DOI: https://doi.org/10.53486/sstc2026.v1.110

CZU: 004.8:004.056.53

THE ROLE OF ARTIFICIAL INTELLIGENCE IN THE EVOLUTION OF CYBERSECURITY RISKS IN THE DIGITAL ECONOMY

ROLUL INTELIGENȚEI ARTIFICIALE ÎN EVOLUȚIA RISCURILOR DE SECURITATE CIBERNETICĂ ÎN ECONOMIA DIGITALĂ

LOBOICO Anastasia, studentă, specialitatea: Informatică și cibernetică economică
ȚURCAN Eric, student, specialitatea: Informatică și cibernetică economică
Academia de Studii Economice din Moldova, Republica Moldova,
Chișinău, str. Bănulescu-Bodoni 61, www.ase.md
e-mail autori: loboico.anastasia@ase.md
eric.turcan.ky@ase.md

Abstract: *This paper examines the dual role of artificial intelligence in the cybersecurity landscape of the digital economy. Drawing on ENISA Threat Landscape reports (2024–2025), Europol intelligence assessments, and recent case studies, the research quantifies AI-driven cyber threats—including automated phishing (responsible for over 80% of phishing campaigns in 2025), deepfake fraud (with incidents increasing by 257% in 2024), and adaptive malware. A comparative analysis contrasts the cybersecurity maturity of EU member states with that of the Republic of Moldova, where cyberattacks tripled after 2022 and institutional capacity remains limited despite the adoption of the Cybersecurity Law (No. 48/2023). The study proposes a set of recommendations for strengthening Moldova's cyber resilience, informed by EU best practices and aligned with the NIS2 Directive transposition requirements.*
Key words: *artificial intelligence, cybersecurity, digital economy, deepfake, phishing, NIS2, Republic of Moldova*
JEL CLASSIFICATION: O33, L86, D83

INTRODUCERE

Economia digitală se află într-o transformare accelerată, catalizată de progresul rapid al inteligenței artificiale (IA). De la automatizarea proceselor operaționale la analiza predictivă a datelor, IA a devenit un pilon al competitivității economice globale. Conform raportului OECD Digital Economy Outlook 2023, adoptarea IA la nivel organizațional a crescut cu peste 50% în ultimii cinci ani, generând eficiență și inovație în sectoare precum finanțele, sănătatea și administrația publică (OECD, 2023).

Totuși, aceleași capabilități care fac IA valoroasă — procesarea limbajului natural, generarea de conținut, recunoașterea tiparelor — sunt exploatate de actorii malițioși pentru a dezvolta atacuri cibernetice de o sofisticare fără precedent. Raportul ENISA Threat Landscape 2024 a analizat peste 11.000 de incidente de securitate și a identificat șapte categorii principale de amenințări, atacurile asupra disponibilității (DDoS) și ransomware-ul fiind cele mai frecvente, reprezentând peste jumătate din evenimentele observate (ENISA, 2024). Ediția din 2025 a aceluiași raport, bazată pe analiza a 4.875 de incidente, confirmă o tendință de convergență între hacktivism, criminalitate cibernetică și operațiuni aliniate statelor, în care IA accelerează inovația ofensivă (ENISA, 2025).

Actualitatea temei este amplificată de contextul geopolitic al Republicii Moldova. După 2022, atacurile cibernetice asupra instituțiilor moldovenești s-au triplat, incluzând atacuri DDoS asupra serverelor guvernamentale și compromiterea serverelor de e-mail ale Parlamentului în contextul alegerilor prezidențiale din 2024 (CSIS, 2025). În același timp, ecosistemul de securitate cibernetică al țării rămâne fragmentat, cu resurse umane și instituționale limitate (RUSI, 2023).

Scopul cercetării este de a analiza modul în care inteligența artificială influențează evoluția riscurilor de securitate cibernetică în economia digitală, cu un accent comparativ pe situația din Uniunea Europeană și Republica Moldova.

