



IT & C

Piața Presei Libere, Nr. 1
Casa Presei Libere, Corp A3, Etaj 1
013701 București, 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 1

Martie 2024

IT & C

Volumul 3, Numărul 1, Martie 2024

Redactor șef: Nicolae Sfetcu

Publicat de MultiMedia Publishing



IT & C

ISSN 2821 – 8469, ISSN – L 2821 – 8469, Volumul 3, Numărul 1, Martie 2024

PUBLICAȚIE TRIMESTRIALĂ DE INFORMARE, STUDII ȘI COMUNICĂRI

DOI: 10.58679/IT15115

REZUMATE

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

Redactor șef: Nicolae Sfetcu

Colegiul de redacție: Dr. Tiberiu Tănase; Dr. ec. Andreea Florina Radu, Darius-Antoniou Ferent

Consiliul științific: Dr. Alexandru Ion, Dr. Ioana Petcu, Constantin Nica

© 2024 MultiMedia Publishing, București, 2024.

CUPRINS / CONTENTS

CUPRINS / CONTENTS.....	2
EDITORIAL / EDITORIAL.....	3
Provocări și limitări în utilizarea inteligenței artificiale	3
TEHNOLOGIA INFORMAȚIEI / INFORMATION TECHNOLOGY	4
Impact of Big Data Technology on Contemporary Society.....	4
Metode, tehnici și modele ale amenințărilor persistente avansate – Ciclul de viață al APT	6
TELECOMUNICAȚII / TELECOMMUNICATIONS	8
The Revolutionary Role of Blockchain Technology in Communication	8
PROGRAMARE / PROGRAMMING	10
Algoritmi IA utilizați în securitatea națională	10
SECURITATE CIBERNETICĂ / CYBER SECURITY	12
Securitatea cibernetică și războiul cibernetic.....	12
Amenințările Persistente Avansate în securitatea cibernetică	14

EDITORIAL / EDITORIAL

Provocări și limitări în utilizarea inteligenței artificiale

Ing. fiz. Nicolae SFETCU¹, MPhil
nicolae@sfetcu.com

Challenges and Limitations in the Use of Artificial Intelligence

Abstract

The use of artificial intelligence (AI) has expanded dramatically across sectors including healthcare, finance, transportation and more, including the military, providing unprecedented opportunities for efficiency, innovation and problem solving. However, this rapid adoption comes with a spectrum of challenges and limitations that require careful consideration. This essay looks at the key challenges and limitations inherent in the use of AI, including ethical concerns, bias and fairness, transparency and explainability, security risks and employment impacts.

Keywords: artificial intelligence, national security, data, vulnerabilities, ethics, bias, explainability, risks

Rezumat

Utilizarea inteligenței artificiale (AI) s-a extins dramatic în diferite sectoare, inclusiv în domeniul sănătății, finanțelor, transporturilor și multe altele, inclusiv în domeniul militar, oferind oportunități fără precedent de eficiență, inovare și rezolvare de probleme. Cu toate acestea, această adoptare rapidă vine cu un spectru de provocări și limitări care necesită o analiză atentă. Acest eseu analizează provocările și limitările cheie inerente utilizării AI, inclusiv preocupările etice, părtinirea și corectitudinea, transparența și explicabilitatea, riscurile de securitate și impactul asupra angajării.

Cuvinte cheie: inteligența artificială, securitatea națională, date, vulnerabilități, etica, prejudecăți, explicabilitate, riscuri

IT & C, Volumul 3, Numărul 1, Martie 2024, pp. 3-10

ISSN 2821 - 8469, ISSN – L 2821 – 8469, DOI: [10.58679/IT76296](https://doi.org/10.58679/IT76296)

URL: <https://www.internetmobile.ro/provocari-si-limitari-in-utilizarea-inteligenței-artificiale/>

© 2024 Nicolae Sfetcu. Responsabilitatea conținutului, interpretărilor și opiniilor exprimate revine exclusiv autorilor.

¹ Researcher - Romanian Academy - Romanian Committee of History and Philosophy of Science and Technology (CRIFST), Division of History of Science (DIS), ORCID: 0000-0002-0162-9973

Impact of Big Data Technology on Contemporary Society

Ing. fiz. Nicolae SFETCU¹, MPhil
nicolae@sfetcu.com

Abstract

This essay explores the profound implications of Big Data technology on various facets of contemporary society. As the digital landscape continues to evolve, the ability to collect, process, and analyze massive volumes of data has become a pivotal force shaping industries, governance, and individual experiences. With the increasing volume of data on the Internet, in social media, cloud computing, mobile devices and government data, Big Data is both a threat and an opportunity for researchers to manage and use this data while maintaining the rights of the involved people. The essay delves into the key features of Big Data technology, its applications across different sectors, and the associated challenges and opportunities.

