and-broadcast” care îmbină intruziunea cibernetică cu manipularea informațiilor,³⁹ operațiunile desfășurate în Republica Moldova au evoluat într-o formă de presiune cronică, multidimensională, menită să permită capturarea statului prin intermediul urnelor de vot.⁴⁰

Alegerile prezidențiale și referendumul privind aderarea la UE din 2024 s-au confruntat cu ceea ce observatorii internaționali au descris drept un „război hibrid” orchestrat din exterior.⁴¹ FIMI au servit drept strat integrator al acestei campanii de coerciție desfășurate pe multiple planuri. Actori aliniați Rusiei au desfășurat o campanie bazată pe narative menite să prezinte guvernul pro-UE ca fiind incompetent, campanie amplificată de rețelele coordonate de pe Telegram și de Biserica Ortodoxă din Republica Moldova.⁴² Acest atac informațional a fost asigurat prin finanțare ilicită la scară largă – cu aproximativ 39 de milioane de dolari canalizate de către un oligarh fugar pentru a finanța cumpărarea de voturi și proteste – și completat de amenințări cu perturbări fizice, cum ar fi amenințări false cu bombă la secțiile de votare din diasporă.⁴³

Tacticile utilizate în 2024 au reprezentat un preludiu la o campanie și mai intensă care viza alegerile parlamentare cruciale din septembrie 2025. Documente de la Kremlin scurse în spațiul public au dezvăluit o strategie multidimensională, menită să contribuie la deraierea Moldovei de la parcursul european și, în cele din urmă, la înlăturarea de la putere a Președintei Sandu.⁴⁴ Planul detalia un model clasic de amenințare hibridă, inclusiv:

- O campanie de dezinformare pe scară largă pe platforme precum Telegram, TikTok și Facebook, cu folosirea unor narațiuni în care Președinta Sandu era prezentată ca o marionetă străină ce trage țara în război.⁴⁵
- Finanțare ilicită la scară largă pentru cumpărarea de voturi și finanțarea partidelor pro-ruse.⁴⁶
- Utilizarea de materiale compromițătoare („kompromat”) pentru exercitarea presiunilor asupra oficialilor și recrutarea diasporei moldovenești pentru a călători și a vota.⁴⁷
- Recrutarea de tineri din cluburi sportive și rețele criminale pentru a organiza provocări violente și proteste perturbatoare.⁴⁸

Acest plan a fost pus în aplicare în mod activ. Pe 22 septembrie 2025, cu doar câteva zile înainte de alegeri, autoritățile moldovenești au desfășurat o operațiune masivă pentru a destructura un complot de destabilizare susținut de Rusia. Poliția a reținut 74 de persoane și a efectuat peste 250 de percheziții, destrucurând o rețea despre care se presupunea că a fost condusă cu sprijinul serviciului de informații rusec, care opera așa-numitul grup media „Trust” pentru a răspândi propagandă.⁴⁹ Această acțiune a urmat unor eforturi anterioare de a reprimă frontul informațional, inclusiv o solicitare oficială de blocare a 443 de canale TikTok.⁵⁰

Acțiunile în cauză se adaugă presiunii cibernetice persistente. Din 2022, grupuri de hackeri pro-ruși au lansat atacuri cibernetice asupra instituțiilor guvernamentale, au creat site-uri web de scurgeri de informații și au spart servere de e-mail ale Parlamentului pentru a pregăti operațiuni de „hack and leak”.⁵¹ Ca răspuns la aceste amenințări tot mai mari, Moldova a beneficiat de sprijin internațional considerabil. În 2023, a fost înființată Misiunea de Parteneriat a UE în Republica Moldova (EUPM) pentru a spori reziliența Republicii Moldova la amenințările hibride, inclusiv în ceea ce privește securitatea cibernetică și FIMI. În plus, în 2025, UE a desfășurat la Chișinău o Echipă de Răspuns Rapid Hibrid și Rezerva de Securitate Cibernetică a UE – prima activare a mecanismului de asistență cibernetică rapidă al UE – pentru a sprijini apărarea electorală a țării.⁵²

Luat în ansamblu, cazul Moldovei demonstrează realitatea ingerinței electorale moderne: nu este vorba de o serie de incidente izolate, ci de un război hibrid complet integrat. Acest lucru subliniază necesitatea ca statele să valorifice expertiza internațională, să învețe unele de la altele și să construiască o apărare la nivelul întregii societăți pentru a-și consolida sistemele democratice critice.

Ucraina: Războiul informațional ca instrument al conflictului convențional

Având în vedere suspendarea alegerilor din Ucraina în baza legii marțiale, campaniile FIMI ale Rusiei împotriva Ucrainei funcționează ca un atac preventiv asupra viitoarelor sale procese democratice. „Contracampania cuprinzătoare împotriva Ucrainei” a Agenției de Design Social este un instrument direct al efortului de război, menit să submineze conducerea Ucrainei, să demoralizeze forțele sale armate și să degradeze coeziunea socială.⁵³ Prin amplificarea narațiunilor de corupție și alimentarea rivalităților politice, campania pe termen lung urmărește să se asigure că, atunci când vor avea loc alegeri postbelice, electoratul va fi fragmentat și receptiv la alternative pro-ruse.⁵⁴

Eforturile actuale au evoluat de la strategiile anterioare, care combinau intruziunile cibernetice cu manipularea informațiilor. Anterior și în timpul alegerilor prezidențiale din Ucraina din 2014, rețelele politice, instituțiile media și intermediarii oligarhi apropiați Moscovei au fost mobilizați pentru a promova agende pro-Kremlin și a estompa traiectoria europeană a Ucrainei. Partidele

și personalitățile pro-ruse au servit drept vectori pentru alinierea politicilor și amplificarea mesajului, în timp ce interesele de afaceri legate de Rusia au extins influența Moscovei.⁵⁵ În paralel, interferențele cibernetice au vizat mecanismele electorale: intruziunile la Comisia Electorală Centrală au șters fișiere și au implantat programe malware concepute pentru a afișa rezultate fabricate, completate de atacuri DDoS pentru a întârzia raportarea; televiziunea de stat rusă a difuzat ulterior grafica falsă - un exemplu timpuriu de combinare a intruziunii cibernetice cu manipularea informațiilor.⁵⁶ Se așteaptă ca următoarele alegeri din Ucraina să aibă loc în circumstanțe dificile, țara urmând să se confrunte probabil cu tentative externe intensificate de a influența sau perturba procesul electoral.

Alegerile prezidențiale americane din 2024: asaltul mai multor actori

Alegerile americane din 2024 au constituit un punct central pentru mai mulți actori străini cu strategii distincte.⁵⁷ Rusia a folosit o gamă largă de instrumente, de la amenințări false cu bombă la secțiile de votare până la deepfake-uri generate de inteligența artificială, utilizarea continuă a rețelei sale de influență „Doppelgänger” și mobilizarea de actori proxy interni.⁵⁸ Departamentul de Justiție a destructurat rețeaua „Doppelgänger”, confiscând 32 de domenii și formulând acuzații împotriva unor agenți ruși, asociați cu mass-media de stat rusă.⁵⁹ Activitatea Chinei a fost mai ținută, concentrându-se pe liniile de falie ale „războiului cultural” din SUA și pe cursele electorale de nivel inferior, mai degrabă decât pe competiția prezidențială.⁶⁰ Iranul a combinat recunoașterea online cu operațiuni de „hack and leak”, autoritățile americane inculpând actori legați de Iran pentru compromiterea unei campanii prezidențiale în scopul furtului și scurgerii de materiale.⁶¹ Ca răspuns, agențiile americane au adoptat o abordare de „pre-bunking” și au folosit o combinație de rechizitorii, sancțiuni și confiscări pentru a crește costurile și a perturba infrastructura.⁶²

Evaluările independente arată că, deși efortul cumulat de influență a fost substanțial și tot mai mult bazat pe inteligență artificială, impactul operațional asupra mecanismelor electorale principale a fost limitat – însă prejudiciul informațional (confuzie, polarizare, cinism) rămâne un risc central pentru ciclurile electorale viitoare.⁶³

2.2. PROVOCĂRI ÎN DETECTARE, ATRIBUIRE ȘI RĂSPUNS

Apărarea împotriva FIMI prezintă mai multe provocări considerabile. Atribuirea rămâne un blocaj critic, deoarece utilizarea proxy-urilor și a tehnicilor complexe de spălare a informațiilor este concepută în mod deliberat pentru a crea ambiguitate și a obstrucționa un răspuns prompt și proporțional.⁶⁴ Viteza și amploarea campaniilor moderne, amplificate de inteligența artificială, copleșesc adesea contramăsurile tradiționale, cum ar fi verificarea faptelor.⁶⁵ În plus, democrațiile se confruntă cu un echilibru dificil între securitate și libertatea de exprimare, o dilemă pe care actorii malițioși o exploatează, calificând acțiunile defensive drept cenzură.⁶⁶

Responsabilitatea platformelor constituie o provocare centrală, deoarece modelele de afaceri ale multor companii de social media recompensează conținutul polarizant, care maximizează implicarea.⁶⁷ Asigurarea unei transparențe semnificative în ceea ce privește algoritmi de clasificare, regulile de moderare a conținutului și accesul cercetătorilor la date rămâne o provocare controversată atât din punct de vedere normativ, cât și politic.⁶⁸ DSA al UE reprezintă un răspuns normativ relevant, transferând obligațiile către platformele online foarte mari pentru a evalua riscurile sistemice și a crește transparența. Aplicarea legii a început, cu proceduri formale legate de integritatea alegerilor în 2024, dar conformitatea rămâne inegală.⁶⁹ În paralel, platformele își recalibrează abordarea: Google și Meta au anunțat planuri de a restricționa sau de înceta difuzarea publicității politice în UE, invocând noul cadru de reglementare.⁷⁰

În timp ce reglementările sunt în creștere, alte forme de transparență se erodează. Retragerea de către Meta a instrumentului său CrowdTangle, care oferea informații în timp real despre conținutul public de pe rețelele sociale, a redus vizibilitatea asupra rețelelor de influență înaintea alegerilor majore din 2024.⁷¹ Eforturile voluntare ale industriei, cum ar fi „Tech

Accord” pentru a combate inteligența artificială înșelătoare în alegeri, au fost criticate pentru lipsa responsabilității și a unor repere măsurabile.⁷²

Un nou front de responsabilitate s-a deschis în jurul provenienței și detectării conținutului generat de inteligență artificială. Deși standarde deschise, cum ar fi C2PA Content Credentials, sunt adoptate pentru a eticheta conținutul autentic, acestea se confruntă cu o dinamică de tip „șoarecele și pisica”, având o acoperire incompletă.⁷³ În paralel, instrumente precum SynthID de la Google DeepMind încorporează filigrane imperceptibile și robuste direct în conținutul generat de inteligența artificială, în momentul creării.⁷⁴ Cu toate acestea, chiar și chatbot-urile cu inteligență artificială ale Google nu au implementat încă acest standard și nu pot detecta conținutul pe care l-au produs. Acest lucru subliniază nevoia urgentă de standarde solide, interoperabile și aplicate cu strictețe pentru proveniența conținutului.

Pe măsură ce inteligența artificială generativă continuă să reducă costurile operațiunilor de influență, chiar dacă platformele introduc mecanisme de protecție, menținerea controlului de reglementare și a supravegherii acestor operațiuni va rămâne o provocare.⁷⁵ Cercetările au documentat, de asemenea, cazuri în care entități asociate unor state sau supuse sancțiunilor au reușit să achiziționeze sau să plaseze conținut de influență în pofida politicilor platformei, subliniind necesitatea unor mecanisme verificabile pentru tehnologia publicitară și a unor mecanisme de verificare a sancțiunilor, care să funcționeze în practică.⁷⁶

2.3. CE SE POATE FACE? STRATEGII PENTRU CONTRACARAREA FIMI CE VIZEAZĂ ALEGERILE

Evoluția ingerinței electorale de la atacuri episodice la o stare de conflict informațional sistemic cronic impune o schimbare fundamentală a strategiei defensive. Viteza și amploarea campaniilor moderne de tip FIMI, amplificate de inteligența artificială, depășesc adesea contramăsurile tradiționale, cum ar fi verificarea reactivă a faptelor. Prin urmare, un răspuns eficient trebuie să fie proactiv, colaborativ și pe mai multe niveluri, abordând dimensiunile instituționale, de reglementare și tehnologice ale amenințării. În mod crucial, combaterea FIMI cere un răspuns conceptual compatibil cu normele democratice. Abordarea modernă, cu respectarea drepturilor, care a fost adoptată de UE, este centrată pe comportament. Se axează pe vizarea comportamentelor observabile, manipulative – precum rețelele de boți sau conturile neautentice coordonate. Aceasta îi permite unui organ statal să contracareze operațiuni ostile pe motive solide, bazate pe dovezi, fără a submina libertatea de exprimare.⁷⁷

„În mod crucial, combaterea FIMI cere un răspuns conceptual compatibil cu normele democratice.”

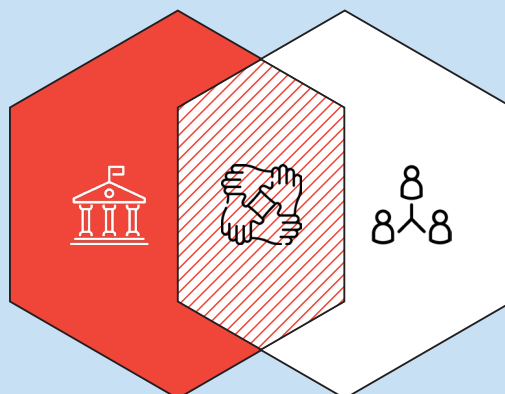
O abordare la nivelul întregului guvern prin intermediul rețelelor de cooperare

Acest raport evidențiază modul în care adversarii exploatează în mod deliberat discrepanțele dintre responsabilitățile diferitor agenții, făcând insuficient un răspuns de securitate izolat. Strategia fundamentală pentru contracararea FIMI care vizează alegerile este de a stabili o apărare la fel de integrată și interconectată, după cum s-a procedat în mai multe țări în timpul alegerilor recente (așa cum este detaliat în Capitolul 5).

O ABORDARE LA NIVELUL ÎNTREGULUI GUVERN

Răspuns guvernamental unificat
Apărare coordonată împotriva amenințărilor

Agenții guvernamentale individuale
Expertiză și resurse specializate



Rețele de cooperare
Schimbul colaborativ de informații și acțiunea coordonată

Consolidarea cadrelor juridice și de reglementare

O provocare majoră în combaterea FIMI este responsabilitatea platformelor. Actul legislativ privind serviciile digitale (DSA) al UE oferă un model foarte important pentru reglementarea mediului informațional, în ciuda dezbatelor existente cu privire la aplicabilitatea sa. Legea transferă către „platformele online foarte mari” obligațiile de a evalua riscurile sistemice la adresa proceselor democratice, de a face sistemele lor de recomandare mai transparente și de a oferi acces la date cercetătorilor verificați. Aplicarea acestor principii este esențială pentru crearea unui mediu informațional mai puțin vulnerabil la manipulare intenționată.

Această abordare de reglementare trebuie să se extindă și la finanțarea politică ilicită, care servește drept vector cheie pentru finanțarea campaniilor FIMI. Este crucial să se elimine lacunele legate de donațiile online anonime, utilizarea nereglementată a terților activiști și cheltuielile opace pentru publicitate pe rețele sociale (așa cum este detaliat în Capitolul 3).

Promovarea unei reziliențe la nivelul întregii societăți

O apărare centrată exclusiv pe stat este insuficientă, deoarece reziliența democratică pe termen lung depinde de o societate informată, critică și implicată. Prin urmare, o strategie esențială constă în a investi într-o abordare la nivelul întregii societăți, care responsabilizează cetățenii și consolidează spațiul public de informare, pornind de la bază.

Ecosistemele media independente sunt esențiale pentru această abordare. Totuși, acestea operează adesea sub constrângeri severe – precaritate financiară, concentrare a pieței, publicitate de stat politizată, și presiune juridică sau fizică – care amenință atât sustenabilitatea, cât și independența editorială. Abordarea acestor provocări necesită direcții de acțiune complementare.

Inițiativele naționale de dezvoltare a alfabetizării în domeniul mass-media și al inteligenței artificiale au un rol crucial pentru înzestrarea cetățenilor cu abilitățile necesare de identificare și evaluare critică a conținutului manipulativ, consolidând astfel „apărarea cognitivă” a populației. Acest aspect trebuie completat printr-un sprijin solid pentru

mass-media independentă, deoarece un peisaj mediatic divers și cu resurse suficiente asigură un bastion vital împotriva dezinformării, oferind cetățenilor alternative fiabile, bazate pe fapte, la propaganda sponsorizată de stat.

Un element esențial al acestui sprijin este investiția dedicată jurnalismului de investigație. În repetate rânduri, mass-media de investigație s-a dovedit a fi extrem de eficientă în dezvăluirea mecanismelor amenințărilor hibride – de la expunerea schemelor complexe de finanțare ilicită și cartografierea rețelelor de dezinformare până la identificarea actorilor din spatele operațiunilor de „hack and leak”. O astfel de muncă este crucială nu numai pentru înțelegerea publicului, ci și pentru furnizarea bazei de dovezi necesare pentru luarea de măsuri oficiale la nivel guvernamental.

Construirea unor mecanisme de apărare proactivă și reziliență tehnologică

Având în vedere dificultatea de a elimina dezinformarea odată ce aceasta s-a răspândit, este esențială adoptarea unei abordări proactive. Obiectivul nu este însă de a contracara fiecare afirmație falsă care circulă online. Centrul de greutate constă în transparență radicală, consecventă, care reduce ambiguitatea și oferă fapte verificabile pe care alții se pot baza.⁷⁸

Acest lucru este operaționalizat prin intermediul unui hub de „sursă de adevăr” accesibil publicului – care conține proceduri, întrebări frecvente, corecții și jurnale de modificări – ce standardizează locurile unde publicul și mass-media găsesc informații autorizate și stabilește un punct de referință durabil în timpul incidentelor.⁷⁹ Astfel de practici reduc considerabil golurile informaționale pe care adversarii le exploatează și consolidează în timp credibilitatea instituțională.⁸⁰

Având în vedere această perspectivă asupra transparenței, pre-bunking-ul este utilizat selectiv și limitat în jurul unor perioade de risc cunoscute (înregistrare, sondaje, rezultate) pentru a preveni anumite tactici și nu pentru a infirma fiecare narațiune, ținându-se cont în același timp de o absorbție inegală și o acoperire incompletă a provenienței.⁸¹ Accentul se pune pe explicații concise de tipul „la ce să vă așteptați/cum să verificați/unde să raportați” care ajută publicul să recunoască tiparele de manipulare (de exemplu, conținut falsificat, încadrare de tip hack-and-leak) și să direcționeze atenția către pagina oficială.⁸² Implementat în acest fel, pre-bunking-ul este mai degrabă accelerator rentabil al transparenței decât un război paralel al conținutului.⁸³

Această abordare își recunoaște limitele. Este imposibil să contracarezi fiecare dezinformare, iar publicul motivat va prefera uneori falsuri congruente. Prin urmare, strategia constă în asumarea faptelor, reducerea ambiguității și vizarea comportamentelor manipulative – astfel încât actorii credibili să aibă un punct de reper stabil, iar publicul să aibă o sursă previzibilă de verificat.⁸⁴

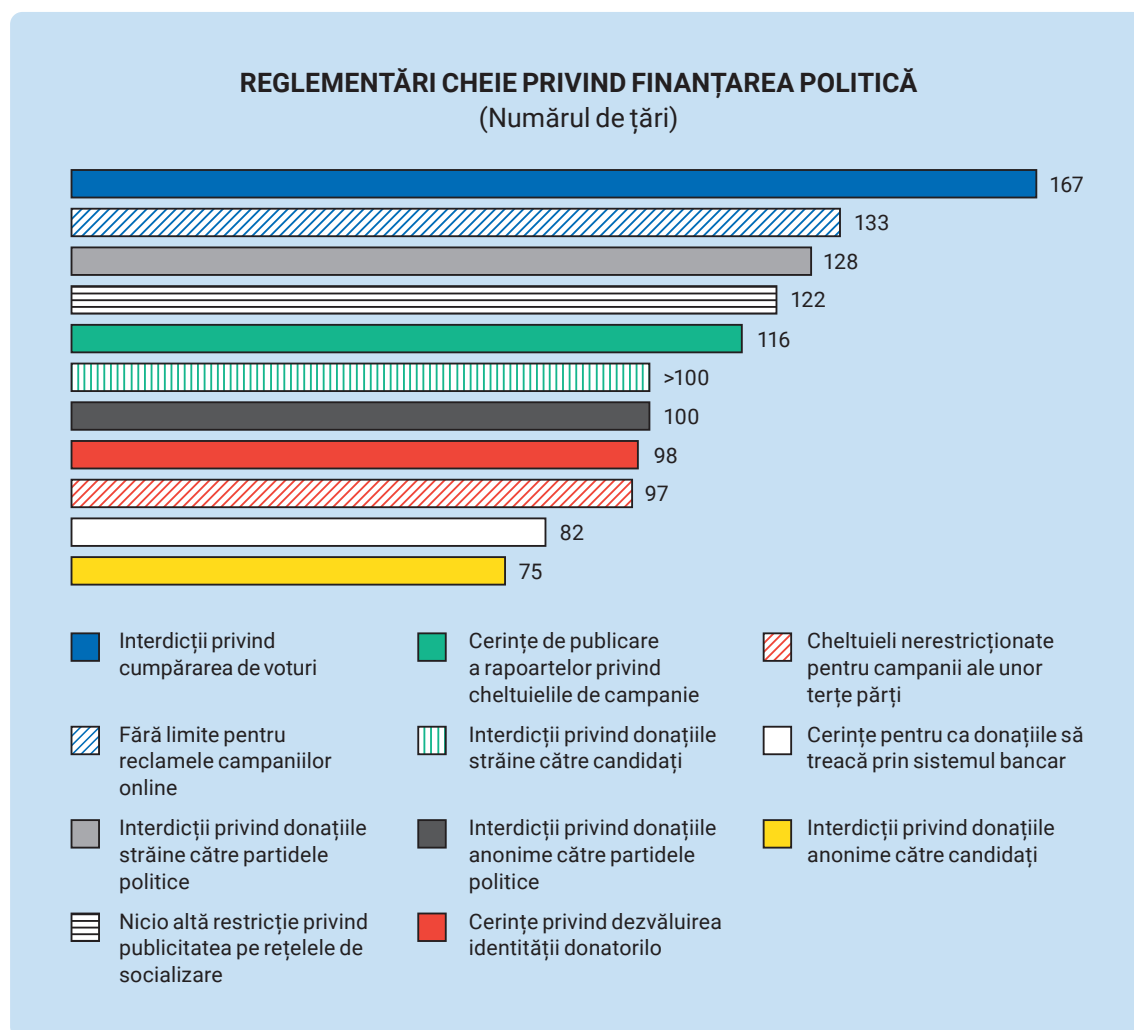
Această strategie de transparență trebuie să fie însoțită de un plan de abordare a cursei înarmărilor tehnologice, în special a provocării reprezentate de conținutul media sintetic generat de inteligența artificială. Apărarea împotriva deepfake-urilor și a clonelor vocale necesită depășirea simplei detectări, care este blocată într-o dinamică de tipul „șoarecele și pisica” cu adversarii.⁸⁵ Strategia orientată spre viitor presupune investiții în tehnologii de certificare a provenienței conținutului și de aplicare a filigranelor digitale (watermarking), precum și promovarea utilizării acestora. Standardele deschise, cum ar fi C2PA Content Credentials, care funcționează ca o etichetă digitală de autenticitate, și instrumentele robuste de marcare cu filigran, cum ar fi SynthID de la Google DeepMind, care încorporează în conținutul media generat de inteligența artificială în momentul creării o semnătură imperceptibilă, lizibilă automat, sunt esențiale pentru restabilirea unui nivel de bază de încredere în ecosistemul digital.⁸⁶

În cele din urmă, aceste strategii trebuie integrate. Conform concluziei generale a raportului, apărarea electorală în epoca modernă trebuie să reprezinte un proces continuu, adaptabil, proactiv și colaborativ.