Obiectivele specifice includ: (1) identificarea și cuantificarea principalelor tipuri de atacuri cibernetice facilitate de IA; (2) analiza comparativă a cadrelor instituționale și legislative din UE și R. Moldova; (3) formularea de recomandări concrete pentru consolidarea rezilienței cibernetice a Moldovei.

METODOLOGIE

Cercetarea utilizează o abordare calitativă, bazată pe următoarele metode:

Analiza literaturii de specialitate — au fost examinate rapoarte instituționale (ENISA Threat Landscape 2024 și 2025, Europol AI and Cybercrime Report 2025, OECD Digital Economy Outlook 2023), studii academice și analize ale organizațiilor internaționale (CSIS, RUSI, UNDP, DCAF). Selecția surselor s-a concentrat pe publicații din perioada 2022–2025 pentru a asigura relevanța temporală.

Metoda comparativă — a fost aplicată pentru a analiza diferențele dintre nivelul de maturitate al securității cibernetice din UE și cel din R. Moldova, folosind indicatori precum: cadrul legislativ, capacitatea instituțională, numărul de incidente raportate, resursa umană și nivelul investițiilor.

Analiza datelor statistice — datele cantitative privind incidentele cibernetice, fraudele deepfake și atacurile de phishing au fost extrase din rapoartele ENISA, IBM Cost of a Data Breach Report 2024, și platformele de threat intelligence (Keepnet, Sumsub, Sift).

CONȚINUTUL DE BAZĂ

Peisajul amenințărilor cibernetice în era IA

Adoptarea pe scară largă a instrumentelor de IA generativă a transformat radical peisajul amenințărilor cibernetice. Conform datelor din 2025, peste 80% din campaniile de phishing utilizează o formă de IA, iar atacurile de tip phishing au înregistrat o creștere de 1.265% în legătură cu tendințele de IA generativă față de 2023 (SlashNext, 2025). Instrumentele de tipul FraudGPT permit infractorilor să genereze e-mailuri de phishing convingătoare și scripturi malițioase fără cunoștințe tehnice avansate (ENISA, 2024).

Raportul ENISA Threat Landscape 2024 a identificat șapte categorii principale de amenințări: atacuri asupra disponibilității (DDoS), ransomware, malware, inginerie socială, amenințări asupra datelor, manipularea informațiilor și atacuri asupra lanțului de aprovizionare. DDoS și ransomware-ul au reprezentat împreună peste jumătate din incidentele observate, iar sectoarele cel mai afectate au fost administrația publică (19%), transportul (11%) și finanțele (ENISA, 2024).

Un element distinctiv al perioadei recente este convergența actorilor de amenințare: granițele dintre hacktivism, criminalitate cibernetică organizată și operațiuni aliniate statelor devin tot mai neclare. Raportul ENISA 2025 semnalează fenomenul "faketivism", în care actori statali operează sub personaje hacktiviste, iar grupurile hacktviste adoptă tactici de ransomware (ENISA, 2025).

Principalele atacuri cibernetice facilitate de IA

Phishing automatizat cu IA. Modelele lingvistice mari (LLM) permit generarea de e-mailuri de phishing cu gramatică perfectă, personalizate pe baza datelor publice ale victimei. Conform IBM, un experiment a demonstrat că IA poate crea o campanie de phishing la fel de eficientă ca una dezvoltată de experți umani în 16 ore, utilizând doar 5 prompturi și 5 minute. În a doua jumătate a anului 2024, atacurile de phishing au crescut cu 202%, iar cele de furt de credențiale cu 703% (SlashNext, 2024).

Deepfake audio și video. Incidentele deepfake au crescut cu 257% în 2024 față de 2023, ajungând la 150 de cazuri documentate, iar numai în primul trimestru al anului 2025 au fost înregistrate 179 de incidente, depășind totalul anului precedent cu 19% (Keepnet, 2025). Cazul emblematic este cel al firmei Arup (în februarie 2024), unde un angajat financiar a transferat 25 milioane USD după o videoconferință în care toți participanții erau deepfake-uri ale conducerii companiei. Pierderile medii per companie din frauda deepfake au atins circa 500.000 USD în 2024,

iar pierderile globale estimate din frauda generativă IA urmează să crească de la 12,3 miliarde USD (2024) la 40 miliarde USD până în 2027 (Deloitte, 2025).

