Supliment al revistei „Strategic Impact”

COLOCVIU STRATEGIC

UNIVERSITATEA NAȚIONALĂ DE APĂRARE „CAROL I”
CENTRUL DE STUDII STRATEGICE DE APĂRARE ŞI SECURITATE

Nr. 6 (232) / 2025
Indexat în Crossref,
CEEOL și ROAD

DOI: 10.53477/1842-8096-25-06

APĂRAREA CIBERNETICĂ – OPORTUNITĂȚI, PROVOCĂRI ȘI ADAPTAREA LA NOILE TEHNOLOGII EMERGENTE

Claudiu-Sorin CLEOANTĂ

Cyber defense – opportunities, challenges and adapting to new emerging technologies

Abstract: *Cyber defense has become an essential component of national security in the context of emerging technologies and increasingly sophisticated cyber threats. The article discusses the opportunities offered by digitalization in strengthening defense capabilities, the main strategic and technical challenges, the need to adapt rapidly to new technologies such as AI, IoT and 5G. Based on these premises, it underlines the importance of international cooperation, the development of the regulatory framework and investments in infrastructure and specialized human resources to ensure an effective and resilient response in cyberspace.*

The paper addresses the main challenges and solutions for adapting to emerging technologies, considering that the integration of these technologies brings operational benefits but also strategic risks, requiring a permanent recalibration of defense strategies and resilience capabilities. It also explores the multidimensional implications of cyber defense, which is treated both as a context of technological and operational opportunities and as an area populated by complex legal, ethical, technical and organizational challenges.

Keywords: *cyber defense, cyber security, emerging technologies, Cyber Defense Command, threats, artificial intelligence.*

Apărarea cibernetică – oportunități, provocări şi adaptarea la noile tehnologii emergente

Rezumat: *Apărarea cibernetică a devenit o componentă esențială a securității naționale, într-un context marcat de tehnologii emergente și amenințări cibernetice tot mai sofisticate. Articolul analizează oportunitățile oferite de digitalizare în consolidarea capacităților de apărare, principalele provocări strategice și tehnice și necesitatea adaptării rapide la noile tehnologii, precum inteligența artificială, internetul lucrurilor și 5G. Plecând de la aceste premise, se subliniază importanța cooperării internaționale, a dezvoltării cadrului normativ și a investițiilor în infrastructură și resursă umană specializată pentru a asigura reziliența necesară a sistemului defensiv și o conduită eficientă, proactivă și reactivă, deopotrivă, față de oportunitățile și amenințările din spațiul cibernetic.*

Lucrarea cuprinde principalele provocări apărute și soluțiile de adaptare la tehnologiile emergente, având în vedere că integrarea acestor tehnologii aduce beneficii operaționale, dar și riscuri strategice, ceea ce impune o recalibrare permanentă a strategiilor de apărare și a capacităților de reziliență. Sunt analizate, de asemenea, implicațiile multidimensionale ale apărării cibernetice, tratând-o atât ca pe un context de oportunități tehnologice și operaționale, cât și ca pe un domeniu populat de provocări complexe de natură juridică, etică, tehnică și organizațională.

Cuvinte-cheie: *apărare cibernetică, securitate cibernetică, tehnologii emergente, Comandamentul Apărării Cibernetice, amenințări, inteligența artificială.*

Aspecte introductive

În contextul actual al transformărilor tehnologice rapide și al intensificării confruntărilor în spațiul informațional, apărarea cibernetică a devenit un domeniu esențial pentru securitatea națională și, implicit, pentru eficiența operațională a forțelor armate. Spațiul cibernetic este astăzi recunoscut ca un domeniu operațional al conflictului modern, alături de dimensiunile convenționale – terestră, aeriană, maritimă și spațială. Principalul obiectiv de cercetare al acestui demers îl reprezintă înțelegerea celor trei cadre care fundamentează apărarea cibernetică în dimensiunea militară: conceptual, operațional și tehnologic.