03 Finanțarea politică ilicită și amenințările hibride

Banii nu sunt, în mod inherent, un factor nociv în procesele electorale; dimpotrivă, ei sunt esențiali. Partidele politice se bazează pe ei pentru a promova idei, a recruta membri și a instrui candidați, în timp ce organele electorale au nevoie de ei pentru educația civică și pentru a administra logistica alegerilor. Cu toate acestea, banii în politică prezintă riscuri serioase pentru democrație, de la accesul inegal la finanțare și stimulente pentru corupție, până la finanțarea ilicită sau ilegală, care vizează influențarea alegerilor.⁸⁷

Aceasta include utilizarea resurselor financiare în mod ilegitim sau ilegal pentru a influența procesele electorale, atât pe plan intern, cât și extern. Cel din urmă aspect este deosebit de îngrijorător, având în vedere distorsiunile pe care le provoacă în întregul sistem democratic, erodarea încrederii publice pe care o generează și implicațiile geopolitice pe care le atrage după sine.



Deși nu reprezintă un fenomen nou, interferența electorală străină prin intermediul finanțării politice ilicite este din ce în ce mai recunoscută. În Muntenegru, de exemplu, în timpul alegerilor parlamentare din 2016, au apărut acuzații de finanțare externă a campaniilor electorale, existând afirmații conform cărora opoziția servea unor interese străine. În mod similar, în timpul alegerilor anticipate din Moldova din 2021, observatorii și-au exprimat îngrijorarea cu privire la finanțarea externă.⁸⁸

3.1. FINANȚAREA POLITICĂ ILICITĂ CA VECTOR DE INTERFERENȚĂ

Există trei domenii critice prin care actorii malițioși încearcă de obicei să influențeze alegerile prin finanțare politică ilicită. Acestea sunt: (1) cumpărarea de voturi; (2) donații străine și anonime, inclusiv prin intermediul criptomonedelor; și (3) contribuții ale terților, finanțarea publicității pe rețele sociale și a influencerilor.

Cumpărarea de voturi

Deși interzisă în 167 de țări, cumpărarea de voturi rămâne o modalitate comună de influențare a alegerilor.⁸⁹ În timpul alegerilor parlamentare din Moldova din 2025, observatorii internaționali au remarcat amploarea schemelor identificate de cumpărare a voturilor care vizau influențarea alegătorilor, aceste eforturi fiind coordonate de o rețea organizată, finanțată de Rusia.⁹⁰

Țara se confruntase deja cu provocări similare în alegerile anterioare. De exemplu, în alegerile locale din 2023, agenți politici legați cu Rusia au fost acuzați că au încercat să canalizeze fonduri în țară în scopul cumpărării de voturi, promovând astfel interesele Rusiei.⁹¹ Mai grav, la alegerile prezidențiale și referendumul constituțional din 2024, observatorii internaționali au remarcat modul în care forțele de ordine, mulți actori internaționali și societatea civilă au descris Republica Moldova drept ținta unui „război hibrid” în curs de desfășurare, ce implica finanțare politică ilicită, dezinformare și atacuri cibernetice.⁹²

Se crede că aceste scheme includeau distribuirea de carduri bancare din Rusia. Analistii au descris presupusul modus operandi după cum urmează:

Potrivit informațiilor disponibile, milioane de dolari în numerar au fost introduse ilegal în țară de către persoane asociate cu oligarhul fugar Ilan Șor, sancționat de SUA, eludând eforturile organelor de aplicare a legii de a stopa fluxul ilegal de fonduri. Autoritățile au organizat percheziții la aeroport pentru a opri această paradă de persoane care călătoreau la Moscova ca să aducă înapoi numerar în mod clandestin. Cu toate acestea, Rusia a găsit alte modalități de a trimite fonduri în Moldova. Prin intermediul sistemului de plăți rusec MIR, resursele financiare ar fi fost direcționate către alegătorii moldoveni, în special prin rețele economice din regiunea transnistreană - un teritoriu separatist care a servit mult timp drept bază pentru operațiunile de influență ale Moscovei.

Autoritățile moldovenești au tras semnale de alarmă cu privire la cumpărarea de voturi la scară largă, Inspectoratul General al Poliției documentând cazuri de luare de mită care au implicat, doar în luna septembrie, cel puțin 130.000 de cetățeni și peste cincisprezece milioane de dolari în transferuri ilicite din Rusia. În realitate, amploarea ar putea fi considerabil mai mare, unii oficiali estimând-o la aproximativ 100 de milioane de dolari pentru întreaga campanie.

Fondurile sunt canalizate către scheme concepute pentru a stabili o rețea națională de cumpărare a voturilor, asemănătoare unor piramide financiare cu straturi complexe de tranzacții, menite să evite verificările. Aceste fonduri variază de la alocații „sociale” pentru pensionari moldoveni până la „bonusuri” salariale pentru angajați ai structurilor administrației locale din teritoriul autonom al Găgăuziei. Bani ajung acum, potrivit poliției și relatărilor independente, și în mâinile așa-numiților „coordonatori” și „susținători” locali ai blocului electoral „Victoria”, o entitate politică creată la Moscova și controlată, se pare, de aceasta (Olari 2024).

FONDURI RUSEȘTI CANALIZATE ÎN MOLDOVA

\$100,000K
\$15,000K
130K

Fonduri inițiale
Fonduri estimate
pentru întreaga
campanie

Transferuri ilicite
Transferuri
documentate doar în
septembrie

Cetățeni mituiți
Cetățenii implicați în
cazuri de luare de mită

Donații străine și anonime

Interdicțiile sau limitele privind donațiile străine și anonime se numără printre cele mai comune reglementări în domeniul finanțării politice. Începând cu 2025, 128 de țări interzic donațiile străine către partidele politice, peste 100 de țări extinzând interdicția la candidați. Donațiile anonime sunt, de asemenea, restricționate în 100 de țări pentru partide și în 75 de țări pentru candidați.⁹³

Interdicția privind donațiile străine se bazează, în general, pe principiul că interesele externe nu ar trebui să influențeze politica națională. În schimb, interdicția privind donațiile anonime își propune, de obicei, să blocheze contribuțiile ilegale. Cu toate acestea, implementarea regulilor date este una dintre cele mai complexe sarcini pentru organele de supraveghere. Contribuțiile străine pentru ingerința în alegeri pot circula peste granițe în mare parte nedetectate, tranzitând adesea jurisdicții offshore și paradisuri fiscale, unde adevărata lor sursă este ușor de ascuns; acest lucru face extrem de dificilă urmărirea fondurilor și identificarea cu certitudine a originii lor străine.⁹⁴

Criptomonedele complică și mai mult peisajul, permițând fluxuri financiare opace, inclusiv provenite de la actori ostili care încearcă să influențeze alegerile în străinătate. Utilizarea lor s-a extins rapid în ultimul deceniu: în timp ce Bitcoin rămâne dominant, peste 16.000 de criptomonede sunt acum tranzacționate la peste 1.300 de burse, cu aproximativ 861 de milioane de utilizatori la nivel mondial - aproximativ 11% din populația globală din peste 150 de țări.⁹⁵ În plus, se așteaptă ca piața să se extindă în continuare, valoarea tranzacționării cu criptomonede fiind proiectată să crească de la 71,35 miliarde de dolari în 2025 la peste 260 de miliarde de dolari până în 2032.⁹⁶

Finanțarea politică a fost afectată în mod direct, deoarece anonimitatea majorității tranzacțiilor cu criptomonede face ca donațiile din străinătate să fie deosebit de dificil de urmărit.⁹⁷ Un exemplu notabil a fost alegerile prezidențiale din SUA din 2016, când un rechizitoriu al marelui juriu a dezvăluit că fonduri rusești ar fi fost canalizate prin intermediul burselor de criptomonede.⁹⁸ Cazul a evidențiat limitele supravegherii, demonstrând că până și un sistem cu garanții relativ solide s-a confruntat cu dificultăți în abordarea criptomonedelor, deoarece legislația permitea comisiilor politice să accepte contribuții, luând în același timp doar măsuri „minim intruzive” pentru a verifica naționalitatea donatorilor.

Contribuții de la terți, finanțare pentru publicitate pe rețele sociale și influenceri

Cheltuielile efectuate de terți pot servi drept canal pentru fonduri străine destinate influențării alegerilor, cu diverse organizații sau persoane fizice, inclusiv societăți-fantomă, ONG-uri sau organizații caritabile acționând ca paravan, făcând campanii pentru sau împotriva partidelor și candidaților și devenind vectori pentru influența externă.⁹⁹

Publicitatea pe rețelele sociale constituie un alt instrument puternic pentru strângerea de fonduri și operațiuni politice, cheltuielile pentru campanii digitale crescând brusc la nivel mondial, în special de la începutul pandemiei de COVID-19.¹⁰⁰ Publicitatea online oferă actorilor străini o modalitate ușoară de a interveni în procesele electorale, avantaj facilitat de distanța fizică dintre sursele mesajelor publicitare și publicul-țintă, precum și de capacitatea de a realiza micro-direcționarea (micro-targeting) și de a personaliza conținutul generat.¹⁰¹ De exemplu, un actor străin poate achiziționa servicii de mesagerie pe rețelele sociale în numele unei campanii, în afara supravegherii interne, în timp ce opacitatea plăților online permite donatorilor să rămână anonimi.¹⁰²

Scandalul Cambridge Analytica din 2018 oferă un exemplu timpuriu, implicând utilizarea abuzivă a datelor private de pe Facebook de la peste 50 de milioane de utilizatori în timpul alegerilor din SUA din 2016. Totodată, a expus angajarea ilegală a zeci de cetățeni străini, a căror activitate în domeniul elaborării mesajelor de campanie, analizei datelor și publicității a fost considerată drept o contribuție în natură din surse străine, nepermisă de legislația electorală.¹⁰³

Alegerile americane din 2024 oferă un alt exemplu. Ca parte a „Operațiunii Doppelganger”, Departamentul de Justiție a confiscat 32 de domenii de internet utilizate de guvernul rus pentru campanii de influențare malignă. Conform anchetei, operațiunea s-a bazat pe influenceri remunerați și reclame plătite pe rețele de socializare, unele dintre ele generate de inteligență artificială, fiind utilizate profiluri de socializare false, care se prezentau drept cetățeni americani sau alți cetățeni non-ruși, pentru a direcționa utilizatorii către site-uri înregistrate prin tehnici de înregistrare abuzivă a numelor de domeniu, deghizate în publicații legitime de știri.¹⁰⁴

În același an, alegerile din România au relevat tipare similare, Curtea Constituțională anulând primul tur de scrutin. Un candidat nu a raportat cheltuieli de campanie, în ciuda unei prezențe online extinse și a informațiilor care indicau finanțare nedeclarată din surse externe. Cazul a evidențiat ample riscuri de corupție strategică, incluzând: finanțare de către terți prin actori proxy pentru reclame digitale, fără a dezvălui originile sau a respecta plafoanele legale, un război hibrid al finanțării politice, care sporește expunerea online din străinătate, precum și o supraveghere slabă din partea autorităților electorale, incapabile să urmărească rețelele complexe de publicitate digitală.¹⁰⁵

Mai recent, în timpul celui de-al doilea tur al alegerilor prezidențiale din Polonia din 2025, observatorii internaționali au raportat reclame pe Facebook suspecte a fi finanțate din străinătate. De la mijlocul lunii aprilie până la mijlocul lunii mai, două profiluri noi au cheltuit aproximativ 500.000 PLN (139.000 USD) pentru peste 100 de reclame video care susțineau un candidat și îi atacau pe alții, depășind chiar și cheltuielile candidaților. Cazul, raportat ca fiind probabil finanțat din surse externe, este încă în curs de soluționare. Observatorii au criticat răspunsul întârziat al autorităților, în timp ce Meta a declarat că reclamele nu au încălcat standardele sale sau legislația națională.

S-a descoperit că un alt cont difuzase reclame în valoare de 388.000 PLN (aproximativ 108.000 USD), folosind fonduri presupuse a fi canalizate din străinătate prin intermediul unei organizații a societății civile. Chiar dacă au fost depuse plângeri la Comisia Electorală Națională și la parchet pentru presupuse finanțări străine ilicite, observatorii au remarcat că „deși Meta aplică limite de cheltuieli agenților de publicitate prin intermediul unui proces automat, implementarea regulilor interne de către o platformă socială este în afara

domeniului de aplicare și a capacității actuale a organului de supraveghere a finanțării campaniilor”.¹⁰⁶ Acest caz subliniază provocarea tot mai mare pe care campaniile online finanțate din surse străine o reprezintă pentru mecanismele naționale de supraveghere, precum și limitele cadrelor de reglementare existente în asigurarea transparenței și responsabilității în publicitatea politică digitală.

3.2. CE SE POATE FACE? STRATEGII PENTRU CONSOLIDAREA REGLEMENTĂRII FINANȚĂRII POLITICE ȘI A SUPRAVEGHERII ÎMPOTRIVA INGERINȚELOR STRĂINE

Având în vedere numeroasele provocări menționate mai sus, ar trebui răspunsul să se concentreze pe stabilirea unor reglementări mai stricte privind finanțarea politică sau pe consolidarea supravegherii?

Înăsprirea reglementărilor

Un răspuns tipic este reducerea limitelor de donații și restricționarea cheltuielilor de campanie. Deși uneori necesare și chiar dezirabile, limitele excesive riscă să creeze noi dezechilibre și, în cele din urmă, să afecteze rezultatul alegerilor. Așa cum am menționat anterior, partidele și candidații au nevoie de acces la fonduri legitime pentru a-și desfășura operațiunile fără ingerințe; în lipsa acestor fonduri, ar putea recurge la sprijin extern ascuns sau la o raportare insuficientă a veniturilor și cheltuielilor.¹⁰⁷

Acestea fiind spuse, sunt adesea necesare reglementări mai stricte pentru a preveni și atenua amenințările hibride la adresa alegerilor, chiar dacă astfel de măsuri trebuie concepute cu atenție pentru a se asigura că orice contra-eforturi nu generează ele însele noi distorsiuni sau restricții care subminează principiile democratice fundamentale.

Interdicții și limitări

Un pas vital constă în interzicerea donațiilor străine și anonime către partide și candidați, acolo unde acestea nu sunt deja interzise.¹⁰⁸ Reglementările pot fi, de asemenea, îmbunătățite prin alinierea perioadelor de raportare cu intervalul de timp real al campaniei – în loc să se bazeze pe perioade de raportare artificiale sau strict definite, care exclud o mare parte din activitatea reală de campanie – atunci când riscul de ingerință străină este, probabil, cel mai semnificativ. Identificarea neconcordanțelor dintre venituri și cheltuieli poate ajuta apoi la descoperirea surselor de finanțare ilicite.

O altă provocare în ceea ce privește supravegherea ingerințelor străine în alegeri este utilizarea unor terțe părți pentru a canaliza cheltuielile de campanie, o practică încă nerestricționată în 97 de țări.¹⁰⁹ Publicitatea pe rețelele sociale constituie o lacună majoră: 133 de țări nu impun limite reclamelor online pentru campanii, iar 122 nu aplică alte restricții. Prin urmare, limitarea influenței străine necesită o reglementare mai strictă a publicității politice online, inclusiv definiții mai precise ale campaniilor digitale și cerințe mai mari de transparență.¹¹⁰

Aliniere internațională

O altă prioritate este consolidarea reglementărilor în toate jurisdicțiile și promovarea normelor și mecanismelor internaționale pentru îmbunătățirea transparenței fluxurilor financiare transnaționale. Acest aspect este crucial, deoarece finanțarea politică ilicită trece adesea prin paradisuri fiscale și structuri offshore pentru a-și ascunde originea. În centrul acestor cadre se află Grupul de Acțiune Financiară Internațională și standardele sale privind combaterea spălării banilor, în special cele referitoare la persoanele expuse politic și jurisdicțiile offshore.¹¹¹

Abordarea problemei criptomonedelor

Abordarea amenințărilor hibride la adresa alegerilor necesită, totodată, reguli mai explicite privind utilizarea criptomonedelor în finanțarea politică, având în vedere statutul lor anonim în majoritatea cazurilor și lipsa unei reglementări robuste. Supravegherea este adesea complicată de lipsa de claritate cu privire la statutul lor juridic – indiferent dacă sunt considerate active, valori mobiliare sau monedă fiduciară – și, în legătură cu aceasta, de tratamentul juridic diferit al contribuțiilor monetare și în natură. În majoritatea sistemelor, criptomonedele sunt considerate active și, prin urmare, sunt tratate ca niște contribuții în natură, însă nu întotdeauna, ceea ce face mai dificilă pentru agențiile de monitorizare determinarea cadrului juridic aplicabil și urmărirea acestora.¹¹²

Ca răspuns, unele țări au limitat sau chiar au interzis complet utilizarea criptomonedelor în finanțarea politică, aliniindu-se la restricțiile mai largi privind donațiile străine și anonime. Irlanda, de exemplu, a adoptat o lege care interzice donațiile de criptomonede către partide în 2022.¹¹³ Astfel de măsuri sunt relevante în special pentru acele criptomonede care sunt inerent anonime, printre care se numără unele dintre cele mai populare.¹¹⁴ O altă modalitate (indirectă) de a limita utilizarea criptomonedelor și de a atenua riscurile aferente în finanțarea politică este de a impune trecerea donațiilor prin sistemul bancar, așa cum este cazul în 82 de țări.¹¹⁵

Îmbunătățirea supravegherii de stat

Mai importantă decât înăsprirea reglementărilor este aplicarea celor deja existente. Cu toate acestea, supravegherea rămâne veriga slabă, agențiile fiind adesea împiedicate de mandate neclare, capacitate limitată și coordonare deficitară. Aspectul dat este deosebit de important în ceea ce privește colaborarea necesară dintre autoritățile electorale și unitățile de informații financiare, având în vedere accesul privilegiat al acestora din urmă la informații cheie indispensabile pentru monitorizarea fluxurilor de finanțare politică.¹¹⁶

„Mai importantă decât înăsprirea reglementărilor este aplicarea celor deja existente.”

O capacitate sporită și o colaborare mai strânsă sunt, în plus, vitale pentru organele de supraveghere care monitorizează tranzacțiile cu criptomonede, în special cooperarea cu platformele de tranzacționare a monedelor virtuale. În calitate de intermediari financiari, acești actori pot furniza informații cheie pentru identificarea donatorilor străini și, în unele jurisdicții, sunt deja obligați să respecte regulile de combatere a spălării banilor.¹¹⁷ Dotarea organelor de supraveghere cu o capacitate mai bună de a monitoriza cheltuielile pentru publicitate online este la fel de esențială.¹¹⁸

În mod relevant, relația dintre supravegherea statală și cea nestatală se consolidează reciproc. Atunci când autoritățile publice informează prompt și într-un mod accesibil, societatea civilă poate analiza mai bine cheltuielile raportate în comparație cu propria monitorizare.¹¹⁹ Deși majoritatea țărilor publice astfel de rapoarte (116), mai puține (98) solicită dezvăluirea identităților donatorilor. Această cerință din urmă este un ingredient vital pentru expunerea actorilor străini care încearcă să influențeze alegerile prin finanțarea partidelor sau a candidaților.¹²⁰

Consolidarea societății civile și monitorizării mass-media

Societatea civilă, jurnaliștii și avertizorii de integritate joacă un rol vital în expunerea finanțării politice ilicite, în special atunci când este legată de actori străini maligni care încearcă să influențeze alegerile. Totuși, libertatea și integritatea presei s-au deteriorat în ultimii ani, Institutul Varieties of Democracy raportând o cenzură sporită în 44 de țări în 2024 și amenințări tot mai mari la adresa jurnaliștilor.¹²¹

Tendința este evidentă și în Europa, unde supravegherea digitală, dezinformarea și influența politică asupra mass-media publice au contribuit la acest declin.¹²²

Într-un sens mai larg, actorii societății civile se confruntă cu o serie de provocări, inclusiv acces limitat la informații și resurse, presiune politică și un spațiu civic restrâns. Acești factori le limitează capacitatea de a-și îndeplini eficient rolul de supraveghere.¹²³ Faptul dat subliniază necesitatea atât a unei transparențe robuste din partea autorităților, cât și a unor protecții pentru supravegherea independentă, garanții de acces la informații, măsuri anti-SLAPP (Proces strategic împotriva participării publice), acces echitabil la piețele publicitare de stat și canale securizate pentru accesul cercetătorilor.¹²⁴

Mai mult decât atât, este important de menționat că mass-media poate fi, la rândul ei, o țintă a ingerințelor străine (a se vedea Capitolul 2 despre FIMI și alegeri). În astfel de cazuri, mass media nu numai că pot eșua în rolul de supraveghere a finanțării politice ilicite, ci pot deveni chiar canale pentru dezinformare și informații înșelătoare.¹²⁵

04 Securitatea cibernetică în alegeri

Domeniul digital rămâne un vector critic și extrem de contestat pentru ingerința electorală. Operațiunile cibernetice sunt rareori evenimente izolate; în schimb, ele sunt adesea integrate în campanii mai ample de amenințări hibride, servind frecvent drept principalul factor de facilitare a manipulării informațiilor și a operațiunilor psihologice. Amenințările pot fi clasificate în linii mari în cele care vizează infrastructura electorală de bază și cele care vizează campaniile, partidele și oficialii ce participă la proces.

