DE LA ANALIZĂ LA PREDICȚIE – DEZVOLTAREA UNUI MODEL PREDICTIV INTEGRAT PENTRU EVALUAREA RISCULUI DE APARIȚIE A AMENINȚĂRILOR HIBRIDE –

Colonel prof. univ. dr. habil. ing. Cezar VASILESCU

Conf. univ. dr. Aura CODREANU

Departamentul Regional de Studii pentru Managementul Resurselor de Apărare, Brașov;
Universitatea Națională de Apărare „Carol I”, București

10.55535/GMR.2024.4.34

This article analyses the common patterns of recent hybrid threats, highlighting some representative cases such as: the information warfare during the US elections (2020), the COVID-19 vaccine disinformation campaign (2020-2021), and the energy crisis in Europe (2021-2022), in order to identify the existence of potential synergies between different tactics (cyber, information, economic) depending on the specific context. On the basis of these patterns, the article proposes the essential parameters of a predictive hybrid threat analysis model (including geopolitical, cyber, economic, social, media, political and technological factors) with the aim of facilitating proactive responses to this type of threats in modern society.

Keywords: hybrid threats; disinformation; modern conflicts; economic pressure; cyber-warfare operations;

INTRODUCERE

În ultimele decenii, mediul de securitate internațional a suferit transformări majore, devenind din ce în ce mai complex și imprevizibil. În prezent, acesta este definit de instabilitate și incertitudine și este influențat de o serie de factori globali (digitalizarea rapidă a societății, interconectarea economiilor naționale, creșterea complexității și interconectivității între state, intensificarea competiției pentru resurse strategice și influență geopolitică, precum și volatilitatea politică), care au determinat apariția de noi vulnerabilități, exploatabile de actori statali și non-statali.

Aceștia își ajustează continuu tacticile folosite pentru a exploata aceste vulnerabilități, având în vedere că utilizarea unor elemente hibride oferă un avantaj semnificativ: costuri relativ reduse, risc minimizat și o probabilitate mai mică de a genera un răspuns militar pe scară largă (Pindják, 2019). De exemplu, utilizarea rețelelor sociale și a altor platforme de comunicare digitală a devenit un instrument esențial în campaniile de influențare și destabilizare (Galeotti, 2019).

În acest context, la nivel global, amenințările hibride au devenit un instrument preferat pentru subminarea stabilității statelor și regiunilor. Spre deosebire de conflictele armate convenționale, aceste amenințări se manifestă sub forme multiple, implicând o combinație de instrumente și metode care vizează atât domeniul militar, cât și pe cel non-militar, cibernetic și informațional (Hoffman, 2007).

Aceste amenințări hibride combină tehnici și tactici neconvenționale multiple (de la atacuri cibernetice împotriva infrastructurilor critice – cum ar fi cele din domeniul sănătății sau al energiei – la campanii de dezinformare și exercitarea de presiuni economice) într-un mod integrat și subtil, în scopul slăbirii stabilității naționale, fără însă a declanșa un răspuns militar tradițional. Un aspect comun al acestor cazuri este *utilizarea unei sinergii între mai multe forme de agresiune*, ceea ce complică procesul de detectare și contracararea acestora.

Conceptul de *„amenințare hibridă”* nu este unul nou, dar utilizarea sa în mod formal în literatura de securitate a crescut exponențial în ultimul deceniu, în special în contextul conflictelor moderne. Amenințările hibride sunt definite ca o combinație de metode convenționale și neconvenționale, incluzând operațiuni de război cibernetic, dezinformare, atacuri economice și tactici de influențare politică și socială. Potrivit unui raport al NATO, amenințările hibride sunt caracterizate

prin *„Utilizarea coordonată și sincronizată a diferitelor mijloace și activități, menite să exploateze vulnerabilitățile societăților și să submineze stabilitatea politică și economică a statelor-țintă”* (NATO, 2020). Acestea se manifestă într-un *„spațiu gri”* al conflictului, unde este dificil să se distingă între pace și război, iar actorii responsabili rămân adesea nedetectați sau fără a putea fi identificați oficial (Mumford, 2021).

De asemenea, Hoffman (2007) definește amenințările hibride ca fiind *„O sinteză a metodelor convenționale și neconvenționale, incluzând terorismul, insurgențele și războiul cibernetic, care sunt combinate într-o singură campanie integrată”*. O altă definiție este oferită de Rid și Hecker (2021) conceptului de amenințări hibride, acestea fiind *„Operațiuni care combină atacuri cibernetice cu alte forme de agresiune, inclusiv presiuni economice și dezinformare”*, accentuând dimensiunea multisectorială a acestora. Consecința imediată a integrării unor domenii multiple de acțiune este aceea că răspunsul la astfel de amenințări devine o sarcină dificilă și provocatoare.

Una dintre caracteristicile fundamentale ale amenințărilor hibride este utilizarea unei game largi de tactici într-o manieră sinergică. Această abordare permite actorilor să exploateze vulnerabilitățile pe mai multe fronturi simultan, creând, astfel, o presiune multidimensională asupra țintei. Sinergia între tactici cibernetice, informaționale și economice a devenit un element definitoriu în conflictele hibride recente. Pentru exemplificare, atacurile cibernetice pot fi coordonate cu campanii de dezinformare pentru a amplifica efectele destabilizatoare, în timp ce presiunile economice pot fi utilizate pentru a slăbi reziliența statelor.

Conform studiilor realizate de Wither (2016), sinergia acestor amenințări se caracterizează prin integrarea și coordonarea mai multor domenii (inclusiv cel cibernetic, informațional și economic). Conform acestora, elementul esențial în definirea unei amenințări hibride este faptul că acestea profită de vulnerabilitățile unui stat-țintă, în special în contextul diviziunilor sociale, economice și politice. Astfel, în timp ce natura atacurilor poate varia, scopul lor comun este destabilizarea ordinii și slăbirea capacităților de răspuns ale țintelor.

În acest context, ipoteza fundamentală aferentă primei părți a acestei lucrări este aceea că *„Amenințările hibride utilizează o combinație de tactici cibernetice, informaționale și economice adaptate contextului specific al fiecărui stat-țintă, iar succesul acestora depinde de gradul de integrare și sincronizare a acestor tactici, a căror sinergie amplifică impactul destabilizator”*.

Pentru a testa această ipoteză, cercetarea va folosi o metodă de analiză comparativă a mai multor cazuri recente de amenințări hibride, selectate pe baza relevanței și a impactului lor geopolitic. Prin analiza acestor cazuri, vom proceda

la *identificarea tiparelor specifice fiecăruia și vom identifica eventualele tipare comune*. De asemenea, vom analiza modul în care tactici diverse (cibernetice, informaționale, economice) au fost combinate și coordonate pentru a atinge obiectivele actorilor implicați.

Această ipoteză presupune că tacticile hibride nu sunt utilizate izolat, ci în mod sinergic (Otaiku, 2018), adaptate la vulnerabilitățile specifice fiecărui stat, fie că acestea sunt economice (precum sancțiunile sau crizele energetice), informaționale (campanii de dezinformare și propagandă) sau cibernetice (atacuri asupra infrastructurii critice).

Printre sursele principale utilizate în această analiză în vederea testării validității ipotezei fundamentale se numără studii și rapoarte recente ale NATO (2020), precum și lucrări teoretice și empirice asupra amenințărilor hibride (Hoffman, 2007; Wither, 2016; Pindjak, 2014 și 2019; Galeotti, 2019; Rid, Hecker, 2021).

În ultimă instanță, vom căuta să demonstrăm că atingerea obiectivelor acestor amenințări hibride este condiționată de coordonarea între domenii multiple și de adaptarea tacticilor la vulnerabilitățile specifice fiecărei ținte.

ANALIZA COMPARATIVĂ A AMENINȚĂRILOR HIBRIDE

Studiul amenințărilor hibride reprezintă o provocare majoră pentru cercetarea în domeniul securității internaționale, dată fiind complexitatea acestora și capacitatea lor de a se adapta rapid la schimbările din mediul de securitate global. Prin analiza comparativă a mai multor cazuri recente și identificarea tiparelor comune de acțiune, această cercetare își propune să ofere o mai bună înțelegere a mecanismelor care stau la baza acestor amenințări și să contribuie la dezvoltarea unor strategii eficiente de contracarare.

În paragrafele următoare vom examina pe scurt fiecare dintre cazurile selectate pentru analiză, folosind ca parametri scopul, tacticile utilizate, vulnerabilitățile exploatate și tiparele identificate.

A. Războiul informațional în timpul alegerilor din SUA (2020) (National Intelligence Council, 2021; Wojnowski, 2021; Menn, 2020).

- Scop: Subminarea încrederii în procesul electoral american și destabilizarea politică
- Tactici utilizate:
  - Dezinformare și propagandă: răspândirea masivă de teorii ale conspirației și informații false privind fraude electorale.
  - Atacuri cibernetice: tentative de hacking asupra sistemelor electorale și a infrastructurii critice.

