Dennis Gabor Memorial Year

Erasmus+

FSFT2026

THE FUTURE OF SECURITY
THE FUTURE OF TRUST

ABSTRACT VOLUME

FSFT2026

THE FUTURE OF SECURITY
THE FUTURE OF TRUST

TABLE OF CONTENTS

DENNIS GÁBOR UNIVERSITY

DIGITAL HORIZONS

09:15-10:00 **REGISTRATION**

10:00-10:10 **RECTOR'S WELCOME ADDRESS** (DR. KRISZTINA ZIMÁNYI, PLENARY HALL / GÁBOR DÉNES HALL)

10:10-12:10 **PLENARY LECTURES** (PLENARY HALL / GÁBOR DÉNES LECTURE HALL)

10:10-10:30 **Olivér Bor,** Cybersecurity Manager, Ernst & Young Consulting Ltd.

10:30-10:50 **Péter Rónaszéki,** Managing Partner, FORTIX Consulting Ltd.
From Compliance to Trust: Why Security Only Works When People Change

10:50-11:10 **Béla Szekeres,** CISA, Expert Security Ltd. - Early Detection of IT Security Incidents

11:10-11:30 **László György Dellei,** Information Security Leader, University of Pécs
Ghost in the Machine: AI Agents in SOC

11:30-11:50 **Dr. Monika Nowikowska online,** Assistant Professor, War Studies University
A Redefinition of the Concept of Information in Cyberspace

11:50-12:10 **Dr. András Zsuffa,** CISO, Rufusz Computer Plc. - The Cyber-Gap Is Opening

12:10-13:00 **LUNCH BREAK** (1ST FLOOR)

13:00-13:20 **Dr. Tamás Tóth,** Department Head, Special Service for National Security
Security Challenges Arising from the Development of Infocommunication

13:20-14:10 **Tamás Bagi, István Hatvani, Dániel Keszthelyi, Zsolt Panyi,** Panel Discussion

14:10-14:30 **Péter Suti,** AEGIS: AI-based NIS2 Compliance Management –
Towards Reliable Closed Cybersecurity Governance

14:30-15:00 **COFFEE BREAK** (1ST FLOOR)

15:00-17:00 **SECTIONS**

15:00-17:00 **1. DIGITAL TRUST FRONTIERS** (SECTION ROOM 1 / GÁBOR DÉNES LECTURE HALL)
SECTION CHAIR: DR. ANDRÁS ZSUFFA

- **Sándor Fehér,** CEO, White Hat IT Security
  From Privlieged Users to AI Agents: Emerging Attack Surfaces and Detection Challenges in Cybersecurity
- **Dr. György Bács Zoltán** - Dynamic Risk Analysis and Assessment System with Predictive Capabilities for Crime Prevention
- **Fanni Fülöpné Bártfai** - Critical Infrastructures – Resillusion?
- **Árpád Vukovics online** - Cybersecurity of Space Infrastructure
- **István Gulyás** - The Significant Cybersecurity and Digital Trust Challenges of Virtual Reality (VR)
- **Dr. András Zsuffa** - Section Closing

15:00-17:00 **2. ADAPTIVE CYBER DEFENSE** (SECTION ROOM 2 / NEMES TIHAMÉR HALL)
SECTION CHAIR: DR. JÓZSEF BERKE

- **Lajos Szabó** - Cybersecurity Risks of Quantum Computing, Cybersecurity Aspects of Artificial Intelligence
- **János Sági Gábor** - The Dual Role of Artificial Intelligence in Cybersecurity: Attack and Defense
- **Márton Miklós** - The Era of AI–Quantum Convergence
- **Dr. Ferenc Horváth** - Experiences in Applying AI-based Methods at a Technology-Oriented Intelligence-Gathering Organization
- **Dr. Máté István Zsolt** - Cybersecurity in Law Enforcement IT – Methodological Synergies of Law Enforcement IT Security in the NIS2 Era

15:00-17:00 **3. ADAPTIVE CYBER DEFENSE** (SECTION ROOM 3 / TRAINING ROOM)
SECTION CHAIR: DR. VERONIKA KOZMA-BOGNÁR

- **Zoltán Belinszki** - Defending the Defenseless?
- **Zsuzsa Gulyás** - The Blind Spot of Cybersecurity – Interpretive Vulnerability as a Structural Risk Beyond the Limits of Technical Compliance
- **Csaba Irányi** - The Shadow Side of AI: The Transformation of Cybersecurity Threats and Defense
- **Dr. László Berke** - Online Scientific Communication as Critical Digital Trust Infrastructure
- **Károly Pál Laska** - Modernization and Large-Scale Empirical Validation of Measuring Information Security Awareness

NIS2

PLENARY SESSIONS

FROM REGULATION TO RESILIENCE: PRACTICAL EXPERIENCES OF NIS2 IMPLEMENTATION

Olivér Bor
Manager, EY, Ph.D. Student, NKE HDI, oliver.bor@hu.ey.com

Abstract: The rapid development of cyber threats has fundamentally rewritten the nature of organizational cyber security risks and the logic of their management. According to ENISA's 2025 threat report, DDoS attacks in Europe are up 85% year-on-year, as attackers use increasingly sophisticated, multi-stage methods to distract incident response teams from concurrent, more serious intrusions (ENISA, 2025). Meanwhile, PurpleSec's data indicates that nearly 98% of cyber attacks are based on some psychological manipulation technique, which emphasizes the unavoidable role of the human factor in cyber security defense (PurpleSec, 2024). Global economic damage from cybercrime is expected to approach $9.5 trillion in 2026, making the protection of critical infrastructures and interconnected digital ecosystems a strategic priority (Bor, 2025b).

In this context, Directive 2022/2555 of the European Union - NIS2 - is not only a regulatory milestone, but also a catalyst for a strategic change in approach towards cyber resilience. The implementation of the directive in Hungary was implemented in LXIX of 2024. is implemented by law, which represents a paradigm shift compared to the previous, narrowly state-focused Ibtv.: it creates a proactive, risk-based, auditable and incident management-oriented cybersecurity ecosystem that affects both public and private sector actors (Bor, 2025a). In this framework, public-private collaborations - as the defining tools of collective cyber resilience - are of particular importance, but their effective operation can only be ensured if clear legal, institutional and organizational conditions exist (Bor, 2025b).

The presentation is structured around three thematic axes. It first reviews current cybersecurity threat trends, with a focus on supply chain vulnerabilities, the prominent role of the human factor, and the emergence of hybrid threats. After that, it presents the essential elements of the NIS2 directive, its regulatory logic and the peculiarities of the Hungarian implementation. In the third, practical part of the presentation, NIS2 preparation and auditing experiences will be presented: what typical organizational, procedural and awareness deficiencies are faced by the organizations involved in achieving and maintaining compliance. According to the conclusion of the presentation, regulatory compliance is a necessary but not sufficient condition for true organizational resilience: the development of long-term resilience requires continuous risk assessment, institutional awareness development and a strategic

approach, the foundations of which are also confirmed by empirical research (Palicz et al., 2022; Bor, 2025a).

Keywords: NIS2, cyber security, cyber resilience, risk management, audit

BIBLIOGRAPHY

1. Bor, O. (2025a). Szabályozási szemléletváltás: A NIS2 hatása a magyar kiberbiztonsági szabályozásra. Hadmérnök.
2. Bor, O. (2025b). Kiberfenyegetések és kollektív védelem: nemzeti és nemzetközi kötelezettségek, együttműködések. Szakmai Szemle.
3. ENISA. (2025). ENISA Threat Landscape 2025. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025
4. Palicz, T., Bonnyai, T., Bencsik, B., Pintér, L., Hornyik, Zs., Joó, T., Bor, O., & Dombrádi, V. (2022). Biztonságtudatosság a kibertérben – a 2020-as országos lakossági felmérés eredményei. Belügyi Szemle.
5. PurpleSec. (2024). 2024 cyber security statistics: The ultimate list of stats, data & trends. https://purplesec.us/resources/cyber-security-statistics
6. Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.) a hálózati és információs rendszerek biztonságáról (NIS2 irányelv). Az Európai Unió Hivatalos Lapja, L 333, 80–152.
7. 2024. évi LXIX. törvény a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről (Kibertv.). Magyar Közlöny, 2024/101.
8. 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (Ibtv.). Magyar Közlöny, 2013/79.