Se impune să întreprindem această analiză având în atenție modalitățile prin care optimizarea celor trei cadre, în special a acelui tehnologic, poate conduce la augmentarea capacității structurilor defensive de a preveni, detecta și identifica amenințarea, de a se

Claudiu-Sorin CLEOANTĂ *este colonel în cadrul Serviciului de Telecomunicații Speciale – Direcția Județeană de Telecomunicații Speciale Vâlcea, Râmnicu Vâlcea (e-mail: sorin.cleoanta@gmail.com).*

apăra și chiar contracara agresiunea și de a se recupera în urma atacurilor cibernetice. O caracteristică extrem de importantă care necesită investigație o reprezintă capacitatea sistemului defensiv de a se adapta, atât pe timpul agresiunii, cât și în context postfactum, în scopul optimizării acțiunilor viitoare. Pentru atingerea acestui obiectiv, sunt avute în vedere următoarele direcții de analiză:

- definirea noțiunilor-cheie asociate apărării cibernetice în context militar;
- identificarea amenințărilor cibernetice specifice mediului de operare al forțelor armate;
- evaluarea cadrului doctrinar și legislativ național și internațional în domeniul apărării cibernetice;
- prezentarea capabilităților și structurilor specializate din cadrul armatei, responsabile cu securitatea cibernetică;
- evidențierea provocărilor actuale și a tendințelor viitoare în ceea ce privește războiul cibernetic.

În cadrul forțelor armate, apărarea cibernetică nu se limitează la protejarea infrastructurilor IT, ci vizează întregul spectru al funcțiilor de comandă și control, comunicații, informații, supraveghere, recunoaștere și logistică, toate fiind din ce în ce mai dependente de sisteme digitale interconectate. Astfel, o breșă de securitate în rețelele cibernetice poate compromite capacitatea de reacție, eficiența misiunilor și chiar siguranța personalului militar.

Totodată, în actualul climat internațional de securitate, se observă o creștere a interesului strategic pentru dezvoltarea de capabilități de apărare activă, care includ nu doar măsuri de protecție pasivă, ci și capacitatea de a desfășura acțiuni cibernetice ofensive, în scopul descurajării sau neutralizării amenințărilor.

Într-o eră în care amenințările cibernetice devin tot mai sofisticate și distribuite, tehnologiile emergente oferă atât provocări, cât și oportunități esențiale pentru consolidarea apărării cibernetice. Inteligența artificială și învățarea automată permit detecția avansată a comportamentelor anormale în rețele informatice, sprijinind mecanismele de prevenire a atacurilor *zero-day* și a compromiterilor silențioase (Giarola et al. 2022). Algoritmii de învățare automată sunt tot mai des integrați în platforme de tip *Security Information and Event Management* (SIEM), reducând considerabil timpul de reacție și volumul alertelor false.

Internetul Lucrurilor adaugă un nou strat de complexitate, prin extinderea suprafeței de atac și apariția unor vectori de risc insuficient securizați. În același timp, datele generate de aceste dispozitive pot fi valorificate pentru întărirea vizibilității operaționale în medii critice, cu condiția implementării unor standarde stricte de securitate (Weber și Studer 2016). Similar, tehnologia 5G permite instalarea rapidă a rețelelor militare distribuite și sprijină desfășurarea operațiilor la nivel tactic în timp real, dar deschide și noi vectori de atac cibernetic, în special prin intermediul furnizorilor și echipamentelor terțe (Kshetri și Voas 2021).

O altă tehnologie emergentă cu impact major este cea care implementează calculul cuantic. Aceasta amenință să submineze criptografia tradițională utilizată în comunicațiile securizate. Din acest motiv, statele membre NATO și UE investesc în dezvoltarea unor soluții de criptografie post-cuantică, capabile să reziste algoritmilor cuantici avansați de decriptare (Mosca, 2018). În paralel, noile capabilități cibernetice impun reformularea doctrinelor militare, actualizarea procedurilor de răspuns la incident și formarea unei resurse umane specializate, adaptate la noile realități tehnologice (ENISA 2023).