  - Exploatarea diviziunilor sociale: amplificarea tensiunilor rasiale și politice prin intermediul conturilor false create pe rețelele sociale.
- Vulnerabilități exploatate:
  - Polarizarea politică: diviziunea profundă între partidele politice și grupurile sociale din SUA.
  - Încrederea scăzută în instituțiile publice: deja existentă, fiind amplificată de campaniile de dezinformare.
  - Dependința de platformele sociale: vulnerabilități în rețelele sociale folosite pentru răspândirea rapidă a dezinformării.
- Tipare identificate:
  - Coordonare multimodală: utilizarea combinată a tehnicilor online (dezinformare și atacuri cibernetice) și offline – ca rezultat al primelor (proteste și tensiuni sociale).
  - Scopuri pe termen lung: crearea unei atmosfere de neîncredere generalizată în instituțiile democratice.

B. Campania de dezinformare împotriva vaccinurilor COVID-19 (2020-2021) (Tsiklauri, 2021; Suarez-Lledo et al., 2021; Stokel-Walker, 2024)

- Scop: Slăbirea răspunsului global la pandemie și amplificarea neîncrederii în autoritățile sanitare.
- Tactici utilizate:
  - Răspândirea dezinformării: informații false despre eficacitatea și siguranța vaccinurilor au fost amplificate pe rețelele sociale.
  - Exploatarea fricilor și a emoțiilor: mesaje care au exploatat teama de necunoscut și suspiciunile față de guverne și corporații.
  - Alianțe informale: utilizarea unor canale de media alternative și influenceri pentru a răspândi mesaje anti-vaccinare.
- Vulnerabilități exploatate:
  - Neîncrederea în autoritățile sanitare: frica și confuzia legate de un nou virus și vaccinuri.
  - Accesul necontrolat la informații pe platformele sociale: a permis propagarea rapidă a teoriilor conspiraționiste.
  - Fragmentarea ecosistemului informațional: accesul la canale alternative de informare, care subminează consensul științific.
- Tipare identificate:
  - Fragmentarea informațională: crearea și alimentarea de ecosisteme informaționale alternative care subminează consensul științific.

  - Timpul ca factor critic: utilizarea perioadelor critice (începutul campaniei de vaccinare) pentru a maximiza impactul negativ.

C. Criza energetică din Europa (2021-2022) (Gilbert et al., 2021; Popkostova, 2022; Gross et al., 2024)

- Scop: Exercitarea de presiune politică asupra Europei pentru a influența pozițiile geopolitice și economice ale statelor membre.
- Tactici utilizate:
  - Manipularea prețurilor energiei: reducerea deliberată a livrărilor de gaze naturale, creând, astfel, o criză a prețurilor la energie.
  - Presiuni economice: amenințări cu întreruperea completă a livrărilor în contextul tensiunilor politice.
  - Dezinformare și mesaje media: amplificarea narativelor care învinovățesc guvernele europene pentru criza energetică, divizând, astfel, opinia publică.
- Vulnerabilități exploatate:
  - Dependența energetică de Rusia: statele europene erau vulnerabile din cauza dependenței de gazele naturale rusești.
  - Structura economică și fragilitatea sectorului energetic: lipsa alternativelor imediate pentru aprovizionarea cu energie.
  - Sensibilități politice interne: creșterea nemulțumirii publice legate de costurile ridicate ale energiei.
- Tipare identificate:
  - Influență economică: utilizarea resurselor economice critice ca armă geopolitică.
  - Sincronizarea acțiunilor: coordonarea între diversele tactici hibride (economice, informaționale) pentru a maximiza impactul.

D. Interferențele cibernetice în campania electorală din Franța (2017) (Vilmer et al., 2018; O'Connor et al., 2020; Ferrara, 2017)

- Scop: Subminarea procesului electoral și influențarea rezultatului alegerilor prezidențiale.
- Tactici utilizate:
  - Atacuri cibernetice: piratarea și publicarea unor emailuri și documente sensibile ale echipei de campanie a candidatului Emmanuel Macron.
  - Dezinformare: răspândirea de informații false și teorii ale conspirației pe rețelele sociale și în media, cu scopul de a discredita candidatul favorizat de Occident.
  - Amplificarea mesajelor: utilizarea rețelelor de social media și a conturilor false pentru a amplifica impactul dezinformării.

- Vulnerabilități exploatate:
  - Infrastructura cibernetică slab protejată: distemele politice și de campanie vulnerabile la atacuri cibernetice.
  - Perioada electorală tensionată: atacurile au fost coordonate în momente cheie, când destabilizarea putea avea cel mai mare impact.
  - Propagarea rapidă a dezinformării online: utilizarea eficientă a rețelelor sociale pentru a amplifica informațiile exfiltrate.
- Tipare identificate:
  - Atacuri cibernetice concertate: coordonarea dintre hacking și diseminarea rapidă a informațiilor pentru a provoca haos înainte de vot.
  - Targetarea perioadei pre-electorale: exploatarea perioadei sensibile dinaintea alegerilor pentru a maximiza impactul destabilizator.

E. Operațiuni hibride în Ucraina (2014-prezent) (Starodubtseva, 2021; Wentzell, 2021; Nübel, 2020)

- Scop: Dezmembrarea integrității teritoriale a Ucrainei și influențarea deciziilor politice.
- Tactici utilizate:
  - Agresiune militară neconvențională: utilizarea de trupe fără însemne, cunoscute sub denumirea de *„omuleții verzi”*, pentru a prelua controlul asupra Crimeei.
  - Dezinformare și propagandă: crearea și diseminarea narativelor care justificau intervenția și creau confuzie cu privire la evenimentele din teren.
  - Presiuni economice: folosirea dependenței Ucrainei de gazele naturale rusești pentru a exercita presiuni politice.
- Vulnerabilități exploatate:
  - Diviziuni etnice și politice: exploatarea tensiunilor dintre regiunile estice proruse și restul Ucrainei.
  - Dependența energetică de Rusia: Ucraina era vulnerabilă din cauza dependenței de gazele rusești.
  - Slăbiciuni militare și politice: lipsa unei pregătiri militare și a unui consens politic intern în fața agresiunii.
- Tipare identificate:
  - Utilizarea combinată de mijloace militare și informaționale: combinația de tactici militare subtile cu o campanie puternică de dezinformare pentru a crea ambiguitate și a preveni o reacție internațională unitară.

  - Presiune asupra resurselor critice: utilizarea resurselor energetice ca pârghie economică pentru a influența deciziile politice ale statului țintă.

F. Criza migrantă în Europa (2015-2016) (Kuvekalović et al., 2017; Braghiroli et al., 2026; Karolewski et al., 2018)

- Scop: Destabilizarea statelor europene prin exacerbarea crizei migrației și amplificarea tensiunilor sociale.
- Tactici utilizate:
  - Manipularea fluxurilor migratorii: facilitarea sau direcționarea fluxurilor de migranți către granițele europene, folosind rețele de trafic de persoane și oferind stimulente.
  - Dezinformare și influențare media: răspândirea dezinformării privind natura și motivele crizei migratorii, amplificând fricile și tensiunile sociale în țările gazdă.
  - Exploatarea vulnerabilităților sociale: alimentarea sentimentelor xenofobe și anti-imigrație în rândul populației europene, divizând, astfel, societățile și punând presiune pe guvernele locale.
- Vulnerabilități exploatate:
  - Lipsa unei politici comune de migrație: Europa era vulnerabilă din cauza lipsei unui mecanism unitar de gestionare a crizei migratorii.
  - Tensiunile sociale și frica de imigrație: exacerbarea sentimentului xenofob în rândul populațiilor europene.
  - Expunerea la dezinformare: folosirea mass-mediei și a rețelelor sociale pentru amplificarea percepției unei crize majore.
- Tipare identificate:
  - Exploatarea crizelor umanitare: utilizarea unor crize umanitare reale pentru a destabiliza statele țintă prin crearea de diviziuni sociale și politice.
  - Amplificare media: folosirea mass-mediei și a rețelelor sociale pentru a amplifica percepția unei crize mult mai grave decât realitatea, intensificând reacțiile publicului.

G. Criza migranților la granița Poloniei și Belarusului (2021) (Zdanowicz, 2023; Bodnar et al., 2023; Jędrzejczyk-Kuliniak, 2023)

- Scop: Destabilizarea Uniunii Europene și crearea tensiunilor interne prin utilizarea migranților ca instrument de presiune politică.
- Tactici utilizate:
  - Migrație forțată: Belarus a orchestrat fluxuri de migranți către granițele UE, în special Polonia, pentru a crea o criză umanitară și a forța o reacție.

- Propagandă: utilizarea mass-mediei controlate de stat pentru a învinui UE de criza umanitară, în timp ce Belarus a negat orice implicare.
- Diplomație coercitivă: amenințarea cu escaladarea crizei dacă cerințele politice nu sunt îndeplinite, inclusiv sancțiunile împotriva regimului lui Lukashenko.

• Vulnerabilități exploatate:
- Granițe slab controlate: lipsa, la acea dată, a unei infrastructuri solide de control al frontierei la granița Poloniei cu Belarus.
- Tensiunile interne din UE: exploatarea divergențelor din UE privind politica de migrație.
- Reacția lentă a autorităților: UE a reacționat încet la manipularea migrației de către Belarus.

