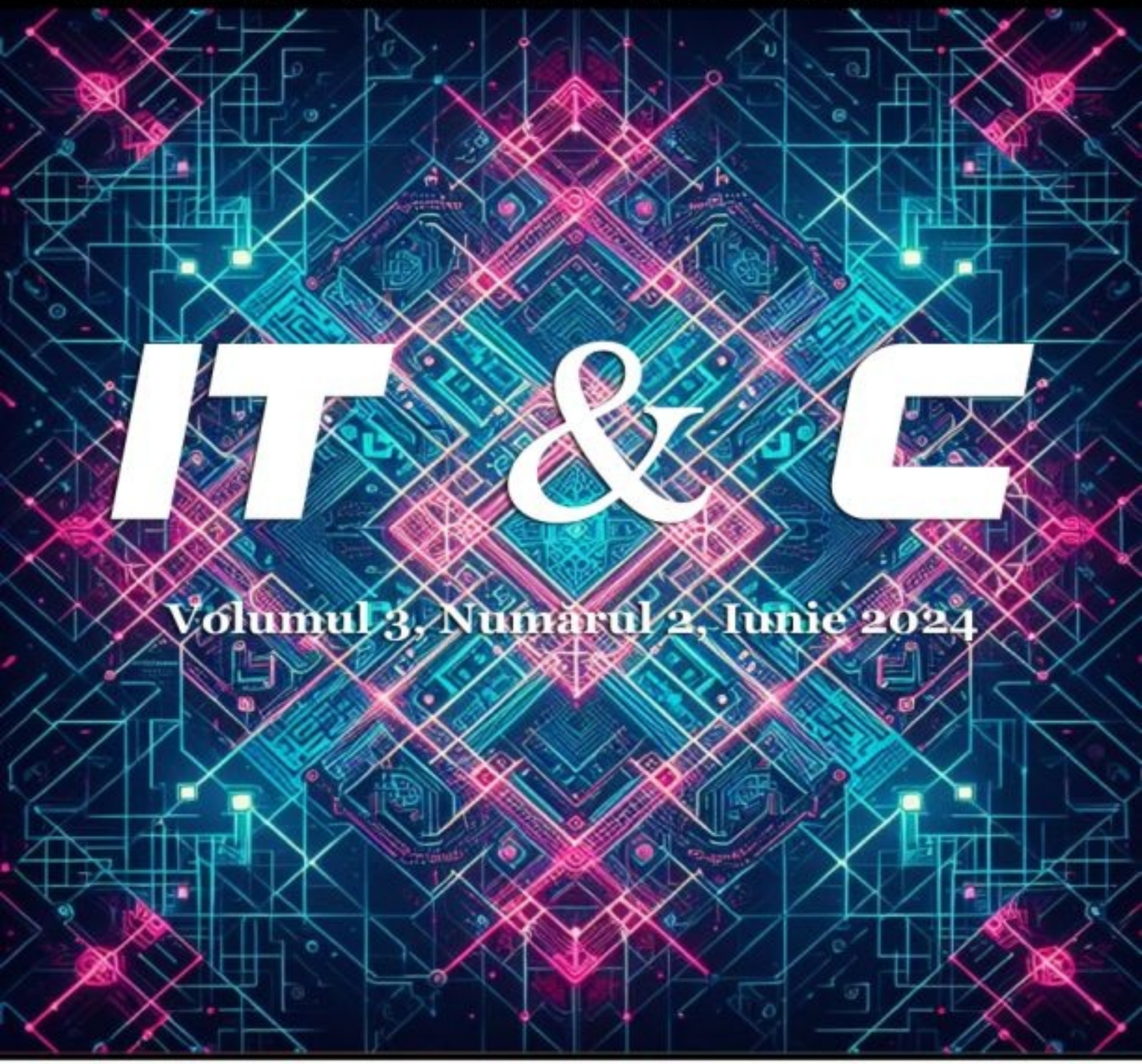
IT & C

Piaţa Presei Libere, Nr. 1
Casa Presei Libere, Corp A3, Etaj 1
013701 Bucureşti, Sectorul 1

Web: www.internetmobile.ro
Email: contact@internetmobile.ro
Tel./WhatsApp: 0745 526 896