Perioada de după 2024 a fost marcată de două tendințe transformatoare: convergența operațiunilor sponsorizate de stat cu ecosistemul criminalității cibernetică și apariția inteligenței artificiale ca un puternic multiplicator de forță pentru actorii rău intenționați.¹²⁶ Această convergență a dus la sofisticare și interconectare sporite ale amenințărilor, estompând liniile dintre spionaj, perturbări și criminalitatea orientată spre profit și necesitând astfel consolidarea continuă a rezilienței securității cibernetică.¹²⁷

4.1. PEISAJUL AMENINȚĂRILOR ÎN EVOLUȚIE: CONVERGENȚĂ, COMERCIALIZARE ȘI INTELIGENȚĂ ARTIFICIALĂ

Schimbările la nivel macro din mediul amenințărilor cibernetice definesc provocările actuale la adresa securității alegerilor. Analiza trebuie să depășească un simplu catalog de amenințări pentru a explica dinamica subiacentă care face ca adversarii să fie mai capabili, mai adaptabili și mai dificil de contracarat.

Ecosistemul de criminalitate cibernetică ca serviciu (CaaS): o simbioză strategică

Distincția tradițională dintre Amenințările Persistente Avansate (APT) sponsorizate de stat și infractorii cibernetici motivați financiar se restrânge - deși nu dispare. Timp de mulți ani, au fost exprimate îngrijorări cu privire la utilizarea politică a atacurilor cibernetice asociate criminalității organizate, scandalurile dezvăluind, de exemplu, crearea unor rețele de spionare a jurnaliștilor.¹²⁸ Un studiu recent al Europol evidențiază în continuare estomparea liniilor de demarcație dintre operațiunile sponsorizate de stat și crima organizată, syndicatele criminale fiind valorificate pentru abilitățile și infrastructura lor tehnică.¹²⁹

Acest lucru a dat naștere unei piețe profesionalizate de criminalitate cibernetică ca serviciu (CaaS), care ajută actorii afiliați unor state prin furnizarea de capacități specializate și un nivel plauzibil de negare.¹³⁰ Aceste servicii sunt utilizate tot mai frecvent în campanii motivate geopolitic, permițând actorilor statali să își sporească abilitățile, să efectueze atacuri distructive și să se angajeze în operațiuni informaționale sofisticate.¹³¹

Ce se schimbă de fapt? Convergența reflectă două dinamici suprapuse:¹³²

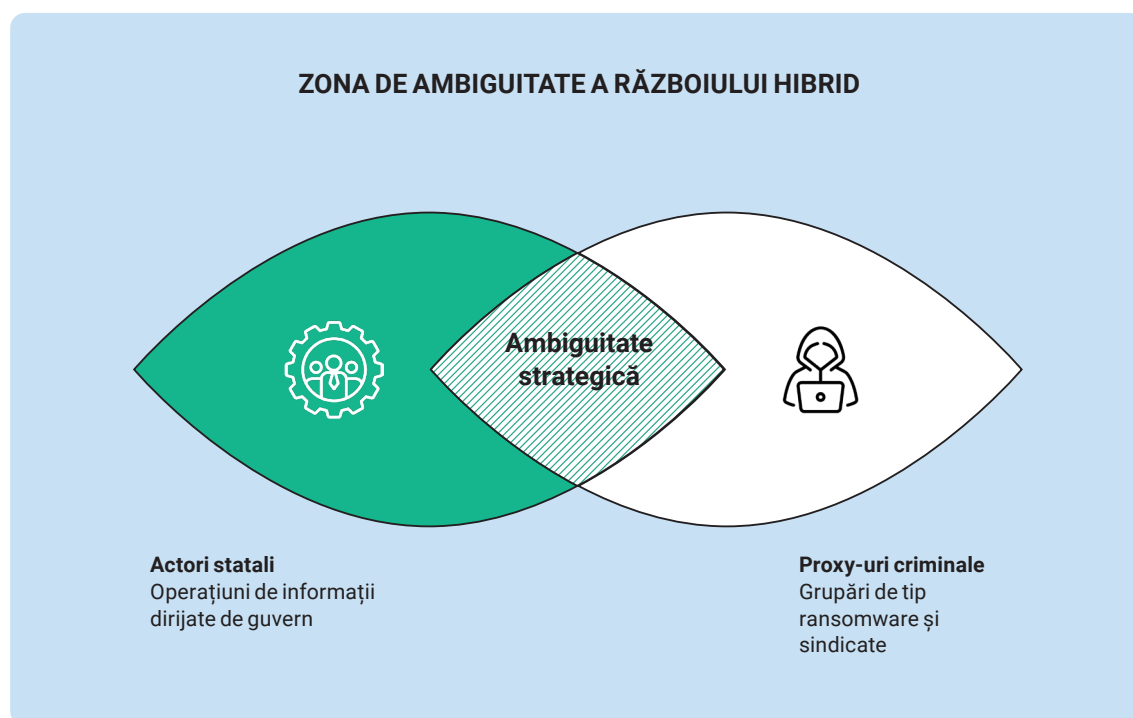
- Externalizare pentru negarea responsabilității: Statele însarcinează, permit sau tolerează operatori infracționali și proxy să creeze straturi suplimentare de separare și să complice atribuirea.
- Difuzarea capacităților prin mecanisme de piață: Ecosistemele criminale oferă acum instrumente adiacente APT de tip „ca serviciu”, reducând costurile și accelerând operațiunile fără a modifica obiectivele strategice de bază ale statelor.

În esență, aceasta nu reprezintă o schimbare doctrinară în intențiile statului, ci mai degrabă o evoluție operațională, care extinde opțiunile pentru o negare plauzibilă și o capacitate rapidă de desfășurare.¹³³

Actorii statali – în special Rusia, China și Iranul – sunt identificați în mod constant ca fiind principalele amenințări externe la adresa infrastructurii critice, inclusiv a sistemelor electorale.¹³⁴ Acum pot valorifica acest ecosistem CaaS într-un mod semnificativ. De exemplu, în iulie și august 2024, în cadrul ciclului electoral din SUA, ReliaQuest – o companie de securitate cibernetică specializată în detectarea amenințărilor și răspunsul la incidente – a investigat o campanie coordonată de phishing care se dădea drept un grup de activiști. E-mailurile îndemnau țintele „să semneze o petiție” și le redirecționau către o infrastructură asociată cu o anumită familie de programe malițioase. Obiectivul era de a atrage utilizatorii să dea clic și, pe site-urile compromise, să declanșeze tehnici drive-by care prezintă în mod obișnuit alerte false de actualizare a browser-ului – instalând în cele din urmă un troian de acces la distanță sau colectând credențialele de acces.¹³⁵ Acest caz ilustrează tehnici operaționale și transferuri tipice ecosistemului, dar nu demonstrează, în sine, o coordonare/direcționare statală.

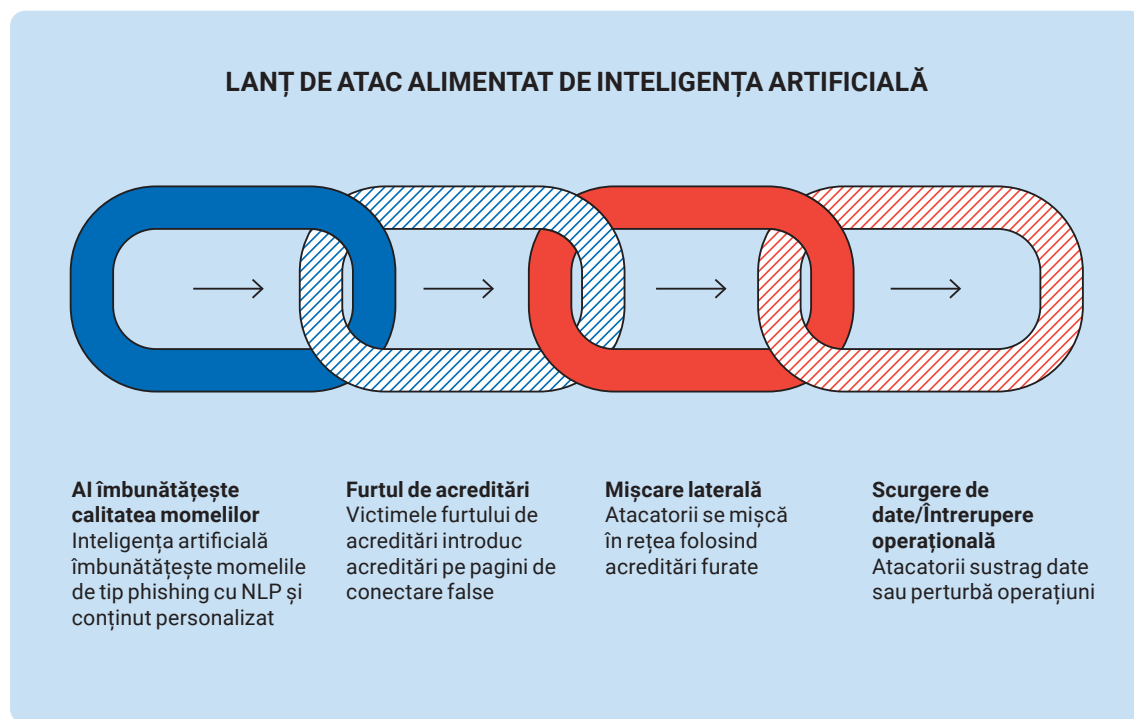
Această simbioză stat - criminalitate constituie o caracteristică deliberată a războiului hibrid modern, concepută pentru a complica descurajarea și atribuirea. Atunci când un actor statal operează prin intermediul unui proxy criminal, se creează ambiguitate strategică. Un atac poate fi lansat de o grupare cunoscută de tip ransomware, dar poate fi direcționat, activat sau tolerat de un serviciu de informații al statului. Această situație poate paraliza cu ușurință mecanismele tradiționale de răspuns. Devine neclar dacă un incident este o chestiune care ține de aplicarea legii pentru a urmări un sindicat criminal sau de agențiile de securitate națională pentru a descuraja un stat ostil. Ambiguitatea creată oferă sponsorului de stat posibilitatea de a nega și încetinește consensul internațional necesar pentru un răspuns coordonat, maximizând astfel impactul perturbator al operațiunii.¹³⁶

Implicația politică este că răspunsurile ar trebui să combine pragurile bazate pe comportament – acționând mai întâi în funcție de prejudiciu și indicatori – cu standarde clare de atribuire și căi legale care să mențină un proces echitabil, permițând în același timp acțiuni defensive în timp util.



Inteligența artificială ca multiplicator de forță malign: utilizări ofensive și defensive

Agencia pentru Securitatea Cibernetică și Infrastructură (CISA) din SUA a evaluat că, pentru perioada 2024-2025, inteligența artificială generativă nu a introdus categorii de risc complet noi, ci le-a amplificat considerabil pe cele existente.¹³⁷ Cu toate acestea, inteligența artificială este utilizată pentru a spori amploarea, viteza și sofisticarea atacurilor de inginerie socială. Aceasta include generarea de e-mailuri de tip phishing mai rafinate, contextuale, producerea de imagini fabricate și videoclipuri deepfake extrem de realiste și crearea de profiluri false pe rețele sociale pentru a sprijini operațiunile de influențare.¹³⁸



Totodată, multe dintre aceleași tehnici de inteligență artificială sunt aplicate în scopuri defensive, cum ar fi detectarea anomaliilor, triajul și liste de așteptare cu clasificare automată pentru phishing, subliniind că tehnologia în sine nu reprezintă principala provocare. În schimb, competiția constă în calitatea adoptării, guvernanta și cursa înarmărilor în continuă evoluție dintre utilizările ofensive și cele defensive.

Un experiment citat pe scară largă, realizat de compania de securitate cibernetică Hoxhunt între 2023 și 2025, a demonstrat în mod empiric această evoluție. La începutul anului 2025, agentul său de phishing bazat pe inteligență artificială a devenit cu 24% mai eficient în înșelarea utilizatorilor decât echipele umane de tip „red team” de nivel înalt, adică specialiști autorizați care imită atacatori reali pentru a identifica punctele slabe.¹³⁹ Deși rezultatele pot varia în funcție de organizație și de nivelul de instruire, acest lucru indică faptul că inteligența artificială poate genera, la scară largă, atacuri eficiente de tip spear-phishing, reducând efectiv barierele în calea capabilităților asociate odinioară cu cei mai avansați adversari.

Studiile de caz din 2024 au demonstrat deja utilizarea înregistrărilor audio și video de tip deepfake în fraude financiare cu miză mare, inclusiv în cadrul unui incident care a defraudat o companie cu 25 de milioane de dolari, ilustrând maturitatea tehnologiei în scopuri înșelătoare, care ar putea fi reutilizată sau adaptată în intenții politice.¹⁴⁰ Cu toate acestea, cazurile izolate de pierderi mari nu ar trebui generalizate excesiv în toate contextele electorale.

Această schimbare tehnologică are implicații profunde pentru securitatea alegerilor, deoarece reduce efectiv bariera de acces pentru efectuarea unor atacuri avansate. Actorii mai puțin calificați pot genera acum conținut de tip spear-phishing personalizat și extrem de persuasiv, care anterior era specific domeniul APT-urilor cu suficiente resurse. Această evoluție crește atât volumul, cât și calitatea generală a amenințărilor. Indicatorii clasici ai e-mailurilor de tip

phishing – cum ar fi gramatica deficitară sau formulele de adresare generice – sunt acum adesea eliminați de inteligența artificială.

Acest lucru face ca apărările centrate pe om, precum instruirea utilizatorilor, să fie necesare, dar mult mai dificile și mai puțin fiabile. Echipile de securitate și lucrătorii electorali din prima linie se confruntă acum cu o provocare și mai mare, deoarece volumul și calitatea potențialelor breșe de securitate cresc probabilitatea de succes a unui atac.

Această situație necesită orientarea strategiei defensive spre controale tehnice stratificate, care se bazează mai puțin pe judecata umană și mai mult pe o infrastructură de tip „zero-trust” – unde fiecare utilizator și dispozitiv sunt verificați în mod continuu – susținută de măsuri tehnice solide de apărare. Acestea includ autentificarea multifactor rezistentă la phishing și accesul cu privilegii minime și condiționat, care acordă utilizatorilor doar accesul minim necesar și numai în anumite condiții.

De asemenea, implică administrarea consimțământului OAuth – adică gestionarea atentă a aplicațiilor externe care se pot conecta la sistemele de bază – precum și izolarea atașamentelor și a linkurilor, ceea ce asigură deschiderea conținutului potențial riscant în medii securizate, izolate. Includerea aplicațiilor în lista de permisiuni este o altă măsură esențială, care permite rularea doar a software-ului aprobat, la fel ca și blocarea macro-comenzilor, care dezactivează codul automat din documente.

Alte măsuri includ conformitatea și atestarea dispozitivelor – asigurându-se că toate dispozitivele conectate îndeplinesc standardele de securitate – precum și administrarea just-in-time, care garantează drepturi de administrator doar pentru scurta perioadă necesară și o separare fizică prudentă a proceselor critice, menținând cele mai sensibile sisteme offline sau în rețele separate. Acolo unde este posibil, aceste controale ar trebui să fie asociate cu o raportare simplificată a incidentelor și protocoale de comunicare clare pentru a limita efectele informațiilor din aval.¹⁴¹

4.2. AMENINȚĂRI LA ADRESA INFRASTRUCTURII ELECTORALE CRITICE (REȚELE, BAZE DE DATE ȘI TEHNOLOGIE DE VOT)

Infrastructura tehnică a alegerilor – care cuprinde totul, de la bazele de date de înregistrare a alegătorilor până la site-urile web oficiale de raportare a rezultatelor – rămâne o țintă cheie pentru actorii rău intenționați. Deși manipularea directă a mașinilor de vot pentru a modifica numărul de voturi este considerată, în general, dificil de realizat la scară largă fără a fi detectată, în special în sistemele cu piste solide de audit pe suport de hârtie, infrastructura aferentă prezintă numeroase vulnerabilități.¹⁴²

O tactică proeminentă observată în ultimii ani este utilizarea atacurilor DDoS. Acestea sunt concepute pentru a suprasolicita cu trafic artificial site-urile web electorale și portalurile de informații pentru alegători, făcându-le inaccesibile. Atacurile de tip ransomware reprezintă o altă amenințare semnificativă. Prin criptarea sistemelor critice și solicitarea de plată pentru deblocarea acestora, aceste atacuri pot provoca perturbări grave.¹⁴³

Încălcări ale sistemelor electorale

Breșele produse în bazele de date electorale reprezintă o amenințare deosebit de insidioasă, deoarece este posibil să nu perturbe serviciile imediat, dar pot eroda încrederea publicului. Orice încălcare, reală sau percepută, poate fi folosită ca armă în campaniile FIMI pentru a submina încrederea publicului în procesul electoral.¹⁴⁴ În 2023, s-a dezvăluit că un actor probabil afiliat unui stat a atacat Comisia Electorală din Regatul Unit, compromițând date ale aproximativ 40 de milioane de alegători. Atacul, atribuit în 2024 unui grup asociat Chinei, a trecut nedetectat timp de mai multe luni. Deși oficialii au declarat că nu a afectat exprimarea sau numărarea voturilor, compromiterea unui registru electoral atât de masiv

subliniază valoarea informațională pe care adversarii o văd în datele electorale.¹⁴⁵

Un caz devenit infam a avut loc în alegerile prezidențiale din Ucraina din 2014. Hackerii ruși s-au infiltrat în rețeaua Comisiei Electorale Centrale și au plasat rezultate false care arătau victoria unui naționalist marginal; deși unitățile de securitate cibernetică ucrainene au neutralizat la timp programul malițios, mass-media de stat rusă a difuzat în continuare victoria fictivă pentru a înșela publicul.¹⁴⁶ Acest incident evidențiază modul în care chiar și un atac cibernetic dejucat poate fi valorificat în războiul informațional pentru a pune la îndoială rezultatele legitime.

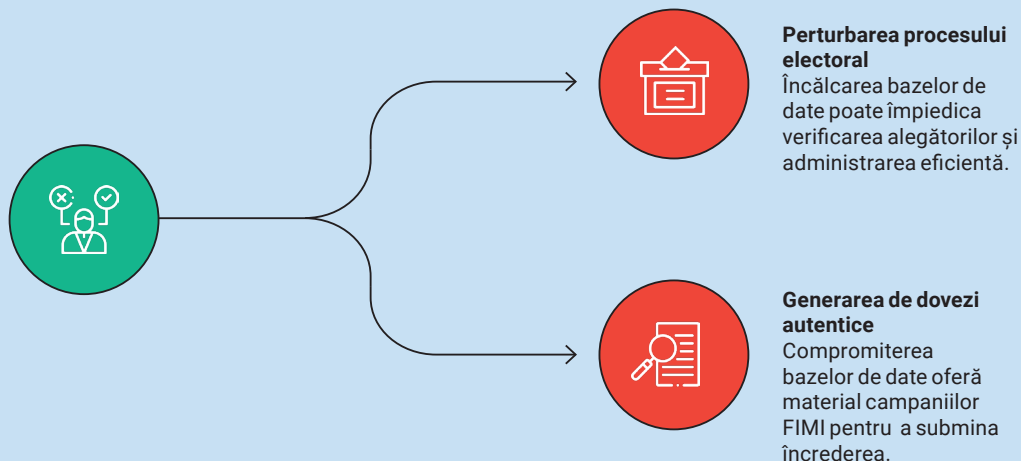
În zone de conflict sau în regiuni ce se confruntă cu tensiuni majore, amenințările cibernetică la adresa infrastructurii însoțesc adesea operațiunile fizice și cele FIMI. Infrastructura electorală a Ucrainei a suferit atacuri repetate din 2014, ca parte a războiului hibrid al Rusiei. Dincolo de episodul din 2014, sistemele IT electorale ale Ucrainei au fost ținte ale unor încercări constante de penetrare; oficialii au raportat valuri de atacuri de tip phishing și malware îndreptate împotriva personalului comisiilor electorale în perioada premergătoare alegerilor din 2019.¹⁴⁷ Începând cu 2022, războiul în desfășurare a amplificat și mai mult îngrijorările: orice alegeri viitoare din Ucraina, suspendate în prezent în temeiul legii marțiale, ar avea loc probabil în contextul unor niveluri extrem de ridicate de amenințări cibernetică, inclusiv cu posibilitatea unor atacuri distructive asupra rețelelor electrice sau a rețelelor de comunicații în timpul votării.¹⁴⁸

Lecția desprinsă din Ucraina și din statele similare din prima linie este că protejarea infrastructurii electorale nu este doar o acțiune tehnică, ci un imperativ de securitate națională, care necesită planificarea rezilienței pentru scenariile cele mai grave, inclusiv în condiții de război.

„Sistemele electorale reprezintă un punct nodal al amenințărilor operaționale și informaționale. Un adversar nu trebuie să schimbe niciun vot pentru a obține o victorie strategică.”