GHOST IN THE MACHINE: AI AGENTS IN SOC

Laszlo Gyorgy DELLEI
CISO, Pécsi Tudományegyetem, dellei.laszlo@pte.hu

Abstract: Security Operations Centers (SOCs) are undergoing a significant transformation driven by the increasing integration of artificial intelligence into detection and response processes. Traditional analyst-driven activities—such as alert triage, event correlation, and incident investigation—are increasingly supported by AI-powered capabilities, particularly within User and Entity Behavior Analytics (UEBA) platforms.

The aim of this presentation is to provide a practical, experience-based overview of how AI-driven solutions are reshaping SOC operations. It outlines key areas where automation already delivers measurable value, including the reduction of alert fatigue, faster anomaly detection, and improved decision support. At the same time, it examines the boundaries where human expertise remains essential. The presentation focuses on three core questions: which SOC tasks can realistically be automated, how the role of the security analyst is evolving, and what risks are associated with over-reliance on AI. Through practical examples, it demonstrates how AI-based modules can augment or partially replace analyst activities in well-defined scenarios. It also addresses key challenges such as explainability, accountability, and trust, particularly in regulated environments influenced by frameworks such as NIS2.

Finally, the presentation introduces the concept of the "augmented SOC," where human expertise and AI capabilities operate together to ensure efficient, controlled, and resilient security operations.

Keywords: SOC, artificial intelligence, UEBA, cybersecurity, automation, NIS2, incident response

BIBLIOGRAPHY

1. ENISA. (2023). Artificial Intelligence and Cybersecurity: Challenges and Opportunities.
2. European Union. (2022). Directive (EU) 2022/2555 (NIS2 Directive).
3. RSA Security. (2023). NetWitness Platform Overview and UEBA Capabilities.
4. Sarker, I. H. (2021). AI in Cybersecurity: A Comprehensive Review. Journal of Network and Computer Applications.

A REDEFINITION OF THE CONCEPT OF INFORMATION IN CYBERSPACE

Monika Nowikowska
Head of the Department of IT Law, War Studies University in Warsaw,
m.nowikowska@akademia.mil.pl

Abstract: The article "A Redefining of the Concept of Information in Cyberspace" analyses the evolutionary shift in the communication paradigm. From the traditional model based on reliability to the contemporary model dominated by speed and algorithmic content selection. The main thesis of the text is the shift from information as a commodity providing objective knowledge to information as "noise". In the digital age, traditional authorities and fact-checking processes are losing their significance in favor of immediacy. Information is becoming a tool for attracting the recipient's attention.

Social media algorithms are a key element of this transformation. Their priority is not to deliver valuable content, but content that evokes strong emotions and generates engagement. As a result, reliability gives way to clickbait. These mechanisms lead to the phenomenon of the attention economy, in which it is not the quality of the message, but the time spent by the user on the platform that constitutes the highest market value

The author points out that in a cyberspace overloaded with information, the individual is unable to process the available data, leading to superficial reception. Knowledge is replaced by short messages. Information in cyberspace is mass-produced, fleeting and devoid of context, which causes polarisation and the spread of disinformation. This redefinition forces audiences to develop new skills, as in the digital ecosystem the battle for attention trumps the pursuit of truth.

Keywords: algorithms, attention economy, clickbait, communication, disinformation, information

BIBLIOGRAPHY

1. Malinowski, M. (2022), Algorytm rekomendacji bazujący na sesjach rekomendacji działający na podstawie zachowań użytkowników oraz atrybutów obiektów w systemie e-Commerce, Wydawnictwo Wojskowa Akademia Techniczna.
2. Nowikowska, M., Kozłowski, M. (2025), Analiza wybranych zagrożeń dla tożsamości cyfrowej wynikających z postępu technologicznego, Journal of Modern Science, no. 3, vol. 63, pp. 781-798
3. 3Noga, E. (2023), Personalizacja treści i profilowanie użytkowników: wybrane zjawiska psychometrii w serwisach społecznościowych na przykładzie Facebooka w świetle analizy piśmiennictwa, Acta Universitatis Lodziensis Folia Librorum, no 2(37), pp. 13-38.

FROM COMPLIANCE TO TRUST: WHY SECURITY ONLY WORKS WHEN PEOPLE CHANGE

Peter Ronaszeki, CISM, CDPSE, ISO27001 LA, LI, ISO22301 LA
Managing director, partner, FORTIX Consulting Ltd., peter.ronaszeki@fortix.hu

Abstract: In recent years, organizations have significantly increased their investment in cybersecurity controls, compliance frameworks, and awareness programs. Despite these efforts, successful cyber attacks—particularly those based on social engineering—continue to rise. This paradox highlights a critical gap between formal security compliance and actual organizational resilience.

This presentation examines the limitations of compliance-driven security models and argues that cybersecurity effectiveness ultimately depends on human behavior and decision-making. Drawing on real-world incidents, including high-profile cases of deepfake-enabled fraud and social engineering attacks, the talk demonstrates how attackers increasingly exploit cognitive biases, trust relationships, and time pressure rather than technical vulnerabilities.

Based on field experience and observed patterns across multiple organizations, the presentation introduces a human-centric perspective on cybersecurity, where “trust” becomes a measurable and manageable risk factor. It outlines how traditional awareness approaches often fail to produce lasting behavioral change and why continuous, context-driven engagement is required to influence decision-making in critical moments.

The findings suggest that organizations must move beyond compliance and adopt a behavioral approach to security, focusing on how employees interpret, react to, and act upon security-relevant situations. This shift has significant implications for the design of security programs, risk management practices, and leadership accountability in the evolving threat landscape.

Keywords: cybersecurity, digital trust, human factor, social engineering, deepfake, behavioral security, decision-making, risk management

BIBLIOGRAPHY

1. Infoguard AG. (2026). Social engineering and AI: The human psyche as a target. InfoGuard Blog.
2. AwareGO. (2026). Social engineering techniques: A deep dive into the psychology of the human hack.
3. Reality Defender. (2025). The psychology of deepfakes in social engineering.

AEGIS: AI-AUGMENTED NIS2 COMPLIANCE MANAGEMENT – TOWARDS TRUSTED, CLOSED-ENVIRONMENT CYBERSECURITY GOVERNANCE

Péter Suti
Business Development Director, Spartan Code Kft., suti.peter@spartancode.hu

Abstract: The accelerating regulatory environment — encompassing the NIS2 Directive, GDPR, DORA, and the EU AI Act — places mounting compliance burdens on organisations of all sizes. Simultaneously, the proliferation of cyber threats demands not only regulatory adherence but genuine, measurable security resilience. This paper presents the AEGIS Compliance Management Platform, developed by Spartan Code, and its AI-augmented NIS2 module, demonstrating how artificial intelligence can fundamentally transform the compliance lifecycle from a labour-intensive, document-centric process into an intelligent, automated governance workflow. A central challenge in NIS2 compliance is the secure, structured collection of organisational knowledge — spanning policies, procedures, audio records and informal practices — and its transformation into actionable compliance evidence. The AEGIS platform addresses this through an AI agent-based ingestion pipeline capable of processing multimodal inputs (documents, audio, structured data), storing the extracted knowledge in a secure, structured intelligent data repository, and surfacing it through targeted, competency-aware interview agents that conduct structured assessments with relevant stakeholders.

The resulting intelligence feeds directly into a fully integrated NIS2 workflow: requirement analysis, GAP assessment, remediation plan management, automated policy generation, and comprehensive audit support — all within a closed, sovereign environment. Unlike conventional approaches that require sensitive compliance data to be shared with external auditors or third-party tools, AEGIS enforces end-to-end data sovereignty: auditors operate within the platform under controlled access, and no sensitive data leaves the system. This architecture addresses a critical but underexplored tension in cybersecurity compliance: the conflict between openness (sharing data with auditors and regulators) and security (keeping sensitive operational data contained). This presentation argues that AI-enabled closed-loop compliance systems represent the next frontier of trusted cybersecurity governance, aligning the Future of Security with the Future of Trust.

