Institutul European din România

Combaterea amenințărilor hibride: competențe instituționale și nevoia de cooperare în România

Maria-Manuela CATRINA
Vlad DRĂGUȘ

București, mai 2024
Policy Brief nr. 15

Combaterea amenințărilor hibride: competențe instituționale și nevoia de cooperare în România

Maria – Manuela CATRINA

Vlad DRĂGUȘ

București, mai 2024

Colecția Policy Briefs, nr. 15

Institutul European din România

Bd. Regina Elisabeta 7-9, București, România
Telefon: (4021) 314 26 96
E-mail: ier@ier.gov.ro; Website: www.ier.gov.ro

Coordonator Seria Working Papers și Policy Briefs:

Mihaela-Adriana PĂDUREANU

Cuprins

Combaterea amenințărilor hibride: competențe instituționale și nevoia de cooperare în România

Rezumat

Acest material analizează succint problematica legată de combaterea amenințărilor hibride la nivel național, în România. Ipoteza de cercetare este că lipsa unui cadru legal clar și a unor definiții unice operaționale pentru amenințările hibride creează dificultăți în identificarea autorităților care au competențe în acest domeniu. În vederea încadrării cercetării, a fost realizată o comparație cu unele state membre ale Uniunii Europene care au identificat soluții în domeniul combaterii amenințărilor hibride, prin organizarea unor grupuri de cooperare interinstituțională. Astfel, în partea de recomandări a lucrării este evidențiată o abordare care prezintă un anume grad de relevanță și reprezintă o potențială soluție care poate fi replicată și în România.

Cuvinte cheie: *riscuri hibride, dezinformare, FIMI, cooperare, competență instituțională.*

Abstract

This paper briefly analyses the issues related to combatting hybrid threats at the national level, in Romania. Our research hypothesis is that the lack of a clear legal framework and single operational definitions for hybrid threats create difficulties in identifying the competent authorities in this field. To present a comparison, some European Union member states have been selected with the purpose of presenting the solutions identified by them in the field of combatting hybrid threats, such as organizing inter-institutional cooperation groups. Thus, in the recommendations, we propose an approach that presents a certain degree of relevance and represents a potential solution for Romania, as well.

Keywords*: Hybrid risks, disinformation, FIMI, cooperation, institutional competence.*

Biografie:

Maria-Manuela Catrina ocupă funcția de adjunct al Directorului Directoratului Național de Securitate Cibernetică și este doctorand în cadrul școlii doctorale multidisciplinare în domeniul Management al SNSPA. Având o formare academică în matematică și informatică, după susținerea licenței a acumulat experiență didactică ca profesor de informatică în limba germană, iar apoi a activat ca asistent universitar și lector. A urmat apoi o carieră în administrație publică, ocupând funcția de secretar de stat în cadrul Ministerului Comunicațiilor și Societății Informaționale. Între 2013 și 2020 a ocupat funcția de director executiv la Institutul Ovidiu Șincai. În activitatea sa de conducere a Departamentului general pentru parteneriate instituționale al DNSC, ea își îndreaptă eforturile în stimularea cadrului de colaborare între instituțiile publice, private, de învățământ și de cercetare, cu obiectivul general de a cultiva o viziune și o abordare realistă și coerentă a securității cibernetice în România.

Vlad Drăguș este expert în politici, strategii și cooperare în Securitate Cibernetică, în cadrul Directoratului Național de Securitate Cibernetică și student doctorand în cadrul Facultății de Drept a Universității București. A acumulat experiență în sectorul societății civile, în care a organizat simulări academice în domeniul relațiilor internaționale. Activitatea profesională principală a reprezentat șapte ani în administrația publică centrală, activând în domeniul documentării legislative și al elaborării de acte normative. În prezent, activitatea lui implică identificarea și gestionarea unor parteneriate și activități de cooperare de tip public – privat, precum și participarea la diverse grupuri de lucru organizate la nivelul Uniunii Europene în domeniul securității cibernetice. Domeniile lui de interes profesional includ: dreptul muncii, dreptul noilor tehnologii și politicile publice.

