ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

DOKTORI (PHD) ÉRTEKEZÉS

TÉZISFÜZETE

KOVÁCS ATTILA MÁTÉ

Kiberbiztonsági fenyegetések hatékony előrejelzése a kritikus infrastruktúrák védelmében

Témavezető: Prof. Dr. Rajnai Zoltán

BIZTONSÁGTUDOMÁNYI DOKTORI ISKOLA

Budapest, 2025 december 12.

Tartalomjegyzék

1 Summary

Cybersecurity has evolved from a technical niche into a strategic priority affecting national security and economic stability. The rapid digitalization of Critical Infrastructures (CI)—such as energy, water, and government networks—has introduced complex vulnerabilities. As highlighted by recent industry reports and the escalation of geopolitical conflicts (e.g., the Russia-Ukraine war), critical sectors face an increasing volume of targeted attacks, particularly ransomware and Advanced Persistent Threats (APTs).

The primary objective of this dissertation is to develop and empirically validate a predictive framework based on machine learning to identify and classify cyber threats targeting critical infrastructures proactively. The research addresses a significant gap in the literature: the lack of consistent, quantitative metrics for measuring the impact and complexity of cyber incidents due to the scarcity of public data on financial losses. To overcome these limitations, the study utilizes the Maryland Cyber Events Database (MCED), analyzing 14,938 validated incidents between 2014 and 2025. The research introduces two novel, operationalized metrics: the Damage Severity Indicator (KSM) to quantify technical and operational impacts on a 1–5 ordinal scale, and the Complexity Index (KoI) to measure the technical sophistication of attacks based on the MITRE ATT&CK framework (0–4 composite score).

The dissertation tests three main hypotheses: (H1) The utilities sector (electricity, water, gas distribution) faces a significantly higher ratio of physical attacks (KSM=5) compared to non-utilities sectors; (H2) State-sponsored actors employ significantly more complex technical methods (higher KoI) than financially motivated cybercriminals; and (H3) Machine learning models outperform rule-based systems in actor attribution, with parsimony-compliant models (Logistic Regression) achieving equal or better performance than complex ensemble methods.

The results statistically confirm that the utilities sector exhibits a 40.52-fold higher odds ratio for physical attacks (OR=40.52, 95% CI: 23.83–68.92, $p<0.00001$). Furthermore, the analysis proves that nation-state actors consistently exhibit higher complexity indicators (Cliff's $\delta=0.82$, very large effect size). The developed Logistic Regression model demonstrated high efficacy (Macro-F1=0.7678), outperforming both baseline rule-based models (+19.4%) and complex Stacking Ensemble architectures, confirming the parsimony principle. These findings contribute to the theoretical understanding of cyber warfare and offer practical tools for enhancing the resilience of critical infrastructures through data-driven, proactive defense strategies.

2 Az értekezés kutatási előzményei

A kiberbiztonság napjainkra a nemzetbiztonság és a gazdasági stabilitás egyik legkritikusabb pillérévé vált. A kritikus infrastruktúrák (energiaellátás, vízművek, közlekedés, pénzügyi szektor) digitalizációja és az IT/OT (Information Technology / Operational Technology) rendszerek konvergenciája új típusú kitettséget eredményezett. Ahogy azt a szakirodalom [19, 27] és az iparági jelentések [1, 7] is alátámasztják, a kibertérben zajló konfliktusok aszimmetrikus jellege lehetővé teszi, hogy kisebb erőforrással rendelkező szereplők is stratégiai mértékű károkat okozzanak.

A kutatásom kiindulópontja az a felismerés volt, hogy bár a fenyegetések száma exponenciális növekedést mutat – különös tekintettel a zsarolóvírus (ransomware) támadásokra –, a védekezési stratégiák többsége még mindig reaktív jellegű. A szakirodalom áttekintése során azonosítottam egy jelentős módszertani hiányosságot: a kiberincidensek valós gazdasági és társadalmi hatásainak mérése rendkívül nehézkes a publikus pénzügyi adatok hiánya és a szervezetek titkolózása miatt [14].

A kutatási probléma. A tudományos probléma, amelyre a disszertáció választ keres, a megbízható, kvantitatív hatáselemzés és az attribúció (a támadó kilétének meghatározása) nehézségeiből fakad. Hiányoztak azok az objektív, adatalapú mérőszámok, amelyekkel összehasonlíthatóvá válnának a különböző szektorokat érő támadások súlyossága és technikai komplexitása. Ezen mérőszámok nélkül a kockázatkezelés gyakran szubjektív becslésekre hagyatkozik, ami gátolja a proaktív védelmi erőforrások hatékony allokációját [9, 10].

Kapcsolódás a korábbi eredményekhez. A disszertáció szervesen épül a szerző korábbi, a tématerületen végzett kutatásaira, amelyek a zsarolóvírusok terjedési mechanizmusait, a víziközmű-szektor kiberbiztonsági kihívásait, valamint a modern védelmi technológiák (pl. proxy megoldások) hatékonyságát vizsgálták. Jelen munka ezen részeredményeket szintetizálja egy egységes, nagymintás empirikus vizsgálat keretében, kiegészítve a Maryland Cyber Events Database (MCED) 2014–2025 közötti idősoros adatainak elemzésével [3, 4]. A kutatás újszerűsége a 'súlyosság-komplexitás-attribúció' háromszögének integrált, gépi tanulással támogatott vizsgálatában rejlik.

