NOILE PARADIGME ALE SECURITĂŢII ŞI IMPACTUL ACESTORA ASUPRA SISTEMELOR INFORMAŢIONALE

NEW SECURITY PARADIGMS AND THEIR IMPACT ON INFORMATION SYSTEMS

Colonel (rtr) prof. univ. dr. Gruia TIMOFTE*
(Academy of Romanian Scientists, 3 Ilfov, 050044, Bucharest, Romania, email: secretariat@aosr.ro)

Rezumat: *Lucrarea prezintă principalele aspecte privind convergența tehnologică a sistemelor informaționale din diverse domenii în noul mediu de securitate și au ca obiectiv principal satisfacerea tuturor cerințelor tehnice, funcționale și operaționale ale elementelor din spațiul de luptă modern. De asemenea, studiul profund al acestor sisteme evidențiază necesitatea pregătirii tuturor categoriilor de personal pentru utilizarea eficientă a acestora și obținerea unor performanțe operaționale superioare în condiții de cooperare și interoperabilitate efective.*

Cuvinte cheie: *paradigmă, securitate, convergență, integrare, data-centric, computing.*

Abstract: *The paper presents the main aspects regarding the technological convergence of information systems from various fields in the security environment and has as its main objective the satisfaction of all technical, functional and operational requirements of all elements in the modern battlespace. Also, the in-depth study of these systems highlights the need to train all categories of personnel for their efficient use and obtaining superior operational performances in conditions of effective cooperation and interoperability.*

Keywords: *paradigm, security, convergence, integration, data-centric, computing.*

INTRODUCERE

A patra revoluție industrială descrie progresul tehnologic rapid din secolul XXI. O parte a acestei faze a schimbărilor industriale este îmbinarea tehnologiilor avansate precum inteligența artificială (IA), editarea genetică cu robotica avansată, care estompează granițele dintre lumea fizică, digitală și biologică. Integrarea tehnologiei inteligente moderne, a comunicării la scară largă între mașini și a internetului lucrurilor (IoT) duce la creșterea automatizării, îmbunătățirea comunicării și automonitorizării, utilizarea mașinilor inteligente care pot analiza și diagnostica diferite probleme fără a fi nevoie de intervenție umană[1].

Convergența tehnologică reprezintă tendința ca tehnologiile care inițial nu aveau legătură între ele să devină strâns integrate și chiar unificate

* Membru titular al Academiei Oamenilor de Știință din România, telefon: 0731684461, email: timmy.gruia@yahoo.com

[1] McKinsey & Company, The Industry 4.0, the Fourth Industrial Revolution, and 4IR, First programmable controller based automation), 2014.

pe măsură ce se dezvoltă și implementează. De exemplu, telefoanele, televiziunea, computerele și platformele de socializare au început ca tehnologii separate, în mare parte fără legătură între ele, au evoluat ulterior într-o industrie interconectată de telecomunicații, media și tehnologie. Convergența constă în integrare profundă a cunoștințelor, instrumentelor și activităților relevante umane pentru un obiectiv comun, acela de a permite societății să răspundă noilor cerințe pentru schimbarea ecosistemului fizic sau social respectiv[2].

Integrarea este un proces de transformare măsurat prin gradul în care diverse medii tehnice, cum ar fi telefonia, transmisia de date și infrastructurile tehnologiei informației, sunt combinate într-o singură platformă cu arhitectură de rețea universală.

Convergența digitală reprezintă tendința ca diverse inovații și medii digitale să devină apropiate în timp. Acest tip de convergență tehnologică creează noi oportunități, în special în domeniul realizării de produse și al strategiilor de dezvoltare pentru companiile de produse digitale. In această situație convergența digitală cuprinde trei fenomene:

- dispozitivele anterior independente sunt conectate prin rețele și software, îmbunătățind semnificativ funcțiile sistemelor;
- produsele anterior independente sunt convergente pe aceeași platformă, creând produse hibride;
- companiile depășesc granițele tradiționale pentru unele produse, cum ar fi hardware-ul și software-ul, în scopul de a oferi altele noi.

Convergența se poate referi și la capacitatea de a rula aceeași aplicație pe diferite dispozitive și a dezvolta aplicații pentru alte dispozitive simultan, cu aceeași bază de cod[3].

2. NOILE PARADIGME ALE SECURITĂŢII ÎN SECOLUL XXI

O *paradigmă de securitate* reprezintă cadrul conceptual și abordarea fundamentală prin care sunt identificate, evaluate și gestionate amenințările. Aceasta evoluează de la modele tradiționale, axate pe stat și apărare militară, către o perspectivă modernă, socială, ecologică și digitală, concentrată pe reziliență, cooperare și securitate umană în fața unor riscuri complexe, precum schimbările climatice sau atacurile cibernetice.

Noile paradigme ale securității în secolul XXI au evoluat de la concentrarea pe apărarea militară statală la un concept multidimensional, definit de amenințări hibride, non-statale și tehnologice. Securitatea modernă integrează dimensiuni economice, cibernetice, sociale și de sănătate, fiind influențată de convergența tehnologică și globalizare.

Caracteristicile esențiale ale acestor noi paradigme cuprind[4]:

---

[2] David Messerschmitt, *The Prospects of Computing Communications Convergence,* Munich, Germany, 2007.

[3] Cristian Barna, Valentin Nicula, *Security Paradigms in the 21st Century*, RISR, No. 23, București, 2020, pp.122-124

- *trecerea de la securitatea statului la securitatea umană:* accentul se pune pe protejarea individului și a comunității, nu doar a frontierelor;

- *amenințări hibride și non-statale:* actorii non-statali și atacurile cibernetice, alături de dezinformare, definesc noile conflicte;

- *convergenta tehnologică*: Inteligența artificială și tehnologiile emergente reconfigurează apărarea și intelligence-ul;

- *securitatea transnațională* vizează probleme precum terorismul, pandemiile și schimbările climatice care necesită cooperare internațională, depășind abordările neorealiste clasice.

Această transformare implică o redefinire a relațiilor internaționale și a modelelor de securitate, trecând de la o abordare pur militară la una holistică, bazată pe informații și securitate cibernetică.

Securitatea în secolul XXI a încetat să vizeze doar mijloacele de luptă si granițele, trecându-se de la viziunea tradițională (militară) la una *multidimensională.*

Principalele schimbări de paradigmă sunt[5]:

- *Securitatea umană:* Accentul s-a mutat de la protejarea statului la protejarea individului. Aceasta include securitatea economică, alimentară, personală și a sănătății.

- *Lărgirea spectrului de analiză:* Securitatea cuprinde acum cinci sectoare esențiale: **militar, politic, economic, societal și de mediu**. O criză economică sau colapsul ecosistemelor sunt privite ca amenințări directe la stabilitate.

- *Amenințările asimetrice și hibride:* Nu mai vorbim doar de războaie între armate regulate, ci de terorism, atacuri cibernetice, dezinformare și presiuni energetice. Granița dintre „pace” și „război” a devenit foarte difuză.

- *Securitatea cibernetică***:** Infrastructura critică (căi de comunicație, electricitate, bănci, spitale) este acum vulnerabilă la atacuri de la distanță, transformând codul digital într-o armă la fel de periculoasă ca un proiectil.

- *Revenirea marii competiții puternice*: Deși amenințările transnaționale (schimbările climatice) persistă, asistăm la o revenire a rivalităților geopolitice clasice dar într-un context de interdependență economică totală.

- Inteligență Artificială nu este doar o nouă tehnologie, ci un *multiplicator de forță* care redefinește viteza și natura conflictelor moderne. Aceasta funcționează ca o „armă cu dublu tăiș”, oferind avantaje tactice imense, dar și noi vulnerabilități.

Principalele direcții de aprofundare sunt:

a.Războiul și Securitatea Cibernetică[6]:

---

[4] Gabriel Gabor, *Caracteristici ale paradigmelor de Securitate în secolul XXI*, București 2014, pp. 35-37.

[5] Cristian Alexandru, *Schimbarea paradigmelor in mediul internațional de securitate*, Intelligence Info No.3, vol.2, 2023, pp. 72-73, 80-81.

[6] Peter Singer, Allan Friedman, *Cybersecurity and Cyberwar*, Oxford University Press, 2014.

b. IA transformă securitatea digitală dintr-un proces reactiv în unul predictiv și autonom.

•*Automatizarea atacurilor*: Atacatorii folosesc IA pentru a descoperi vulnerabilități în câteva secunde, proces care înainte dura ore.

•*Apărarea proactivă*: Sistemele defensive pot detecta anomalii și răspunde la incidente în timp real, fără intervenție umană constantă.

•*Sisteme autonome*: Apar agenți software capabili să adapteze strategiile de atac sau apărare „din mers", depășind capacitatea de reacție a analiștilor umani.

b. Manipularea percepției și războiul informațional:

IA a multiplicat crearea de conținut fals, transformând dezinformarea într-o amenințare la adresa stabilității democratice.

•*Deepfakes și clonarea vocii:* Acestea pot fi folosite pentru a discredita lideri politici sau pentru a induce panică socială.

•*Micro-targeting*: Algoritmii analizează datele masive pentru a livra mesaje de dezinformare personalizate, care exploatează temerile specifice ale unor grupuri de populație.

c. Intelligence și analiză strategică:

Pentru serviciile de informații, IA este soluția referitoare la volumul mare de date din secolul XXI.

•*Analiza Big Data*: Poate corela miliarde de puncte de date din surse deschise pentru a anticipa crize sau mișcări de trupe.

•*Avertizarea timpurie*: Modelele predictive permit identificarea semnalelor slabe care anunță un atac terorist sau o criză geopolitică înainte ca acestea să se materializeze.

d. Dileme etice și riscuri existențiale

Integrarea IA în securitate ridică întrebări fundamentale despre controlul uman.

Principiul „Human-in-the-loop": Există o dezbatere intensă dacă decizia de a folosi forța letală ar trebui lăsată vreodată pe seama unui algoritm („cutia neagră").

•*Sisteme de arme autonome*: Acestea promit reducerea riscului pentru proprii soldați, dar cresc riscul de escaladare accidentală a conflictelor.

În țara noastră se pune accentul pe utilizarea etică și creșterea rezilienței cibernetice în fața acestor noi provocări.

3.CONVERGENŢA TEHNOLOGICĂ ÎN CONTEXTUL NOILOR PARADIGME DE SECURITATE

Aceasta reprezintă fuziunea dintre tehnologiile digitale avansate, securitatea fizică și capacitățile analitice, redefinind modul în care amenințările sunt detectate, prevenite și gestionate în secolul XXI. Această integrare estompează granițele dintre securitatea cibernetică și cea fizică, creând ecosisteme unificate.

Tendințele esențiale de convergență tehnologică (2025-2026)[7]:

•*Inteligența Artificială la margine (Edge IA):* Camerele video și senzorii moderni integrează IA nativă pentru a trece de la simpla detectare a mișcării la înțelegerea comportamentală (ex: identificarea ‚rătăcirilor', abandonului de obiecte, aglomerărilor sau agresiunilor).

•*Sistemele hibride unificate:* Integrarea sistemelor de televiziune, controlului accesului și a sistemelor de efracție într-o singură platformă de management permite operatorilor o vizualizare holistică a situației de securitate.

•*Analiza predictivă:* Tehnologiile moderne utilizează datele pentru a prognoza potențialele amenințări înainte ca acestea să se materializeze.

•*IoT și securitatea cibernetică:* Numărul mare de dispozitive conectate (IoT) necesită o securitate cibernetică robustă pentru a preveni transformarea acestora în puncte de intrare pentru atacatori.

*Noile paradigme de securitate sunt***:**

•*Securitatea tehnologică:* Devine un domeniu crucial, dependența de tehnologie însemnând că investițiile în acest sector sunt esențiale pentru a nu rămâne în urmă.

•*Reziliența entităților critice:* Convergența necesită o atenție sporită asupra securității infrastructurilor critice, IA și confidențialității datelor.

•*Tehnologiile cuantice și umane***:** Elementele de convergență ale acestor tehnologii sunt identificate ca instrumente care schimbă fundamental paradigma securității și a „perfecționării" umane.

În țara noastră, provocările includ nevoia de adaptare prin reinstruire și utilizarea tehnologiilor digitale, având în vedere importanța securității informaționale și economice ca suport pentru securitatea militară.

Convergența tehnologică în noile paradigme de securitate conduce la dispariția granițelor dintre securitatea fizică, cea cibernetică și sistemele de guvernanță. Nu mai vorbim de soluții izolate, ci de un ecosistem interconectat.

Pilonii principali ai acestei evoluții sunt următorii[8]*:*

a. *Integrarea IoT cu infrastructura teritorială:* Securitatea nu mai vizează doar datele de pe servere, ci și infrastructura critică (rețele electrice, transporturi). Un atac cibernetic are acum consecințe fizice imediate.

b. *Inteligența Artificială și automatizarea:* IA este folosită dual. Pe de o parte, pentru detectarea proactivă a anomaliilor (identificarea atacurilor înainte să se producă), iar pe de altă parte, în scopul de a crea mijloace și proceduri de protecție.

c. *Cloud native și Zero trust:* Trecerea de la conceptul de „perimetru securizat" la cel de „încredere zero", unde identitatea utilizatorului este verificată constant, indiferent de locație sau dispozitiv.

[7] *** US Congressional Research Service, *The Army' Project Convergence*, Washington, DC, 2022, pp.2-3.

[8] Jeremy Gannon, *Telecom Systems Integration*, University of Phoenix, USA, 2024, pp. 4-5.

d. *Big Data și analitica predictivă:* Capacitatea de a procesa volume masive de date în timp real pentru a corela evenimente aparent disparate care, împreună, indică o breșă de securitate complexă.

e. *Blockchain pentru integritate:* Utilizarea registrelor distribuite pentru a asigura nerespingerea datelor și securizarea lanțurilor de aprovizionare.

Efectul principal: Securitatea a devenit o funcție de business și de siguranță națională, nu doar o sarcină a departamentului IT.

Convergența tehnologică transformă strategiile de apărare dintr-un model reactiv și fragmentat în unul *proactiv și unificat*. Principalele schimbări în strategiile de apărare ale companiilor vizează[9]:

a. *Unificarea securității fizice și cibernetice*

Companiile renunță la gestionarea separată a celor două domenii pentru a elimina vulnerabilitățile de interdependență.

•*Sisteme de alarmă integrate:* Folosirea senzorilor IoT și a controlului accesului bazat pe cloud pentru a crea un scut digital-fizic comun.

•*Echipe cros-funcționale:* Crearea unor structuri de comandă comune între departamentele IT și cel de securitate fizică pentru a răspunde coordonat la incidente.

•*Eficiență prin sinergie:* Reducerea costurilor prin eliminarea investițiilor redundante în echipamente care pot servi ambelor domenii (ex: camere video cu analiză IA pentru securitate și fluxuri de date IT).

b. *De la perimetru la zero trust*

Modelul tradițional este considerat depășit în 2026 din cauza muncii hibride și a cloud-ului.

•*Verificare continuă:* Strategia presupune că niciun utilizator sau dispozitiv (intern sau extern) nu este implicit de încredere.

•*Micro-segmentare:* Rețeaua este împărțită în segmente mici pentru a preveni deplasarea laterală a atacatorilor în interiorul sistemului.

c**.** *Apărarea bazată pe IA*

Deoarece atacatorii folosesc IA pentru a automatiza controlul breșelor, companiile adoptă strategii de *apărare autonomă.*

•*Detectarea anomaliilor în timp real*: Algoritmii de Machine Learning analizează comportamentul utilizatorilor pentru a identifica atacuri subtile, înainte ca acestea să producă daune.

•*Răspuns automatizat:* Automatizarea acțiunilor de contraofensivă pentru a bloca instantaneu adresele IP suspecte sau a izola conturile compromise.

d. *Reziliența lanțului de aprovizionare*

Strategiile se extind acum dincolo de propria companie, către furnizori și parteneri.

[9] Quentin Hodgson, Susan Gates, *Getting the Fundamentals of Cyberspace Force Readiness Right*, Rand Corporation, Santa Monica, USA, 2025.

•*Monitorizarea terţilor***:** Auditarea constantă a nivelului de securitate al furnizorilor de software și servicii cloud pentru a preveni atacurile de tip „trambulină”.

e. *Strategia condusă de conformitate*

Securitatea a devenit un pilon de business impus de reglementările tot mai stricte.

•*Standardizarea:* Adoptarea protocoalelor standardizate pentru a asigura interoperabilitatea sistemelor defensive la nivel zonal și global.

4. DEZVOLTAREA NOILOR SISTEME DATA- CENTRIC DE COMUNICAŢII ŞI CALCULATOARE

Convergența noilor sisteme data-centric de comunicații și computere[10] reprezintă fuziunea dintre infrastructurile de calcul de înaltă performanță, tehnologiile de stocare și rețelele avansate, având ca scop procesarea eficientă a volumelor foarte mari de date (Big Data) direct la sursă sau în proximitatea acesteia. Această integrare transformă arhitecturile tradiționale, punând datele și utilitatea lor în centrul dezvoltării tehnologice.

Elementele esențiale ale schimbării de paradigmă cuprind:

•*Trecerea de la securitatea tradițională la cea modernă:* Paradigma tradițională, bazată pe realism și apărarea frontierelor, este înlocuită de abordări non-tradiționale care includ securitatea cibernetică, economică și ecologică.

•*Securitatea socio-ecologică***:** Se pune accent pe amenințări transnaționale, precum schimbările climatice, pierderea biodiversității și insecuritatea alimentară/apelor, necesitatea unei abordări integrate.

•*Securitatea cibernetică centrată pe date***:** Paradigmele digitale noi se concentrează pe protecția datelor și a utilizatorilor spre deosebire de modelele vechi axate doar pe perimetrul rețelei.

•Securitatea Europeană Cooperativă - nouă abordare în Europa, bazată pe cooperare, reziliență și securitate strategică.

•*Securitatea umană* - focalizarea pe bunăstarea indivizilor și siguranței acestora, nu doar pe securitatea statului.

Această schimbare este declanșată de complexitatea noilor amenințări, care nu mai pot fi gestionate doar prin forță militară, ci necesită o abordare integrată și o mai bună înțelegere a riscurilor interconectate.

Principalele aspecte ale convergenței acestor sisteme sunt[11]:

•*Internetul Lucrurilor și Edge Computing*: IoT permite conectarea a miliarde de dispozitive, transformându-se dintr-o tehnologie de conectivitate într-o paradigmă de conectare care generează volume enorme de date. Convergența cu *Edge Computing* permite procesarea acestor date local, reducând latența și necesarul de lățime de banda de frecvențe.

[10] Mrs. N. Gayathri, *Computer Communications and Networks,* The American College, Mumbai, India, 2021.

[11] Alexandra Zabala-Lopez, Sonia Haiduc*, Data-centric technologies supporting decision-making*, Defence Technology, No. 43, 2024, pp. 226-246.

•*Inteligența Artificială și Big Data:* IA se află în centrul transformării digitale, analizând datele colectate pentru a extrage informații relevante, cu aplicații în diverse domenii, de la e-guvernare la sectorul privat.

•*Comunicații și Sisteme Informaționale (C4ISR):* În domeniile critice, precum cel militar sau de securitate, se observă o fuziune între sistemele de comanda, control, comunicații, computere, informații, supraveghere si recunoaștere. Acest lucru asigură o prelucrare rapidă a informațiilor în situații de criză sau război electronic.

•*Transformarea digitală și e-Guvernarea:* Implementarea sistemelor Big Data și a soluțiilor de securitate cibernetică în administrația publică și sectorul privat îmbunătățește managementul și arhivarea documentelor.

•*Managementul Resurselor și Calității Serviciilor:* Noile sisteme data-centric integrează algoritmi de control al calității serviciului pentru a gestiona eficient resursele informatice în rețelele moderne. Această convergență duce la o societate informațională bazată pe utilizarea intensivă a informației, influențând decisiv activitățile economice și sociale.

Convergența sistemelor de comunicații și computere într-un model *data-centric* (centrat pe date) reprezintă tranziția de la rețelele tradiționale, unde accentul era pus pe conectarea dispozitivelor la o infrastructură unde prioritatea este accesul eficient și securizat la informație, indiferent de locația fizică a resurselor.

Pilonii principali ai acestei convergențe sunt:

a**.** *Evoluția către Serviciul de Distribuție a Datelor (DDS)*

Spre deosebire de modelele clasice client-server, sistemele moderne utilizează standarde care oferă un model de tip "publish-subscribe".

•*Decuplare*: Comunicarea este decuplată în timp și spațiu deoarece aplicațiile nu trebuie să știe unde se află celelalte componente.

•*Spațiu Global de Date*: Creează un spațiu virtual de date partajat, facilitând interoperabilitatea în medii complexe precum Industrial IoT.

b. Integrarea Cloud-Edge-IoT

Convergența presupune eliminarea barierelor dintre procesarea locală și cea centralizată:

•*Edge Computing*: Procesarea datelor se mută mai aproape de sursă (senzori, dispozitive mobile) pentru a reduce latența.

•*Infrastructuri coerente*: La nivel guvernamental și industrial, se urmărește crearea unor infrastructuri digitale integrate care să asigure fluxul de date între diferite instituții sau departamente.

c**.** *Impactul Tehnologiilor Big Data și IA*

Sistemele data-centric transportă datele și le analizează în timp real.

•*Eficiență operațională*: Utilizarea sistemelor Big Data permite creșterea eficienței serviciilor publice și private prin analiză predictivă.

•*Mentenanță inteligentă*: Integrarea IA permite monitorizarea resurselor complexe în timp real.

d**.** *Securitatea în Noul Model*

Într-un sistem centrat pe date, securitatea se mută de la nivelul central spre elementele componente.

Zero Trust: Accesul este verificat constant, indiferent dacă cererea vine din interiorul sau exteriorul rețelei.

•*Standarde Europene*: Strategiile de transformare digitală, precum cele implementate în unele centre urbane, pun accent pe reziliența cibernetică a acestor sisteme convergente.

În domeniul militar, tranziția către sisteme *data-centric* marchează trecerea de la "Network-Centric Warfare", unde accentul era pus pe conexiunea fizică între platforme, la o arhitectură în care datele sunt tratate ca un activ strategic independent de rețeaua sau aplicația care le-a generat.

Această evoluție este esențială pentru concepte moderne precum *JADC2 (Joint All-Domain Command and Control – Comanda și controlul tuturor domeniilor întrunite)*, utilizat de forțele NATO pentru a asigura "avantajul decizional" în fața adversarilor.

Caracteristicile Sistemelor Militare Data-Centric[12]:

Sistemele moderne trebuie să respecte principiile stabilite de Departamentul Apărării al SUA și adoptate ca referință în cadrul NATO., care precizează cerințele impuse datelor.

Componente și Tehnologii Esențiale (2024-2026)

1.*Internet of Military Things (IoMT):* O rețea de senzori purtați de militari, vehicule autonome și echipamente care comunică în timp real.

2.*Inteligența Artificială și Big Data*: Algoritmi care procesează volume uriașe de informații (imagini din satelit, interceptări) pentru a oferi elemente necesare de acțiune și mentenanță predictivă.

3.*Digital Twins (Gemenii digitali):* Utilizarea replicilor virtuale ale câmpului de luptă pentru a testa scenarii tactice fără riscuri umane.

4.*Edge Computing & Cloud Hybrid*: Procesarea datelor direct pe câmpul de luptă pentru a reduce latența, urmată de sincronizarea cu centrele de date strategice.

5.*Securitate Zero Trust*: Fiecare cerere de acces la date este verificată riguros, eliminând ideea de "rețea internă sigură" implicită.

Avantajele Operative sunt**:**

•*Eliminarea silozurilor informaționale*: Datele de la artilerie, informații (intelligence) și logistică sunt integrate într-o imagine operațională comună.

•*Viteza de reacție*: Scurtarea ciclului OODA (Observare-Orientare-Decizie-Acțiune), permițând comandanților să ia decizii mai rapide decât adversarul.

•*Interoperabilitate între Aliați*: Permite forțelor multinaționale (ex. în cadrul NATO) să colaboreze eficient prin utilizarea standardelor specifice.

[12] Teamraft, *Data Platforms for a Data-Centric Force*, Whitepaper, Reston, USA, p.30, 2026.

5. CONCLUZII

Articolul abordează unele probleme deosebit de importante pentru structurile de comandă și comunicații în procesul de trecere la noile reglementări privind implementarea conceptului data-centric în care elementele primordiale sunt 'datele'. Astfel, colectarea, prelucrarea și prezentarea datelor se realizează în centrele cloud computing și se stochează în bazele de date. Beneficiarii acestor date, au drepturi de accesare a datelor (simboluri de 1 – semnal cu curent, 0 semnal nul), în funcție de rolul îndeplinit în cadrul statului major sau unității, utilizând aplicațiile specifice.

Tranziția de la sistemele informaționale clasice la cele de date reprezintă eforturi de dotare cu mijloace tehnice și produse software specializate, instruire a întregului personal cu procedurile de acces, utilizare, securitate, reziliență, interoperabilitate etc.

Procesul de pregătire pentru noul sistem data-centric trebuie să înceapă în instituțiile de învățământ, unități militare, centre de perfecționare a pregătirii naționale și centre ale NATO și UE etc.

BIBLIOGRAFIE

ALEXANDRU C., *Schimbarea paradigmelor in mediul internațional de securitate*, Intelligence Info No.3, vol.2, 2023;

BARNA C., NICULA V., *Security Paradigms in the 21st Century,* RISR, No. 23, București, 2020;

GABOR G*., Caracteristici ale paradigmelor de Securitate în secolul XXI*, București 2014;

GANNON J., *Telecom Systems Integration*, University of Phoenix, USA, 2024;

GAYATHRI N., *Computer Communications and Networks,* The American College, Mumbai, India, 2021;

HODGSON Q., GATES S., *Getting the Fundamentals of Cyberspace Force Readiness Right*, Rand Corporation, Santa Monica, USA, 2025;

MESSERSCHMITT D., *The Prospects of Computing Communications Convergence*, Munich, Germany, 2007;

SINGER P., FRIEDMAN A., *Cybersecurity and Cyberwar*, Oxford University Press, 2014;

ZABALA-LOPEZ A., HAIDUC S., *Data-centric technologies supporting decision-making,* Defence Technology, No. 43, 2024;

Teamraft, *Data Platforms for a Data-Centric Force*, Whitepaper, Reston, USA, 2026;

McKinsey & Company*, The Industry 4.0, the Fourth Industrial Revolution, and 4IR*, First programmable controller (based automation), 2014;

*** US Congressional Research Service, *The Army' Project Convergence,* Washington, DC, 2022.