• Tipare identificate:
- Migrație ca armă de destabilizare: folosirea fluxurilor de migranți pentru a exercita presiune politică asupra unei entități regionale.
- Combinația dintre coercitivitate și propagandă: amplificarea unei crize create artificial prin campanii de dezinformare și propagandă.

H. Intervenția în Referendumul pentru independența Cataloniei (2017) (Vakarchuk, 2020; Arcos, 2021; Barberà, 2020)

• Scop: Amplificarea diviziunilor regionale și slăbirea unității naționale a Spaniei.

• Tactici utilizate:
- Dezinformare și manipulare: răspândirea de narative care susțineau independența Cataloniei și încurajau confruntarea între guvernul central și separatiști.
- Atacuri cibernetice: sabotarea site-urilor și a infrastructurii digitale asociate cu guvernul spaniol pentru a îngreuna răspunsul la criza politică.
- Proteste și agitație socială: încurajarea și organizarea de proteste masive și acțiuni de nesupunere civilă pentru a amplifica tensiunile sociale.

• Vulnerabilități exploatate:
- Tensiunile naționaliste și regionale: conflictul istoric dintre Catalonia și guvernul central spaniol.
- Slăbiciunile instituționale: guvernul central a avut dificultăți în gestionarea crizei, ceea ce a agravat tensiunile.
- Expunerea la dezinformare: exploatarea narativelor naționaliste și a campaniilor de dezinformare pentru a alimenta protestele.

• Tipare identificate:
- Exploatarea diviziunilor politice regionale: focusul pe tensiunile naționaliste regionale pentru a destabiliza statul național.
- Sinergia între dezinformare și mobilizare socială: combinarea dezinformării cu acțiuni sociale directe pentru a crea o criză politică majoră.

I. Intervenția în criza politică din Venezuela (2019) (Rouvinski, 2019; Aulia et al., 2024; Rozental et al., 2022)

• Scop: Influențarea echilibrului politic în favoarea guvernului de la Caracas, în ciuda opoziției internaționale.

• Tactici utilizate:
- Dezinformare internațională: răspândirea de narative care legitimau guvernul lui Nicolás Maduro și delegitimau opoziția sprijinită de Occident.
- Intervenție economică și sancțiuni: folosirea resurselor economice și a relațiilor comerciale pentru a susține regimul în fața sancțiunilor internaționale.
- Alianțe și suport militar: oferirea de suport militar și logistic prin aliați externi pentru a menține controlul regimului.

• Vulnerabilități exploatate:
- Economia fragilă: criza economică severă din Venezuela a fost un teren fertil pentru manipulări și dezinformare.
- Polarizarea politică: divizarea adâncă între susținătorii regimului și opoziție.
- Izolarea internațională: regimul a profitat de sprijinul unor state externe, contracarând sancțiunile internaționale.

• Tipare identificate:
- Sancțiuni și contramăsuri economice: utilizarea mijloacelor economice pentru a contracara sancțiunile și a sprijini stabilitatea regimului.
- Război informațional: o campanie globală de dezinformare care vizează nu doar publicul local, ci și percepția internațională a crizei politice.

J. Amenințările hibride din Venezuela (2019-prezent) (Cañizález et al., 2020; Beaton, 2021; Chaguaceda et al., 2023)

• Scop: Menținerea regimului lui Nicolás Maduro în fața crizei economice și politice, precum și a presiunii internaționale.

• Tactici utilizate:
- Reprimarea internă: utilizarea forțelor de securitate pentru a suprima protestele și a neutraliza opoziția politică.

- Controlul informației: restricționarea accesului la informații prin cenzură, controlul mass-mediei și limitarea accesului la internet.
- Dezinformare: răspândirea narativelor care blamează puteri străine pentru criza economică și politică, astfel consolidând sprijinul intern.

- Vulnerabilități exploatate:
  - Sistem politic autoritar: folosirea represiunii și a controlului informațional pentru a rămâne la putere.
  - Dependența de resurse: controlul asupra resurselor naturale (petrol) a permis regimului să reziste sancțiunilor.
  - Slăbiciunea opoziției: fragmentarea și lipsa unui lider puternic al opoziției au fost exploatate de regim.
- Tipare identificate:
  - Represiune internă și controlul informației: utilizarea simultană a forței și a cenzurii pentru a menține controlul asupra populației.
  - Dezinformare pentru legitimarea regimului: răspândirea dezinformării pentru a contracara criticile internaționale și a mobiliza sprijinul intern.

K. Criza politică din Belarus (2020-prezent) (Hardy, 2022; Giannakopoulou, 2022; Astapova et al., 2022)

- Scop: Menținerea regimului lui Alexander Lukașenko în fața presiunilor interne și externe pentru schimbare.
- Tactici utilizate:
  - Represiune și violare a drepturilor omului: folosirea forței împotriva protestatarilor și activiștilor pro-democrație pentru a suprima mișcările de opoziție.
  - Dezinformare: Propagarea narativelor care delegitimau mișcările de opoziție și prezentau regimul ca fiind singura forță stabilizatoare.
  - Sprijin extern: recursul la suport din partea Rusiei, inclusiv sprijin militar și economic, pentru a menține regimul în fața sancțiunilor internaționale.
- Vulnerabilități exploatate:
  - Existența unui sistem autoritar: Lukașenko a folosit represiunea și dezinformarea pentru a suprima mișcările de opoziție.
  - Dependența de Rusia: vulnerabilitatea Belarusului la influența economică și militară a Rusiei.
  - Tensiunile sociale interne: exploatarea fricii de schimbare în rândul populației conservatoare.

- Tipare identificate:
  - Represiune internă combinată cu dezinformare: utilizarea simultană a forței brute și a dezinformării pentru a descuraja opoziția și a păstra controlul.
  - Suport extern pentru stabilitate: dependența de sprijinul unui aliat puternic pentru a supraviețui presiunii internaționale și interne.

L. Influența Chinei în Asia de Sud-Est (2020-prezent) (Schmidt, 2008; Pal, 2021; Ferchen et al., 2023)

- Scop: Extinderea influenței economice și politice a Chinei în regiune și contracararea influenței occidentale.
- Tactici utilizate:
  - Diplomație coercitivă: utilizarea pârghiilor economice, cum ar fi investițiile și datoriile, pentru a exercita influență politică asupra statelor din Asia de Sud-Est.
  - Dezinformare și propagandă: promovarea narativelor favorabile Chinei în regiune, prin mass-media controlată de stat și prin rețelele sociale.
  - Activități maritime agresive: extinderea pretențiilor teritoriale în Marea Chinei de Sud prin construirea de insule artificiale și militarizarea zonei.
- Vulnerabilități exploatate:
  - Dependența economică: statele din Asia de Sud-Est sunt vulnerabile din cauza datoriilor și a prezenței investițiilor chineze.
  - Conflictele teritoriale: statele din regiune sunt vulnerabile din cauza disputelor teritoriale din Marea Chinei de Sud.
  - Slăbiciuni democratice: regimurile mai slabe sau autoritare sunt ușor de influențat prin pârghii economice.
- Tipare identificate:
  - Folosirea puterii economice ca armă politică: utilizarea dependențelor economice create prin investiții și împrumuturi pentru a controla deciziile politice ale altor state.
  - Agresiune non-militară și militară: combinarea tacticilor economice cu prezența militară pentru a domina o regiune strategică și a limita influența rivalilor.

M. Interferența Chinei în politica Taiwanului (2019-prezent) (Chang et al., 2021; Hung et al., 2022; Hartnett et al., 2021)

- Scop: Subminarea independenței politice a Taiwanului și reducerea sprijinului internațional pentru guvernul de la Taipei.

- Tactici utilizate:
  - Dezinformare: răspândirea de știri false și teorii ale conspirației pentru a slăbi încrederea cetățenilor taiwanezi în guvernul lor.
  - Atacuri cibernetice: atacuri asupra instituțiilor guvernamentale și a infrastructurii critice din Taiwan pentru a destabiliza sistemul politic și economic.
  - Presiune economică: restricționarea accesului Taiwanului la piețele internaționale și presiuni asupra altor state să nu recunoască suveranitatea taiwaneză.
- Vulnerabilități exploatate:
  - Dependența economică: Taiwanul este vulnerabil la presiunea economică exercitată de China asupra partenerilor comerciali.
  - Izolarea diplomatică: Taiwanul are puțini aliați internaționali și este supus unei presiuni constante din partea Chinei.
  - Tensiuni politice interne: exploatarea diviziunilor politice interne din Taiwan.
- Tipare identificate:
  - Sinergia între atacuri cibernetice și dezinformare: utilizarea combinată a atacurilor cibernetice și a campaniilor de dezinformare pentru a destabiliza un regim democratic.
  - Presiune economică pentru izolare politică: folosirea influenței economice pentru a limita sprijinul internațional al unei țări țintă.

