HADMÉRNÖK

Kiemelt közlemények

Horváth János, Horváth Zsuzsa: *Bolygóvédelem és NEO-kockázatok*

Kirovné Rácz Réka Magdolna, Scholtz Emánuel István: *A mesterséges intelligencia és gépi tanulás algoritmusainak alkalmazása a hidrológiai katasztrófák elleni védekezésben*

Pozderka Gábor: *A kibervédelmi és kiberműveleti gyakorlatok rendszerének átalakulása, az aktuális kihívások vizsgálata*

20. évf. (2025)
4. szám

ISSN 1788-1919 (elektronikus)

LUDOVIKA
EGYETEMI KIADÓ

IMPRESSZUM

Hadmérnök
Katonai műszaki tudományok online folyóirata
ISSN 1788-1919 (elektronikus)

Nemzeti Közszolgálati Egyetem
1101 Budapest, Hungária krt. 9–11.
Postacím: 1581 Budapest, Pf. 15.
„A” épület 9. emelet, 901. iroda
Telefon: +36-1-432-9000/29-289, Fax: +36-1-432-9025
E-mail: hadmernok@uni-nke.hu
Web: https://folyoirat.ludovika.hu/index.php/hadmernok

Kiadó
Nemzeti Közszolgálati Egyetem Ludovika Egyetemi Kiadó
Székhely: 1083 Budapest, Ludovika tér 2.
Kapcsolat: www.ludovika.hu; kiadvanyok@uni-nke.hu
A kiadásért felel: Deli Gergely rektor
Olvasószerkesztők: Bujdosó Hajnalka, Resofszki Ágnes

Tartalom

Védeleminformatika

Gábor Farkas: *Electronic Warfare Framework* 5

Károly Kassai: *Cybersecurity Challenges of the Integration of Artificial Intelligence (AI) Solutions* 17

Zoltán Kovács: *The Use of Artificial Intelligence in Cyberattacks, Part 1* 39

Zoltán Kovács: *The Use of Artificial Intelligence in Cyberattacks, Part 2* 53

Pozderka Gábor: *A kibervédelmi és a kiberműveleti gyakorlatok rendszerének átalakulása, az aktuális kihívások vizsgálata* 69

Tóth Ádám: *Zero trust network access az ipari (OT) kiberbiztonságban.* 87

Környezetbiztonság

Horváth János, Horváth Zsuzsa: *Bolygóvédelem és NEO-kockázatok* 103

Kirovné Rácz Réka, Scholtz Emánuel: *A mesterséges intelligencia és gépi tanulás algoritmusainak alkalmazása a hidrológiai katasztrófák elleni védekezésben* 125

Sibalin Iván, Kátai-Urbán Maxim, Cimer Zsolt: *Az energiaipari-biztonság és a környezeti fenntarthatóság egyes összefüggéseinek értékelése, 1. rész.* . . . 149

Védelemgazdaság

Szöllősi Annamária: *Az innováció mint stratégiai fegyver* 161

HADMÉRNÖK
VÉDELEMINFORMATIKA
20. évfolyam (2025) 4. szám 5–16.
DOI: 10.32567/hm.2025.4.1

Gábor Farkas[1]

Electronic Warfare Framework

An Approach to Accelerate Research and Development

Abstract

The increasing dependence of modern societies and military operations on radio frequency-based and networked systems has made the electromagnetic spectrum a critical operational domain. Electronic warfare capabilities must therefore evolve toward more adaptive and rapidly deployable solutions. This article addresses the challenge of accelerating electronic warfare related research and development by introducing a compact, modular framework that enables efficient testing and validation of signal processing and machine learning-based detection algorithms in real-world conditions. To achieve this, comparison of possible technologies and architecture was made to select the optimal components. The proposed system combines a software-defined radio and an embedded processing unit to create a field-deployable platform for radio frequency signal collection, analysis and countermeasure evaluation. The framework's functionality was demonstrated through an FPV drone detection use case, where video signals transmitted by a drone were successfully identified and disrupted.

Keywords: electronic warfare, ESM, software-defined radio, machine learning, CUAV, FPV drone

Introduction

Information technology has become an integral part of modern society, fundamentally shaping daily life and global operations. The interconnection of billions of electronic devices like computers, mobile phones, and IoT (Internet of Things) systems has created a new operational domain commonly referred to as cyberspace. Instant data

[1] PhD student, Ludovika University of Public Service, Doctoral School of Military Engineering, e-mail: farkas.gabor.csp@gmail.com

exchange within this environment enables rapid development in numerous fields, including financial services, remote monitoring of critical infrastructure and social communication. However, this heavy dependence on cyberspace also introduces vulnerabilities, for example any disruption or sabotage of these services can have serious social, economic or even military consequences.[2] In the field of defence and EW (electronic warfare), ESM (electronic support measures) plays a central role in understanding, monitoring and controlling the electromagnetic environment.[3] My research focuses on exploring the applicability of ML (machine learning) methods within this domain. Specifically, evaluating different ML models to determine which are most suitable for various signal processing tasks. The primary objective is to automate the detection and classification of specific RF (radio frequency) signals, thereby enhancing the ability to respond quickly and effectively to emerging threats.[4]

A key consideration in my work is embedded applicability. Any proposed detection method should not only be accurate, but also computationally efficient enough to operate on compact, low-power devices suitable for field use. Therefore, both algorithmic performance and hardware resource requirements are carefully evaluated. To validate detection methods, I implemented them on physical hardware, consisting of an SDR (software-defined radio) and an embedded computer unit. Although this setup has proven effective in laboratory conditions, field deployment revealed limitations in portability and usability. To overcome these issues, I designed a modular EW framework. A compact, flexible platform that supports on-field experimentation and real-time testing. Such equipment not only accelerates research but also enables rapid capability development, which is critical when facing dynamic or unpredictable threats. The Russian–Ukrainian conflict has provided several examples of rapid technological adaptation, such as the deployment of improvised drones within days of the beginning of hostilities, highlighting the importance of adaptable research platforms.[5]

This article presents the design and validation of the proposed EW framework. It begins with the fundamental considerations behind the framework's architecture and the selection of its main components, including the SDR and signal processing unit. The subsequent sections describe the system's construction, followed by a real-world test scenario focusing on FPV (first person view) drone detection. The expected outcome is a practical, adaptable EW platform that not only supports ongoing research into ML-based signal processing but also provides a foundation for accelerated R&D (research and development) and hands-on education in the field of electronic warfare.

The fundamentals of the framework

As for basic elements, the framework needs to include an SDR and a signal processing unit as shown in Figure 1. In this scenario there is a single RX (receiver) antenna for capturing RF signals. Without going into details, basically the RF tuner will amplify,

[2] Haig 2021: 91.
[3] Németh–Virágh 2023: 3.
[4] Farkas et al. 2025.
[5] Olloy 2024: 17.

down-mix and filter the received stream. Then the ADC (analogue-to-digital converter) will convert it to a digital representation that will source the signal processing unit. The signal processing unit should be capable of running ML models. This can be implemented into an MCU (micro-controller), an FPGA (field programmable gate array) or a PC (personal computer).[6] The result is then handled by the result logic. At this point we can do many things with the gathered information. It is possible to display the results or transfer them for further analysis over the user interface. Further on, the results can be used to control the SDR, therefore make it possible to achieve swiping or signal following functionality.[7]

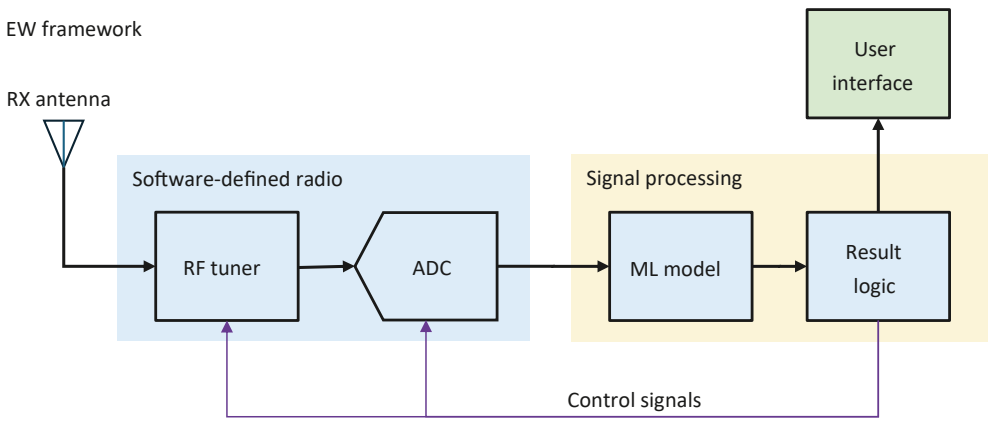


Figure 1: Basic concept of the EW framework, including an SDR and a signal processing unit

Note: The control signal feedback makes it possible to automatically control the SDR based on the results. An additional user interface is added to have control over the results.

Source: compiled by the author

The diagram of the framework gives an overview of the major components, but further investigation needs to be done to select the exact parts to be used. The overall data throughput required will outline the minimum requirements and help in selecting the right platform.[8]

Software-defined radio

The SDR device fundamentally determines the RF capability of the EW framework. Its frequency coverage, instantaneous bandwidth, dynamic range and transmit capability set the envelope of what can be observed, recorded and tested. Therefore, before selecting an SDR we must define the target signal types, the carrier bands of

[6] Branco et al. 2019: 1–5.
[7] Şorecău 2025.
[8] Farkas 2024.

interest, required instantaneous bandwidth, and the deployment constraints, like size, weight, power and cost.

For the current study the primary detection target is the VTX (video transmitter) used on FPV drones. VTX signals are practical detection targets for several reasons. They are typically transmitted with relatively high RF power compared to low-power control links, occupy relatively wide analogue or digital video bandwidths, and their signal strength increases as the drone approaches. Observations of FPV usage in recent conflicts indicate that the majority of COTS (commercial off-the-shelf) VTX hardware operates in the 1.2 GHz and 5.8 GHz ISM (industrial, scientific and medical) band with selectable power levels from ~10 mW up to 800–2000 mW. Representative product specifications are summarised in *Table 1*.

Table 1: Working frequency range and transmitter power of VTXs commonly used in the Russian–Ukrainian war

Device	Typical frequency band	Max. TX power
TBS Unify Pro 5G8 V3[9]	5.8 GHz	800 mW
Eachine TX805S[10]	5.8 GHz	1.6 W
RushFPV Tank Solo[11]	5.8 GHz	1 W
HumbirdTec 1G3TE-V2[12]	1.2 GHz	2 W
DarwinFPV 1.2G 1.6W VTX[13]	1.2 GHz	1.6 W

Source: compiled by the author

Given the target frequency band centred around 1.2 GHz and 5.8 GHz, and the requirement to detect relatively wideband video carriers, four practical constraints follow:

- Frequency coverage: The SDR must at minimum cover the 1.2 GHz and 5.8 GHz FPV bands. Preferably other bands too to allow future expansion
- Instantaneous/baseband bandwidth: For analogue video pattern recognition a modest sample rate of 1 MSPS (mega-sample per second) is generally sufficient for initial detection. Higher sample rates will be required for raw-capture, complex demodulation or multiple-channel monitoring
- Portability and power: The framework is intended for field tests and mobile deployment, so small form factors and modest power draw are critical design drivers
- Ease of development: Research throughput is accelerated by a platform that supports high-level development and rapid prototyping (Python, GNU Radio, standard toolchains)

To make an informed selection I compared three widely available SDRs that are commonly used in research and field-deployable setups. The Ettus USRP B210, the

[9] See the manual *TBS Unify Pro 5G8 (HV) Video Transmitter* 2018.
[10] *Eachine TX805S Transmitter Product Instruction Manual* [s. a.].
[11] *RUSHFPV Tank Solo User Manual* [s. a.].
[12] *HumbirdTec VTX-1G3TE* [s. a.].
[13] *DarwinFPV 1.2G 1.6W VTX* [s. a.].

HackRF One R9, and the RTL-SDR Blog V4 dongle. Their summarised characteristics are presented in Table 2.

Table 2: Comparing features of selected SDRs

SDR type	Frequency coverage	Max. sample rate	Notes
Ettus USRP B210[14]	70 MHz – 6 GHz Dual Rx/Tx channels	56 MSPS	High dynamic range, excellent front end and sensitivity FPGA is available for custom processing
HackRF One R9[15]	1 MHz – 6 GHz Half-duplex single channel	20 MSPS	Moderate sensitivity for general use Transceiver (TX/RX) capable 8-bit I/Q Good community support
RTL-SDR Blog V4[16]	500 kHz – 1.766 GHz Only RX, single channel	3.2 MSPS	Low cost; receive-only Limited bandwidth and dynamic range compared to HackRF and USRP

Source: compiled by the author

For a field-deployable EW framework to detect FPV drone VTXs, support embedded testing, be compact and battery-operable and accelerate iterative R&D, HackRF One represents a reasonable compromise:

- Frequency coverage from 1 MHz to 6 GHz comfortably includes the 1.2 GHz and 5.8 GHz bands and allows future expansion into other bands without hardware change
- RX and TX (transmit) capability enables not only passive detection but also controlled active tests in lab conditions
- Baseband throughput up to 20 MSPS is more than sufficient for the 1 MSPS pattern recognition requirement I described, while still permitting higher-rate captures for analysis when necessary
- SWaP (size, weight and power) and cost favour HackRF over a USRP B210. HackRF is smaller, cheaper and easier to integrate in a mobile enclosure. It also gives rapid software prototyping via GNU Radio and Python

A practical caveat is that HackRF's ADC resolution and front-end filtering make its absolute sensitivity and dynamic range lower than Ettus USRP devices. Later on, if required to maximise detection range or operate in extremely congested RF environments, a higher-performance transceiver should be considered. For an R&D and field-trial platform where rapid iteration and portability matter, HackRF One is an optimal choice.

[14] *Ettus USRP B210* [s. a.].
[15] HackRF documentation: https://hackrf.readthedocs.io/en/latest/index.html
[16] See: www.rtl-sdr.com/about-rtl-sdr

Signal processing unit

After the radio front-end and data acquisition functions are realised by the Software Defined Radio (SDR), the next essential stage in the framework is the signal processing unit. While the SDR is responsible for digitising the received radio frequency (RF) spectrum and forwarding the sampled data, the processing unit interprets this information to identify relevant patterns or potential threats. The efficiency and accuracy of this step depend largely on the computing architecture used, as it must balance high computational demand with low power consumption and real-time responsiveness. Therefore, the selection of an appropriate processing platform is a critical design decision in building a deployable EW framework.

For signal processing tasks, a wide range of computing platforms can be utilised. The goal of my work is to identify the most suitable technological direction that provides an optimal balance between computational performance, energy consumption and development complexity. In this study, four hardware architectures were examined: FPGA, CPU (Central Processing Unit), GPU (Graphics Processing Unit), and ASIC (Application-Specific Integrated Circuit). Their relative computational capacity and power demand are illustrated in Figure 2.[17]

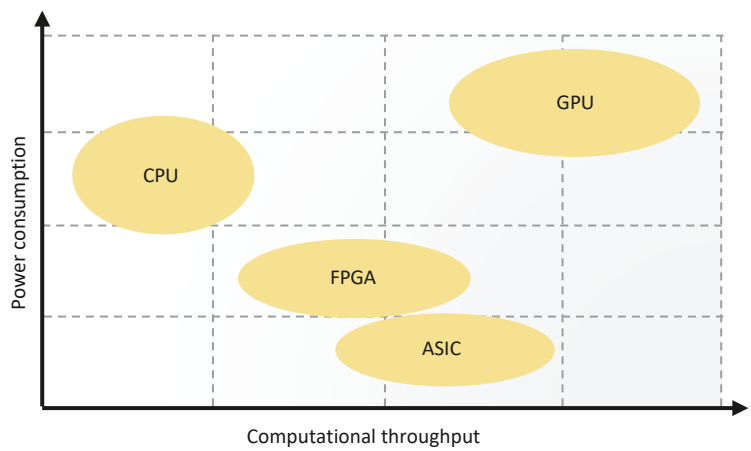


Figure 2: Comparison of power consumption and throughput of different technologies
Source: compiled by the author

Each architecture offers distinct advantages and limitations:

- FPGA: These devices provide highly parallel and deterministic processing, making them ideal for low-latency signal processing applications such as real-time demodulation or protocol decoding. However, FPGA development requires specialised knowledge of hardware description languages (HDL) and toolchains, which significantly increases development time. Although their energy efficiency is excellent, their flexibility is limited once the logic has been synthesised.

[17] Zhang 2019: 49.

- CPU: Traditional processors offer great flexibility and ease of programming, with extensive software support and mature development environments. While CPUs generally provide lower raw processing throughput compared to GPUs or FPGAs, they remain sufficient for a wide range of signal processing tasks when paired with efficient algorithms and optimised libraries. Their low power consumption and compact form factor make them particularly suitable for mobile and embedded EW applications.
- GPU: Designed for massive parallel computation, GPUs deliver extremely high performance for data-intensive operations such as deep learning or spectral analysis. However, their high energy demand and typically bulky thermal management requirements limit their use in field-deployable systems. In addition, GPU programming, while more accessible today through CUDA or OpenCL, still requires specific expertise and careful optimisation to achieve full performance.
- ASIC: These are custom-designed chips optimised for a specific task, providing unmatched energy efficiency and performance once manufactured. Nevertheless, the extremely high development cost and lack of reconfigurability make ASICs impractical for research and prototyping, especially in fast-changing electronic warfare environments where adaptability is critical.