Sistemele electorale reprezintă un punct nodal al amenințărilor operaționale și informaționale. Un adversar nu trebuie să schimbe niciun vot pentru a obține o victorie strategică. Prin penetrarea cu succes a unei baze de date de alegători, un atacator poate atinge două obiective simultan. În primul rând, acesta perturbă procesul electoral prin împiedicarea capacității oficialilor de a verifica alegătorii și de a administra procesul eficient. În al doilea rând, și mai important, acesta generează „dovezi” puternice și autentice care pot fi folosite pentru a alimenta campanii FIMI menite să submineze încrederea în legitimitatea alegerilor. Acest lucru face ca aceste baze de date să fie, fără îndoială, cea mai valoroasă țintă pentru un actor de amenințare hibridă, deoarece compromiterea lor servește mai multor obiective strategice simultan.

EFFECTELE ÎNCĂLCĂRILOR SISTEMELOR ELECTORALE



Vulnerabilitatea persistentă a bazelor de date de înregistrare a alegătorilor

Sistemele de înregistrare a alegătorilor reprezintă o țintă principală pentru atacurile cibernetice și breșele de securitate. Atacurile de tip ransomware au avut un impact direct asupra administrației electorale, vizând aceste sisteme. Un incident din 2024 în Statele Unite a forțat un comitat să întrerupă conexiunea la sistemul de stat de înregistrare a alegătorilor ca măsură de precauție.¹⁴⁹ În mod similar, la sfârșitul anului 2024, un atac de tip ransomware legat de Rusia asupra Biroului Grefierului din comitatul Jefferson, Kentucky, deși nu a compromis sistemul de vot în sine, a perturbat operațiunile și a evidențiat vulnerabilitatea sistemelor guvernamentale interconectate.¹⁵⁰

Bazele de date de înregistrare a alegătorilor stabilesc cine poate vota și unde. Dacă atacatorii le fac indisponibile – prin ransomware sau denial-of-service – sau modifică pe ascuns înregistrări, cum ar fi adresele sau datele de identificare, consecințele probabile includ cozi mai lungi, utilizare mai largă a buletinelor de vot provizorii, sosirea alegătorilor la secția de votare greșită și probleme de eligibilitate – chiar dacă numărarea voturilor în sine nu este afectată.

Stimulentele pentru atacatori sunt triple: disponibilitate, adică perturbări cibernetice care blochează înregistrarea alegătorilor sau întrerup sincronizarea registrului electronic de votare (actualizarea în timp real a listelor de alegători în secțiile de votare și în sistemele centrale); integritate, care implică editarea sau ștergerea înregistrărilor pentru a crea fricțiuni sau priver selectivă de dreptul de vot; și confidențialitate, prin furtul de date cu caracter personal în scopul intimidării sau al pirateriei electronice. Datele de autentificare furate pot fi folosite și pentru infiltrarea în alte sisteme electorale.

Furtul datelor alegătorilor constituie o problemă omniprezentă. Datele scurse din statele americane reprezintă aproximativ 78% din totalul datelor alegătorilor care circulă pe dark web, cel puțin 23 de state suferind breșe de securitate. Aceste informații expuse sunt apoi folosite ca armă pentru dezinformare ținută, tactici de suprimare a votului și manipulare a identității, cu potențialul de a trimite mesaje înșelătoare despre secțiile de votare sau chiar de a întreprinde tentative de vot fraudulos.¹⁵¹

Dubla amenințare a atacurilor de tip ransomware și DDoS

Atacurile DDoS continuă să fie o tactică comună pentru perturbarea accesului la site-urile

web legate de alegeri, inclusiv la portalurile de informații ale alegătorilor și site-urile de raportare a rezultatelor.¹⁵² Ciclul electoral din SUA din 2024 a înregistrat o creștere semnificativă a unor astfel de atacuri care au vizat site-urile web ale campaniilor, partidele politice și infrastructura la nivel de comitat. Compania de securitate cibernetică Cloudflare a raportat blocarea a peste 6 miliarde de cereri rău intenționate, care au vizat infrastructura alegerilor din SUA numai în primele șase zile ale lunii noiembrie 2024, unele atacuri ajungând la 700.000 de cereri pe secundă.¹⁵³ Campanii DDoS similare, motivate politic, au fost observate în timpul alegerilor pentru Parlamentul European din 2024, site-urile web ale partidelor politice olandeze fiind scoase din funcțiune.¹⁵⁴

Scopul strategic al acestor atacuri se extinde adesea dincolo de perturbările tehnice. După cum au remarcat public CISA și Biroul Federal de Investigații al SUA, deși este puțin probabil ca atacurile DDoS să împiedice vreun alegător eligibil să voteze, ele pot împiedica în mod eficient accesul publicului la informațiile oficiale și pot crea o percepție de haos și incompetență.¹⁵⁵ Această percepție devine mai apoi un teren fertil pentru exploatare de către campaniile de dezinformare, care pot amplifica incidentul pentru a submina încrederea publicului în integritatea generală a alegerilor și, prin extensie, în principiile, valorile și procesele democratice.¹⁵⁶

În mod similar, atacurile de tip ransomware asupra administrațiilor locale, chiar dacă nu vizează birourile electorale în mod direct, pot provoca daune colaterale serioase. O creștere a incidentelor de tip ransomware ce aveau ca țintă administrații statale, regionale, tribale și teritoriale a fost raportată în al doilea trimestru al anului 2024. Aceste atacuri pot perturba funcționarii electorali care se bazează pe infrastructura IT comună a comitatului.¹⁵⁷ Incidentele nu sunt doar probleme tehnice; sunt instrumente ale activităților de influențare a informațiilor. Ținta lor principală este percepția publică, mai degrabă decât un server.

Succesul adversarului nu se măsoară în servere scoase din funcțiune, ci în articole de știri scrise și în postări pe rețele sociale, care prezintă narațiuni despre „alegeri piratate”. Acest lucru face ca răspunsul de comunicare strategică la un astfel de incident să fie la fel de important ca cel tehnic.

Compromiterea lanțului de aprovizionare cu tehnologie electorală

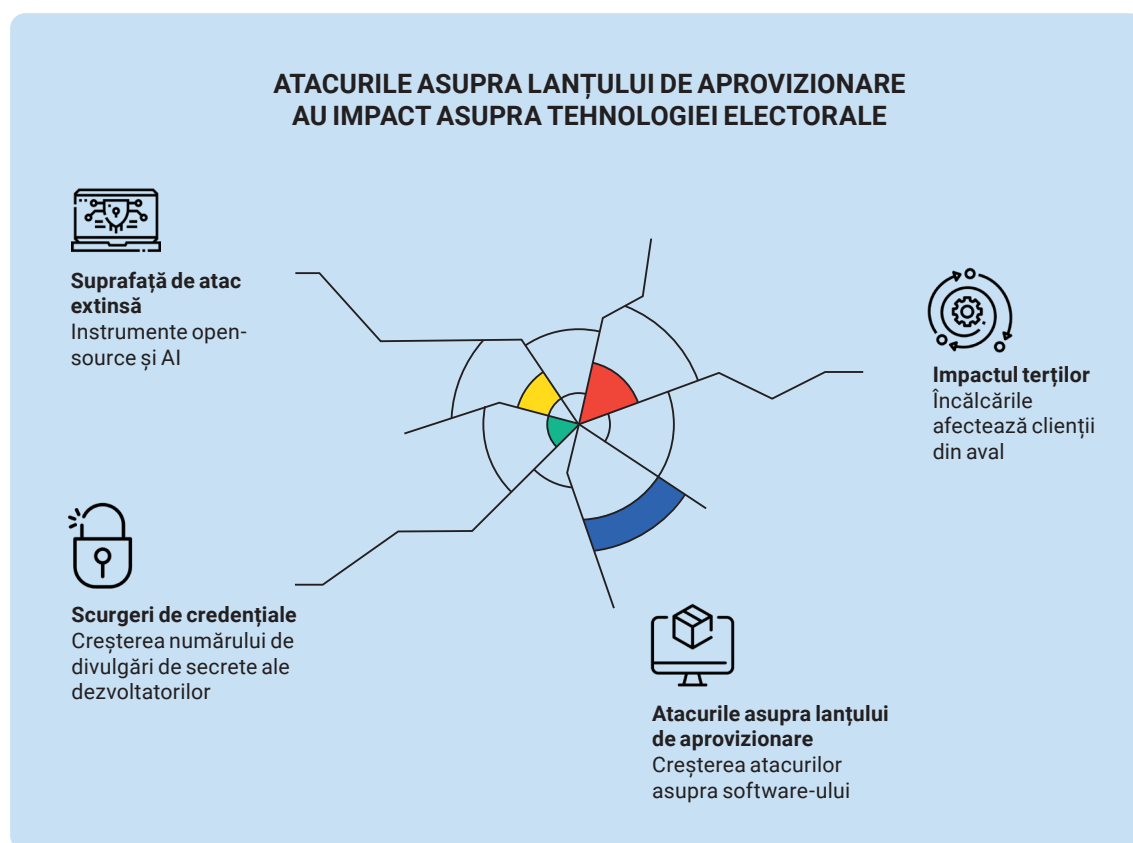
Securitatea tehnologiei electorale depinde în mare măsură de un lanț complex de aprovizionare cu software, care a devenit o țintă principală pentru adversari sofisticăți.¹⁵⁸ În acest context, frecvența atacurilor asupra lanțului de aprovizionare cu software s-a amplificat în continuare, cu o creștere de 25% a incidentelor de la sfârșitul anului 2024 până la mijlocul anului 2025.¹⁵⁹

Natura acestor amenințări a evoluat semnificativ. Dincolo de inserarea clasică de cod malițios în actualizările de software sau „alterarea pachetelor”, un raport din 2025 a evidențiat o tendință mai insidioasă: o creștere cu 12% a expunerilor de secrete ale dezvoltatorilor – parole integrate în codul sursă, token-uri și chei API utilizate pentru autentificarea între servicii – găsite încorporate în produse comerciale.¹⁶⁰ Luate în ansamblu, aceste modele indică faptul că adversarii vizează întregul ciclu de viață al dezvoltării de software, nu doar produsul final. În același timp, utilizarea pe scară largă a software-ului open-source și creșterea rolului instrumentelor de dezvoltare AI au extins suprafețele complexe de atac care pot fi exploatare.¹⁶¹

Breșele de securitate de mare anvergură la principalii furnizori de software și servicii demonstrează impactul în cascadă asupra terților al unei singure compromiteri a lanțului de aprovizionare, afectând mii de clienți din aval.¹⁶² Acestea servesc drept avertisment pentru sectorul tehnologiei electorale, care se bazează pe componente și servicii similare ale terților. Pentru sistemele electorale, aceasta înseamnă că riscurile se propagă prin intermediul unor furnizori și componente comune. Amenințarea a trecut de la simpla „infectare a produsului” la „compromiterea sistematică a procesului”. Prin furtul credențialelor dezvoltatorului sau exploatarea unui design nesigur, un adversar poate obține acces persistent și multiple căi pentru exploatare ulterioară.

„Amenințarea a trecut de la simpla «infectare a produsului» la «compromiterea sistematică a procesului».”

Cu alte cuvinte, acesta este un compromis strategic, pe termen lung, care reprezintă o povară considerabilă pentru funcționarii electorali în timpul procesului de achiziții. Aceștia nu se mai pot baza exclusiv pe certificările deținute de un furnizor, ci trebuie să evalueze și măsura în care acesta aplică principii de dezvoltare securizată din proiectare. Prin urmare, o vulnerabilitate critică poate să nu rezide în codul specific electoral, ci în biblioteca terță de care depinde, ceea ce face ca detectarea și remedierea să fie mult mai dificile.



4.3. ATACURI CIBERNETICE CARE VIZEAZĂ CAMPANII, PARTIDE ȘI FUNCȚIONARI ELECTORALI

Campaniile politice, partidele și oficialii sunt ținte principale pentru atacurile cibernetice care vizează influențarea alegerilor.¹⁶³ Cea mai eficientă tactică este operațiunea „hack-and-leak”, în care materialele furate, cum ar fi e-mailurile și documentele, sunt publicate strategic în mediul online pentru a alimenta dezinformarea și a provoca daune politice maxime.¹⁶⁴ Acest model operațional a fost folosit în mod repetat, de la operațiunile Rusiei în contextul alegerilor din SUA din 2016 și Franța din 2017 până la compromiterea unei campanii prezidențiale americane din 2024 de către hackeri asociați Iranului. Aceste atacuri sunt adesea inițiate prin campanii de spear-phishing, ce implică e-mailuri extrem de personalizate, concepute pentru a păcăli indivizii să își divulge credențialele de acces sau alte informații sensibile.¹⁶⁵

O amenințare emergentă este clonarea vocii bazată pe inteligență artificială, cunoscută și sub

numele de „vishing”, în care un adversar folosește inteligența artificială pentru a imita prin telefon vocea unei persoane de încredere – o tactică despre care CISA avertizează că ar putea fi folosită pentru a imita înalți funcționari electorali.¹⁶⁶

Funcționarii electorali se confruntă, totodată, cu o serie de amenințări, inclusiv phishing și doxing (publicarea rău intenționată a informațiilor personale), atât din partea unor actori străini, cât și a celor interni care încearcă să-i intimideze sau să le fure credențialele.¹⁶⁷ Aceste instrumente au fost folosite în mod disproporționat ca arme împotriva femeilor din politică și jurnalism prin hărțuire și crearea de materiale pornografice de tip „deepfake” realizate fără consimțământul victimelor.¹⁶⁸

Această evoluție implică faptul că, în campaniile electorale, partidele și oficialii ar trebui să plece de la premisa că pot fi ținte constante pe parcursul ciclului electoral, anticipând furtul de credențiale și tentativele de tip hack-and-leak. În cazul în care informațiile indică o scurgere iminentă de date, atribuirea preventivă măsurată poate atenua impactul. Având în vedere că inteligența artificială îmbunătățește calitatea ademenirii și permite imitarea vocii, agențiile guvernamentale ar trebui să interzică aprobările exclusiv vocale și să solicite verificarea prin apel telefonic sau pe un al doilea canal. Mai mult decât atât, este nevoie de a proteja persoanele și sistemele, pentru a oferi căi legale de sprijin femeilor care se confruntă cu deepfake-uri bazate pe gen precum și de a proteja oficialii de expunerea informațiilor personale și a hărțuirii.¹⁶⁹

4.4. CE SE POATE FACE? CELE MAI BUNE PRACTICI PENTRU REZILIENȚA SECURITĂȚII CIBERNETICE ELECTORALE

O apărare eficientă împotriva amenințărilor cibernetice și informaționale moderne necesită o abordare continuă, adaptivă și colaborativă.¹⁷⁰ S-a conturat un consens larg în jurul unui set de bune practici, care constituie nucleul rezilienței securității cibernetice electorale.¹⁷¹ În ansamblu, acestea transformă reziliența tehnică în legitimitate electorală. Principiile de guvernare și securitate din proiectare reduc ratele de eroare și elimină punctele unice de eșec, operațiunile proactive și răspunsul exersat minimizează timpul de staționare al atacatorului în sistem și vizibilitatea perturbărilor, eliminând astfel lacunele informaționale, iar parteneriatele cu caracter permanent permit o comunicare credibilă între diferite agenții și o verificare independentă.

Rezultatul este continuitatea serviciilor – asigurarea faptului că oamenii pot vota – combinată cu dovezi de integritate, ceea ce înseamnă că rezultatele sunt verificabile, și cu o explicație demnă de încredere, asigurând că publicul înțelege ce s-a întâmplat și de ce. Aceste trei condiții susțin atât legitimitatea percepută, cât și cea reală a alegerilor.

Guvernanță și tehnologie fundamentale

Reziliența începe cu o evaluare cuprinzătoare a riscurilor întregului ecosistem electoral, de la înregistrarea alegătorilor până la raportarea rezultatelor.¹⁷² Bazându-se pe acest fundament, autoritățile electorale ar trebui să adopte tehnologii care sunt securizate din proiectare, solicitând furnizorilor să integreze securitatea pe tot parcursul ciclului de viață al dezvoltării software-ului.¹⁷³ În practică, acest lucru implică din ce în ce mai mult implementarea unei arhitecturi Zero Trust, care elimină încrederea implicită și verifică continuu fiecare utilizator, dispozitiv și sarcină de lucru conectată la sistemele critice.¹⁷⁴ Aceste opțiuni de bază reduc punctele unice de eșec și fac controalele ulterioare mai eficiente.

Operațiuni și răspuns proactive

Abordarea defensivă trebuie să fie proactivă. Aceasta înseamnă consolidarea continuă a sistemelor prin controale tehnice, cum ar fi autentificarea multifactorială și segmentarea rețelei, monitorizarea amenințărilor prin detectarea intruziunilor și căutarea activă a programelor malware preinstalate cu mult înainte de alegeri.¹⁷⁵

La fel de important este să existe planuri de răspuns la incidente bine exersate, care să integreze izolarea tehnică cu o comunicare strategică, prevenind escaladarea problemelor operaționale în crize de legitimitate.¹⁷⁶ Această disciplină operațională transformă reziliența tehnică în încredere publică.

Parteneriate susținute

În cele din urmă, o apărare eficientă este imposibilă în mod izolat. Reziliența depinde de parteneriate cu caracter permanent și de stabilirea unor rețele robuste de cooperare electorală. Aceste structuri formalizează colaborarea dintre autoritățile de management electoral agențiile de securitate cibernetică, serviciile de informații și organele de aplicare a legii, creând conștientizarea comună necesară pentru un răspuns rapid și coordonat la amenințările emergente.¹⁷⁷ Prin conectarea guvernării, operațiunilor și parteneriatelor, autoritățile pot detecta mai devreme, pot răspunde mai rapid și pot comunica mai credibil - consolidând astfel atât legitimitatea percepută, cât și cea reală a alegerilor.

05 *Contracacarea amenințărilor hibride la adresa alegerilor: argumente pentru crearea unor rețele de cooperare electorală*

Caracterul multi-domeniu și cu actori multipli al amenințărilor hibride face ca măsurile de securitate tradiționale, aplicate în mod izolat, să fie insuficiente. Adversarii exploatează în mod deliberat suprapunerile în responsabilitățile agențiilor – de exemplu, în timpul alegerilor – atacând simultan infrastructura cibernetică, mediul informațional și securitatea fizică. O autoritate de management electoral poate fi pregătită pentru provocări logistice, o agenție de securitate cibernetică pentru intruziuni în rețea și o agenție de aplicare a legii pentru amenințări la securitatea fizică, dar niciuna nu este echipată individual pentru a gestiona un atac sincronizat care le combină pe toate trei.¹⁷⁸ Actorii malițioși înțeleg aceste diviziuni instituționale și își proiectează operațiunile pentru a le exploata, creând o provocare strategică ce poate fi abordată doar cu o apărare la fel de integrată și interconectată.¹⁷⁹ Prin urmare, o apărare eficientă necesită o schimbare fundamentală spre stabilirea unor rețele robuste și permanente de cooperare electorală, atât la nivel național, cât și internațional.¹⁸⁰

Aceste rețele sunt esențiale pentru instituționalizarea colaborării, depășind gestionarea ad-hoc a crizelor pentru a construi o postură defensivă proactivă și rezilientă. Scopul principal al acestor rețele este de a dezvolta o imagine operațională comună între toți actorii cheie, facilitând detectarea și răspunsul rapid și coordonat la amenințările emergente. Cadrul cuprinzător pentru combaterea amenințărilor hibride la adresa alegerilor, elaborat de Centrul European de Excelență pentru Contracacarea Amenințărilor Hibride, identifică funcțiile cheie pe care aceste rețele ar trebui să se concentreze, inclusiv actualizarea legislației, efectuarea de evaluări ale vulnerabilității, creșterea rezilienței, îmbunătățirea comunicării, desfășurarea de exerciții comune și consolidarea capacităților de detectare și răspuns.¹⁸¹

Această abordare proactivă în rețea este aliniată cu orientările oficiale de la nivel european. Comisia Europeană a recomandat în mod explicit statelor membre ale UE să înființeze rețele naționale de cooperare electorală, recunoscându-le drept platforme vitale pentru ca autoritățile electorale să colaboreze cu alte entități cheie de securitate. O astfel de cooperare, după cum notează Comisia, este esențială pentru detectarea promptă a amenințărilor și aplicarea eficientă a normelor.¹⁸²

O lecție crucială din eforturile recente de protejare a alegerilor este că nicio cooperare nu poate fi improvizată în timpul unei crize. Relațiile, încrederea și protocoalele pentru schimb de informații trebuie stabilite și exersate cu mult timp înainte, deoarece eforturile ad-hoc reunite sub presiune sunt adesea ineficiente. Prin urmare, instituționalizarea rețelelor de cooperare

permanente și formale nu este doar o practică optimă, ci o condiție prealabilă fundamentală pentru dezvoltarea rezilienței necesare pentru a face față presiunii cronice a amenințărilor hibride moderne.¹⁸³

5.1. ARHITECTURI DE COLABORARE NAȚIONALĂ

Deși principiul apărării cooperative este larg acceptat, nu există un model universal valabil pentru o rețea de cooperare electorală. Structurile naționale sunt modelate de guvernanta unică a unei țări și de percepțiile acesteia asupra amenințărilor cu care se confruntă.

Exemplele de mai jos rezumă mecanismele de bază și domeniul de aplicare al fiecărui model.