N. Criza politică și de securitate din Mali (2012-prezent) (Thurston et al., 2013; Cox et al., 2018; Maza et al., 2020)

- Scop: Menținerea puterii și a controlului asupra resurselor naturale prin destabilizarea regiunii și limitarea influenței guvernului central și a forțelor internaționale de menținere a păcii.
- Tactici utilizate:
  - Insurgență și terorism: grupările jihadiste folosesc tactici de gherilă, atentate și răpiri pentru a destabiliza regiunea.
  - Dezinformare și propagandă: răspândirea ideologiei extremiste prin rețele sociale și canale locale, consolidând sprijinul populației pentru grupurile insurgente.
  - Exploatarea vulnerabilităților sociale: manipularea tensiunilor etnice și religioase pentru a fragmenta coeziunea socială și a slăbi guvernul.

- Vulnerabilități exploatate:
  - Slăbiciunea guvernului central: guvernul malian nu a putut să controleze toate regiunile țării.
  - Tensiuni etnice și religioase: exploatarea rivalităților tribale și etnice din Mali.
  - Prezența grupurilor extremiste: vulnerabilitatea la influența grupurilor jihadiste active în regiune.
- Tipare identificate:
  - Combinarea insurgenței cu dezinformarea: sinergia între operațiunile de teren și propaganda online pentru a recruta și a legitima acțiunile violente.
  - Exploatarea diviziunilor sociale: utilizarea conflictelor etnice și religioase pentru a intensifica instabilitatea și a împiedica formarea unui guvern centralizat eficient.

O. Campania de interferență cibernetică a Iranului (2018-prezent) (Spataro, 2019; Elswah et al., 2021; Lehto, 2022)

- Scop: Subminarea stabilității politice a inamicilor și obținerea de avantaje strategice prin atacuri cibernetice și dezinformare.
- Tactici utilizate:
  - Atacuri cibernetice: Iranul a orchestrat atacuri asupra infrastructurii critice din SUA și aliații săi, inclusiv rețele energetice și sisteme financiare.
  - Furt de proprietate intelectuală: sustragerea de date sensibile și proprietate intelectuală din industrii critice pentru dezvoltarea propriilor capacități tehnologice.
  - Campanii de dezinformare: lansarea de campanii online pentru a răspândi narative pro-iraniene și a discredita guvernele occidentale.
- Vulnerabilități exploatate:
  - Infrastructura critică neprotejată: sistemele cibernetice din SUA și alte țări aliate erau expuse la atacuri cibernetice.
  - Proprietatea intelectuală slab protejată: Iranul a exploatat sistemele neprotejate pentru a sustrage date critice.
  - Percepția negativă a guvernelor occidentale: amplificarea narativelor anti-occidentale.
- Tipare identificate:
  - Agresiune cibernetică strategică: folosirea persistentă a atacurilor cibernetice pentru a destabiliza adversarii și a obține beneficii economice și militare.

- Dezinformare ca suport pentru acțiuni cibernetice: răspândirea dezinformării pentru a amplifica efectele atacurilor cibernetice și a crea confuzie în rândul populației țintă.

P. Influența Rusiei în Balcanii de Vest (2014-prezent) (Lika, 2021; Cipan et al., 2024; Kase, 2024)

- Scop: Împiedicarea integrării statelor din Balcanii de Vest în UE și în NATO și menținerea sferei de influență rusească în regiune.
- Tactici utilizate:
  - Sprijinirea partidelor pro-ruse: susținerea financiară și logistică a partidelor și mișcărilor politice pro-ruse pentru a influența politicile naționale.
  - Dezinformare: răspândirea dezinformării pentru a delegitima Uniunea Europeană și NATO, promovând în același timp narative pro-ruse.
  - Tensiuni etnice și religioase: exploatarea sensibilităților etnice și religioase pentru a crea instabilitate și a împiedica cooperarea regională.
- Vulnerabilități exploatate:
  - Instabilitatea politică: regiunile din Balcani au fost marcate de conflicte etnice și politice aflate în stare latentă.
  - Dependența energetică: statele balcanice depind de gazele naturale rusești.

Slăbiciuni economice și corupție: exploatarea sărăciei și corupției pentru a câștiga influență.

- Tipare identificate:
  - Influență politică prin suport financiar: utilizarea sprijinului material pentru a influența direct politicile interne ale statelor țintă.
  - Exacerbarea diviziunilor sociale: folosirea tensiunilor istorice și etnice pentru a preveni integrarea europeană și a destabiliza regiunea.

*

Analiza acestor cazuri permite evidențierea câtorva tipare comune în utilizarea amenințărilor hibride, care subliniază natura complexă a acestora, după cum urmează:

- **Sinergie între diverse domenii de acțiune:** În toate cazurile analizate au fost combinate mai multe tipuri de acțiuni/tactici (cibernetice, informaționale, economice) pentru a crea presiune multidimensională asupra adversarilor și pentru a putea fi atinse obiectivele propuse. Aceasta sinergie este esențială pentru eficiența unei amenințări hibride.

- **Exploatarea** și manipularea c**rizelor existente sociale și/sau politice:** Fie că este vorba de crize politice, economice sau teritoriale, au fost exploatate vulnerabilitățile sociale și psihologice (cum ar fi frica, diviziunile politice sau neîncrederea în instituții) pentru a destabiliza statele țintă.
- **Propagandă și dezinformare ca tactică cheie:** Au fost utilizate pe scară largă propaganda și dezinformarea, cu scopul de a modela percepțiile publice și a legitima acțiuni internaționale discutabile. Controlul și manipularea informației au fost esențiale pentru a influența percepțiile și a destabiliza societatea.
- **Flexibilitate și adaptabilitate:** Cazurile analizate au demonstrat capacitatea actorilor din spatele amenințărilor hibride de a se adapta rapid la situații în schimbare, utilizând mijloace diferite în funcție de contextul specific (de exemplu, creșterea atacurilor cibernetice în timpul unei campanii electorale sau manipularea pieței energetice în contextul unei crize politice).
- **Influență pe termen lung:** Majoritatea acțiunilor hibride analizate au fost concepute pentru a avea efecte pe termen lung, vizând destabilizarea graduală a încrederii în instituții și în alianțe internaționale.

*

În ceea ce privește tacticile hibride utilizate, constatăm că acestea nu au fost folosite izolat, ci în mod sinergic. Astfel, în *tabelul 1* prezentăm o sinteză a acestora, cu scopul de a identifica modul în care au fost combinate și coordonate pentru a atinge obiectivele actorilor implicați și tipul de sinergie aplicat.

*Tabelul 1: Tactici hibride utilizate pentru fiecare caz analizat **în parte*** (concepția autorilor)

Amenințare hibridă	**Tactici utilizate**			**Tip sinergie**
	cibernetice (C)	**informaționale (I)**	**economice (E)**	
Războiul informațional în timpul alegerilor din SUA (2020)	Atacuri cibernetice asupra infrastructurii electorale	Campanii de dezinformare și propagandă	-	C-I

Amenințare hibridă	Tactici utilizate			Tip sinergie
	cibernetice (C)	informaționale (I)	economice (E)	
Campania de dezinformare împotriva vaccinurilor COVID-19 (2020-2021)	-	Dezinformare și propagandă privind eficacitatea și siguranța vaccinurilor prin mesaje anti-vaccinare	-	I
Criza energetică din Europa (2021-2022)	-	Dezinformare și mesaje media care blamează guvernele europene	Manipularea prețurilor energiei și presiuni economice	I-E
Interferențele cibernetice în campania electorală din Franța (2017)	Atacuri cibernetice asupra echipei de campanie Macron	Dezinformare și propagandă	-	C-I
Operațiuni hibride în Ucraina (2014-prezent)	Atacuri cibernetice asupra infrastructurii guvernamentale	Dezinformare și propagandă	Presiuni economice asupra resurselor energetice	C-I-E
Criza migrantă în Europa (2015-2016)	-	Dezinformare privind criza migratorie	Manipularea fluxurilor migratorii pentru crearea de presiuni economice și sociale	I-E
Criza migranților la granița Poloniei și Belarusului (2021)	-	Propagandă anti-UE	Migrație forțată ca presiune politică	I-E

Amenințare hibridă	Tactici utilizate			Tip sinergie
	cibernetice (C)	informaționale (I)	economice (E)	
Intervenția în Referendumul pentru independența Cataloniei (2017)	Atacuri cibernetice asupra infrastructurii guvernamentale	Dezinformare și manipulare	-	C-I
Intervenția în criza politică din Venezuela (2019)	-	Dezinformare internațională	Intervenții economice și sancțiuni	I-E
Amenințările hibride din Venezuela (2019-prezent)	-	Dezinformare internă pentru consolidarea regimului	Presiuni economice și represiune internă	I-E
Criza politică din Belarus (2020-prezent)	-	Dezinformare și propagandă pentru delegitimarea opoziției	Sprijin economic și militar din partea Rusiei	I-E
Influența Chinei în Asia de Sud-Est (2020-prezent)	-	Dezinformare și propagandă regională	Diplomație coercitivă economică	I-E
Interferența Chinei în politica Taiwanului (2019-prezent)	Atacuri cibernetice asupra instituțiilor din Taiwan	Dezinformare	Presiune economică asupra Taiwanului	C-I-E
Criza politică și de securitate din Mali (2012-prezent)	-	Dezinformare și propagandă jihadistă	Exploatarea resurselor naturale și a tensiunilor sociale	I-E
Campania de interferență cibernetică a Iranului (2018-prezent)	Atacuri cibernetice și furt de proprietate intelectuală	Campanii de dezinformare	-	C-I

Amenințare hibridă	Tactici utilizate			Tip sinergie
	cibernetice (C)	informaționale (I)	economice (E)	
Influența Rusiei în Balcanii de Vest (2014-prezent)	-	Dezinformare pentru exacerbarea tensiunilor etnice	Sprijin economic și logistic pentru partidele pro-ruse	I-E

Vom prezenta și sub formă grafică *tabelul 1*, de forma unei diagrame de tip *„heat map”* (hartă termică), care va reprezenta prezența sau absența tacticilor specifice pentru toate cele 16 amenințări hibride (de la a la p), într-un mod bidimensional. Această nouă reprezentare permite o analiză mai intuitivă a prevalenței fiecărei tactici în cadrul amenințărilor hibride și facilitează identificarea rapidă a modelelor și tendințelor în utilizarea acestor tactici.

