„În războiul hibrid, inteligența artificială este arta supremă a strategiei.”

Rolul Inteligenței Artificiale /în/ Securitatea Națională

Provocări, soluții și perspective pentru România

Ovidiu Bernaschi
B.Sc. Hons. in Computer Applications Information Systems
Coordonator:
Lector univ.dr. Tiberiu Tanase

inovitec.eu

inovitec.ro

Ovidiu Bernaschi

Fondator InoviTeC & Cloudimpuls

Absolvent al Dublin City University & Universitatea Româno-Americană

Instructor academic la nivel de Master in Cybersecurity (U.L.B. Sibiu)

Ofiţer (rzv) Comunicaţii, Tehnologia Informației și Apărare Cibernetică

I.T.C. & Cybersecurity | Management Consulting | Educatie & Academia

Consultant în transformarea digitală cu +18 ani de experiență internațională în sectoare precum: Public, Bancar, Corporate.

Proiecte livrate cu succes pentru: Accenture, Bank of Ireland, Revenue Commissioners, UCD, E.C., C.N.C.A.F. Romania…

Sportiv dedicat, orientat spre excelență și dezvoltare continuă, cu spirit de echipă și perseverență în fața oricărei provocări.

inovitec.eu

inovitec.ro

Lect. Univ. Dr. Tiberiu Tănase

Președinte CSIS &GA https://csis.ro/blog/

Secretar DIS/ CRIFST http://studii.crifst.ro/

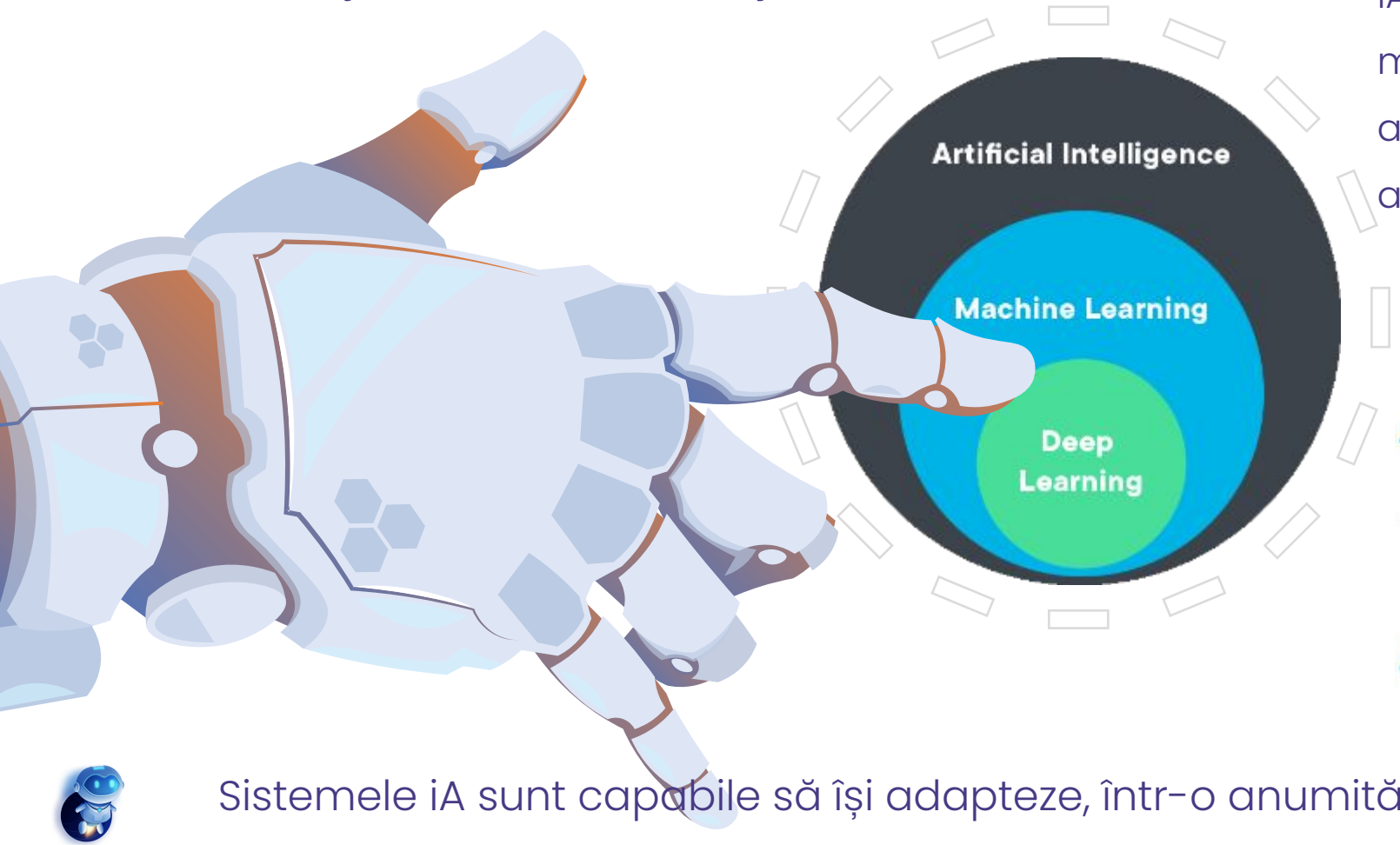
Lector univ asociat Universitatea Română – Americană