Prin urmare, apărarea cibernetică eficientă nu mai poate fi concepută fără integrarea tehnologiilor emergente, în special pentru că potențialele amenințări le conțin deja. Această adaptare presupune o abordare multidisciplinară, în care securitatea, inovația și reziliența operațională trebuie să fie tratate ca elemente interdependente.

1. Comandamentul Apărării Cibernetice – rol și importanță strategică

În arhitectura instituțională a apărării naționale, *Comandamentul Apărării Cibernetice* (CApC) reprezintă structura specializată a Ministerului Apărării Naționale (MApN) responsabilă cu planificarea, coordonarea și executarea misiunilor din domeniul apărării cibernetice. Înființat ca răspuns la evoluțiile geopolitice și tehnologice recente, Comandamentul reflectă angajamentul României de a-și consolida capacitățile de apărare în spațiul cibernetic, în conformitate cu cerințele Alianței Nord-Atlantice și ale Uniunii Europene (CApC 2025).

În ansamblu, CApC acționează ca un nod critic în rețeaua de securitate națională și internațională, gestionând riscurile cibernetice emergente și sprijinind desfășurarea în siguranță a acțiunilor militare moderne. Principalul obiectiv al Comandamentului constă în asigurarea protecției și rezilienței infrastructurilor cibernetice militare, precum și în prevenirea, detectarea, neutralizarea și contracararea atacurilor cibernetice care pot afecta sistemele și rețelele aflate în responsabilitatea MApN.

Pe lângă misiunile de apărare pasivă, CApC are și un rol proactiv, implicându-se în:

- dezvoltarea de politici, proceduri și standarde privind securitatea cibernetică militară;
- coordonarea măsurilor de răspuns la incidente cibernetice;
- integrarea capabilităților cibernetice în operațiile militare comune;
- cooperarea internațională, în principal în cadrul *NATO Cyber Defence Pledge*[1];
- instruirea și dezvoltarea resursei umane specializate în domeniul apărării cibernetice (CApC 2025).

Activitatea Comandamentul Apărării Cibernetice

[1] Pentru mai multe detalii privind cadrul de cooperare *NATO Cyber Defence Pledge* consultați referința (NATO 2016).

din cadrul MApN este reglementată printr-un ansamblu de acte normative și documente strategice, care stabilesc cadrul juridic, organizatoric și funcțional al acestei structuri militare specializate. Aceste reglementări sunt esențiale pentru a asigura coerența operațională, interoperabilitatea cu aliații și adaptarea continuă la evoluțiile din domeniul securității cibernetice.

Principalul document care reglementează activitatea CApC este Hotărârea Guvernului nr. 1321/2021, prin care a fost aprobată *Strategia de Securitate Cibernetică a României pentru perioada 2022-2027*, împreună cu *Planul de acțiune* aferent acesteia. Strategia are un caracter interinstituțional și vizează crearea unui spațiu cibernetic național sigur, inclusiv prin consolidarea și dezvoltarea rezilienței capabilităților militare de apărare cibernetică. Documentul reafirmă rolul Armatei în sistemul național de securitate cibernetică și subliniază necesitatea continuării investițiilor în capabilități de apărare proactivă și reactivă în spațiul cibernetic.

Conform prevederilor strategiei, CApC este un actor instituțional relevant în asigurarea protecției infrastructurilor critice din domeniul apărării naționale, precum și în realizarea obiectivelor privind răspunsul la incidente, cooperarea interinstituțională, parteneriatele internaționale și dezvoltarea resursei umane specializate (Guvernul României 2021).

Menționăm că acest Comandament a fost înființat prin Ordinul MApN nr. M.173/2018, iar activitatea sa este integrată în cadrul organizatoric stabilit de Legea nr. 346/2006 privind organizarea și funcționarea MApN, cu modificările și completările ulterioare. Structura este parte a Forțelor pentru Operații în Spațiul Cibernetic și are atribuții în prevenirea, detectarea, monitorizarea și contracararea incidentelor cibernetice care pot afecta capabilitățile militare esențiale ale României (Parlamentul României 2006).