ISSN 2821 - 8469 ISSN - L 2821 - 8469 Volumul 3 Numărul 2 Iunie 2024



Redactor şef: Nicolae Sfetcu

Publicat de MultiMedia Publishing

IT & C

ISSN 2821 – 8469, ISSN – L 2821 – 8469, Volumul 3, Numărul 2, Iunie 2024

PUBLICAȚIE TRIMESTRIALĂ DE INFORMARE, STUDII ȘI COMUNICĂRI

DOI: 10.58679/IT78551

Piața Presei Libere, Nr. 1, Casa Presei Libere, Corp A3, Etaj 1

013701 București, Sectorul 1

https://www.internetmobile.ro

Email: contact@internetmobile.ro

Tel./WhatsApp: 0745 526 896

CUPRINS / CONTENTS

EDITORIAL / EDITORIAL

Utilizarea științei datelor în detectarea amenințărilor persistente avansate

Ing. fiz. Nicolae SFETCU[1], MPhil
nicolae@sfetcu.com

Levering Data Science in the Detection of Advanced Persistent Threats

Abstract

In today's interconnected digital landscape, the threat of cyber attacks is greater than ever. Among the most insidious of these threats are advanced persistent attacks (APTs), sophisticated attacks orchestrated by savvy adversaries with specific goals in mind, such as espionage, data theft, or sabotage. Advanced persistent threats are a significant cybersecurity issue of concern today, posing serious risks to organizations, governments, and individuals. Traditional security measures attempt to detect and mitigate APTs due to their complex and ever-evolving nature. The advent of data science has provided new ways to identify and effectively combat these threats, playing a crucial role in detecting advanced persistent threats today. The complexity and stealth of APT requires advanced detection techniques, where data science methodologies are essential.
Keywords: data science, advanced persistent threats, anomaly detection, behavioral analysis, machine learning, analytics

Rezumat

În peisajul digital interconectat de astăzi, amenințarea atacurilor cibernetice este mai mare ca niciodată. Printre cele mai insidioase dintre aceste amenințări se numără atacurile persistente avansate (APA), atacuri sofisticate orchestrate de adversari pricepuți cu obiective specifice în minte, cum ar fi spionajul, furtul de date sau sabotajul. Amenințările persistente avansate sunt astăzi o problemă de securitate cibernetică semnificativă îngrijorătoare, care prezintă riscuri grave pentru organizații, guverne și indivizi.
Măsurile de securitate tradiționale încearcă să detecteze și să atenueze APA datorită naturii lor complexe și în continuă evoluție. Apariția științei datelor a oferit noi căi pentru identificarea și combaterea eficientă a acestor amenințări, jucând astăzi un rol crucial în

[1] Cercetător - Academia Română - Comitetul Român de Istoria și Filosofia Științei și Tehnicii (CRIFST), Divizia de Istoria Științei (DIS), ORCID: 0000-0002-0162-9973

detectarea amenințărilor persistente avansate. Complexitatea și caracterul ascuns al APA necesită tehnici avansate de detectare, unde metodologiile științei datelor sunt esențiale.
Cuvinte cheie: știința datelor, amenințările persistente avansate, detectarea anomaliilor, analiza comportamentală, învățarea automată, analitica

IT & C, Volumul 3, Numărul 2, Iunie 2024, pp. 3-21
ISSN 2821 - 8469, ISSN – L 2821 – 8469, DOI: 10.58679/IT60001
URL: https://www.internetmobile.ro/utilizarea-stiintei-datelor-in-detectarea-amenintarilor-persistente-avansate/

TEHNOLOGIA INFORMAȚIEI / INFORMATION TECHNOLOGY

Detectarea amenințărilor persistente avansate în războiul cibernetic – Studii academice

Ing. fiz. Nicolae SFETCU[1], MPhil
nicolae@sfetcu.com

Detecting Advanced Persistent Threats in Cyber Warfare – Academic Studies

Abstract

In the ever-evolving landscape of cybersecurity, advanced persistent threats pose a formidable challenge. Detecting advanced persistent threats is a complex and ongoing challenge for organizations and cybersecurity professionals, requiring a multi-layered strategy incorporating various tools, techniques, and approaches. This essay explores the methods and challenges involved in detecting APTs.
Keywords: advanced persistent threats, APT, anomaly detection, behavioral analysis, sandbox, machine learning, cyber warfare, academic studies