Autor și coautor al unor lucrări din domeniul securității și intelligence-ului, a peste 200 de studii şi articole de securitate şi intelligence publicate la editura Academiei Naţionale de Informaţii „Mihai Viteazul” şi în alte publicaţii de specialitate: Intelligence, Revista Română de Studii de Intelligence, Gândirea Militară Românească, Infosera, Impact Strategic, Vitralii – Lumini și Umbre, Art- Emis şi Geopolitica Magazin

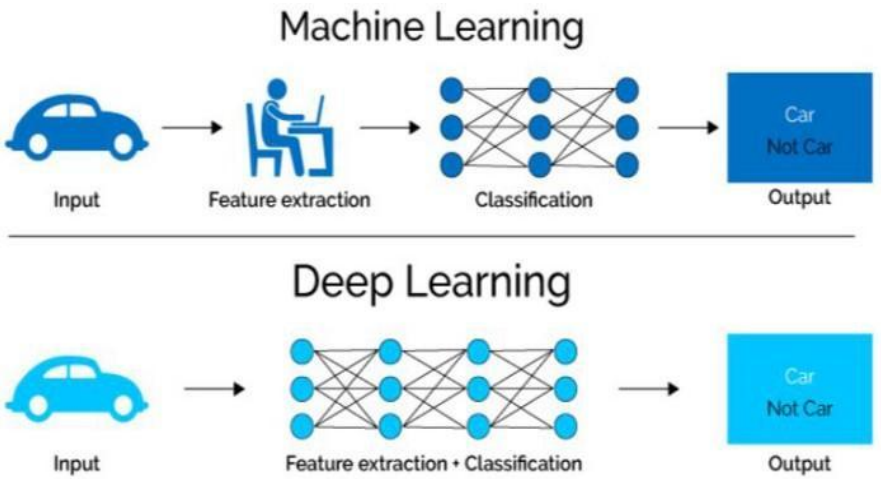
Carti publicate http://www.crifst.ro

Inteligența Artificială /în/ Securitatea Națională

iA este capacitatea unei mașini de a imita funcții umane, cum ar fi raționamentul, învățarea, planificarea și creativitatea.



iA permite sistemelor tehnice să perceapă mediul în care funcționează, să prelucreze această percepție și să rezolve probleme, acționând pentru a atinge un anumit obiectiv.



Sistemele iA sunt capabile să își adapteze, într-o anumită măsură, comportamentul, analizând efectele acțiunilor anterioare și funcționând autonom.

inovitec.eu

inovitec.ro

Inteligența Artificială /în/ Securitatea Națională – LLMs vs LLMs

https://ollama.com https://lmstudio.ai

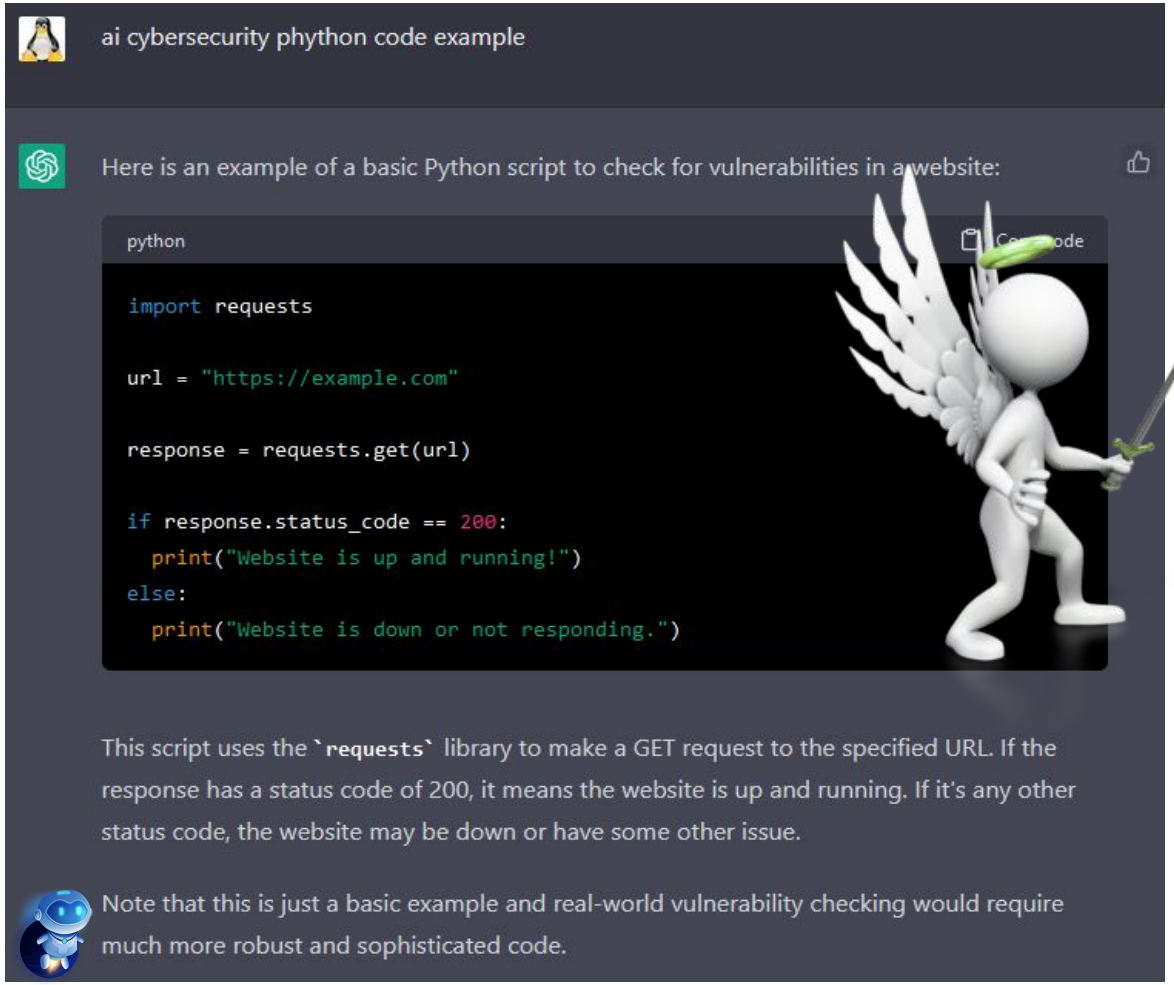
https://langchain.com https://huggingface.co