Abrevieri

Alin. – Aliniat

Art. – Articol

CNA – Consiliul Național al Audiovizualului

CSIRT – Computer Security Incident Response Team

DNSC – Directoratul Național de Securitate Cibernetică

EEAS – Serviciul European de Acțiune Externă (SEAE)

FIMI – Manipularea și ingerința informațiilor străine (FIMI)

IA –Inteligență artificială

IT&C – Information Technology and Communications

NSC – National Security Center/ Regatul Unit

OUG – Ordonanță de urgență

UE – Uniunea Europeană

1. Încadrarea conceptului de amenințări hibride

Globalizarea, în special prin dimensiunea sa tehnologică a condus la o accentuare a interconectării la nivel mondial. Acest lucru a contribuit la facilitarea interacțiunii dintre actorii statali și non-statali. Pe lângă beneficii, gradul ridicat de interconectivitate poate să predispună la un risc crescut de atacuri de tip informatic mai complexe din partea anumitor actori ostili[1] din mediul online. Aceștia desfășoară activități care urmăresc obiective diverse, motivate de interesele lor și care pot fi contrare părților care sunt amenințate. Destabilizarea poate începe prin exercitarea unei presiuni economice sporite asupra țării vizate, cu scopul de a perturba activitatea instituțiilor publice sau de a influența cursul politic al societății în direcțiile urmărite de aceștia. Mecanismele specifice statului de drept presupun aplicarea unor măsuri bazate pe principiul legalității, în concordanță cu drepturile fundamentale ale omului. Toți cetățenii, instituțiile și entitățile trebuie să fie trase la răspundere în conformitate cu reglementările din domeniu, aplicate în mod egal, conform unor decizii invidualizate pentru fiecare caz în parte.

Într-un astfel de context, promovarea unor informații incorecte, false sau incomplete cu scopul de a schimba comportamentul cetățenilor este foarte răspândită – 51% dintre europeni cred că au fost expuși unor informații false în mediul online[2]. Dezinformarea contribuie la accentuarea amenințărilor de tip hibrid, acele amenințări care combină atât mijloace militare, cât și nemilitare[3]. Potrivit unui ghid despre privind amenințările hibride care a fost publicat recent de *Hybrid CoE Research Reports*[4], una dintre cele mai mari provocări în contextul combaterii amenințărilor de tip hibrid este reprezentată de lipsa unui cadrul legal la nivel național (în statele membre). Considerăm că acest cadru legal ar trebui să se concentreze, în primul rând, pe definirea amenințării de tip hibrid ca prim pas către stabilirea instituției sau instituțiilor competente pentru intervenția și gestionarea amenințărilor hibride. Spre exemplu, Serviciul de Acțiune Externă al Uniunii Europene (SEAE) definește amenințările hibride ca fiind combinația de activități coercitive și subversive, metode convenționale și

[1] Termen folosit în National Cyber Security Center Annual Review 2023, disponibil la: https://www.ncsc.gov.uk/files/Annual_Review_2023.pdf, accesat la 5 aprilie 2024.
[2] Comisia Europeană, Consolidarea Codului de bune practici privind dezinformarea https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/new-push-european-democracy/protecting-democracy/strengthened-eu-code-practice-disinformation_ro, accesat la 4 aprilie 2024.
[3] NATO, Countering hybrid threats, disponibil la: https://www.nato.int/cps/en/natohq/topics_156338.htm, accesat la 19 martie 2024.
[4] Krátka V., Poleščuk Š. & A., *Raportul de cercetare nr. 10 - Prevenirea interferențelor electorale: Bune practici și recomandări,* The European Centre of Excellence for Countering Hybrid Threats, 2023 disponibil la: https://www.hybridcoe.fi/wp-content/uploads/2023/09/20230912-Hybrid-CoE-Research-Report-10-PEI-WEB.pdf, accesat la 27 februarie 2024.

neconvenționale, utilizate în mod coordonat pe mai multe domenii. Exemple de acțiuni de atacuri hibrid includ: manipularea de informații, atacurile cibernetice, constrângerea economică etc[5].

Ghidul sus-menționat propune definirea amenințărilor hibride ca fiind interferențe efectuate prin manipulare sau nedorite, printr-o varietate de instrumente precum: răspândirea dezinformării/informațiilor viciate, crearea de narațiuni istorice puternice (dar incorecte sau doar parțial corecte), interferența electorală, atacurile cibernetice, interferențele economice etc.[6] Definiția propusă de SEAE nu are un caracter universal, ci reprezintă o încercare de a cuprinde cât mai plastic un fenomen complex și de cele mai multe ori schimbător, instabil. Dificultatea de a obține o explicație cât mai cuprinzătoare și operativă constă în caracterul dinamic și versatil al acestui mediu. În cadrul acestei analize ne vom referi la amenințările hibride în raport cu cadrul oferit în *The landscape of Hybrid Threats: A conceptual model*[7], model cu referințe în grupurile de lucru de la nivelul instituțiilor Uniunii Europene. Conform documentului, există trei mari dimensiuni pe care trebuie să le cuprindă conceptul amenințărilor hibride: militar, academic și politic.