În această reprezentare:

- Fiecare coloana reprezintă o amenințare hibridă din tabelul anterior, etichetată cu litera corespunzătoare (a-p).
- Rândurile reprezintă cele trei tipuri de tactici: C (Cibernetice), I (Informaționale), E (Economice).
- Celulele roșii indică prezența unei tactici pentru o anumită amenințare.
- Celulele albe indică absența unei tactici.

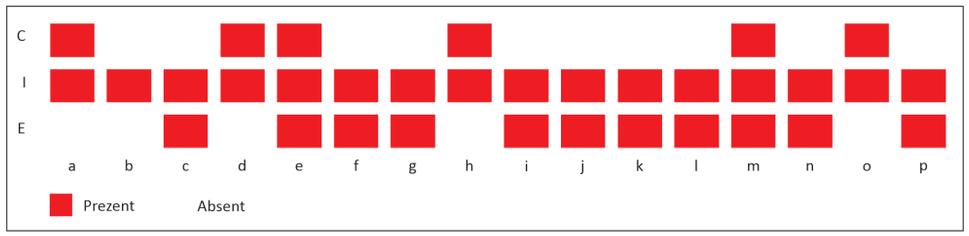

Figura 1: Tacticile hibride utilizate pentru fiecare amenințare hibridă
(diagramă de tip „heat map”/hartă termică) (concepția autorilor)

În cele ce urmează prezentăm câteva observații bazate pe cele două reprezentări grafice. În ceea ce privește întrebuințarea combinațiilor de tactici, observăm prezența asocierii C-I (doar cibernetice și informaționale) în 3 cazuri, a celei I-E (doar informaționale și economice) în 8 cazuri, a celei C-I-E (toate cele trei tactici) în 3 cazuri și a celei I (doar informaționale) într-un singur caz. De asemenea, tactica

informațională (I) este cea mai frecvent utilizată, formând o linie aproape continuă de celule roșii, fiind aplicată în aproape toate cazurile, cu excepția unuia singur. Acest fapt subliniază importanța crucială a componentei informaționale în cadrul amenințărilor hibride. Tacticile cibernetice (C) sunt mai puțin frecvente (apărând în doar 6 din cele 16 cazuri) și apar în combinație cu cele informaționale în mai multe cazuri. Acest lucru sugerează că, deși importante, atacurile cibernetice nu sunt întotdeauna o componentă universală a amenințărilor hibride. Tacticile economice (E) sunt prezente în aproximativ jumătate din amenințări, adesea în combinație cu cele informaționale, formând un model alternant. Acest fapt sugerează că presiunea economică este o componentă semnificativă, dar nu universală, a amenințărilor hibride. Nu în ultimul rând, există câteva amenințări care utilizează toate cele trei tipuri de tactici (rândurile complet roșii).

Devine evident faptul că tacticile informaționale joacă un rol central în toate amenințările hibride, în timp ce tacticile economice și cibernetice sunt utilizate selectiv, în funcție de natura specifică a amenințării.

În ceea ce privește ipoteza că tacticile hibride au fost adaptate la vulnerabilitățile specifice fiecărui stat/entități țintă în parte, *tabelul 2* permite fundamentarea unei astfel de concluzii.

Tabelul 2: Adaptarea tacticilor utilizate în amenințările hibride la vulnerabilitățile existente în cazurile analizate (concepția autorilor)

Amenințare hibridă	Vulnerabilități	Modul de adaptarea tacticilor
Războiul informațional în timpul alegerilor din SUA (2020)	Polarizarea politică, încrederea scăzută în mass-media, utilizarea masivă a rețelelor sociale	Dezinformarea a exploatat diviziunile politice și tensiunile rasiale, în timp ce atacurile cibernetice au vizat infrastructura electorală
Campania de dezinformare împotriva vaccinurilor COVID-19 (2020-2021)	Lipsa de informații corecte despre vaccinuri, neîncrederea în autorități și instituțiile medicale	Mesajele de dezinformare au fost direcționate către grupuri reticente și au folosit social media pentru a amplifica neîncrederea
Criza energetică din Europa (2021-2022)	Dependența energetică de Rusia, vulnerabilitatea pieței europene la fluctuațiile de preț	Rusia a folosit tăierea livrărilor de gaze ca armă economică și dezinformarea pentru a amplifica nemulțumirile publicului față de guverne

Amenințare hibridă	Vulnerabilități	Modul de adaptarea tacticilor
Interferențele cibernetice în campania electorală din Franța (2017)	Sistemul politic fragmentat, prezența puternică a social media în campanii	Atacuri cibernetice și scurgeri de informații vizând echipa lui Macron, acompaniate de campanii de dezinformare
Operațiuni hibride în Ucraina (2014-prezent)	Diviziuni etnice și lingvistice, instabilitate economică și corupție	Rusia a combinat propaganda, sprijinul militar neoficial și atacurile cibernetice pentru a destabiliza țara
Criza migrantă în Europa (2015-2016)	Sistemul de imigrație suprasolicitat, creșterea partidelor populiste anti-imigrație	Dezinformarea a amplificat temerile legate de imigrație, iar manipularea fluxurilor de migranți a creat presiuni economice și sociale
Criza migranților la granița Poloniei și Belarusului (2021)	Tensiuni geopolitice între UE și Belarus, retorica anti-imigrație din Europa de Est	Belarus a folosit migrația ca presiune politică, iar propaganda a încercat să divizeze statele membre ale UE
Intervenția în Referendumul pentru independența Cataloniei (2017)	Tensiuni regionale între guvernul spaniol și autoritățile catalane	Campanii de dezinformare au amplificat narațiuni separatist-propagandistice, iar atacurile cibernetice au vizat destabilizarea guvernului
Intervenția în criza politică din Venezuela (2019)	Economia în colaps, instabilitate politică, lipsa susținerii populare pentru Maduro	Tacticile economice au inclus sancțiuni internaționale și dezinformare pentru manipularea opiniei internaționale
Amenințările hibride din Venezuela (2019-prezent)	Economia disfuncțională, controlul strict al guvernului asupra instituțiilor și media	Dezinformarea a fost folosită pentru control intern, iar sancțiunile economice au fost folosite pentru a slăbi economia și opoziția
Criza politică din Belarus (2020-prezent)	Lipsa unei opoziții bine organizate, sprijin extern din partea Rusiei	Dezinformarea a fost folosită pentru a discredita protestele, iar sprijinul Rusiei a consolidat regimul

Amenințare hibridă	Vulnerabilități	Modul de adaptarea tacticilor
Influența Chinei în Asia de Sud-Est (2020-prezent)	Dependența economică de China, disputele teritoriale din Marea Chinei de Sud	China a folosit diplomația coercitivă economică și propagandă pentru a controla statele din regiune
Interferența Chinei în politica Taiwanului (2019-prezent)	Recunoașterea internațională limitată a Taiwanului, dependența economică de China	China a intensificat presiunile economice și atacurile cibernetice asupra Taiwanului, însoțite de dezinformare
Criza politică și de securitate din Mali (2012-prezent)	Instabilitate politică, prezența grupurilor jihadiste, dependență de ajutor internațional	Jihadiștii au folosit dezinformarea pentru recrutare și au exploatat tensiunile sociale, manipulând accesul la resurse naturale
Campania de interferență cibernetică a Iranului (2018-prezent)	Tensiuni geopolitice, sancțiuni economice severe, infrastructură cibernetică vulnerabilă	Iranul a desfășurat atacuri cibernetice sofisticate și campanii de dezinformare pentru a-și destabiliza adversarii externi
Influența Rusiei în Balcanii de Vest (2014-prezent)	Tensiuni etnice, instabilitate politică, interes economic redus al UE	Rusia a folosit propaganda pentru a exacerba tensiunile etnice și a sprijinit logistic partidele pro-ruse din regiune

Aceste cazuri arată faptul că fiecare stat a fost vulnerabil la anumite tipuri de tactici hibride, iar actorii implicați și-au adaptat acțiunile în funcție de contextul local și de punctele slabe specifice.