Keywords: Compliance management NIS2, AI agent, intelligent data repository, data sovereignty, closed audit environment, automated policy generation

BIBLIOGRAPHY

1. European Parliament and the Council. (2022). Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). Official Journal of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555
2. Lewis, J. A. (2023). Cyber Governance in an Uncertain World. Center for Strategic and International Studies (CSIS). https://www.csis.org/analysis/cyber-governance-uncertain-world
3. Gao, Y., Xiong, Y., Gao, X., Jin, H., Liu, H., Xiong, Z., Li, Z., Shen, Z., Wu, F., & Wang, H. (2024). Retrieval-augmented generation for large language models: A survey. arXiv preprint arXiv:2312.10997. https://arxiv.org/abs/2312.10997
4. ENISA. (2023). NIS2 implementation: Key challenges and emerging best practices. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/nis2-implementation
5. Schmitt, P., & Flechais, I. (2023). Automated compliance: Risks and opportunities of AI-driven regulatory adherence. Computers & Security, 128, 103170. https://doi.org/10.1016/j.cose.2023.103170

EARLY DETECTION OF IT SECURITY INCIDENTS

Béla Szekeres
CISA, Expert Security, bela.szekeres@xsec.eu

Abstract: Any IT system can be hacked. The question is whether we will detect it in time to mitigate or possibly prevent the damage. Unfortunately, international experience is quite bad; the average detection time has not decreased in recent years. Software development cycles have accelerated, IT systems are becoming increasingly complex, all of which increase the chances of IT security vulnerabilities. Attackers have many new tools at their disposal to exploit these vulnerabilities. In this presentation, we will look at the tools we have for early detection, the challenges we face, and what can be done to overcome them. We will discuss basic design principles that are worth following when designing the IT environment. We will address the human resources required for defense systems and the consequences of their scarcity. We will discuss some common misconceptions among decision-makers and the consequences of them on the security of the organization. At the end of the presentation, we will review what recently introduced standards can bring, both positively and negatively.

The argument of the presentation is that creating an IT security environment is not a one-time activity, but an ongoing journey, where our chances are quite bad, but if we use our existing tools wisely, our chances can be significantly improved.

Keywords: early detection, SIEM, Secure by Design

BIBLIOGRAPHY

1. Yaman Roumani (2021), Detection time of data breaches https://www.sciencedirect.com/science/article/abs/pii/S0167404821003321
2. Australian Signals Directorate (2024), Identifying and Mitigating Living Off the Land Techniques https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories/identifying-and-mitigating-living-off-the-land-techniques
3. Sławomir Żurawski1, Aneta Chrząszcz, et al. (2025), Effectiveness of Information Security Incident Management Systems: Identifying Practices, Challenges and Development Perspectives https://ersj.eu/journal/3922/download/Effectiveness+of+Information+Security+Incident+Management+Systems+Identifying+Practices+Challenges+and+Development+Perspectives.pdf

SOME SECURITY CHALLENGES OF THE DEVELOPMENT OF INFOCOMMUNICATION

Tamás Tóth
department head, Special Service for National Security, toth.tamas@nbsz.gov.hu

Abstract: Trends related to the development of the information and communication technology environment (ICT) include connectivity, convergence, multimodality, and the strengthening of data protection, and from the security aspect. The infocommunication opportunities offered by new disruptive technologies are also used by those monitored by law enforcement and national security organizations. The analysis of the ICT environment from a security aspect requires a very complex approach, which is why it is necessary to analyze the social, technological, legal, and security environment.

Regarding social and user trends, it can be stated that there are 8.8 billion mobile phones for approximately 8.3 billion inhabitants of the Earth, more than 6 billion have internet access, which numbers are increasing, even if only in terms of the time spent using the internet. The most popular internet consumption devices are smartphones, and the services are communication applications.

In terms of the technological environment, it can be seen that new-generation mobile communication networks have an exponentially increasing crowding-out effect on previous ones, with the increase in data transfer speed, bandwidth and service coverage requirements, the decrease in latency, and the appearance of increasingly heterogeneous and advanced security-marked data packets appearing on networks. Due to the above, a shift in the architectural structure of terrestrial communication networks towards airspace and outer space is expected by 2030, which is induced on the one hand by the demand for the spread of smart city ecosystems.

In connection with the regulation of new infocommunication technologies, the issue of efficiency and topicality, the balance between the value duality of data protection and security, the rise of human rights fundamentalism and the need for effective international legal regulation and multilateral and bilateral cooperation due to global services.

In relation to the security environment, it can be seen that communication applications that provide end-to-end encryption based on Internet technology are also used in connection with terrorism, criminal organizations, extremist groups, and the sexual exploitation of children, so the lawful control of communication carried out on them is a matter of public interest.

The global nature of services, the development of network infrastructure and cryptography, the need for effective regulation, and the use of encrypted communication applications in criminal activities can be assessed as a challenge from the point of view of lawful communication control, which has a negative impact on security interests. Thus, effective international cooperation with service providers, the development of an effective legal environment, and the development of alternative cryptographic solutions that complement each other ensure the expected data protection and the enforcement of security interests.
Visszajelzés küldése

Keywords: infocommunication, Information and Communication Technologies, law enforcement, national security, terrorism, organized crime

BIBLIOGRAPHY

1. Tóth, T. (2024). The effects of changes in the ICT environment on the development of information gathering in the 21st century. Doctoral (PhD) thesis. NUPS MDS. https://tudasportal.uni-nke.hu/xmlui/handle/20.500.12944/101088
2. Kovács, Z. (2015). Az infokommunikációs rendszerek nemzetbiztonsági kihívásai. Doctoral (PhD) thesis. NUPS MTDS. https://adoc.tips/az-infokommunikacios-rendszerek-nemzetbiztonsagi-kihivasai.html
3. Lapsánszky, A. (Eds.) (2013). Communications regulation and administration in Hungary and the European Union. Wolters Kluwe CompLex.

THE CYBER-GAP IS OPENING

András Zsuffa
CISO, Rufusz Computer Corp., zsuffa.andras@rufusz.hu

Abstract: When estimating cybersecurity risks, we typically assume that defensive and offensive capabilities evolve at a similar pace. Empirical evidences, however, paint a far more complex and uncomfortable picture. Multiple independent sources — including industry incident data, threat intelligence reports, and AI capability assessments — indicate that attacker capabilities are not developing linearly, but are accelerating across multiple dimensions simultaneously. The time required to exploit vulnerabilities is shrinking dramatically and continuously, in some cases collapsing from weeks to days or even hours. Attack techniques are increasingly built on scalable, automated, and reusable components, while the attacker ecosystem is becoming progressively more organized along business-like lines. In parallel, artificial intelligence is rapidly expanding offensive capabilities, broadening the range of automatable and delegable attack tasks in short cycles. These trends do not merely reflect an increase in the number of attacks, but a qualitative transformation of attacker capabilities: the combined amplification of speed, scalability, and adaptability. As a result, traditional defensive approaches — reactive and compliance-driven by design — are entering a state of structural disadvantage. The central claim of this presentation is that the "cyber gap" is not only opening, but that its rate of expansion is also increasing under current defense models. The question is therefore no longer whether this gap can be eliminated, but rather what new approaches can slow its growth and keep its impact within manageable bounds.

Keywords: Cyber-gap, attack automation, AI, asymmetry

BIBLIOGRAPHY

1. Erukude, S. T., Marella, V. C., & Veluru, S. R. (2026).AI-driven cybersecurity threats: A survey of emerging risks and defensive strategies. arXiv. https://arxiv.org/abs/2601.03304
2. Iturbe, E., Llorente-Vazquez, O., Rego, A., Rios, E., & Toledo, N. (2024). Unleashing offensive artificial intelligence: Automated attack technique code generation. Computers & Security, 147, 104077. https://doi.org/10.1016/j.cose.2024.104077
3. Zhuo, T. Y., Ding, Y., Guo, W., & Meng, R. (2026). To defend against cyber attacks, we must teach AI agents to hack. arXiv. https://arxiv.org/abs/2602.02595
4. Charan, P. V. S., Chunduri, H., Anand, P. M., & Shukla, S. K. (2023). From text to MITRE techniques: Exploring the malicious use of large language models for generating cyber attack payloads. arXiv. https://arxiv.org/abs/2305.15336

1. DIGITAL TRUST FRONTIERS

DYNAMIC RISK ANALYSIS AND ASSESSMENT SYSTEM WITH PREDICTIVE CAPABILITIES FOR CRIME PREVENTION

Zoltán György BÁCS
Assistant professor, Ludovika University of Public Service, bacs.zoltan.gyorgy@uni-nke.hu

Abstract: According to the well-spread expression of the Professor Emeritus of the Ludovika University of Public Service, Géza Finszter, the most tolerable by the society crime is that one which has not been perpetrated at all. Therefore, the crime prevention is one of the key areas of law-enforcement bodies.