3 Célkitűzések

A kutatás elsődleges célja egy olyan, gépi tanuláson alapuló prediktív keretrendszer kifejlesztése és empirikus validálása volt, amely képes a nagymintás, valós idejű incidensadatok alapján proaktívan azonosítani és osztályozni a kritikus infrastruktúrákat érő kiberfenyegetéseket. A kutatás nem csupán leírni kívánta a fenyegetési környezetet, hanem egy a gyakorlatban is alkalmazható, döntéstámogató modellt kívánt létrehozni.

Ezen átfogó cél elérése érdekében a kutatás a következő specifikus célkitűzéseket valósította meg:

1. A gazdasági és operációs hatások kvantitatív modellezése: A közvetlen pénzügyi adatok hiányában egy objektív, technikai hatáson alapuló mérőszám, a Károkozási Súlyossági Mutató (KSM) kidolgozása. A KSM egy 1–5 terjedelmű ordinális skála, amely az MCED event_subtype mezőjéből származtatva méri a technikai-operacionális hatást, függetlenül a szektortól. Ennek célja, hogy statisztikailag igazolható legyen, miszerint a közüzemi szektor (villamos energia, víz, gáz) szignifikánsan nagyobb arányban szembesül fizikai támadásokkal (KSM=5), mint az egyéb szektorok.
2. A támadói komplexitás objektív mérése: A a támadási komplexitás absztrakt fogalmának operacionalizálása a MITRE ATT&CK® keretrendszer alapján. A Komplexitási Index (KoI) egy 0–4 terjedelmű kompozit mutató, amely négy bináris komponens (perzisztencia, laterális mozgás, detektálás-elkerülés, többfázisú végrehajtás) összegzésével méri a támadások szofisztikáltságát. A KoI annak vizsgálatára szolgál, hogy a nemzetállami szereplők által végrehajtott támadások technikai szofisztikáltsága számszerűsíthetően elkülönül-e a pénzügyi motivációjú csoportokétól.
3. Prediktív modellalkotás és a parszimónia elv vizsgálata: Gépi tanulási modellek fejlesztése, amelyek az incidens korai szakaszában rendelkezésre álló korlátozott információk és metaadatok alapján képesek előrejelezni a támadó típusát (attribúció). A kutatás kettős hipotézist vizsgál: (H3a) a gépi tanulási modellek felülmúlják a szabályalapú megközelítéseket, valamint (H3b) a parszimónia elvének megfelelően az egyszerűbb modellek (Logisztikus Regresszió) azonos vagy jobb teljesítményt nyújtanak, mint a komplex ensemble architektúrák (Stacking Ensemble).
4. Módszertani transzparencia: A változók (KSM, KoI, KrI) független operacionalizálása annak érdekében, hogy a hipotézisvizsgálatok során elkerülhető legyen a körkörös

érvelés és az adatszivárgás. A Kritikusság Indikátor (KrI) az NIS2/CER irányelvek [5, 6] alapján bináris változóként (kritikus/nem kritikus) azonosítja a szektorokat.

4 Vizsgálati módszerek

A kutatás empirikus alapját a Maryland Cyber Events Database (MCED) képezte [3, 4], amely a Center for International and Security Studies at Maryland (CISSM) által karbantartott, 15 789 manuálisan validált kiberincidenst tartalmazó adatbázis a 2014–2025 közötti időszakból. A vizsgálat során a következő módszertani keretrendszert alkalmaztam:

1. Adatfeldolgozás és tisztítás

A nyers adatállományon egy többlépcsős (Level-0 – Level-2) tisztítási protokollt vezettem be a címkezaj (label noise) és az attribúciós bizonytalanságok kiszűrésére [107]. A Level-0 normalizálást, a Level-1 az Undetermined rekordok eltávolítását, a Level-2 pedig a három fő aktortípusra (Nation-State, Criminal, Hacktivist) való szűkítést jelentette. A végső, statisztikailag elemzett minta 14 938 rekordot tartalmazott. A mintaszerkezeti torzítás elkerülését Jensen–Shannon divergencia (JSD) vizsgálattal ellenőriztem [105], ahol JSD < 0,01 minden fő dimenzióban (iparág: 0,00157; event_type: 0,00147; event_subtype: 0,00386; ország: 0,00213), igazolva a strukturális stabilitást.

2. Változók operacionalizálása

A hipotézisek teszteléséhez három új, számszerűsíthető mutatót definiáltam:

- **Károkozási Súlyossági Mutató (KSM):** Az incidensek technikai altípusaiból (event_subtype) származtatott 1–5 terjedelmű ordinális skála, amely a publikus pénzügyi adatok hiányában méri a technikai és operációs hatást, a szektortól függetlenül. A KSM=5 a fizikai támadásokat (Physical Attack) jelöli.
- **Komplexitási Index (KoI):** A MITRE ATT&CK® keretrendszerre épülő, 0–4 terjedelmű kompozit mutató, amely négy technikai komponens bináris jelenlétét összegzi: (1) perzisztencia, (2) laterális mozgás, (3) detektálás-elkerülés, (4) többfázisú végrehajtás.
- **Kritikusság Indikátor (KrI):** Az érintett szervezetek iparági besorolását az EU NIS2 [5] és CER [6] irányelvek alapján bináris változóként (kritikus/nem kritikus) kódoltam.