Acest cadru reglementar conferă CApC statutul de comandament de sprijin, cu atribuții de planificare, coordonare și executare a operațiilor cibernetice, în concordanță cu nevoile operaționale ale forțelor armate.

Pe lângă documentele care constituie cadrul legislativ specific, activitatea Comandamentului este reglementată și de documente doctrinare și reglementări interne ale MApN, precum ordine ale ministrului apărării naționale, regulamente specifice apărării cibernetice și proceduri operaționale standardizate. Acestea stabilesc modalitățile de organizare a apărării cibernetice la nivel tactic, operativ și strategic, precum și regulile de angajare în cadrul operațiilor cibernetice defensive și (în anumite condiții) ofensive.

O caracteristică esențială a CApC este că acesta funcționează în conformitate cu angajamentele internaționale asumate de România, în special în cadrul Alianței Nord-Atlantice și Uniunii Europene, ceea ce permite integrarea rapidă a capabilităților naționale în arhitectura cibernetică de apărare colectivă a NATO. Astfel, țara noastră este semnatară a *NATO Cyber Defence Pledge*, iar Comandamentul participă activ la exerciții cibernetice multinaționale, ca de exemplu *Locked Shields* sau *Cyber Coalition* (AApC 2025), la schimburi de informații și contribuie activ la inițiative de consolidare a interoperabilității în domeniul apărării cibernetice, în coordonare cu structurile aliate, precum Cooperative Cyber Defence Centre of Excellence (NATO 2016).

2. Oportunitate, provocare și adaptare

În actualul mediu de operare, în care amenințările hibride, atacurile persistente avansate (*Advanced Persistent Threats* – APT) și acțiunile agresive în domeniul cibernetic se intensifică, tehnologiile emergente devin instrumente esențiale pentru menținerea superiorității informaționale. Integrarea acestora în arhitectura de apărare cibernetică a MApN oferă oportunități strategice relevante, dar impune și adaptări instituționale și operaționale.

În acest cadru, oportunitățile generate de tehnologiile emergente se manifestă nu doar prin sporirea capacității de detecție, analiză și răspuns la incidente cibernetice, ci și prin posibilitatea dezvoltării unor capabilități proactive, bazate pe automatizare inteligentă și analitică predictivă. Cu toate acestea, ritmul accelerat al inovării tehnologice impune un efort susținut de adaptare din partea structurilor de apărare, în special în ceea ce privește actualizarea arhitecturilor de securitate, interoperabilitatea sistemelor informatice și asigurarea unui management eficient al riscurilor cibernetice. Provocările sunt amplificate de deficitul de personal specializat, de complexitatea integrării noilor soluții în infrastructuri existente și de necesitatea asigurării unui cadru normativ coerent, care să reglementeze utilizarea responsabilă și sigură a acestor tehnologii. În acest sens, MApN trebuie să adopte o abordare flexibilă și anticipativă, care să permită nu doar absorbția tehnologiilor emergente, ci și transformarea digitală instituțională în acord cu noile paradigme de securitate cibernetică.

2.1. Inteligența artificială și învățarea automată

Inteligența artificială (*Artificial Intelligence* – AI) și învățarea automată (*Machine Learning* – ML) pot fi utilizate în identificarea amenințărilor, în analiza comportamentală a atacurilor și în detecția automată a anomaliilor în rețelele militare. Capabilitățile care implementează aceste tehnologii pot „învăța” din atacurile anterioare și pot optimiza răspunsul în timp real. În plus, pot sprijini misiuni de *threat hunting*[2], detecție a atacurilor *zero-day*[3] și automatizarea proceselor penru luarea unor decizii rapide și eficiente.

[2] Metodă proactivă de apărare cibernetică, prin care specialiști instruiți, denumiți vânători de amenințări, detectează în mod activ atacuri avansate sau ascunse, care reușesc să treacă neobservate de sistemele tradiționale de securitate.

[3] Acest tip de atacuri exploatează o vulnerabilitate a unui software, hardware sau firmware, de regulă necunoscută producătorului sau furnizorului, pentru care nu există încă o soluție de remediere disponibilă.