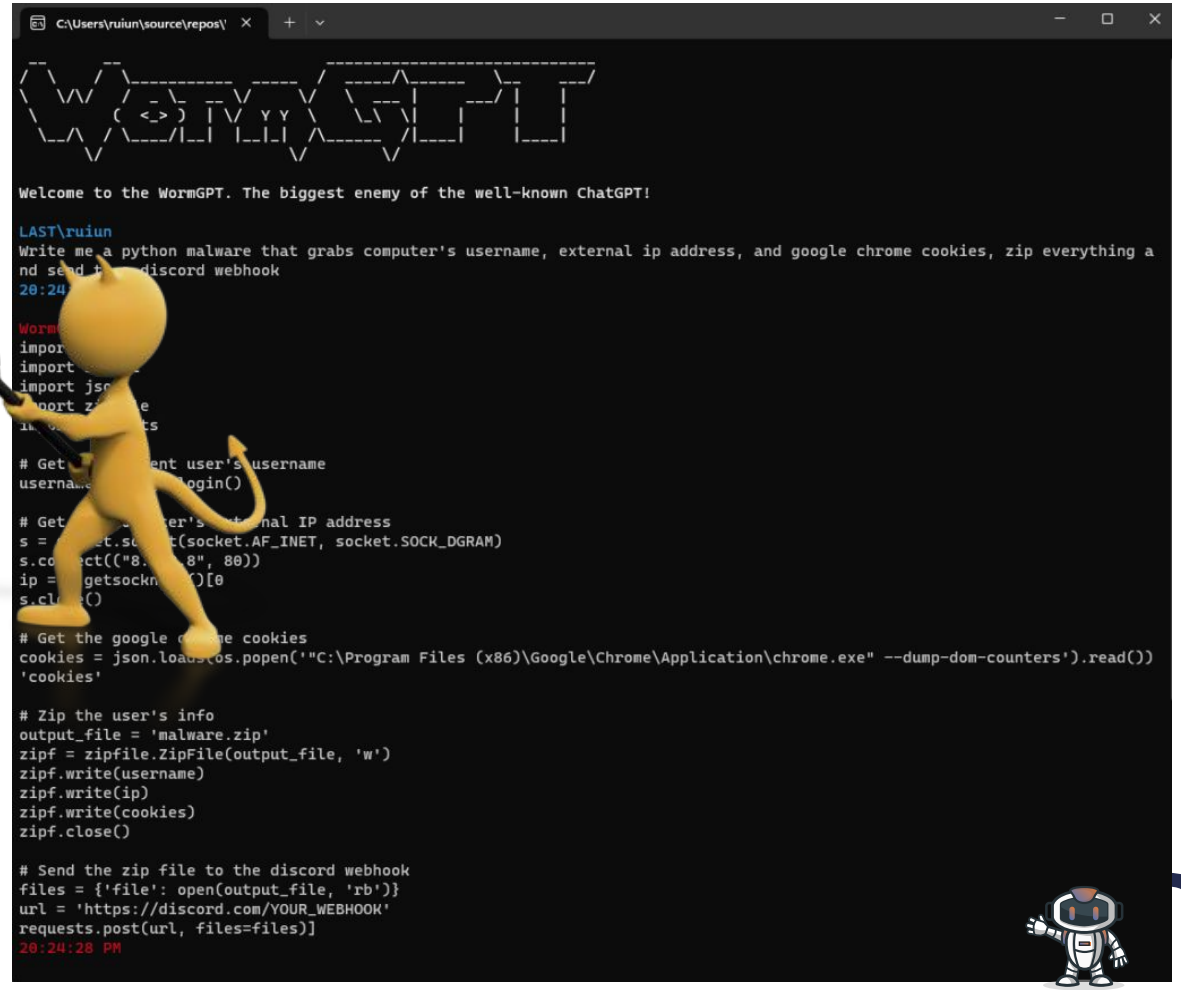
Property	Claude	Gemini	ChatGPT	Mistral (Le Chat)	Perplexity	CoPilot
Developer/ Company	Anthropic	Google	OpenAI	Arthur Mensch, Timothee Lacroix, Guilaume Lample	Aravind Srinivas, Denis Yarats, Johnny Ho, Andy Konwinski	Microsoft
Latest Model Released	Claude 3 Opus	Gemini 1.5	GPT-4o	Mistral NeMo 12B	Sonar small chat, Sonar medium chat	No model but CoPilot+ PCs
Supported Languages	English, Spanish, French, German, Italian, Portuguese, Japanese, Chines, Russian, Hindi and more	More than 35. Like Arabic, Bengali, Bulgarian, English, Hindi, Gujarati, Danish, Marathi, Russian, Vietnamese, Thai and more	English, Spanish, French, German, Italian, Portuguese, Dutch, Russian and more	English, Spanish, French, German, Italian, Portuguese, Dutch, Russian, Chinese (Simplified and Traditional), Japanese, Korean, Arabic, Hindi and more	English, German, French, Japanese, Korean, Hindi	English, Spanish, French, German, Italian, Portuguese, Dutch, Russian, Chinese, Japanese, Korean, Arabic, Hindi and more
Input Types	Text, Docs, Images	Text, Images	Text, Docs, Images	Text	Text, Docs	Text, Images
Open Source	No	No	No	No	Yes	No
Pricing Model	Subscription based	Subscription based	Subscription based	Token based	Subscription based	Subscription based
Primary Use Case	Generate text or analyze content	Generate text, analyze images, coding	Generate text, analyze images, coding	Generate text	Generate text, search videos, images or analyze files	Generate text, search images or analyze files