The comparison clearly shows that no single architecture is universally superior. The optimal choice depends on the operational context and design priorities. In my research, the CPU-based approach has been selected, specifically implemented using the Raspberry Pi platform. This decision was guided by the following considerations:

- Low power consumption: Suitable for mobile and battery-powered field applications
- Compact design: Easily integrates with SDR hardware
- Ease of programming: Supports high-level languages such as Python, enabling rapid prototyping and flexible model deployment
- Adequate performance: Sufficient computational capacity to execute machine learning-based signal detection in real time

By utilising the Raspberry Pi as the signal processing unit, the framework achieves an effective balance between performance, energy efficiency and portability, while maintaining the flexibility necessary for rapid research and development cycles.

Construction

After selecting the two core components, the Raspberry Pi as the signal processing unit and the HackRF One as the SDR transceiver, the next objective was to design a compact and field-deployable EW platform that constitutes the hardware foundation of the proposed framework. The assembled system aims to serve as both a research platform and a functional prototype, capable of real-time signal collection, analysis and active testing in realistic environments.

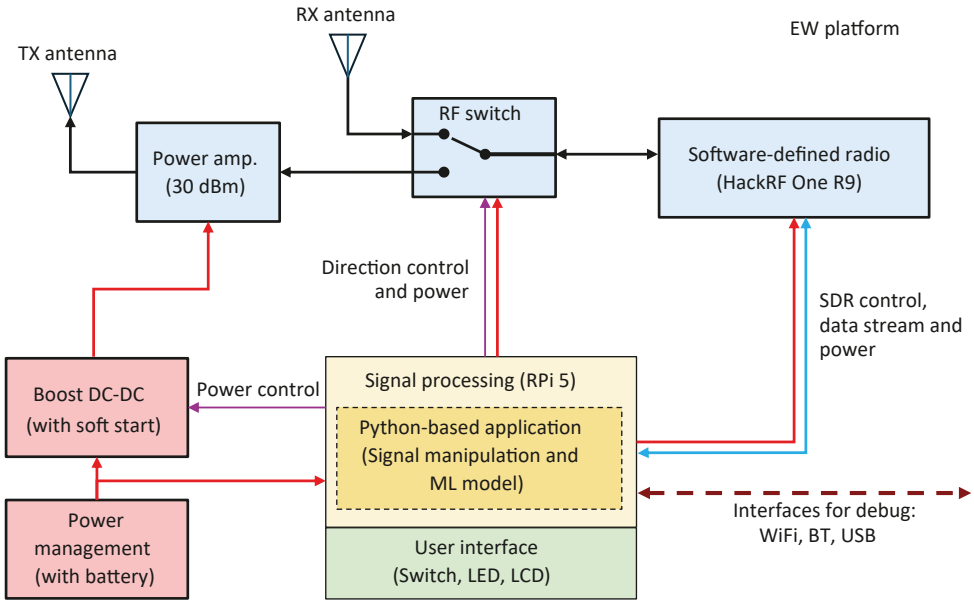


Figure 3: Block diagram of the EW platform, including SDR, signal processing CPU, power management and additional RF components

Source: compiled by the author

A high-level block diagram of the platform is presented in Figure 3. The system consists of several interconnected modules, each fulfilling a distinct role in the overall architecture.

- Software-Defined Radio (HackRF One R9): Operates as the RF front end, responsible for capturing and transmitting signals within the 1 MHz to 6 GHz frequency range. Because HackRF operates in half-duplex mode, an RF switch is included to alternate between transmit and receive paths.
- Signal Processing Unit (Raspberry Pi 5): Acts as the central control and signal processing node. It runs the machine learning algorithms responsible for detection and classification, provides the user interface, and manages communication between subsystems. The Raspberry Pi is equipped with a small touch LCD display, which allows real-time debugging, visual feedback and configuration during field tests.
- RF Power Amplifier (PA): The transmit chain includes a broadband power amplifier with an output power of approximately 30 dBm. While it can support general tasks such as signal emulation, system calibration and active testing, its primary purpose within the EW framework is to enable controlled jamming experiments.
- Power Management System: The entire setup is powered by an integrated battery pack with onboard power regulation. Between the main power system and the RF amplifier, a Boost DC-DC converter with a soft-start function is implemented to provide the required 12 V rail for the amplifier while avoiding current surges at startup. The remaining modules are powered from the regulated low-voltage outputs of the power pack.

- User Interface and Indicators: To support standalone operation and quick situational awareness, three status LEDs are installed: green for system power, yellow for warnings or system activity, and red to indicate transmitter operation. A small buzzer provides audible feedback for system events or alerts. The transmit function can be manually enabled or disabled using a dedicated hardware switch, ensuring safe and controlled RF emission during testing.

The mechanical layout emphasises compactness and ease of integration. All modules are mounted within a lightweight enclosure that provides sufficient shielding between the RF and digital sections. The resulting unit can operate autonomously in the field or be connected to a development workstation for debugging and data analysis.

Functionally, the Raspberry Pi serves as the core development platform, allowing to deploy, test and refine signal processing algorithms or trained neural networks directly on hardware. Because the setup combines SDR flexibility, embedded processing and local user interaction, it effectively bridges the gap between simulation environments and real-world EW testing. As my research primarily focuses on AI-assisted RF signal processing, the constructed equipment enables both RF data collection and on-site validation of developed detection and classification models. This dual-use capability accelerates the research cycle and supports iterative model improvement based on real signal conditions.

In summary, the constructed EW equipment represents a compact, modular, and energy-efficient platform suitable for both laboratory research and field deployment. Its architecture allows rapid reconfiguration of the SDR and processing algorithms, supporting a wide range of experiments from passive signal monitoring to active transmission tests. The integration of an embedded processing unit, power management and intuitive user interface ensures autonomous operation without external peripherals. These characteristics make the system an ideal testbed for validating machine learning-based signal processing approaches under realistic conditions.

Real-life scenario

As an initial validation of the developed EW framework, a practical FPV drone detection and countermeasure scenario was implemented. The objective was to identify approaching FPV drones based on their VTX signals and to test the operational effectiveness of the hardware setup in real conditions. The applied detection method is based on our previously published study.[18] In this implementation, the SDR continuously samples short segments of the RF spectrum over selected frequency bands where FPV VTX signals are typically found. The sampling rate is intentionally kept low to minimise computational load, while still preserving enough temporal and spectral resolution to reconstruct a coarse representation of the transmitted video waveform. Rather than performing full colour or frame decoding, only the signal structure is analysed to determine whether it corresponds to a composite video signal or not.

[18] Farkas et al. 2025: 2–7.

An autocorrelation-based detection algorithm is currently applied. This method identifies the repetitive frame patterns characteristic of analogue FPV video transmissions. When a potential FPV video signal is detected, the system provides audio and visual feedback:

- The LCD display and LEDs indicate a detection event
- An acoustic warning is generated through the buzzer
- The SDR locks onto the detected frequency for further observation

Once a detection is confirmed, the operator can manually activate the jammer. In this mode, a narrowband interference signal, approximately with 100 kHz bandwidth that is significantly narrower than the video channel, is transmitted through the RF power amplifier. The intention is to disrupt the drone operator's video link by injecting localised interference, effectively blinding the drone operator, and potentially causing to lose control over the drone or abort the mission. The final platform with a rugged enclosure is demonstrated in Figure 4.

Figure 4: Realised EW platform in a rugged enclosure for field testing
Source: compiled by the author

Field tests demonstrated that the detection and jamming functionality works effectively in the 1.2 GHz band, achieving reliable detection within 100–300 meters, depending on environmental conditions and the transmitter's output power. However, due to the reduced sensitivity of HackRF One in the 5.8 GHz range, the detection range at

that band is limited to approximately 10 meters. For extended-range detection in the 5.8 GHz band, employing a USRP B210 or a comparable high-sensitivity SDR would be a suitable improvement.

Future work will focus on replacing the current autocorrelation-based approach with a neural network-based detection algorithm, leveraging CNNs (convolutional neural networks) trained on real RF samples. The constructed EW platform and framework will be used to collect, label and process these training datasets, enabling the development of more robust and adaptive detection models. This way the framework will not only serve as an operational tool but also as a scalable R&D platform for AI-driven EW applications.

Conclusion

The original objective of my research was to accelerate EW research and development by designing a modular and field-deployable framework that enables rapid testing of signal processing algorithms and embedded implementations. The motivation arose from the increasing complexity of the electromagnetic environment, the proliferation of unmanned aerial systems and the growing reliance on real-time situational awareness in modern conflicts. Detecting, classifying and responding to different RF emissions requires a flexible, scalable, and hardware-validated approach. To address these challenges, an EW framework concept was developed that combines SDR technology with embedded signal processing on a compact computing platform. The article presented the logical build-up of this framework, including the selection and comparison of hardware components, system integration and functional validation.

In the first stage, various SDR platforms were evaluated based on frequency coverage, bandwidth, sensitivity, power consumption and cost. HackRF R9 was selected as the most balanced solution for field research, offering sufficient performance and flexibility at a moderate cost and size. For signal processing, four processing were analysed, and the Raspberry Pi was chosen as the processing unit due to its low power demand, small form factor and ease of software development in Python. A compact EW prototype was then constructed. The resulting equipment supports both passive monitoring and active transmission, and it is suitable for mobile field tests.

To validate the framework, a real-life FPV drone detection scenario was implemented. The system successfully detected analogue and digital FPV video signals using an autocorrelation-based algorithm, providing visual and acoustic alerts and enabling manual activation of a narrowband jammer. The experiment demonstrated the feasibility and operational readiness of the concept for short-range detection and countermeasure testing.

Beyond the immediate results, the developed EW framework has broader implications. It provides a research and educational platform that can be easily adapted for various signal analysis tasks, machine learning experiments, or system demonstrations. Future work will focus on implementing neural network-based signal classification, expanding detection range with higher-sensitivity SDRs, and refining power management for extended autonomous operation. In summary, the presented

work delivers a functional and adaptable electronic warfare research platform that bridges the gap between laboratory simulations and field-ready experimentation. By combining flexible SDR technology, embedded computing and AI-based signal processing, the framework contributes to faster prototyping, better adaptability and improved response capability in future EW system development.

References

Branco, Sérgio – Ferreira, André G.– Cabral, Jorge (2019): Machine Learning in Resource-Scarce Embedded Systems, FPGAs, and End-Devices: A Survey. *Electronics,* 8(11). Online: https://doi.org/10.3390/electronics8111289

DarwinFPV 1.2G 1.6W VTX [s. a.]. Online: https://darwinfpv.com/products/darwinfpv-fpv-drone-replaces-matek-1-2g-1-3g-1-6w-vtx

Eachine TX805S Transmitter Product Instruction Manual [s. a.]. Online: https://manuals.plus/wp-content/sideloads/eachine-tx805s-transmitter-manual-original.pdf

Ettus USRP B210 [s. a.]. Online: www.ettus.com/all-products/ub210-kit/

Farkas, Gábor (2024): SDR-adatfolyam feldolgozása korszerű módszerekkel. *Hadmérnök,* 19(2), 87–95. Online: https://doi.org/10.32567/hm.2024.2.7

Farkas, Gábor – Fazekas, Gábor – Németh, András (2025): FPV-drónok detektálásának alternatív megoldása konvolúciós neurális hálózattal. *Haditechnika,* 59(2), 2–7. Online: http://doi.org/10.23713/HT.59.2.01

HackRF documentation. Online: https://hackrf.readthedocs.io/en/latest/index.html

Haig, Zsolt (2021): Relationships between Cyberspace Operations and Information Operations. *Advances in Military Technology,* 16(1), 91–105. Online: https://doi.org/10.3849/aimt.01466

HumbirdTec VTX-1G3TE [s. a.]. Online: https://prom.ua/m-687057894700745642 8-fpv-videoperedatchik-humbirdtec.html

Németh, András – Virágh, Krisztián (2023): Mesterséges intelligencia és haderő – További katonai alkalmazási lehetőségek VIII. rész. *Haditechnika,* 57(2), 2–5. Online: https://doi.org/10.23713/HT.57.2.01

Olloy, Oleksandra (2024): *Drones in Modern Warfare: Lessons Learnt from the War in Ukraine.* Australian Army Occasional Paper No. 29. Online: https://doi.org/10.61451/267513

RUSHFPV Tank Solo User Manual [s. a.]. Online: https://distributions.com.ua/files/Istrukciya_RUSH-DA14_Pryami_dysstrybucii.pdf

RTL-SDR product page. Online: www.rtl-sdr.com/about-rtl-sdr/

Șorecău, Mirela et al. (2025): *Enhanced RF Spectrum Monitoring with SDR-Based Frequency-Sweep Methods.* 2025 International Symposium on Electromagnetic Compatibility – EMC Europe, Paris, France. Online: https://doi.org/10.1109/EMCEurope61644.2025.11176413

TBS Unify Pro 5G8 (HV) Video Transmitter (2018). Online: www.team-blacksheep.com/media/files/tbs-unify-pro-5g8-manual.pdf

Zhang, Qianru et al. (2019): Recent Advances in Convolutional Neural Network Acceleration. *Neurocomputing,* 323, 37–51. Online: https://doi.org/10.1016/j.neucom.2018.09.038

HADMÉRNÖK
VÉDELEMINFORMATIKA

20. évfolyam (2025) 4. szám 17–38.
DOI: 10.32567/hm.2025.4.2

Károly Kassai[1]

Cybersecurity Challenges of the Integration of Artificial Intelligence (AI) Solutions

Military Requirements, Question Marks and Efforts

Abstract

The applicability of artificial intelligence (AI) is no longer in question today. AI has become so integrated into countless areas of the economy and society that we no longer even notice that a given service is provided by an AI system. The use of AI systems is a sensitive issue in many areas, such as the armed forces. This paper draws attention to the diversity of military applications of AI and the general risks involved. The armed forces need to use not just one or two AI systems, but dozens of AI solutions that must be integrated into military information systems. These AI systems perform tasks at different operational levels or support the operation of other systems.

The study provides guidance on the most important steps in the necessary risk management, based on the legal framework, standards and best practices. Tailored risk management provides the basis for local, system-specific regulation of military organisations, which must be compiled from existing cybersecurity framework elements. The study emphasises that AI systems cannot be exempt from cybersecurity regulations, so it is necessary to review and supplement existing tools and provide training.

Keywords: artificial intelligence (AI), military information system, cybersecurity, trustworthiness, risk

[1] Section Head, Ludovika University of Public Service, Faculty of Military Science and Officer Training, Department of Military National Security, e-mail: karoly.kassai@yahoo.com

Introduction

Artificial intelligence (AI) is introducing new military capabilities and augmenting existing ones at *strategic, operational* and *tactical* levels. Military organisations operate a diverse ecosystem of AI systems and AI-supported services that must interoperate with legacy platforms, communications networks and each other.

Some systems deliver advanced technical effects through speed, scale and precision; others collect and analyse critical operational data and sensitive tactical sensor streams, contribute to strategic decision preparation, or support decisions where errors can cause military operational disadvantage, injury or serious damage.

This complexity creates new design, operational and governance challenges for military information systems.

We can recognise that, alongside these characteristics, the situation is further complicated by the fact that cybersecurity considerations are an integral part of integrating AI into the military information environment.

A dedicated literature review shows that AI-related issues are receiving growing attention within military science. Hungarian scholarship documents the evolution of AI technologies,[2] illustrates the diversity of military AI system solutions (dozens of land, air and naval devices).[3]

Broader reviews of AI and other disruptive technologies emphasise the need for holistic perspectives and illustrate diverse applications (for example, healthcare; education; energy; finance; supply chains; social media; law enforcement; intelligence). Those studies also highlight legal, ethical, economic and social implications and governance challenges such as oversight and control.[4]

Another Hungarian study examines AI's military application within intelligence branches, exploring analytic and evaluative capabilities in this sensitive domain.[5]

A dedicated Hungarian volume examines AI's social and ethical impacts; general regulatory and legal issues (robot law and human rights); data protection and communications; and economic considerations.[6]

Alongside these extensive, high-level studies, domain-specific functional examinations also exist that address security in various formulations. However, such works treat cybersecurity and operational security issues *only marginally*.

This paper pursues two objectives. The primary research objective is to review and compare regulatory and governance elements from policy domains analogous to AI (for example, cybersecurity, data protection, critical infrastructure protection, classified information protection) to identify institutional functions and pillars that support AI safety and security, without performing a formal legal analysis.

The practical research objective is to synthesise cybersecurity considerations for AI as an information system to support organisational implementation and strategic risk analysis.

[2] Négyesi 2022: 194–195.
[3] Négyesi 2023.
[4] Kovács 2023.
[5] Erdész 2023.
[6] Török–Ződi 2021.

In order to achieve the research objectives, we shall establish two guiding hypotheses for testing:

- H1. Organisational processes and governance elements relevant to cybersecurity for AI systems are broadly comparable to those in regulated domains, permitting transfer of useful regulatory and organisational design lessons.
- H2. The traditional cybersecurity risk analysis approach is a viable starting framework for AI cybersecurity, provided it is extended with AI-specific trustworthiness dimensions (for example, privacy, auditability, fairness and safety).

The study employs a targeted qualitative, comparative content analysis. Selected EU and Hungarian legislation, ISO[7] standards and ENISA[8] recommendations, sectoral regulatory documents and relevant scholarly literature were examined to map the functional elements and institutional pillars of domains analogous to AI.

The selection of high-level comparison pillars is based on practical experience. We can easily see that these are the most important requirements, which provide the framework for organisational-level regulation.

The analytical framework overlays traditional cybersecurity objectives (confidentiality, integrity, availability) with AI-specific trustworthiness dimensions. Identified regulatory and operational functions were mapped into an analytic matrix against these dimensions.

Risk analysis in this study is high-level and qualitative. Rather than performing a full quantitative risk assessment, the second part focuses on a compact, three-parameter framework – threats, affected security objectives and AI-specific trustworthiness factors supplemented by attention to life-cycle stages –, to demonstrate a practicable, logically coherent basis. In this examination, the selection of sources serves to test the logical line of "mandatory", "recommended" and "optional".