Malware adaptiv. Programele malware bazate pe IA utilizează învățarea automată pentru a-și modifica comportamentul în funcție de mediul țintă, evitând astfel detecția de către soluțiile tradiționale de securitate. Raportul ENISA din 2024 a semnalat 19.754 de vulnerabilități identificate, din care 9,3% critice și 21,8% cu severitate ridicată (ENISA, 2024). Cercetătorii de la Cornell au demonstrat în 2024 funcționalitatea unui vierme AI (Morris II), capabil să se infiltreze în sisteme, să extragă date sensibile și să trimită spam cu software malițios.

Manipularea informațiilor (FIMI). IA permite generarea de conținut fals la scară industrială. ENISA semnalează că actorii de amenințare experimentează cu IA pentru manipularea informațională, deși fenomenul rămâne încă la o scară limitată dar în evoluție (ENISA, 2024). Acest risc este deosebit de relevant pentru Republica Moldova, țintă a unui război hibrid de intensitate ridicată (UNDP, 2025).

Tabelul 1. Principalele atacuri cibernetice facilitate de IA: tipologie, impact și nivel de risc

Tip atac	Descriere	Impact	Nivel risc
Phishing automatizat cu IA	Mesaje personalizate generate de modele lingvistice mari (LLM), cu gramatică perfectă și context adaptat victimei	Furt de credențiale, pierderi financiare; rata de succes cu 27% mai mare decât phishing-ul tradițional	Ridicat
Deepfake audio/video	Clonarea vocii și chipului persoanelor din conducere pentru autorizarea frauduloasă a tranzacțiilor	Pierderi de până la 25 mil. USD per incident (cazul Arup, 2024); deteriorarea încrederii organizaționale	Ridicat
Malware adaptiv (AI-powered)	Software malițios care utilizează învățarea automată pentru a-și modifica comportamentul și a evita detectarea	Acces neautorizat la infrastructura critică; exfiltrarea datelor sensibile	Mediu-Ridicat
Atacuri asupra verificării identității	Utilizarea deepfake-urilor pentru a înșela sistemele biometrice de autentificare	Compromiterea conturilor; fraudă financiară la scară largă	Ridicat
Manipularea informațiilor (FIMI)	Generarea de conținut fals la scară industrială pentru dezinformare și destabilizare politică	Erodarea încrederii publice; interferență electorală (ex.: alegerile din R. Moldova, 2024)	Mediu

Sursa: elaborat de autori pe baza ENISA (2024,2025), IBM (2024), Keepnet (2025), Deloitte (2025)

Analiză comparativă: UE vs. Republica Moldova

Diferențele dintre nivelul de maturitate al securității cibernetice din Uniunea Europeană și cel din Republica Moldova sunt semnificative și se manifestă pe mai multe dimensiuni.

Cadrul legislativ. UE beneficiază de Directiva NIS2 (2022/2555), intrată în vigoare în 2024, care impune obligații stricte de raportare a incidentelor și măsuri de gestionare a riscurilor pentru operatorii de servicii esențiale. În paralel, AI Act (2024) reglementează utilizarea IA în funcție de nivelul de risc. Republica Moldova a adoptat Legea securității cibernetice (nr. 48/2023), intrată în vigoare în ianuarie 2025, care transpune parțial NIS2 și stabilește obligații de raportare pentru furnizorii de servicii esențiale (NCSI, 2025).

Capacitate instituțională. ENISA coordonează eforturile de securitate cibernetică la nivel european, iar statele membre dispun de CERT-uri naționale mature. În R. Moldova, Agenția pentru

Securitate Cibernetică (ASC) a fost înființată în decembrie 2023 și avea doar 30 de angajați în 2025. CERT-GOV-MD, responsabil de răspunsul la incidente guvernamentale, avea doar 4 angajați în 2022 (RUSI, 2023). Cu toate acestea, progresul este vizibil: în 2025, Moldova a format prima alianță cibernetică regională cu Ucraina și România (AFCEA, 2026).