Keywords: big data, technology, ethics, challenges, trends, applications, research, society

Impactul tehnologiei Big Data asupra societății contemporane

Rezumat

Acest eseu explorează implicațiile profunde ale tehnologiei Big Data asupra diferitelor fațete ale societății contemporane. Pe măsură ce peisajul digital continuă să evolueze, capacitatea de a colecta, procesa și analiza volume masive de date a devenit o forță esențială care modelează industriile, guvernarea și experiențele individuale. Odată cu creșterea volumului de date pe Internet, în rețelele sociale, cloud computing, dispozitive mobile și date guvernamentale, Big Data este atât o amenințare, cât și o oportunitate pentru cercetători de a gestiona și utiliza aceste date, păstrând în același timp drepturile persoanelor implicate. Eseul analizează caracteristicile cheie ale tehnologiei Big Data, aplicațiile sale în diferite sectoare și provocările și oportunitățile asociate.

¹ Researcher - Romanian Academy - Romanian Committee of History and Philosophy of Science and Technology (CRIFST), Division of History of Science (DIS), ORCID: 0000-0002-0162-9973

Cuvinte cheie: big data, tehnologie, etică, provocări, tendințe, aplicații, cercetare, megadate, date massive, date mari, societate

IT & C, Volumul 3, Numărul 1, Martie 2024, pp. 11-19

ISSN 2821 - 8469, ISSN – L 2821 – 8469, DOI: [10.58679/IT73078](https://doi.org/10.58679/IT73078)

URL: <https://www.internetmobile.ro/impact-of-big-data-technology-on-contemporary-society/>

© 2023 Nicolae Sfetcu. Responsabilitatea conținutului, interpretărilor și opiniilor exprimate revine exclusiv autorilor.

Metode, tehnici și modele ale amenințărilor persistente avansate – Ciclul de viață al APT

Ing. fiz. Nicolae SFETCU¹, MPhil
nicolae@sfetcu.com

Methods, Techniques and Patterns of Advanced Persistent Threats – APT Lifecycle

Abstract

Advanced persistent threats use a variety of methods and techniques, the most commonly used being phishing and spear-phishing, social engineering, drive-by-download, zero-day exploits, malware and backdoors, and watering hall). In APTs, it is difficult to identify who the attacker is, as they often use the concept of false flag, impersonating someone else, to camouflage their operations. In addition to state actors, there are privately funded and non-governmental cybercriminal groups using various methods of propagation. In general, the cyber espionage carried out by these actors targets diplomatic organizations and the information technology industry.

Keywords: advanced persistent threats, phishing, spear-phishing, social engineering, drive-by-download, exploit zero-day, malware, backdoor, watering hole

Rezumat

Amenințările persistente avansate folosesc o varietate de metode și tehnici, cele mai utilizate fiind phishing și spear-phishing, inginerie socială, descărcare neintenționată (drive-by-download), exploit zero-day, programe malware și backdoor, și gura de apă (watering hole). În APT, este dificil de identificat cine este atacatorul, întrucât aceștia folosesc adesea conceptul de steagul fals, identificându-se drept altă persoană, pentru a-și camufla operațiunile. Pe lângă actorii statali, există grupuri de criminali cibernetici cu finanțare privată și care nu răspund intereselor guvernamentale, folosind diferite metode de propagare. În general spionajul cibernetic realizat de acești actori au ca ținte organizațiile diplomatice și industria tehnologiei informației.

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

Cuvinte cheie: amenințările persistente avansate, phishing, spear-phishing, inginerie socială, drive-by-download, exploit zero-day, malware, backdoor, watering hole

IT & C, Volumul 3, Numărul 1, Martie 2024, pp. 20-39

ISSN 2821 - 8469, ISSN – L 2821 – 8469, DOI: [10.58679/IT18363](https://doi.org/10.58679/IT18363)

URL: <https://www.internetmobile.ro/metode-tehnici-si-modele-ale-amenintarilor-persistente-avansate-ciclul-de-viata-al-apt/>

© 2024 Nicolae Sfetcu. Responsabilitatea conținutului, interpretărilor și opiniilor exprimate revine exclusiv autorilor.