Concluzionând, studiul acestor cazuri permite formularea unei recomandări privitoare la necesitatea unei abordări integrate și proactive pentru a contracara strategiile sofisticate ale amenințărilor hibride moderne. De asemenea, este de subliniat necesitatea și importanța existenței unei monitorizări multidisciplinare, autoritățile și experții trebuind să supravegheze constant o gamă largă de factori (de la activitățile cibernetice la narativele media), pentru a detecta și a răspunde eficient la amenințările hibride.

În ceea ce privește strategiile de răspuns, este esențial să se dezvolte contramăsuri care să fie la fel de sinergice și interconectate ca și tacticile hibride ale adversarilor, combinând securitatea cibernetică, strategiile de comunicare publică și reziliența economică.

PARAMETRII UNUI POSIBIL MODEL PREDICTIV INTEGRAT PRIVIND EVALUAREA RISCULUI DE APARIȚIE A AMENINȚĂRILOR HIBRIDE

Implementarea unui model predictiv pentru analiza amenințărilor hibride necesită o abordare metodologică integrată, capabilă să combine și să coreleze variabile din multiple domenii (Valenza et al., 2022). Modelul trebuie să funcționeze ca un mecanism adaptabil, care evoluează în funcție de schimbările din mediul de securitate internațional, economic și tehnologic, permițând, astfel, anticiparea și detectarea timpurie a unor potențiale atacuri hibride. În același timp, este general acceptat faptul că *„Amenințările hibride sunt în mod tradițional dificil de anticipat ...,* însă *este esențial să fie analizate, în scopul executării de răspunsuri cu promptitudine."* (Ib.).

Într-o analiză predictivă a amenințărilor hibride, modelul utilizat trebuie să se bazeze pe un set de parametri esențiali care reflectă atât contextul actual, cât și tiparele identificate anterior. Acești parametri sunt esențiali pentru crearea unei cunoașteri cuprinzătoare a situației și pentru evaluarea probabilității unei amenințări hibride și a impactului acesteia. Avand în vedere tipologia tacticilor descrise anterior, precum și faptul că *„Problemele geopolitice ale spațiului cibernetic sunt strâns legate de considerente politice, economice, sociale și culturale"* (Douzet, 2014), considerăm că un astfel de model trebuie să includă parametri ce pot fi grupați în următoarele categorii: ***geopolitici, cibernetici, economici, socio-culturali, media și informaționali, politici*** și ***tehnologici***.

Prezentăm, în paragrafele următoare, principalii parametri pe care îi considerăm că ar trebui incluși într-un astfel de model, precum și detalii privitoare la conținutul fiecăruia, după cum urmează:

A. Parametri geopolitici

Aceștia pot fi descriși de un set de subindicatori specifici, cum ar fi ***tensiunile internaționale*** (nivelul de tensiune între state sau blocuri regionale – de exemplu, conflicte latente, sancțiuni economice, competiții teritoriale), ***stabilitatea și coeziunea alianțelor și acordurilo rinternaționale*** (NATO sau UE și efectul eventualelor rupturi asupra securității regionale), ***schimbările în politicile naționale*** (modificări legislative sau politice care ar putea influența poziția unui stat pe scena internațională: alegeri, schimbări de guvern sau politici economice care pot provoca reacții internaționale) și ***crizele umanitare/sociale*** (situații de criză umanitară, migrații în masă sau tensiuni sociale interne care pot fi exploatate de actori hibrizi pentru destabilizare societală).

B. Parametri cibernetici

La rândul lor, aceștia pot fi descriși de un set de subindicatori specifici, cum ar fi ***volumul și natura atacurilor cibernetice*** (frecvența și tipul atacurilor cibernetice – phishing, ransomware sau atacuri DDoS – detectate împotriva unei ținte specifice), ***vulnerabilități cibernetice cunoscute*** (nivelul de expunere al infrastructurii critice la atacuri cibernetice, incluzând lipsa de actualizări software, acces neautorizat sau practici de securitate slabe), ***capacități cibernetice ale actorilor implicați*** (date de evaluare a capacităților tehnice și a resurselor disponibile actorilor hibrizi cunoscuți – state naționale sau grupări cibernetice – care ar putea lansa un atac).

C. Parametri economici

Și aceștia pot fi descriși de un set de subindicatori specifici, cum ar fi ***dependența economică de resurse critice*** (vulnerabilități economice legate de dependența de anumite resurse sau furnizori – energie și materii prime, care ar putea fi utilizate ca pârghii în strategii hibride), ***fluctuații economice și crize*** (indicatori economici, cum ar fi inflația, fluctuațiile valutare, scăderile bursei de valori sau crizele financiare care pot fi exploatate de actori hibrizi pentru destabilizare), precum și ***sancțiuni economice și comerț*** (impactul sancțiunilor internaționale sau al restricțiilor comerciale asupra unui stat sau a unei regiuni și modul în care acestea ar putea amplifica vulnerabilitățile economice existente).

D. Parametri sociali și culturali

La rândul lor, aceștia pot fi descriși de un set de subindicatori specifici, cum ar fi ***diviziuni sociale*** (gradul de polarizare socială și politică, tensiunile etnice sau religioase și alte forme de fragmentare care pot fi exploatate prin dezinformare și propagandă), ***sentimentul public și încrederea în instituții*** (nivelul de încredere al populației în instituțiile guvernamentale, mass-media și alte instituții esențiale, scăderea încrederii putând facilita acțiuni hibride de dezinformare), precum și ***activitatea și influența în social media*** (monitorizarea narativelor dominante pe rețelele sociale și identificarea dezinformării sau a campaniilor de influențare coordonată).

E. Parametri media și informaționali

Pentru acest indicator, setul de subindicatori specifici poate cuprinde ***răspândirea dezinformării*** (frecvența și amploarea campaniilor de dezinformare identificate și tipurile de narațiuni utilizate pentru a manipula opinia publică), ***controlul și manipularea mediatică*** (gradul de control asupra mass-mediei și influența asupra agendei publice, inclusiv tacticile de amplificare a mesajelor prin canale alternative și conturi false) și ***capacitatea de reziliență a publicului*** (nivelul de alfabetizare media și reziliența publicului la dezinformare, fapt ce influențează eficacitatea campaniilor informaționale hibride).

F. Parametri politici

Aceștia pot fi descriși de un set de subindicatori specifici, cum ar fi ***stabilitatea politică internă*** (stabilitatea și unitatea internă a guvernului, riscul de revolte sau mișcări de opoziție care ar putea fi încurajate de actori externi), ***politicile de securitate națională*** (eficacitatea politicilor de securitate și capacitatea statului de a răspunde la amenințări hibride prin instituții precum armata, poliția și serviciile de informații), ***relațiile cu actorii externi*** (nivelul de cooperare sau conflict cu alte state, care pot influența probabilitatea unei acțiuni hibride externe, precum și alianțele strategice).

G. Parametri tehnologici

Pentru acest indicator, setul de subindicatori specifici poate cuprinde ***accesul la tehnologii avansate*** (capacitatea actorilor de a accesa tehnologii avansate – inteligența artificială, drone și criptare avansată, care pot fi utilizate în operațiuni hibride), ***inovații în comunicații și media*** (rolul tehnologiilor emergente în facilitarea sau contracararea campaniilor hibride, inclusiv utilizarea de platforme descentralizate sau aplicații de mesagerie criptată).

CONCLUZII

În baza acestor parametri și a seturilor de subindicatori specifici identificați, se poate construi un model predictiv care să ofere o evaluare a riscului pentru diverse scenarii de amenințări hibride. Lucrarea de față își propune doar să sugereze modul în care acesta poate fi implementat și elementele esențiale ce trebuie avute în vedere, lăsând aspectele ulterioare în sarcina unei cercetări viitoare.

Pentru ca acest model să fie funcțional, un aspect fundamental constă în colectarea și integrarea continuă a datelor din diverse surse. Conform Shan et al. (2024), *„Un mecanism de analiză predictivă, integrat cu platforme de informații cu privire la amenințări, utilizează datele istorice și tendințele actuale, pentru a prognoza care sunt vectorii de atac și țintele potențiale”.* În mod ideal, implementarea începe prin construirea unei infrastructuri de date care să adune informații din surse variate și relevante: rapoarte geopolitice, date economice în timp real, analize de securitate cibernetică și date sociale (inclusiv analize bazate de informații din rețelele sociale). Această infrastructură de date poate fi susținută de un sistem centralizat, capabil să armonizeze și să actualizeze constant seturile de date într-un mod dinamic, reflectând evoluțiile recente.