Un exemplu elocvent este *Project Maven* al Pentagonului, inițiat de Departamentul apărării al SUA, care a demonstrat cum analiza avansată a datelor prin intermediul algoritmilor de învățare automată poate identifica eficient ținte înregistrate de platforme aeriene fără pilot (*Unmanned Aerial Vehicles* – UAV), reducând substanțial volumul de muncă uman necesar pentru procesarea informațiilor. Astfel de aplicații evidențiază potențialul transformator al inteligenței artificiale în domeniul securității și apărării și subliniază, totodată, nevoia unor mecanisme robuste de integrare, testare și guvernanță tehnologică (Sayler 2020).

Pentru a răspunde provocărilor și a valorifica potențialul noilor tehnologii, menționez o serie de măsuri orientate spre integrarea inteligenței artificiale și a învățării automate în structurile existente. În acest sens, o primă direcție de acțiune constă în înființarea, în cadrul CApC, a unei celule specializate AI/ML, cu rolul de a dezvolta și integra algoritmi adaptivi în rețelele C4ISR, contribuind la creșterea capacității de reacție și anticipare în operațiile informatice.

În paralel, ar fi utilă implementarea de soluții de tipul Managementului evenimentelor și informațiilor de securitate (*Security Information and Event Management* – SIEM) și dotarea centrelor de operații cibernetice cu capabilități AI pentru a permite analiza automatizată și contextualizată, în timp real, a evenimentelor de securitate (IBM 2025). Nu în ultimul rând, formarea personalului devine esențială, ceea ce presupune dezvoltarea competențelor tehnice prin programe de instruire în programare (în special limbaje precum *Python*) și în utilizarea platformelor ML, pentru a facilita o abordare proactivă și orientată spre inovație în domeniul securității cibernetice.

2.2. Internetul lucrurilor (IoT) și Internetul militar al lucrurilor (IoMT)

Internetul lucrurilor (*Internet of Things* – IoT) și Internetul militar al lucrurilor (*Internet of Military Things* – IoMT) extind semnificativ suprafața de atac, dar oferă și posibilitatea monitorizării constante a mediului de operare, în special a echipamentelor militare și capabilităților de sprijin logistic. Vulnerabilitățile determină apariția riscurilor, în condițiile existenței unei amenințări fizice, a lipsei actualizărilor și a segmentării.

Prin izolarea dispozitivelor sensibile care compun IoT în segmente de rețea dedicate, se reduce riscul ca un atac asupra unuia dintre acestea să compromită întregul sistem. Această practică este recomandată și pentru rețelele militare IoMT, unde echipamentele trebuie să fie izolate de rețelele generale pentru a proteja integritatea și confidențialitatea datelor (Weber și Studer 2016). De asemenea, în mediile critice, cum ar fi cele militare operaționale, criptarea *end-to-end* este esențială pentru prevenirea interceptării și modificării datelor, având în vedere vulnerabilitatea inerentă a acestora.

Pentru consolidarea securității dispozitivelor IoMT, se propune implementarea unui protocol dedicat care să includă măsuri fundamentale precum segmentarea rețelelor, criptarea datelor și verificarea integrității *firmware*-ului. Aceste măsuri sunt esențiale pentru prevenirea accesului neautorizat și pentru asigurarea funcționării sigure a dispozitivelor militare conectate.

2.3. Rețelele 5G și comunicațiile de nouă generație

Având în vedere faptul că rețelele 5G oferă latență redusă, conectivitate densă și viteză crescută – beneficii pentru comunicațiile militare distribuite –, integrarea acestei tehnologii devine o prioritate strategică. Dezavantajele asociate vizează crearea unor dependențe față de furnizori comerciali și deschide noi vectori de atac la nivel de rețea de bază (*core network*) (TELCOMA Global. 2025). În acest sens, este necesară implementarea unui cadru normativ și operațional privind utilizarea rețelelor 5G în operații militare, cu accent pe definirea condițiilor de funcționare, securitate și interoperabilitate a rețelelor private 5G dedicate.