NATO key aspects of the military application of AI systems

The NATO Secretary General noted in 2023 that the AI, the autonomous systems and other emerging technologies *are transforming conflict dynamics,* thereby requiring new capability development, enhanced private-sector partnerships and global standards.[9]

The NATO's revised AI Strategy accelerates and mainstreams the integration of AI into Allied defence capabilities under six principles of responsible use. The document emphasises the indispensable role of AI-ready quality data, harmonised standards and a comprehensive testing, evaluation, verification and validation framework, while actively shaping international norms for the secure and transparent use of AI.[10]

The NATO Science and Technology Strategy guides the Alliance to lead both AI development and its rapid adoption. Its strategic objectives – Anticipate and Invest (fostering AI R & D), Safeguard and Protect (securing AI assets and expertise) and

[7] ISO: International Organization for Standardization.
[8] ENISA: European Network and Information Security Agency.
[9] NATO 2023.
[10] NATO 2024: 2, 5 and 13.

Orchestrate and Energise (fast-track AI deployment in operations) – provide a clear roadmap.[11]

EU high-level approach

President von der Leyen emphasised in 2025 that European AI underpins the EU's strategic autonomy and sectoral resilience, from healthcare to defence. She called for precise mandates under the proposed Cloud and AI Development Act and the Quantum Sandbox, and underscored public-private cooperation via the European AI & Tech Declaration.[12]

The European Parliament welcomes proposals for joint European defence projects, including AI development for sovereign infrastructure and critical support assets. Where possible, development should focus on *rapidly available European technologies* (reducing dependency).[13]

We must accept as a limitation that a detailed comparison of the EU and NATO AI objectives and processes is not possible due to the lack of publicly available information. However, the presented high-level statements illustrate similar approach to the strategic requirements and future plans regarding AI application.

Ethical and legal considerations

An EU parliamentary report notes that most current AI systems fall into the low-risk category. However, systems designed, developed or operated under inadequate supervision in military command centres *pose significant risks* and may contribute to conflict escalation.[14]

A fundamental question regarding autonomous weapon systems is that human involvement and oversight *must play a central role* in the lethal decision-making process. The European Parliament emphasises that it is extremely important to prevent the development and production of lethal autonomous weapon systems that lack human control in critical functions, such as target selection and engagement.[15]

Scientists, industrial experts and Pentagon officials are predicting the emergence of fully autonomous lethal weapons in the U.S. Human control will still remain, but the question is whether this is real control or just some sort of supervisory role. The U.S. military is heavily working on human–machine collaboration (e.g. the Air Force's "loyal wingman" programme, where F-16 pilots and autonomous drones work together).[16]

Strict prohibitions regarding the application of AI systems provoke new ideas that examine the legitimacy of traditional prohibitions in the current context, and

[11] NATO 2025b: 4, 11, 18.
[12] European Commission 2025.
[13] European Parliament 2025a: 58.
[14] Voss 2022: 4.
[15] European Parliament 2018: G and point 4.
[16] Bajak 2023.

encourage a modern assessment of the advantages and disadvantages, which may be particularly important in the field of nuclear deterrence.

AI systems provide opportunities to strengthen nuclear deterrence by increasing precision and efficiency. Thus, the capability for nuclear deterrence becomes *more credible*. Due to concerns related to AI, it should not be excluded from the reinforcement of nuclear deterrence. At the same time, the reinforcement using AI systems must serve a strategic purpose; it cannot be merely a routine deployment. A balance must be struck on this difficult issue, as science is still unable to answer every question accurately.[17]

We can assume that the aforementioned air force solutions, alongside nuclear deterrent systems, involve AI systems that support intelligence, strategic decision-making preparation, target identification and tactical combat management operations, *employing a wide range of technical solutions*.

Consequently, it is *unlikely that a single model could address the issue of integrating* – or substituting – the human control point. At present, we can state that, given knowledge of the specific processes, elements and operational mechanisms, it is possible to identify approximate points for assessing the transition from human oversight to full autonomy, as well as the associated risks.

We will later observe the latest development regarding the international approach.

Emerging international cooperation

An international initiative has been established to solve the problems related to AI and autonomous systems, initiated by the U.S.

The purpose of the Declaration is to establish guidelines and norms regarding the military application of AI and autonomous systems. The document provides an opportunity for participants (with Hungary as a founding member) to create a normative framework, establish international consensus, as well as to facilitate the exchange of experiences and capacity building.[18] The outcome of the initiative is greatly influenced by the number and capabilities of the participating states, and the group of non-participating countries can also be regarded as a *clear signal*. The need for international cooperation related to AI systems can also be identified in the civil sector.

The aim of the cooperation established by the EU Member States (Declaration of Cooperation on Artificial Intelligence) is to leverage the opportunities offered by AI systems and to collectively address the challenges (e.g. legal and ethical considerations, trust and accountability).[19]

AI systems that operate without human supervision raise moral, social and legal questions and problems. Due to the pace of technological development, there is a need for the development of policies, procedures and standards related to applications,

[17] Puwal 2024.
[18] U.S. Department of State 2024.
[19] European Commission 2018.

going beyond the best practices currently considered "human-in-the-loop" solutions. Additionally, there is a need to rethink the human-machine relationship, as future AI-based systems will have *both humans and AI systems as users.*[20]

The technical levels of EU–NATO cooperation are not public information, but the annual report on EU–NATO collaboration provides guidance on the role of AI. We can see that the political dialogue section considers AI as an important objective, alongside other goals, such as resilience, quantum technologies, arms control, military mobility, energy security, space cooperation, digital transformation, capability development and countering hybrid threats. Within the Emerging and Disruptive Technologies (EDT) domain, a key area of cooperation is the defence and dual-use applications of AI, quantum technologies and biotechnology, as well as related investments, technology testing, validations and innovation standards. Among research areas, AI and its responsible use are also highlighted, alongside technical foresight, research security and energy security.[21]

The UN Secretary-General's report (A/79/88) signals strong support for a legally binding instrument to ensure meaningful human control. Following informal consultations in 2025, a concrete proposal is expected in 2026, potentially forming the basis of a future international legal framework on lethal autonomous weapons systems.[22]

We can see that the positions presented so far are clear indicators for us that AI operations, including security issues, *need to be addressed on a priority basis.*

We can also perceive that international initiatives reflect significant interest and the necessity of sharing resources, which accelerates the pace of development and introduces *numerous new perspectives.*

At the same time, it is also clear to us that *significant challenges must still be addressed* before the successful establishment of international regulations for military applications.

After highlighting some examples of AI applications, the following chapters will present the Hungarian military situation based on the available information, including the significant regulatory measures with a security focus that have been taken so far.

Trends and directions

Recent public announcements clearly illustrate the speed of adaptation of AI:

- NATO's Smart Indication and Warning Broad Area Detection (SINBAD) satellite surveillance system maps change along the eastern flank at unprecedented frequency, issuing AI-driven threat warnings[23]
- The Maven Smart System of NATO Communications and Information Agency (NCIA), procured in just six months, delivers intelligence fusion, targeting, battlespace awareness and decision support[24]

[20] Jenkins 2023.
[21] European Council – NATO 2025: 3, 10.
[22] United Nations 2024: 1–3, 15–17.
[23] Fratsyvir 2025.
[24] NATO 2025a.

- SAAB's Gripen E "Centaur" tests integrate AI-driven autonomous manoeuvres directly into the aircraft, bypassing separate test and experimental environments.[25] (The Hungarian Air Force has Gripen fighters in service)
- France's Collaboration Homme-Machine (CoHoMa) programme trials legged, wheeled and tracked autonomous platforms in realistic battlefield simulations, emphasising the transition from lab prototypes to operational environments and a complementary human–machine partnership[26]

These examples represent a subset of global military AI projects. In the following, we can see that the Hungarian approach to the military application of artificial intelligence systems follows international trends.

Kristóf Szalay-Bobrovniczky (Hungarian Minister of Defence), in his presentation titled *Algorithms on the Frontline* at the AI Summit Conference 2025 in Budapest, stressed Hungary's political-level AI requirements for the armed forces. Digitalisation is central to force modernisation: the digital battlefield and personal-equipment sensors demand AI-driven data processing. Key military AI application areas include autonomous systems, training and logistics, with attention to cybersecurity, legal and ethical issues.[27]

According to Gergely Németh, Chief Executive Officer (2025), the new technology laboratory at the Defence Innovation Research Institute offers novel opportunities for Hungarian military development. Development programmes focus on machine-learning-based data analysis and drone control, with additional objectives including the testing and operational implementation of unmanned systems, training modules and autonomous capabilities.[28]

We can clearly see that the political and leadership opinion argues in favour of using AI, which is also reflected in the national strategy.

The second-generation Hungarian Artificial Intelligence Strategy (2025–2030) builds on its predecessor, summarising achievements and outlining new objectives. The Strategy defines military and national military security objectives at a high level (for example, automation of decision support; predictive analytics; development of autonomous systems and human–machine collaboration; modelling and simulation; data collection, processing and analysis) and introduces the new "Chief Artificial Intelligence Officer" function.[29]

After a brief examination, we can state that currently no other published official Hungarian military strategic-level document (e. g. strategy, action plan, roadmap or blueprint) can be identified, but the scientific examination of the topic has begun.

In summary, we can conclude that rejecting the use of AI and seeking other alternative solutions is *not a realistic approach.* Furthermore, the rapid pace of AI development precludes hesitation, despite current legal, social and other reservations.

[25] Defensemirror.com 2025.
[26] Kajal 2025.
[27] Erős 2025.
[28] Honvéd Vezérkar 2025.
[29] Magyarország Mesterséges Intelligencia Stratégiája (2025–2030) 2025: 78, 79.

These examples demonstrate that the challenge lies not in a single AI solution but in integrating multiple AI systems and embedded AI services.

This dual challenge requires armed forces to prepare existing systems and networks for AI integration and identify essential AI capabilities, select candidate systems, assess emerging risks and define integration parameters.

We can state that a critical step is to identify or develop AI systems that meet the military operational requirements of the Hungarian land and air forces, followed by comprehensive testing, where necessary.

Implementation decisions should be made based on early-stage data on AI solution architecture, operational characteristics, functional and security risks, development processes and prior deployment experiences. This underlines the importance of *effective military – defence industrial cooperation* and common thinking.

To shorten procurement cycles, defining precise operational requirements must be strengthened, and procurement planning and procedures streamlined and accelerated. Considering *life cycle stages and supply chain processes is essential.* Threats can cause *cascade risks,* potentially undermining the trustworthiness of the AI system.

We can confirm that successful AI implementation also depends on factors such as NATO and EU interoperability, preparing forces for AI–human teaming across all command levels, and close collaboration with research institutes, universities and defence-tech companies.

The examples also illustrate that, beyond concerns about lethal autonomous weapons, there is a growing emergence of AI platforms that replace humans – autonomous "combat robots" – driven by advanced human–machine collaboration, which raise *control, regulatory* and *operational* challenges.

In the Hungarian Defence Forces, core requirements for autonomous weapons and defence systems are set at the legislative level (for example, human-intervention capability, awareness of system operation and adherence to operational rules) under the National Defence Act.[30] These regulations require further specification at subordinate levels and integration of emerging international standards.

The military Chief Artificial Intelligence role can prioritise land and air force AI developments, minimise resource competition and ensure adequate resourcing. Defining its authority and position within the organisational hierarchy is essential.

The following sections will provide us with an overview of important high-level risk considerations regarding the military application of AI systems in Hungary.

High-level risk considerations of AI systems

The European Commission Recommendation (2023) ranked AI as one of the top *four threats among ten critical technical areas.* The Commission calls on Member States to conduct a collective risk assessment to identify major threat categories; threatening actors (including geopolitical adversaries); likelihood of occurrence; the technology

[30] Act CXL of 2021, para. 3, para. 92. Section (1).

value chain; and chokepoints. The risk assessment focuses on risks with European wide impact.[31]

Based on the EU's proposal, we can assume that the investigations conducted by the member states contribute to the identification of AI threats and the development of risk management through synergistic effects across various domains.

Reviewing the EU and national frameworks provides an opportunity to explore security-related analogies. Among the possible areas, we examine those that appear to be significant from the perspective of AI: on the infrastructure side, *general network security* and *critical infrastructures,* and on the data management side, the *protection of classified information* as well as *personal data.*

As an introduction, we need to identify a specific limitation. The main EU and national requirements are considered publicly accessible information. NATO regulatory documents in similar areas (e.g. directives and supporting guidelines) are classified information or not publicly accessible; therefore, their examination or comparison with EU rules cannot be carried out in this study.

Identifying parameters of different areas based on the same criteria enables the formulation of general conclusions.

Table 1 shows that the structure of the regulatory framework at EU and national level is clear and understandable, so that important steps in the field of AI can also be predicted at national level. We can observe that, despite the EU-level exemption for the defence sector, according to the Hungarian approach, *national legislation also covers the military domain.*

We also note that, in the four areas, the relevant national legislation specifies the designation of the national competent authorities.

Similarly, it can be identified that implementing organisations must designate the responsible organisational element or individual and develop organisation-specific regulations based on risk analysis. To address threats at the national level, organisational entities are required to report incidents to the national authorities.

The draft Hungarian AI Act indicated in the table sets out the establishment of AI authorities as defined by the EU AI Act and the reporting procedure, and lays down rules for the Hungarian AI Council and the regulatory sandbox for AI.[32]

The draft decree designates the AI authorities, the reporting procedure, possible fines and detailed rules relating to the Council.[33]

These drafts were developed based on the government resolution on the establishment of a national framework for AI[34] and a subsequent government resolution.[35]

[31] European Commission 2023: 1–3.
[32] Act of 2025 (draft) on the implementation of the European Union Regulation on Artificial Intelligence, paras. 4, 5, 8, 9 and 10.
[33] Decree of Government (draft) on the implementation of the European Union Regulation on Artificial Intelligence Act, paras. 1–5.
[34] Government Resolution of 1301/2024 (IX. 30.), point 2.
[35] Government Resolution of 1149/2025 (V. 14.), points 2–3.

Table 1: Regulatory frameworks related to AI

Area	**Data protection**	**Cybersecurity**	**Resilience of critical entities**	**Classified information protection**	**Artificial Intelligence**
Identification of EU regulation	Regulation (EU) 2016/679 (GDPR)[36]	Directive (EU) 2022/2555 (NIS2 Directive)	Directive (EU) 2022/2557 (CER Directive)[37]	Council Decision 2013/488/EU (EUCI)[38]	Regulation (EU) 2024/1689 (AI Act)
Type of enforcement	Directly applicable	Enforced by national legislation	Enforced by national legislation	Enforced by national legislation	Directly applicable
Type of national regulation	Act	Strategy, Act, supporting decrees	Strategy, Act, supporting decrees	Act, supporting decrees	Act (draft), supporting decree (draft)
National responsible organisation	National Authority for Data Protection and Freedom of Information	National Cyber Security Centre	National Directorate General for Disaster Management, Ministry of the Interior	National Security Authority	National AI Office (planned)
Designation of a responsible person or organisational element	Yes	Yes	Yes	Yes	Yes
Organisational-level risk management obligation	Yes	Yes	Yes	Yes	Yes
Organisational level regulatory obligation	Yes	Yes	Yes	Yes	Yes
Obligation to notify the national responsible organisation	Yes	Yes	Yes	Yes	Yes
Incident reporting obligation	Yes	Yes	Yes	Yes	Yes
Applicable to the Hungarian Defence Forces	Yes	Yes	Yes	Yes	Yes

Source: compiled by the author

[36] Regulation (EU) 2016/679 of the European Parliament and of the Council (GDPR).
[37] Directive (EU) 2022/2557 of the European Parliament and of the Council.
[38] Council Decision of 23 September 2013 (2013/488/EU).

In the topic of the responsible organisational element, the question is about the representation of the military role (e.g. an independent military responsible organisational element or integration into the national authority).

After studying the AI related drafts, we can conclude that *they do not address AI-specific cybersecurity requirements.* Based on this, we can state that measures related to the security of AI systems should be developed and maintained *within the framework of general, cross-sector security regulations.*

The EU AI Act (2024) mandates that high-risk AI systems operate under a documented, maintained risk-management system covering the entire lifecycle and addressing known and foreseeable risks.[39] While the regulation is clear, a recurring question is whether general standards can be applied to AI.

An ENISA report (2023) responds that, despite AI's unique attributes, it remains fundamentally software; hence, established software requirements and procedures can be adapted.[40]

The EU NIS2[41] Directive (2024) obliges Member States to implement security requirements and controls for the cybersecurity of electronic systems and services, including supply chain risk management procedures.[42]

We have previously observed the emergence of procurement and supply chain security issues. Going forward, it will become apparent that these issues may pose significant risks in relation to AI systems.

The associated NIS2 Implementation Regulation (2024) elaborates basic requirements for risk management frameworks, incident management, business continuity and crisis management and supply chain security.[43]

These high-level provisions can be applied to AI system security, with domain-specific adaptations.

The Cybersecurity Act (2024)[44] at national level sets out the general security requirements in line with EU NIS2 and the Implementing Regulation, while details are provided in Decree 7/2024 (VI. 24.).[45]

To establish the protective measures for an AI system – as an electronic information system – we need to review the elements that are more significant from a risk analysis perspective. The general cybersecurity framework does not define an exact risk management methodology, thereby granting applying organisations considerable decision-making flexibility.

Among the key issues, we should identify the *cyber threats, cybersecurity objectives* and *critical lifecycle stages* to consider. Other mandatory elements of risk analysis, such as the severity and likelihood of occurrence, may perhaps be more easily adopted for AI cases.