Un element cheie în acest proces îl constituie algoritmii de învățare automată (machine learning), care oferă modelului capacitatea de a identifica tipare din seturile de date istorice și contemporane. Prin antrenarea algoritmilor cu date

din scenarii hibride anterioare (atât reușite, cât și eșuate), se poate construi un model care detectează corelațiile dintre diferiți factori de risc. Acești factori sunt regăsiți în parametrii geopolitici, cibernetici, economici, politici și informaționali, care, împreună, formează structura unui atac hibrid. De exemplu, modificările bruște ale relațiilor internaționale sau tensiunile geopolitice, combinate cu creșterea activității cibernetice într-o anumită regiune, pot fi indicatori timpurii ai unui atac hibrid coordonat.

Un alt aspect esențial este modul în care datele sunt analizate, pentru a simula scenarii potențiale. Modelul ar trebui să fie capabil să genereze simulări multiple, care să exploreze diverse direcții de evoluție a amenințărilor hibride, pe baza modificărilor în parametrii geopolitici sau economici. Aceste simulări pot lua în considerare nu doar un eveniment izolat, ci și sinergia dintre diferitele tactici utilizate în mod frecvent în atacurile hibride: atacuri cibernetice combinate cu campanii de dezinformare sau utilizarea presiunilor economice pentru a destabiliza ținte vulnerabile.

Pentru ca acest model să fie implementat cu succes, trebuie să fie dezvoltat și un sistem de alertă timpurie. Acesta ar trebui să fie programat pentru a declanșa alerte automate atunci când combinația de factori atinge anumite praguri critice. De exemplu, o creștere a tensiunilor sociale combinată cu o intensificare a atacurilor cibernetice și a campaniilor de dezinformare poate sugera că o criză hibridă este iminentă. Pragurile critice trebuie definite pe baza analizei scenariilor anterioare, iar ajustările constante trebuie să fie integrate în sistem, pe măsură ce noi informații devin disponibile.

O altă dimensiune importantă în implementare este componenta de reziliență. Odată ce modelul identifică o posibilă amenințare, este important ca autoritățile responsabile să aibă la dispoziție un set de măsuri proactive, care să includă consolidarea rezilienței cibernetice, implementarea de campanii pentru creșterea încrederii publicului în instituțiile naționale și internaționale și coordonarea cu partenerii internaționali pentru a contracara efectele amenințărilor hibride într-un mod coordonat.

În acest fel, acest model predictiv are potențialul de a deveni un instrument esențial pentru factorii de decizie politică și militară, care își pot planifica resursele pentru a preveni și diminua impactul amenințărilor hibride, înainte ca acestea să provoace daune semnificative. Cu o structură flexibilă și o actualizare constantă a datelor, modelul poate oferi un cadru comprehensiv pentru anticiparea amenințărilor, reducerea riscurilor și sporirea siguranței infrastructurilor critice și a securității naționale.

BIBLIOGRAFIE:

1. Arcos, R. (2021). *Information influencing in the Catalan illegal referendum and beyond*. În: Hybrid Warfare. DOI:10.5040/9781788317795.0023.
2. Astapova, A., Navumau, V., Nizhnikau, R., Polishchuk, L. (2022). *Authoritarian cooptation of civil society: The case of Belarus*. Europe-Asia Studies, 74(1), pp. 1-30.
3. Aulia, J.D., Kurniati, E. (2024). *Analysis of Russian factors supporting Nicolas Maduro in the Venezuelan crisis from Alexander Wendt's constructivist perspective.* Siyar Journal, 4(1), pp. 59-73, https://jurnalfisip.uinsa.ac.id/index.php/siyar/article/download/584/334, accesat la 12 iunie 2024.
4. Barberà, O. (2020). *All fake? Information disorders and the 2017 referendum in Catalonia*. În Misinformation in Referenda (pp. 281-298). Routledge.
5. Beaton, A.C. (2021). *Social Media in Venezuela: A Tool for Authoritarians, a Boost to Social Movements, or Both?* Doctoral dissertation, Monterey, CA; Naval Postgraduate School, https://apps.dtic.mil/sti/trecms/pdf/AD1164874.pdf, accesat la 12 august 2024.
6. Bertolini, M., Minicozzi, R., Sweijs, T. (aprilie 2023). *Ten Guidelines for Dealing with Hybrid Threats*. *A Policy Response Framework*. The Hague Centre for Strategic Studies, https://hcss.nl/wp-content/uploads/2023/04/Guidelines-for-the-Deterrence-of-Hybrid-Threats-HCSS-2023.pdf, accesat la 17 iunie 2024.
7. Bodnar, A., Grzelak, A. (2023). *The Polish–Belarusian border crisis and the (lack of) European Union response*. Białostockie Studia Prawnicze, 28(1), pp. 57-86, https://intapi.sciendo.com/pdf/10.15290/bsp.2023.28.01.04, accesat la 17 iunie 2024.
8. Braghiroli, S., Makarychev, A. (2018). *Redefining Europe: Russia and the 2015 refugee crisis.* Geopolitics, 23(4), pp. 823-848
9. Cañizález, A., Hernández, L., Torrealba, L. (2020). *Disinformation as a Society-Wide Threat: Journalism and 'Fakecracy'in Venezuela*. În vol. Fake news is bad news – hoaxes, half-truths and the nature of today's journalism, available at https://www.intechopen.com/chapters/73501, accesat la 22 mai 2024.
10. Chaguaceda, A., Pelaez, J.C., Puerta, M.I. (2023). *Illiberal Narratives in Latin America: Russian and Allied Media as Vehicles of Autocratic Cooperation*. Journal of Illiberalism Studies, vol. 3, nr. 2 (2023): pp. 111-123.
11. Chang, H.C H., Haider, S., Ferrara, E. (2021). *Digital civic participation and misinformation during the 2020 Taiwanese presidential election*. Media and Communication, vol. 9, nr. 1, pp. 144-157, DOI: 10.17645/mac. v9i1.3405, accesat la 12 mai 2024.
12. Cipan, V., Kirichenko, D. (2024). *Russian influence and disinformation operations in the Balkans*. Georgetown Security Studies Review, vol. 11, nr. 2, pp. 65-85.
13. Cox, K., Marcellino, W., Bellasio, J., Ward, A., Galai, K.&Meranto, S., Paoli, G. P. (2018). *Social media in Africa*. *A double-edged sword for security and development.* RAND Europe, https://www.undp.org/sites/g/files/zskgke326/files/migration/africa/UNDP-RAND-Social-Media-Africa-Research-Report_final_3-Oct.pdf, accesat la 22 mai 2024.
14. Douzet, F. (2014). *Understanding cyberspace with geopolitics*. Hérodote, 2014/1, nr. 152-153, pp. 3-21, https://shs.cairn.info/journal-herodote-2014-1-page-3?lang=en, accesat la 17 iunie 2024.
15. Elswah, M., Alimardani, M. (2021). *Propaganda chimera: Unpacking the Iranian perception information operations in the Arab world*. Open Information Science, 5(1), pp. 163-174.

16. Ferchen, M., Mattlin, M. (2023). *Five modes of China's economic influence: Rethinking Chinese economic statecraft*. The Pacific Review, 36(5), pp. 978-1004, https://www.tandfonline.com/doi/pdf/10.1080/09512748.2023.2200029, accesat l 22 mai 2024.
17. Ferrara, E. (2017). *Disinformation and social bot operations in the run up to the 2017 French presidential election*, SSRN First Monday 22(8), http://dx.doi.org/10.2139/ssrn.2995809, accesat la 22 mai 2024.
18. Galeotti, M. (2019). *Russian political war: moving beyond the hybrid*. Routledge.
19. Giannakopoulou, S. (2022). *How social media mobilize the social and political reaction in authoritarian regimes: The Belarus experience*. Faculty of Economic and Political Sciences, https://ikee.lib.auth.gr/record/341645/files/GRI-2022-36486.pdf, accesat la 13 iunie 2024.
20. Gilbert, A., Bazilian, M.D., Gross, S. (2021). *The emerging global natural gas market and the energy crisis of 2021-2022*. Foreign Policy, Brookings, 1, pp. 1-10, https://www.brookings.edu/wp-content/uploads/2021/12/FP_20211214_global_energy_crisis_gilbert_bazilian_gross.pdf, accesat la 22 mai 2024.
21. Gross, S., Stelzenmüller, C. (18 iunie 2024). *Europe's messy Russian gas divorce*, Brookings Institution, https://www.brookings.edu/articles/europes-messy-russian-gas-divorce/, accesat la 22 august 2024.
22. Hardy, J. (2022). *Moving the goalposts: A Comparative case study analysis of the Belarusian regime*. Sciences, 10(9), pp. 100-107.
23. Hartnett, S.J., Su, C. (2021). *Hacking, debating, and renewing democracy in Taiwan in the age of "post-truth" communication*. Taiwan Journal of Democracy, 17(1), pp. 21-43.
24. Hoffman, F. (2007). *Conflict in the 21st Century: The rise of hybrid wars*. Potomac Institute for Policy Studies.
25. Hung, T.C., Hung, T.W. (2022). *How China's cognitive warfare works: A frontline perspective of Taiwan's anti-disinformation wars*. Journal of Global Security Studies, 7(4), pp. 1-18, https://doi.org/10.1093/jogss/ogac016, accesat la 22 iunie 2024.
26. Jędrzejczyk-Kuliniak, K. (2023). *Polish-Belarus Border in the Political Narrative During the Migration Crisis in 2021-2022*, în Producing Cultural Change in Political Communities: The Impact of Populism and Extremism on the International Security Environment (pp. 159-181). Cham: Springer Nature Switzerland.
27. Kase, L.M. (2024). *The European Case for Kosovo, Serbia, and North Macedonia: A Western Balkan Focus*, https://digitalcommons.liberty.edu/cgi/viewcontent.cgi?article=1461&context=hsgconference, accesat la 22 august 2024.
28. Karolewski, I.P., Benedikter, R. (2018). *Europe's refugee and migrant crisis: Political responses to asymmetrical pressures*. Politique européenne, (2), pp. 98-132, https://shs.cairn.info/revue-politique-europeenne-2018-2-page-98?lang=fr, accesat la 22 mai 2024.
29. Kuvekalović, J., Stojanović, G., Filipović, M. (2017). *Security implications of the migrant crisis in Europe 2015-2016*, Faculty of Security Studies.
30. Lehto, M. (2022). *Cyber-attacks against critical infrastructure.* În Cyber security: Critical infrastructure protection (pp. 3-42). Springer International Publishing. Methods in Applied Sciences, 56, https://doi.org/10.1007/978-3-030-91293-2_1, accesat la 22 mai 2024.
31. Lika, L. (2021). *The Western Balkans at the crossroads of European integration and the emerging powers' projection of influence*. The Journal of Cross-Regional