Comisia Europeană consideră ameniățările hibride ca fiind o amenințare constantă și complexă cu care se confruntă. Comisia consideră că aceste amenințări se referă la actorii care încearcă să exploateze vulnerabilitățile UE în propriul lor avantaj, utilizând într-un mod coordonat un mix de măsuri (diplomatice, militare, economice, tehnologice). Exemple oferite de Comisia Europeană pentru astfel de amenințări sunt: împiedicarea proceselor democratice de luare a deciziilor prin campanii masive de dezinformare, utilizarea rețelelor sociale pentru a controla narațiunea politică sau pentru a radicaliza, recruta și direcționa actori de tip *proxy*[8]. Pentru a răspunde acestor amenințări, Uniunea Europeană are patru piloni de acțiune: 1. creșterea gradului de conștientizare a situației, 2. creșterea gradului de reziliență în toate sectoarele critice, 3. oferirea unui răspuns adecvat și redresare în caz de criză și 4. cooperarea cu țări și organizații similare, în special NATO.

---

[5] Serviciul European de Acțiune Externă, Countering hybrid threats (18.03.2024), disponibil la: https://www.eeas.europa.eu/eeas/countering-hybrid-threats_en, accesat la 4 aprilie 2024.
[6] Krátka V., Poleščuk Š. & A., *op. cit.*, p. 9.
[7] Comisia Europeană și Centrul European de Excelență pentru Contracararea Amenințărilor Hibride, *The landscape of hybrid threats: A conceptual model*, Publications Office of the European Union, Luxemburg, 2021, p. 8, disponibil la: https://www.hybridcoe.fi/publications/the-landscape-of-hybrid-threats-a-conceptual-model/, accesat la 4 aprilie 2024.
[8] Comisia Europeană, Hybrid Threats, disponibil la: https://defence-industry-space.ec.europa.eu/eu-defence-industry/hybrid-threats_en, accesat la 4 aprilie 2024.

Când discutăm despre termenul de „amenințări hibride” trebuie să avem în vedere că este un concept mai degrabă utilizat în spațiul occidental cu scopul de a dezbate o problematică de securitate cu care se confruntă aceste state care, fie au un regim politic democratic, fie sunt în faza de democratizare. De cele mai multe ori, aceasta este dimensiunea/paradigma de încadrare în majoritatea literaturii occidentale referitoare la amenințări hibride. Conceptul a pătruns, însă, și în doctrina rusă și chineză, nefolosindu-se însă aceeași terminologie. Pentru spațiul rusesc tendințele războiului modern sunt teoretizate sub ideile generale a ceea ce este cunoscut ca „doctrina Gerasimov”. În februarie 2013, generalul Valery Gerasimov, șeful Statului Major al Federației Ruse, a publicat un articol în publicația săptămânală rusă *Military-Industrial Kurier*, intitulat: „Valoarea științei este în previziune”. În acest articol, Gerasimov argumentează că rolul mijloacelor nemilitare de a atinge obiectivele politice și strategice a crescut și, în multe cazuri, au depășit puterea forței armelor convenționale în eficacitatea lor. Articolul poate fi considerat o articulare a strategiei moderne a Federației Ruse, o viziune a războiului total care plasează politica și războiul în același spectru de activități, din punct de vedere filozofic, dar și logistic[9].

La nivel european au fost luate mai multe măsuri pentru a răspunde amenințărilor hibride. Astfel, conform *Comunicării Comisiei către Parlamentul European și Consiliu*[10] *Cadrul comun privind contracararea amenințărilor hibride. Un răspuns al Uniunii Europene* definiția amenințărilor hibride trebuie să rămână flexibilă, pentru a fi cât mai cuprinzătoare, dat fiind faptul că abordăm un domeniu dinamic și versatil, însă suficient de specifică pentru a putea fi folosită în explicarea diferitelor fenomene din lumea reală. Un exemplu concret oferit în acest sens a fost utilizarea campaniilor de dezinformare masivă, care folosesc platforme de comunicare socială pentru a influența discursul politic sau pentru a radicaliza, a recruta și coordona actori intermediari.