TELECOMUNICAȚII / TELECOMMUNICATIONS

The Revolutionary Role of Blockchain Technology in Communication

Ing. fiz. Nicolae SFETCU¹, MPhil
nicolae@sfetcu.com

Abstract

Communication is the cornerstone of human interaction, and as technology advances, so does the way we connect with each other. One of the most groundbreaking innovations in recent years is blockchain technology, initially designed to underpin cryptocurrencies like Bitcoin. However, its applications extend far beyond the financial sector. This essay explores the transformative impact of blockchain technology on communication, examining its key features, benefits, and potential challenges. Starting with 2014, new technology applications have been developed for more sophisticated smart contracts that share documents or automatically send owners' dividends if profits reach a certain level, and communication.

Keywords: blockchain, blockchain technology, communication, cryptocurrencies, cryptographic messages

Rolul revoluționar al tehnologiei blockchain în comunicare

Rezumat

Comunicarea este piatra de temelie a interacțiunii umane și, pe măsură ce tehnologia avansează, la fel crește și modul în care ne conectăm unul cu celălalt. Una dintre cele mai inovatoare inovații din ultimii ani este tehnologia blockchain, concepută inițial pentru a susține criptomonede precum Bitcoin. Cu toate acestea, aplicațiile sale se extind cu mult dincolo de sectorul financiar. Acest eseu explorează impactul transformator al tehnologiei

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

blockchain asupra comunicării, examinând caracteristicile sale cheie, beneficiile și provocările potențiale. Începând cu 2014, au fost dezvoltate noi aplicații tehnologice pentru contracte inteligente mai sofisticate care partajează documente sau trimit automat dividende proprietarilor dacă profiturile ating un anumit nivel și comunicare.

Cuvinte cheie: blockchain, tehnologie blockchain, comunicații, criptomonede, mesaje criptografice

IT & C, Volumul 3, Numărul 1, Martie 2024, pp. 40-46

ISSN 2821 - 8469, ISSN – L 2821 – 8469, DOI: [10.58679/IT88509](https://doi.org/10.58679/IT88509)

URL: <https://www.internetmobile.ro/the-revolutionary-role-of-blockchain-technology-in-communication/>

© 2024 Nicolae Sfetcu. Responsabilitatea conținutului, interpretărilor și opiniilor exprimate revine exclusiv autorilor.

PROGRAMARE / PROGRAMMING

Algoritmi IA utilizați în securitatea națională

Ing. fiz. Nicolae SFETCU¹, MPhil
nicolae@sfetcu.com

AI Algorithms Used in National Security

Abstract

Artificial intelligence is a fast -growing technological field, which captures the attention in the field of defense, political decision makers and international competitors. Artificial intelligence is increasingly playing a significant role in the analysis of intelligence, which is the process of collecting, evaluating and interpreting information to produce actionable intelligence, and national security in general.

Keywords: artificial intelligence, defense, national security, data, natural language processing, recognition, analysis, monitoring, vulnerabilities

Rezumat

Inteligența artificială este un domeniu tehnologic în creștere rapidă, care captează atenția în domeniul apărării, factorilor de decizie politică și concurenților internaționali deopotrivă. Inteligența artificială joacă din ce în ce mai mult un rol semnificativ în analiza inteligenței, care este procesul de colectare, evaluare și interpretare a informațiilor pentru a produce inteligență acționabilă, și securitatea națională în general.

Cuvinte cheie: inteligența artificială, apărare, securitatea națională, date, procesarea limbajului natural, recunoașterea, analiza, monitorizare, vulnerabilități

¹ Researcher - Romanian Academy - Romanian Committee of History and Philosophy of Science and Technology (CRIFST), Division of History of Science (DIS), ORCID: 0000-0002-0162-9973

IT & C, Volumul 3, Numărul 1, Martie 2024, pp. 47-56

ISSN 2821 - 8469, ISSN – L 2821 – 8469, DOI: [10.58679/IT96935](https://doi.org/10.58679/IT96935)

URL: <https://www.internetmobile.ro/algorithmi-ia-utilizati-in-securitatea-nationala/>

© 2023 Nicolae Sfetcu. Responsabilitatea conținutului, interpretărilor și opiniilor exprimate revine exclusiv autorilor.