Which crime's prevention should have the absolute priority? The answer is as simple as complex. There are different legal aspects and investigation technics required for preventing pick-pocketing or highly sophisticated cyber crimes. Following the logic of law-enforcement bodies the efforts shall be concentrated on prevention of crimes which cause more material and financial losses and are also spread widely that might impact the trust of the society in official entities, law-enforcement, the judiciary system and even in the government.

These crimes are mostly perpetrated in the cyber space therefore we call them cybercrimes. The perpetrators use false identity masking themselves as representatives of banks, charity organizations, financial entities, law-enforcement officers, service suppliers, etc. ... Their intention is the gain the trust of the ordinary people who will realize they have become victims of a crime when they face that their bank accounts have been hacked.

The prevention of this kind of crime is far more complicated than the others. The necessary information should be gathered beforehand by scanning the cyberspace in general and paying a special attention to illegal trade of databases on the dark web. The first task is to achieve the operational capability to monitor the dark web just to clarify the main actors involved in cybercrimes and to reveal the patterns of their activities. After this it becomes possible to detect any activity demonstrating the same patterns. The next phase is to trace the electronic devises involved in criminal activities and the definition of their physical allocation.

All these functions might be carried out by setting up a new approach to information and a new dynamic analysis and assessment system based on the new theory of information (Gondolatok az információ szerepéről...) The new information theory is capable to detect the dynamic changes of the risk factors depending on their possible threatening consequences (Network-researched Based Dynamic Method in Crime Prevention and Investigation)

Another incomparable advantage of the dynamic risk analysis and assessment system is its predictive capabilities. The effect is the possible reduction of crimes based on informatic devises and linked to the dark web. The system is also capable to give a dynamic prediction of the foreseeable tendencies in crimes.

Keywords: information theory, dynamism, reduction of criminality

BIBLIOGRAPHY

1. Bács Zoltán György: Gondolatok az információ szerepéről – más, egyéni szemszögből NEMZETBIZTONSÁGI SZEMLE (ONLINE) 11 : 3 pp. 83-92. , 10 p. (2023)
2. Zoltán György BÁCS: Network-researched Based Dynamic Method in Crime Prevention and Investigation In: Dobák, Imre; Farkas, Johanna (szerk.) 2nd Law Enforcement Security and sychology (LEPSY) CEEPUS Network Conference Budapest, Magyarország : Law Enforcement and Psychology CEEPUS Network (2025) 58 p. ISBN: 9789634986812
3. Új, innovatív módszer megalapozása az elemző-értékelő munkában MAGYAR RENDÉSZET 22 : 3 pp. 83-99. , 17 p. (2022)

FROM PRIVILEGED USERS TO AI AGENTS: EMERGING ATTACK SURFACES AND DETECTION CHALLENGES IN CYBERSECURITY

Sándor Fehér
CEO, White Hat IT Security, sandor.feher@whitehat.eu

Abstract: This presentation examines how attackers have historically compromised enterprise networks by obtaining the credentials or access rights of highly privileged users. Through two case studies based on previous real-world incidents, the presentation demonstrates how adversaries were able to gain initial access, escalate privileges, move laterally across the network, and ultimately reach critical systems. These examples highlight a longstanding principle in cybersecurity: privileged access remains one of the most valuable targets for attackers, as it enables them to bypass controls, expand their reach, and increase the potential business impact of an intrusion.

Building on these lessons, the presentation connects traditional privileged account compromise to the current era of artificial intelligence agents. As organizations increasingly deploy AI agents to support business operations, software development, IT administration, security workflows, and automated decision-making, these agents are often granted access to data, systems, APIs, and execution environments. Consequently, the permissions assigned to AI agents may become attractive targets for attackers in much the same way as privileged user accounts have been in the past.

A key concern is that detection, monitoring, logging, and behavioral analysis capabilities around AI agents are often less mature than those applied to traditional users, administrators, or service accounts. This creates a growing visibility gap in modern enterprise security architectures. The final part of the presentation introduces the ten most typical AI-related cybersecurity risks, with particular focus on access control, data exposure, prompt manipulation, model and API abuse, supply-chain risks, and weaknesses in detection and governance.

Keywords: AI agent, cyber security incident, AI risks

BIBLIOGRAPHY

1. 1 MITRE. (n.d.). MITRE ATLAS™. Retrieved May 7, 2026, from https://atlas.mitre.org/
2. OWASP Foundation. (2025). OWASP Top 10 for Large Language Model Applications 2025. OWASP. https://genai.owasp.org/resource/owasp-top-10-for-llmapplications-2025/
3. Uber Team. (2022, September 16). Security update. Uber Newsroom. https://www.uber.com/-newsroom/security-update/
4. CyberArk Blog Team. (2022, September 20). Unpacking the Uber breach. CyberArk. https://www.cyberark.com/resources/blog/unpacking-the-uber-breach

CRITICAL INFRASTRUCTURES - RESILLUSION?

Fanni Fülöpné Bártfai
PhD Student, NKE-KMDI, fannibartfai@gmail.com

Abstract: A wide range of motivations may lie behind cyberattacks, from financial gain through political and ideological objectives to the execution of traditional military operations [1]. The common factor among them, however, is that critical infrastructures can represent attractive targets for all such attacks, as the functioning of modern societies heavily depends on information and communication systems [2].

In the past five years, numerous significant examples have illustrated cyberattacks against critical infrastructure. During the 2021 Colonial Pipeline incident, a ransomware attack severely disrupted fuel supply along the eastern coast of the United States, highlighting the indirect vulnerabilities of cyber-physical systems and the severity of economic consequences. Similar threats have also emerged in Europe, where coordinated hybrid attacks targeting airports and energy systems have tested defensive capabilities.

The changing security environment has required enhanced measures at allied [3], European, and national levels alike, which led to the adoption of Directive (EU) 2022/2557 on the resilience of critical entities (CER).

The objective of the directive is to establish a uniform and robust level of resilience across the Union, requiring critical infrastructures to develop and maintain measures and procedures that ensure operational continuity and resistance to disruptions. Two key pillars of this requirement are comprehensive risk assessment covering the entire operational environment and a resilience plan. Affected organizations must understand that preparing and maintaining these documents goes beyond administrative burdens aimed solely at legal compliance; instead, they can contribute to increased competitiveness. Resilient operations, supported by properly designed, organization- and process-based, and practically tested contingency planning or incident management plans, can reduce response times in the event of an incident, thereby significantly minimizing the extent of damage.

For organizations that already operate integrated management systems based on international standards reflecting real operations (e.g., ISO 27001, ISO 22301), developing a resilience plan is not unfamiliar, as they typically already possess tested business continuity

and disaster recovery plans, a service catalog, and comprehensive risk assessments covering the entire environment.

The presentation will demonstrate how a well-developed resilience plan can serve as a practical guideline.

Keywords: critical infrastructures, cybercrime, cyber operations, resilience

BIBLIOGRAPHY

1. Krasznay Csaba (szerk) (2023): Taktikák és stratégiák a kiberhadviselésben
2. Kovács László (2023): Hadviselés a 21. században: kiberműveletek
3. Mógor Judit – Angyal István (2025): A kritikus infrastruktúrák ellenálló képesség fejlesztését célzó szabályozás mérföldkövei 2022-2025

THE SIGNIFICANT CYBERSECURITY AND DIGITAL TRUST CHALLENGES OF VIRTUAL REALITY (VR)

István Gulyás
researcher, University of Dunaújváros, igulyas@mac.com

Abstract: The rapid rise of virtual reality (VR) and extended reality (XR) technologies is opening up new dimensions in digital interactions, while also posing significant cybersecurity and digital trust challenges. The aim of this study is to analyze the security risks of VR-based systems and the sustainability of trust, with a particular focus on the evolution of cyberattacks, software and supply chain security, and the protection of critical infrastructure. The results highlight that VR systems offer an expanded attack surface due to sensors, biometric data, and real-time data processing, which goes beyond the risks of traditional IT systems. The evolution of cyberattacks — including ransomware, phishing, deepfake-based social manipulation, and denial-of-service attacks — is targeting virtual environments in increasingly sophisticated ways, exploiting weaknesses in identity management and authentication. Due to the IoT-like architecture of VR platforms, traditional vulnerabilities (e.g., misconfigurations, software bugs) remain relevant but are supplemented by new, immersion-specific threats.