Mai jos, regăsim câteva exemple de categorii de atacuri hibride, așa cum sunt identificate de Serviciului European de Acțiune Externă al UE (SEAE)[11]:

---

[9] Molly K Mckew, The Gerasimov Doctrine, *Politico*, Septembrie – Octombrie 2017, disponibil la: https://www.politico.com/magazine/story/2017/09/05/gerasimov-doctrine-russia-foreign-policy-215538/, accesat la: 4 aprilie 2024.

[10] Comunicarea Comisiei către Parlamentul European și Consiliu privind cadrul comun privind contracararea amenințărilor hibride - JOIN/2016/018 final, disponibilă la: https://eur-lex.europa.eu/legal-content/ro/TXT/?uri=CELEX:52016JC0018, accesată la 27 februarie 2024.

[11] Serviciu European de Acțiune Externă, 2nd EEAS Report on Foreign Information Manipulation and Interference Threats, disponibil la: https://www.eeas.europa.eu/eeas/2nd-eeas-report-foreign-information-manipulation-and-interference-threats_en, accesat la: 27 februarie 2024.

- Dezinformarea, conform definiției operative utilizate de instituțiile UE[12], se referă la un conținut fals sau înșelător care este răspândit cu intenția de a înșela sau de a asigura câștiguri economice sau politice și care poate cauza prejudicii publice;
- *Foreign Information Manipulation Interference*, conform SEAE, este un model de comportament care amenință sau are potențialul de a avea un impact negativ asupra valorilor, procedurilor și proceselor politice. O astfel de activitate are un caracter manipulativ, desfășurată într-o manieră intenționată și coordonată. Actorii unei astfel de activități pot fi statali sau nestatali, inclusiv împuterniciții lor, din interiorul sau/și din afara propriului teritoriu.[13]
- Conținutul generat de IA (inteligența artificială) poate fi folosit pentru a răspândi dezinformarea și, astfel, pentru a manipula opinia publică. În mod special, în ultimii doi ani, tehnologia de tip *deep fake* a fost dezbătută în spațiul public și poate fi considerată , o amenințare majoră la adresa democrației. Conform proiectului legislativ național[14], *deep fake* reprezintă orice conținut falsificat, de tip imagine, audio și/sau video realizat, de regulă, cu ajutorul inteligenței artificiale, a realității virtuale, a realității augmentate sau a altor mijloace, astfel încât să creeze aparența că o persoană a spus sau a făcut lucruri cu consimțământul său. În realitate, acestea nu au fost spuse sau făcute de acea persoană niciodată.

În această secțiune a lucrării am prezentat principalele probleme care sunt reliefate de discuția asupra amenințărilor de tip hibrid cum ar fi: tensiunea dintre respectarea drepturilor și libertăților individuale, specifică regimurilor politice democratice și asigurarea unui răspuns eficient în raport cu actorii care urmăresc influențarea proceselor democratice profitând de această transparență și deschidere a democrațiilor. De asemenea, am arătat că este dificilă formularea unei definiții unanim acceptate a amenințărilor hibride, dar că au avut loc demersuri semnificative în acest sens. În cele ce urmează vom aborda problematica privind competența teritorială și materială în domeniul combaterii amenințărilor hibride.

[12] Definiție disponibilă în Codul UE privind dezinformarea, disponibil la: https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation, accesat la 4 aprilie 2024.
[13] Serviciu European de Acțiune Externă, *op. cit.*, pg. 4.
[14] A se vedea Proiectul de Lege PL-x nr. 471/2023 privind utilizarea responsabilă a tehnologiei în contextul fenomenului deep fake. Disponibil la: https://www.cdep.ro/pls/proiecte/upl_pck2015.proiect?idp=20853, accesat la 5 aprilie 2024.

2. Competența teritorială în materie de combatere a amenințărilor hibride

Revenind la chestiunea competenței, dificultatea din momentul de față este dată de identificarea competenței teritoriale, dar și a celei materiale a actorilor instituționali responsabili. Combaterea amenințărilor hibride este o responsabilitate complexă, care necesită o abordare multisectorială și o colaborare strânsă între instituțiile cu atribuții în acest domeniu. Deși statele membre au competență exclusivă în gestionarea amenințărilor hibride care afectează securitatea națională, apărarea și ordinea publică[15], multe dintre aceste amenințări depășesc granițele naționale și necesită o acțiune coordonată la nivel european și în spațiul euroatlantic.