[39] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022, Section (9).
[40] Bezombes et al. 2023: 17.
[41] Network and Information Security.
[42] Directive (EU) 2022/2555, Section (21).
[43] Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024, Section (11)–(15) and Annex points 1–5.
[44] Act LXIX of 2024 on the cyber security of Hungary.
[45] Decree 7/2024 (VI. 24.) of the Prime Minister's Office on the requirements for security classification and the specific protective measures applicable to each security classification.

As an initial step, we can select general cybersecurity considerations, which can then be further developed. During the development process, following the line of *regulations (requirements), international standards, recommendations* and other sources provides comprehensive solutions.

This approach offers a general, flexible model that can be finalised based on organisational and technical specific parameters, as well as other sensitive information.

We need to clarify two important factors in advance:

- These regulations set out a framework and allow organisations to tailor security measures to their specific needs
- The decree combines security measures with traditional cybersecurity objectives (confidentiality, integrity and availability), which must be supplemented with "identification" in accordance with the EU NIS2 Directive (Article 6) – a factor that is also significant in the case of AI systems

The decree sets out minimum requirements (Annex 3), that must be applied to threat aspects ("threat list"), which must also be applied to AI systems. The Hungarian National Cyber Security Centre published a guide on security classification and practical application of national requirements to support organisations.[46] The guide outlines general risk-management tasks – such as defining procedures, assigning responsibilities, assessing and approving risks and periodic reviews – that apply regardless of technology, leaving room for AI-specific adaptations.

The ENISA 2020 report, following ISO 27005 standard, identifies asset, threat, and threat-actor mapping as essential to risk analysis. Based on the report, we can clearly identify that the traditional security objectives (confidentiality, integrity, availability) apply to artificial intelligence, complemented by authentication, access control and non-repudiation.

AI-specific attributes include robustness, trustworthiness, safety, transparency, explainability, accountability and data protection. The report categorises 74 AI-related cyber threats into eight groups, mapped to lifecycle stages to guide responsible stakeholders.[47] The "security-by-design" principle embeds security considerations throughout the product lifecycle. The ENISA 2023 report proposes AI evaluation criteria slightly different from the previous report – privacy protection, explainability, robustness, fairness – each of which is related to risk assessment and management processes (these aspects have also been incorporated into the cybersecurity goals in Table 2).[48]

The ISO/IEC[49] 5338 Standard defines lifecycle stages as inception, design and development, verification and validation, implementation, operation and monitoring, continuous validation, reassessment and withdrawal.[50]

[46] National Cyber Security Centre 2025: 3.
[47] Malatras–Dede 2020: 12, 25, 27 and Annex B, D.
[48] Pascu – Barros Lourenco 2023: 11.
[49] ISO/IEC: International Organization for Standardization/International Electrotechnical Commission.
[50] ISO/IEC 2023a: 5.

The U.S. national AI risk management standard applies a different approach, namely plan and design, collect and process data, build and use models, verify and validate, deploy and use, operate and monitor.[51]

As an interesting point, we observe that beyond the life cycle phases of standards, it is worthwhile to examine a scientific approach (Table 2), which clearly illustrates flexible solution options.

Table 2: Threats, cybersecurity goals and life cycle stages of AI

Threat categories	**Cybersecurity goals and supplements**
Elements of the threat catalogue (Decree 7/2024, Annex 3) Elements of ENISA 2020 report, in 8 groups: Nefarious activity/abuse Eavesdropping/Interception/ Hijacking Physical attacks Unintentional damage Failures or malfunctions Outages Disaster Legal Elements of EU AI threat reports Elements of EU and NATO military threat reports	Confidentiality, integrity, availability and identification (as basic cybersecurity elements) and AI specific supplements (ENISA 2020): Authentication Authorisation Non-repudiation Robustness Trustworthiness Safety Transparency Explainability Accountability Data protection Possible additions based on ISO/IEC 23894:52 AI expertise Environmental impact Fairness Maintainability Privacy Robustness Other military speciality, depends on functions, elements
Life cycle stages	
ISO/IEC 5338: inception, design and development, verification and validation, implementation, operation and monitoring, continuous validation, reassessment and withdrawal AI RMF: Plan and design, collect and process data, build and use model, verify and validate, deploy and use, operate and monitor Technical approach:[53] Data sources, input data, data cleaning, data storage, data processing, data analysis, model development, machine learning, output data and communication networks	

Source: compiled by the author

[51] NIST 2023: 10.
[52] ISO/IEC 2023b: Annex A, A3, A5–9.
[53] Kollár 2019: 62.

We can identify that the elements related to threats and security objectives have been *significantly expanded* in Table 2. Subsequently, it becomes possible to supplement these with organisation and military specifications (or to remove non-essential elements). We note that this option also represents a limitation. If security management does not filter the organisation-specific and the applied (or planned) AI parameters, the establishment of a risk analysis will not be feasible.

We also recognise that, compared to the standards and recommendations, the lifecycle phases included in the academic classification are more detailed and practical. This also supports a more refined risk-based approach. The modular structure allows us to adapt a risk analysis methodology that aligns with organisational characteristics and AI specifications.

Table 2 also supports another conclusion. The situation for security management will become more difficult because as the number of parameters increases, the possible combinations multiply. In the case of a complex information system, *manual risk analysis is practically impossible*.

We must not forget that integrating AI into an organisational information system involves examining both the existing system (and its elements) and the software (or AI-containing platform) that comprises the AI together.

In summary, the presented method enables an organisation to define the security objectives for a specific AI product, the relevant lifecycle stages and the scope of applicable threats. The table indicates the necessity of incorporating military specifications, but we strongly emphasise that processing and integrating military operational and tactical requirements is essential, as failing to do so *may lead to serious issues*.

The key question is whether the implementing organisation is capable of customising the set of mandatory and optionally selectable elements. It can also be observed that the terminology and conceptual framework appearing in international AI standards (and other sources) have not yet been fully clarified. The components of "trustworthiness", considered a fundamental attribute of AI, are not unified, which allows for different interpretations. Therefore, the security management has a key responsibility in establishing an approved and functional organisational risk methodology or model, providing clear framework for the interpreted parameters. Based on the experience from Table 1, it is advisable to establish a working group whose members are experienced in risk analysis across various domains.

The collected information provides a basis for further conclusions that we can also draw.

The examination of AI platforms (system components), which consist of existing and new infrastructure elements, should begin at the earliest possible stage. The organisation's existing risk assessment documentation (as well as incident management and audit reports) should be reviewed, and the tests and evaluation materials carried out in previous lifecycle phases of the planned AI system should also be examined. This again requires close cooperation and institutionalisation of horizontal organisational relationships, as well as collaboration between the military organisation and defence industry actors (including necessary authorisations and information security considerations).

Furthermore, based on what we have observed so far, we can also conclude that the assessment and quantification of new organisational security objectives (e.g. trustworthiness and its components) must be ensured to meet the criterion of verifiability.

Cybersecurity considerations

Risk analysis is not an end in itself, but rather a practical tool for determining system-specific security controls.

The AI-specific additions to security objectives outlined in Table 2, by themselves, do not contain implementable security controls (e.g. in the case of "accountability" or "explainability"). Therefore, it is necessary to apply system-specific frameworks that include *technically interpretable, measurable parameters and repeatable procedures* aligned with general objectives.

We present that in the domains of security objectives, one of the tools for gradually establishing measurability is the application of the AI Trust Framework and Maturity Model (AI-TMM) which is aligned with risk analysis. Within the framework of the Maturity Indicator Levels (MIL 1–3), each objective (or domain) begins with the documentation of fundamental principles (L1: formulation of principles), continues with the introduction of initial indicators and management practices (L2: indicators, managed processes), and culminates in a fully integrated, continuously monitored and audited system (L3: monitoring and audit).

The model thus serves as a diagnostic instrument for identifying risks and provides the foundation for appropriate protective measures, ensuring the transparent traceability of trustworthiness.[54]

In another solution, we demonstrate that the AI Trustworthiness Assessment Framework (AI TAF) is capable of mapping human risks in detail. The framework identifies the affected groups and models, based on specific scenarios, how an AI failure or misuse could cause physical, economic or psychological harm. To what extent are the harms reversible? The method takes into account exposure and vulnerability, assigns controls (preventive, detective, corrective) to each risk, establishes go/no-go thresholds, and is intended to be complemented by integration into the lifecycle.[55]

We can see that these models provide measurability and enable the development of specific parameters related to the AI system to ensure the enforceability of security controls.

The aforementioned Hungarian decree (7/2024), which defines national cybersecurity requirements, contains hundreds of security controls, grouped into several categories and assigned to three security classes (low, medium, and high).

We know that military organisations regulate the cybersecurity of their information systems (including AI systems) according to their operational maturity and mission profile. This may take the form of a comprehensive, lengthy regulation or

[54] Mylrea–Robinson 2023.
[55] Seralidou et al. 2025: 4.

a structured framework consisting of high-level requirements supported by detailed procedural documents.

When developing and maintaining cybersecurity controls and procedures, it is essential to understand and correctly manage dependencies between systems. AI capabilities operated by tactical units – or their failure – can have cascading effects, causing significant disadvantages at the operational or even strategic level.

We can state that during the design phase of an AI capability, the technical operational requirements and the security classification of the system must be identified as early as possible. Failure to do so can lead to complex interoperability issues between the host network and the AI system, necessitating costly retroactive investments.

Unique procedures must be established to ensure the cooperation (integration, interconnection of services) of platforms with different security classifications. A higher security classification may also compel the operating organisation to make substantial additional security investments.

In addition to the aforementioned, we must also *highlight the role of incident management*. Due to the possibility of cascade-type security incidents, incident management procedures must be continuously refined during development and deployment in order to minimise damage.

These considerations underscore the importance of *close cooperation between developers, producers and the military organisation* during the design phase. Early engagement with cybersecurity specialists and alignment with recognised international standards can reduce long-term costs and improve resilience.

Finally, we emphasise that higher command has the authority to influence the regulatory practices of subordinate military organisations and to coordinate tasks when shared resources are involved. This top-down alignment is critical to ensuring consistent security postures, avoiding duplication of effort and maintaining operational readiness.

We present the following high-level recommendations outlining the practical steps for integrating robust security practices into AI-supported military systems:

- early security classification
- tailored control implementation
- cross-disciplinary design teams
- dependency and interoperability management
- alignment with international standards
- continuous monitoring and audit
- top-down regulatory coordination
- lifecycle security management
- secure supply chain oversight
- incident response preparedness

By using these guides, military stakeholders can ensure that AI-enabled capabilities remain secure, resilient and aligned with mission objectives throughout their operational lifecycle.

Conclusion

The paper demonstrates that military forces must adopt AI with the same urgency seen in social and economic domains. The military force modernisation requires integrating AI systems and services; failure to do so invites significant operational and strategic risks.

The issue of lethal autonomous weapons remains urgent, with evolving regulatory and ethical challenges. Hungary must continuously harmonise its national military requirements with international norms.

When the military uses AI capabilities, numerous technical, operational, legal, and ethical considerations demand attention. The paper points out that secure deployment is not possible without knowledge of the necessary technical, operational, and procedural parameters.

We can summarise that the planned review of regulations in the analogous field, as well as the examination of opportunities for developing elements supporting risk analysis, yield practical, usable results.

We can observe that, according to H1, existing organisational starting points can, with further efforts, support the operation of AI systems. Similar steps can be expected in the case of regulatory needs for new technologies (e.g. quantum). During the examination, we can conclude that, based on the presented existing legal requirements, the regulation of AI cybersecurity is not unrealistic, but it requires a great deal of clarification and refinement. Based on this, hypothesis H1 can be validated.

We can confirm that in the area specialised for risk analysis, based on H2, organisation-specific models and methods can be developed, and it can be seen through examples that the new parameters can be made measurable (enabling their verification). Based on the examples presented, we can confirm as a general observation that alongside legal, international standards and best practice (recommendation) sources, it is also advisable to *take academic initiatives into consideration.* Based on this, we can state that hypothesis H2 is valid. This is further reinforced by the fact that the new perspectives and factors significantly complicate the task of security management.

Given budgetary and personnel constraints, prioritising AI support for land or air forces is essential. Effective prioritisation and resource allocation can be facilitated by the Chief Artificial Intelligence Officer role, ideally positioned within the Ministry of Defence. We note that the best tool for determining the priority order of tasks and scheduling resources is to develop a *military AI strategy (or action plan).* This can represent the requirements, the responsibilities of the participants (including operational and security management requirements, development and integration plans), deadlines, as well as visible training tasks, in order to ensure the success of further progress.

Based on the presented information, it is clear that the reviewed sources emphasise that AI is not exempt from cybersecurity requirements. The protective measures mapped to predefined security classes – augmented with AI-specific clarifications – can fulfil system cybersecurity requirements.

The future will show whether this prediction will be fulfilled or refuted. A follow-up study in several years is recommended.

References

Bajak, Frank (2023): Pentagon's AI initiatives Accelerate Hard Decisions on Lethal Autonomous Weapons. *AP News,* 25 November 2023. Online: https://apnews.com/article/us-military-ai-projects-0773b4937801e7a0573f44b57a9a5942

Bezombes, Patrick – Brunessaux, Stéphan – Cadzow, Scott (2023): *Cybersecurity of AI and Standardisation.* European Union Agency for Cybersecurity (ENISA). Online: https://doi.org/10.2824/277479

DefenseMirror.com (2025): Saab Tests AI co-Pilot in Gripen Fighter Jet for First Time. *DefenseMirror.com,* 11 June 2025. Online: www.defensemirror.com/news/39650

Erdész, Viktor (2023): *A mesterséges intelligencia alkalmazása a katonai nemzetbiztonsági hírszerzésben* [The Use of Artificial Intelligence in Military National Security Intelligence]. Budapest: Katonai Nemzetbiztonsági Szolgálat.

Erős, Hunor (2025): A mesterséges intelligencia a magyar honvédségbe is beépült [Artificial Intelligence has also been Integrated into the Hungarian Military]. *Magyar Nemzet,* 9 September 2025. Online: https://magyarnemzet.hu/belfold/2025/09/a-mesterseges-intelligencia-a-magyar-honvedsegbe-is-beepult

European Commission (2018): *EU Member States Sign Up to Cooperate on Artificial Intelligence.* 10 April 2018. Online: https://digital-strategy.ec.europa.eu/en/news/eu-member-states-sign-cooperate-artificial-intelligence

European Commission (2023): *Commission Recommendation of 03 October 2023 on Critical Technology Areas for the EU's Economic Security for Further Risk Assessment with Member States.* C(2023) 6689 final. Online: https://defence-industry-space.ec.europa.eu/commission-recommendation-03-october-2023-critical-technology-areas-eus-economic-security-further_en

European Commission (2025): State of the Union Address by President von der Leyen, 10 September 2025. Online: https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_25_2053

European Council – NATO (2025): *Tenth Progress Report on the Implementation of the Common Set of Proposals Endorsed by EU and NATO Councils on 6 December 2016 and 5 December 2017.* Online: www.consilium.europa.eu/media/f54kvokr/250605-progress-report-nr10-eu-nato.pdf

European Parliament (2018): European Parliament Resolution of 12 September 2018 on Autonomous Weapon Systems (2018/2752(RSP). Online: www.europarl.europa.eu/doceo/document/TA-8-2018-0341_EN.html

European Parliament (2025): *White paper on the future of European Defence.* European Parliament Resolution of 12 March 2025 on the White Paper on the Future of European Defence (2025/2565(RSP)). Online: www.europarl.europa.eu/doceo/document/TA-10-2025-0034_EN.pdf

Fratsyvir, Anna (2025): NATO Expands Satellite Surveillance to Monitor Ukraine, Eastern Flank. *The Kyiv Independent,* 12 June 2025. Online: https://kyivindependent.com/nato-expands-satellite-surveillance-to-monitor-ukraine-eastern-flank/

Honvéd Vezérkar [Armed Forces General Staff] (2025): Újdonságok a védelmi innováció területén [News in the Field of Defence Innovation]. *Honvédelem.hu,*

2 June 2025. Online: https://honvedelem.hu/hirek/ujdonsagok-a-vedelmi-innovacio-teruleten.html

ISO/IEC (2023a): Information Technology – Artificial Intelligence – AI System Life Cycle Processes. ISO/IEC 5338. First edition.

ISO/IEC (2023b): Information Technology – Artificial intelligence – Guidance on Risk Management. ISO/IEC 23894. First edition.

Jenkins, Michael P. (2023): The Impact and Associated Risks of AI on Future Military Operations. *Federal News Network,* 18 October 2023. Online: https://federalnewsnetwork.com/commentary/2023/10/the-impact-and-associated-risks-of-ai-on-future-military-operations/

Kajal, Kapil (2025): France Plans to Deploy Combat Robots by 2027, Eyes Full Robot Army by 2040. *Interesting Engineering,* 8 May 2025. Online: https://interestingengineering.com/military/france-eyes-all-robot-army-by-2040

Kollár, Csaba (2019): A mesterséges intelligencia, mint komplex rendszer információbiztonsági kihívásai [Information Security Challenges of Artificial Intelligence as a Complex System]. In Rajnai, Zoltán (ed.): *Kiberbiztonság/Cybersecurity*. Budapest: Biztonságtudományi Doktori Iskola, 62–70. Online: https://drkollar.hu/wp-content/uploads/2020/01/kiadvany-2019.pdf

Kovács, Zoltán ed. (2023): *A mesterséges intelligencia és egyéb felforgató technológiák hatásainak átfogó vizsgálata* [Comprehensive Review of the Impact of Artificial Intelligence and Other Disruptive Technologies]. Budapest: Katonai Nemzetbiztonsági Szolgálat.