- În **Suedia** guvernarea descentralizată și cultura axată pe consens produc o rețea cu mai multe niveluri, bazată pe un model de colaborare. La nivel național, Autoritatea Electorală Suedeză prezidează o rețea națională de cooperare electorală, completată de rețele regionale și locale.¹⁸⁴ Printre caracteristicile practice se numără grupuri permanente de schimb de informații, exerciții comune de rutină și o delimitare clară a rolurilor între îndrumare la nivel național și execuție la nivel municipal.
- În **Statele Unite ale Americii**, structura puternic federalizată necesită un model descentralizat, în care agențiile federale se coordonează cu 50 de sisteme electorale de stat, gestionate în mod independent. Coordonarea se realizează prin mecanisme voluntare – cum ar fi Centrul de Partajare și Analiză a Informațiilor privind Infrastructura Electorală, manuale comune și sprijin pentru răspunsul la incidente – mai degrabă decât printr-o dirijare centralizată.¹⁸⁵
- În **Franța**, tradiția etatistă a dat naștere unui organ statal dedicat, cu autoritatea de a identifica public ingerințele străine. Acest organ, Viginum (Service de vigilance et de protection contre les ingérences numériques étrangères), materializează un model centralizat, care prioritizează autoritatea de investigare, avizele publice rapide și atribuirea de sarcini la nivel de stat departamentelor operaționale.¹⁸⁶
- **Canada** a dezvoltat un model axat pe informații, care este atent separat de sfera politică imediată.¹⁸⁷ Acest model este centrat pe Grupul operativ pentru amenințări la adresa securității electorale și a informațiilor, care efectuează o evaluare integrată a amenințărilor, și pe Grupul de protocol public pentru incidente electorale critice, care gestionează comunicarea publică bazată pe praguri. Elections Canada nu este membru nici al Grupului operativ, nici al Grupului de protocol; rămâne independent, dar se coordonează cu agențiile de securitate și primește informații.¹⁸⁸

Exemplele date arată că, deși funcțiile de bază ale cooperării sunt universale, forma instituțională trebuie adaptată contextului național. Dincolo de structurile lor specifice, rețelele eficiente de cooperare electorală au în comun un set de funcții operaționale de bază și bune practici, care sunt esențiale pentru succes. Aceste practici îi permit unei țări să-și schimbe abordarea defensivă, de la una de tip reactivă, determinată de evenimente, la una proactivă și continuă. O analiză a diferitor modele naționale relevă un ghid standard de acțiuni pe care aceste rețele trebuie să le întreprindă ca să fie eficiente.

Stabilirea unei imagini operaționale comune: Conceptul de celulă de fuziune

O practică fundamentală pentru o cooperare eficientă este înființarea unei „celule de fuziune”. Acest concept implică reunirea, în același spațiu, a analiștilor și ofițerilor de legătură din toate agențiile participante, fie fizic, fie virtual, pentru a permite schimbul de informații în timp real și a promova o înțelegere comună a mediului de amenințări.¹⁸⁹ Prin eliminarea compartimentării informaționale, celulele de fuziune formate din diverși experți – de la respondenți cibernetici la analiști de informații și comunicatori strategici – pot sintetiza

fluxuri multiple de amenințări într-o singură „imagine operațională comună” coerentă.

Pentru a echilibra integrarea analitică cu autonomia instituțională, celulele de fuziune ar trebui să funcționeze pe principiul „analizăm împreună, acționăm în cadrul mandatului”: analiza este partajată, în timp ce deciziile operaționale și autoritățile rămân în cadrul fiecărei instituții. Această conștientizare comună reprezintă fundamentul unui răspuns coordonat și poate fi concepută cu respectarea independenței operaționale a Organelor de Gestionare a Alegerilor.¹⁹⁰

În practică, echilibrul este menținut printr-o partajare a datelor limitată scopului și acces bazat pe roluri, memorandumuri de înțelegere formalizate, separare strictă între activitățile de analiză și operațiuni, precum și prin jurnale de partajare auditabile. Soluția constă în modul de proiectare, nu în distanță: celulele de fuziune ar trebui să rămână strict analitice, cu un schimb de informații limitat scopului, care să mențină deciziile operaționale în cadrul mandatului fiecărei instituții, asigurându-se că organismele de management electoral își păstrează autoritatea exclusivă asupra proceselor electorale.

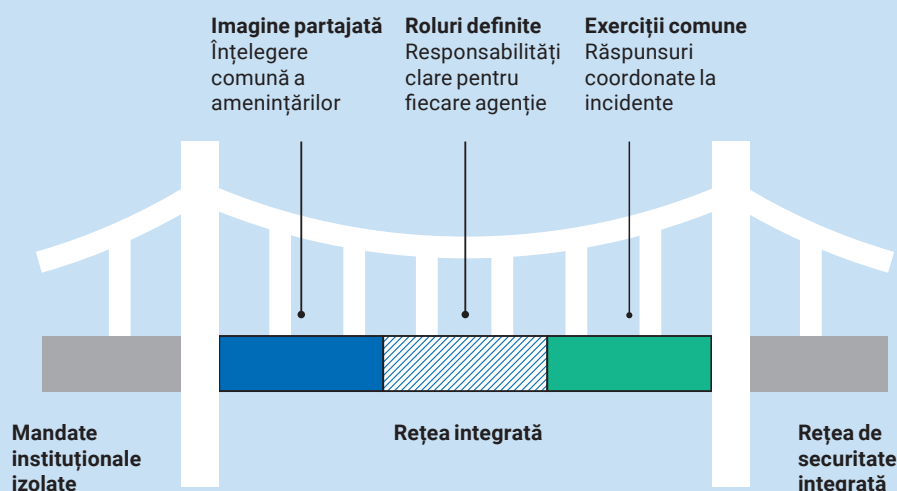
Atunci când sunt implementate în acest mod, celulele de fuziune oferă rezultate tangibile, inclusiv detectarea și trierea mai rapidă a amenințărilor („timpul de detectare”), reducerea duplicării eforturilor între agenții, precum și o încredere și o coerență sporite ale mesajelor în răspunsurile comune.

Muncă proactivă și continuă între ciclurile electorale

Rețelele eficiente funcționează continuu, nu doar în lunile premergătoare votului. Printre activitățile proactive cheie se numără:

- **Evaluări comune ale riscurilor și vulnerabilităților:** Cartografierea regulată și sistematică a ecosistemului electoral pentru a identifica și prioritiza riscurile înainte ca acestea să poată fi exploatate.¹⁹¹
- **Planificare bazată pe scenarii și exerciții comune:** Efectuarea în mod regulat de exerciții practice și funcționale pentru a testa planurile de răspuns, a identifica lacunele de coordonare și a dezvolta „memoria musculară” instituțională.¹⁹² Exercițiile comune de securitate cibernetică ale UE înainte de alegerile parlamentare sunt un exemplu cheie.¹⁹³
- **Protocoale formalizate pentru schimbul de informații și răspuns:** Stabilirea unor protocoale clare, convenite în prealabil, ce guvernează modul în care amenințările sunt raportate, evaluate și abordate. Acest lucru evită improvizația în timpul unei crize și ajută la depolitizarea procesului decizional.¹⁹⁴

REDUCEREA LACUNELOR DINTRE INSTITUȚII PENTRU O SECURITATE ÎMBUNĂTĂȚITĂ



5.2. REȚEA DE REȚELE

Într-un mediu informațional globalizat, apărarea pur națională este insuficientă, necesitând o „rețea de rețele”, care să conecteze organele naționale la cadre internaționale robuste.

UE are cel mai sofisticat ecosistem regional. Rețeaua Europeană de cooperare privind alegerile servește drept centru principal pentru autoritățile naționale, ce permite schimbul de bune practici în toate domeniile, de la securitatea cibernetică la combaterea dezinformării.¹⁹⁵ Aceasta este conectată la rețele specializate, cum ar fi Sistemul de alertă rapidă pentru amenințările FIMI, și este susținută de un mecanism comun pentru reziliență electorală, care poate desfășura echipe de experți în statele membre. Acest sistem integrat a fost considerat esențial pentru asigurarea desfășurării fără probleme a alegerilor pentru Parlamentul European din 2024.¹⁹⁶

O cooperare mai amplă are loc prin intermediul Organizației Tratatului Atlanticului de Nord (NATO), care identifică amenințările hibride drept o provocare centrală de securitate și lucrează pentru îmbunătățirea schimbului de informații între aliați, și prin Mecanismul de răspuns rapid al G7, care coordonează răspunsurile la dezinformarea sponsorizată de state străine.¹⁹⁷ La nivel global, organizațiile interguvernamentale precum Institutul Internațional pentru Democrație și Asistență Electorală joacă un rol cheie în crearea normelor și promovarea unei comunități de practică prin inițiative precum Rețeaua globală pentru asigurarea integrității electorale.¹⁹⁸

5.3. PROVOCĂRI ÎN CALEA COOPERĂRII EFICIENTE

În ciuda progreselor semnificative înregistrate în stabilirea mecanismelor de apărare cooperativă, eficacitatea și viabilitatea acestora pe termen lung se confruntă cu provocări profunde și persistente. În practică, printre acestea se numără fluctuațiile și polarizarea politică, deficitul de finanțare, instabilitatea legislativă și disfuncționalitățile curente în ceea ce privește schimbul de date și coordonarea.

Un paradox cheie al persistenței amenințărilor hibride constă în faptul că mecanismele construite pentru a contracara presiunile informaționale, cibernetice și financiare coordonate pot deveni ele însele ținte – vulnerabile la delegitimare, polarizare și atacuri de ordin legal sau bugetar inițiate de FIMI din partea acelorași actori cărora sunt menite să le reziste. Simplu spus, balustradele pe care le construim pot fi slăbite chiar de forțele pe care sunt menite să le rețină.

Aceste obstacole – care acoperă domeniile politic, financiar și operațional – amenință să erodeze chiar structurile create pentru a proteja procesele democratice. Depășirea lor este esențială pentru dezvoltarea unei reziliențe durabile, mai degrabă decât episodice.

„Calea către o reziliență durabilă necesită nu doar crearea acestor rețele, ci și un efort societal mai amplu pentru a depolitiza securitatea alegerilor și a o integra ca pe un interes național fundamental, nenegociabil.”

Prin urmare, durabilitatea pe termen lung depinde de izolarea instituțională practică – mandate clare, susținere între partide și bugete protejate – combinată cu un sprijin politic larg, care să dureze mai mult decât orice guvern individual. Calea către o reziliență durabilă necesită nu doar crearea acestor rețele, ci și un efort societal mai amplu pentru a depolitiza securitatea alegerilor și a o integra ca pe un interes național fundamental, nenegociabil. Aceasta ar trebui să fie ancorată într-un contract social comun și în încrederea publică și operaționalizată, printr-o abordare la nivelul întregii societăți.

06 Concluzii și recomandări

Perioada din 2024 până în prezent a confirmat că amenințările hibride reprezintă o provocare persistentă, adaptivă și din ce în ce mai sofisticată la adresa integrității electorale la nivel mondial. Analiza cazurilor recente de atacuri hibride ce vizează alegerile subliniază evoluția acestor amenințări – de la interferențe episodice la o formă cronică și sistemică de conflict care funcționează acum ca o campanie cu spectru complet. Aceste campanii combină FIMI, operațiunile cibernetice, finanțarea politică ilicită, folosirea legii ca armă și presiunea offline, coordonate între actori statali, proxy și infracționali și programate pentru a exploata breșele instituționale pe tot parcursul ciclului electoral.

Analiza evenimentelor recente subliniază câteva constatări cheie:

- **Trecerea la un conflict cronic:** Ingerința electorală a trecut de la incidente ocazionale la un conflict informațional continuu. Actorii statali rău intenționați lucrează în mod constant pentru a submina sistemele democratice prin erodarea încrederii publice, alimentarea polarizării și slăbirea instituțiilor.¹⁹⁹
- **Operațiuni la scară industrială și tehnologii noi:** Adversarii operează acum la scară industrială, valorificând rețele de propagandă sofisticate, controlate în mod centralizat.²⁰⁰ Transformarea în armă a inteligenței artificiale a devenit un multiplicator de forță semnificativ, permițând crearea rapidă și la costuri reduse de medii sintetice și de dezinformări hiperrealiste, crescând dramatic atât volumul, cât și calitatea amenințărilor.²⁰¹
- **Integrarea vectorilor de amenințare:** Operațiunile hibride derulate cu succes se bazează rareori pe o singură metodă. În schimb, acestea integrează manipularea informațiilor, finanțarea politică ilicită și atacurile cibernetice perturbatoare în campanii coerente. Fondurile ilicite – adesea canalizate prin criptomonede și terțe părți – susțin activități de influențare a informațiilor și cumpărarea de voturi. În același timp, atacurile cibernetice sunt folosite pentru a fura date pentru operațiuni de tip „hack-and-leak” și a perturba procesele electorale, semănând confuzie și neîncredere.²⁰²
- **Detectarea, atribuirea și responsabilitatea reprezintă blocaje în continuare:** Utilizarea proxy-urilor, spălarea informațiilor și accesul fragmentat la date împiedică răspunsurile prompte și proporționale. Între timp, transparența inconsecventă a platformelor limitează supravegherea externă. Progresele în ceea ce privește standardele deschise pentru proveniență și accesul cercetătorilor la date ar trebui să fie însoțite de controale auditabile ale tehnologiei publicitare și de o verificare eficientă a conformității cu sancțiunile.²⁰³

6.1. RECOMANDĂRI

Aceste constatări subliniază necesitatea construirii și consolidării apărării în rețea. Întrucât adversarii exploatează în mod deliberat fisurile dintre mandatele instituționale, răspunsurile tradiționale izolate de securitate nu mai sunt suficiente.

Următoarele recomandări se adresează părților interesate responsabile de protejarea proceselor democratice. Acestea sunt organizate în jurul a patru acțiuni principale, care vizează promovarea unei reziliențe naționale și internaționale durabile.

1. **Consolidarea capacității interne a agenției:** Fiecare instituție trebuie să își asume responsabilitatea pentru propria apărare, susținută de mandate clare și proceduri profesionale.

Aceasta începe cu responsabilități explicite atribuite pentru cartografierea riscurilor, coordonarea răspunsului la incident, comunicarea publică și gestionarea furnizorilor, toate documentate în planuri practice și ușor de utilizat. Planurile în cauză ar trebui integrate în practica zilnică prin exerciții regulate ce simulează scenarii de amenințări hibride, inclusiv un manual de răspuns la scurgeri de informații, care să fie exersat, cu mesaje pre-aprobate și eforturi de remediere post-exercițiu urmărite până la finalizare.

Tehnologia și procedurile ar trebui să respecte principiile securității prin proiectare – acces cu privilegii minime, verificare continuă a utilizatorilor și dispozitivelor, precum și copii de rezervă offline pentru operațiunile critice – pentru a asigura continuitatea în condiții de stres. Standardele de achiziții ar trebui să impună dovezi ale unor practici de dezvoltare securizate, raportare promptă a incidentelor și transparența componentelor terțe pentru a evita punctele unice de eșec.

Indicatorii de progres includ detectarea și limitarea mai rapidă a incidentelor, actualizări publice prompte și transparente, precum și mecanisme de audit cuprinzătoare, care contribuie la clarificarea incidentelor fără a dezvălui informații sensibile.

2. **Promovarea unui ecosistem național de sprijin:** Capacitatea internă trebuie consolidată printr-o rețea robustă, la nivelul întregului guvern, deoarece nicio agenție nu poate reuși singură.

O rețea de cooperare ar trebui să funcționeze permanent, conectând autoritatea electorală cu partenerii tehnici, de reglementare, de securitate și de supraveghere. Un model simplificat de tip celulă de fuziune permite schimbul de informații în timp real („analizăm împreună, acționăm în cadrul mandatului”), asigurându-se că toate părțile mențin o înțelegere comună, totodată păstrând independența operațională. Serviciile comune pot include o linie de asistență pentru autoritățile locale și organizațiile mai mici, canale de escaladare rapidă către principalele platforme online și un mecanism de verificare a înregistrărilor audio sau video suspecte, pentru a ajuta jurnaliștii și publicul să acceseze surse autorizate.

Cooperarea legală și proporțională ar trebui garantată prin protocoale scrise, acces bazat pe roluri și înregistrări transparente ale informațiilor partajate. Astfel de rețele permit avertizări mai timpurii între agenții, reduc duplicarea eforturilor și promovează o comunicare publică mai coerentă, atunci când contează cel mai mult.

3. **O abordare care implică întreaga societate:** Reziliența democratică depinde de implicarea mass-media independente, a societății civile, a mediului academic, a autorităților locale, a sectorului privat și a comunităților pentru a îmbunătăți alfabetizarea, verificarea și comunicarea publică incluzivă – implementate în moduri care să respecte drepturile, transparența și pluralismul.

Ar fi necesar ca transparența să devină o practică standard prin intermediul unor pagini web, dedicate și ușor accesibile, pentru fiecare proces cheie. Utilizarea mesajelor preventive ar trebui să fie limitată și aliniată cu ciclul electoral, axându-se pe indicii clare – la ce să vă așteptați, cum să verificați și unde să raportați – și direcționând în mod constant publicul către surse oficiale.

Organizațiile și canalele de informare locale de încredere pot contribui la extinderea acoperirii, oferind explicații predefinite, potrivite pentru republicare. Ar fi bine ca sprijinul pentru mass-media independentă și jurnalismul de investigație să fie extins, dar menținut la distanță pentru a proteja independența editorială, și completat prin căi clare de combatere a hărțuirii, doxingului și abuzului bazat pe gen.

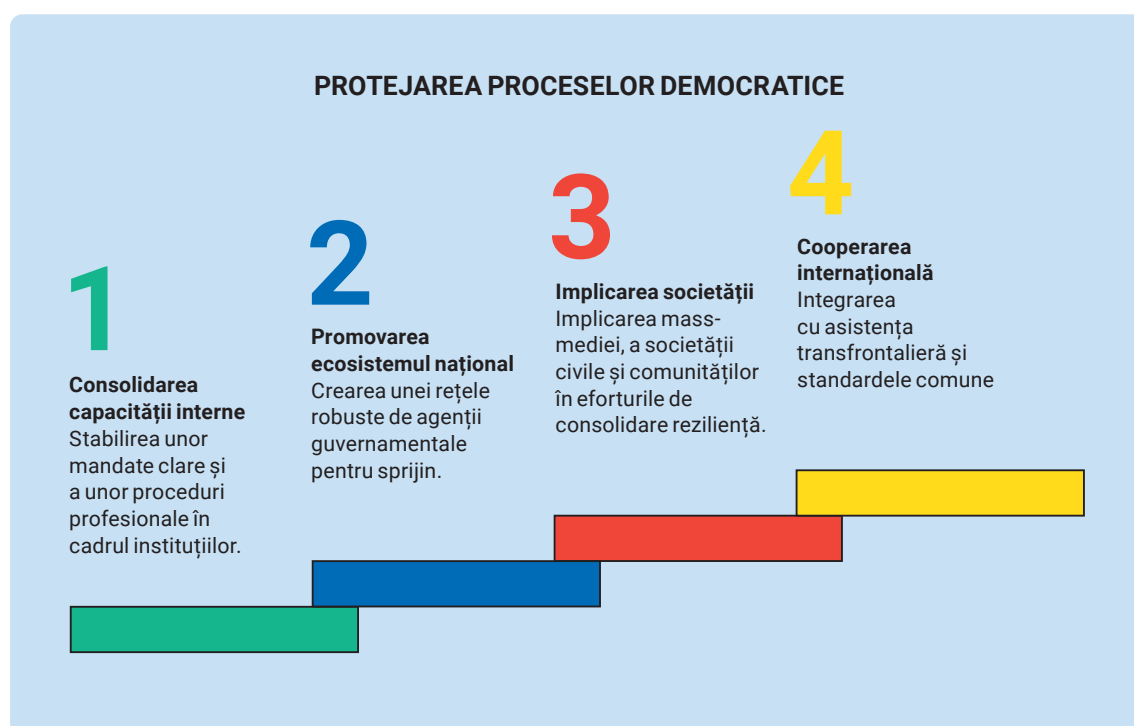
Colaborarea cu furnizorii privați ar trebui să asigure verificarea securizată a solicitărilor sensibile, un răspuns rapid în cazul răspândirii de conținut dăunător și o mai mare transparență în ceea ce privește publicitatea politică.

În cele din urmă, această abordare favorizează un public mai informat și mai implicat, o corectare mai rapidă a zvonurilor și o reutilizare pe scară mai largă a informațiilor de încredere.

- 4. Dezvoltarea cooperării internaționale și a mecanismelor de sprijin:** Sistemele naționale ar trebui să se integreze cu asistența transfrontalieră, standardele împărtășite și acțiunile comune, permițând extinderea sprijinului atunci când atacurile depășesc capacitatea internă.

Aranjamentele de ajutor reciproc ar trebui să fie pregătite în avans și să abordeze răspunsul tehnic, sprijinul criminalistic și comunicarea publică în perioadele electorale. Ar trebui stabilite canale practice pentru acțiuni transfrontaliere de eliminare de conținut sau acțiuni conexe, cu șabloane pre-aprobate, pentru a minimiza întârzierile. Ar trebui armonizate standardele de referință privind protejarea sistemelor relevante pentru alegeri și privind dezvăluirea incidentelor, iar practicile de bază privind trasabilitatea provenienței pentru mass-media oficială ar trebui adoptate unde este posibil, pentru a simplifica verificarea și a crește transparența.

Cunoștințele ar trebui transferate înainte de ciclurile primare prin schimburi și detașări, în timp ce rețelele de cooperare ar trebui să „colaboreze” cu omologii din străinătate pentru a partaja indicatori și manuale. Rezultatele includ o asistență mai rapidă atunci când contează cel mai mult, actualizări mai clare între jurisdicții și dovezi mai solide atunci când este în joc responsabilitatea – transformând reziliența în legitimitate atât la nivel intern, cât și în relația cu partenerii internaționali.



Toate contramăsurile trebuie să fie legale, necesare și proporționale și să urmeze o abordare bazată pe drepturile omului. În practică, aceasta înseamnă vizarea comportamentului manipulativ mai degrabă decât a discursului legitim, respectiv prioritizarea remediilor procedurale – transparență, proveniență și responsabilitate – față de eliminarea conținutului. De asemenea, implică implementarea minimizării datelor și a confidențialității din proiectare; utilizarea unor acțiuni limitate în timp și în scop, cu supraveghere independentă, piste de audit și căi de atac respectiv menținerea transparenței proactive printr-o sursă canonică de adevăr, care permite publicului să verifice afirmațiile.

Aceste garanții se aliniază cu garanțiile privind accesul la informație (de exemplu, Convenția de la Tromsø), standardele privind libertatea de exprimare (de exemplu, Pactul internațional privind drepturile civile și politice, Observația generală nr. 34) și guvernanta platformelor care respectă drepturile (de exemplu, DSA). Totodată, pluralismul mass-media și independența editorială contrabalansează excesul de zel, asigurând că măsurile defensive protejează chiar valorile democratice pe care amenințările hibride la adresa alegerilor încearcă să le erodeze.