O abordare eficientă a amenințărilor hibride impune o cooperare strânsă între nivelul statelor membre și nivelul cel comunitar (al UE). Politicile și instrumentele UE pot contribui semnificativ la consolidarea gradului de conștientizare a amenințărilor hibride, la îmbunătățirea capacității statelor membre de a preveni și de a răspunde la atacuri hibride și la consolidarea rezilienței generale a Uniunii Europene. Acțiunea externă a Uniunii Europene, care urmărește printre altele și combaterea amenințărilor hibride, este ghidată de principiile fundamentale ale democrației, statului de drept, respectării drepturilor omului și a dreptului internațional.

3. Competența materială privind combaterea amenințărilor hibride

Dată fiind competența exclusivă a statelor membre de a gestiona aspectele aferente amenințărilor hibride, problema se ramifică, urmând să stabilim autoritatea competentă în acest sens. Fără să sugerăm că am avea soluții concrete sau răspunsuri la definirea/deslușirea acestor zone de vid legislativ, putem afirma că nivelul de complexitate și dinamism al atacurilor hibride implică în mod imperativ cooperarea dintre toți actorii implicați, problematica stabilirii competenței având relevanță doar pentru clarificarea gestionării problemei.

Nu este în vigoare un act normativ care să stabilească în mod clar competența privind amenințările hibride în general, iar, în particular, există mari dileme în legătură cu competența privind dezinformarea[16], FIMI sau atacurile care utilizează IA, acestea implicând mai multe

[15] Conform art. 72-73 din Tratatului privind funcționarea Uniunii Europene versiunea consolidată publicată în Jurnalul Oficial al UE – C 326 din 26.10.2012, statele membre sunt responsabile pentru asigurarea ordinii publice și a securității interne, dar pot stabili forme de cooperare între autoritățile competente în această arie în funcție de nevoi, disponibil la: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT, accesat 23.04.2024.

[16] În baza funcției sale stipulate la art. 4 lit. G) din Regulamentul de organizare și funcționare al Autorității Electorale Permanente din 26.10.2020, publicată în M. Of. nr. 992 din 27 octombrie 2020, care prevede că AEP

elemente specifice. Putem însă identifica o direcție de politică publică în acest sens prin consultarea *Strategiei naționale de apărare a țării 2020 – 2024*.[17] Contracararea amenințărilor hibride apare ca parte a obiectivului general de creștere a capacității sistemelor naționale de prevenire și de gestionare a situațiilor de criză interne și externe, militare sau de natură civilă, a mecanismelor de cooperare interinstituțională și capabilităților de combatere a amenințărilor asimetrice și hibride, care pot să asigure reziliența statului în situații de urgență ori de criză și să permită funcționarea continuă a instituțiilor și a serviciilor esențiale[18]. Concret, un obiectiv național de securitate este reprezentat de creșterea nivelului de reziliență în raport cu riscurile și amenințările asimetrice și de tip hibrid, de natură a afecta securitatea națională a României.

Pentru a contribui la dezbaterea care are loc în acest sens, am identificat trei cauze care ar putea determina riscul unui conflict de competență în cazul gestionării potențialelor riscuri ale acțiunilor hibride:

1. Complexitatea activităților de natură hibridă face dificilă atât autosesizarea, cât și chiar sesizarea autorităților care desfășoară activități în sectorul dedicat;
2. Lipsa unei definiții unice duce la dificultatea gestionării atacurilor de tip hibrid, prin dificultatea identificării cadrului legal aplicabil;
3. Lipsa unor pârghii care să poată facilita acțiunea imediată. Ne gândim, în acest sens, la faptul că de multe ori conținutul în cauză poate fi diseminat pe spațiul platformelor sociale și de comunicare.

Elementele menționate presupun, din partea legiuitorului, o abordare cuprinzătoare, dar flexibilă în același timp, dat fiind faptul că ne referim la un fenomen aflat în desfășurare și continuă evoluție, astfel încât eventuala rezolvare privind atribuirea competenței materiale ar putea lua trei forme:

- Înființarea unei noi structuri sau chiar a unei noi instituții cu atribuții specifice în acest sens;

„promovează alegerile libere și corecte și urmărește formarea și dezvoltarea atitudinilor și a comportamentelor democratice ale alegătorilor”, Autoritatea Electorală Permanentă a elaborat, în contextul alegerilor din 2024, un Ghid de prevenire și combatere a acțiunilor de dezinformare a alegătorilor, acesta este disponibil la: https://www.roaep.ro/prezentare/wp-content/uploads/2024/03/GHID_GLFN_FINAL.pdf accesat 23.04.2024.

[17] Administrația Prezidențială, Strategia națională de apărare a țării pentru perioada 2020 – 2024, disponibilă la: https://www.presidency.ro/files/userfiles/Documente/Strategia_Nationala_de_Aparare_a_Tarii_2020_2024.pdf, accesată la 4 aprilie 2024.