Magyarország Mesterséges Intelligencia Stratégiája (2025–2030) [Hungary's Artificial Intelligence Strategy (2025–2030)]. (2025). Online: https://cdn.kormany.hu/uploads/document/c/c0/c0d/c0dfdbd37cfa520ae37361a168d244c85e7295af.pdf

Malatras, Apostolos – Dede, Georgia (2020): *AI Cybersecurity Challenges. Threat Landscape for Artificial Intelligence.* European Union Agency for Cybersecurity (ENISA). Online: https://doi.org/10.2824/238222

Mylrea, Michael – Robinson, Nikki (2023): Artificial Intelligence (AI) Trust Framework and Maturity Model: Applying an Entropy Lens to Improve Security, Privacy, and Ethical AI. *Entropy,* 25(10). Online: https://doi.org/10.3390/e25101429

NATO (2023): *Speech by Secretary General Jens Stoltenberg at the NATO-Industry Forum.* 25 October 2023. Online: www.nato.int/cps/en/natohq/opinions_219128.htm

NATO (2024): *Summary of NATO's revised Artificial Intelligence (AI) Strategy.* 10 July 2024. Online: www.nato.int/cps/en/natohq/official_texts _227237.htm

NATO (2025a): *NATO Acquires AI-Enabled Warfighting System.* 14 April 2025. Online: https://shape.nato.int/news-releases/nato-acquires-aienabled-warfighting-system-

NATO (2025b): *NATO Science & Technology Strategy. Defending the future, today!* Online: www.nato.int/content/dam/nato/webready/documents/sto/STO-strategy-2025.pdf

Négyesi, Imre (2022): *A mesterséges intelligencia katonai felhasználásának lehetőségei: Első kötet* [The Possibilities of Military Use of Artificial Intelligence Vol. I]. Budapest: HM Zrínyi Média Közhasznú Nonprofit Kft.

NÉGYESI, Imre (2023): *A mesterséges intelligencia katonai felhasználásának lehetőségei: II. kötet* [The Possibilities of Military Use of Artificial Intelligence Vol. II]. Budapest: HM Zrínyi Média Közhasznú Nonprofit Kft.

Nemzeti Kiberbiztonsági Intézet [National Cyber Security Centre] (2025): *Elektronikus Információs Rendszerek és Szervezetek Kiberbiztonsági Követelménykatalógusának Alkalmazási Útmutatója. Kozkázatkezelés* [Guideline for the Application of the Cybersecurity Requirements Catalogue of Electronic Information Systems and Organisations. Risk Management]. Online: https://nki.gov.hu/wp-content/uploads/2025/09/15.-Kockazatkezeles-ver.-1.1.pdf

NIST (2023): *Artificial Intelligence Risk Management Framework* (AI RMF 1.0). Online: https://doi.org/10.6028/NIST.AI.100-1

PASCU, Corina – BARROS LOURENCO, Marco eds. (2023): *Artificial Intelligence and Cybersecurity Research.* ENISA Research and Innovation Brief. European Union Agency for Cybersecurity (ENISA). Online: https://data.europa.eu/doi/10.2824/808362

PUWAL, Steffan (2024): Should Artificial Intelligence Be Banned from Nuclear Weapons Systems? *NATO Review,* 12 April 2024. Online: https://archives.nato.int/uploads/r/nato-archives-online/d/3/8/d388000c2ba6b51ffb20865bb71d1828203cb6e45312f46ec1cf202fe918ca81/2024-04-12_Should_artificial_intelligence_be_banned_from_nuclear_weapons_systems_ENG.pdf

SERALIDOU, Eleni – KIOSKLI, Kitty – FOTIS, Theofanis – POLEMI, Nineta (2025): AI_TAF: A Human-Centric Trustworthiness Risk Assessment Framework for AI Systems. *Computers,* 14(7). Online: https://doi.org/10.3390/computers14070243

TÖRÖK, Bernát – ZŐDI, Zsolt eds. (2021): *A mesterséges intelligencia szabályozási kihívásai* [The Regulatory Challenges of AI]. Budapest: Ludovika Egyetemi Kiadó.

U.S. Department of State (2024): *Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy.* Online: www.state.gov/bureau-of-arms-control-deterrence-and-stability/political-declaration-on-responsible-military-use-of-artificial-intelligence-and-autonomy

United Nations (2024): *Lethal Autonomous Weapons Systems: Report of the Secretary-General* (A/79/88). Online: https://digitallibrary.un.org/record/4059475

VOSS, Axel (2022): *Report on Artificial Intelligence in a Digital Age.* European Parliament Report A9 0088/2022. Online: www.europarl.europa.eu/doceo/document/A-9-2022-0088_EN.html

Legal sources

2021. évi CXL. törvény a honvédelemről és a Magyar Honvédségről [Act CXL of 2021 on National Defence and Hungarian Defence Forces]

2024. évi LXIX. törvény Magyarország kiberbiztonságáról [Act LXIX of 2024 on the Cyber Security of Hungary]

2025. évi … törvény az Európai Unió mesterséges intelligenciáról szóló rendeletének magyarországi végrehajtásáról [Act of 2025 (draft) on the implementation of the European Union Regulation on Artificial Intelligence]. Online: https://cdn.

kormany.hu/uploads/document/b/b9/b92/b929cdec547b87da4bd23bce694d-b86ce328e1c6.pdf

1301/2024. (IX. 30.) Korm. határozat a mesterséges intelligenciáról szóló európai parlamenti és tanácsi rendelet végrehajtásához szükséges intézkedésekről [Government Resolution of 1301/2024 (IX. 30.) on measures necessary for the implementation of the Regulation of the European Parliament and of the Council on artificial intelligence]

1149/2025. (V. 14.) Korm. határozat a mesterséges intelligenciáról szóló európai parlamenti és tanácsi rendelet végrehajtásához szükséges intézkedésekről szóló 1301/2024. (IX. 30.) Korm. határozatban foglalt feladatok végrehajtásáról [Government Resolution of 1149/2025 (V. 14.) on the implementation of the tasks set out in GR of 1301/2024 (IX. 30.) on the measures necessary for the implementation of the Regulation of the European Parliament and of the Council on artificial intelligence]

7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről [Decree 7/2024 (VI. 24.) of the Prime Minister's Office on the requirements for security classification and the specific protective measures applicable to each security classification]

A Kormány rendelete az Európai Unió mesterséges intelligenciáról szóló rendeletének magyarországi végrehajtásáról szóló 2025. évi … törvény végrehajtásáról [Decree of Government (draft) on the implementation of the on the implementation of the European Union Regulation on Artificial Intelligence]

Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures and further specification of the cases in which an incident is considered to be significant with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers

Council Decision of 23 September 2013 on the security rules for protecting EU classified information (2013/488/EU)

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)

HADMÉRNÖK
VÉDELEMINFORMATIKA

20. évfolyam (2025) 4. szám 39–51.
DOI: 10.32567/hm.2025.4.3

Zoltán Kovács[1]

The Use of Artificial Intelligence in Cyberattacks, Part 1

Fundamental Concepts of Artificial Intelligence and the Cyber Kill Chain Model

Abstract

The rapid advancement of artificial intelligence (AI) technology has fundamentally transformed the field of cybersecurity, impacting both defensive and offensive capabilities. This series of articles analyses the malicious applications of artificial intelligence in cyberattacks, structured around the Cyber Kill Chain model. It details how AI can increase the effectiveness, automation and stealth of attacks in all phases of cyberattacks described by the Cyber Kill Chain model, from reconnaissance to actions on objectives. The aim of this series of articles is to provide a comprehensive overview of current threats and to highlight the importance of further research and proactive defence strategies. This article, the first in the series, covers the definitions of AI and the Cyber Kill Chain model to the extent necessary for understanding.

Keywords: artificial intelligence, cybersecurity, cyberattack, Cyber Kill Chain, machine learning, deep learning, phishing, malware

Introduction

In the current phase of the information society, where digital transformation permeates everything and global reliance on digital infrastructure is continuously increasing, the associated risks are also on the rise. Indeed, the vulnerability of information and communication networks and systems has reached unprecedented levels. At the same time, artificial intelligence (hereinafter: AI) has undergone explosive development,

[1] Senior Lecturer, Ludovika University of Public Service, e-mail: zkovacs.24@gmail.com

enabling machines to perform tasks similar to human intelligence, such as data analysis, pattern recognition, decision-making, and automation.[2] AI has now developed to the point where it is widely applied on a daily basis in areas such as cybersecurity, healthcare, manufacturing, education and financial modelling, but as a personal assistant, it is also assisting the work of an increasing number of companies worldwide in all areas of life.

However, in addition to areas that can now be considered classic, AI is also appearing in a completely different area, the so-called metaverse, where it plays a prominent role. The metaverse is a global virtual ecosystem born from the convergence of physical, augmented and virtual spaces connected by the internet, virtual reality (VR), and augmented reality (AR), where people (and companies) can communicate openly with each other. Increasingly advanced AI, especially in relation to AI-driven avatars that enable human-like interaction, is an essential part of the Metaverse. On the one hand, without increasingly advanced AI, there would be no Metaverse, as it is essential for handling vast amounts of complex data and creating dynamic, interactive environments. On the other hand, the Metaverse itself has a significant impact on the development of AI, as its complexity allows the AI models used to be trained for a wide variety of highly diverse tasks.[3] However, the emergence of AI in cybersecurity is a double-edged sword. On the one hand, it assists defensive personnel by offering significant potential for strengthening cyber defence systems and automated threat detection, On the other hand, however, it also provides malicious actors with an extremely effective tool for executing sophisticated, adaptive and difficult-to-detect cyberattacks.[4] This dual nature results in a spiral-like, constantly escalating *AI arms race* in the field of cybersecurity. As attackers utilise increasingly sophisticated AI-based tools, defenders must rely on increasingly advanced AI-based detection and incident response solutions to operate effectively, which in turn generates a rapid innovation cycle on both sides. This phenomenon is not only of operational technological significance, but also of strategic importance, as superiority in AI capabilities in cyber warfare can fundamentally influence national security and the protection of critical infrastructure.[5] State-sponsored actors, whether on the defensive or offensive side, are expected to invest significant resources in the development of AI-based cyber weapons in the near future, which will enable them to carry out targeted, large-scale and covert attacks with much greater efficiency than they currently can against any selected target, including critical infrastructure.

This series of articles examines the offensive applications of artificial intelligence during cyberattacks along the lines of the Cyber Kill Chain (hereinafter: CKC) model developed by Lockheed Martin, which is now considered as an industry standard. The CKC is a strategic framework developed by Lockheed Martin to describe the phases of cyberattacks, thereby facilitating the focused application of cyber defence mechanisms during different stages of attacks.[6] Although this series of articles pro-

[2] Jordan–Mitchell 2015.
[3] Wolfenstein 2023; Team Antier 2022.
[4] Abbadi–Lachkar 2024.
[5] Erdész 2023; Mattioli et al. 2023.
[6] Microsoft [s. a.b].

vides a brief overview of CKC and the basic definitions of AI, it is not intended to be a detailed presentation of the CKC model and artificial intelligence. These and related concepts are explained only to the extent necessary for understanding the content. The primary goal of this series of articles is to provide a comprehensive overview of how AI can significantly increase the effectiveness of attackers in certain phases of cyberattacks, outline the rapidly evolving threat landscape associated with this, and, in addition, make recommendations for further research directions.

Basic concepts of artificial intelligence and the Cyber Kill Chain model

In order for this series of articles to achieve its goal, namely, to demonstrate the means and methods attackers use to utilise AI in cyberattacks, it is first necessary to review the basic terms of artificial intelligence and examine why the Cyber Kill Chain model is appropriate as a basis for this examination.

The most important basic concepts of artificial intelligence

John McCarty Professor Emeritus at Stanford University, defined artificial intelligence as follows:

"It is the science and engineering of making intelligent machines, especially intelligent computer programs. It is related to the similar task of using computers to understand human intelligence, but AI does not have to confine itself to methods that are biologically observable."[7]

According to Hungary's Artificial Intelligence Strategy 2020–2030, "Artificial intelligence (AI) […] is the totality of algorithmic systems capable of teaching and improving themselves based on the data fed into them".[8] Hungary's Artificial Intelligence Strategy (2025–2030), which was published on 3 September 2025 as a revision of the previous strategy, states the following:

"Artificial intelligence (AI) has now moved beyond being merely a collection of algorithmic systems that teach and improve themselves based on data. AI is increasingly capable of simulating human understanding, learning, and problem-solving, as well as mapping and enhancing the efficiency of certain segments of human capabilities. The mapping of human capabilities by 'learning machines' is leading to significant efficiency gains in economic, administrative, and private life processes, while also creating new revenue opportunities."[9]

At the same time, artificial intelligence is essentially an interdisciplinary field of science that deals with the ability of computer systems to perform tasks that require human

[7] McCarthy 2007.
[8] *Hungary's Artificial Intelligence Strategy 2020–2030* 2020.
[9] *Magyarország Mesterséges Intelligencia Stratégiája (2025–2030)* 2025.

intelligence. For the purposes of this series of articles, the following AI subfields are particularly relevant in the context of cyberattacks:

- *Machine Learning* (hereinafter: ML): A subset of AI, ML is the branch of AI that develops algorithms and statistical models that enable information and communication systems to learn and improve from input or incoming data without being specifically programming for this purpose. ML algorithms are capable of recognising patterns in data, making predictions, and taking decisions. In cyberattacks, ML is frequently used for data collection, target identification and adaptation of malicious code.
- *Deep Learning* (hereinafter: DL): Deep learning is a specialised, more sophisticated form of machine learning in which AI systems process complex data structures using multi-layered neural networks that emulate the neural pathways of the human brain. Deep learning uses artificial neural networks with many so-called hidden layers to recognise complex patterns and generalities in vast amounts of data. DL is particularly effective at analysing unstructured data (such as images, text and sound) and generating accurate information and predictions from them, which can be crucial in areas such as advanced phishing and the creation of generative malware.
- *Reinforcement Learning* (hereinafter: RL): An approach to machine learning in which a software *agent* learns how to behave based on feedback in the form of rewards and penalties during its interactions in a given environment. The goal of learning is for the *agent* to maximise long-term rewards. This type of approach may be ideal for developing autonomous attack systems that are capable of independently identifying and performing reconnaissance on targets, making decisions and executing attacks, while continuously adapting to the target system's responses.
- *Natural Language Processing* (hereinafter: NLP): The area of AI that deals with interaction between computers and human (natural) language. The capabilities of NLP, particularly through the latest Large Language Models (hereinafter: LLMs), play a key role in generating convincing phishing messages, fraudulent emails, and deepfake content, which significantly increase the effectiveness of social engineering attacks.
- *Generative Artificial Intelligence* (hereinafter: Generative AI): Generative AI is a form of deep learning, a branch of AI that can create new, original data (such as text, images, sound, code) based on patterns learned from training data. Generative AI models, such as Large Language Models (LLMs), are capable of performing complex tasks including answering questions, generating images from text, writing complex texts and generating content. This group also includes, for example, Generative Adversarial Networks (hereinafter: GANs), where two neural networks are operated in competition with each other in order to generate more authentic new data from a given training data set, as well as language models based on transformer architecture, where words are processed in parallel and independently of each other rather than sequentially.

> With the help of these technologies, attackers can create realistic fake content, adaptive malware variants and personalised attack scripts.[10]

The evolution from machine learning through deep learning further to generative AI and advanced NLP represents an increasing sophistication of AI moving from analytical to creative capabilities. However, this shift fundamentally influences the cyber threat landscape, as it enables attackers to create novel, adaptive, and highly effective malicious code, such as polymorphic malware or even deepfakes for social engineering attacks. Table 1 below summarises the relevance of AI sub-sectors in cyberattacks.

Table 1: Relevance of artificial intelligence sub-sectors in cyberattacks

AI sub-sector	Brief definition	Offensive application mode
Machine learning (ML)	Algorithms and statistical models that enable systems to learn and improve from data	Data collection, target identification, adaptation of malicious code
Deep learning (DL	A specialised form of machine learning that uses artificial neural networks to recognise complex patterns in vast amounts of data	Analysis of unstructured data (image, text, audio), advanced phishing, creation of generative malware
Reinforcement learning (RL)	A software 'agent' that learns behaviour in a given environment based on feedback through rewards and penalties	Development of autonomous attack systems, independent target reconnaissance, attack execution, adaptation
Natural language processing (NLP)	The area of AI that deals with the interaction between computers and human language	Generation of convincing phishing messages, fraudulent emails, deepfake content, increasing the effectiveness of social engineering attacks
Generative artificial intelligence (Generative AI)	A branch of AI capable of creating new, original data (text, image, audio, code) based on patterns learned from the training data	Creation of realistic fake content, adaptive malware variants, personalised attack scripts

Source: compiled by the author based on Usman et al. 2024; AWS [s. a.]; Badman–Kosinski [s. a.]; Microsoft [s. a.a]

Introduction to the Cyber Kill Chain framework

Various organisations and companies have developed several types of frameworks for identifying and managing cyberattacks more effectively. Different threat models employ different approaches to representing detected attackers, as well as their behaviour and tools. Some models, such as Lockheed Martin's Cyber Kill Chain and Microsoft's STRIDE, represent a high level of abstraction and summarise the multiple and complex steps taken by an attacker into a short list of steps. Other models, such as MITRE CVE, take

[10] Usman et al. 2024; AWS [s. a.]; Badman–Kosinski [s. a.]; Microsoft [s. a.a].

a low-level approach and typically detail very specific items, such as detailed system vulnerabilities and their exploitation. Mid-level abstraction models (such as MITRE ATT&CK, CAPEC, FiGHT) are typically positioned between the two, describing the individual steps of an attack, the attack techniques and technologies used therein, and integrating them into a unified framework.[11]

These models often build upon each other and assist the work of cyber defence professionals at different levels. Figure 1 below illustrates the hierarchy of the Cyber Kill Chain model (developed by Lockheed Martin, which treats cyberattacks as a high-level model), MITRE's Att&ck model (which treats cyberattacks as a mid-level model), and models that treat cyberattacks as a low-level model (e.g. CVE).

