DOI: https://doi.org/10.53486/sstc2026.v1.97
CZU: 004.056:004.8

THE DUALITY OF ARTIFICIAL INTELLIGENCE: FROM PROACTIVE THREAT DETECTION TO AUTOMATED CYBER ATTACKS

DUALITATEA INTELIGENȚEI ARTIFICIALE: DE LA DETECTAREA PROACTIVĂ A AMENINȚĂRILOR LA ATACURI CIBERNETICE AUTOMATIZATE

DODONOV Parascovia, studentă, anul II, specialitatea: Business și administrarea afacerilor
Academia de Studii Economice din Moldova
Republica Moldova, Chișinău, str. Mitropolit Gavriil Bănulescu Bodoni 61, https://ase.md/
e-mail autor: parascovia801@gmail.com

Abstract: *Artificial Intelligence (AI) has become one of the most controversial and, at the same time, most powerful technologies of the digital era- capable of protecting entire systems while also rendering them vulnerable. On one hand, AI is transforming cybersecurity through its ability to detect anomalies, analyze massive volumes of data in real time, and automatically respond to incidents- significantly reducing the time interval between the emergence of a threat and its neutralization. On the other hand, these same capabilities are being exploited by malicious actors to automate cyberattacks, generate sophisticated phishing campaigns, create convincing deepfakes, and develop adaptive malware that is difficult to detect through conventional methods. This contradiction places AI at the center of an unprecedent technological race, in which the boundary between protection and threat becomes increasingly fluid and difficult to define. The purpose of this research is to comparatively analyze the two dimensions of artificial intelligence use in cybersecurity- defensive and offensive- within the context of todays digital economy, with the aim of identifying mechanisms through which AI can be governed responsibly, maximizing its protective benefits while minimizing the risks associated with its malicious use.*
Keywords: *Artificial Intelligence, technology, cybersecurity, automated attacks, duality, phishing*.
JEL CLASSIFICATION: O33

INTRODUCERE

Importanța înțelegerii și gestionării dualității Inteligenței Artificiale în securitatea cibernetică devine, în contextul economiei digitale globale, o chestiune de supraviețuire instituțională și stabilitate națională, nu doar o prioritate tehnologică.

Transformarea digitală a economiei globale a plasat Inteligența Artificială (IA) în centrul unui paradox de securitate fără precedent. Atacatorii folosesc astăzi IA pentru a-și amplifica volumul atacurilor, a lansa campanii de inginerie socială- precum escrocheriile deepfake- și a personaliza atacurile pentru ținte individuale, crescându-și semnificativ ratele de succes. Această realitate plasează IA simultan în rolul de scut și sabie al lumii digitale, generând o cursă tehnologică în care granița dintre protecție și amenințare devine tot mai greu de definit.

Înțelegerea și gestionarea acestei dualități reprezintă una dintre cele mai urgente provocări ale securității cibernetice contemporane, cu implicații directe asupra stabilității economiei digitale la nivel global.

Scopul prezentei cercetări este de a analiza comparativ cele două dimensiuni ale utilizării inteligenței artificiale în securitatea cibernetică- defensivă și ofensivă – în contextul economiei digitale actuale cu scopul de a identifica mecanismele prin care IA poate fi guvernată responsabil, maximizând beneficiile sale protective și minimizând riscurile asociate utilizării sale malițioase.

Obiectivele principale abordate în cercetare sunt:

Analiza mecanismelor de detecție pro activă a amenințărilor bazate pe IA și a impactului acestora asupra reducerii timpului de răspuns la incidente cibernetice.

Identificarea și clasificarea principalelor tipuri de atacuri cibernetice automatizate facilitate sau amplificate de IA.

Evaluarea comparativă a capacităților defensive față de cele ofensive ale IA, pentru determinarea gradului de risc net la nivelul organizațiilor din economia digitală.

Formularea unor recomandări privind guvernanța responsabilă a IA în domeniul securității cibernetice, cu accent pe echilibrul dintre inovație tehnologică și protecția datelor.