[18] *Ibidem*, p. 15.

- Extinderea competenței uneia dintre instituțiile care gestionează momentan, marginal amenințările hibride;
- Înființarea unei comisii / unui grup de lucru interinstituțional care să aibă atribuții în acest sens.

Această soluție a legiuitorului pe termen lung trebuie să țină cont de foarte mulți factori, între care cei pe care i-am amintit anterior în legătură cu caracteristicile amenințărilor hibride. Dat fiind faptul că nu avem o abordare unitară în momentul de față la nivel național sau chiar al Uniunii Europene privind definirea fenomenelor ce intră în sfera amenințărilor hibride, considerăm că soluția ce trebuie abordată în momentul de față ar putea fi una provizorie, în contextul anului electoral 2024.

4. Exemple din Finlanda și Regatul Unit privind cooperarea instituțională în materie de combatere a amenințărilor hibride

Ordonanța de urgență nr. 104/2021 privind înființarea Directoratului Național de Securitate Cibernetică[19] stabilește pentru această instituție mai multe funcții, dintre care amintim: funcția de autoritate competentă la nivel național de reglementare, supraveghere și control - asigură reglementarea și gestionarea securității cibernetice a României și a spațiului cibernetic național civil; funcția de CSIRT (*Computer Security Incident Response Team*) național; funcția de echipă de răspuns la incidente de securitate cibernetică pentru produse și servicii informatice utilizate în cadrul sectorului guvernamental; funcția de evaluare a securității cibernetice a noilor tehnologii.

Ne putem imagina un context în care, printr-un atac de tip hibrid, DNSC poate fi sesizat. Această ipoteză nu se depărtează de realitate, incidente similare având loc deja în Slovacia și în Spania. În cadrul alegerilor din aceste state, tehnologiile de tip *deep fake* au fost utilizate pentru a induce în eroare publicul cu privre la anumite informații provenind din surse, aparent oficiale. Astfel de practici pot potența atacuri de tip *phishing*, în care mii de utilizatori pot fi afectați. Cu toate acestea, în contextul în care același incident ar implica mesaje de dezinformare electorală, nu este deloc exagerat să ne gândim la competența Consiliului Național al Audiovizualului, a Poliției Române sau chiar a Autorității Electorale Permanente.

[19] Ordonanța de urgență nr. 104/2021 privind înființarea Directoratului Național de Securitate Cibernetică, publicată în M. Of nr. 918 din 24 septembrie 2021, disponibilă la: https://legislatie.just.ro/Public/DetaliiDocumentAfis/246652, accesată la 5 aprilie 2024.

Astfel de zone de vid de reglementare pot fi identificate în mai multe state, deoarece domeniul analizat este unul cu caracter de noutate. Există însă state europene care pot fi considerate ca un potențial model în formarea unui *Grup de cooperare pentru securitatea și siguranța alegerilor*.

Fără a oferi o soluție de reglementare formală a competenței pe aceste zone, putem spune că **Finlanda** este un bun exemplu în materie de soluții alternative, destinate în mod special contextului electoral. În Finlanda, un astfel de grup este prezidat de Ministerul Justiției, care deține și autoritatea electorală. Acest grup acoperă toate aspectele legate de alegerile naționale, inclusiv riscurile cibernetice. Grupul este format din următoarele instituții:

- Ministerul Justiției;
- Centrul Registrului Juridic (responsabil cu sistemul informatic principal pentru alegeri);
- Biroul Prim-ministrului (responsabil în Finlanda pentru coordonarea ministerelor și, de asemenea, organismul de experți pentru combaterea FIMI);
- Serviciul finlandez de securitate și informații;
- Ministerul Afacerilor Externe (responsabil cu organizarea votului din străinătate);
- Centrul Național de Securitate Cibernetică (responsabil pentru conștientizarea situațiilor legate de securitate cibernetică și coordonarea gestionării incidentelor cibernetice majore);
- Biroul Național de Investigații (poliția națională, responsabilă cu cercetarea preliminară în cauzele penale dar și cu siguranța fizică a secțiilor de votare și a candidaților);
- Comitetul de Securitate (responsabil cu asistența guvernului finlandez și a ministerelor în probleme de securitate).

Acest grup operează la nivel strategic pentru a împărtăși informații cu privire la toate aspectele bunei desfășurări a alegerilor. Începe să se întâlnească cu circa șase luni înainte de ziua votării cu o periodicitate lunară a ședințelor[20].