Software supply chains pose a significant risk, as the compromise of third-party components and developer tools can lead to system-wide vulnerabilities. A significant portion of modern cyberattacks occurs indirectly through supply chains, which is particularly critical for VR ecosystems due to their high degree of integration. Flaws identified in VR software — particularly interface and resource management vulnerabilities — further increase risks, especially in the early stages of the development lifecycle.

The VR-based integration of critical infrastructure (e.g., healthcare, industrial systems, education) imposes additional security requirements. Disruption or manipulation of VR devices can have a direct impact on operational processes, so protecting them requires a multi-layered defense strategy that goes beyond traditional IT security.

Overall, maintaining digital trust in VR environments requires a complex, interdisciplinary approach that includes the use of “zero-trust” architectures, continuous monitoring, standardized security frameworks, and increased user awareness. This study emphasizes that the security of future VR ecosystems is crucial for ensuring the widespread adoption of the technology and the stability of the digital economy.

Keywords: virtual reality, cybersecurity, digital trust, critical infrastructure

BIBLIOGRAPHY

1. Cayir, A., Odeleye, B. P., & O'Hagan, A. (2024): Security and privacy in virtual reality: a literature survey., DOI: 10.1007/s10055-024-01079-9
2. P. Wang, H. Liang, S. Wu, & L. Sun (2024): Sensor Security in Virtual Reality: Exploration and Mitigation, DOI: 10.1145/3643832.3661389
3. H. Zhang, X. Li, & J. Wei (2025): An Empirical Study on Virtual Reality Software Security, DOI: 10.48550/arXiv.2507.17324

CYBERSECURITY OF SPACE INFRASTRUCTURE

Árpád Vukovics
Alumni, Capella University, 107 Meryton Dr. Dallas, GA 30157, arpad.vukovics@mac.com

Abstract: This presentation aims to examine the growing importance of cybersecurity for space infrastructure as satellites and related systems become increasingly essential to modern life, economic activity, public safety, defense, and global communications. It introduces the evolving space ecosystem, including ground, space, communication, and user segments, and highlights how the transition from isolated, analog, and hardware-based systems toward networked, digital, and software-driven architectures has expanded the cyber threat surface. The presentation explains why satellite security matters by connecting space systems to everyday services such as GPS, internet access, logistics, utilities, weather forecasting, and disaster response. It also reviews core cybersecurity principles, including confidentiality, integrity, availability, reliability, authenticity, accountability, and non-repudiation. Special attention is given to major threat vectors, including supply-chain vulnerabilities, cloud infrastructure risks, signal interference, malware, insider threats, payload hijacking, and anti-satellite capabilities. The 2022 Viasat KA-SAT cyberattack is presented as a concrete example of how a satellite-network incident can disrupt internet access, energy infrastructure, emergency services, and remote communities. Finally, the presentation considers emerging risks such as quantum computing, artificial intelligence, the Internet of Things, and Kessler syndrome, while outlining mitigation approaches through encryption, resilience, risk management, NIST standards, FIPS publications, and the SPARTA framework.

Keywords: Satellite cybersecurity; cyber threats; satellite communications; ground segment security; signal interference; Viasat KA-SAT attack; quantum-resistant encryption

BIBLIOGRAPHY

1. Pratt, T., & Allnutt, J. (2020). Satellite Communications (3rd ed.) Wiley. ISBN 9781119482178
2. SANS Cyberdefense (2024). The Risk to Space: Satellite Communications Systems and Ground Networks as Attack Targets. Retrieved from: https://www.youtube.com/watch?v=Myk8QzXbmq8
3. Peled, R., Aizikovich, E., Habler, E., Elovici, Y., & Shabtai, A. (2023). Evaluating the Security of Satellite Systems.Cornell University. arXiv preprint arXiv:2312.01330.
4. NIST (n.d.). Cybersecurity framework, 2025. Retrieved from: https://www.nist.gov/cyberframework
5. Barett, T. (2024). Looking to the skies: The importance of satellite cybersecurity. Retrieved from: https://www.ussc.edu.au/the-importance-of-satellite-cybersecurity

2. ADAPTIVE CYBER DEFENCE

EXPERIENCES IN IMPLEMENTING NEW TRAINING METHODS AT A TECHNOLOGY-CENTERED INTELLIGENCE ORGANIZATION

Ferenc Horváth
SSNS, fhorvath25@gmail.com

Abstract: Humanity remains the fundamental cornerstone of cybersecurity. To ensure that users do not become the "weakest link," mere instruction is insufficient; organizations must actively shape mindsets and cultivate deep-rooted security awareness. For educational content to translate into real-world utility, training programs must engage all neurological levels that are active during the practical exercise of a specific competence. Simply transplanting traditional, "Prussian-style" educational principles into the digital realm is no longer an effective strategy. The true breakthrough occurs when the focus shifts entirely toward the learners themselves—their unique needs, behaviors, and individual characteristics. The primary objective should be the creation of user-friendly learning opportunities rather than the imposition of mandatory training. This pedagogical transition prioritizes competence development over simple knowledge transfer, interaction over top-down communication, and multimodal experiences over passive listening. Furthermore, it replaces rigid mandates with gamification, memory-based testing with practical application, and instructor authority with collaborative partnership. This presentation examines the challenges overcome and the measurable results achieved while establishing an organizational training framework built upon these modern principles within a technology-centric intelligence environment.

Keywords: Cybersecurity Awareness, Mindset Shaping, Multimodal Learning, Competence Development, Gamification

BIBLIOGRAPHY

1. Horváth, F., (2024). Új képzési módszerek alkalmazásának tapasztalatai a Nemzetbiztonsági Szakszolgálatnál. NEMZETBIZTONSÁGI SZEMLE (ONLINE) (2064-3756): 12 2 pp 81-97. https://orcid.org/0000-0001-8639-2700
2. Horváth, F., (2022). “From Top to Toe”: Choosing the Appropriate Training Method NEMZETBIZTONSÁGI SZEMLE (ONLINE) (2064-3756): 10 3 pp 44-56. doi: 10.32561/nsz.2022.3.4

CYBERSECURITY IN DIGITAL FORENSICS - CYBERSECURITY OF DIGITAL FORENSICS: METHODOLOGICAL SYNERGIES WITHIN THE NIS2 FRAMEWORK

István Zsolt MÁTÉ
digital forensic expert, Hungarian Institute for Forensic Sciences, mateizs@nszkk.gov.hu

Abstract: Digital forensics and cybersecurity are traditionally considered to be distinct fields within the applied sciences. The fundamental reason for the methodological divide between the two fields lies in the divergence of their respective approaches. Digital forensics is fundamentally based on ex post (post-mortem) investigations and examines digital traces from an exploratory-analytical perspective for the purpose of evidence gathering. In contrast, cybersecurity focuses on ex ante prevention and real-time, active incident management.

However, the convergence of these two fields has accelerated in recent times. The intricate nature of cyber threats and the impermanence of evidence necessitate novel methodological synergies, leading to the convergence of defensive and investigative functions. The concept of forensic readiness is also reflected in this principle, which can be defined as the conscious design of systems that ensures the provision of legally relevant evidence without compromising defence mechanisms.

The presentation highlights these complex challenges through case studies—based on the methodological framework of the ISO/IEC 27043:2015 standard and the NIS2 Directive—and finally formulates adaptive expert responses that ensure digital trust remains sustainable even amid technological advancements and an increasingly stringent legal environment.