SECURITATE CIBERNETICĂ / CYBER SECURITY

Securitatea cibernetică și războiul cibernetic

Ing. fiz. Nicolae SFETCU¹, MPhil
nicolae@sfetcu.com

Cyber Security and Cyber Warfare

Abstract

Cyber security is the totality of measures to protect computer systems and networks against attacks by malicious actors that can affect digital or physical assets, or the image of a person or organization, disrupt a certain activity or negatively influence a certain trend. The field of cyber security is in constant flux, adapting to the ever-changing digital landscape. Cyber warfare involves the use of state-level cyber attacks, causing damage comparable to actual warfare and/or disrupting enemy infrastructure and systems. The future of cyber security and cyber warfare remains uncertain. Emerging technologies such as quantum computing and artificial intelligence are expected to revolutionize both offensive and defensive capabilities. The global community must anticipate the evolving threat landscape and adapt its strategies accordingly.

Keywords: artificial intelligence, cyber security, cyber warfare, advanced persistent threats, quantum computing, escalation dilemma

Rezumat

Securitatea cibernetică reprezintă totalitatea măsurilor de protecție a sistemelor și rețelelor informatice împotriva atacurilor de către actori rău intenționați prin care se pot aduce atingere activelor digitale sau fizice, sau imaginii unei persoane sau organizație, se poate perturba o anumită activitate sau influența negativ o anumită tendință. Domeniul securității cibernetică este în flux constant, adaptându-se la peisaj digital în continuă schimbare. Războiul cibernetic implică

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

utilizarea atacurilor cibernetice la nivel statal, provocând daune comparabile războiului real și/sau perturbând infrastructura și sistemele inamice. Viitorul securității cibernetice și al războiului cibernetic rămâne incert. Tehnologii emergente precum calculul cuantic și inteligența artificială se așteaptă să revoluționeze capabilitățile atât ofensiv cât și defensiv. Comunitatea globală trebuie să anticipeze evoluția peisajului amenințărilor și să-și adapteze strategiile în consecință.

Cuvinte cheie: inteligența artificială, securitatea cibernetică, războiul cibernetic, amenințări persistente avansate, calculul cuantic, dilema de escaladare

IT & C, Volumul 3, Numărul 1, Martie 2024, pp. 57-64

ISSN 2821 - 8469, ISSN – L 2821 – 8469, DOI: [10.58679/IT37085](https://doi.org/10.58679/IT37085)

URL: <https://www.internetmobile.ro/securitatea-cibernetica-si-razboiul-cibernetice/>

© 2024 Nicolae Sfetcu. Responsabilitatea conținutului, interpretărilor și opiniilor exprimate revine exclusiv autorilor.

Amenințările Persistente Avansate în securitatea cibernetică

Ing. fiz. Nicolae SFETCU¹, MPhil
nicolae@sfetcu.com

Advanced Persistent Threats in Cyber Security

Abstract

Advanced persistent threats are a class of cyber threats that pose a significant challenge to organizations and nations around the world. They are known for their advanced tactics, techniques, and procedures, as well as their ability to infiltrate and operate persistently on target systems for long periods of time. Advanced persistent threats are characterized by persistence (remaining undetected in a target environment for long periods, sometimes even years), pinpoint targeting (selective, tailoring their attacks to the vulnerabilities or weaknesses of targets), and sophistication (advanced and cutting-edge techniques generation, some even innovative, often using zero-day exploits, social engineering and other sophisticated methods).

Keywords: Advanced Persistent Threats, cyber security, cyber threats, cyber warfare, multi-stage attacks

Rezumat

Amenințările persistente avansate sunt o clasă de amenințări cibernetică care reprezintă o provocare semnificativă pentru organizații și națiuni din întreaga lume. Ele sunt cunoscute pentru tacticile, tehnicile și procedurile lor avansate, precum și pentru capacitatea lor de a se infiltra și de a opera în mod persistent în sistemele țintă pentru perioade îndelungate. Amenințările persistente avansate se remarcă prin persistență (rămân nedetectate într-un mediu țintă pentru perioade lungi, uneori chiar ani), țintire punctuală (selective, personalizându-și atacurile pentru vulnerabilitățile sau punctele slabe ale țintelor), și rafinament (tehnică avansată și de ultimă generație, unele chiar inovative, utilizând adesea exploatări zero-day, inginerie socială și alte metode sofisticate).

Cuvinte cheie: Amenințările Persistente Avansate, securitatea cibernetică, amenințări cibernetică, război cibernetic, multi-stage attacks

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 1, Martie 2024, pp. 65-74

ISSN 2821 - 8469, ISSN – L 2821 – 8469, DOI: 10.58679/IT35506

URL: <https://www.internetmobile.ro/amenintarile-persistente-avansate-in-securitatea-cibernetica/>

© 2024 Nicolae Sfetcu. Responsabilitatea conținutului, interpretărilor și opiniilor exprimate revine exclusiv autorilor.