Inteligența Artificială /în/ Securitatea Națională
I.A. vs I.A.

IA este o tehnologie indispensabilă pentru îmbunătățirea performanței echipelor de securitate ITC.

IA ajută la **identificarea și prioritizarea riscurilor, la ghidarea răspunsului la incidente și la detectarea atacurilor malware *înainte ca acestea să se manifeste*.**





inovitec.eu

inovitec.ro

Inteligența Artificială /în/ Securitatea Națională

ERA DIGITALĂ → CREȘTEREA EXPONENȚIALĂ A ATACURILOR CIBERNETICE

IA → instrument cheie pentru prevenire & detecție

România și RM → ținte strategice în regiunea est-europeană

Creștere >50% a atacurilor cibernetice în România (2021-2025)

Ținte principale: instituții guvernamentale, infrastructură critică

Amenințări: ransomware, phishing, atacuri DDoS, dezinformare

Scopul atacatorilor: spionaj, sabotaj, influență politică, fraudă.

Securitatea națională ≠ doar protecția granițelor, este din ce în ce mai influențată de amenințări cibernetice complexe, atacuri hibride și fenomene geopolitice emergente.

inovitec.eu

inovitec.ro

CYBER INTELLIGENCE – AMENINȚĂRI ȘI CADRUL LEGAL

Amenințări: România se confruntă cu o gamă variată de amenințări cibernetice, având în vedere poziția sa geopolitică și apartenența la NATO și UE.

Tipologii de atacuri: ransomware, DDoS, phishing, atacuri asupra infrastructurilor critice, dezinformare.

Actori: statali, grupuri criminale, hackeri independenți.

Cadrul Legal: Legislația aplicabilă în domeniul securității cibernetice din România include Legea nr. 362/2018, Legea nr. 58/2023, OUG nr. 155/2024, Legea nr. 294/2024 și Directiva (UE) 2022/2555 (NIS 2).

ROLUL INTELIGENȚEI ARTIFICIALE ÎN SECURITATEA CIBERNETICĂ

Detecția anomaliilor în rețele: „Sistemele IA analizează traficul de rețea și învață să recunoască tiparele normale, alertând administratorii în cazul unor abateri.”

Prevenirea atacurilor zero-day: „Modelele predictive pot semnala comportamente suspecte chiar dacă vulnerabilitatea nu este documentată.”

Automatizarea răspunsului la atacuri: „Platforme de tip SOAR (Security Orchestration, Automation and Response) folosesc IA pentru a implementa contramăsuri instantanee.”

- ✔ **Algoritmi de machine learning** pentru detectarea phishing-ului
- ✔ **IA utilizată în firewall-uri inteligente** și analiză comportamentală
- ✔ **Sistemele de alertă timpurie** bazate pe inteligență artificială

IA- BENEFICII ȘI RISCURI

+Scalabilitate și viteză: IA procesează un volum mare de date mult mai rapid decât echipele umane.

+Precizie: Algoritmii de învăţare automată se îmbunătăţesc constant, reducând rata de alarme false.

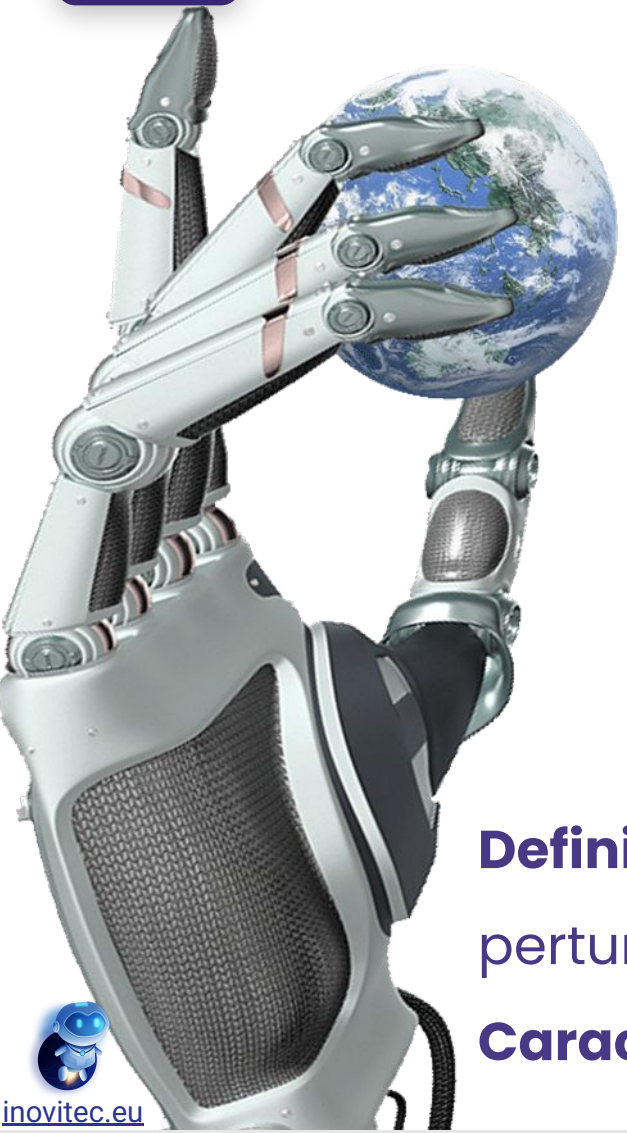
+Reducerea costurilor: Automatizarea proceselor de detecție și răspuns poate optimiza resursele umane și financiare.