Un alt exemplu al unor practici de cooperare în vederea abordării riscurilor emergente față de procesul electoral poate fi identificat în **Regatul Unit al Marii Britanii și Irlandei de**

[20] Materialele și informațiile privind grupul de cooperare sunt disponibile la: https://oikeusministerio.fi/en/project?tunnus=OM026:00/2020, accesat la 4 martie 2024.

Nord. Pe 28 noiembrie 2023 a fost activat grupul de lucru *Defending Democracy Taskforce.* Acesta va lucra cu Guvernul, Parlamentul, Administrațiile locale, Serviciile de Informații, administratorii infrastructurilor electorale, dar și cu mediul privat în scopul asigurării securității și rezilienței proceselor electorale în fața amenințărilor multiple. Sfera acoperită de amenințările hibride include:

- FIMI;
- dezinformare;
- amenințări fizice și cibernetice la adresa instituțiilor democratice și a funcționarilor lor; interferența străină în funcții publice, partide politice și universități;
- represiunea transnațională.

Grupul de lucru va avea ca scop inclusiv asigurarea securității oficialilor aleși, asigurându-se că infrastructura electorală de bază este sigură. Activitatea grupului operativ va raporta Consiliului Național de Securitate (NSC)[21].

În completarea acestui grup multioperativ, și cu atribuții mai specifice, activează și *Joint Election Security and Preparedness Unit*, care coordonează activitatea de securitate și de pregătire electorală în cadrul guvernului și pe plan extern. Această structură își desfășoară cea mai mare parte a activității sale de urmărire și atenuare a riscurilor prin intermediul funcționarilor din alte departamente guvernamentale și al comunității de informații din Regatul Unit, inclusiv cu administrațiile deconcentrate, autoritățile locale și Comisia Electorală Centrală. Atribuția de coordonare derivă din situarea lor în cadrul Biroului Prim-ministrului, din punct de vedere instituțional[22].

5. Concluzii și recomandări

În contextul anului electoral 2024, amenințările hibride reprezintă o realitate care nu doar că nu poate fi ignorată, ci trebuie confruntată în mod imperativ pentru asigurarea integrității instituțiilor statului de drept. Evoluția tehnologiilor din ultimii ani, precum și

[21] Comunicat de presă al Guvernului Regatului Unit din data de 28.11.2011, disponibil la: https://www.gov.uk/government/news/ministerial-taskforce-meets-to-tackle-state-threats-to-uk-democracy, accesat la 5 martie 2024.
[22] Informație extrasă din interpelarea parlamentară UIN 12399 din 31.01.2024, disponibilă la: https://questions-statements.parliament.uk/written-questions/detail/2024-01-31/12399/, accesată la 5 martie 2024.

creșterea activității actorilor statali ostili[23] fac probabilitatea unui astfel de incident semnificativ mai ridicată. În acest context, întrebarea pe care trebuie să și-o pună autoritățile oricărui stat, nu este dacă se va întâmpla, ci când se va întâmpla un incident care implică un atac hibrid, dar mai ales, dacă autoritățile sunt pregătite în astfel de situații.

De aceea, un prim pas în abordarea problematicii va fi **eliminarea vidului reprezentat de competența concretă a uneia sau mai multor instituții**. Această problematică reclamă o viziune pe termen lung, coroborată cu strategiile naționale relevante. Până la acest moment, însă, reiterăm **nevoia de colaborare și cooperare între actorii implicați**, iar în contextul anului 2024, cel mai important an electoral din istoria recentă a României, poate fi luată în considerare crearea, prin Hotărâre de Guvern, a unui **Grup de lucru interinstituțional**, din care să facă parte și reprezentanți ai instituțiilor cu atribuții în organizarea, gestionarea și supravegherea procesului electoral, pentru a putea acoperi cât mai eficient complexitatea acestui fenomen reprezentat de amenințările hibride. Componența acestui grup ar urma să fie stabilită prin Decizie a Prim-ministrului, iar funcționarea lui ar putea lua o formă temporară în contextul alegerilor sau una permanentă, în vederea schimbului constant de informații în acest sens.