Pentru guverne și legislatori

1. Crearea și menținerea unei rețele naționale de cooperare în domeniul alegerilor:

Transformarea acestui aspect într-o prioritate de securitate națională prin crearea unei instituții oficiale și permanente, care să reunească autoritatea de gestionare a alegerilor, agențiile de securitate cibernetică, serviciile de informații, organele de aplicare a legii și unitățile de comunicare strategică. Această rețea ar trebui să funcționeze continuu pentru a efectua evaluări comune ale riscurilor, a derula exerciții de simulare și a elabora protocoale comune de răspuns.

2. Consolidarea cadrelor legislative și de reglementare:

- **Finanțare politică ilicită:** Acolo unde nu există deja prevăzut, interzicerea donațiilor anonime și din străinătate către actori politici. Actualizarea reglementărilor pentru a aborda utilizarea criptomonedelor, consolidarea transparenței în publicitatea online și solicitarea ca donațiile politice care depășesc o anumită sumă să treacă prin sistemul bancar formal pentru a îmbunătăți trasabilitatea și supravegherea.
- **Responsabilitatea platformelor:** Implementarea și aplicarea unor cadre de reglementare robuste pentru platformele de socializare, cu accent pe transparență în procesul de selecție algoritmică a conținutului, publicitate politică și acces la date pentru cercetătorii verificați.
- **Codul electoral și cel penal:** Realizarea unei revizui cuprinzătoare a cadrului juridic electoral pentru a identifica și a elimina lacunele vulnerabile la amenințări hibride. Modernizarea codului penal, pentru a defini și pedepsi în mod explicit infracțiunile care vizează procesul electoral – cum ar fi campaniile coordonate de dezinformare și atacurile cibernetice asupra infrastructurii – pentru a asigura urmărirea penală eficientă.

3. Investirea într-o strategie de reziliență la nivelul întregii societăți: Finanțarea și sprijinirea inițiativelor naționale care sporesc reziliența publică printr-o dublă abordare. În primul rând, capacitatea cetățenilor și a societății civile prin investiții în campanii de alfabetizare media și inteligență artificială pe termen lung și prin furnizarea de sprijin susținut pentru un sector media divers și independent. O componentă critică a acestui aspect este finanțarea dedicată jurnalismului de investigație, esențială pentru expunerea mecanismelor amenințărilor hibride. În al doilea rând, aceste eforturi societale ar trebui completate de angajamentul propriu al guvernului față de comunicarea proactivă, realizată prin infirmarea preventivă (pre-bunking) a narațiunilor probabile și prin înființarea unor centre oficiale de referință, de tip „sursă de adevăr”, pentru a ancora informațiile publice și a contribui la imunizarea cetățenilor împotriva manipulării.

4. **Furnizarea unei infrastructuri și servicii tehnice comune:** Crearea și finanțarea unei capacități centralizate pentru furnizarea de servicii partajate de securitate cibernetică și comunicații securizate pentru instituțiile democratice cheie. Aceasta ar trebui să includă protecții esențiale – cum ar fi atenuarea atacurilor DDoS – pentru site-urile web ale instituțiilor de gestionare a alegerilor și ale altor ținte de mare valoare, asigurând că acestea rămân accesibile publicului, în special în timpul crizelor.

Pentru Organismele de management electoral

5. **Adoptarea unei abordări continue a securității cibernetice:** Tratarea securității electorale ca pe un proces cu caracter permanent. Introducerea unui model de apărare proactivă, care include implementarea unor controale tehnice fundamentale – cum ar fi autentificarea multi-factor rezistentă la atacuri de tip phishing pentru toate conturile critice – adoptarea unei arhitecturi Zero Trust și impunerea unor principii de securitate din punct de vedere al designului în toate achizițiile de tehnologie.
6. **Elaborarea și exersarea planurilor de răspuns integrat:** Crearea și actualizarea periodică a planurilor de răspuns la incidente, care să combine izolarea tehnică cu o comunicare strategică. Agențiile trebuie să fie pregătite să comunice clar și transparent cu publicul în timpul unui incident cibernetic sau informațional, pentru a preveni dezinformarea și a menține încrederea.

Un prim pas, esențial la elaborarea unor astfel de planuri, constă în stabilirea unei guvernante interne, transparente, prin numirea unui lider superior, cu mandat și autoritate de a convoca personal juridic, IT și din domeniul comunicării, care să-și asume responsabilitatea finală pentru gestionarea răspunsului în timpul unui incident. Aceste planuri trebuie, de asemenea, să pregătească agenția pentru dezvoltări de informații ostile. Acestea includ dezvoltarea unui ghid de declasificare, care stabilește protocoale legale clare pentru divulgarea cu daune minime a informațiilor sub presiunea urgenței unei operațiuni de hacking și scurgere de informații, asigurându-se că agenția poate răspunde într-un mod controlat și conform legii.

7. **Participarea activă la rețele de cooperare:** Instituțiile implicate ar trebui să acționeze ca parteneri activi și consecvenți în cadrul rețelei naționale de cooperare electorală. Folosirea acestui forum pentru schimbul reciproc de informații privind amenințările, consolidarea gradului de conștientizare referitor la peisajul mai larg al riscurilor și coordonarea acțiunilor defensive cu agențiile de securitate și informații.

Pentru actorii de sprijin internațional

8. **Promovarea unei „rețele de rețele”:** Prioritizarea consolidării cadrelor de cooperare internațională, cum ar fi colaborarea UE-NATO și Mecanismul de răspuns rapid al G7. Facilitarea schimbului de bune practici și informații privind amenințările între rețelele naționale de cooperare în scopul de a construi o comunitate globală de practică pentru apărarea democratică.
9. **Oferirea unei asistențe tehnice și strategice personalizate:** Oferirea de asistență specifică țărilor partenere pentru a le ajuta să își stabilească propriile rețele naționale de cooperare. Sprijinul ar trebui adaptat contextului național și orientat spre implementarea practică, inclusiv facilitarea exercițiilor comune de simulare și furnizarea de expertiză în domenii specializate, cum ar fi securitatea cibernetică și combaterea FIMI.
10. **Adoptarea unei abordări modulare a finanțării:** Pentru a asigura un sprijin practic și orientat spre rezultate, donatorii ar trebui să ia în considerare finanțarea unor module specifice de capacități cu impact ridicat. Investițiile strategice în servicii comune pot genera economii de scară semnificative. Modulele cheie ar putea include:

- Un Secretariat al Rețelei Naționale de Cooperare în Domeniul Alegerilor, pentru gestionarea coordonării.
- Un sistem de securitate cibernetică de bază pentru a oferi servicii partajate, cum ar fi protecția împotriva DDoS, pentru site-urile web ale autorităților electorale și ale altor agenții critice.
- Pachete de consolidare a capacităților la nivel de agenție, destinate finanțării creării unor centre de referință („source-of-truth”) și a unor manuale de răspuns la incidente în cadrul instituțiilor cheie.
- Gradul de pregătire al țării gazdă pentru a beneficia de sprijin internațional prin pregătirea cadrului juridic, organizațional și tehnic – cum ar fi desemnarea unui punct național de contact și a unor modele juridice pre-aprobate – pentru primirea de asistență de specialitate în caz de criză.
- Echipe internaționale specializate de intervenție rapidă pentru a oferi expertiză de nișă, mobilă, pentru gestionarea tacticilor complexe de amenințare hibridă, cum ar fi echipe dedicate care răspund la atacuri cibernetice și operațiuni de tip „hack-and-leak” sau care oferă sprijin pentru comunicare strategică. Sprijinul ar trebui să fie practic, bazat pe cerere și axat pe o colaborare autentică.

În cele din urmă, însă, succesul pe termen lung constă în prevenirea materializării amenințărilor. Acest lucru poate fi realizat doar prin excelență operațională: derularea impecabilă a proceselor electorale, comunicarea cu o transparență radicală și recunoașterea cu sinceritate a erorilor. Tocmai acest efort constant de construire a unei capacități instituționale durabile și de consolidare a încrederii publice, câștigate cu greu, reprezintă cea mai puternică apărare împotriva celor care încearcă să submineze procesul democratic.

07 Referințe

AAgawal, H., Hamada, Y. și Fernández Gibaja, A. (2021). Reglementarea finanțării campaniilor online: Urmărind fantoma? International IDEA. <https://www.idea.int/publications/catalogue/regulating-online-campaign-finance>

Alihodžić, S. (2023). Protejarea alegerilor: Managementul riscurilor, consolidarea rezilienței și gestionarea crizelor în alegeri. International IDEA. <https://www.idea.int/publications/catalogue/protecting-elections-risk-management-resilience-building-and-crisis>

Alianța pentru Asigurarea Democrației. (2019). Hackerii ruși în spatele creșterii numărului de atacuri cibernetice care vizează alegerile din Ucraina. <https://securingdemocracy.gmfus.org/incident/russian-hackers-behind-surge-in-cyberattacks-targeting-ukrainian-election/>

Anghel, V. (2024). De ce România tocmai și-a anulat alegerile prezidențiale. Journal of Democracy (exclusiv online). <https://www.journalofdemocracy.org/online-exclusive/why-romania-just-canceled-its-presidential-election/>

Antoniuk, D. (7 ianuarie 2023). Guvernul Republicii Moldova, lovit de un val de atacuri de tip phishing. The Record. <https://therecord.media/moldovas-government-hit-by-flood-of-phishing-attacks>

Antoniuk, D. (21 octombrie 2024). O ingerință „fără precedent” vizează alegerile din Moldova. The Record / Recorded Future News. <https://therecord.media/unprecedented-interference-moldova-elections-cyberattack>

Antoniuk, D. (22 septembrie 2025). Rusia își intensifică eforturile de dezinformare pentru a influența votul parlamentar al Republicii Moldova. The Record. <https://therecord.media/russia-steps-disinfo-moldova-election>

Consiliul Atlantic. (11 septembrie 2018). Definirea ingerinței rusești în alegeri: o analiză a incidentelor cibernetice selectate din 2014–2018. <https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/defining-russian-election-interference-an-analysis-of-select-2014-to-2018-cyber-enabled-incidents-2/>

Consiliul Atlantic. (24 februarie 2023). Război narativ: Cum au justificat Kremlinul și agențiile de știri rusești un război de agresiune împotriva Ucrainei. [https://www.atlanticcouncil.org/](https://www.atlanticcouncil.org/wp-content/uploads/2023/02/Narrative-Warfare-Final.pdf)

[wp-content/uploads/2023/02/Narrative-Warfare-Final.pdf](https://www.atlanticcouncil.org/wp-content/uploads/2023/02/Narrative-Warfare-Final.pdf)

Consiliul Atlantic / DFRLab. (4 noiembrie 2024). Tendințele privind ingerința Chinei în alegerile din SUA ilustrează strategia sa de mai lungă durată. <https://dfrlab.org/2024/11/04/china-us-election-interference/>

Bakken, M. (3 februarie 2025). Observarea alegerilor și amenințările hibride. European Democracy Hub. <https://europeandemocracyhub.epd.eu/election-observation-and-hybrid-threats/>

Balmforth, T. și Dysa, Y. (2 noiembrie 2024). Moldova susține că Rusia intenționează să perturbe votul expatriaților în turul doi de duminică. Reuters. <https://www.reuters.com/world/europe/moldova-claims-russia-plans-disrupt-expatriate-voting-sundays-runoff-2024-11-02/>

Barata, J. și Lăză, E. (27 ianuarie 2025). Va salva DSA democrația? Testul recentelor alegeri prezidențiale din România. Tech Policy Press. <https://techpolicy.press/will-the-dsa-save-democracy-the-test-of-the-recent-presidential-election-in-romania>

Bateman, J. și Jackson, D. (2024). Combaterea eficientă a dezinformării: un ghid de politici bazat pe dovezi. Fondul Carnegie pentru Pace Internațională. <https://carnegieendowment.org/research/2024/01/countering-disinformation-effectively-an-evidence-based-policy-guide?lang=en>

Bay, S. (2024). Contracararea amenințărilor hibride la adresa alegerilor: De la actualizarea legislației la stabilirea de rețele de colaborare (Centrul European de Excelență pentru Contracararea Amenințărilor Hibride, Raportul de cercetare 12). Hybrid CoE. <https://www.hybridcoe.fi/publications/hybrid-coe-research-report-12-countering-hybrid-threats-to-elections-from-updating-legislation-to-establishing-collaboration-networks/>

Bay, S. (2025). Protejarea integrității electorale: Cazul Suediei. International IDEA. <https://www.idea.int/publications/catalogue/protecting-electoral-integrity-case-sweden>

Bay, S., Appelgren, J., Isaksson, E., Lindgren, J. și Thunholm, P. (2022). Amenințări la adresa alegerilor publice suedeze – Exemple și scenarii pentru Administrația Electorală (FOI-R--5298--SE). FOI. <https://foi.se/en/foi/reports/report-summary.html?reportNo=FOI-R--5298--SE>

Bing, C. și Vicens, AJ (23 octombrie 2024). Un grup de hackeri iranian vizează site-urile web și mass-media electorale din SUA înainte de vot, susține Microsoft. Reuters. <https://www.reuters.com/technology/cybersecurity/iranian-hacker-group-focuses-us-election-websites-media-ahead-vote-microsoft-2024-10-23/>

Bjola, C. (7 februarie 2025). Invazii algoritmice: Cum amenință războiul informațional flancul estic al NATO. NATO Review. <https://archives.nato.int/nato-review-algorithmic-invasions-how-information-warfare-threatens-natos-eastern-flank>

Centrul Brennan pentru Justiție. (octombrie 2020). Lecțiile anului 2020 pentru securitatea alegerilor. <https://www.brennancenter.org/our-work/research-reports/2020s-lessons-election-security>

Bryjka, F. (2024). Ingerința Rusiei aproape a copleșit alegerile prezidențiale – votul pentru referendum din Republica Moldova. Institutul Polonez pentru Afaceri Internaționale (PISM). <https://pism.pl/publications/russian-interference-nearly-overwhelmed-moldovan-presidential-election-referendum-vote>

C2PA. (2024). Acreditări de conținut și prezentare generală C2PA. <https://c2pa.org>

Canada (Guvernul Canadei). (8 iulie 2025). Perspective multipartite: Un compendiu privind combaterea imixtiunii în alegeri. <https://www.canada.ca/en/democratic-institutions/services/paris-call-trust-security-cyberspace/multistakeholder-insights-compendium-countering-election-interference.html>

Centrul Carter. (8 iulie 2025). Program pentru democrație. <https://www.cartercenter.org/peace/democracy>

Centrul pentru un Public Informat, Laboratorul de Criminalistică Digitală, Graphika și Observatorul de Internet Stanford. (2021). Fitolung: Dezinformarea și alegerile din 2020. Parteneriatul pentru Integritatea Alegerilor. <https://purl.stanford.edu/tr171zs0069>

Centrul pentru Securitatea Internetului. (8 iulie 2025a). EI ISAC. <https://www.cisecurity.org/ei-isac>

Centrul pentru Securitatea Internetului. (8 iulie 2025b). Ciclul de viață IT – Ghidul CIS pentru achizițiile de tehnologie electorală. https://election-procurement.docs.cisecurity.org/en/latest/IT_product_services_lifecycle.html

Centrul pentru Securitatea Internetului. (2025c). Securitatea alegerilor în centrul atenției – atacuri DDoS. <https://www.cisecurity.org/insights/spotlight/election-security-spotlight-ddos-attacks>

Cerulus, L. (iunie 2025). UE ia apărarea Moldovei împotriva atacurilor cibernetice rusești. POLITICO. <https://www.politico.eu/article/eu-moldova-election-cyber-security-russia-hacking/>

Chainalysis. (2024a). Indicele de adoptare a criptomonedelor în 2024. <https://www.chainalysis.com/blog/2024-global-crypto-adoption-index>

Chainalysis. (2024b). Ingerința malignă și criptomonedele: Cum poate urmărirea tranzacțiilor criptografice să expună și să perturbe eforturile de influență malignă. <https://www.chainalysis.com/blog/malign-interference-and-crypto/>

Chan, K. (17 decembrie 2024). UE investighează TikTok în legătură cu garanțiile de securitate pentru alegerile prezidențiale din România. AP News. <https://apnews.com/article/0638e90cb3898fc61619e8aed4731a53>

Chan, K. (25 iulie 2025). Meta va înceta difuzarea reclamelor politice în Uniunea Europeană până în toamnă, invocând noile reguli ale blocului comunitar. AP News. <https://apnews.com/article/meta-instagram-facebook-eu-european-union-political-89efec96723308d2a0469740d24d433>

CISA (Agenția pentru Securitate Cibernetică și Infrastructură). (18 ianuarie 2024a). Riscul în centrul atenției: AI generativă și ciclul electoral din 2024. <https://www.cisa.gov/resources-tools/resources/risk-focus-generative-ai-and-2024-election-cycle>

CISA. (2024b). #Protect2024: Securitatea alegerilor. <https://www.cisa.gov/topics/election-security/protect2024>

CISA. (8 iulie 2025). Alăturați-vă Centrului de Partajare și Analiză a Informațiilor privind Infrastructura Electorală (EI-ISAC). <https://www.cisa.gov/resources-tools/groups/join-elections-infrastructure-information-sharing-and-analysis-center-ei-isac>

CISA și EAC. (2024a). Ghid de comunicare privind răspunsul la incidentele din infrastructura electorală. https://www.eac.gov/sites/default/files/2024-10/Election_Infrastructure_Incident_Response_Comms_Guide_508.pdf

CISA și EAC. (2024b). Îmbunătățirea securității alegerilor prin intermediul comunicărilor publice. https://www.eac.gov/sites/default/files/2024-06/Enhancing_Election_Security_Through_Public_Communications.pdf

Cisco (Outshift). (8 iulie 2025). Top 15 atacuri asupra lanțului de aprovizionare software: Studii de caz. <https://outshift.cisco.com/blog/top-10-supply-chain-attacks>

Clayton, M. (17 iunie 2014). Alegerile din Ucraina au evitat la limită „distrugerea gratuită” din partea hackerilor. The Christian Science Monitor. <https://www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers>

Cloudflare. (8 iulie 2025). Explorarea schimbărilor traficului de internet și a atacurilor cibernetice în timpul alegerilor americane din 2024. <https://blog.cloudflare.com/exploring-internet-traffic-shifts-and-cyber-attacks-during-the-2024-us-election/>

CNN. (26 aprilie, 2024a). Un atac cibernetic obligă comitatul Georgia să întrerupă conexiunea la sistemul de înregistrare a alegătorilor din stat. <https://edition.cnn.com/2024/04/26/politics/georgia-coffee-county-cyberattack-voter-system/index.html>

CNN. (2024b, 19 august). SUA concluzionează că Iranul se află în spatele tentativelor de piraterie informatică care vizează campaniile lui Trump și Biden Harris. <https://edition.cnn.com/2024/08/19/politics/us-concludes-iran-behind-trump-biden-harris-hacking/index.html>

Coherent Market Insights. (17 martie 2025). Dimensiunea și prognoza pieței de schimb valutar pentru criptomonede, 2025–2032. <https://www.coherentmarketinsights.com/industry-reports/crypto-exchange-market>

CoinGecko. (2025). Prețuri, grafice și capitalizări de piață ale criptomonedelor. <https://www.coingecko.com>

Universitatea Columbia, SIPA IGP. (8 iulie 2025). Un oficial francez prezintă abordarea guvernului pentru combaterea operațiunilor online străine. <https://igp.sipa.columbia.edu/news/french-official-outlines-government-approach-countering-foreign-online-operations>

Institutul Canadian pentru Securitatea Comunicațiilor. (martie 2025). CSE publică actualizarea din 2025 pentru a raporta cu privire la amenințările cibernetice la adresa procesului democratic din Canada. <https://www.canada.ca/en/communications-security/news/2025/03/communications-security-establishment-canada-releases-2025-update-to-report-on-cyber-threats-to-canadas-democratic-process.html>

Constella Intelligence. (8 iulie 2025). Scurgerile de informații din baza de date a alegătorilor amenință alegerile americane din 2024. <https://constella.ai/2024-u-s-election-voter-database-leaks/>

Consiliul Europei. (2024). Votul prin internet în alegerile postbelice din Ucraina: riscuri și provocări – rezultatele studiului prezentat. <https://www.coe.int/en/web/kyiv/-/internet-voting-in-post-war-elections-in-ukraine-risks-and-challenges-results-of-the-study-presented>

Consiliul Europei. (8 iulie 2025). Ingerință străină în procesele electorale la nivel local și regional. <https://rm.coe.int/0900001680b4cb53>

Comitatul San Luis Obispo, Grefier registrator. (1 august 2024). Agențiile federale spun că un atac cibernetic ar putea împiedica accesul public la informațiile electorale, nu și alegerile în sine. <https://www.slocounty.ca.gov/departments/clerk-recorder/news-announcements/federal-agencies-say-cyber-attacks-could-hinder-public-access-to-election-information-but-not-to-ele>

CrowdStrike. (2025a). Securitatea Zero Trust explicată: Principiile modelului Zero Trust. <https://www.crowdstrike.com/en-us/cybersecurity-101/zero-trust-security>

CrowdStrike. (2025b). Comunicat de presă: CrowdStrike publică raportul privind vânatoarea de amenințări pe 2025. <https://www.crowdstrike.com/en-us/press-releases/crowdstrike-releases-2025-threat-hunting-report/>

Csernaton, R. (2024). Poate democrația să supraviețuiască puterii distructive a inteligenței artificiale? Carnegie Endowment. <https://carnegieendowment.org/research/2024/12/can-democracy-survive-the-disruptive-power-of-ai>

Cyble. (2024). Securitatea cibernetică a UE în 2024: Informații din cel mai recent raport al ENISA. <https://cyble.com/blog/eu-cybersecurity-in-2024-insights-from-enisa-latest-report>

Cyble. (8 iulie 2025). Atacurile asupra lanțului de aprovizionare software au crescut în intensitate în aprilie și mai. <https://cyble.com/blog/supply-chain-attacks-surge-in-april-may-2025>

Deloitte. (2024). Peisajul amenințărilor ENISA 2024: Peisajul amenințărilor cibernetice în sectorul financiar. <https://www.deloitte.com/ro/en/our-thinking/articles/raportul-enisa-threat-landscape-2024-peisajul-amenintarilor-cibernetice-sectorul-financiar.html>