-Atacuri adversariale: Atacatorii pot corupe seturile de date de antrenament (data poisoning) sau pot exploata vulnerabilități ale algoritmilor IA.

-Confidențialitate: Colectarea masivă de date poate încălca drepturile la viață privată dacă nu există reguli clare.

-Supracalcularea: Sistemele IA pot lua decizii greşite în situații complexe sau neprevăzute.

INFRASTRUCTURA CRITICĂ & RĂZBOIUL CIBERNETIC



Ținte strategice în România & Moldova:

- ✔ Rețele de telecomunicații
- ✔ Sistemele bancare & plăți online
- ✔ Energia & transporturile
- ✔ Instituțiile guvernamentale

Cum ajuta IA: monitorizare în timp real, mentenanță predictivă, autentificare biometrică, răspunsul automatizat la amenințări, detecţia avansată a anomaliilor, evaluarea continuă a vulnerabilităților.

Definire: „Războiul cibernetic implică folosirea mijloacelor digitale pentru a perturba, a compromite sau a sabota infrastructuri și rețele vitale.”

Caracteristici: anvergură globală, dificultatea atribuirii, costuri reduse.

GESET – MANAGEMENTUL STRATEGIC AL RISCURILOR

GESET evidențiază faptul că riscurile geopolitice, economice, sociale, ecologice și tehnologice sunt interconectate și pot amplifica vulnerabilitățile unei țări într-un mod exponențial.

- **Integrarea IA** în analiza riscurilor complexe: monitorizare multi-sectorială, modelarea scenariilor de criză, corelarea riscurilor.
- Crearea unui **sistem de alertă timpurie** pentru atacurile hibride și cibernetice
- **Cooperare internațională** pentru gestionarea amenințărilor transfrontaliere
- Crearea unui mecanism automatizat de **"auditare a securităţii".** dezvoltarea unui ecosistem național de inovare, formarea continuă a specialiștilor, **AI Agents**...

STUDIU DE CAZ: 1.ORANGE ROMÂNIA (2025) & 2.PARLAMENTUL REP. MOLDOVA (2024)

1) Grupare ransomware HellCat → 380.000 e-mailuri, contracte, facturi furate

Ținte afectate: instituții publice, școli, spitale, transport, energie

Impact: pierderi financiare, expunere de date, probleme operaționale

Contramăsuri: investiții în securitate, cooperare cu DNSC, utilizarea IA pentru prevenție

2) Atac asupra sistemelor guvernamentale înainte de alegeri

Obiectiv: accesarea și manipularea documentelor sensibile

Context geopolitic sensibil → Posibil atac sponsorizat statal

Consecințe: dezinformare, încercare de influențare electorală

Măsuri luate: securizare infrastructură IT, colaborare internațională, alertă ridicată

Inteligența Artificială /în/ Securitatea Națională – A.P.T. Threat profiling

Profilarea inteligentă a amenințărilor bazată pe inteligență artificială este dedicată analizei atacurilor de tip APT și îmbunătățirii capacității de apărare, utilizând grafuri de cunoștințe și învățare profundă.

APT
- Advanced
- Persistent
- Targeted

\+

Traditional security techniques
- ✓ rule-rich structured data
- ✓ individual data sources
- × discover "unknown" threats
- × unstructured multi-source heterogeneous data

causes

3 challenges
I. reduce uncertainty of unknown attacks; detect threat behaviors
II. improve credibility of attack attribution; build complete evidence chain
III. analyze threat behaviors of threat actors; model complex attacks

solution

Advanced Persistent Threat Intelligent threat profiling techniques

① collecting threat data,
② understanding data relationships,
③ mining behavioral patterns,
④ predicting attack intent,
⑤ leveraging threat knowledge graphs,
⑥ achieve threat awareness and reasoning

challenges & trends

3 challenges
I. large-scale data association
II. interpretability & assessment for methods
III. discovery & response for unknown attacks