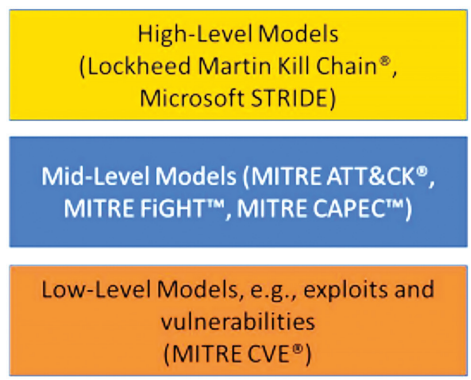


Figure 1: Abstraction layers of cyber defence frameworks
Source: Radle et al. 2023

Definition and purpose of the Cyber Kill Chain

The Cyber Kill Chain is a high-level cybersecurity framework developed by Lockheed Martin, which has now become one of the fundamental frameworks of cybersecurity. The model's purpose is to assist cybersecurity professionals in understanding the progress of cyberattacks, identifying potential points of detection for an attack, and thereby developing defence strategies. The Cyber Kill Chain framework is part of the Intelligence Driven Defense model,[12] also created by Lockheed Martin, which is used for identifying and preventing cyberattacks and helps to understand the steps opponents need to take to achieve their goals.

The Cyber Kill Chain describes the complete lifecycle of a cyberattack, breaking it down into separate, sequential phases.[13] The primary goal of developing CKC was to provide a structured approach for understanding and analysing cyberattacks and,

[11] Radle et al. 2023.
[12] The philosophy behind Lockheed Martin's Intelligence Driven Defense is to stop offensive manoeuvres during cyberattacks while maintaining a defensive position. Every defensive action and every offensive manoeuvre launched is guided by human intelligence gathering.
[13] Radle et al. 2023.

ultimately, to assist in preventing and disrupting them. By recognising the typical steps of cyberattacks, organisations can improve their resilience thereby enhancing their threat detection and response capabilities, identify vulnerabilities in their systems in a more structured manner, strengthen their defences, and proactively mitigate their cybersecurity risks, rather than merely reacting to recognised, successful attacks.[14]

As a result, CKC has become indispensable for cybersecurity professionals in establishing and maintaining effective defences, conducting cybersecurity operations, responding to incidents, and in the cyber threat intelligence.[15]

Despite the above advantages and widespread adoption, CKC faces several challenges. Although understanding the cyberattack chain can help companies and governments proactively prepare for and respond to even complex, multi-stage cyber threats, relying solely on this can leave an organisation vulnerable to other types of cyberattacks. Several disadvantages are often cited in relation to CKC, such as:

- Focuses on malware: The original cyber kill chain framework was designed to detect and respond to malware and is not as effective against other types of attacks, such as unauthorised access gained with stolen credentials.
- Ideal for perimeter security mostly: The CKC model was well adapted when the emphasis was on protecting endpoints and only a single or a small number of network perimeter areas needed to be protected. Today, with the rise in the number of remote or home workers, the significant increase in the use of cloud-based systems, and the surge in the number of devices that remotely access corporate assets, it is nearly impossible to manage all endpoint vulnerabilities, especially with this approach.
- It is not prepared for internal threats: Malicious internal employees or external partners who already have access to certain systems are difficult to detect with defences based on the CKC model. Instead, organisations need to monitor and detect changes in user activity (as well).
- Too linear: Although many cyberattacks correspond to the attack methodology described in the CKC (and presented below), which consists of seven (+ n) steps, there are also many attacks that do not follow this methodology or combine several steps into a single operation. Organisations that focus too narrowly on specific stages of the CKC may fail to detect cyber threats that use a different attack methodology.

In addition to all this, or despite it, it can be concluded that the CKC model is an appropriate choice for examining the chosen topic of AI use in cyberattacks and cyber defence. The attack and defence capabilities and options analysed using CKC provide a comprehensive picture of AI use on both the offensive and defensive sides.

[14] Microsoft [s. a.b].
[15] Goss 2024.

The seven (+ n) phases of the Cyber Kill Chain

The CKC framework consists of seven sequential main phases, each of which is an essential step in achieving the attacker's goals. These phases are illustrated in Figure 2 and described briefly thereafter. This series of articles does not aim to provide a detailed description of CKC, so the following description is a simplified summary of the essentials necessary for understanding.

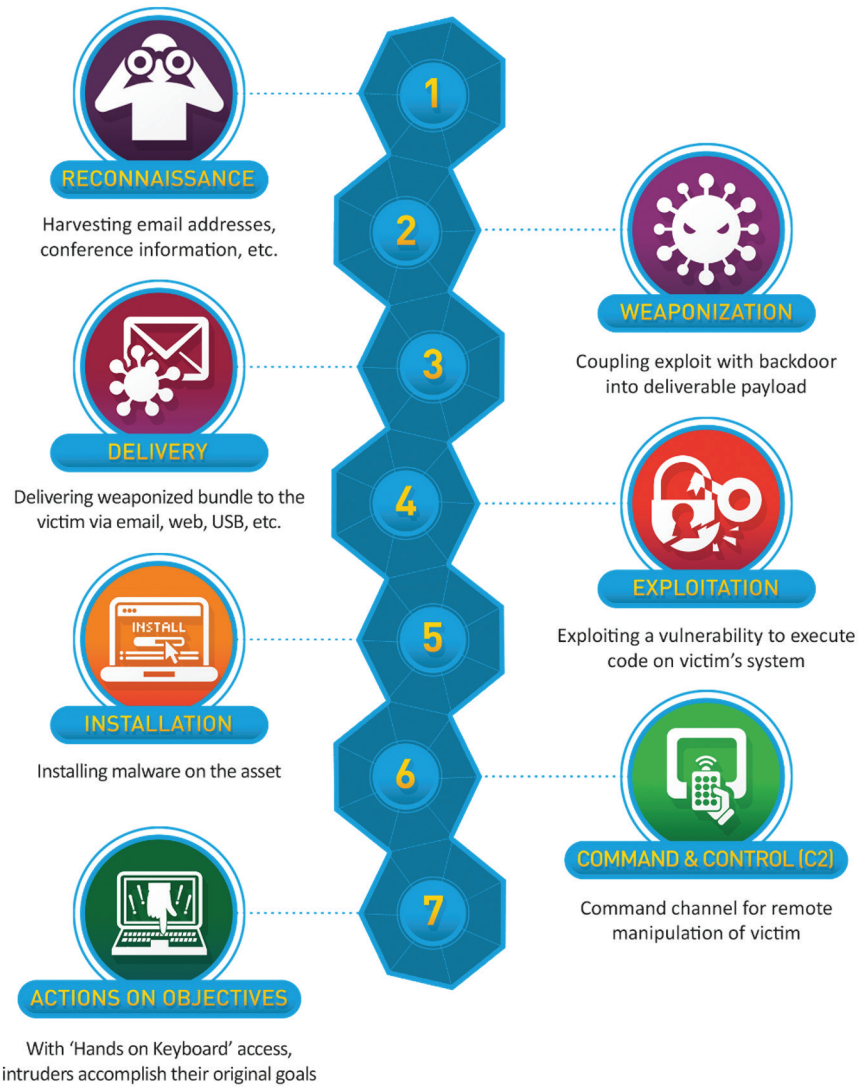


Figure 2: Phases of the Cyber Kill Chain
Source: The Cyber Kill Chain® s. a.

Reconnaissance: At this point, attackers gather information about the target, such as network structure, employees of selected companies and security technologies used for protection. In more detail, this phase includes searching for, identifying and selecting targets, followed by gathering information about the selected targets, such as finding vulnerabilities, identifying third parties connected to the target's systems, and determining what data the attackers can access. Reconnaissance can be carried out both online and offline, typically using OSINT[16] methods, which often involve mapping websites, conference publications, mailing lists, email addresses, social connections or information about specific technologies.

Weaponization: After the attacker has gathered all the necessary information about potential targets, the next step is to create or obtain malicious code or other harmful content to be delivered to the target. For example, attackers compile code that exploits a vulnerability (exploit[17]) and malicious software (payload), then package them into a format that can be delivered to the target (e.g. PDF, Word document, executable file). This can be done by modifying existing malicious attack codes or creating new types of malicious codes. An example of weaponization is combining a remote access Trojan with an exploit and integrating them into some kind of carrier (e.g. the aforementioned Adobe Portable Document Format (PDF) or Microsoft Office documents), or making minor modifications to an existing ransomware variant, etc.

Delivery: In this phase, the attackers deliver the prepared *cyber weapon* to the target. Forms of delivery include, for example, email attachments, infected websites, USB data storage devices, and exploiting vulnerabilities in the target organisation's information and communication systems.

Exploitation: In this phase of the CKC, attackers activate the exploitable vulnerability to exploit the vulnerability of the target system, thereby gaining access to certain elements of the target system. They then move further (e.g. laterally) across the network in an attempt to reach their intended targets.

Installation: During this phase, attackers attempt to install malicious software and/or other cyber weapons on the target network in order to take control of the systems and send valuable data from them. They may use Trojan programs, backdoors or command line interfaces for installation.

Command and Control (C2): At this stage of the attack, the attackers establish a communication channel with the compromised system and use it to remotely control the installed malicious software, sending instructions to it in order to achieve their attack objectives. Such objectives may include, for example, controlling botnets to carry out a Distributed Denial of Service (hereinafter: DDoS[18]) attack against a selected target, or forwarding confidential company documents to the attackers, etc. If

[16] OSINT: Open Source Intelligence, refers to the collection and analysis of publicly available data.

[17] Exploit: exploiting a vulnerability in software or hardware, allowing an attacker to cause unexpected behaviour in the system, such as gaining administrator privileges or causing denial of service.

[18] Distributed Denial of Service (DDoS): This is a malicious attack aimed at completely or partially paralyzing an IT service and preventing it from functioning properly. In the process, attackers flood the server with data traffic of a certain type and volume from multiple sources (in a distributed manner) to the extent that it disrupts its normal operation.

necessary, attackers can also use this channel to install new malicious code or add new modules to the attack tools that have already been installed.

Actions on Objectives: After the attackers have successfully completed the previous phases, i.e. developed the cyber weapons, installed them on the target network, and taken control of the target network, they begin the final phase of the cyberattack: executing the actual objectives of the cyberattack. In other words, this phase is when the attacker achieves their ultimate goal, e.g. involving infected machines in a DDoS attack, stealing information, modifying or destroying data, causing system malfunctions, spreading malicious code, running ransomware, etc.[19]

In recent years, several individuals have been attempting to further develop the CKC framework in various ways, primarily with the aim of eliminating the disadvantages listed above. As a result, many new versions have been created, two of which are worth highlighting here.

One is that the original CKC model has been supplemented with an eighth, so-called monetisation phase, the content of which is as follows:

- Monetization: The step following Lockhead Martin's original CKC phases, which refers to the activities carried out by attackers to generate revenue from the attack, such as using ransomware to extort money from victims or selling sensitive data on the dark web.20

The other is when maintaining the presence of the attack and lateral movements are treated in separate phases (in a loop). Mandiant's attack lifecycle model is presented in Figure 3 below.

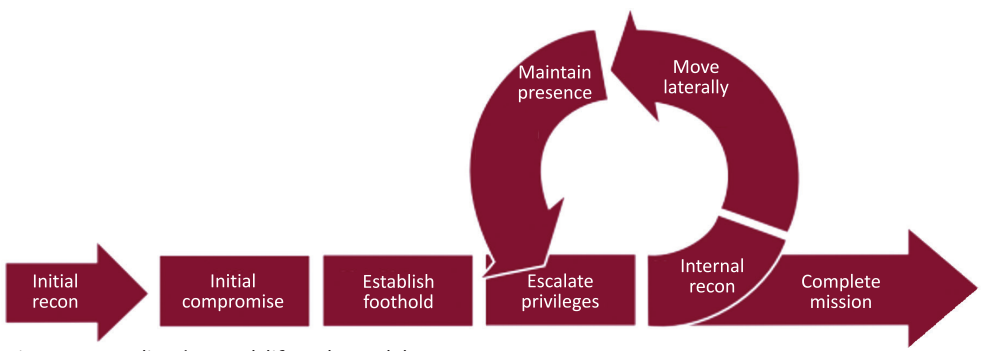


Figure 3: Mandiant's attack lifecycle model
Source: Velazquez 2015: 16

These additional phases – while significant in their own right and useful as supplements in certain attacks – are not necessary for examining the topic of this series of articles, namely the use of artificial intelligence in cyberattacks. The original CKC model is a reasonable choice for this purpose, as the attack options and solutions

[19] Microsoft [s. a.b]; Kidd 2024; Goss 2024.
[20] Microsoft [s. a.b].

analysed along the original 7-phase CKC can provide a comprehensive picture of the use of AI on the attacking side.

Based on the analysis described above, it can be concluded that the Cyber Kill Chain is not merely a list of separate or isolated attack activities, but rather a description of a progressive, interconnected series of attack events. The basic assumption of the CKC framework is that an attack must typically complete each phase sequentially, meaning that each phase or step depends on the success of the previous one, and its success lays the foundation for the feasibility of the next phase.[21] This chained sequential dependency is the fundamental logic behind the CKC concept. However, this also means that interrupting or disrupting the attack chain at any point can prevent the entire attack from being successful, i.e. prevent the attacker from achieving their objectives. This creates an opportunity for cybersecurity professionals to implement multi-layered security measures for the systems they protect, allowing attacks to be detected and neutralised at multiple levels and points. In other words, even if an attacker successfully bypasses certain defensive elements/measures, other tools and defensive methods can detect and interrupt the attack in its next phase. This increases the likelihood of preventing successful attacks.

The CKC framework aims to improve threat detection and response capabilities by identifying the different stages of a cyberattack and enabling defenders to determine the potentially appropriate security measures and equipment that can be effectively used to detect or interrupt a cyberattack.[22] This goes far beyond a purely reactive approach to cyber defence (based on responding to unauthorised intrusions). CKC thus serves as a powerful proactive planning framework, not just a retrospective, post-mortem analysis tool. It helps cybersecurity professionals understand the mindset of attackers, anticipate their moves and deploy appropriate defences at all strategically possible points of attack. This paradigm shift from reactive incident response to proactive threat disruption is key to building resilient cybersecurity architectures. To this end, it is very helpful to examine which AI-supported attack methods and tools are used or can be used by attackers and at which stages of CKC, and which AI-supported defence solutions are used or can be used by defenders at which stages to counter them.

The Cyber Kill Chain model has a significant impact on cybersecurity. It provides cybersecurity professionals with an opportunity to understand how attackers plan and execute their attacks, thereby allowing them to more easily identify and effectively mitigate vulnerabilities in their systems and organisations, and helping them recognise signs of compromise early stages in a cyberattack. For this reason, many organisations use the Cyber Kill Chain model to proactively implement security measures and as a guideline for developing their incident response strategies. Although CKC was originally a defence framework, it is increasingly being used in threat hunting to predict attacker behaviour. By understanding how AI strengthens each phase of the attack chain, defenders can shift their focus from reactive defence to proactive threat hunting and preventive measures that significantly mitigate damage, concentrating

[21] Goss 2024; Pentera [s. a.].
[22] Microsoft [s. a.b]; Goss 2024.

their resources where AI-driven attacks are most likely to occur. This strategic shift moves the focus from merely detecting intrusions into one's own systems to predicting attacks, or at least detecting them early, thereby interrupting the entire attack chain at an early stage or effectively disrupting the various or all phases.

Conclusions

This series of articles deals with the use of artificial intelligence in cyberattacks. Nowadays, there are many scientific publications, reports written by cybersecurity experts, blog posts, etc. that discuss the use of AI in cyberattacks. However, these typically either discuss a specific type of attack in detail or present several such possibilities in a general form. In addition, only a few publications show AI-supported cyberattacks using the CKC, and those that do typically present only a few well-known forms, without attempting to provide detailed content summarising as many forms of attack as possible.

Based on the first part of the series of articles, it can be concluded that the Cyber Kill Chain model, despite all its limitations, is suitable for achieving the goal of the series of articles, i.e. it can be used to demonstrate how attackers can use AI in cyberattacks. This will provide a suitable basis for further research into where and how defenders will be able to detect and disrupt AI-assisted attacks, and what tools they will have at their disposal. However, this requires a comprehensive description that summarises the methods and tools available to attackers in each phase of the CKC.

The following parts of the series of articles will show the actual application possibilities of artificial intelligence in the various phases of the Cyber Kill Chain model on the offensive side and then describe the current challenges and trends arising on this side.