Referințe:

- Administrația Prezidențială, *Strategia națională de apărare a țării pentru perioada 2020-2024*, disponibilă la: https://www.presidency.ro/files/userfiles/Documente/Strategia_Nationala_de_Aparare_a_Tarii_2020_2024.pdf, accesată la 4 aprilie 2024.
- Comisia Europeană și Centrul European de Excelență pentru Contracararea Amenințărilor Hibride, *The landscape of hybrid threats: A conceptual model*, Publications Office of the European Union, Luxemburg, 2021, disponibil la: https://www.hybridcoe.fi/publications/the-landscape-of-hybrid-threats-a-conceptual-model/, accesat la 4 aprilie 2024.
- Comisia Europeană, Hybrid Threats, disponibil la: https://defence-industry-space.ec.europa.eu/eu-defence-industry/hybrid-threats_en, accesat la 4 aprilie 2024.

[23] Termen folosit în National Cyber Security Center Annual Review 2023, disponibil la: https://www.ncsc.gov.uk/files/Annual_Review_2023.pdf, accesat la 5 aprilie 2024.

- Comisia Europeană, Codul UE privind dezinformarea, disponibil la: https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation, accesat la 4 aprilie 2024.
- Comunicarea Comisiei către Parlamentul European şi Consiliu privind cadrul comun privind contracararea ameninţărilor hibride - JOIN/2016/018 final, disponibilă la: https://eur-lex.europa.eu/legal-content/ro/TXT/?uri=CELEX:52016JC0018, accesată la 27 februarie 2024.
- Guvernul Regatului Unit, Ministerial Taskforce meets to tackle state threats to UK democracy, comunicat de presă din data de 28.11.2011, disponibil la: https://www.gov.uk/government/news/ministerial-taskforce-meets-to-tackle-state-threats-to-uk-democracy, accesat la 4 aprilie 2024.
- Krátka V., Poleščuk Š. & A., *Raportul de cercetare nr. 10 - Prevenirea interferenţelor electorale: Bune practici şi recomandări,* The European Centre of Excellence for Countering Hybrid Threats, 2023 disponibil la: https://www.hybridcoe.fi/wp-content/uploads/2023/09/20230912-Hybrid-CoE-Research-Report-10-PEI-WEB.pdf, accesat la 27 februarie 2024.
- Ministerul Justiţiei din Finlanda, Cooperation group on election security preparedness, disponibil la: https://oikeusministerio.fi/en/project?tunnus=OM026:00/2020, accesat la 4 martie 2024.
- Molly K Mckew, The Gerasimov Doctrine, Politico, Septembrie – Octombrie 2017, disponibil la: https://www.politico.com/magazine/story/2017/09/05/gerasimov-doctrine-russia-foreign-policy-215538/, accesat la: 4 aprilie 2024.
- NATO, Countering hybrid threats, disponibil la: https://www.nato.int/cps/en/natohq/topics_156338.htm, accesat la 19 martie 2024.
- National Cyber Security Centre, National Cyber Security Centre Annual Review 2023, disponibil la: https://www.ncsc.gov.uk/files/Annual_Review_2023.pdf, accesat la 5 aprilie 2024.
- Ordonanţa de urgenţă nr. 104/2021 privind înfiinţarea Directoratului Naţional de Securitate Cibernetică, publicată în M. Of nr. 918 din 24 septembrie 2021, disponibilă la: https://legislatie.just.ro/Public/DetaliiDocumentAfis/246652, accesată la 5 aprilie 2024.

- Parlamentul Regatului Unit, Interpelarea parlamentară UIN 12399 din 31.01.2024, disponibilă la: https://questions-statements.parliament.uk/written-questions/detail/2024-01-31/12399/, accesată la 5 martie 2024.
- Proiectul de Lege PL-x nr. 471/2023 privind utilizarea responsabilă a tehnologiei în contextul fenomenului deep fake. Disponibil la: https://www.cdep.ro/pls/proiecte/upl_pck2015.proiect?idp=20853, accesat la 5 aprilie 2024
- Regulamentul de organizare și funcționare al Autorității Electorale Permanente din 26.10.2020, publicat în M. Of. nr. 992 din 27 octombrie 2020, disponibil la: https://www.roaep.ro/prezentare/wp-content/uploads/2024/03/GHID_GLFN_FINAL.pdf accesat 23.04.2024.,
- Serviciul European de Acțiune Externă, Countering hybrid threats (18.03.2024), disponibil la: https://www.eeas.europa.eu/eeas/countering-hybrid-threats_en, accesat la 4 aprilie 2024.
- Serviciul European de Acțiune Externă, 2nd EEAS Report on Foreign Information Manipulation and Interference Threats, disponibil la: https://www.eeas.europa.eu/eeas/2nd-eeas-report-foreign-information-manipulation-and-interference-threats_en, accesat la: 27 februarie 2024.