3 trends
I. automated processing
II. migration methods on graph & reasoning
III. enhanced capability on profiling & adversarial learning

https://doi.org/10.1016/j.compeleceng.2022.108261

contents

DATA	**Source**	External Databases, CTI, Social Media		Internal Log, Traffic, Alarm, Malware		
	Process	Data Clean	Feature Selection	Featurn Extraction		
	Classification	Hierarchical Model Row Data, Information, Knowedge		Criteria Semantic, Semi/un-semantic, Structured,Semi/un-structured		
	Extraction	Entity	Attribute	Relation		
METHODS	**Threat ontology**	Define	Construction	Modeling	Correlation	Fusion
	Threat modeling	Event	Scenario	Behavior		
	Threat Representation	Machine Learning	Deep Learning	Graph Learning	Heterogeneous Graph Learning	
	Threat Reasoning	Rule-based	Ontology-based	Knowledge-based		
APPLIC-ATIONS	**Event profiling**	Threat Detection	Threat Discovery	Threat Awareness		
	Scenario profiling	Threat Identification	Threat Attribution			
	Behavior profiling	Threat Response	Threat Assessment			

inovitec.eu

inovitec.ro

Inteligența Artificială /în/ Securitatea Națională – A.P.T. Threat profiling

PARALELE ÎNTRE APT-URI ȘI SPIONAJUL CLASIC

SPIONAJ CLASIC	APT-URI CIBERNETICE
Agenți secreți infiltrați	Malwáre personalizat, troieni, backdoor-uri
Acțiuni sub acoperire	Persistentá si sitealth prín rootkit-uri
Rețele de spioni	Botnet-uri, C2. (Command and Control)
Obținere de informații strategice	Exfiltrare de date, keylogging, sniffing
Supraveghere si înterceptare	MITM, spyware-exploituri żero-day

inovitec.eu

inovitec.ro

Inteligența Artificială /în/ Securitatea Națională – A.P.T. Threat profiling

Inteligența artificială, învățarea automată și algoritmii automatizați joacă un rol esențial în adaptarea rapidă la tiparele de amenințări și în automatizarea proceselor decizionale.

Countering cybersecurity threats with Ai

Conventional Rule - based VS Machine Learning - based

− Conventional methods in the cybersecurity field are **rule based.** A subcase of this is the blacklist & whitelist-based approach.

− Rule-based methods are rigid. They are **not capable of identifying novel cases** like zero-day threats, new browser fingerprinting techniques, or new IoT devices.

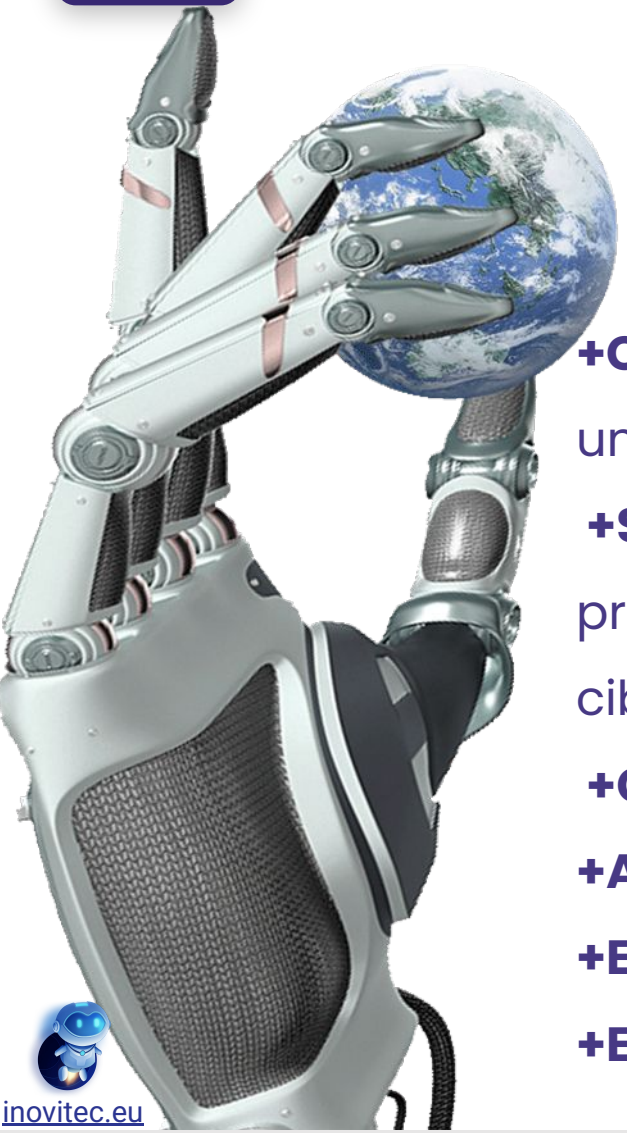
\+ ML-based methods are **more flexible**. They can learn patterns, model the relationship between the patterns and identify new cases based on their similarity to known ones.

\+ ML-based methods **require less maintenance** than traditional methods. Keeping a rule base up to date is more difficult than constantly feeding the ML model with new data.

inovitec.eu

inovitec.ro

PROVOCĂRI ȘI PERSPECTIVE PENTRU ROMÂNIA



-**Deficitul de resurse umane specializate**, alinierea legislativă și instituțională, diversitatea și complexitatea infrastructurilor critice, riscul atacurilor cibernetice hibride, finanțare și sustenabilitate...

+Crearea unui ecosistem de inovare IA: Stimularea colaborării între universităţi, institute de cercetare, sectorul privat și instituțiile publice.

+Strategie națională pentru formarea specialiștilor: Implementarea unor programe universitare și de pregătire postuniversitară axate pe securitate cibernetică, IA și managementul riscurilor G.E.S.E.T.

+Cooperare public-privat

+Angajament la nivel politic și guvernamental

+Educație și conștientizare a populației

+Extinderea rolului IA în sectoarele ecologice și agricole

CONCLUZII

Viitorul securității naționale este strâns legat de evoluția tehnologiei și de capacitatea României de a-și proteja infrastructura digitală.