CONȚINUTUL DE BAZĂ

1. Analiza succintă a surselor bibliografice.

Securitatea cibernetică este un subiect cu o abordare destul de detaliată și des folosit în era propriu-zisă, datorită influenței atât pozitive cât și negative asupra surselor de informație deținute la nivel global. În cazul cercetării respective, au fost consultate surse multiple, din diverse categorii ce stau la baza unei înțelegeri mai profunde a termenului ”securitate cibernetică” deoarece majoritatea sunt la curent cu existența acestuia, însă puține persoane înțeleg cu adevărat complexitatea fenomenului, mecanismele prin care acesta funcționează și mai ales, modul în care inteligența artificială îi redefinește profund limitele atât ca instrument de protecție, cât și ca vector de atac.

Principalele surse bibliografice folosite în demonstrarea temei cercetate le reprezintă: rapoarte corporative și de industrie, platforme tehnice specializate, studii academice și publicații științifice, date statistice și analize de tendință.

2. Descrierea metodelor de cercetare utilizate.

Pentru a înțelege și a analiza dualitatea inteligenței artificiale în securitatea cibernetică, au fost aplicate mai multe metode de cercetare, fiecare sprijinită de surse concrete și actuale. În cazul literaturii de specialitate, au fost studiate și comparate surse recunoscute la nivel internațional, printre care platforma ”Microsoft Security”, care explică în termeni clari cum funcționează IA în securitatea cibernetică- de la detectarea automată a amenințărilor până la răspunsul în timp real la atacuri. Sistemele de inteligență artificială învață continuu din noile date, îmbunătățindu-și capacitatea de a identifica și atenua amenințările emergente, de a reduce rezultatele fals pozitive și de a scala mai eficient eforturile de securitate.

Analiza comparativă a fost utilizată pentru a pune față în față cele două laturi ale IA- cea care protejează și cea care atacă. Platforma OPSWAT a furnizat informații concrete despre modul în care aceeași tehnologie este exploatată de infractorii cibernetici pentru a automatiza atacuri, a genera mesaje de phishing personalizate și de a dezvolta malware inteligent, greu de detectat prin metode tradiționale. Comparând aceste date cu mecanismele defensive, s-a putut determina clar unde IA ajută și unde creează vulnerabilități noi.

Au fost consultate rapoarte de referință precum (IBM Cost of a Data Breach Report, 2024), considerat cel mai credibil studiu anual din industria securității cibernetice, bazat pe analiza a sute de organizații la nivel global. Aceste date au oferit o imagine concretă asupra costurilor reale ale atacurilor cibernetice și a beneficiilor financiare aduse de adoptarea IA în apărarea digitală.

Studiul comprehensiv publicat în (Springer Nature- Discover Applied Sciences, 2025) explorează tehnici avansate de învățare automată și profundă în detectarea intruziunilor, analiza malware-ului, detectarea phishing-ului și autentificarea utilizatorilor, furnizând un cadru analitic solid pentru evaluarea comparativă a soluțiilor defensive bazate pe IA.

Prin combinarea acestor metode, cercetarea reușește să abordeze tema din multiple unghiuri- tehnic, statistic și teoretic- oferind o perspectivă echilibrată și fundamentată asupra dualității inteligenței artificiale în securitatea cibernetică.

3. Beneficiile utilizării securității cibernetice

Beneficiile pe care le aduce o securitate cibernetică bine implementată se resimt atât la nivel organizațional, cât și economic și social:

Protecția datelor și a activelor digitale - fără această protecție, organizațiile riscă pierderea unor active digitale valoroase, cu consecințe financiare și reputaționale grave.

Crearea de valoare și stimulare a inovației - investiția în securitatea cibernetică nu înseamnă doar protecție, ci și un avantaj competitiv real pe piață.

Reducerea costurilor pe termen lung - organizațiile la nivel global au investit în automatizarea detectării amenințărilor, iar optimizarea instrumentelor tehnologice și simplificarea soluțiilor de securitate cibernetică pot reduce cheltuielile și în același timp pot spori vizibilitatea și diminua numărul de puncte vulnerabile

Educația și conștientizarea - cursurile de securitate cibernetică sunt deosebit de importante în cadrul organizațiilor, unde educarea angajaților poate reduce semnificativ riscul de atacuri și breșe de securitate, iar într-o lume în care tehnologia evoluează constant, cunoștințele în domeniu oferă instrumentele necesare pentru a face față provocărilor digitale zilnice.