Pentru asigurarea unei infrastructuri comunicaționale reziliente și securizate, Serviciul de Telecomunicații Speciale are capacitatea necesară în vederea dezvoltării și operării rețelelor mobile de luptă (*combat mobile network*), optimizate pentru mediul de operare de nivel tactic și adaptate cerințelor acțiunilor militare moderne. Complementar, este de luată în considerare crearea unei capabilități dedicate testării tehnologiei 5G în contexte militare, care să permită validarea performanței și fiabilității acesteia în scenarii operaționale variate, reale sau fictive (simulate), inclusiv în condiții de mediu ostile și în prezența unor amenințări cibernetice avansate.

2.4. Calculul cuantic și criptografia post-cuantică

Evoluțiile accelerate în domeniul calculului cuantic prezintă riscuri semnificative pentru securitatea cibernetică, întrucât algoritmii criptografici clasici, precum *Rivest-Shamir-Adleman* – RSA și *Elliptic Curve Cryptography* – ECC[4], pot deveni vulnerabili în fața puterii de procesare oferite de computerele cuantice. Această realitate deschide perspective îngrijorătoare privind capacitatea actorilor statali ostili de a intercepta și descifra comunicații critice, în viitorul apropiat. În acest context, tranziția către criptografia post-cuantică (*Post-quantum cryptography* – PQC) devine imperativă pentru protejarea comunicațiilor și datelor sensibile din domeniul apărării (Chen și alții 2016).

Pentru a răspunde acestei provocări, se propune inițierea unui program național de tranziție către criptografie post-cuantică, cu aplicabilitate directă în structurile MApN. Acest program ar trebui să includă atât evaluarea riscurilor actuale, cât și planificarea trecerii la algoritmi criptografici rezistenți la atacuri cuantice.

[4] Sistemul RSA se referă la un algoritm criptografic cu chei publice, iar ECC la criptografia cu curbe eliptice.

De asemenea, este esențială colaborarea cu instituții academice și de cercetare, precum și cu partenerii internaționali din cadrul NATO, în vederea dezvoltării unor protocoale de criptare standardizate, testate și compatibile cu infrastructurile militare aliate. Nu în ultimul rând, revizuirea standardelor criptografice aflate în uz și auditarea infrastructurilor existente devin pași obligatorii pentru identificarea vulnerabilităților sistemului actual și asigurarea unei tranziții coerente și eficiente către arhitecturi de securitate compatibile cu era post-cuantică.

2.5. Sisteme autonome de automatizare și robotică cibernetică

Automatizarea reprezintă un vector esențial în consolidarea capacității de apărare cibernetică, oferind posibilitatea de a răspunde rapid și eficient la incidente de securitate, fără a depinde de intervenția umană directă. Prin implementarea unor mecanisme automate pot fi realizate o serie de acțiuni, precum izolarea rețelelor compromise, remedierea vulnerabilităților și coordonarea intervențiilor în timp real (Paraschiv 2017).

În plus, robotica cibernetică – sistem autonom de detecție și reacție – poate desfășura patrule virtuale și scanări în rețele IT complexe, contribuind la prevenirea și atenuarea atacurilor informatice avansate. Robotica cibernetică este un domeniu interdisciplinar care combină robotica, tehnologia cibernetică și sistemele informatice avansate pentru a dezvolta roboți capabili să interacționeze autonom cu mediul înconjurător, să ia decizii inteligente și să îndeplinească sarcini complexe. Această abordare presupune integrarea unor componente precum senzori, actuatori, algoritmi de învățare automată și rețele neuronale, care permit roboților să perceapă și să reacționeze la schimbările din mediu într-un mod autonom și eficient (Correll 2016).

În acest context, se propun următoarele direcții strategice de adaptare:

- dezvoltarea unor capabilități specifice de automatizare, în cadrul centrelor de comandă și control, pentru a susține procesele decizionale și acționale, în timp real;
- elaborarea unui cadru doctrinar clar privind utilizarea armelor cibernetice autonome cu scop defensiv, în conformitate cu normele etice și juridice internaționale aplicabile în domeniul militar;
- integrarea soluțiilor de automatizare în procedurile standard de reacție în spațiul cibernetic, prin utilizarea de manuale de strategie care să permită un răspuns coordonat și scalabil la incidentele de securitate.