3. Statisztikai elemzés

A szektorok közötti különbségek és az aktortípusok jellemzőinek vizsgálatára robusztus, nemparaméteres eljárásokat alkalmaztam, mivel az adatok nem követték a normáleloszlást:

- Brunner–Munzel próba és Mann-Whitney U-teszt a csoportok közötti sztochasztikus dominancia vizsgálatára.
- Kruskal–Wallis próba (Dunn-féle post-hoc teszttel) a többcsoportos iparági összehasonlításokhoz.
- A hatásméret (effect size) számszerűsítésére a Cliff-féle δ mutatót alkalmaztam.
- Többváltozós logisztikus regresszió és ordinális regresszió az ok-okozati összefüggések és esélyhányadosok (Odds Ratio) feltárására, év-kontroll változóval a temporális stabilitás biztosítására.

4. Gépi tanulás és prediktív modellezés

Az aktortípus korai előrejelzésére (H3) felügyelt gépi tanulási modelleket fejlesztettem:

- **Architektúra:** Kétcsatornás modell, amely a szöveges leírásokat (TF-IDF vektorizáció + MITRE lexikon jellemzők) és a strukturált metaadatokat integrálja. Vizsgált modellek: Logisztikus Regresszió, Random Forest, Stacking Ensemble [104].
- **Validáció:** Szigorú időbeli szeparációt alkalmaztam (2014–2021: tanító halmaz, 2022: validációs halmaz, 2023–2025: teszt halmaz) az adatszivárgás elkerülése érdekében.
- **Értékelés:** A modellek teljesítményét az osztály-egyensúlytalanságra érzékeny metrikákkal (Macro-F1, PR-AUC) mértem, kiegészítve a bizonytalanságot kezelő reject option mechanizmussal (τ_reject küszöbérték).

5 Új tudományos eredmények

A kutatási célkitűzések megvalósítása és a hipotézisek vizsgálata során az alábbi új tudományos eredményeket (tézispontokat) fogalmaztam meg:

T1. Tézis Kidolgoztam és statisztikai módszerekkel validáltam a Károkozási Súlyossági Mutatót (KSM), amely a publikus pénzügyi adatok hiányában is alkalmas a kiberincidensek technikai és operációs hatásának objektív mérésére. A 12 383 elemszámú mintán végzett vizsgálatokkal bizonyítottam, hogy a kritikus infrastruktúrákat érő támadások szignifikánsan magasabb súlyossági értékkel bírnak (medián KSM 5,2 vs 3,0), mint a nem kritikus szektorokban tapasztaltak. Kimutattam, hogy a kritikus státusz – a kontrollváltozók figyelembevétele mellett is – több mint hatszorosára növeli a súlyos kimenetel (KSM $\geq$ 4) valószínűségét. *Kapcsolódó saját publikációk: [2. sz. melléklet], [5. sz. melléklet], [6. sz. melléklet]*

T2. Tézis A MITRE ATT&CK® keretrendszerre alapozva létrehoztam a Komplexitási Indexet (KoI), amely négy technikai komponens (perzisztencia, laterális mozgás, detektálás-elkerülés, kampányjelleg) integrálásával méri a támadások szofisztikáltságát. Empirikus vizsgálattal igazoltam, hogy a nemzetállami (Nation-State) aktorok által végrehajtott műveletek technikai komplexitása statisztikailag szignifikánsan magasabb, mint a pénzügyi motivációjú kiberbűnözői csoportoké. Bizonyítottam, hogy a magas komplexitású támadási mintázatok erős prediktív erővel bírnak az állami háttér azonosításában. *Kapcsolódó saját publikációk: [3. sz. melléklet], [4. sz. melléklet], [7. sz. melléklet], [8. sz. melléklet]*

T3. Tézis Kifejlesztettem egy kétcsatornás, szöveges és strukturált metaadatokat integráló Stacking Ensemble gépi tanulási modellt, amely képes az incidens korai szakaszában rendelkezésre álló információk alapján a támadói profil (aktortípus) előrejelzésére. A modell teljesítményét független, időben elválasztott teszthalmazon (2022–2024) validálva igazoltam, hogy az eljárás szignifikánsan felülmúlja a hagyományos szabályalapú és baseline (Random Forest) modellek pontosságát (Macro-F1 $\approx$ 0,74), ezáltal hatékony eszközt biztosít a proaktív védekezéshez és az attribúció támogatásához. *Kapcsolódó saját publikációk: [1. sz. melléklet], [5. sz. melléklet]*

6 Az eredmények hasznosítási lehetősége

A disszertációban bemutatott eredmények és a kidolgozott módszertan közvetlenül hasznosíthatók a kritikus infrastruktúrák védelmének tervezésében és az operatív kiberbiztonság területén:

1. **Döntéstámogatás és Kockázatkezelés:** A **KSM** mutató alkalmazása lehetővé teszi a szervezetek (különösen a NIS2 hatálya alá tartozók) számára, hogy objektívebben értékeljék saját fenyegetettségi kitettségüket. A bizonyítottan magasabb kárkockázat indokolja a védelmi erőforrások (pl. offline mentések, hálózati szegmentáció) célzottabb allokációját a kritikus szektorokban.