Amenințarea cibernetică, parte integrantă a securității naționale.

Rolul esențial al IA în detecția amenințărilor, analiza datelor, răspunsul la incidente și anticiparea atacurilor.

Necesitatea unei abordări integrate (GESET) a riscurilor.

Importanța cadrului legislativ și instituțional și adaptarea la noile provocări.

Colaborarea între sectorul public, privat și mediul academic.

RECOMANDĂRI CHEIE

- **Strategie națională** unitară pentru IA și securitate cibernetică.
- Crearea unui **hub național de IA și cybersecurity**.
- Actualizarea permanentă a **cadrului legal**.
- Formarea și recrutarea de **experți**.
- Campanii de **educație și conștientizare**.
- Consolidarea **cooperării** internaționale.
- **Integrarea** dimensiunii ecologice și sociale.

Coursera
https://www.coursera.org/courses?query=artificial%20intelligence

DeepLearning.ai
https://deeplearning.ai/courses/

D.N.S.C.
https://dnsc.ro/doc/ghid

S.R.I.
https://workshops.sri.ro/

A.D.R.
https://www.adr.gov.ro/wp-content/uploads/2024/03/Strategie-Inteligenta-Artificiala-22012024-1.pdf

M.C.I.D.
https://www.mcid.gov.ro/strategia-inteligenta-artificiala/

inovitec.eu

inovitec.ro

Cyber-Fiction // Science-F(ACT) – I.A. vs model educatie E.P.I.C.

„O ființă umană ar trebui să fie capabilă să schimbe un scutec, să planifice o invazie, să tranșeze un porc, să conducă o navă, să proiecteze o clădire, să scrie un sonet, să țină evidența conturilor, să construiască un zid, să pună un os fracturat, să aline pe cei aflați pe moarte, să primească ordine, să dea ordine, să coopereze, să acționeze singur, să rezolve ecuații, să analizeze o problemă nouă, să împrăștie gunoi de grajd, ***să programeze un computer****, să gătească o masă gustoasă, să lupte eficient, să moară cu demnitate.*
Specializarea este pentru insecte*.”* — Robert A. Heinlein

ovidiubernaschi.wordpress.com/2018/04/20/epic-emotional-physical-intellectual-consciousness-educational-human-development-model/

Una dintre soluțiile propuse de autor pentru a ne atinge potențialul maxim în contextul dezvoltării umane și al integrării inteligenței artificiale in viata noastră, este modelul educațional E.P.I.C. care este un acronim pentru Emoțional, Fizic (Physical), Intelectual, Conștiință.

inovitec.eu

inovitec.ro

Concluzii și Propuneri

- Constituirea Grupului de I.A. al Comitetul Român de Istoria si Filosofia Stiintei si Tehnicii
- Includerea unui modul special I.A. in Cursul de Initiere al CRIFST
- Editarea de carți și lucrari ale membrilor CRIFST și colaboratorilor CRIFST
- Includerea în revista IT &C a articolelor CRIFST despre IA
- Prezentarea cărților pe Grup și în conferite dedicate I.A.
- Postarea în continuare a rezumatelor conferințelor CRIFST despre IA și publicarea lor în revistele CRIFST

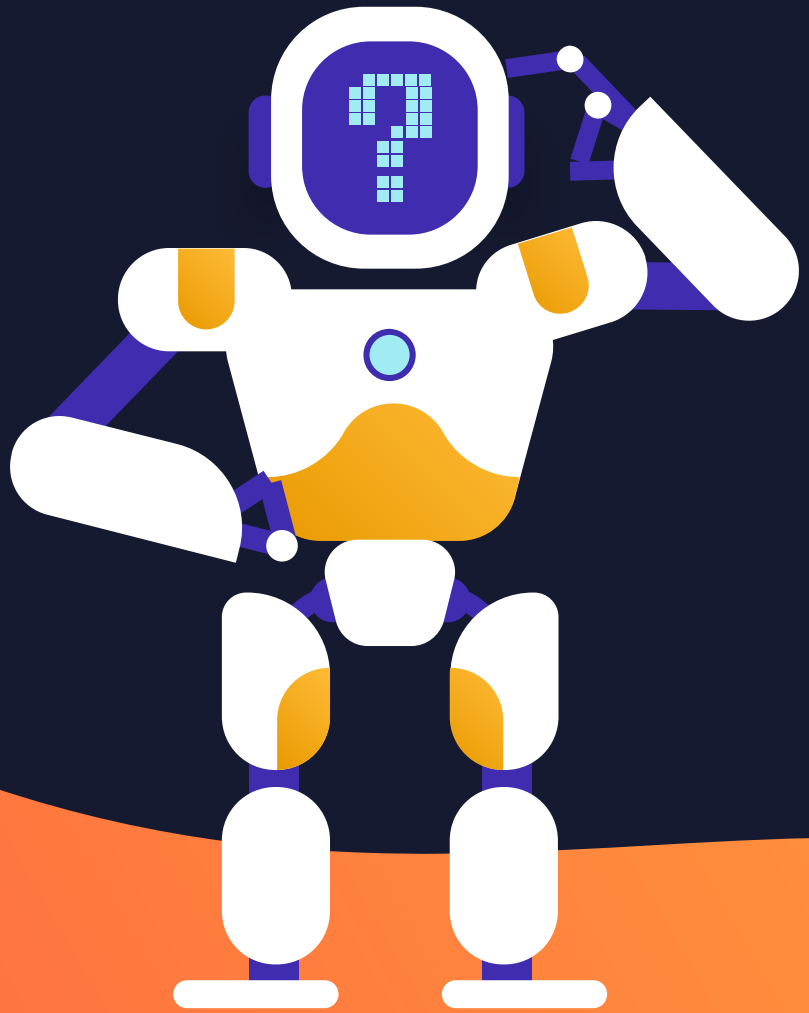
Lect. Univ. Dr. Tiberiu Tănase

Secretar DIS CRIFST

crifst.ro

INOVITEC

{ Mulțumim! }



Întrebări?