Keywords: cybersecurity, digital forensic, forensic readiness, methodological synergy

BIBLIOGRAPHY

1. Máté, I. Zs. (2018). Informatikai rendszerek elleni támadások szakértői vizsgálata – a digitális nyomok rögzítésének szerepe [Expert investigation of attacks against information systems – the role of recording digital traces]. Belügyi Szemle / Academic Journal of Internal Affairs, 66(7–8), 36–54.
2. Máté, I. Zs. (2020). Az igazságügyi informatikai szakértő feladatai [The tasks of the digital forensic expert]. In P. Ruzsonyi (Ed.), Közbiztonság: Fenntartható biztonság és társadalmi környezet tanulmányok III. [Public Security: Sustainable Security and Social Environment Studies III] (pp. 1871–1894). Ludovika Egyetemi Kiadó.
3. Máté, I. Zs., Darabos, Z., Morber, Sz. K., & Sándor, G. (2021). Módszertani levél az elektronikus adatok vizsgálatának általános alapelveiről [Methodological Guideline on the general principles of the examination of electronic data]. Hungarian Chamber of Judicial Experts (MISZK).
4. Máté, I. Zs. (2025). Mesterséges intelligencia az igazságügyi szakértői munkában [Artificial intelligence in forensic expert work]. In J. Répás (Ed.), Alverad-Bánki Nemzetközi Kiberbiztonsági és Kutatás-Fejlesztési Konferencia: Konferenciakötet – Book of Abstracts [Alverad-Bánki International Cybersecurity and Research & Development Conference: Conference Proceedings – Book of Abstracts] (p. 67). Óbudai Egyetem; Alverad Technology Focus Kft.
5. Máté, I. Zs. (2026). Forensic expert case registry (2007–2026) [Unpublished raw data].

THE AI-QUANTUM COLLISION

Márton Miklós
CEO, ACPM IT Zrt., President, Hungarian Cybersecurity Cluster
marton.miklos@acpmit.com

Abstract: As of 2026, the cybersecurity landscape has entered the "Collision Era," where the convergence of frontier AI models and quantum computing has fundamentally shifted global security paradigms. This research aims to analyze the emergence of "Automated Offense" and the resulting collapse of traditional boundaries between human expertise and machine speed. It explores the urgent necessity for organizations to transition from reactive, manual security models to AI-native, quantum-resilient frameworks.

Recent developments in AI have demonstrated a pivotal moment for cybersecurity. Mythos has successfully automated the discovery of high-severity zero-day vulnerabilities—such as a decade-old Apache ActiveMQ flaw—in minutes rather than weeks. This acceleration has triggered an remediation crisis characterized by a bottleneck where the volume of AI-generated bug reports exceeds human patching capacity.

Simultaneously, the rise of "Harvest Now, Decrypt Later" (HNDL) attacks and the approaching "Q-Day" threaten the functional lifespan of RSA and Elliptic Curve encryption.

The research finds that cryptographic agility is no longer optional; organizations must migrate to NIST-approved Post-Quantum Cryptography (PQC) standards like ML-KEM to survive the quantum transition. Furthermore, the study identifies a strategic shift toward continuous compliance to automate the mapping of complex 2026 mandates like the EU AI Act. Ultimately, successful defense in 2026 requires utilizing quantum-enhanced AI to automate the remediation process, thereby matching the speed of automated offensive tools..

Keywords: Post-Quantum Cryptography (PQC), AI-Native Defense, Claude Mythos, Q-Day, CRQC, Automated Offense, Continuous Compliance, Remediation Crisis, Harvest Now Decrypt Later

BIBLIOGRAPHY

1. Anthropic Red Team Report (April 7, 2026): "Assessing Claude Mythos Preview's Cybersecurity Capabilities." Key Fact: Documented the model's ability to find 27-year-old bugs in OpenBSD and 16-year-old flaws in FFmpeg.
2. Radware Blog (April 28, 2026): "Anthropic Claude Mythos and the 2026 Cybersecurity Landscape." Key Fact: Details on Project Glasswing, the defensive coalition of 40 organizations (Google, Microsoft, etc.) testing Mythos before public release.
3. Help Net Security (April 9, 2026): "Claude helps researcher dig up decade-old Apache ActiveMQ RCE vulnerability (CVE-2026-34197)." Key Fact: Horizon3.ai researcher used Claude to identify a 13-year-old "unauthenticated RCE" path in the ActiveMQ Classic codebase.
4. Cybernews (April 8, 2026): "AI is breaking bug bounty programs by finding too much." Key Fact: Coverage of HackerOne pausing new submissions for the Internet Bug Bounty due to the overwhelming volume of AI-assisted reports outstripping human patch capacity.
5. Cloud Security Alliance Whitepaper (April 13, 2026): "Claude Mythos: AI Vulnerability Discovery and Containment Failures." Key Fact: Analysis of the "Remediation Gap"—where discovery speed increased by 10,000% while patching speed remained linear.
6. CISA Technical Advisory (January 24, 2026): "Product Categories for Technologies Using Post-Quantum Cryptography Standards." Key Fact: Mandated that federal agencies stop procuring legacy (RSA/ECC) products for "Widely Available" categories like Cloud and Web Browsers.
7. NIST Special Publication (March 2026): "NIST IR 8547: A Roadmap for Transitioning to Post-Quantum Cryptography." Key Fact: Official finalization and implementation guide for ML-KEM and ML-DSA algorithms.
8. Google Cloud Security (November 2025): "Cybersecurity Forecast 2026: The Rise of Harvest Now, Decrypt Later (HNDL) Infrastructure."
9. Deutsche Telekom Event (March 18, 2026): "TRANSFORM 2026: Scaling AI & Data for a Trusted Digital Future." Key Fact: Keynote by Klaus Werner on using AI Security Agents to embed governance directly into the network fabric.
10. Openlayer Blog (April 24, 2026): "EU AI Act Post-Market Monitoring Guide: April 2026 Enforcement." Key Fact: Explains the Article 72 requirement for continuous monitoring and how major telcos like Telefonica use Openlayer to automate real-time compliance evidence.
11. European Commission (February 2, 2026): "Standardized Template for AI Post-Market Monitoring Plans." Key Fact: The regulatory trigger that forced telcos to move from static audits to automated AI monitoring.
12. Google Cloud Security Forecast 2026: Comprehensive report on "Shadow Agents" and the virtualization of the threat landscape.
13. CVE-2025-59536: Documentation of the first major "AI Supply Chain" RCE discovered in popular AI coding assistants.

THE DUAL ROLE OF ARTIFICIAL INTELLIGENCE IN CYBERSECURITY: ATTACK AND DEFENSE

Gábor János Sági
cyber security expert, gaborjanos.sagi@hungarocontrol.hu

Abstract: The rapid development of Artificial Intelligence (AI) has fundamentally transformed attack and defense tactics in cyberspace, making it a dual-use technology. Cyber attackers automate and scale their operations using AI-based tools. With the help of generative models, they create personalized, context-aware phishing campaigns and deepfake content (Mohamed, 2023). Through machine learning, they develop adaptive, self-mutating malware that evades traditional defense systems (Telrandhe et al., 2025), and they employ deceptive patterns to bypass or poison ML-based detectors (Vitorino et al., 2023).

In parallel, cyber defenders are also increasingly applying AI technologies. Deep learning methods improve intrusion detection and anomaly recognition through the analysis of complex network traffic patterns (Nakıp & Gelenbe, 2024). Self-supervised learning approaches enable real-time threat detection against changing attack vectors (Neha & Bhatia, 2025). AI-based threat intelligence systems perform predictive risk assessment and accelerate the workflows of Security Operations Centers (SOC) (Sharma, 2024). Automated incident response platforms reduce reaction times (Nnaka et al., 2025).

However, the dual use of AI poses serious challenges; defense systems themselves are vulnerable to adversarial attacks, therefore hybrid approaches, adversarial training, and continuous retraining are required (Mohamed, 2025). The research highlights that the effectiveness of AI-driven cybersecurity can only be ensured through the integrated, synergistic application of technological solutions and human oversight.