Comisia Electorală (Regatul Unit). (2024). Răspunsul Comisiei Electorale la atribuirea atacurilor cibernetice. <https://www.electionalcommission.org.uk/media-centre/electional-commission-response-cyber-attack-attribution-0>

Alegeri Canada. (8 iulie 2025). Colaborarea noastră cu agențiile de securitate și partenerii – Ghid media pentru alegeri generale în cel de-al 45-lea legislativ. <https://www.elections.ca/content.aspx?section=med&dir=guide&document=p19&lang=e>

Electionline. (octombrie 2024). Peisajul amenințărilor la adresa alegerilor din 2024. <https://electionline.org/wp-content/uploads/2024/10/2024-Election-Threat-Landscape-TLP-CLEAR.pdf>

Grupul de cooperare ENISA / NIS. (2024). Compendiu privind securitatea cibernetică și reziliența alegerilor. Comunicat de presă: <https://www.enisa.europa.eu/news/safeguarding-eu-elections-amidst-cybersecurity-challenges>

Euromaidan Press. (2014). Tentativa de piraterie informatică a Rusiei eșuează, dar sunt difuzate știri false despre alegeri. <https://euromaidanpress.com/2014/05/26/russian-hacking-attempt-fails-but-fake-election-news-airs/>

Comisia Europeană. (2016). Cadrul comun privind combaterea amenințărilor hibride: Un răspuns al Uniunii Europene (JOIN(2016) 18 final). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52016JC0018>

Comisia Europeană. (2024). Comisia inițiază proceduri oficiale împotriva TikTok în temeiul DSA (IP/24/6487). https://ec.europa.eu/commission/presscorner/detail/en/ip_24_6487

Comisia Europeană. (2025a). Amenințări hibride – Industria de apărare și spațiu. https://defence-industry-space.ec.europa.eu/eu-defence-industry/hybrid-threats_en

Comisia Europeană. (2025b). Rețeaua europeană de cooperare privind alegerile. https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/democracy-eu-citizenship-anti-corruption/democracy-and-electoral-rights/european-cooperation-network-elections_en

Comisia Europeană. (2025c, 12 iunie). Serviciile Comisiei și autoritățile moldovenești efectuează un test de rezistență privind potențialele amenințări hibride digitale la adresa integrității alegerilor înaintea alegerilor parlamentare din Republica Moldova. Modelarea viitorului digital al Europei. <https://digital-strategy.ec.europa.eu/en/news/commission-services-and-moldovan-authorities-conduct-stress-test-potential-digital-hybrid-threats>

Observatorul European al Mass-Mediei Digitale (EDMO). (2024). Raport final – Rezultatele unui efort la nivelul întregii comunități (alegerile PE). <https://edmo.eu/publications/final-report-results-and-outcomes-of-a-community-wide-effort/>

Serviciul European de Acțiune Externă (SEAE). (2024). Al doilea raport al SEAE privind amenințările legate de manipularea informațiilor și ingerințele străine (FIMI). https://www.eeas.europa.eu/sites/default/files/documents/2024/EEAS-2nd-Report%20on%20FIMI%20Threats-January-2024_0.pdf

Serviciul European de Acțiune Externă (SEAE). (2025a). Al treilea raport al SEAE privind amenințările legate de manipularea informațiilor și ingerințele străine (FIMI). <https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf>

Serviciul European de Acțiune Externă (SEAE). (2025b). Integritatea informațiilor și combaterea FIMI. https://www.eeas.europa.eu/eeas/information-integrity-and-counter-foreign-information-manipulation-interference-fimi_en

Serviciul European de Acțiune Externă (SEAE). (2025c). Despre Misiunea de Parteneriat a UE în Republica Moldova (EUPM Moldova). https://www.eeas.europa.eu/eupm-moldova/about-eu-partnership-mission-republic-moldova_en

EUvsDisinfo. (2024a). Doppelganger ripostează: Dezvăluirea activităților FIMI care vizează alegerile pentru Parlamentul European. <https://euvsdisinfo.eu/doppelganger-strikes-back-unveiling-fimi-activities-targeting-european-parliament-elections/>

EUvsDisinfo. (2024b). Cui îi este frică de Moldova europeană? <https://euvsdisinfo.eu/who-is-afraid-of-the-european-moldova/>

Europol. (28 februarie 2025). ADN-ul crimei organizate se schimbă – la fel și amenințarea la adresa Europei. <https://www.europol.europa.eu/media-press/newsroom/news/dna-of-organised-crime-changing-and-so-threat-to-europe>

FBI. (5 noiembrie 2024). Declarație privind amenințările cu bombă la adresa secțiilor de votare. <https://www.fbi.gov/news/press-releases/fbi-statement-on-bomb-threats-to-polling-locations>

Forbes. (10 martie 2025). Phishing-ul și deepfake-urile bazate pe inteligență artificială: Viitorul fraudei digitale. <https://www.forbes.com/councils/forbestechcouncil/2025/03/10/ai-driven-phishing-and-deep-fakes-the-future-of-digital-fraud/>

Freedom House. (2024). Libertatea în lume în 2024: Daunele tot mai mari ale alegerilor defectuoase și conflictelor armate. <https://freedomhouse.org/report/freedom-world/2024/mounting-damage-flawed-elections-and-armed-conflict>

GAO (Oficiul pentru Responsabilitatea Guvernamentală din SUA). (februarie 2020). Securitatea alegerilor: Sunt necesare urgent planuri ale DHS... <https://www.gao.gov/assets/gao-20-267.pdf>

Gavin, W. (23 septembrie 2025). Moldova arestează 74 de persoane într-un complot de perturbare a alegerilor. Cum își propune o rețea de știri false, finanțată de Rusia, să perturbe alegerile din Europa - anchetă BBC. BBC News. <https://www.bbc.com/news/articles/c4g5kl0n5d2o>

Gilbert, D. (11 aprilie 2024). Lucrătorii electorali sunt deja epuizați – și în alertă maximă.

WIRED <https://www.wired.com/story/election-officials-threats-disinformation/>

Global Witness. (6 decembrie 2024). TikTok promovează conținut despre candidați de extremă dreapta în alegerile din România, arată ancheta. <https://www.globalwitness.org/en/press-releases/tiktok-pushes-far-right-candidate-content-romanian-election-global-witness-investigation-shows/>

Global Witness. (15 mai 2025). Înaintea celui de-al doilea tur de scrutin, TikTok continuă să promoveze conținut de extremă dreapta în România. <https://globalwitness.org/en/campaigns/digital-threats/tiktok-algorithm-continues-to-push-multiple-times-more-far-right-content-to-users-ahead-of-romanian-election>

Google Cloud. (August 2023). Subminarea sondajelor: Amenințări cibernetice la adresa alegerilor globale. <https://cloud.google.com/blog/topics/threat-intelligence/cyber-threats-global-elections>

Google DeepMind. (2025). SynthID – Un instrument pentru filigranarea și identificarea conținutului generat prin inteligență artificială. <https://deepmind.google/science/synthid/>

Hedenskog, J. și Hjelm, M. (25 octombrie 2020). Propaganda prin proxy: oligarhi ucraineni, TV și influența Rusiei (FOI Memo 7312). FOI. <https://www.foi.se/rest-api/report/FOI%20Memo%207312>

Hedling, E. (15 aprilie 2025). Identități sociale și vulnerabilități democratice: Învățând din exemple de dezinformare direcționată (Centrul European de Excelență pentru Contracurarea Amenințărilor Hibrice, Document de Lucru 24). Hybrid CoE. https://www.hybridcoe.fi/wp-content/uploads/2025/04/20250415-Hybrid_CoE_Paper-24-WEB.pdf

Hoffman, FG (2022). Către un al cincilea val al teoriei și practicii descurajării (Centrul European de Excelență pentru Contracurarea Amenințărilor Hibrice, Document de Lucru 12). Hybrid CoE. <https://www.hybridcoe.fi/publications/hybrid-coe-paper-12-detering-hybrid-threats-towards-a-fifth-wave-of-deterrence-theory-and-practice/>

Hollis, DB și Ohlin, JD (2021). Apărarea democrațiilor: Combaterea ingerințelor electorale străine într-o eră digitală. Editura Universității Oxford. <https://global.oup.com/academic/product/defending-democracies-9780197556979>

Hoogensen Gjør, G. și Jalonen, O. (2023). Identitatea ca instrument de dezinformare (Centrul European de Excelență pentru Contracurarea Amenințărilor Hibrice, Analiza Strategică 34). Hybrid CoE. <https://www.hybridcoe.fi/publications/hybrid-coe-strategic-analysis-34-identity-as-a-tool-for-disinformation-exploiting-social-divisions-in-modern-societies/>

Hoxhunt. (8 iulie 2025). Phishing-ul bazat pe inteligență artificială îi depășește pe infractorii cibernetici de elită în 2025. <https://hoxhunt.com/blog/ai-powered-phishing-vs-humans>

Huo, J. (12 noiembrie 2024). Eforturile de influență străină au atins apogeul în timpul alegerilor din 2024. NPR. <https://www.npr.org/2024/11/09/nx-s1-5181965/2024-election-foreign-influence-russia-china-iran>

Centrul European de Excelență pentru Contracurarea Amenințărilor Hibrice. (ianuarie 2024). Întrebări frecvente despre amenințările hibride. <https://www.hybridcoe.fi/wp-content/uploads/2024/01/FAQ-on-Hybrid-Threats.pdf>

Centrul European de Excelență pentru Contracurarea Amenințărilor Hibrice. (2025). Amenințări hibride. <https://www.hybridcoe.fi/hybrid-threats/>

Fundația Internațională pentru Sisteme Electorale (IFES). (20 decembrie 2024). Anularea alegerilor din 2024 în România: Abordarea amenințărilor emergente la adresa integrității electorale. <https://www.ifes.org/publications/romanian-2024-election-annulment-addressing-emerging-threats-electoral-integrity>

IGP (Inspectoratul General al Poliției). (22 septembrie 2025). Trust Media responsabil de propaganda pro-rusă și dezinformare, finanțat printr-o schemă complexă de spălare de bani, vizat în perchezițiile de astăzi. Poliția Republicii Moldova. <https://www.igp.gov.md/ro/politia-actiune/trust-media-responsabil-de-propaganda-pro-rusa-si-dezinformare-finantat-printr-o>

IGP (Inspectoratul General al Poliției). (2025, 13 august). Autoritățile intensifică acțiunile împotriva dezinformării în spațiul digital: peste 400 de canale TikTok vizate pentru blocare. Poliția Republicii Moldova. <https://politia.md/ro/noutati/autoritatile-intensifica-actiunile-impotriva-dezinformarii-spatiul-digital-pest-400-de>

International IDEA. (2019). Colaborare interinstituțională privind securitatea cibernetică în alegeri: Discuție la masă rotundă. <https://www.idea.int/news/inter-agency-collaboration-cybersecurity-elections-roundtable-discussion>

International IDEA. (28 noiembrie 2023). Mauritius: Colaborare interinstituțională împotriva amenințărilor hibride. <https://www.idea.int/news/mauritius-inter-agency-collaboration-against-hybrid-threats>

International IDEA. (17 septembrie 2024). Starea globală a democrației 2024: Consolidarea legitimității alegerilor într-o perioadă de incertitudine radicală. <https://www.idea.int/publications/catalogue/global-state-democracy-2024-strengthening-legitimacy-elections>

International IDEA. (2025). Baza de date privind finanțarea politică. <https://www.idea.int/data-tools/data/political-finance-database>

ISACA. (8 iulie 2025). Raportul din 2025 privind securitatea lanțului de aprovizionare cu software. <https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2025/the-2025-software-supply-chain-security-report>

Ivanti. (8 iulie 2025). Riscul de atacuri asupra lanțului de aprovizionare cu software este în creștere. <https://www.ivanti.com/blog/software-supply-chain-attack-risk>

Kovalčíková, N. și Spatafora, G. (17 decembrie 2024). Viitorul democrației: Lecții din lupta SUA împotriva ingerințelor electorale străine în 2024 (EUISS Brief). Institutul UE pentru Studii de Securitate. <https://www.iss.europa.eu/publications/briefs/future-democracy-lessons-us-fight-against-foreign-electoral-interference-2024>

Kubica, L. (2024). Lupta Republicii Moldova împotriva amenințărilor hibride din partea Rusiei (Centrul European de Excelență pentru Contracurarea Amenințărilor Hibride. Document de lucru 28). Hybrid CoE. <https://www.hybridcoe.fi/publications/hybrid-coe-working-paper-28-moldovas-struggle-against-russias-hybrid-threats-from-counteracting-the-energy-leverage-to-becoming-more-sovereign-overall>

Ledford, H. (2024). Deepfake-uri, troli și cybertrooperi: Cum ar putea rețelele sociale să influențeze alegerile din 2024. *Nature*, 626(7902), 463–464. <https://www.nature.com/articles/d41586-024-00274-7>

Levin, DH (2020). Imixtiunea la urne: Cauzele și efectele intervențiilor electorale partizane. Oxford University Press. <https://academic.oup.com/book/36920>

Lewandowsky, S., Cook, J., Ecker, UKH, Albarracín, D., Amazeen, MA, Kendeou, P. și Zaragoza, MS (2020). Manual de dezmințire 2020. <https://www.climatechangecommunication.org/wp-content/uploads/2020/10/DebunkingHandbook2020.pdf>

Liberties (Uniunea pentru Libertăți Civile pentru Europa). (2025). Raport privind statul de drept 2025. https://dq4n3btxm8c9.cloudfront.net/files/vdxw3e/Liberties_Rule_of_Law_Report_2025_v.pdf

Lopatka, J. (27 martie 2024). Cehii sancționează site-ul Medvedchuk pentru influența sa politică pro-rusă în UE. Reuters. <https://www.reuters.com/world/europe/czechs-sanction-medvedchuk-website-over-pro-russian-eu-political-influence-2024-03-27>

Lores, R. (2025). Global Crypto User Index 2025. Statista. https://www.statista.com/outlook/fmo/digital-assets/cryptocurrencies/worldwide?srltid=AfmBOorgqEAOLng7cSMAFDInxing0Kw13xMpvwg1gJcvm_ZC590gOuQg

Martin, T. (11 noiembrie 2022). Atacurile cibernetice ale Rusiei au avut ca scop „destabilizarea” Moldovei, spune premierul. The Record. <https://therecord.media/russias-cyberattacks-aimed-at-destabilizing-moldova-pm-says>

McGrath, S. (22 septembrie 2025). Moldova a reținut 74 de persoane în legătură cu un presupus complot de tulburări susținut de Rusia în ajunul unor alegeri cheie. AP News. <https://apnews>.

McGrath, S. și Alexandru, A. (9 septembrie 2025). Președintele Republicii Moldova acuză Rusia că poartă un „război hibrid” înaintea unor alegeri cheie. AP News. <https://apnews.com/article/moldova-elections-russia-influence-europe-8cc882551dd52957491e3cfd112cc878>

McGrath, S. și Dumitrache, N. (13 mai 2025). Reluarea alegerilor prezidențiale de către România este un test cu miză mare pentru o democrație afectată. AP News. <https://apnews.com/article/romania-election-presidency-europe-far-right-russia-baf335441276aa88859c010bc04da686>

Meaker, M. (3 octombrie 2023). Falsificările electorale din Slovacia arată că inteligența artificială este un pericol pentru democrație. WIRED. <https://www.wired.com/story/slovakias-election-deepfakes-show-ai-is-a-danger-to-democracy>

Microsoft. (octombrie 2025). Raportul Microsoft privind apărarea digitală 2025. <https://aka.ms/Microsoft-Digital-Defense-Report-2025#page=1>

Centrul de analiză a amenințărilor Microsoft. (4 aprilie 2024a). Aceleași ținte, noi strategii: actorii de amenințare din Asia de Est folosesc metode unice. <https://www.microsoft.com/en-us/security/security-insider/threat-landscape/east-asia-threat-actors-employ-unique-methods>

Centrul de analiză a amenințărilor Microsoft. (27 septembrie 2024b). Operatori legați de Rusia s-au angajat în eforturi ample de influențare a alegătorilor americani. <https://www.microsoft.com/en-us/security/security-insider/threat-landscape/russia-linked-operators-engaged-in-expansive-efforts-to-influence-us-voters>

Molas, B. (15 decembrie 2024). Doxing: o analiză a literaturii de specialitate. Centrul Internațional pentru Combaterea Terorismului. <https://icct.nl/publication/doxing-literature-review>

Moldpres – Agenția Informațională de Stat. (13 august 2025). Serviciul de Informații și Securitate al Republicii Moldova, Poliția și ANRCETI solicită blocarea a peste 400 de canale TikTok. <https://www.moldpres.md/eng/society/moldova-s-intelligence-and-security-service-police-anrceti-ask-to-block-over-400-tiktok-channels>

Militära underrättelse- och säkerhetstjänsten (Must). (2025). Raport anual 2024. <https://www.forsvarsmakten.se/contentassets/546bbe13064a4c739e1cbc4b5e4571f7/2024-must-annual-report.pdf>

Nakamura, D., Belton, C. și Sommer, W. (4 septembrie 2024). Departamentul de Justiție acuză doi agenți media ruși de o presupusă schemă. The Washington Post. <https://www.washingtonpost.com/national-security/2024/09/04/justice-department-election-security>

Nardelli, A. (22 septembrie 2025). Dezvăluit: Planul secret al lui Putin de a pirata alegerile cruciale din Moldova. Bloomberg. <https://www.bloomberg.com/news/articles/2025-09-22/moldova-elections-russia-s-plan-to-hack-the-vote>

Grupul operativ național privind crizele electorale. (8 iulie 2025a). Grupul operativ național privind crizele electorale. Protejați democrația. <https://protectdemocracy.org/work/national-task-force-on-election-crises>

Grupul operativ național privind crizele electorale. (2025b, 8 iulie). Lecții învățate din alegerile generale din 2024. <https://electiontaskforce.org/lessons-from-the-2024-general-election>

NATO. (2022). Concept strategic. https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf

NATO. (2024). Contracararea amenințărilor hibride. https://www.nato.int/cps/en/natohq/topics_156338.htm

NATO. (2025). Abordarea NATO pentru contracararea amenințărilor informaționale (text oficial). https://www.nato.int/cps/en/natohq/official_texts_231905.htm

NCSC (Regatul Unit). (2025). Cadrul de evaluare cibernetică v4.0. <https://www.ncsc.gov.uk/files/NCSC-Cyber-Assessment-Framework-4.0.pdf>

Newman, N., Fletcher, R., Robertson, CT, Ross Arguedas, A. și Nielsen, RK (2024). Raport de știri digitale 2024. Institutul Reuters. https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2024-06/RISJ_DNR_2024_Digital_v10%20lr.pdf

Institutul Național de Standarde și Tehnologie (NIST). (2020). SP 800 207: Arhitectura Zero Trust. <https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf>

Institutul Național de Standarde și Tehnologie (NIST). (2022). SP 800 218: Cadrul de dezvoltare software securizat (SSDF) v1.1. <https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-218.pdf>

Institutul Național de Standarde și Tehnologie (NIST). (2023). SP 800 207A: Un model de arhitectură Zero Trust pentru controlul accesului în aplicații cloud-native în medii multi-cloud <https://csrc.nist.gov/pubs/sp/800/207/a/final>

Institutul Național de Standarde și Tehnologie (NIST). (2024). SP 800 218A: Practici securizate de dezvoltare software pentru inteligență artificială generativă și modele de bază cu utilizare duală. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218A.pdf>

O'Brien, M. și Swenson, A. (16 februarie 2024). Companiile de tehnologie semnează un acord pentru combaterea trucurilor electorale generate de inteligența artificială. AP News. <https://apnews.com/article/ai-generated-election-deepfakes-munich-agreement-meta-google-microsoft-tiktok-x-c40924ffc68c94fac74fa994c520fc06>

Ohlin, JD (2020). Ingerința în alegeri: Dreptul internațional și viitorul democrației.

Editura Universității Cambridge. <https://doi.org/10.1017/9781108859561>

Olari, V. (18 octombrie 2024). Ce trebuie să știți despre influența malignă a Rusiei în alegerile din Republica Moldova. Atlantic Council. <https://www.atlanticcouncil.org/blogs/new-atlanticist/what-to-know-about-russian-malign-influence-in-moldovas-upcoming-election>

Olari, V. (6 martie 2025a). Rețeaua Telegram încearcă să manipuleze discursul politic local din Republica Moldova. DFRLab. <https://dfrlab.org/2025/03/06/telegram-network-moldova/>

Olari, V. (26 martie 2025b). O campanie multiplatformă seamănă diviziuni anti-europene în Moldova. DFRLab. <https://dfrlab.org/2025/03/26/cross-platform-campaign-sows-anti-europe-division-in-moldova/>

OSCE/ODIHR. (2017). Muntenegru, Alegeri parlamentare, 16 octombrie 2016: Raport final. <https://www.osce.org/odihr/elections/montenegro/295511>

OSCE/ODIHR. (2021). Republica Moldova, Alegeri parlamentare anticipate, 11 iulie 2021: Raport final. <https://www.osce.org/odihr/elections/moldova/501518>

OSCE/ODIHR. (2024). Moldova, Alegeri prezidențiale și referendum constituțional, 20 octombrie 2024: Declarație privind constatările și concluziile preliminare. <https://www.osce.org/odihr/elections/moldova/578815>

OSCE/ODIHR. (20 februarie 2025a). Polonia, Alegeri prezidențiale, Turul doi, 2025: Raport final.