Incidente și vulnerabilități. După invazia rusească a Ucrainei din 2022, atacurile cibernetice asupra Moldovei s-au triplat (CSIS, 2024). În 2024, serverele de e-mail ale Parlamentului au fost compromise înaintea alegerilor prezidențiale, iar Comisia Electorală Centrală a respins atacuri cibernetice semnificative (The Record, 2024). Indicele Global de Securitate Cibernetică al Moldovei a scăzut de la poziția 53 (2018) la 63 (2020), indicând o regresie relativă față de alte state (RUSI, 2023).

Tabelul 2. Analiză comparativă: securitatea cibernetică în UE vs. Republica Moldova

Indicator	**Uniunea Europeană**	**Republica Moldova**
Cadru legislativ	NIS2 (Directiva 2022/2555) — în vigoare din 2024; AI Act (2024)	Legea securității cibernetice nr. 48/2023 — în vigoare din ianuarie 2025; transpune parțial NIS2
Autoritate responsabilă	ENISA + autorități naționale (ANSSI, BSI etc.)	Agenția pentru Securitate Cibernetică (ASC) — înființată decembrie 2023, 30 angajați (2025)
Capacitate CERT	CERT-uri naționale mature, cu sute de specialiști	CERT-GOV-MD — 4 angajați în 2022; în curs de dezvoltare
Indicele Global de Securitate Cibernetică	Statele UE: primele 30 de poziții (media)	Poziția 63 (2020), în scădere de la poziția 53 (2018)
Incidente raportate	Peste 11.000 incidente analizate de ENISA (2023–2024)	Atacurile cibernetice s-au triplat după 2022; atacuri DDoS și phishing frecvente
Investiții în securitate cibernetică	Buget mediu dedicat de 5–10% din bugetul IT	Investiții limitate; dependență de asistența internațională (UE, Estonia, UNDP)

Sursa: elaborat de autori pe baza ENISA (2024,2025), NCSI (2025), RUSI (2023), CSIS (2025), AFCEA (2026)

IA ca instrument defensiv

Dincolo de rolul său ofensiv, IA reprezintă și un instrument esențial de apărare cibernetică. Conform raportului IBM Cost of a Data Breach 2024, organizațiile care utilizează extensiv IA și automatizarea în operațiunile de securitate au înregistrat un cost mediu al brecelor de date de 3,84 milioane USD, comparat cu 5,72 milioane USD pentru cele fără IA — o economie de 1,88 milioane USD și o reducere a timpului de identificare și remediere cu circa 100 de zile (IBM, 2024).

Piața globală a securității cibernetice bazate pe IA a atins 29,64 miliarde USD în 2025, cu o proiecție de 146,52 miliarde USD până în 2034, crescând cu un CAGR de 19,34% (Precedence Research, 2025). Aproximativ 69% dintre companii consideră IA o componentă necesară a apărării cibernetice, iar integrarea IA în stiva de securitate poate amplifica capacitatea de detecție a amenințărilor de 1,6 ori (SoSafe, 2025).

CONCLUZII.

Cercetarea confirmă că inteligența artificială are un impact dublu asupra securității cibernetice în economia digitală. Pe de o parte, IA amplifică semnificativ capacitățile ofensive ale actorilor de amenințare: peste 80% din campaniile de phishing utilizează IA, incidentele deepfake au crescut cu 257% în 2024, iar pierderile estimate din frauda generativă IA vor atinge 40 miliarde USD până în 2027. Pe de altă parte, IA poate reduce costul mediu al brecelor de date cu 1,88 milioane USD și timpul de răspuns cu 100 de zile.