Rezumat

În peisajul în continuă evoluție al securității cibernetice, amenințările persistente avansate reprezintă o provocare formidabilă. Detectarea amenințărilor persistente avansate este o provocare complexă și continuă pentru organizații și profesioniștii în securitate cibernetică, necesitând o strategie cu mai multe straturi care încorporează diverse instrumente, tehnici și abordări. Acest eseu explorează metodele și provocările implicate în detectarea APT-urilor.
Cuvinte cheie: amenințările persistente avansate, APT, detectarea anomaliilor, analiza comportamentală, sandbox, învățarea automată, războiul cibernetic, studii academice

IT & C, Volumul 3, Numărul 2, Iunie 2024, pp. 22-31
ISSN 2821 - 8469, ISSN – L 2821 – 8469, DOI: 10.58679/IT78363
URL: https://www.internetmobile.ro/detectarea-amenintarilor-persistente-avansate-in-razboiul-cibernetic-studii-academice/

[1] Cercetător - Academia Română - Comitetul Român de Istoria și Filosofia Științei și Tehnicii (CRIFST), Divizia de Istoria Științei (DIS), ORCID: 0000-0002-0162-9973

TELECOMUNICAȚII / TELECOMMUNICATIONS

Inteligența artificială în comunicații în războiul electronic

Ing. fiz. Nicolae SFETCU[1], MPhil
nicolae@sfetcu.com

Artificial Intelligence in Communications in Electronic Warfare

Abstract

Artificial intelligence is a critical force multiplier in electronic warfare and can be a highly effective tool when applied to areas such as signal recognition, emission and signal control, emitter classification, threat recognition, and jamming identification. From tactical situational awareness and management, threat recognition and classification, and emission and signature control tactics, to over-the-horizon targeting and non-kinetic sights using non-organic electronic warfare capabilities, AI will be a huge asset in force lethality. Looking ahead, continued research and development in AI technologies, along with strong ethical and regulatory frameworks, will shape the future landscape of electronic warfare communications for years to come.
This article explores the integration of artificial intelligence into electronic warfare communications, its implications, challenges, and potential future directions.
Keywords: artificial intelligence, machine learning, electronic warfare, jamming, threats, communications, telecommunications

Rezumat

Inteligența artificială este un multiplicator de forță critică în războiul electronic și poate fi un instrument extrem de eficient atunci când este aplicat în domenii precum recunoașterea semnalului, controlul emisiilor și semnalului, clasificarea emitenților, recunoașterea amenințărilor și identificarea bruiajului. De la conștientizarea și gestionarea situației tactice, recunoașterea și clasificarea amenințărilor și tacticile de control al emisiilor și semnăturilor, până la țintirea peste orizont și vizările non-cinetice folosind capabilități de război electronic non-organice, inteligența artificială va fi un avantaj enorm în letalitatea forței. Privind în perspectivă, cercetarea și dezvoltarea continuă în tehnologiile inteligenței artificiale, împreună cu cadre etice și de reglementare solide, vor modela peisajul viitor al comunicațiilor de război electronic în anii următori.

[1] Cercetător - Academia Română - Comitetul Român de Istoria și Filosofia Științei și Tehnicii (CRIFST), Divizia de Istoria Științei (DIS), ORCID: 0000-0002-0162-9973

Acest articol explorează integrarea inteligenței artificiale în comunicațiile de război electronic, implicațiile sale, provocările și potențialele direcții viitoare.
Cuvinte cheie: inteligența artificială, învățarea automată, război electronic, bruiaj, amenințări, comunicații, telecomunicații

IT & C, Volumul 3, Numărul 2, Iunie 2024, pp. 32-49
ISSN 2821 - 8469, ISSN – L 2821 – 8469, DOI: 10.58679/IT20921
URL: https://www.internetmobile.ro/inteligenta-artificiala-in-comunicatii-in-razboiul-electronic/