<https://www.osce.org/odihr/elections/poland/591761>

OSCE/ODIHR. (2025b, 28 septembrie). Republica Moldova, declarație privind constatările și concluziile preliminare. <https://www.osce.org/files/f/documents/4/7/597800.pdf>

OSCE/ODIHR. (2025c, 14 martie). Republica Moldova: Alegeri prezidențiale și referendum constituțional, 20 octombrie și 3 noiembrie 2024, Raport final. https://www.osce.org/files/f/documents/3/9/587451_0.pdf

OSCE/ODIHR. (2025d, 5 mai). Eforturi notabile de abordare a integrității electorale, dar anumite aspecte... (România). <https://www.osce.org/odihr/elections/romania/590330>

Pamment, J., Nothhaft, H., Agardh-Twetman, H. și Fjällhed, A. (2018). Contracararea activităților de influență informațională: Starea actuală a domeniului. MSB. <https://rib.msb.se/filer/pdf/28697.pdf>

Pamment, J. și Tsursumia, D. (mai 2025). Dincolo de Operațiunea Doppelgänger: O evaluare a capacității Agenției de Design Social (SDA). Universitatea Lund și Agenția Suedeză de Apărare Psihologică. <https://www.psychologicaldefence.lu.se/sites/psychologicaldefence.lu.se/files/2025-05/Beyond%20Operation%20Doppelg%C3%A4nger.pdf>

Pamment, J. și Isaksson, E. (2024). Apărare psihologică: concepte și principii pentru anii 2020 (Seria de rapoarte MPF 6/2024). Universitatea Lund și Agenția Suedeză de Apărare Psihologică. https://www.mpf.se/wp-content/uploads/2024/03/mpf_rapport_6_2024_psychological_defence.pdf

Perdomo, C. și Uribe Burcher, C. (2017). Bani, influență, corupție și captură: poate democrația să fie protejată?. Starea globală a democrației 2017. Explorarea rezilienței democrației. International IDEA. <https://www.idea.int/gsod-2017/files/IDEA-GSOD-2017-REPORT-EN.pdf>

Popescu Zamfir, R. (2025, 26 septembrie). Alegerile din Moldova sunt un test pentru influența Rusiei în Europa. Fondul Carnegie pentru Pace Internațională.

<https://carnegieendowment.org/research/2025/09/moldovas-election-is-a-test-for-russian-influence-in-europe?lang=en>

Posetti, J. și colab. (2020). Violența online împotriva jurnalistelor: o imagine globală a incidenței și impacturilor. UNESCO. <https://unesdoc.unesco.org/ark:/48223/pf0000375136/PDF/375136eng.pdf.multi>

Rainsford, S. (4 decembrie 2024). România lovită de o campanie electorală majoră de influență și de atacuri cibernetice rusești. BBC. <https://www.bbc.com/news/articles/cgq18w507dko>

ReliaQuest. (24 septembrie 2024). Alegerile din SUA din 2024: Principalele amenințări cibernetice și impactul asupra organizațiilor. <https://www.reliaquest.com/blog/2024-us-election-top-cyber-threats-organizational-impacts/>

Reuters. (24 octombrie 2024a). Operațiunea de influență chineză vizează cursele electorale regionale din SUA, susține Microsoft. <https://www.reuters.com/world/us/chinese-influence-operation-targets-us-down-ballot-races-microsoft-says-2024-10-23/>

Reuters. (2024b, 5 noiembrie). FBI susține că amenințări false cu bombă legate de Rusia vizează secții de votare din state conflictuale. <https://www.reuters.com/world/us/fake-bomb-threats-linked-russia-briefly-close-georgia-polling-locations-2024-11-05/>

Radio Europa Liberă Moldova. (25 octombrie 2024). Poliția moldovenească acuză oligarhul pro-rus de schemă de cumpărare a voturilor în valoare de 39 de milioane de dolari. <https://www.rferl.org/a/moldova-police-accuse-shor-russia-oligarch-39m-vote-buying/33172951.html>

Roth, A. (4 septembrie 2024). Rusia acuzată că încearcă să influențeze alegătorii americani prin intermediul campaniei online. The Guardian. <https://www.theguardian.com/us-news/2024/sep/04/russia-us-election-online-campaign-sanctions>

Saeva, E. și Tasheva, I. (2024). Alegerile europene din 2024 și securitatea cibernetică: o retrospectivă și lecții învățate. European View (Centrul Martens). <https://www.martenscentre.eu/wp-content/uploads/2024/11/12.pdf>

Schroeder, DT, Cha, M., Baronchelli, A., Bostrom, N., Christakis, NA, Garcia, D., ... Kunst, J.

R. (2025). Cum pot amenința democrația roiriile de inteligență artificială malițioasă. arXiv. <https://doi.org/10.48550/arXiv.2506.06299>

Centrul Stimson. (8 august 2024). Sesiune RAI: AI și democrație (eveniment). <https://www.stimson.org/event/rai-session-ai-democracy>

Stockwell, S., Hughes, M., Swatton, P., Zhang, A., Hal, J. și Kieran. (2024). Operațiuni de influențare bazate pe inteligență artificială: Protejarea alegerilor viitoare. Institutul Alan Turing (CETaS). <https://cetas.turing.ac.uk/publications/ai-enabled-influence-operations-safeguarding-future-elections>

Tanas, A. (24 octombrie 2024). Președintele Republicii Moldova spune că mita a afectat alegerile, promite un al doilea tur de scrutin. Reuters. <https://www.reuters.com/world/europe/moldova-police-say-businessman-shor-channelled-24-million-pay-off-voters-2024-10-24/>

Institutul Turing / CETaS. (2024). Operațiuni de influență bazate pe inteligență artificială: Protejarea alegerilor viitoare. <https://cetas.turing.ac.uk/publications/ai-enabled-influence-operations-safeguarding-future-elections>

Uribe Burcher, C. (2017). Evaluarea amenințării pe care o prezintă legătura dintre crima organizată și politica democratică: Identificarea factorilor. International Relations and Diplomacy, 5(1). <https://www.davidpublisher.com/index.php/Home/Article/index?id=30183.html>

Uribe Burcher, C. (2019). Criptomonedele și finanțarea politică. International IDEA.

<https://www.idea.int/publications/catalogue/cryptocurrencies-and-political-finance>

Comandamentul Cibernetic al SUA. (12 septembrie 2024). Campania de dezinformare rusească, Doppelgänger, demascată: O rețea de înșelăciuni. <https://www.cybercom.mil/Media/News/Article/3895345/russian-disinformation-campaign-doppelgnger-unmasked-a-web-of-deception>

Departamentul de Justiție al SUA (DOJ). (2024a). Amenințări electorale. <https://www.justice.gov/archives/voting/election-threats>

Departamentul de Justiție al SUA (DOJ). (2024b, 4 septembrie). Departamentul de Justiție al SUA întrerupe o operațiune sub acoperire de influență malignă străină sponsorizată de guvernul rus. <https://www.justice.gov/archives/opa/pr/justice-department-disrupts-covert-russian-government-sponsored-foreign-malign-influence>

Oficiul Directorului Serviciului Național de Informații al SUA (ODNI). (11 martie 2024). Evaluarea anuală a amenințărilor la adresa comunității de informații a SUA. <https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf>

Oficiul Directorului Serviciului Național de Informații al SUA (ODNI). (18 martie 2025). Evaluarea anuală a amenințărilor la adresa comunității de informații a SUA 2025. <https://www.dni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf>

Trezoreria SUA (OFAC). (4 septembrie 2024a). Trezoreria ia măsuri ca parte a unui răspuns al guvernului SUA la operațiunile de influență malignă ale Rusiei în străinătate. <https://home.treasury.gov/news/press-releases/jy2559>

Trezoreria SUA (OFAC). (2024b, 31 decembrie). Trezoreria sancționează entitățile din Iran și Rusia care au încercat să se amestece în alegerile din SUA din 2024. <https://home.treasury.gov/news/press-releases/jy2766>

Institutul V-Dem. (2024). Raportul privind democrația 2024: Democrația câștigă și pierde la vot. <https://v-dem.net/publications/democracy-reports>

Institutul V-Dem. (2025). Autocratizarea devine virală: Raportul privind democrația 2025. <https://v-dem.net/publications/democracy-reports>

Vanderlee, K. și Collier, J. (25 aprilie 2024). Subminarea sondajelor: Amenințări cibernetice la adresa alegerilor globale. Google Cloud / Mandiant. <https://cloud.google.com/blog/topics/threat-intelligence/cyber-threats-global-elections>

Weatherbed, J. (14 noiembrie 2024). Google declară că va înceta să difuzeze reclame politice în UE. The Verge. <https://www.theverge.com/2024/11/14/24296510/google-dropping-political-ads-in-the-eu-ttpa>

Fundația Westminster pentru Democrație (WFD). (2025). Înțelegerea și abordarea costului politicii. <https://www.wfd.org/cost-of-politics>

WHAS11. (8 iulie 2025). Biroul grefierului comitatului Jefferson declară că sistemul de vot rămâne sigur după atacul ransomware. <https://www.youtube.com/watch?v=diY7hpMIY5o>

Wilson, A. (2023). Democrația sub asediu: Abordarea ingerinței Rusiei în Moldova. ECFR. <https://ecfr.eu/article/democracy-under-siege-tackling-russian-interference-in-moldova/>

Centrul Wilson. (19 martie 2025). Alegerile prezidențiale din Ucraina în mijlocul războiului: Provocări politice, juridice și de securitate. <https://www.wilsoncenter.org/blog-post/ukraines-presidential-elections-amid-war-political-legal-and-security-challenges>

08 *Note finale*

- 1 Global Witness, 2025; Meaker, 2023; Rainsford, 2024; McGrath și Alexandru, 2025
- 2 Bay și colab., 2022; Hollis și Ohlin, 2021
- 3 Bay, 2024; SEAE, 2025a
- 4 Bay și colab., 2022; Bay 2024; Levin, 2020; Ohlin, 2020
- 5 Pamment și Tsursumia, 2025
- 6 Oficiul Directorului Serviciului Național de Informații al SUA, 2025; Centrul Canadian
7 pentru Securitate Cibernetică, 2025
- 8 Bay, 2024
- 9 Stockwell și colab., 2024; Csernaton, 2024; Schroeder și colab., 2025
- 10 Stockwell și colab., 2024; Csernaton, 2024; Schroeder și colab., 2025
- 11 Bay, 2024; Hybrid CoE, 2025
- 12 Bay, 2024
- 13 Bay, 2024; Alihodžić, 2023; Centrul pentru un Public Informat și colab., 2021
- 14 International IDEA, 2024
- 15 Bryjka, 2024; OSCE/ODIHR, 2025b; OSCE/ODIHR, 2025c
- 16 Gilbert, 2024
- 17 Centrul pentru un Public Informat și colab., 2021
- 18 Centrul pentru un Public Informat și colab., 2021; International IDEA, 2024; DFRLab,
19 2023; EUvsDisinfo 2024
- 20 Huo, 2024; Hedling, 2025
- 21 Hedling, 2025
- 22 Hoogensen Gjörv & Jalonen, 2023
- 23 Hedling, 2025
- 24 Hedling, 2025
- 25 Oficiul Directorului Serviciului Național de Informații al SUA, 2025
- 26 Pamment și Tsursumia, 2025
- 27 Bay, 2024
- 28 Hoffman, 2022
- 29 Consiliul Atlantic 2023; Pamment și Tsursumia, 2025
- 30 Bay, 2024; Comisia Europeană, 2016; SEAE, 2024; SEAE 2025a; NATO, 2022;
31 NATO, 2025
- 32 SEAE, 2025a; SEAE, 2025b
- 33 cf. Huo, 2024; Pamment și Tsursumia, 2025; Stockwell și colab., 2024
- 34 Pamment și Tsursumia, 2025; Centrul de analiză a amenințărilor Microsoft, 2024a;
35 Centrul de analiză a amenințărilor Microsoft, 2024b
- 36 SEAE, 2025a; Comandamentul Cibernetic al SUA, 2024
- 37 Pamment și Tsursumia, 2025
- 38 EDMO, 2024
- 39 Pamment și Tsursumia, 2025
- 40 EUvsDisinfo, 2024a
- 41 Bjola, 2025; IFES, 2024; Global Witness, 2024
- Chan 2024; Comisia Europeană, 2024
- Clayton, 2014; Consiliul Atlantic, 2018
- Nardelli, 2025
- OSCE/ODIHR, 2024; OSCE/ODIHR, 2025b

42 Kubica, 2024; EUvsDisinfo, 2024b
 43 Tanas, 2024; Balmforth și Dysa, 2024
 44 Antoniuk, 2024; Antoniuk, 2025; Olari, 2024; Olari, 2025a; Olari, 2025b
 45 Kubica, 2024; EUvsDisinfo, 2024a; DFRLab, 2024
 46 Tanas, 2024; Balmforth & Dysa 2024; OSCE/ODIHR 2025; Radio Europa Liberă Moldova, 2024
 47 DFRLab, 2024; EUvsDisinfo, 2024a; Balmforth și Dysa, 2024
 48 McGrath, 2025; IGP, 2025
 49 McGrath, 2025; IGP, 2025
 50 Moldpres, 2025; IGP, 2025
 51 Antoniuk, 2023; Antoniuk, 2024; Antoniuk, 2025; Martin, 2022; OSCE/ODIHR, 2021
 52 Cerulus, 2025; SEAE 2025c; Comisia Europeană 2025c
 53 Pamment și Tsursumia, 2025
 54 Euromaidan Press, 2014; SEAE, 2025a
 55 Hedenskog & Hjelm, 2020; Lopatka, 2024
 56 Clayton, 2014; Consiliul Atlantic, 2018; Euromaidan Press, 2014
 57 ODNI, 2024; ODNI, 2025
 58 FBI, 2024; Reuters, 2024a; Roth, 2024; Trezoreria SUA, 2024a, 2024b
 59 Departamentul de Justiție, 2024b; Centrul de Analiză a Amenințărilor Microsoft, 2024b; Nakamura, Belton și Sommer, 2024
 60 Consiliul Atlantic, 2024; Centrul de Analiză a Amenințărilor Microsoft, 2024a; Reuters, 2024a
 61 Bing și Vicens, 2024; Departamentul de Justiție, 2024a. Gavin, 2025.
 62 Departamentul de Justiție, 2024a; FBI, 2024; Trezoreria SUA, 2024a; 2024b
 63 Kovalčíková și Spatafora, 2024; Grupul operativ național privind crizele electorale, 2025a; Grupul operativ național privind crizele electorale, 2025b; Turing CETaS, 2024
 64 Bay, 2024
 65 Ledford, 2024
 66 Pamment și Tsursumia, 2025
 67 Zuboff, 2019
 68 Cf. Mutu, 2024; Newman, Fletcher, Robertson, Ross Arguedas și Nielsen, 2024
 69 Comisia Europeană, 2024
 70 Weatherbed, 2024; Chan, 2025
 71 Elliott, 2024
 72 O'Brien și Swenson, 2024; Centrul Brennan pentru Justiție, 2024
 73 C2PA, 2024
 74 Google DeepMind, 2025
 75 Newman și colab., 2024
 76 Pamment și Tsursumia, 2025
 77 Bateman & Jackson, 2024; Bay, 2025; Pamment și colab. 2018; Pamment și Isaksson, 2024
 78 OCDE 2021; OCDE 2022
 79 ENISA 2023; International IDEA 2023; Bay 2025
 80 Centrul pentru un Public Informat și colab. 2021
 81 Lewandowsky și colab., 2020
 82 SEAE, 2025
 83 OCDE, 2021
 84 Centrul pentru un Public Informat și colab., 2021; C2PA, 2024; ENISA, 2023
 85 OCDE, 2022
 86 C2PA, 2024; Google DeepMind, 2025
 87 Perdomo și Uribe Burcher, 2017: 128; WFD, 2025
 88 Bakken, 2025; Popescu-Zamfir, 2025; OSCE/ODIHR, 2017: 12; 2021: 16
 89 International IDEA, 2025
 90 OSCE/ODIHR, 2025a: 1–2
 91 Wilson, 2023
 92 Wilson, 2023; OSCE/ODIHR, 2025b: 1
 93 International IDEA, 2025
 94 Perdomo și Uribe Burcher, 2017: 134
 95 CoinGecko, 2025; Lores, 2025; Chainalysis, 2024a

96 Perspective coerente asupra pieței, 2025
 97 Uribe Burcher, 2019: 14
 98 Uribe Burcher, 2019: 13; Chainalysis, 2024b
 99 International IDEA, 2025
 100 Perdomo & Uribe Burcher, 2017: 139; Wolfs, 2025: 3–4
 101 Wolfs, 2025: 5
 102 Agrawal, Hamada și Fernández Gibaja, 2021: 12
 103 Ryan, 2018; Britzky, 2018
 104 DOJ, 2024a
 105 IFES, 2024
 106 OSCE/ODIHR, 2025a: 8–9
 107 Perdomo și Uribe Burcher, 2017: 137–138
 108 Consiliul Europei, 2025: 4
 109 International IDEA, 2025
 110 Wolfs, 2025: 2
 111 Perdomo și Uribe Burcher, 2017: 141
 112 Uribe Burcher, 2019: 7, 9–11
 113 Vasani, James și Holly, 2022
 114 Uribe Burcher, 2019: 15–16
 115 International IDEA, 2025
 116 Perdomo și Uribe Burcher, 2017: 138–139
 117 Uribe Burcher, 2019: 16
 118 Wolfs, 2025: 2
 119 Perdomo și Uribe Burcher, 2017: 144
 120 International IDEA, 2025
 121 V-Dem, 2024; V-Dem, 2025; UNESCO, 2025; Posetti și colab., 2020
 122 Consiliul Europei, 2025; Liberties, 2025; Freedom House, 2024
 123 CIVICUS, 2024; OSCE/ODIHR, 2023
 124 OCDE, 2021; OSCE/ODIHR, 2023
 125 Perdomo și Uribe Burcher, 2017: 136
 126 Europol, 2025a; Hoxhunt, 2025
 127 Bay, 2024
 128 Uribe Burcher, 2017
 129 Europol, 2025a
 130 Cyble, 2024
 131 Deloitte, 2024
 132 Europol, 2025a
 133 Europol 2025a; Deloitte 2024
 134 Must, 2025; ReliaQuest, 2024
 135 ReliaQuest, 2024; Centrul pentru Securitatea Internetului, 2025a
 136 Europol, 2025a
 137 CISA, 2024
 138 CISA, 2024
 139 Hoxhunt, 2025
 140 Forbes 2025
 141 CISA 2024a; NIST 2020; Alianța FIDO 2023; ENISA 2023; MS-ISAC 2024; C2PA 2024
 142 Bay, 2024; ReliaQuest, 2024
 143 Bay și colab., 2022
 144 Bay, 2024
 145 Comisia Electorală a Regatului Unit, 2024
 146 Euromaidan Press, 2014
 147 Alianța pentru Asigurarea Democrației, 2019
 148 Consiliul Europei, 2024; Centrul Wilson, 2025
 149 CNN, 2024a
 150 WHAS11, 2025
 151 Constella Intelligence, 2025
 152 Centrul pentru Securitatea Internetului, 2025a; Centrul pentru Securitatea Internetului, 2025b; Centrul pentru Securitatea Internetului, 2025c

153 Cloudflare, 2025
 154 Saeva și Tasheva, 2024
 155 Bay și colab., 2022; Comitatul San Luis Obispo, 2024
 156 Bay, 2024; ReliaQuest, 2024
 157 Electionline, 2024
 158 Ivanti, 2025
 159 Cyble, 2025
 160 ReversingLabs 2025; ISACA, 2025
 161 ISACA, 2025
 162 Cisco, 202
 163 International IDEA, 2019
 164 Bay, 2024
 165 Google Cloud, 2023
 166 CISA, 2024
 167 Molas, 2024; Analiză a securității cibernetice, 2024
 168 Centrul Stimson, 2024
 169 International IDEA 2019; Bay 2024; Google Cloud 2023; CISA 2024a;
 Centrul Stimson 2024
 170 cf. Microsoft, 2025
 171 Vanderlee și Collier, 2024; NCSC, 2025
 172 Bay, 2024; International IDEA, 2023
 173 Centrul pentru Securitatea Internetului 2025a; NIST, 2022; NIST, 2024
 174 CrowdStrike 2025a; NIST, 2020; NIST, 2023
 175 CISA, 2024b; CrowdStrike, 2025b
 176 CISA & EAC, 2024a; CISA & EAC, 2024b; CISA, 2024b
 177 Bay, 2024; Bay, 2025
 178 Bay, 2024
 179 Canada, 2025
 180 Bay, 2024
 181 Bay, 2024
 182 Comisia Europeană, 2016; Comisia Europeană, 2025b
 183 Bay, 2024; Bay, 2025
 184 Bay, 2025
 185 GAO, 202
 186 Universitatea Columbia, 2025
 187 Alegeri Canada, 2025
 188 Guvernul Canadei, 2025; PCO, 2025
 189 Canada, 2025, CISA 2025
 190 Cf Bay, 2025
 191 Hybrid CoE, 2024
 192 Bay, 2025; Canada, 2025
 193 Comisia Europeană, 2025b
 194 Bay, 2024; Alegeri Canada, 2025
 195 Comisia Europeană, 2025b
 196 Comisia Europeană, 2025a
 197 NATO, 2024; Alegeri Canada, 2025
 198 International IDEA, 2025; Centrul Carter, 2025
 199 Oficiul Directorului Serviciului Național de Informații al SUA, 2025; Pamment și Tsurtsu
 mia, 2025
 200 Pamment și Tsursumia, 2025
 201 Stockwell și colab., 2024; CISA, 2024a
 202 IFES 2024; Bay, 2024
 203 Centrul Brennan pentru Justiție, 2020; Elliott, 2024; Comisia Europeană, 2024;
 C2PA, 2024; Pamment și Tsursumia, 2025

Academia Folke Bernadotte (FBA) este agenția guvernamentală suedeză pentru pace, securitate și dezvoltare. Ca parte a cooperării internaționale pentru dezvoltare a Suediei, promovăm pacea în țările afectate de conflicte. Oferim instruire și consiliere și efectuăm cercetări pentru a susține consolidarea păcii și guvernarea, în contexte de pace și securitate. Mai mult decât atât, detașăm personal civil în operațiuni de pace și misiuni de observare a alegerilor conduse în principal de ONU, UE și OSCE. Agenția este numită după contele Folke Bernadotte, primul mediator de pace al ONU.

Dacă doriți să aflați mai multe despre FBA, ne puteți găsi pe:

-  [linkedin.com/FolkeBernadotteAcademy](https://www.linkedin.com/FolkeBernadotteAcademy)
-  [instagram.com/FolkeBernadotteAcademy](https://www.instagram.com/FolkeBernadotteAcademy)
-  [facebook.com/FolkeBernadotteAcademy](https://www.facebook.com/FolkeBernadotteAcademy)
-  [soundcloud.com/FolkeBernadotteAcademy](https://www.soundcloud.com/FolkeBernadotteAcademy)

www.fba.se