Adoptarea acestor astfel de măsuri ar contribui la creșterea rezilienței infrastructurilor critice și la modernizarea arhitecturilor de apărare cibernetică, într-un peisaj de amenințări din ce în ce mai complex și automatizat.

2.6. Big Data și analiza predictivă

Analiza *Big Data* oferă un avantaj strategic semnificativ în domeniul apărării cibernetice, prin capacitatea sa de a corela incidente disparate, de a anticipa campanii de influențare sau APT-uri și de a sprijini luarea deciziilor pe baza unor seturi de date extinse, în timp real și predictive. Acest tip de analiză permite trecerea de la o abordare reactivă la una proactivă, bazată pe anticiparea amenințărilor și identificarea timpurie a modalităților de atac.

Un exemplu notabil, în acest sens, este oferit de conflictul din Ucraina, unde analiza *Big Data*, informațiile din surse deschise (*Open Source Intelligence* – OSINT) și instrumentele de analiză predictivă au contribuit la prevenirea atacurilor cibernetice de tip DDoS și *phishing*[5], oferind sprijin informațional esențial pentru operațiunile digitale ale forțelor armate (Greenberg 2022).

Pentru valorificarea acestor capacități în cadrul structurilor militare naționale, se propun următoarele direcții de adaptare:

- crearea unei infrastructuri militare dedicate analizei *Big Data* în cadrul CApC, care să integreze atât surse interne, cât și surse OSINT relevante;
- formarea unei echipe specializate în analiză operațională predictivă, capabilă să extragă informații valoroase din volume mari de date;
- elaborarea unor proceduri standardizate de analiză, inclusiv pentru trierea alertelor și corelarea datelor din surse multiple, cu scopul de a îmbunătăți viteza și acuratețea deciziilor operaționale în spațiul cibernetic.

Implementarea unor astfel de măsuri ar contribui la creșterea rezilienței digitale a structurilor de apărare și la dezvoltarea unei culturi organizaționale orientate spre prevenție și anticipare informațională.

Concluzii

Articolul evidențiază faptul că adoptarea tehnologiilor emergente impune modificări organizaționale, doctrinare și operaționale în structurile de apărare cibernetică. În primul rând, Comandamentul Apărării Cibernetice are rol operațional și apoi un rol de centru pentru inovație, cercetare aplicată și integrare tehnologică, capabil să anticipeze și să răspundă dinamic la noile amenințări. Adaptarea permanentă și cooperarea internațională (în special la nivel NATO și UE) reprezintă direcții de acțiune fundamentale, care contribuie major la realizarea superiorității informaționale și rezilienței strategice necesară în domeniul securității cibernetice.

Apărarea cibernetică este privită ca mediu de opor-

[5] Refuzul distribuit al serviciului (*Distributed Denial of Service* – DDoS) este un atac cibernetic care inundă un server, un site web sau o rețea cu trafic excesiv de internet pentru a perturba serviciile, iar atacul de tip *phishing* presupune inducerea în eroare a utilizatorilor pentru a face să dezvăluie informații confidențiale sau sensibile.

tunitate prin prisma progreselor tehnologice asociate, care permit dezvoltarea unor capabilități de detecție, prevenire și răspuns tot mai eficiente, precum și integrarea inteligenței artificiale, a automatizării și a analizelor avansate de date în arhitectura de securitate a statelor și organizațiilor. Adaptarea structurilor militare și civile la mediul cibernetic creează premise pentru o apărare anticipativă, mai dinamică și mai interoperabilă în cadrul alianțelor strategice.

Apărarea cibernetică nu mai reprezintă o opțiune, ci o necesitate critică și un deziderat care contribuie semnificativ la realizarea securității, dar care presupune investiții susținute, adaptabilitate instituțională și cooperare internațională consolidată. Printr-o viziune integrată și anticipativă, statele pot transforma provocările digitale în avantaje strategice.

Bibliografie

CApC. 2025. Organizare. Comandamentul Apărării Cibernetice / Ministerul Apărării Naționale. https://cybercommand.ro/pages/organizare.

Correll, Nikolaus, Bradley Hayes, Christoffer Heckman, Alessandro Roncone. 2022. *Introduction to Autonomous Robots: Mechanisms, Sensors, Actuators, and Algorithms*. Cambridge: The MIT Press.

Chen, Lily, Stephen Jordan, Yi-Kai Liu, Dustin Moody, Rene Peralta, Ray Perlner, Daniel Smith-Tone. 2016. *Report on Post-Quantum Cryptography*. National Institute of Standards and Technology Internal Report 8105. U.S. Department of Commerce.

ENISA. 2023. *ENISA Threat Landscape 2023*. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202023.pdf.

Giarola, E., Longega, M., & Vespignani, A. (2022). *AI and Cybersecurity: Opportunities and Risks*. ACM Computing Surveys, 55(6), 1-36.

Guvernul României. 2021. *Hotărârea nr. 1321 din 30 decembrie 2021 privind aprobarea Strategiei de securitate cibernetică a României, pentru perioada 2022-2027, precum şi a Planului de acţiune pentru implementarea Strategiei de securitate cibernetică a României, pentru perioada 2022-2027*. Monitorul Oficial nr. 2 din 3 ianuarie 2022.

Greenberg, Andy. 2022. Inside the Pentagon's race to predict cyberattacks with AI and Big Data. WIRED.

Kshetri, N., & Voas, J. (2021). *5G, IoT, and Cybersecurity: Challenges and Future Directions*. IT Professional, 23(1), 4-12.

AApC. 2025. *Locked Shields 2025 – exercițiu NATO de apărare cibernetică*. 15 mai. Agenția de Apărare Cibernetică / Comandamentul Apărării Cibernetice. https://certmil.ro/locked-shields-2025-exercitiu-nato-de-aparare-cibernetica.

Mosca, Michele. 2018. *Cybersecurity in an Era with Quantum Computers: Will We Be Ready?* IEEE Security & Privacy, 16(5), 38-41.

NATO. 2016. *Cyber Defence Pledge*. 8 July. Press Release (2016) 124. https://www.nato.int/cps/en/natohq/official_texts_133177.htm.

Paraschiv, Nicolae. 2017. *Introducere în automatică şi calculatoare*. Editura Universității Petrol-Gaze din Ploiești.

Parlamentul României. 2006. *Legea nr. 346 din 21 iulie 2006 (republicată) privind organizarea și funcționarea Ministerului Apărării Naționale*. Monitorul Oficial nr. 867 din 2 noiembrie 2017.

Sayler, Kelley M. 2020. *Artificial Intelligence and National Security*. Updated 26 August. CRS Report No. R45178. Congressional Research Service.

TELCOMA Global. 2025. *5G Technology Introduction*. 5G Technology Fundamentals course. https://www.telcomaglobal.com/courses/course1/lectures/14408479.

Weber, Rolf H., Evelyne Studer (2016). Cybersecurity in the Internet of Things: Legal aspects. Computer Law & Security Review, 32(5), 715-728.

IBM. 2025. *What is security information and event management (SIEM)?* The 2025 Guide to Cybersecurity. https://www.ibm.com/think/topics/siem.

Colocviu strategic
Redactor: CS II dr. Cristian BĂHNĂREANU
E-mail: colocviustrategic@unap.ro
Webpage: https://cssas.unap.ro/ro/cs.htm
e-ISSN 1842-8096, 661/16.10.2025

Centrul de Studii Strategice de Apărare și Securitate
Adresă: Șoseaua Panduri, nr. 68-72, sector 5,
cod poștal 050662, București, România
Telefon: +4021.319.56.49, Fax: +4021.319.57.80
E-mail: cssas@unap.ro, Website: https://cssas.unap.ro