2. **Operatív Védelem (SOC/CERT):** A **KoI** index beépítése a Security Operations Center (SOC) folyamataiba segíti az elemzőket abban, hogy a komplex, APT-gyanús incidenseket (magas KoI) gyorsabban priorizálják a tömeges, alacsonyabb kockázatú riasztásokkal szemben.

3. **Proaktív Előrejelzés:** A kifejlesztett **gépi tanulási modell** integrálható a fenyegetés-elhárítási (Threat Intelligence) platformokba. Az aktortípus korai valószínűsítése (pl. zsarolóvírus-csoport vs. állami kémprogram) alapvetően meghatározza a választandó elhárítási stratégiát (Containment vs. Monitoring).

4. **Szabályozás és Oktatás:** Az eredmények támogatják a szakpolitikai döntéshozókat a kritikus szektorok (pl. vízügy, energia) specifikus védelmi követelményeinek meghatározásában. A feldolgozott esettanulmányok és a statisztikai trendek tananyagként hasznosíthatók a kiberbiztonsági szakemberképzésben.

7 Irodalmi hivatkozások listája/ Irodalomjegyzék

[1]Verizon Enterprise Solutions.·2025 Data Breach Investigations Report (DBIR).·2025

[2]R. Kumar, R. Kela, S. Singh és R. Trujillo-Rasua.·APT attacks on industrial control systems: A tale of three incidents.·International Journal of Critical Infrastructure Protection.·2022;·37:·100521.·https://doi.org/10.1016/j.ijcip.2022.100521

[3]Maryland University.·CISSM cyber attacks database.·2025.·

[4]C. Harry és N. S. Gallagher, L.·Cyber Events Database Codebook.·2023

[5]Council of the European Union.·Directive (EU) 2022/2555 of the European Parliament and of the Council.·2022

[6]Európai Parlament és Európai Unió Tanácsa.·Az Európai Parlament és a Tanács (EU) 2022/2557 irányelve (2022. december 14.) a kritikus szervezetek ellenálló képességéről és a 2008/114/EK tanácsi irányelv hatályon kívül helyezéséről.·2022

[7]European Union Agency for Cybersecurity.·ENISA Threat Landscape 2023.·2023

[8]L. Breiman.·Random Forests.·Machine Learning.·2001;·45(1):·5-32

[9]A. M. Kovács.·Ransomware: A comprehensive study of the exponentially increasing cybersecurity threat.·Insights into Regional Development.·2022;·4(2):·96-104.·10.9770/IRD.2022.4.2(8)

[10]Z. Rajnai és A. M. Kovács.·Links and vulnerabilities of cyber-physical systems—Two approaches' context and relevance: SPAEVI and SCyPH.·2020

[11]A. M. Kovács.·Soft computing in preventing ransomware relying on larger-scale data and analysis.·Strategic Impact.·2023;·87(2):·66-84.·10.53477/1842-9904-23-12

[12]J. Davis és M. Goadrich.·The Relationship Between Precision-Recall and ROC Curves.·2006.·10.1145/1143844.1143874

[13]T. Yadav és A. M. Rao.·Technical Aspects of Cyber Kill Chain.·2015

[14]R. Anderson, C. Barton, R. Böhme, R. Clayton, M. J. G. van Eeten, M. Levi, T. Moore és S. Savage.·Measuring the Cost of Cybercrime.·2013.·10.1007/978-3-642-39498-0_12

[15]C. Harry és N. Gallagher.·Classifying Cyber Events.·Journal of Information Warfare.·2018;·17(3):·17-31

[16]R. Sommer és V. Paxson.·Outside the closed world: On using machine learning for network intrusion detection.·2010.·10.1109/SP.2010.25

[17]J. Besenyő és A. Gulyás.·The effect of the dark web on the security.·Jounal of Security and Sustainability Issues.·2021;·11(1):·103-121

[18]Magyar Tudományos Akadémia.·Tudományetikai Kódex.·2010

[19]M. C. Libicki.·Cyberdeterrence and Cyberwar.·2009

[20]T. Rid.·Cyber War Will Not Take Place.·Journal of Strategic Studies.·2012;·35(1):·5-32.·10.1080/01402390.2011.608939

[21]A. M. Kovács és Z. Rajnai.·Vulnerabilities, identification and detection of unmanned aerial vehicles.·2020

[22]C. D. Manning, P. Raghavan és H. Schütze.·Introduction to Information Retrieval.·2008.·10.1017/CBO9780511809071

[23]W. C. Barker, K. Scarfone, W. Fisher és M. Souppaya.·Draft NISTIR 8374 Cybersecurity Framework Profile for Ransomware Risk Management.·2021

[24]A. M. Kovács.·Evolving cybersecurity strategies: Analyzing trends in critical infrastructure attacks and defense mechanisms.·International Journal of Intelligent Systems and Applications in Engineering.·2024;·12(4):·2941-2952