Keywords: AI in offence, AI in defense, AI in cybersecurity

BIBLIOGRAPHY

1. Mohamed, N. (2023). Current trends in AI and ML for cybersecurity: A state-of-the-art survey. Cogent Engineering, 10(2), Article 2272358. https://doi.org/10.1080/23311916.2023.2272358
2. Mohamed, N. (2025). Cutting-edge advances in AI and ML for cybersecurity: A comprehensive review of emerging trends and future directions. Cogent Business & Management, 12(1), Article 2518496. https://doi.org/10.1080/23311975.2025.2518496
3. Nakıp, M., & Gelenbe, E. (2024). Online self-supervised deep learning for intrusion detection systems. IEEE Transactions on Information Forensics and Security, 19, 5668–5683. https://doi.org/10.1109/TIFS.2024.3402148
4. Neha, & Bhatia, T. (2025). Adaptive intrusion detection system leveraging dynamic neural models with adversarial learning for 5G/6G networks. In Proceedings of the 2025 4th International Conference on Computer Technologies (ICCTech) (pp. 103–107). IEEE. https://doi.org/10.1109/ICCTech66294.2025.00028
5. Nnaka, K. I., Mbamalu, P. O., Nwaigbo, J. C., Ozo-ogueji, P. C., Njoku, V. I., & Ekechi, C. C. (2025). AI-powered threat detection: Opportunities and limitations in modern cyber defense. World Journal of Advanced Research and Reviews, 27(2), 210–223. https://doi.org/10.30574/wjarr.2025.27.2.2854
6. Sharma, S. K. (2024). AI-enhanced cyber threat detection and response systems. Shodh Sagar Journal of Artificial Intelligence and Machine Learning, 1(2), 43–48. https://doi.org/10.36676/ssjaiml.v1.i2.14
7. Telrandhe, A. V., Nishane, D., Puri, C., & Gayaki, U. (2025). AI-powered threat detection and response system for next-gen cyber defense. In Proceedings of the 2025 2nd International Conference on Electronic Circuits and Signaling Technologies (ICECST) (pp. 1132–1137). IEEE. https://doi.org/10.1109/icecst66106.2025.11307219
8. Vitorino, J., Praça, I., & Maia, E. (2023). SoK: Realistic adversarial attacks and defenses for intelligent network intrusion detection. Computers & Security, 134, Article 103433. https://doi.org/10.1016/j.cose.2023.103433

CYBER RISKS OF QUANTUM COMPUTING AND CYBERSECURITY ASPECTS OF ARTIFICIAL INTELLIGENCE

Lajos Szabó
Director, National Cybersecurity Centre, Hungary, lajos.szabo@nki.gov.hu

Abstract: This presentation examines the cybersecurity implications of quantum computing and artificial intelligence (AI), with particular focus on emerging technological risks and adaptation strategies. The advancement of quantum computing is expected to significantly impact currently deployed cryptographic systems, especially widely used asymmetric encryption methods. The presentation discusses the long-term nature of the quantum threat landscape and introduces the “harvest now, decrypt later” approach, which creates substantial risks for sensitive data requiring long-term confidentiality. In addition, the presentation highlights the importance of post-quantum cryptography and crypto-agile systems, as well as the preparedness challenges organizations are expected to face in the coming years. The second part of the presentation focuses on the cybersecurity aspects of artificial intelligence from both offensive and defensive perspectives. It presents current trends related to AI-assisted phishing campaigns, deepfake technologies, automated vulnerability research, and AI-driven malware development. At the same time, the presentation also addresses defensive applications of AI, including anomaly detection, spam and fraud filtering, and automated network traffic analysis. The presentation concludes that both quantum computing and artificial intelligence represent not only technological but also strategic challenges, requiring a new cybersecurity mindset and long-term preparedness.

Keywords: quantum computing, post-quantum cryptography, artificial intelligence, cybersecurity, deepfake, AI-driven attacks, crypto agility

BIBLIOGRAPHY

1. Nemzeti Kiberbiztonsági Intézet. (2025). Kvantumszámítógépen fut a DOOM? 1. rész [Podcast epizód] https://kibertamadas.simplecast.com/episodes/kvantum-szamitog-epen-fut-a-doom-1-vendegunk-dr-asboth-janos-orokzold
2. Nemzeti Kiberbiztonsági Intézet. (2025). Kvantumszámítógépen fut a DOOM? 1. rész [Podcast epizód] https://kibertamadas.simplecast.com/episodes/kvantumszamitoge-pen-fut-a-doom-2-vendegunk-dr-asboth-janos-orokzold
3. Nemzeti Kiberbiztonsági Intézet. (2024). Mesterséges intelligencia a kiberbűnözés szolgálatában – az AI-vezérelt adathalászat új korszakában. https://nki.gov.hu/it-biztonsag/hirek/mesterseges-intelligen-cia-a-kiberbunozes-szolgalataban-az-ai-vezerelt-adathalaszat-uj-korszaka/?utm_source=chatgpt.com
4. Google Cloud Threat Intelligence Blog (2025). Threat actor usage of AI tools for cyber operations. https://c-loud.google.com/blog/topics/threat-intelligence/threat-actor-usage-of-ai-tools?utm_source=chatgpt.com

3. DIGITAL INTEGRITY VS. MANIPULATED REALITY

PROTECT THE UNPROTECTABLE?

Zoltán Belinszki
PhD student, PTE, zbelinszki72@gmail.com

Abstract: Despite the continuous development of technology and tools, the tightening of regulations, and the steps aimed at making information security global, the protection of content posted on the Internet cannot be solved 100 percent. Self-restriction, i.e. filtering and reducing content shared on the World Wide Web, can work in many areas.

In the field of art, this choice is unacceptable. Creators would not only lose the opportunity for self-expression, but also a large part of their audience. A band cannot help but post a video of a new song on the Internet, lest others copy it and generate new songs from it, earning advertising revenue with the „new album". A fashion designer cannot help but publish his latest creation, lest unauthorized people make money from it under the pretext of fast fashion. A literary scholar cannot help but not publish his poem, lest he be seen as a Coelho meme.

Some artists use special software as legitimate self-defense in order to preserve their copyrights. Platform law has changed the paradigm: it forces large social platforms to take preliminary measures.

How can information security be increased int he field of art? Is global regulation an illusion or the only solution? Can the reinterpretation of other people's works be considered an independent work? The lecture will discuss topics affecting the sense of security of rights holders as the starting points for research assessing this.

Keywords: art, information security, copyright, ex ante

BIBLIOGRAPHY

1. Konrád, B. (2026): Another band has fallen victim to AI fraud on Spotify. www.dalszerzo.hu
2. Hohmann, B. (2025): Selected chapters from the field of European platform law. PTE ÁJK, Pécs
3. Pogácsás, A. – Újhelyi, D. (2025): Intellectual property law (2nd revised edition), Budapest, Pázmány Press, 2025

ONLINE SCIENTIFIC COMMUNICATION AS A CRITICAL DIGITAL TRUST INFRASTRUCTURE

László Berek
library director, Obuda University, berek.laszlo@uni-obuda.hu

Abstract: The scientific communication ecosystem now serves as a foundational trust infrastructure within digital society. Research outputs shape not only the scientific community but also exert direct influence on healthcare, energy systems, industry, education, and strategic and regulatory decision-making. Hence, the integrity and credibility of scientific communication have long been a matter of information security and societal trust, and not simply a purely academic matter.

Expanding upon these foundational concerns, this presentation analyzes how the rapidly evolving digital environment and the emergence of generative artificial intelligence have introduced new vulnerabilities into scientific publishing and communication systems. It examines threats to the credibility of scientific information, such as AI-generated scientific content, manipulated peer-review processes, citation manipulation, predatory journals, and the increasing influence of paper mill networks.

The presentation also frames the scientific publishing ecosystem as a complex digital supply chain, in which compromised or manipulated content may pose risks analogous to other forms of critical infrastructure. Scientific disinformation manipulated research findings, and AI-driven content generation may impact academic reputation, public trust, and policy decision-making.

In response to these identified risks, the presentation proposes institutional and information security strategies to safeguard the integrity of scientific communication. It emphasizes pre-submission manuscript screening models, AI-based detection solutions, methods for identifying predatory journals, and the critical role of university libraries and research support organizations in upholding scientific trust.