References

Abbadi, Driss – Lachkar, Abdelkader (2024): Cyber Threats in the Age of Artificial Intelligence. Exploiting Advanced Technologies and Strengthening Cybersecurity. *International Journal of Science and Research Archive,* 13(1), 2576–2588. Online: https://doi.org/10.30574/ijsra.2024.13.1.1961

AWS [s. a.]: What is Deep Learning in AI? *AWS,* s. a. Online: https://aws.amazon.com/what-is/deep-learning/

Badman, Annie – Kosinski, Matthew [s. a.]: What is AI security? *IBM/think*. Online: www.ibm.com/think/topics/ai-security

Erdész, Viktor (2023): *A mesterséges intelligencia alkalmazása a katonai nemzetbiztonsági hírszerzésben.* Budapest: Katonai Nemzetbiztonsági Szolgálat. Online: https://bit.ly/4tKmx65

Goss, Adam (2024): The Cyber Kill Chain: A Powerful Model For Analyzing Cyberattacks. *Kraven Security,* 11 March 2024. Online: https://kravensecurity.com/cyber-kill-chain/

Hungary's Artificial Intelligence Strategy 2020–2030 (2020). AI Coalition – Digital Success Programme – Ministry for Innovation and Technology. Online: https://mik.neum.hu/wp-content/uploads/2025/03/2020-hungarian-AI-strategy.pdf

Jordan, Michael I. – Mitchell, Tom M. (2015): Machine Learning: Trends, Perspectives, and Prospects. *Science,* 349(6245), 255–260. Online: https://doi.org/10.1126/science.aaa8415

Kidd, Chrissy (2024): Cyber Kill Chains: Strategies & Tactics. *Splunk,* 26 August 2024. Online: www.splunk.com/en_us/blog/learn/cyber-kill-chains.html

Magyarország Mesterséges Intelligencia Stratégiája (2025–2030) [Hungary's Artificial Intelligence Strategy (2025–2030)] (2025). Online: https://cdn.kormany.hu/uploads/document/c/c0/c0d/c0dfdbd37cfa520ae37361a168d244c85e7295af.pdf

Mattioli, Rossella et al. (2023): *Identifying Emerging Cybersecurity Threats and Challenges for 2030.* European Union Agency for Cybersecurity (ENISA). Online: https://doi.org/10.2824/117542

McCarthy, John (2007): *What is Artificial Intelligence?* Online: https://www-formal.stanford.edu/jmc/whatisai.pdf

Microsoft [s. a.a]: What is AI for Cybersecurity? *Microsoft Security,* s. a. Online: www.microsoft.com/en-us/security/business/security-101/what-is-ai-for-cybersecurity

Microsoft [s. a.b]: What is the Cyber Kill Chain? *Microsoft Security,* s. a. Online: www.microsoft.com/en-us/security/business/security-101/what-is-cyber-kill-chain

Pentera [s. a.]: Cyber Kill Chain. Glossary *Pentera,* s. a. Online: https://pentera.io/glossary/cyber-kill-chain-framework-explained/

Radle, Andrew J. et al. (2023): *MITRE FiGHT™: High-Level Overview. MITRE Five-G Hierarchy of Threats (FiGHT).* The MITRE Corporation. Online: https://fight.mitre.org/FiGHT_High-Level_Overview_PRS-23-2698.pdf

Team Antier (2022): DAO és Metaverzum: Egy kiváló kombináció és megoldás a holnap világa számára. *Antier Solutions*. 4 October 2022. Online: www.antiersolutions.com/hu/blogok/A-dao-%C3%A9s-a-metaverzum-egy-kiv%C3%A1l%C3%B3-kombin%C3%A1ci%C3%B3-%C3%A9s-megold%C3%A1s-a-holnap-vil%C3%A1ga-sz%C3%A1m%C3%A1ra/

The Cyber Kill Chain® [s. a.]. Lockheed Martin. Online: www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Usman, Yusuf – Upadhyay, Aadesh – Chataut, Robin – Gyawali, Prashnna K. (2024): *Is Generative AI the Next Tactical Cyber Weapon for Threat Actors? Unforeseen Implications of AI Generated Cyber Attacks.* arXiv:2408.12806. Online: https://doi.org/10.48550/arXiv.2408.12806

Velazquez, Chris (2015): *Detecting and Preventing Attacks Earlier in the Kill Chain.* Global Information Assurance Certification Paper. The SANS Institute. Online: www.giac.org/paper/gsec/36774/detecting-preventing-attacks-earlier-kill-chain/145219

Wolfenstein, Konrad (2023): Mesterséges intelligencia vagy metaverzum? Mi a fontosabb? Vagy itt szinergiák alakulnak ki a további úttörő fejlesztések érdekében? *Xpert.Digital,* 28 December 2023. Online: https://xpert.digital/hu/ki-metaverzum/

HADMÉRNÖK
VÉDELEMINFORMATIKA

20. évfolyam (2025) 4. szám 53–67.
DOI: 10.32567/hm.2025.4.4

Zoltán Kovács[1]

The Use of Artificial Intelligence in Cyberattacks, Part 2

Phases 1–4 of the Cyber Kill Chain Model

Abstract

The first part of this series of articles provided an overview of artificial intelligence (AI) and its various subfields (e.g. machine learning, generative AI, etc.), and showed that the Cyber Kill Chain (CKC) model, despite all its limitations, is suitable for achieving the goal of this series of articles, i.e. it can be used to demonstrate how attackers can use AI in cyberattacks. In order to develop adequate cyber defence against AI-assisted cyberattacks, it is necessary to know what AI-assisted tools attackers can use in each phase of the attack. This article focuses on the first four phases of the CKC model (reconnaissance, weaponization, delivery and exploitation) to examine where and how attackers are already using artificial intelligence in the first four phases of the Cyber Kill Chain model to achieve their goals, and how this helps attackers.

Keywords: artificial intelligence, cybersecurity, cyberattack, Cyber Kill Chain, OSINT, exploit, evasion, phishing, malware

Introduction

The emergence of AI in cybersecurity is a double-edged sword. On the one hand, it assists defensive personnel by offering significant potential for strengthening cyber defence systems and automated threat detection, On the other hand, however, it also provides malicious actors with an extremely effective tool for executing sophisticated, adaptive, and difficult-to-detect cyberattacks.[2] In order to build adequate

[1] Senior Lecturer, Ludovika University of Public Service, e-mail: zkovacs.24@gmail.com
[2] Abbadi–Lachkar 2024.

and effective defence against sophisticated AI-powered cyberattacks, it is necessary to understand what means and methods can be used by attackers. In this regard, Sun Tzu's words in *The Art of War* ring true:

"If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. […] If you know neither the enemy nor yourself, you will succumb in every battle."[3]

This series of articles therefore focuses on providing a summary description of the AI-supported forms of attack currently in use in each phase of cyberattacks according to the Cyber Kill Chain model.

Numerous scientific articles, reports prepared by cybersecurity companies, blog posts written by experts, etc. have been published on AI-assisted attacks. However, based on the topic and main objective of this series of articles, they can typically be classified into three categories. The first category includes those that analyse an AI-assisted attack in depth. These descriptions help defenders prepare for a given attack and take preventive measures in the appropriate elements of their overall defence system (e.g., implementing new firewall rules, searching for indicators of compromise, or IoCs,[4] and loading them into defence tools for blocking, etc.). At the same time, defenders need to deal with each of these individually when developing their defences, gathering and synthesising the knowledge necessary to develop general defence principles.

The second category includes descriptions that provide a more general, comprehensive overview of several AI-supported attack types in a single document. These typically contain fewer technical details and instead provide an overview of several types of attacks. These documents help defenders develop more general defence methods and identify missing defence elements. However, these descriptions do not typically present AI-assisted attacks following the steps defined by the CKC, so defenders need to break them down and classify the individual parts of the attack method into the CKC phases if they want to take advantage of the defences built on this basis. The third category includes documents that describe AI-assisted attack forms according to the CKC model. On the one hand, the number of such works is low, and on the other hand, they typically do not attempt to summarise previously published cases. Such documents are typically published by cybersecurity companies, which present their own detected cases in this way. These documents help defenders develop effective defence systems according to the CKC, but even in this case, defenders need to process and synthesise many similar documents to achieve their goal of effective defence.

Based on the above, a document that synthesises and summarises numerous and wide-ranging AI-supported cyberattack methods based on the CKC could fill a gap, providing defenders with a general and comprehensive picture that they can use to

[3] Giles 2013.

[4] IoC (Indicator of Compromise) refers to digital traces that indicate the presence of a cyberattack, such as hacking or malware infection, on a system or network. These can include suspicious IP addresses, unknown file hashes, unusual network traffic or changes to system files.

develop effective defences. At the same time, further detailed studies are needed to develop defences (e.g. where and how traditional, i.e. non-AI-supported defence tools can still be used, what AI-supported cyber defence tools are available, how their operation can be coordinated with the help of, for example, SOAR[5], etc.). However, due to the depth and scope of the topic, these will be the subject of another series of articles. This series of articles focuses on summarising AI-supported attacks and breaking them down according to CKC, which is necessary to build a foundation for this.

The second part of this series of articles examines the options currently available to attackers in the first four phases of CKC if they wish to use AI-supported tools for their attacks and shows how these tools can help attackers achieve their goals.

The application of AI in the individual phases of the Cyber Kill Chain

The capabilities of artificial intelligence, and thus its use, significantly enhance attackers' capabilities in cyberattacks, enabling them to accelerate, automate and refine their execution. The following chapters describe in detail how attackers utilise artificial intelligence in each phase of the CKC (i.e. the cyberattack chain) and what specific technologies can be used by attackers to achieve their malicious goals. By using AI capabilities, attackers have achieved spectacular results in their attacks, for example, by developing phishing, creating polymorphic malicious code, or carrying out highly deceptive identity theft. Based on data reported by various organisations, the speed of detected cyberattacks has increased by 250% over the past 3 or 4 years, with detected security incidents taking less than an hour from compromise to exfiltration in 20% of cases.[6]

Phase 1: Reconnaissance

Reconnaissance is the first and essentially foundational phase of a cyberattack, the main purpose of which is to select the target(s) and gather relevant information about them in order to plan the attack strategy.[7] AI can significantly speed up and improve the efficiency of this process, allowing attackers to gain deeper and more accurate insight into the target(s)' system(s) and more easily find their potential weaknesses.[8] Such AI-supported tools and methods may be for example:

- *Automated open-source intelligence (OSINT) gathering and target profiling:* AI-based tools, especially natural language processing (NLP) and machine learning (ML), enable attackers to automatically collect and analyse vast amounts of publicly available data (e.g. social media profiles, company websites, patent databases, (cyber)security reports, job offers, news articles,

[5] SOAR: security orchestration, automation and response tool enabling coordinated, automated management and response to security incidents.
[6] Verton 2025.
[7] Hutchins et al. 2011.
[8] Schröer et al. 2025.

public code repositories, dark web, forums, etc.) and create profiles. From the information collected in this way, AI can, for example, identify the hierarchy of employees, email addresses and naming conventions, the technological infrastructure and software being used, network topologies, and even information about the organisational culture at the target company. This is why automated OSINT is critically important during reconnaissance, and AI can exponentially increase the efficiency of this process. Consider, for example, a case where AI-supported entity recognition can automatically identify key individuals and roles in a company's hierarchy and correlate them with public profiles (e.g. social media), which can form the basis for (even automated) targeted phishing attacks (e.g. spear-phishing,[9] whaling[10]).[11]

- *Network topology and infrastructure mapping:* AI can passively monitor network traffic and publicly available DNS records to automatically build the topology of the target network. The AI algorithms used by attackers can identify active services, open ports, operating system types and network device characteristics, often even when defenders attempt to hide them. This ability allows attackers to identify key vulnerabilities, recognise how to achieve a persistent presence in the compromised network and choose more effective attack vectors.[12]
- *Vulnerability detection and prediction:* Traditional vulnerability scanners used (also) by attackers are often signature-based and therefore easily detected by defenders. Instead, AI-based vulnerability scanners use machine learning algorithms to identify patterns in network protocols or system configurations that may indicate potential zero-day vulnerabilities. So-called *hunting* AIs are increasingly able to automatically identify these potential vulnerability patterns in code bases. In addition, AI-supported attack tools are able to search for and find correlations between large vulnerability databases (e.g. CVE) and target system parameters, predicting which vulnerabilities will be able to be successfully exploited by attackers.[13]
- *Analysis of employee behaviour and their weaknesses:* The analytical capabilities of advanced AI-powered attack systems can extend beyond information and communication systems to include the human factor. The AI algorithms used by attackers are capable of analysing employees' online spatial behaviour (e.g. posts, areas of interest), which they can use to identify individuals who are susceptible to psychological manipulation based social engineering attacks or to recognise poor cyber hygiene habits. This can form the basis for personalised attacks. The combination of AI-driven OSINT and AI-supported behavioural analysis provides attackers with extremely effective, *human-centric* vulnerability detection capabilities. This possibility shifts the focus of attacks

[9] Spear phishing is a type of cybercrime where attackers try to trick their victims (a specific person or organisation) with personalised messages to get confidential info. It's different from traditional phishing because it's way more targeted and personalised.

[10] Whaling is a highly targeted form of phishing that specifically targets individuals in senior positions (CEOs, CFOs, etc.), who are referred to as *whales*.

[11] Mirsky et al. 2023; Dees 2025.

[12] Yamin et al. 2021.

[13] Amster [s. a.]; Glynn 2025.

from merely detecting and exploiting technical vulnerabilities to detecting and exploiting human and organisational weaknesses, thereby bypassing traditional perimeter-based cyber defence systems and therefore making them less effective. Social engineering attacks based on psychological manipulation, including BEC (Business Email Compromise) threats, email scams and phishing, are becoming increasingly sophisticated thanks to AI-generated, deceptively realistic content. This also means that attacks no longer rely solely on technical weaknesses and vulnerabilities in systems, but increasingly exploit user inattention and poor digital hygiene, highlighting the importance of focusing on the human factor in defence.[14]

- *Acoustic side-channel attacks:* AI can also be used for acoustic side-channel attacks, for example, by analysing the sounds of keyboard keystrokes, it is possible to deduce which keys were originally pressed and thus recover the information entered in this way. This capability can be effective even with limited input data and provides new attack surfaces during the CKC reconnaissance phase.[15]

Overall, it can be said that the use of AI by attackers in the CKC reconnaissance phase significantly helps them to drastically reduce the manual effort and time required to detect targets, enabling them to identify their targets and vulnerabilities in greater numbers and with greater precision. This increase in efficiency allows attackers to move forward with their attacks more quickly, increasing the scale and number of their offensive operations, thereby further reducing the time available to defenders to identify and fix their own vulnerabilities.

Phase 2: Weaponization

In this phase, based on the information gathered during the reconnaissance phase, the attacker prepares and packages the malicious tool (exploit + payload) needed for the attack, i.e. prepares their cyber weapon. AI greatly increases the customisation, sophistication and resistance to detection by cyber defence tools of this cyber weapon.[16]

- *AI-based malware creation and adaptation:* Generative AI models, especially generative adversarial networks (GANs), could revolutionise the development of malicious code. GANs consist of two neural networks (generator and discriminator) that compete with each other and ultimately produce better output (results) than if only one network were operating and providing results for a given question or task.[17] In terms of malware, this means that the generator creates new malicious code, while the discriminator attempts to distinguish the newly generated code from existing malicious code or the

[14] Al-Azzawi et al. 2025; Cybersecurity Forecast 2025.
[15] Park et al. 2025.
[16] Navigating a New Threat Landscape 2024.
[17] Goodfellow et al. 2020.

original malware on which the development is based, feeding back the results so that the generator can continuously improve the newly generated malicious code. Within that, the main focus is on the new malware's ability to remain hidden from security systems. AI also enables the creation of polymorphic[18] and metamorphic[19] malware that continuously changes its code or structure, thereby increasing the likelihood that traditional cyber defence tools, such as signature-based antivirus software, will fail to detect it. In addition, AI can optimise the code of newly generated malware based on specific characteristics of the target system, such as the version of the operating system used in the target system, the security software installed, or even the hardware architecture, thereby increasing the likelihood of a successful attack. By using GANs, attackers can create new malware that is not yet included in the databases of defence systems, making traditional signature-based detection less effective against them. This capability fundamentally changes the nature of cyber threats, shifting the focus from static, relatively easy-to-identify patterns to dynamic, evolving and difficult-to-detect threats.

- Malicious, especially generative AI models specifically designed for this purpose (Generative Pre-trained Transformers, GPTs), such as WormGPT or FraudGPT, are capable of generating functional malware, including obfuscated[20] and polymorphic variants that can evade traditional detection methods. In addition to creating new malware, these large language models are also capable of modifying and rewriting the code of publicly available malicious software, thereby creating new variants. They can do this by translating them into other programming languages or by adding new features to existing malware, thereby modifying it. An example of the latter is adding AES encryption to existing code, which makes it more difficult to detect, track and analyse the new variant generated in this way.
- Due to their easy accessibility and simplicity of use, tools such as FraudGPT and WormGPT can serve as a kind of *cybercriminal starter kit* as they are capable of generating hard-to-detect malicious code, phishing sites and other hacking tools based on a few entered commands. This significantly lowers the

[18] Polymorphic malware: malicious software that can change its own code with each infection in order to make it more difficult to detect by traditional defence tools, such as antivirus software. Polymorphic malware changes its original code so that each time it infects a system, it has a different, unique code fragment and binary code structure, while its malicious function remains unchanged. Malware often includes a mutation engine that automatically generates new encryption keys and algorithms (translated by the author). itszótár.hu 2025.

[19] Metamorphic malware: in addition to the characteristics of polymorphic malware, it is also capable of changing, rewriting, translating, and editing its own code, so that each new version differs from the previous one, all without using an encryption key. This is a more advanced technique than polymorphic malware, which uses a key to modify the code. Metamorphic malware is more difficult to detect and identify because its code is constantly changing, it has no constant part that would identify it, and it does not return to its original form; each distributed version differs from the previous ones. This rewriting may involve changing the order of the code, adding unnecessary instructions (so-called *garbage code*), or replacing existing instructions with instructions that have equivalent functionality but different code (translated by the author). itszótár.hu 2025.