Analiza comparativă evidențiază un decalaj semnificativ între UE și Republica Moldova. În timp ce UE beneficiază de un cadru legislativ matur (NIS2, AI Act), CERT-uri naționale dezvoltate

și investiții consistente, Moldova se confruntă cu resurse limitate, o instituție de securitate cibernetică tânără (ASC — 30 angajați) și o vulnerabilitate amplificată de contextul geopolitic.

Cu toate acestea, progresul Moldovei este notabil: adoptarea Legii securității cibernetice, înființarea ASC, crearea alianței cibernetice regionale cu Ucraina și România și înființarea Centrului de Excelență în Securitate Cibernetică (Cybercor) reprezintă pași importanți.

RECOMANDARI.

Pe baza rezultatelor cercetării, se formulează următoarele recomandări pentru consolidarea securității cibernetice în Republica Moldova:

1. Creșterea capacității instituționale a ASC — extinderea personalului de la 30 la minimum 80–100 de specialiști până în 2028, conform modelului agențiilor similare din statele baltice.
2. Transpunerea completă a Directivei NIS2 — extinderea obligațiilor de raportare și gestionare a riscurilor la toate sectoarele critice, în linie cu cerințele de aderare la UE.
3. Implementarea de programe de educație cibernetică — simulari de phishing cu IA și instruire privind deepfake-urile la nivel organizațional, care pot reduce incidentele cu până la 50% în 12 luni (Brightside AI, 2025).
4. Adoptarea soluțiilor de securitate bazate pe IA — integrarea instrumentelor de detecție a amenințărilor bazate pe IA în infrastructura critică, urmând modelul investițiilor din UE.
5. Consolidarea cooperării internaționale — aprofundarea parteneriatului cu alianța cibernetică regională (Ucraina–România–Moldova), participarea la exercițiile CCDCOE NATO și extinderea colaborării cu ENISA.

REFERINȚE:

1. AFCEA. (2026). Moldova's Mighty Mission to a Cyber Resilient State. AFCEA International / SIGNAL Media.
2. Brightside AI. (2025). AI-Generated Phishing vs Human Attacks: 2025 Risk Analysis. Brightside AI Blog.
3. CSIS. (2024). Moldova's Sisyphean Security Struggle. Center for Strategic and International Studies.
4. CSIS. (2025). Strengthening Moldova's Cyber Landscape. Center for Strategic and International Studies.
5. DCAF. (2020). Cybersecurity Governance Assessment of Moldova. Geneva Centre for Security Sector Governance.
6. Deloitte. (2025). Generative AI Fraud Projections. Deloitte Center for Financial Services.
7. ENISA. (2024). ENISA Threat Landscape 2024. European Union Agency for Cybersecurity.
8. ENISA. (2025). ENISA Threat Landscape 2025. European Union Agency for Cybersecurity.
9. European Commission. (2024). Digital Economy Report. European Commission.
10. Europol. (2025). AI and Cybercrime Report. Europol.
11. IBM. (2024). Cost of a Data Breach Report 2024. IBM Security.
12. Keepnet Labs. (2025). Deepfake Statistics and Trends 2026. Keepnet Labs Blog.
13. NCSI. (2025). National Cyber Security Index: Moldova. e-Governance Academy.
14. OECD. (2023). Digital Economy Outlook 2023. OECD Publishing.
15. Precedence Research. (2025). AI Cybersecurity Market Size and Forecast. Precedence Research.
16. RUSI. (2023). Battening Down the Hatches: Moldova's Cyber Defence. Royal United Services Institute.
17. SlashNext. (2024). State of Phishing Report H2 2024. SlashNext.
18. SoSafe. (2025). AI in Cybersecurity: Global Trends Report. SoSafe.
19. The Record. (2024). Unprecedented Interference Targets Moldova's Elections. Recorded Future News.
20. UNDP. (2025). Cybersecurity for Justice Governance in Moldova — Project Document. United Nations Development Programme.

Coordonator științific: ȚURCAN Aurelia, dr.,conf.univ.
Academia de Studii Economice din Republica Moldova,
Chișinău, str. Bănulescu-Bodoni 61
e-mail: turcan.aurelia.4u8h@ase.md