Keywords: Scientific communication, Digital trust, Information security, Generative AI, Research integrity, Predatory journals

BIBLIOGRAPHY

1. Berek, L. (2023). Researcher's Choice or Just a Necessity? The Consequences of Publishing in a Predatory Journal. Interdisciplinary Description of Complex Systems, 21(4), 324-332. https://doi.org/10.7906/indecs.21.4.1
2. Berek, L. (2025). Az egyetemi könyvtárak szerepe a tudományos kibocsátás biztonságában és az intézményi reputáció erősítésében. Safety and Security Sciences Review, 4(7), 1. https://doi.org/10.12700/btsz.2025.7.4.1
3. Berek, L. (2024). Artificial Intelligence-Generated Text in Higher Education—Usage and Detection in the Literature. Interdisciplinary Description of Complex Systems, 22(3), 238-245. https://doi.org/10.7906/indecs.22.3.1
4. Pierce, M. (2025). Academic Librarians, Information Literacy, and ChatGPT Sounding the Alarm on a New Type of Misinformation. College and Research Libraries News, 86(2), 68-70. https://doi.org/10.5860/crln.86.2.68
5. De, S., & Mondal, P. (2025). Assessing the Impact of Misinformation by Predatory Journals on Academic Integrity. Serials Librarian, 86(1-2), 17-28. https://doi.org/10.1080/0361526X.2025.2471922

THE BLIND SPOT OF CYBERSECURITY - INTERPRETIVE VULNERABILITY AS A STRUCTURAL RISK BEYOND TECHNICAL COMPLIANCE

Zsuzsa Gulyás
Lecturer, Gábor Dénes University, PhD Candidate, Faculty of Law, University of Pécs, MÉDÉSZ Researcher and Educational Development Specialist, gulyas.zsuzsa@medesz.hu

Abstract: Cybersecurity has long defined vulnerability within technical frames of reference, linking risk to system flaws, misconfigurations and attack surfaces. This perspective leaves a distinct layer unexamined, one that does not arise from system malfunction but from divergence in interpretation. This paper proceeds from the assumption that a considerable share of security incidents cannot be fully explained by technical failure. They emerge from discrepancies between regulatory prescriptions, operator understanding and the execution logic of automated systems. Within this configuration, vulnerability is not confined to code but manifests at the level of meaning. The analysis introduces interpretive vulnerability as a structural category of risk that forms at communicative boundaries. These boundaries extend beyond the interface between human and system and include divisions across organisational units, professional frameworks and normative expectations. Under such conditions, security cannot be reduced to technical compliance but depends on the maintenance of interpretive coherence. The paper contends that prevailing cybersecurity practices render certain risks visible while systematically obscuring others. Without the capacity to identify interpretive divergence, interventions remain confined to symptomatic correction and fail to address the underlying sources of disruption.

Keywords: sInterpretive vulnerability, cybersecurity, semantic risk, organisational communication, compliance, human–machine interaction, interpretive divergence, structural risk, meaning intelligence, MÉDÉSZet

BIBLIOGRAPHY

1. Bada, M., Sasse, M. A., & Nurse, J. R. C. (2019). Cybersecurity awareness campaigns. ACM Computing Surveys, 52(4).
2. ENISA. (2023). Threat landscape report. European Union Agency for Cybersecurity.
3. Floridi, L. (2022). Ethics of information. Oxford University Press.
4. Kiss, A. (2022). Kiberbiztonság és humán tényezők. Hadmérnök, 17(2).
5. NIST. (2020). Cybersecurity framework. National Institute of Standards and Technology

THE DARK SIDE OF THE AI PIPELINE: CYBERSECURITY THREATS IN THE MODELING PROCESS

Csaba Irányi
Machine Learning Engineer, e-Corvina Ltd., csaba.iranyi@gmail.com

Abstract: The lecture will examine the cybersecurity aspects of machine learning modeling across the entire AI lifecycle, from data processing in local environments through cloud-based training to production deployment. Its central argument is that the data science and modeling pipeline is not merely a vehicle of technological innovation, but also a broad attack surface in which data, models, software components, and services can all become targets. The presentation will address attacks against sensitive data, including personal, health-related, classified, and proprietary business information, and will show how large-scale, temporally distributed data transfers and archiving processes can create difficult-to-detect risks of data leakage and unauthorized access. It will also explore different forms of data poisoning: how datasets collected from open sources, acquired from vendors, or generated internally may be distorted, and how mislabeling, bias, manipulated associations, and hidden intent can emerge within training data. Special attention will be given to the vulnerabilities of transfer learning and fine-tuning, including the modification of foundation models, the insertion of hidden triggers, and the dangers posed by deceptive or counterfeit public model repositories. The lecture will further discuss model theft, the manipulation of weights and parameters, and supply chain attacks targeting frameworks, APIs, notebooks, plugins, and open-source libraries. Finally, the compromise of cloud services, risks associated with multi-tenant environments, and denial-of-service attacks will illustrate the financial, reputational, and legal consequences that define the real threat landscape in which modern AI systems must operate.

Keywords: machine learning, cybersecurity, data poisoning, cloud security, model integrity

BIBLIOGRAPHY

1. Gu, T., Dolan-Gavitt, B., Garg, S. (2019). BadNets: Identifying Vulnerabilities in the Machine Learning Model Supply Chain. New York University. https://doi.org/10.48550/arXiv.1708.06733
2. Eykholt, K., Evtimov, I., Fernandes, E., Li, B., Rahmati, A., Xiao, Ch., Prakash, A., Kohno, T., Song, D. (2018). Robust Physical-World Attacks on Deep Learning Models. University of Michigan. https://doi.org/10.48550/arXiv.1707.08945
3. Madry, A., Makelov A., Schmidt L., Tsipras D., Vladu A. (2019). Towards Deep Learning Models Resistant to Adversarial Attacks. MIT. https://doi.org/10.48550/arXiv.1706.06083

MODERNISING THE MEASUREMENT OF INFORMATION SECURITY AWARENESS THROUGH LARGE-SAMPLE EMPIRICAL VALIDATION

Pál Károly Laska
Ph.D. Student, NKE, laska.pal.karoly@uni-nke.hu

Abstract: Approximately three-quarters of cybersecurity incidents can be traced back to the human factor, making the objective measurement of human security awareness a key issue of cyber resilience. The most widely applied instrument in the international literature, the HAIS-Q (Human Aspects of Information Security Questionnaire), is, however, no longer capable of keeping pace with the changes of the digital environment — the new challenges posed by artificial intelligence, cloud-based services, IoT devices, and modern authentication solutions. Our research therefore aimed to develop and validate a new measurement instrument, the SAM (Security Awareness Model).

Within the framework of contingency theory, SAM builds upon the foundations of HAIS-Q while significantly expanding and modernising it. The model operationalises information security awareness across seven focus areas (authentication, internet services, information management, device use, incident management, regulation, and awareness) and ten dimensions, following the Knowledge–Attitude–Behaviour (KAB) approach, through a 120-item questionnaire structured as a hierarchical formative measurement model.

The empirical validation of the model was conducted through two large-sample, nationally representative data collections: residential (n = 3,144) and corporate (n = 2,184) populations, using IPF weighting and Partial Least Squares Structural Equation Modelling (PLS-SEM) in SmartPLS. The reliability of the dimensions proved adequate (Cronbach's $\alpha > 0.8$). Our findings refute several stereotypes: high knowledge alone does not lead to security-aware behaviour — the strongest effect is linked to attitude ($\beta = 0.769$), which plays both a mediating and moderating role; the older age group is objectively more aware than digital natives; and SME employees underestimate their own level of awareness. The effect of income is only indirect, primarily mediated through educational attainment.

The SAM model is suitable for longitudinal measurement, profiling, identification of risk zones, and the documentable assessment of human-related requirements of ISO/IEC 27001, NIS2, and GDPR. The practical implication of the research: the key to effective prevention lies not in knowledge transfer, but in attitude-shaping, experience-based, and gamified interventions.

Keywords: Security Awareness Model, information security awareness, HAIS-Q, KAB model, PLS-SEM, cyber resilience

BIBLIOGRAPHY

1. Bak, G., Berek, L., Som, Z., Ujhegyi, P., & Répás, J. (2024). On the way to updating the measurement of information security awareness: A literature analysis. Interdisciplinary Description of Complex Systems, 22(3), 305–316.
2. Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. Computers & Security, 66, 40–51. https://doi.org/10.1016/j.cose.2017.01.004
3. Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). Computers & Security, 42, 165–176. https://doi.org/10.1016/j.cose.2013.12.003
4. Hermawan, D. S., Setiadi, F., & Oktaria, D. (2022). Measurement level of information security awareness for employees using KAB model with study case at XYZ agency. In 2022 1st International Conference on Software Engineering and Information Technology (ICoSEIT) (pp. 174–179). IEEE. https://doi.org/10.1109/ICoSEIT55604.2022.10029989

FSFT2026

THE FUTURE OF SECURITY
THE FUTURE OF TRUST


DENNIS GABOR
UNIVERSITY
DIGITAL HORIZONS