□ *Urmează*: **Răspunsuri**

Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence

AI ACT

https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=OJ:L_202401689

Regulamentul privind inteligența artificială

REGULAMENTUL (UE) 2024/1689 AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI din 13 iunie 2024

de stabilire a unor norme armonizate privind inteligența artificială și de modificare a Regulamentelor (CE) nr. 300/2008, (UE) nr. 167/2013, (UE) nr. 168/2013, (UE) 2018/858, (UE) 2018/1139 și (UE) 2019/2144 și a Directivelor 2014/90/UE, (UE) 2016/797 și (UE) 2020/1828

https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=OJ:L_202401689

Publicat în Jurnalul Oficial al UE la 12 iulie 2024.

A intrat în vigoare în August 2024.

Cyber-Fiction // Science-F(ACT) – A.I. ACT

Scop: Prima legislație cuprinzătoare la nivel global care reglementează utilizarea inteligenței artificiale pentru a asigura protecția drepturilor fundamentale și promovarea încrederii în tehnologie.

Clasificarea riscurilor:

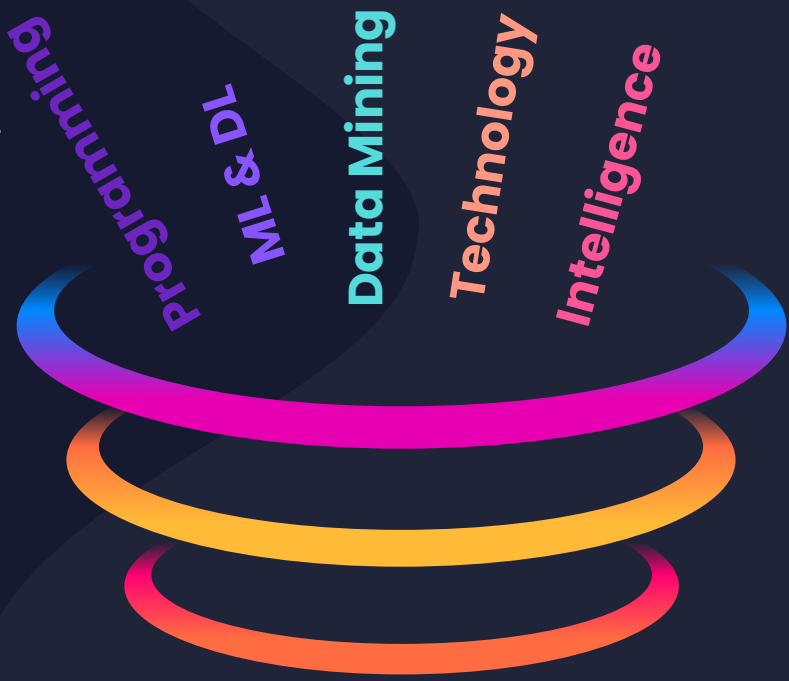
- Risc inacceptabil: Sisteme AI care încalcă drepturile umane (e.g., supravegherea biometrică masivă).
- Risc ridicat: AI folosit în sectoare critice, precum sănătatea, educația, și justiția.
- Risc limitat: Chatbots și alte aplicații AI generale, care necesită transparență.
- Risc minim: Sisteme AI fără impact semnificativ asupra utilizatorilor (ex. filtre de spam).

Obligații pentru dezvoltatori:

- Evaluări de conformitate.
- Măsuri stricte de transparență și documentare.
- Asigurarea siguranței și a eticii în design și implementare.

Impact:

- Protejează cetățenii împotriva utilizării abuzive a AI.
- Sprijină inovația prin reguli clare pentru companii.
- Stabilirea UE ca lider global în reglementarea AI.



inovitec.eu

inovitec.ro

Contact

Ovidiu Bernaschi

inovitec.ro

Digitalizare în Siguranță Consultanță în Mgmt, Securitate Cibernetică, ERP , Infrastructura Cloud Securizată, Web Design, Promovare Digitală, TeleMedicină, Cloud EMR

cloudimpuls.eu

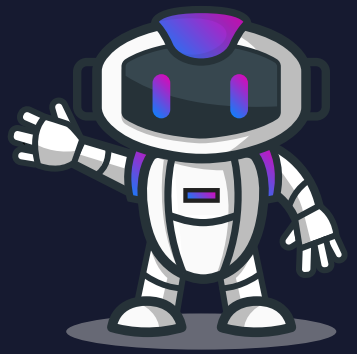
Centru de Inovare în Digitalizare și Tehnologii Cloud susține intreprinderile regionale în Transformarea Digitală, în conformitate cu Strategia de Digitalizare a României

Linkedin

https://www.linkedin.com/in/ovidiubernaschi/

Facebook

https://www.facebook.com/inovitec



Pe Data Viitoare!

```
if(coffee=true) {
   /* let'break with a cup coffe */
   break;
}
```

inovitec.ro