Dialogues, nr. 2/2021, pp. 7-30, https://orbi.uliege.be/bitstream/2268/265217/1/Article%20Liridon%20Lika%20JCRD.pdf, accesat la 22 mai 2024.
32. Maza, K.D., Koldas, U., Aksit, S. (2020). *Challenges of countering terrorist recruitment in the Lake Chad region: The case of Boko Haram.* Religions, 11(2), p. 96.
33. Menn, J. (2020). *Russian-backed organizations amplifying QAnon conspiracy theories, researchers say*, Reuters, https://www.reuters.com/article/us-usa-election-qanon-russia-idUSKBN25K13T, accesat la 12 mai 2024.
34. Mumford, A. (2021). *Hybrid Warfare: Past, Present, and Future*. Polity Press.
35. National Intelligence Council (10 martie 2021). Foreign Threats to the 2020 US Federal Elections, https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf, accesat la 22 mai 2024.
36. NATO (2010). *A hybrid warfare strategy*. NATO Review.
37. NATO (2020). *NATO's Approach to countering hybrid warfare*. NATO Strategic Communications Centre of Excellence.
38. Nübel, K. A. (2020). *THE rise of new types of war: A case study on Russian hybrid warfare in the Ukrainian crisis in 2014*, Master's thesis, University of Twente, https://essay.utwente.nl/82683/1/N%C3%BCbel_MA_BMS.pdf, accesat la 22 mai 2024.
39. O'Connor, S., Hanson, F., Currey, E., Beattie, T. (2020). *Cyber-enabled foreign interference in elections and referendums* (vol. 28). Canberra: Australian Strategic Policy Institute, https://ad-aspi.s3.amazonaws.com/2020-10/Cyber%20enabled%20foreign%20interference_0.pdf, accesat la 22 mai 2024.
40. Otaiku, A.A. (2018). *A framework for hybrid warfare: threats, challenges and solutions*. Journal of Defense Management, https://www.longdom.org/open-access/a-framework-for-hybrid-warfare-threats-challenges-and-solutions-25432.html, accesat la 22 mai 2024.
41. Pal, D. (2021). *China's influence in south Asia. Carnegie Endowment for International Peace*, https://carnegie-production-assets.s3.amazonaws.com/static/files/202110-Pal_SouthAsiaChina_final1.pdf, accesat la 22 mai 2024.
42. Pindjak, P. (2014). *Deterring hybrid warfare: A NATO Perspective*. NATO Defense College Research Paper, 123, pp. 1-8.
43. Pindják, P. (2019). *The Hybrid threat: Blurring the line between war and peace*. Journal of Strategic Studies, 42(3-4), pp. 271-292.
44. Popkostova, Y. (2022). *Europe's energy crisis conundrum*. European Union Institute for Security Studies, https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief_2_Energy%20Crisis.pdf, accesat la 12 mai 2024.
45. Rid, T., Hecker, M. (2021). *The rise of hybrid warfare*. Oxford University Press.
46. Rouvinski, V. (2019). *Russian-Venezuelan relations at a crossroads*. Woodrow Wilson International Center for Scholars, Latin American Program, 1.
47. Rozental, D., Jeifets, L. (2022). *Russia and Venezuela: Russia's Gateway to Latin America*. În Rethinking Post-Cold War Russian–Latin American Relations (pp. 193-205). Routledge.
48. Schmidt, J.D. (2008). *China's soft power diplomacy in Southeast Asia*. The Copenhagen Journal of Asian Studies, 26(1), pp. 22-49.
49. Shan, A., Myeong, S. (2024). *Proactive threat hunting in critical infrastructure protection through hybrid machine learning algorithm application*. Sensors, 24(15):4888, p. 5, https://doi.org/10.3390/s24154888, accesat la 12 mai 2024.

50. Spataro, J.G. (2019). *Iranian Cyber Espionage*. Utica College ProQuest dissertations & theses , https://www.proquest.com/openview/7816e26f17ba341674713046f4a249fa/1?pq-origsite=gscholar&cbl=18750&diss=y, accesat la 22 mai 2024.
51. Starodubtseva, A. (2021). *Russian hybrid warfare in Ukraine: Comparative analysis of two cases and identification of critical elements in the successful application of hybrid tactics*. Master thesis, Praga: Charles University, Faculty of Social Sciences, Department of Security Studies, https://dspace.cuni.cz/bitstream/handle/20.500.11956/124589/120381167.pdf?sequence=1&isAllowed=y, accesat la 22 mai 2024.
52. Stokel-Walker, C. (2024). *Medical misinformation on social media - are the platforms equipped to be the judge?,* The BMJ, 2024, DOI: 10.2196/17187.
53. Suarez-Lledo, V., Alvarez-Galvez, J. (2021). *Prevalence of health misinformation on social media: systematic review*. J. Med Internet Res 2021; 23(1): e17187, https://www.jmir.org/2021/1/e17187, accesat la 22 mai 2024.
54. Thurston, A., Lebovich, A. (2013). *A handbook on Mali's 2012-2013 crisis*. Institute for the Study of Islamic Thought in Africa, https://sahelresearch.africa.ufl.edu/wp-content/uploads/sites/170/ISITA-13-001-Thurston-Lebovich.pdf, accesat la 12 mai 2024.
55. Tsiklauri, G. (2021). *Hybrid Warfare in Cyber domain: Case Study of hybrid threats in cyberspace.* Master thesis, Praga: Charles University, Faculty of Social Sciences, Department of Security Studies, pp. 42-48, https://dspace.cuni.cz/bitstream/handle/20.500.11956/127657/120387067.pdf?sequence=1&isAllowed=y, accesat la 22 mai 2024.
56. Vakarchuk, K.V. (aprilie 2020). *The impact of the media on the Catalonia referendum*. Rhetoric and Communications, nr. 43, ISSN 1314-4464, https://rhetoric.bg/wp-content/uploads/2020/06/Vakarchuk-issue-April-2020-pp.83-95.pdf, accesat la 12 mai 2024.
57. Valenza, F., Karafili, E., Steiner, R.V., Lupu, E.C. (2022). *A hybrid threat model for smart systems*. În: IEEE transactions on dependable and secure computing, vol. 20, nr. 5, pp. 440 -4417, ISSN 1545-5971, Elettronico.
58. Vilmer, J.B.J., Conley, H.A. (2018). *Successfully countering Russian electoral interference*. Washington: Center for Strategic & International Studies, https://www.jbjv.com/IMG/pdf/180621_Vilmer_Countering_russiam_electoral_influence.pdf, accesat la 12 mai 2024.
59. Wentzell, T.D. (2021). *Russia's Green Men: The Strategic Storytellers of Hybrid Warfare*. Canadian Military Journal, 22(1), pp. 42-48, https://www.journal.forces.gc.ca/PDFs/CMJ221Ep42.pdf, accesat la 22 mai 2024.
60. Wither, J.K. (2016). *Making sense of hybrid warfare*. Connections: The Quarterly Journal, 15(2), pp. 73-87.
61. Wojnowski, M. (2021). *Russian interference in the U.S. Presidential elections in 2016 and 2020 as an attempt to implement a revolution-like information warfare scheme*, în US democracy as the target of Russian secret services, Warsaw Institute, Polonia, https://warsawinstitute.org/wp-content/uploads/2021/07/RS_06-2021_EN.pdf, accesat la 22 mai 2024.
62. Zdanowicz, M. (2023). *The migration crisis on the Polish-Belarusian border.* Białostockie Studia Prawnicze, 1(28), pp. 103-115, https://intapi.sciendo.com/pdf/10.15290/bsp.2023.28.01.06, accesat la 22 mai 2024.