PROGRAMARE / PROGRAMMING

Algoritmi de inteligență artificială în războiul electronic

Ing. fiz. Nicolae SFETCU[1], MPhil
nicolae@sfetcu.com

Artificial Intelligence Algorithms in Electronic Warfare

Abstract

Electronic warfare is a critical area where the convergence of technology and strategy is shaping the battlefield. In this field, artificial intelligence algorithms have emerged as indispensable tools, providing unmatched capabilities in detection, processing and response. IA algorithms provide decision support to operators by suggesting optimal countermeasures or defensive actions. These systems can assess multiple threats and prioritize responses based on learned enemy tactics and the criticality of assets at risk.
This article explores the multifaceted role of IA algorithms in electronic warfare, illuminating their applications, challenges, and implications for future conflicts.
Keywords: electronic warfare, artificial intelligence, algorithms, radar, neural networks

Rezumat

Războiul electronic reprezintă un domeniu critic în care convergența tehnologiei și strategiei modelează câmpul de luptă. În acest domeniu, algoritmii de inteligență artificială au apărut ca instrumente indispensabile, oferind capacități de neegalat în detectare, procesare și răspuns. Algoritmii IA oferă operatorilor suport de decizie, sugerând contramăsuri optime sau acțiuni defensive. Aceste sisteme pot evalua amenințările multiple și pot prioritiza răspunsurile pe baza tacticilor învățate ale inamicului și a criticității activelor expuse riscului.
Acest articol explorează rolul multiforme al algoritmilor IA în războiul electronic, luminând aplicațiile, provocările și implicațiile acestora pentru conflictele viitoare.
Cuvinte cheie: războiul electronic, inteligența artificială, algoritmi, radar, rețele neuronale

[1] Cercetător - Academia Română - Comitetul Român de Istoria și Filosofia Științei și Tehnicii (CRIFST), Divizia de Istoria Științei (DIS), ORCID: 0000-0002-0162-9973

IT & C, Volumul 3, Numărul 2, Iunie 2024, pp. 50-59
ISSN 2821 - 8469, ISSN – L 2821 – 8469, DOI: 10.58679/IT25231
URL: https://www.internetmobile.ro/algoritmi-de-inteligenta-artificiala-in-razboiul-electronic/

SECURITATE CIBERNETICĂ / CYBER SECURITY

Studii de caz privind atacurile cibernetice – Amenințările persistente avansate

Ing. fiz. Nicolae SFETCU[1], MPhil
nicolae@sfetcu.com

Cyber Attack Case Studies – Advanced Persistent Threats

Abstract

In the rapidly evolving technology landscape, the proliferation of cyberattacks has become a pervasive threat, permeating every sector of society. From government institutions to private businesses and individual users, no entity is immune to the pernicious effects of cybercrime. Understanding the anatomy of past cyberattacks is crucial to strengthening defenses and fostering resilience in the face of future threats. These incidents underscore the importance of cybersecurity measures and the constant need for vigilance against evolving cyber threats.
Keywords: cyberattacks. advanced persistent threats, Titan Rain., Sykipot, GhostNet, Stuxnet, Duqu, Flame, Carbanak, Red October

Rezumat

În peisajul cu evoluție rapidă a tehnologiei, proliferarea atacurilor cibernetice a devenit o amenințare omniprezentă, pătrunzând în fiecare sector al societății. De la instituții guvernamentale la întreprinderi private și utilizatori individuali, nicio entitate nu este imună la efectele pernicioase ale criminalității informatice. Înțelegerea anatomiei atacurilor cibernetice din trecut este crucială pentru întărirea apărării și încurajarea rezilienței în fața amenințărilor viitoare. Aceste incidente subliniază importanța măsurilor de securitate cibernetică și nevoia constantă de vigilență împotriva amenințărilor cibernetice în evoluție.
Cuvinte cheie: atacuri cibernetice. amenințările persistente avansate, Titan Rain., Sykipot, GhostNet, Stuxnet, Duqu, Flame, Carbanak, Red October

[1] Cercetător - Academia Română - Comitetul Român de Istoria și Filosofia Științei și Tehnicii (CRIFST), Divizia de Istoria Științei (DIS), ORCID: 0000-0002-0162-9973

IT & C, Volumul 3, Numărul 2, Iunie 2024, pp. 60-71
ISSN 2821 - 8469, ISSN – L 2821 – 8469, DOI: 10.58679/IT23220
URL: https://www.internetmobile.ro/studii-de-caz-privind-atacurile-cibernetice-amenintarile-persistente-avansate/