[20] Obfuscated code: the source code is deliberately made difficult to understand and unreadable, i.e. it is modified (e.g. by using meaningless variable names) to make it difficult to analyse, but the programme continues to function unchanged.

threshold for entering the world of cybercrime, meaning that even those with little or moderate IT knowledge can successfully enter this branch of crime.[21]

- *Exploit selection:* AI is capable of matching existing or newly generated malicious code with known exploits needed to benefit from it, as well as automating the selection of documents used as bait, thereby significantly increasing the effectiveness and speed of attacks.[22]
- *Intelligent exploit generation:* AI can also accelerate the discovery of new code-level vulnerabilities by analysing patterns in existing vulnerabilities. AI can also help attackers by automating the creation of exploit codes for previously known or newly discovered vulnerabilities. LLMs have been proven in a research environment to be capable of identifying vulnerabilities in various network and software systems and can even generate Proof-of-Concept (PoC) code for real exploits. Although this is still largely in the research phase, reinforcement learning (RL) and deep learning (DL) have the potential to be used to generate autonomous exploits, i.e. exploits that operate independently, without human intervention, and are capable of automatically intruding into a system and exploiting its vulnerabilities. RL agents can learn how to search for code patterns that may contain potential vulnerabilities in software and how to develop exploits that can exploit them (e.g. buffer overflow, format string vulnerability). AI can therefore be capable of code analysis, debugging and generating effective exploit code by simulating possible exploit vectors, which can drastically reduce the time and expertise required for exploit development.[23]
- *Generating spear-phishing and social engineering content:* natural language processing (NLP) and generative AI models (especially LLMs) are extremely effective at automatically generating hyper-personalised and realistic, i.e., customised, convincing and grammatically flawless phishing emails, messages (smishing[24]) or even voice calls (vishing[25]). Based on information obtained in the earlier stages of the attack, AI is able to mimic the target's communication style, incorporate personal or corporate information collected during the reconnaissance phase into messages intended for the target, and even dynamically change the type of content (e.g. urgent financial request, HR notification, IT support). AI-based deepfake technology, which enables the creation of extremely realistic but fake video and audio content, is a great help to attackers in producing such content. Attackers often use Generative Adversarial Networks (GANs), described earlier, to produce deepfake content.
- Generative AI also facilitates transnational and translingual cybercrime by enabling attackers from countries that do not speak the language of the target

[21] Usman et al. 2024; Arif et al. 2024.
[22] Salem–Mrian 2025.
[23] Zhu et al. 2025; Haurogné et al. 2024.
[24] Smishing: a form of phishing that takes place via text messages. Fraudsters use text messages to try to trick recipients into revealing confidential information, such as personal details, bank details or access codes.
[25] Vishing: a word combining the English words voice and phishing. An online fraud method in which attackers attempt to obtain sensitive data from victims over the phone.

country to bridge significant language gaps and create convincing phishing attacks or other attackable content with perfect grammar.
- All of these factors significantly increase the likelihood of successful social engineering attacks.[26]
- *Integration of AI-driven defence evasion techniques:* As a part of preparing the cyber weapon used for the attack, artificial intelligence elements can be integrated into the payload so that it can intelligently evade the deployed cyber defence systems. This may include the ability for AI to adaptively modify the attack execution logic, the file size of the attack code, its hash, or even its network communication in order to circumvent defences such as antivirus software, intrusion detection systems (IDS[27]), intrusion prevention systems (IPS[28]), or even sandboxing environments. AI can recognise and learn the behaviour of the security tools of the target system, even if they are AI-controlled, and carry out adversarial attacks that can deceive even defensive AI models. This ability allows attackers to not only evade existing security protocols, but also actively manipulate the AI-based detection mechanisms of the defence systems.[29]

Overall, it can be said that by exploiting the capabilities of AI, attackers will become more effective in the second, weaponization phase of CKC. AI significantly simplifies the creation of new variants or even completely new malicious code and cyber weapons, and its built-in functions help them remain hidden from security systems. AI is also a great help in producing deceptive content that can be used for attacks. This fundamentally transforms the weaponization phase, as attackers can develop more effective and adaptable tools with less effort, making traditional signature-based detection methods increasingly obsolete.

Phase 3: Delivery

In the delivery phase, the attacker delivers the weapons prepared in the previous phase (e.g. malware, exploit) to the target system or user. AI also assists the attacker in this phase of the attack by making delivery as covert and effective as possible. It increases the effectiveness of social engineering or phishing attacks used by the attacker.[30]

- *Optimised delivery channels and timing:* AI can analyse the network traffic of target systems, the security configurations of target systems and user behaviour patterns in order to choose the least conspicuous and least protected delivery route for delivering malicious code. For example, machine learning

[26] Falade 2023; Yu et al. 2024.
[27] IDS: intrusion detection system, a system that monitors and analyses network traffic in order to detect malicious activity and policy violations and then issues an alert when something is detected.
[28] IPS: intrusion prevention system, a security technology that monitors network traffic in real-time for malicious activity and automatically takes action to block or prevent threats like malware, exploits and unauthorised access.
[29] Fritsch et al. 2022; Singh–Cheema 2024.
[30] 'What is the cyber kill chain?', Microsoft [s. a.].

(ML) can identify periods that may be more favourable for carrying out an attack (e.g. outside of working hours, on weekends when users are less attentive or during periods when security systems are under higher load). AI can also dynamically select the delivery method tailored to the target, whether it be email, an infected website, a software update, or even a suggestion to use physical data storage. AI can also help attackers configure and deploy malware. AI-driven adaptive attack strategies allow attackers to adapt in real time to changes in the defence mechanisms and infrastructure of target systems, thereby helping to maximise the success and impact of the attack.[31]

- *Hiding delivery using steganography*[32] *and polymorphism:* AI can also help attackers deliver their cyber weapons (malicious payloads) to their targets in a way that is difficult to detect, for example by hiding them in legitimate files (such as images or audio files) using steganography techniques. Polymorphic code generation has already been discussed in the section on the *Weaponization* phase. However, this is also an effective aid for attackers during delivery, as the ability of malware to change its form allows it to avoid detection by signature-based detection tools, such as network intrusion detection systems (NIDS[33]), during delivery.[34]
- *Automated password cracking:* Even if the attacker already has certain data (e.g. username) to access the target system, they may still need additional valid authentication data (e.g. password). AI-based password cracking tools (e.g. PassGAN) can effectively assist the attacker, as they can quickly generate likely passwords by learning from databases of leaked credentials. This generative AI tool models the distribution of real passwords and produces highly accurate results without human intervention or input rules. This increases the speed at which certain authentication data can be cracked.[35]
- *Execution of intelligent phishing campaigns:* The capabilities of generative AI and natural language processing (NLP) are not only useful for generating personalised malicious content for attacks but are also extremely important for attackers in executing attack campaigns. AI can refine the delivery pattern of already hyper-personalised and realistic phishing messages in real time, taking into account the reactions of recipients and the defences of the attacked system (e.g. number of opens, number of clicks, ending up in the spam folder, etc.). AI can automatically modify the subject line, sender name, or even the structure of embedded malicious links if it detects that previous attempts have been unsuccessful and/or have been detected by the target's security systems. This adaptive behaviour significantly increases the effectiveness of attack campaigns and the likelihood of avoiding detection. Attack campaigns

[31] Potter et al. 2025; Kumar–Chauhan 2025.

[32] Steganography is a branch of computer science/cryptography that aims to hide secret messages, not by encrypting the message itself (using cryptography), but by hiding the fact of communication from others, most often by embedding it in media files (e.g. images, sounds).

[33] NIDS: network intrusion detection system, which monitors network traffic and issues alerts when it detects suspicious activity or violation of rules.

[34] Fadhil 2025; Potter et al. 2025.

[35] Hitaj et al. 2019.

thus become more resistant to the initial defensive responses of target systems, creating a continuous learning loop for attackers and obsoleting static cyber defence mechanisms.
- AI-generated phishing emails have a worrying success rate, and fully AI-based, automated phishing attacks now have a success rate that has overtaken attacks carried out with human involvement.
- In this phase, AI-based chatbots also assist attackers, as they can be used to automate real-time communication with targets in specific cases in such a way that they are almost indistinguishable from a human being on the other end of the conversation. This greatly facilitates the collection of authentication data, for example.[36]
- *Attacks against the supply chain:* Attackers can also use AI in supply chain attacks, for example to inject malicious code into the software supply chain. Vulnerabilities in AI models, such as data poisoning or Trojan models, can also help attackers deliver malicious code if they use public AI models at the target organisation.[37]

Overall, it can be said that in the third phase of CKC, the use of AI in delivery effectively increases the success rate of attacks by facilitating evasion, supporting password cracking, and enabling highly targeted and persuasive campaigns that overcome human perception and language barriers. The latter, as AI-generated content becomes increasingly indistinguishable from legitimate communication, further reinforces the fact that humans will be the most vulnerable part of the defence of information and communication systems.

Phase 4: Exploitation

In the exploitation phase, the cyber weapon that has been prepared and delivered becomes active and exploits one (or more) vulnerabilities in the target system in order to gain access to the target network or one of its components. In this case, AI can also increase the speed and accuracy of the attack, help evade the target network's defence systems, combine vulnerabilities that can be exploited by the attacker, and improve the chances of obtaining the authentication data needed for impersonation, thereby helping the attacker to raise their level of authorisation.[38]

- *Autonomous exploit execution and optimisation:* AI, especially reinforcement learning (RL), and AI-driven attack strategies such as adaptive exploit execution, enable attackers to adapt in real time to the defence mechanisms of the target system and changes in the infrastructure of the victim, thereby significantly increasing the likelihood of a successful attack. Based on the responses of the target system, AI is capable of dynamically modifying the execution of the

[36] Dean 2025; Hoxhunt [s. a.].
[37] Fernández 2025; Blake 2025.
[38] Hutchins et al. 2011.

exploit in real time. If an exploit does not work the first time, AI can analyse the errors, the error codes returned, or even the behaviour of the system, and modify the attack parameters accordingly to ensure the attack is successful. This capability minimises the need for human intervention and speeds up the exploitation phase of the attack.[39]

- *Intelligent evasion techniques during the exploitation phase:* In the Weaponization phase, attackers can use the elements integrated into the payload described in Phase 2. AI-controlled exploits are capable of detecting and adapting to the target system and its security elements, actively circumventing cybersecurity elements such as antivirus (AV) software, intrusion detection systems (IDS/IPS) and sandbox environments. This is possible because AI can learn the detection mechanisms of defence systems and carry out adversarial attacks that deliberately deceive even machine learning-based detection models. For example, an attacking AI can change the exploit code, or the sequence of system calls to appear legitimate to the defensive AI or even manipulate the inputs of defensive AI models to cause them to make incorrect classifications or decisions.
- In order to evade detection by security systems used in the target system, they may also attack AI-based protection solutions themselves, for example by manipulating input data, which leads to incorrect predictions or event classification. Such attacks may include poisoning training databases, continuously and subtly altering input data (e.g. by adding noise), or modifying the parameters of pre-trained models (model manipulation). Attackers do all this in order to negatively influence the accuracy of defence AI-based systems, thus also resulting in incorrect decision-making and/or event classification. These, in turn, directly affect the ability of defence AI to detect and report attack attempts. These attacks are already effectively a direct *AI against AI* type of ongoing battle, which will intensify in the near future. On both the offensive and defensive sides, speed, the ability to respond to changes, and ultimately adaptive learning will make the use of AI alongside humans indispensable.[40]
- *Application of polymorphism and metamorphism during exploitation:* Malware generated with the help of AI can change its code or behaviour in real time if it detects signs or attempts at detection. This makes it even more difficult for defence mechanisms such as dynamic analysis or behaviour-based detection to work, as the malicious software constantly *changes its shape* while running. Attackers can also use this feature of malware to their advantage during the exploitation phase.[41]

AI can also provide significant assistance to cyber attackers during the exploitation phase of a CKC. Autonomous exploit execution, the use of intelligent evasion techniques, and the dynamic, autonomous adaptation of malicious code to a given target

[39] Rohlf 2025; Luong et al. 2025.
[40] Nobles 2024; Syed 2025.
[41] Alrzini–Pennington 2020; SentinelOne 2025.

system all make detection significantly more difficult and increase the likelihood of a successful intrusion. In addition, adaptive exploitation means that even patched vulnerabilities can be re-exploited by attackers through new, AI-generated attack vectors, requiring continuous, real-time vulnerability assessment and remediation on the defence side. This requires a lot of resources from them.

Conclusions

The second part of this series of articles examined where and how attackers use artificial intelligence in the first four phases of the Cyber Kill Chain model to achieve their goals, and how this helps them. In 2024, major cybersecurity companies wrote in their annual studies that attackers typically used artificial intelligence in the first two phases of the CKC, i.e. reconnaissance and weaponization, for example, to create fake profiles, processing large amounts of data collected from stolen or publicly available information when mapping targets, phishing, creating deepfake videos, generating malicious code, and possibly controlling DDoS attacks in later phases. Based on an examination of the first four phases, it can already be said that the development of AI over the past 1.5–2 years has also led to significant advances in its malicious use. In order for the defence side to keep up with this, it is necessary to understand where and how attackers use AI in the later phases, and further research is needed to examine what options are available to defenders and where further developments are needed to create effective defences. The next part of the series continues this investigation and examines AI-assisted attacks in the last three (plus one) phases of the CKC. It then discusses the current challenges and trends in the use of AI on the offensive side, making recommendations for the direction of further research.

References

Abbadi, Driss – Lachkar, Abdelkader (2024): Cyber Threats in the Age of Artificial Intelligence. Exploiting Advanced Technologies and Strengthening Cybersecurity. *International Journal of Science and Research Archive,* 13(1), 2576–2588. Online: https://doi.org/10.30574/ijsra.2024.13.1.1961

Al-Azzawi, Mays – Doan, Dung – Sipola, Tuomo – Hautamäki, Jari – Kokkonen, Tero (2025): Red Teaming with Artificial Intelligence-Driven Cyberattacks: A Scoping Review. *arXiv:2503.19626.* Online: https://doi.org/10.48550/arXiv.2503.19626

Alrzini, Joma – Pennington, Diane (2020): A Review of Polymorphic Malware Detection Techniques. *International Journal of Advanced Research in Engineering and Technology (IJARET),* 11(12), 1238–1247. Online: https://doi.org/10.34218/IJARET.11.12.2020.119

Amster, Alex [s. a.]: Automating Vulnerability Detection in Networks with AI. *AllStarsIT,* s. a. Online: www.allstarsit.com/blog/automating-vulnerability-detection-in-networks-with-ai

Arif, Aftab – Khan, Muhammad Ismaeel – Khan, Ali Raza A (2024): An Overview of Cyber Threats Generated by AI. *International Journal of Multidisciplinary Sciences and Arts,* 3(4), 67–76. Online: https://doi.org/10.47709/ijmdsa.v3i4.4753

Blake, Harrison (2025): *AI-Powered Threats in Supply Chains: A Looming Cybersecurity Challenge.* ResearchGate. Online: www.researchgate.net/profile/Harrison-Blake-2/publication/389274676_AI-Powered_Threats_in_Supply_Chains_A_Looming_Cybersecurity_Challenge/links/67bc8c29461fb56424e8923e/AI-Powered-Threats-in-Supply-Chains-A-Looming-Cybersecurity-Challenge.pdf

Cybersecurity Forecast 2025 (2025): Google Cloud Security. Online: https://cloud.google.com/blog/topics/threat-intelligence/cybersecurity-forecast-2025

Dean, B. (2025): New Report: Over 80% of Cyberattacks Now Use AI. *Programs.com*, 8 August 2025. Online: https://programs.com/resources/ai-cyberattack-stats/

Dees, Mels (2025): CrowdStrike Introduces Tools to Block Malicious AI Models. *Techzine Global,* 30 April 2025. Online: www.techzine.eu/news/security/130990/crowdstrike-introduces-tools-to-block-malicious-ai-models/

Fadhil, Ammar (2025): Enhancing Data Security: A Hybrid Approach of AI-Driven Steganography and Encryption. *The Indonesian Journal of Computer Science,* 14(2). Online: https://doi.org/10.33022/ijcs.v14i2.4759

Falade, Polra V. (2023): Decoding the Threat Landscape: ChatGPT, FraudGPT, and WormGPT in Social Engineering Attacks. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology,* 9(5), 185–198. Online: https://doi.org/10.32628/CSEIT2390533

Fernández, Rodrigo (2025): AI-Driven Supply Chain Attacks: The New Cyber Risk in 2025. *NeuralTrust,* 25 September 2025. Online: https://neuraltrust.ai/blog/ai-driven-supply-chain-attacks

Fritsch, Lothar – Jaber, Aws – Yazidi, Anis (2022): An Overview of Artificial Intelligence Used in Malware. In Zouganeli, Evi – Yazidi, Anis – Mello, Gustavo – Lind, Pedro (eds.): *Nordic Artificial Intelligence Research and Development.* Cham: Springer International Publishing, 41–51. Online: https://doi.org/10.1007/978-3-031-17030-0_4

Giles, Lionel (2013): *Sun Tzu on the Art of War.* London: Routledge. Online: https://doi.org/10.4324/9781315030081

Glynn, Fergal (2025): AI Vulnerability Scanner: 6 Practical Metrics Every Security Team Should Monitor. *Mindgard,* 25 August 2025. Online: https://mindgard.ai/blog/ai-vulnerability-scanner-metrics

Goodfellow, Ian et al. (2020): Generative Adversarial Networks. *Communications of the ACM,* 63(11), 139–144. Online: https://doi.org/10.1145/3422622

Haurogné, Jean – Basheer, Nihala – Islam, Shareeful (2024): Vulnerability Detection Using BERT based LLM Model with Transparency Obligation Practice towards Trustworthy AI. *Machine Learning with Applications,* 18. Online: https://doi.org/10.1016/j.mlwa.2024.100598

Hitaj, Briland – Gasti, Paolo – Ateniese, Giuseppe – Perez-Cruz, Fernando (2019): PassGAN: A Deep Learning Approach for Password Guessing. *arXiv:1709.00440.* Online: https://doi.org/10.48550/arXiv.1709.00440

Hutchins, Eric M. – Cloppert, Michael J. – Amin, Rohan M. (2011): Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. *Leading Issues in Information Warfare & Security Research,* 1(1), 1–14.

ITszótár.hu (2025): Metamorf és polimorf kártevők: Ezen kártékony szoftverek működésének magyarázata. *ITszotar.hu,* 15 May 2025. Online: https://itszotar.hu/metamorf-es-polimorf-kartevok-ezen-kartekony-szoftverek-mukodesenek-magyarazata/

Kumar, