BULETINUL
UNIVERSITĂȚII NAȚIONALE DE APĂRARE „CAROL I"
https://buletinul.unap.ro

Cultura de securitate și reziliența organizațională în contextul războiului cibernetic: cazul României

Security Culture and Organizational Resilience in the Context of Cyberwarfare: the Case of Romania

Mihail-George GURANDA*
Dr. Dănuț MAFTEI**
*Expert Senior în Afaceri Juridice și Reglementare | Politici de Securitate Cibernetică la nivelul UE | Consilier Strategic în Politici Publice
e-mail: mihaigu@riseup.net
**Directoratul Național de Securitate Cibernetică, București, România
e-mail: dn.maftei@gmail.com

Abstract

Articolul analizează relația dintre războiul cibernetic (Cyber Warfare), cultura de securitate și reziliența organizațională în România, din perspectiva interacțiunii dintre cadrul normativ, arhitectura instituțională și practicile de guvernanță publică. În contextul extinderii conflictelor hibride și al convergenței dintre dimensiunea tehnică, strategică și cognitivă a amenințărilor, cultura de securitate nu mai poate fi tratată ca o temă auxiliară, ci ca o condiție a rezilienței organizaționale și statale. Metodologic, lucrarea utilizează o cercetare calitativă, bazată pe analiză doctrinară, analiză juridico-instituțională și studiu de caz asupra României, având ca repere legislația națională relevantă, acquis-ul Uniunii Europene, documente instituționale ale DNSC, ENISA și NATO, precum și literatura academică de specialitate. Argumentul central este că arhitectura normativă și instituțională dezvoltată recent în România, în special prin Legea nr. 58/2023, OUG nr. 155/2024, prin operaționalizarea SNAC și conectarea la mecanismele NIS2, creează premise pentru consolidarea culturii de securitate și rezilienței, fără a garanta automat internalizarea comportamentelor de securitate.

This article examines the relationship between Cyber Warfare, security culture, and organizational resilience in Romania through the interaction of the legal framework, institutional architecture, and public governance practices. In the context of expanding hybrid conflicts and the convergence of technical, strategic, and cognitive threat dimensions, security culture can no longer be treated as a secondary issue, but as a condition for organizational and state resilience. Methodologically, the study relies on qualitative research combining doctrinal analysis, legal-institutional analysis, and a case study of Romania, drawing on relevant national legislation, the European Union acquis, institutional documents issued by DNSC, ENISA, and NATO, as well as relevant academic literature. The central argument is that Romania's recently developed normative and institutional architecture, particularly Law no. 58/2023, G.E.O. no. 155/2024, the operationalization of SNAC, and integration with NIS2 mechanisms, creates premises for strengthening security culture and resilience, without automatically guaranteeing the internalization of security behaviours.

Cuvinte-cheie:
război cibernetic; cultură de securitate; securitate cibernetică; apărare cibernetică; crize cibernetice; amenințări; reziliență; guvernanță cibernetică.

Keywords:
Cyber Warfare; Security Culture; Cybersecurity; Cyber Defense; Cyber Crisis; Threats; Resilience; Cyber Governance.

Info articol
Primit: 13 februarie 2026; Evaluat: 23 februarie 2026; Acceptat: 17 martie 2026; Disponibil online: 8 aprilie 2026

Citare: Guranda, M.G. și D. Maftei. 2026. „Cultura de securitate și reziliența organizațională în contextul războiului cibernetic: cazul României." *Buletinul Universității Naționale de Apărare „Carol I"*, 15(1): 138-151. https://doi.org/10.53477/2065-8281-26-09

Introducere

În ultimul deceniu, războiul cibernetic (*Cyber Warfare*) a modificat profund modul în care statele percep raportul dintre securitate, conflict și funcționarea instituțiilor publice. Spre deosebire de amenințările informatice tradiționale, asociate predominant criminalității sau protecției tehnice a rețelelor, războiul cibernetic se înscrie într-o logică strategică mai amplă, în care operațiunile digitale pot fi folosite pentru spionaj, perturbarea serviciilor critice, coerciție, influență străină și slăbirea încrederii publice în instituțiile democratice (Lin 2012, 515-531).

Analiza amenințărilor atribuite grupărilor APT (*Advanced Persistent Threat*) ilustrează gradul ridicat de sofisticare al operațiilor cibernetice derulate de către diverși actori statali. Astfel, gruparea APT43 (alias *Kimsuky*), sprijinită de Coreea de Nord, a devenit un simbol al acestei evoluții, desfășurând activități complexe de spionaj și de culegere de informații strategice din domeniile diplomatic, tehnologic și apărare (Mishra 2025). Această grupare malițioasă combină tehnici avansate de persistență și de exploatare a instrumentelor legitime ale sistemelor de operare, ocolind metodele convenționale de detecție și afectând instituții guvernamentale, think-tankuri, centre de cercetare și infrastructuri informaționale critice din statele membre (SM) UE, din Statele Unite ale Americii, din Japonia sau din Coreea de Sud.

O tendință similară se observă în cazul capabilităților rusești asociate grupului *Curly COMrades*, care utilizează tehnologii de virtualizare pentru a ascunde cod malițios într-un mediu izolat, reducând drastic posibilitatea de detectare (Lyons 2025). Această inovație ofensivă demonstrează folosirea creativă a tehnologiilor legitime în scopuri ostile și marchează schimbarea paradigmei defensive: simpla detecție la nivel de endpoint devine insuficientă în fața amenințărilor care exploatează arhitecturi virtualizate și mecanisme de persistență dinamică.

Această transformare are consecințe directe asupra culturii de securitate. În paradigma clasică, securitatea cibernetică era tratată frecvent ca problemă de specialitate tehnică. Pe de altă parte, în paradigma actuală, ea devine o problemă de guvernanță, de comportament organizațional, de coordonare interinstituțională și reziliență societală. Literatura de specialitate evidențiază că o cultură de securitate cibernetică matură presupune nu doar reguli și controale, ci și valori, atitudini, practici și mecanisme de învățare care influențează comportamentul concret al actorilor organizaționali (Huang și Pearlson 2019).

În cazul României, această evoluție este deosebit de relevantă. Tranziția de la o abordare fragmentată a securității cibernetice către un model mai coerent de guvernanță a crizelor și de alertare cibernetică este indicată de:

- dezvoltările legislative recente, precum Legea nr. 58/2023 privind securitatea și apărarea cibernetică a României, OUG nr. 155/2024 privind instituirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil (Guvernul României 2024);

- dezvoltările instituționale, precum înființarea Directoratului Național de Securitate Cibernetică (DNSC), operaționalizarea Sistemului Național de Alertă Cibernetică (SNAC), precum și integrarea în mecanismele Directivei (UE) 2022/2555 – NIS2 (EUR-Lex 2022) și ale *Rețelei Europene a Organizațiilor de Legătură în materie de Crize Cibernetice (European Cyber Crisis Liaison Organisation Network* / EU-CyCLONe).

Cu toate acestea, existența unei arhitecturi normative și instituționale mai robuste nu rezolvă automat problema centrală a reziliență: modul în care normele, procedurile, mecanismele de alertă și cooperarea interinstituțională se traduc în practici stabile, în reflexe organizaționale și încredere publică. Aceasta este, în esență, problema culturii de securitate.

Lucrarea pornește de la următoarea întrebare de cercetare: **În ce măsură și prin ce mecanisme arhitectura normativă și instituțională a securității cibernetice din România contribuie la dezvoltarea culturii de securitate și a rezilienței organizaționale în contextul războiului cibernetic?**

În raport cu această întrebare, articolul formulează trei ipoteze de lucru:

- Ipoteza 1: claritatea normativă și distribuția formală a competențelor sporesc capacitatea de coordonare în crize cibernetice.
- Ipoteza 2: mecanismele de alertă, cooperarea interinstituțională și comunicarea publică pot favoriza internalizarea comportamentelor de securitate.
- Ipoteza 3: în absența unor indicatori de implementare și a unor date sistematice privind conformarea și învățarea instituțională, efectul cadrului juridic asupra culturii de securitate rămâne unul plauzibil, dar numai parțial demonstrabil.

În condițiile prezentate, articolul propune, pe de-o parte, o reordonare conceptuală a relației dintre războiul cibernetic, cultura de securitate și reziliența organizațională, iar pe de altă parte, oferă o analiză structurată a cazului României, plasând evoluțiile normative și instituționale interne în contextul convergenței UE - NATO și al exigențelor europene recente privind managementul incidentelor și crizelor cibernetice.

1. Cadrul conceptual

Claritatea conceptuală este esențială pentru orice analiză științifică a securității cibernetice. În lipsa unei delimitări riguroase, noțiuni precum „război cibernetic", „cultură de securitate" și „reziliență organizațională" tind să fie folosite metaforic sau interschimbabil, ceea ce afectează atât coerența argumentului, cât și posibilitatea evaluării empirice.

1.1. Războiul cibernetic

În literatura de specialitate, *Cyber Warfare* nu se reduce la simpla existență a unor atacuri informatice. El descrie folosirea capacităților cibernetice într-o logică strategică de conflict, în special de către state sau actori, sponsorizați de diverse state

și guverne, pentru a produce efecte politice, militare, economice sau psihologice negative asupra unui adversar. Analizele conflictelor cibernetice subliniază tocmai dificultatea de a separa dimensiunea tehnică a atacului de finalitatea sa strategică și de efectele sale asupra ordinii politice și instituțiilor (Sutton și Tompson 2023).

În sensul prezentului articol, putem defini Cyber Warfare ca fiind ansamblul acțiunilor ofensive, defensive și de influență, desfășurate în și prin spațiul cibernetic, în scopul afectării capacității de funcționare, decizie, încredere sau rezistență a unui stat, a unor instituții ori a unor infrastructuri informaționale critice. Acesta se desfășoară în mediul informațional, cu agenți și cu ținte atât în domeniul fizic, cât și în cel nonfizic, iar nivelul de violență poate varia, în funcție de circumstanțe (Taddeo 2012). Această definiție permite includerea atât a dimensiunii tehnice, cât și a celei cognitive și instituționale.

1.2. Cultura de securitate

Conceptul de *cultură de securitate* trebuie separat de simpla conformare formală. Literatura relevantă în domeniu precizează că o cultură de securitate presupune un set de valori, credințe, atitudini și comportamente împărtășite, care influențează modul în care membrii unei organizații înțeleg riscurile, reacționează la reguli și participă la protecția activelor digitale. Modelele recente accentuează legătura dintre cultură și comportament, educația, leadershipul, normele de grup, comunicarea și sistemele de recompensă, influențând direct conduita de securitate.

Cultura de securitate este definită în România de *Ghidul Strategiei Naționale de Apărare a Țării pentru perioada 2015-2019*. Documentul în cauză definește cultura de securitate ca fiind reprezentată de totalitatea acelor valori, norme, atitudini sau acțiuni care determină înțelegerea și asimilarea la nivelul unei societăți a conceptului de securitate și a celor derivate (securitate națională, internațională, colectivă, insecuritate, politică de securitate etc.) (Administrația Prezidențială 2015). Astfel, actorii relevanți (instituții, organizații și cetățeni) percep riscurile cibernetice, acordă importanță securității și acționează coerent pentru prevenirea, raportarea și gestionarea incidentelor.

În sensul prezentului articol, subliniem și existența unei *culturi de securitate cibernetică*, aceasta fiind reprezentată atât de normele și de valorile pe care membrii unei organizații le au în ceea ce privește securitatea cibernetică, cât și de modul în care acestea se manifestă în comportamentul lor (Sutton și Tompson 2023).

1.3. Reziliența organizațională

Noțiunea de *reziliență organizațională* este utilizată frecvent în dezbaterile de securitate, dar adesea fără operaționalizare. Aceasta este descrisă de literatura recentă de specialitate ca o *capacitate multifazică*, ce include anticiparea și pregătirea, rezistența și răspunsul, recuperarea și învățarea ulterioară.

Conform definiției oferite de The British Standards Institution (BSI), reziliența organizațională este reprezentată de capacitatea unei organizații de a anticipa, de a

se pregăti, de a răspunde și de a se adapta la schimbări și perturbări bruște pentru a supraviețui și a prospera (Hilio 2025). În cazul Cyber Warfare, aceasta presupune flexibilitate, agilitate și inovație în fața provocărilor, precum și menținerea funcțiilor esențiale în timpul unui incident cibernetic, recuperarea într-un interval rezonabil și integrarea lecțiilor învățate în politici, proceduri și viitoare arhitecturi.

1.4. Relația dintre concepte

Relația dintre cele trei concepte poate fi formulată astfel: *Cyber Warfare* reprezintă mediul conflictual și tipul de presiune strategică; *cultura de securitate* reprezintă dimensiunea socioorganizațională prin care actorii percep și internalizează riscul; *reziliența organizațională* reprezintă capacitatea efectivă de a face față perturbării. În această logică, cultura de securitate nu este sinonimă cu reziliența, dar constituie una dintre premisele esențiale pentru atingerea acesteia.

2. Metodologie

Articolul utilizează o metodologie calitativă, structurată în jurul a trei metode complementare: analiza doctrinară, analiza juridico-instituțională și studiul de caz. Această opțiune metodologică este adecvată, deoarece obiectul cercetării nu vizează măsurarea statistică a comportamentelor individuale, ci examinarea raportului dintre norme, instituții, mecanisme de coordonare și concepte de securitate într-un context național specific.

Analiza doctrinară urmărește delimitarea conceptelor-cheie și plasarea lor în literatura de specialitate privind *Cyber Warfare, cultura de securitate* și *reziliența organizațională*. Analiza juridico-instituțională examinează actele normative și documentele relevante care definesc competențele, mecanismele de alertă și arhitectura de coordonare la nivel național și european. Studiul de caz aplică aceste repere asupra României, cu accent pe DNSC, SNAC, Consiliul Operativ de Securitate Cibernetică (COSC), Centrul Național de Gestionare a Crizelor de Securitate Cibernetică (CNGCSC) și integrarea cu mecanismele europene, prevăzute de Directiva NIS2 .

Corpusul analizat include legislație națională, norme și metodologii administrative, documente europene, surse instituționale ENISA (ENISA 2026b), DNSC (DNSC 2026) și NATO (NATO 2026b), precum și lucrări academice relevante pentru cultura de securitate și reziliență. Din perspectiva designului cercetării, România este tratată ca ”*most likely case*” pentru analiza modului în care consolidarea juridică și instituțională poate crea premise pentru maturizarea culturii de securitate, fără ca acest fapt să demonstreze automat existența unei relații cauzale complet validate empiric.

Pentru a evita afirmațiile speculative, în lucrare este folosit un set explicit de criterii analitice pentru evaluarea contribuției cadrului normativ și instituțional la cultura de securitate și reziliență: claritatea rolurilor și competențelor; existența mecanismelor

de alertă și escaladare (DNSC 2025); capacitatea de coordonare interinstituțională; integrarea comunicării publice; includerea exercițiilor, planificării și învățării; alinierea la mecanismele europene și euroatlantice.

Limitele cercetării sunt corelate cu faptul că cercetarea științifică nu a inclus interviuri, anchete sociologice, seturi de indicatori cantitativi sau comparații sistematice între mai multe state. Din acest motiv, concluziile privind efectele asupra culturii de securitate sunt formulate prudent, în termeni de „premise instituționale", „mecanisme favorizante" sau „condiții de posibilitate", nu ca demonstrații empirice definitive.

3. Arhitectura europeană a rezilienței cibernetice

În ultimii ani, Uniunea Europeană a trecut de la o abordare centrată predominant pe cooperarea tehnică la o arhitectură mai complexă de management al incidentelor și crizelor cibernetice (ENISA 2026a). În această evoluție, ENISA, Rețeaua UE a Echipelor de Intervenție în caz de Incidente de Securitate Cibernetică *(Cyber Security Incident Response Teams*/CSIRTs Network) și, mai recent, EU-CyCLONe au devenit elemente centrale ale unei guvernanțe multinivel orientate nu doar spre răspuns tehnic, ci și spre coordonare strategică și conștientizare situațională comună (EUR-Lex 2022).

Directiva NIS2 este deosebit de relevantă, aceasta conținând prevederi care structurează cooperarea dintre statele membre ale UE în jurul unor obligații mai clare privind managementul riscurilor, notificarea incidentelor, coordonarea și pregătirea. Articolul 16 al Directivei NIS2 consacră rolul EU-CyCLONe în coordonarea strategică a incidentelor și crizelor cibernetice de amploare, completând rolul mai tehnic al CSIRTs Network.

Această dualitate tehnic - strategic este importantă pentru subiectul cercetat. Ea sugerează că reziliența cibernetică nu mai poate fi redusă doar la capabilitatea tehnică de detecție și remediere (EUR-Lex 2024), ci presupune și mecanisme instituționale de interpretare, decizie, comunicare și cooperare între diferite niveluri de guvernanță. Din această perspectivă, modelul european oferă un cadru util pentru înțelegerea modului în care securitatea cibernetică este integrată progresiv în logica mai largă a rezilienței democratice și instituționale.

În plus, inițiativele europene privind exercițiile de criză, rezerva de securitate cibernetică și interoperabilitatea transfrontalieră indică o mutație doctrinară importantă: accentul se deplasează de la securizarea infrastructurilor către pregătirea sistemelor publice pentru continuitate, cooperare și recuperare. Această mutație are consecințe directe pentru statele membre ale UE, inclusiv pentru România, deoarece obligă instituțiile naționale să dezvolte mecanisme compatibile atât tehnic, cât și procedural.

4. Cadrul normativ și instituțional din România

4.1. De la fragmentare la coordonare

În plan național, evoluțiile recente indică o consolidare a arhitecturii de securitate și apărare cibernetică. Prin OUG nr. 104/2021, (art.3 lit. [o] și art. 17), a fost întărit rolul DNSC în managementul crizelor cibernetice pe timp de pace și au fost create premisele instituționale pentru funcționarea unui centru național de gestionare a crizelor de securitate cibernetică (Guvernul României 2021).

Legea nr. 58/2023 a aprofundat această dezvoltare, configurând un cadru instituțional integrat pentru gestionarea riscurilor, incidentelor și crizelor cibernetice. Din perspectiva prezentului studiu, importanța legii nu constă doar în introducerea unor obligații și competențe, ci și în formalizarea unei logici de coordonare strategică între diferite niveluri instituționale (Parlamentul României 2023).

Rolul COSC, relația acestuia cu DNSC și Consiliul Suprem de Apărare a Țării – CSAT, precum și mecanismele asociate nivelurilor de alertă cibernetică indică o încercare de a depăși fragmentarea tradițională a responsabilităților (CSAT 2026). În termeni analitici, aceasta poate fi interpretată ca o condiție favorabilă pentru cultura de securitate, întrucât claritatea responsabilităților și existența unui lanț decizional reduc ambiguitatea organizațională și sporesc predictibilitatea răspunsului.

4.2. Operaționalizarea SNAC

Operaționalizarea Sistemului Național de Alertă Cibernetică, în baza Ordinului DNSC nr. 180/2024 pentru aprobarea Metodologiei privind nivelurile de alertă cibernetică și modalitățile de acțiune în situații de alertă cibernetică (DNSC 2024) constituie unul dintre cele mai relevante elemente pentru tema prezentului articol. SNAC nu este doar un instrument tehnic de semnalare a riscurilor, ci și un mecanism cu potențial cultural și organizațional, deoarece conectează analiza tehnică, decizia instituțională și comunicarea publică.

Din perspectiva culturii de securitate, relevanța SNAC rezultă din trei elemente: standardizarea reacției prin niveluri de alertă și planuri de acțiune asociate; includerea actorilor privați și sectoriali în logica alertării și a pregătirii; dimensiunea de comunicare publică, ce creează posibilitatea trecerii de la o guvernanță exclusiv tehnică la una care vizează comportamente și percepții sociale.

Totuși, este important să se facă următoarea precizare metodologică: faptul că SNAC este conceput să contribuie la conștientizare și coordonare nu demonstrează automat efectul său real asupra culturii de securitate. În absența unor date privind gradul de înțelegere publică a alertelor, nivelul de conformare al actorilor vizați sau impactul exercițiilor și al notificărilor asupra comportamentelor, concluzia adecvată este că SNAC instituie un mecanism cu potențial de cultură de securitate, nu că produce deja, în mod demonstrat, maturizare societală.

4.3. Integrarea cu mecanismele europene

Un element important al cazului românesc îl reprezintă conectarea arhitecturii naționale la mecanismele prevăzute de Directiva NIS2. OUG nr. 155/2024 și aprobarea sa ulterioară prin Legea nr. 124/2025 (Parlamentul României 2025) care au consolidat această aliniere prin consacrarea DNSC ca autoritate națională de gestionare a crizelor cibernetice pe timp de pace și ca punct de contact pentru EU-CyCLONe.

În 2024, România a demonstrat aplicarea practică a acestui cadru prin activarea procedurilor aferente, în contextul securității alegerilor. În acest context, DNSC a operat simultan în relație cu:

- ENISA, pentru suport strategic și instrumente de schimb de informații;
- EU-CyCLONe, unde nivelul rețelei a fost escaladat la modul Avertizare (*Warning Mode*), activând canalele dedicate și cooperarea operațională;
- Rețeaua ofițerilor de legătură ENISA (NLO Network), pentru briefinguri și solicitări de informații;
- EU CSIRTs Network, unde s-a discutat trecerea la modul Cooperare Alerte (*Alert Cooperation Mode*) și s-au transmis date tehnice relevante.

Exemplul este important, deoarece evidențiază trecerea de la simpla transpunere legislativă la utilizarea operațională a canalelor de cooperare.

Din punct de vedere analitic, aceste aspecte susțin ideea că reziliența nu este doar o proprietate internă a statului, ci și rezultatul apartenenței la o arhitectură mai largă de cooperare. În acest sens, cultura de securitate instituțională trebuie înțeleasă și ca o cultură a interoperabilității, a schimbului de informații și a reflexelor comune de acțiune (Cheng 2023).

Din aceeași perspectivă, convergența UE-NATO completează dimensiunea europeană a rezilienței cibernetice. Pentru România, relevanța NATO nu constă doar în dimensiunea militară strictă, ci și în integrarea civil–militară a planificării, exercițiilor și evaluării riscului strategic. Mecanisme precum Cyberspace Operations Centre (CyOC), NATO Integrated Cyber Defence Centre (NICC) și CCDCOE oferă un cadru util pentru lecții învățate, exerciții și interoperabilitate doctrinară, în timp ce inițiative precum *Defence Innovation Accelerator for the North Atlantic* (DIANA 2026) și *NATO Innovation Fund* (NATO 2026a) indică faptul că inovația tehnologică și cooperarea cu sectorul civil devin parte a ecosistemului mai larg de apărare și reziliență digitală (NATO 2025). În acest sens, această convergență întărește ideea rezilienței ca produs al cooperării multinivel, nu doar al capacității naționale.

4.4. Control democratic și legitimitate constituțională

Jurisprudența Curții Constituționale a României – CCR conturează un cadru clar: **securitatea rețelelor și a sistemelor informatice nu mai este un domeniu pur tehnic, ci unul de interes general, aflat în strânsă interdependență cu securitatea națională** (CCR 2026).

Acest aspect este relevant nu doar din punct de vedere juridic, ci și în plan conceptual. Prin Decizia nr. 17/2015, Curtea Constituțională a României trasează o linie politică

și instituțională clară: **coordonarea securității cibernetice la nivel național trebuie să fie exercitată de un organism civil, sub control democratic, nu de structuri de informații, de aplicare a legii sau de apărare** (CCR 2015).

Opțiunea coordonării securității cibernetice la nivel național contează pentru cultura de securitate din cel puțin două motive. În primul rând, legitimitatea și încrederea publică pot fi afectate de percepția asupra instituțiilor care coordonează securitatea. În al doilea rând, o cultură de securitate democratică nu poate fi construită durabil în afara exigențelor de claritate normativă, de proporționalitate și protecție a drepturilor fundamentale.
Prin urmare, cadrul constituțional și convențional nu este exterior rezilienței, ci face parte din condițiile ei. O reziliență construită prin măsuri opace, disproporționate sau insuficient controlate poate genera reacții de neîncredere care slăbesc chiar cultura de securitate pe care pretinde că o consolidează.

5. Impactul asupra culturii de securitate și rezilienței organizaționale

Cyber Warfare produce efecte care depășesc sfera strict tehnică a securizării rețelelor și sistemelor informatice, influențând cultura de securitate, coordonarea instituțională și capacitatea organizațiilor de a funcționa sub presiune, în condiții de stres. În acest cadru, reziliența organizațională trebuie înțeleasă nu doar ca abilitate de continuitate operațională, ci ca aptitudine de a anticipa, absorbi, adapta și integra lecțiile rezultate din incidentele cibernetice, campaniile hibride și perturbările întâmpinate la nivel strategic. În cazul României, dezvoltările legislative și instituționale recente sugerează trecerea de la o abordare predominant tehnică la una de guvernanță strategică, în care cultura de securitate devine variabila de legătură dintre norme, instituții și comportamente organizaționale.

5.1. De la protecție tehnică la cultură organizațională de securitate
Una dintre principalele consecințe ale războiului cibernetic este deplasarea accentului dinspre protecția exclusiv tehnică spre capacitatea organizațiilor de a reacționa coerent și adaptiv în condiții de stres persistent. Atacurile sofisticate, exploatarea lanțurilor de aprovizionare și campaniile de influență arată că vulnerabilitatea nu rezultă doar din lipsa controalelor tehnice, ci și din deficiențe de coordonare, de comunicare și învățare instituțională. Din această perspectivă, cultura de securitate presupune mai mult decât conformare formală: ea implică reflexe organizaționale, claritate decizională și transformarea regulilor în practici repetitive și asumate.

5.2. Arhitectura instituțională și efectele sale asupra rezilienței
În România, Legea nr. 58/2023, OUG nr. 155/2024, operaționalizarea SNAC și conectarea la mecanismele NIS2 creează premise importante pentru consolidarea rezilienței organizaționale. Acest cadru reduce fragmentarea, clarifică roluri și introduce o logică de alertare, escaladare și coordonare, care poate standardiza reacția instituțională în situații de criză. Totuși, relația dintre arhitectura instituțională

și cultura de securitate trebuie formulată prudent: existența procedurilor și a competențelor este o condiție necesară, dar nu o dovadă suficientă că organizațiile au internalizat comportamente stabile de securitate.

5.3. Dimensiunea societală și cognitivă a culturii de securitate

Impactul războiului cibernetic nu se limitează la instituții, ci se extinde asupra modului în care societatea percepe riscul și reacționează la crize digitale. În practică, efectele cele mai relevante apar atunci când incidentele cibernetice sunt însoțite de dezinformare, de presiune informațională și de perturbarea încrederii în instituții (Maftei 2025). În acest context, componenta de comunicare publică asociată SNAC este importantă, deoarece poate susține reacții mai rapide și mai proporționale, fără a transforma însă automat securitatea cibernetică într-o cultură societală matură. Rezultatul obținut va depinde de continuitatea comunicării, de credibilitatea instituțională și de capacitatea publicului de a interpreta semnalele de risc (Fomnya 2024).

5.4. Competențe, factor uman și provocarea erei Inteligenței Artificiale

Un alt efect major al transformării mediului de securitate este creșterea importanței competențelor digitale. Integrarea accelerată a Inteligenței Artificiale (IA) în procese operaționale și decizionale obligă organizațiile să gestioneze simultan riscuri cibernetice clasice și riscuri asociate interacțiunii dintre oameni, date și sisteme automate (Palma 2026). În acest cadru, reziliența depinde nu doar de tehnologie, ci și de existența unui personal capabil să înțeleagă limitele automatizării, să utilizeze critic instrumentele digitale și să păstreze controlul uman asupra proceselor sensibile (Maftei 2024).

5.5. Implicații pentru România

Pentru România, impactul războiului cibernetic asupra culturii de securitate și rezilienței organizaționale trebuie interpretat la intersecția dintre guvernanță, capacitate administrativă și pregătire profesională. Cadrul normativ recent, rolul DNSC, funcționarea SNAC și interoperabilitatea europeană oferă o infrastructură de coordonare mai robustă decât în etapa anterioară, dar efectul său de durată depinde de exerciții recurente, de evaluare, formare continuă și de integrarea lecțiilor învățate în practici instituționale.

În consecință, consolidarea culturii de securitate nu poate fi tratată ca rezultat automat al reformei legislative, ci ca proces continuu de operaționalizare, coordonare și învățare. Acest proces presupune mecanisme clare de planificare, distribuirea responsabilităților între actorii publici și privați și transformarea normelor juridice în rutine organizaționale verificabile.

În plan practic, dezvoltarea rezilienței organizaționale reclamă operaționalizarea coerentă a planificării de criză, desfășurarea periodică a exercițiilor interinstituționale, integrarea lecțiilor învățate în proceduri și consolidarea comunicării publice în situații de alertă. În același timp, responsabilitatea nu aparține exclusiv autorităților centrale, ci trebuie distribuită între instituțiile publice competente, operatorii de servicii esențiale, organizațiile private și actorii implicați în formarea profesională.

În această logică, cultura de securitate funcționează nu doar ca exigență normativă, ci și ca practică socială și organizațională, dependentă de continuitatea exercițiului instituțional, de claritatea lanțului decizional și de capacitatea actorilor relevanți de a coopera în condiții de presiune și incertitudine. Tocmai de aceea consecința esențială pentru România nu este doar consolidarea cadrului juridic, ci transformarea acestuia într-un mecanism efectiv de adaptare, coordonare și reziliență.

Concluzii

Analiza de față arată că România se află într-o etapă de consolidare normativă și instituțională semnificativă în domeniul securității și apărării cibernetice. Evoluțiile legislative și administrative recente indică existența unei arhitecturi mai clare de alertare, coordonare și interoperabilitate europeană față de perioada anterioară, mai ales prin rolul DNSC, operaționalizarea SNAC și integrarea în mecanismele asociate Directivei NIS2.

Răspunsul la întrebarea de cercetare este totuși unul nuanțat. Arhitectura normativă și instituțională a securității cibernetice din România contribuie la dezvoltarea culturii de securitate și a rezilienței organizaționale prin clarificarea rolurilor, standardizarea alertelor, întărirea coordonării și conectarea la rețele europene și euroatlantice de cooperare. Cu toate acestea, aceste evoluții trebuie interpretate prudent. Ele creează premise solide pentru consolidarea culturii de securitate, dar nu echivalează, prin ele însele, cu demonstrarea unei internalizări depline a comportamentelor de securitate la nivel organizațional și societal.
Rezultatul principal al studiului științific este așadar unul de tip condițional. România dispune de baze juridice și instituționale mai robuste pentru consolidarea rezilienței, însă efectele de durată ale acestui cadru rămân dependente de implementarea și de transformarea normelor în practici instituționale stabile.

Studiul sugerează, de asemenea, că reziliența organizațională trebuie privită într-o logică mai largă față de cea a securizării tehnice. Ea include capacitatea de coordonare instituțională, comunicarea publică, interoperabilitatea europeană și euroatlantică, precum și pregătirea unei forțe de muncă apte să opereze într-un mediu caracterizat de convergența dintre amenințări cibernetice, presiune informațională și utilizarea extinsă a IA.

În plan de politici publice, rezultă patru direcții prioritare. **Prima** dintre acestea este legată de dezvoltarea unor indicatori de maturitate pentru cultura de securitate și reziliența organizațională în sectorul public și în sectoarele esențiale. **A doua** direcție este legată de consolidarea exercițiilor naționale și a interoperabilității cu mecanismele europene și NATO, cu integrarea lecțiilor învățate în ciclul normativ și operațional. **A treia** direcție prioritară este cea a întăririi comunicării publice și a alfabetizării digitale, într-o logică de prevenție și reacție proporțională. **A patra** este reprezentată de adaptarea formării profesionale la noile riscuri asociate utilizării AI, automatizării și interacțiunii om-sistem în procesele critice.

Prin urmare, principala miză a securității și apărării cibernetice în România nu este doar dezvoltarea unor capabilități tehnice superioare, ci transformarea acestora într-o cultură instituțională și organizațională suficient de robustă pentru a susține reziliența într-un mediu strategic persistent contestat.

Referințe

Administrația Prezidențială. 2015. „Ghidul Strategiei Naționale de Apărare a Țării pentru perioada 2015-2019.” https://www.presidency.ro/ro/presa/securitate-nationala-si-aparare/ghidul-strategiei-nationale-de-aparare-a-tarii-pentru-perioada-2015-2019.

CCR. 2015. „Decizia nr. 17 din 21 ianuarie 2015 asupra obiecției de neconstituționalitate a dispozițiilor Legii privind securitatea cibernetică a României.” https://www.ccr.ro/wp-content/uploads/2020/07/Decizie_17_2015.pdf.

___. 2026. „Curtea Constituțională a României.” https://www.ccr.ro/.

Cheng, Joseph. 2023. ”Building Cyberresilience From Collaborative Culture.” https://www.isaca.org/resources/isaca-journal/issues/2023/volume-3/building-cyberresilience-from-collaborative-culture.

CSAT. 2026. „Consiliul Suprem de Apărare a Țării.” https://csat.presidency.ro/.

DIANA. 2026. ”Defence Innovation Accelerator for the North Atlantic.” https://www.diana.nato.int/.

DNSC. 2024. „Ordin nr. 180 din 21 februarie 2024 pentru aprobarea Metodologiei privind nivelurile de alertă cibernetică și modalitățile de acțiune în situații de alertă cibernetică.” https://legislatie.just.ro/Public/DetaliiDocument/279736.

___. 2025. „Raport anual de activitate 2024.” https://www.dnsc.ro/vezi/document/dnsc-raport-anual-2024.

___. 2026. „*Directoratul Național de Securitate Cibernetică.*” https://www.dnsc.ro/.

ENISA. 2026a. ”EU incident response and cyber crisis management.” https://www.enisa.europa.eu/topics/eu-incident-response-and-cyber-crisis-management.

___. 2026b. ”European Union Agency for Cybersecurity.” https://www.enisa.europa.eu/.

EUR-Lex. 2022. „Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune.” https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555.

___. 2024. „Regulamentul (UE) 2024/2847 al Parlamentului European și al Consiliului din 23 octombrie 2024 privind cerințele orizontale în materie de securitate cibernetică pentru produsele cu elemente digitale.” https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng.

Fomnya, Hyelda Joseph. 2024. „The Influence of Cybersecurity. Risk Management Practices on Organizational Resilience.” https://hallford.education/wp-content/uploads/2026/01/The-Influence-of-Cybersecurity-Risk-Management-Practices-on-Organizational-Resilience.docx.pdf.

Guvernul României. 2021. „Ordonanță de urgență nr. 104 din 22 septembrie 2021 privind înființarea Directoratului Național de Securitate Cibernetică." https://legislatie.just.ro/Public/DetaliiDocumentAfis/246652.

___. 2024. „Ordonanță de urgență nr. 155 din 30 decembrie 2024 privind instruirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil." https://legislatie.just.ro/Public/DetaliiDocumentAfis/293121.

Hilio. 2025. „Reziliența individuală și organizațională – Definiție, rol și strategii de dezvoltare." https://hilio.com/ro/blog/humancapital/ce-este-rezilienta-organizationala.

Huang, Keman, și Keri Pearlson. 2019. "For What Technology Can't Fix:Building a Model of Organizational Cybersecurity Culture." *Proceedings of the 52nd Hawaii International Conference on System Sciences.* doi:https://doi.org/10.24251/HICSS.2019.769.

Lin, Herbert. 2012. "Cyber conflict and international humanitarian law." *International Review of the Red Cross* 94 (886): 515-531. https://international-review.icrc.org/sites/default/files/irrc-886-lin.pdf.

Lyons, Jessica. 2025. "Russian spies pack custom malware into hidden VMs on Windows machines." https://www.theregister.com/2025/11/04/russian_spies_pack_custom_malware/?cid=soc%7Cn%7Csprout%7Cemp&blaid=8069358.

Maftei, Dănuț. 2024. "The Cyber Competences Act – a Vital EU Regulation Concerning Mandatory Certification of Critical Network and Information Systems' Operators across the European Union." *Informatica Economică* 28 (2): 45-60. doi:10.24818/issn14531305/28.2.2024.04.

___. 2025. "«Three Warfares» versus «Hybrid Warfare»." New Generation Warfare – New Approaches and Challenges." *Revista GeoPolitica.* https://www.geopolitic.ro/in/topics/geointellicence/page/2/.

Mishra, Siddhant. 2025. "Inside the Shellcode: Dissecting North Korean APT43's Advanced PowerShell Loader." https://systemweakness.com/inside-the-shellcode-dissecting-north-korean-apt43s-advanced-powershell-loader-e6c51b77f486.

NATO. 2025. "Request for Information (RFI) to engage with industry, academia and nations." https://www.act.nato.int/wp-content/uploads/2025/12/rfi025112.pdf.

___. 2026a. "NATO Innovation Fund." https://www.nif.fund/.

___. 2026b. "North Atlantic Treaty Organization." https://www.nato.int/en.

Palma, Bryan. 2026. "The cybersecurity paradox: training the next generation workforce." https://www.weforum.org/stories/2026/01/cybersecurity-paradox-training-the-next-generation-workforce/.

Parlamentul României. 2025. „Lege nr. 124 din 7 iulie 2025 pentru aprobarea Ordonanței de urgență a Guvernului nr. 155/2024 privind instituirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil." https://legislatie.just.ro/public/DetaliiDocument/299675.

___. 2023. „Lege nr. 58 din 14 martie 2023 privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative." https://legislatie.just.ro/Public/DetaliiDocument/265677.

Sutton, Anna și Lisa Tompson. 2023. ”Towards a Cybersecurity Culture-Behaviour Framework: A Rapid Evidence Review.” doi:https://doi.org/10.31234/osf.io/h4uby.

Taddeo, Mariarosaria. 2012. ”An analysis for a just cyber warfare.” *2012 4th International Conference on Cyber Conflict (CYCON 2012).* Tallinn, Estonia. https://ieeexplore.ieee.org/document/6243976.