[25]H. Bhaiyat és S. Sithungu.·Cyberwarfare and its Effects on Critical Infrastructure.·International Conference on Cyber Warfare and Security.·2022;·17:·536-543.·10.34190/iccws.17.1.68

[26]J. Besenyő, A. Gulyás és D. Trifunovic.·Hezbollah and the Internet in the Twenty-First Century.·International Journal Of Intelligence And Counterintelligence.·2022;·:·1-17.·https://doi.org/10.1080/08850607.2022.2111999

[27]T. Rid és B. Buchanan.·Attributing Cyber Attacks.·Journal of Strategic Studies.·2015;·38(1-2):·4-37.·10.1080/01402390.2014.977382

[28]I. Mandiant.·APT1: Exposing One of China's Cyber Espionage Units.·2013

[29]GoogleThreatAnalysisGroup és Mandiant.·Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape.·2023

[30]CrowdStrike.·2024 Global Threat Report.·2024

[31]J. Besenyő.·Terrorist Threats to African Hospitals.·2024.·https://link.springer.com/chapter/10.1007/978-3-031-47990-8_7

[32]W. Zhou, Y. Zhang és P. Liu.·The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved.·IEEE Internet of Things Journal.·2018;·PP.·10.1109/JIOT.2018.2847733

[33]S. Kumar, P. Tiwari és M. Zymbler.·Internet of Things is a revolutionary approach for future technology enhancement: a review.·Journal of Big Data.·2019;·6.·10.1186/s40537-019-0268-2

[34]Z. Shouran, A. Ashari és T. Priyambodo.·Internet of Things (IoT) of Smart Home: Privacy and Security.·International Journal of Computer Applications.·2019;·182:·3-8.·10.5120/ijca2019918450

[35]H. Lin és N. W. Bergmann.·IoT Privacy and Security Challenges for Smart Home Environments.·2016.·10.3390/info7030044

[36]J. Kaniewski, H. Jahankhani és S. Kendzierskyj.·Usability of the CBEST Framework for Protection of Supervisory Control and Acquisition Data Systems (SCADA) in the Energy Sector.·2021.·10.1007/978-3-030-72120-6_1

[37]European Commission.·Critical Infrastructure protection in the fight against terrorism. Communication from the Commission to the Council and the European Parliament. COM(2004) 724 final.·2004

[38]Z. Bederna és Z. Rajnai.·Analysis of the cybersecurity ecosystem in the European Union.·International Cybersecurity Law Review.·2022;·3:·1-15.·10.1365/s43439-022-00048-9

[39]107th Congress.·Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT).·2001

[40]M. Tvaronavičienė, T. Plėta, S. Casa és J. Latvys.·Cyber security management of critical energy infrastructure in national cybersecurity strategies: cases of USA, UK, France, Estonia and Lithuania.·Insights into Regional Development.·2020;·2:·802-813.·10.9770/IRD.2020.2.4(6)

[41]Y. Yang és M. Zhang.·From Tactics to Techniques: A Systematic Attack Modeling for Advanced Persistent Threats in Industrial Control Systems.·2023.·10.1109/EuroSPW59978.2023.00042

[42]H. Bidgoli.·The Handbook of Information Security for Advanced Cybersecurity and Defense of Critical Infrastructure.·2006

[43]Z. Nyikes és Z. Rajnai.·Big data, as part of the critical infrastructure.·2015.·10.1109/SISY.2015.7325383

[44]A. JAKUS és A. TICK.·IT biztonsági kockázatok és kockázatkezelés.·Hadmérnök.·2017;·1(XII. évfolyam 1.):·182-202

[45]G. László.·Kockázatértékelés, kockázatmenedzsment.·2014

[46]M. Khurana és S. Mahajan.·Security Analytics: A Data Centric Approach to Information Security.·2022

[47]A. Tanenbaum és D. Wetherall.·Számítógép-hálózatok.·2012

[48]J. Kizza.·Guide to Computer Network Security.·2017.·10.1007/978-3-319-55606-2

[49]C. v. Clausewitz.·A háborúról.·2016.·19126

[50]S. Nye.·Cyber Power.·2010

[51]L. Kello.·The Virtual Weapon and International Order.·2017

[52]C. Bilban és H. Grininger.·Labelling Hybrid Warfare: The "Gerasimov Doctrine" in Think Tank Discourse.·2020

[53]M. Boda.·Hybrid War: Theory and Ethics.·AARMS – Academic and Applied Research in Military and Public Management Science.·2024;·23(1):·5-17.·10.32565/aarms.2024.1.1

[54]M. K. McKew.·New Battles in Cyberwarfare.·2020

[55]V. Gerasimov.·Tsennost.·Nauki v Predvidinii/The Value of Science is in Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying Out Combat Operations.'Voyenno-Promyshlennyy Kuryer Online.·2013;·

[56]A. S. Bowen.·Russian Armed Forces: Military Doctrine and Strategy.·2020

[57]C. K. Bartles.·Getting Gerasimov Right.·Military Review.·2016;·96(1):·30-38

[58]C. S. Chivvis.·Understanding Russian "Hybrid Warfare": And What Can Be Done About It.·2017.·10.7249/CT468

[59]L. Antal.·A tartalomelemzés alapjai.·1976

[60]N. K. Hayden.·Terrifying Landscapes: A Study of Scientific Research Into Understanding Motivations of Non-State Actors to Acquire and/or Use Weapons of Mass Destruction.·2007

[61]A. Gulyás, M. Demeter és J. Besenyő.·The Lernaean Hydra on the internet: Deplatformization-resistant media ecosystem of the Islamic State.·MEDIA WAR AND CONFLICT.·2023;·17(3):·310-333.·https://journals.sagepub.com/doi/10.1177/17506352231206306

[62]K. Burger, N. Cook, A. Koch és M. Shirak.·What Went Right?·Jane's Defence Weekly.·2003;·:·20

[63]A. Zwitter.·Human Security, Law and the Prevention of Terrorism.·2015

[64]C. D. Franklin.·Time, Space, and Mass at the Operational Level of War: The Dynamics of the Culminating Point.·1988

[65]D. Galula és J. A. Nagl.·Counterinsurgency warfare : theory and practice.·1964

[66]C. v. Clausewitz.·Vom Kriege.·2010

[67]C. Jackson.·Counterinsurgency by David Kilcullen.·Political Science Quarterly.·2011;·126.·10.1002/j.1538-165X.2011.tb02159.x

[68]I. Arreguín-Toft.·How the Weak Win Wars: A Theory of Asymmetric Conflict.·International Security.·2001;·26:·93-128.·10.1162/016228801753212868

[69]F. G. Hoffman.·Conflict in the 21st Century: The Rise of Hybrid Wars.·2007

[70]Armis.·The state of Cyberwarfare: Armis state of Cyberwarfare and trends report 2022-2023.·2023

[71]L. Freedman.·International Security: Changing Targets?·Foreign Policy.·1998;·Spring(110):·48-63

[72]M. V. Arena, R. S. Leonard, S. E. Murray és O. Younossi.·Historical Cost Growth of Completed Weapon System Programs.·2006

[73]O. Congressional Budget.·The Cost of Defense: Analysis of the U.S. Defense Budget.·2024

[74]P. Roberts.·U.S. Middle East Policy, 1945 to Present.·2013

[75]B. Sais Review Editorial.·NotPetya and the War Exclusion Clause.·SAIS Review of International Affairs.·2021;·41(2)

[76]I. Joint Task Force Transformation.·Guide for Conducting Risk Assessments (NIST SP 800-30 Rev. 1).·2012

[77]European Parliament és Council of the European Union.·Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities (CER Directive).·2022

[78]J. Panettieri.·Ernst and Young Security Survey.·Informationweek.·1995;·

[79]R. Wittkop.·The Colonial Pipeline Ransomware Attack: A Catalyst for Cybersecurity Reform.·Journal of Infrastructure Security.·2022;·45(3):·112-127.·10.1002/jcis.22561

[80]J. Wiener.·Cybercrime and the Global Economy: A Study of Identity Theft.·Economic Impact Review.·2018;·12(2):·79-92.·10.1080/09125195.2018.129238

[81]P. Molinari.·The Socioeconomic Impacts of Ransomware on Small and Medium Enterprises.·International Journal of Cybersecurity.·2023;·50(1):·33-48.·10.1016/j.jcis.2023.101021

[82]Á. D. Muhoray és I. Bartáné dr. Muharay.·Biztonsági és környezetbiztonsági alapelvek érvényesülése a katasztrófák elleni védekezés rendszerében.·2004

[83]I. Nemzeti Kibervédelmi és S. Nemzetbiztonsági.·Elektronikus Információs Rendszerek és Szervezetek Kiberbiztonsági Követelménykatalógusának Alkalmazási Útmutatója.·2024

[84]C. Kollár.·A szervezeti információbiztonsági folyamatok monitorozása és a vezetői döntések támogatása kulcs teljesítménymutatók segítségével. I. rész – Az információbiztonság rendszerelméleti megközelítése.·Szakmai Szemle.·2017;·XV(4):·43–56

[85]Cybersecurity és A. Infrastructure Security.·Cyber-attack against Ukrainian critical infrastructure (IR-ALERT-H-16-056-01).·2021

[86]M. Akbanov és V. Vassilakis.·WannaCry Ransomware: Analysis of Infection, Persistence, Recovery Prevention and Propagation Mechanisms.·Journal of Telecommunications and Information Technology.·2019;·1:·113-124.·10.26636/jtit.2019.130218

[87]D. Roper.·Big Data as Part of the Critical Infrastructure.·2023

[88]M. Bishop.·Computer Security: Art and Science.·2003

[89]C. Cash.·‘Not the Same Co-op’: Lessons From a Devastating Ransomware Attack.·

[90]L. Muha, . és et al.·Informatikai biztonságmenedzsment.·2008

[91]J. M. Kizza.·Guide to Computer Network Security.·2007

[92]O. V. Póserné.·IT kockázatok elemzésük, kezelésük.·HADMÉRNÖK.·2007;·2(3):·206-214

[93]C. A. Ericson.·Fault Tree Analysis — A History.·2005

[94]U. S. Nuclear Regulatory Commission. Advisory Committee on Reactor Safeguards.·Report to Congressman Morris K. Udall, Chairman, Subcommittee on Energy and the Environment, U.S. House of Representatives, on the Reactor Safety Study (RSS, WASH-1400, NUREG-75/014).·1976

[95]E. Ruijters és M. Stoelinga.·Fault tree analysis: A survey of the state-of-the-art in modeling, analysis and tools.·Computer Science Review.·2015;·15-16:·29-62.·https://doi.org/10.1016/j.cosrev.2015.03.001

[96]National Institute of Standards and Technology.·Security and Privacy Controls for Information Systems and Organizations (NIST SP 800-53 Rev. 5).·2020

[97]C. Engle, J. Brewster és G. Blokdijk.·ISO/IEC 20000 Certification and Implementation Guide - Standard Introduction, Tips for Successful ISO/IEC 20000 Certification, FAQs, Mapping Responsibilities, Terms, Definitions and ISO 20000 Acronyms.·2008

[98]P. Hopkin.·Fundamentals of Risk Management: Understanding, Evaluating and Implementing Effective Risk Management.·2017

[99]Y. Diogenes és E. Ozkaya.·Cybersecurity? Attack and Defense Strategies: Infrastructure Security with Red Team and Blue Team Tactics.·2018

[100]L. Coles-Kemp és M. Theoharidou.·Insider Threat and Information Security Management.·2010.·10.1007/978-1-4419-7133-3_3

[101]M. W. Harkins.·Managing Risk and Information Security: Protect to Enable.·https://doi.org/10.1007/978-1-4842-1455-8.·10.1007/978-1-4842-1455-8

[102]L. Muha és T. Szádeczky.·Irányítási rendszerek.·2014

[103]M.-F. Panettiere.·Virus Software and the First Amendment.·1995

[104]D. H. Wolpert.·Stacked generalization.·Neural Networks.·1992;·5(2):·241-259.·10.1016/S0893-6080(05)80023-1

[105]D. Endres és J. Schindelin.·A new metric for probability distributions.·Information Theory, IEEE Transactions on.·2003;·49:·1858-1860.·10.1109/TIT.2003.813506

[106]M. Fernández-Delgado, E. Cernadas, S. Barro és D. Amorim.·Do we need hundreds of classifiers to solve real world classification problems?·Journal of Machine Learning Research.·2014;·15(1):·3133-3181

[107]B. Frénay és M. Verleysen.·Classification in the Presence of Label Noise: A Survey.·Neural Networks and Learning Systems, IEEE Transactions on.·2014;·25:·845-869.·10.1109/TNNLS.2013.2292894

[108]The New York Times.·Aramco Says Cyberattack Was Aimed at Production.·2012.·https://www.nytimes.com/2012/12/10/business/energy-environment/saudi-aramco-says-hackers-aimed-to-halt-oil-production.html

[109]T. Brewster.·NotPetya Ransomware Hackers 'Took Down Ukraine Power Grid'.·

[110]T. Brewster.·Ukraine Claims Hackers Caused Christmas Power Outage.·

[111]S. Abdelkader, J. Amissah, S. Kinga, G. Mugerwa, E. Ebinyu, D.-E. Mansour, M. Bajaj, V. Blazek és L. Prokop.·Securing Modern Power Systems: Implementing Comprehensive Strategies to Enhance Resilience and Reliability Against Cyber-Attacks.·Results in Engineering.·2024;·23:·102647.·10.1016/j.rineng.2024.102647

[112]D. Whitehead, K. Owens és D. Gammel.·Ukraine cyber-induced power outage: Analysis and practical mitigation strategies.·2017.·10.1109/CPRE.2017.8090056

[113]L. Gawazah.·To Pay or Not to Pay- The US Colonial Pipeline Ransomware Attack.·2024;·

[114]S. e. a. Adam.·The State of Ransomware 2022.·2022

[115]N. Perlroth és C. Krauss.·A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try.·2018

[116]I. Ilascu.·Eletrobras, Copel energy companies hit by ransomware attacks.·2021

[117]D. Goodin.·Two US power plants infected with malware spread via USB drive.·2013

[118]Z. Horváth.·Informatikai rendszerek biztonsága.·2013

[119]R. Klipper.·Risk Management in IT Security.·2011

[120]A. Calder és S. Watkins.·IT Governance: A Manager's Guide to Data Security and ISO 27001 / ISO 27002.·2008

[121]R. Jasmontaitė-Zaniewicz, S. Calvi, D. Nagy és D. Barnard-Wills.·Data Protection and Privacy: The Age of Intelligent Machines.·2020

[122]R. Anderson.·Security Engineering: A Guide to Building Dependable Distributed Systems.·2001

[123]R. Sinha.·Cybersecurity: Accountability and Compliance.·2018

[124]G. Stoneburner, A. Goguen és A. Feringa.·Risk Management Guide for Information Technology Systems.·2002

[125]International Organization for Standardization.·ISO/IEC 27002:2022: Information Security, Cybersecurity, and Privacy Protection — Information Security Controls.·2022

[126]P. Cichonski, T. Millar, T. Grance és K. Scarfone.·Computer Security Incident Handling Guide (NIST Special Publication 800-61 Revision 2).·2012

[127]L. Berek.·Biztonságtechnika.·2014

[128]Z. Berkes, Z. Déri, C. Krasznay és L. Muha.·Informatikai Biztonsági Irányítási Rendszer (IBIR).·2008

[129]Center for Internet Security.·Enterprise Asset Management Policy Template.·2022

[130]L. Muha és Á. Bodlaki.·Az informatikai biztonság tanúsítási és minősítési eljárásrendjének terve.·1997

[131]B. Shojaie, H. Federrath és I. Saberi.·Getting the full benefits of the ISO 27001 to develop an ISMS based on organisations' InfoSec culture.·2016

[132]H. F. Tipton és M. K. Nozaki.·Information security management handbook.·2007

[133]International Organization for Standardization ISO.·ISO/IEC 27001:2022 - Information technology — Security techniques — Information security management systems — Requirements.·2022

[134]E. Humphreys.·Information security management system standards.·Datenschutz und Datensicherheit - DuD.·2011;·35:·7-11.·10.1007/s11623-011-0004-3

[135]J. Yellin.·The Nuclear Regulatory Commission's Reactor Safety Study: Reply.·The Bell Journal of Economics.·1976;·7(2):·711-715.·10.2307/3003283

[136]N. Limnios.·A formal definition of fault tree graph models and an exhaustive test of their structural data.·Reliability Engineering.·1987;·18(4):·267-274.·https://doi.org/10.1016/0143-8174(87)90031-X

[137]K. Tráj és P. László.·Kockázatelemzési módszerek szemléltetése a diákélet egy példáján keresztül – Demonstration of risk assessment methods through a student life problem.·2015

[138]Á. Szeghegyi, G. Kiss és O. Gulyás.·Tudásmenedzsment és kiberbiztonság összefüggésrendszere a bankszektorban.·2022

[139]Miniszterelnöki Kabinetiroda.·7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről.·2024

[140]M. Jariwala.·The Cyber Security Roadmap: A Comprehensive Guide to Cyber Threats, Cyber Laws, and Cyber Security Training for a Safer Digital World.·2023

[141]M. Gosling és A. Hiles.·Business Continuity Statistics: Where Myth Meets Fact.·2010

Tézisfüzet számozott hivatkozások listája

8 Publikációk

8.1 A tézispontokhoz kapcsolódó tudományos közlemények

1. Kovács, A. M. (2024). Comparative Analysis of Traditional and Modern Proxy Solutions in Cyber Security. International Journal of Communication Networks and Information Security, 16(2), Paper 6689.
2. Kovács, A. M. (2024). Migration Perspectives of Water Sector Cybersecurity. Journal of Environmental and Earth Sciences, 6(3), 217–232.
3. Kovács, A. M. (2024). Evolving Cybersecurity Strategies: Analyzing Trends in Critical Infrastructure Attacks and Defense Mechanisms. International Journal of Intelligent Systems and Applications in Engineering, 12(4), 2941–2952.
4. Rajnai, Z., & Kovács, A. M. (2024). Threats and Opportunities Related to the Internet of Things (IoT) and Specific African Healthcare Developments and Risks. In J. Besenyő, M. B. Khanyile, & D. Vogel (Eds.), Terrorism and Counter-Terrorism in Modern Sub-Saharan Africa (pp. 207–225). Springer Nature Switzerland.
5. Kovács, A. M. (2023). Soft Computing in Preventing Ransomware Relying on Larger-Scale Data and Analysis. Strategic Impact, 87(2), 66–84.
6. Kovács, A. M. (2022). Ransomware: A Comprehensive Study of the Exponentially Increasing Cybersecurity Threat. Insights into Regional Development, 4(2), 96–104.
7. Rajnai, Z., & Kovács, A. M. (2020). Links and vulnerabilities of cyber-physical systems—Two approaches' context and relevance: SPAEVI and SCyPH. In Eight International Scientific Web-conference of Scientists and PhD. students or candidates (TIEES 2020) (pp. 193–198). Óbuda University.
8. Kovács, A. M., & Rajnai, Z. (2020). Vulnerabilities, Identification and Detection of Unmanned Aerial Vehicles. In Eight International Scientific Web-conference of Scientists and PhD. students or candidates (TIEES 2020) (pp. 177–183). Óbuda University.

8.2 További tudományos közlemények (opcionális)

9. Kovács, A. M. (2024). Creating Cyber Resiliency in Critical Infrastructures. Advanced Sciences and Technologies for Security Applications, 2024, 247–256.
10. Kovács, A. M. (2022). Here there be Dragons: Evolution, Potentials and Mitigation Opportunities of Cybercrime in Nigeria. Journal of Central and Eastern European African Studies, 2(1), 68–81.

11. Besenyő, J., Kovács, A. M. (2023). Healthcare Cybersecurity Threat Context and Mitigation Opportunities. Security Science Journal, 4(1), pp. 83–101.
12. Kovács, A. M. (2020). Biometric technologies and developmental and information security issues related to their growth in Africa. Biztonságtudományi Szemle, 2(1. Különszám), 49–60.