4. Rezultatele obținute.

Datele prezentate în continuare vezi (Tabelul 1) sunt extrase din (IBM Cost of a Data Breach Report, 2024) cel mai complet și credibil raport anual din industria securității cibernetice, realizat de Ponemon Institute pe baza analizei a 604 organizații din 17 industrii și 16 țări, în perioada martie 2023 - februarie 2024.

Tabelul 1. Costurile breșelor de securitate cibernetică - IBM Cost of a Data Breach Report 2024

Indicator	Valoare
Costul mediu global al unei breșe de securitate (2024)	4,88 milioane USD
Creșterea față de 2023	+10% (cea mai mare creștere de la pandemie)
Costul mediu al unei breșe în sectorul financiar	6,08 milioane USD
Costul breșelor ce implică date din mai multe medii cloud	4,75 milioane USD
Costul total al activităților post - breșă	2,8 milioane USD (cel mai ridicat din ultimii 6 ani)

Sursa: Raportul complet IBM Cost of a Data Breach 2024 https://newsroom.ibm.com/2024-07-30-ibm-report-escalating-data-breach-disruption-pushes-costs-to-new-highs

Pentru a înțelege originea acestor costuri, este esențial să examinăm principalele cauze și vectorii de atac care stau la baza breșelor de securitate cibernetică, prezentați în tabelul următor.

Tabelul 2. Principalele cauze și vectori inițiali de atac

Vector de atac/ Cauză	Pondere/ Cost mediu
1. Credențiale furate sau compromise	16% din totalul breșelor
2. Phishing	Cost mediu 4,88 milioane USD
3. Atacuri din interior (insider malicious)	Cost mediu 4,99 milioane USD (cel mai costisitor vector)
4. Date shadow (negestionate) implicate în breșe	35% din totalul breșelor
5. Creștere cost per breșă cu date shadow	+16% față de medie

Sursa: IBM Newsroom (date despre vectorii de atac)
https://newsroom.ibm.com/2024-07-30-ibm-report-escalating-data-breach-disruption-pushes-costs-to-new-highs

CONCLUZII

Inteligența Artificială reprezintă fără îndoială, cea mai puternică tehnologie a erei digitale capabilă să protejeze sisteme întregi, dar și să le vulnerabilizeze în mod decisiv.

Cercetarea de față a demonstrat că această dualitate fundamentală nu poate fi ignorată sau minimalizată, ci trebuie înțeleasă, gestionată și guvernată responsabil. Datele analizate confirmă că organizațiile care adoptă IA în mod strategic în procesele lor de securitate sunt semnificativ mai reziliențe în fața atacurilor cibernetice, înregistrând costuri mai mici, timpi de răspuns mai rapizi și pierderi considerabile reduse.

În același timp, aceeași tehnologie, plasată în mâinile actorilor malițioși, amplifică amenințările la o scară fără precedent. Într-o lume digitală în continuă accelerare, răspunsul nu

constă în a evita IA, ci în a o adopta responsabil, a o reglementa inteligent și a construi în jurul ei o cultură solidă de securitate cibernetică la nivel individual, organizațional și global.

REFERINȚE:

1. Microsoft Security (2024). Ce este Inteligența Artificială pentru securitatea cibernetică? https://www.microsoft.com/ro-ro/security/business/security-101/what-is-ai-for-cybersecurity
2. OPSWAT (2024). Atacurile cibernetice bazate pe inteligența artificială- Cum să detectăm, să prevenim și să ne apărăm împotriva amenințărilor inteligente. https://romanian.opswat.com/blog/ai-powered-cyberattacks
3. Bittnet (2024). Top 20 cele mai frecvente tipuri de atacuri de securitate cibernetică. https://www.bittnet.ro/noutati/top-20-cele-mai-frecvente-tipuri-de-atacuri-de-securitate-cibernetica/
4. IBM& Ponemon Institute (2024). Cost of a Data Breach Report 2024. IBM Corporation https://newsroom.ibm.com/2024-07-30-ibm-report-escalating-data-breach-disruption-pushes-costs-to-new-highs
5. IBM (2024). Cost of a Data Breach 2024- Financial Industry. https://www.ibm.com/think/insights/cost-of-a-data-breach-2024-financial-industry

Coordonator științific: CAPAȚINA Valentina, dr., conf. univ.,
Academia de Studii Economice din Moldova
Republica Moldova, Chișinău,
str. Mitropolit Gavriil Bănulescu Bodoni 61, https://ase.md/
e-mail: valentina@ase.md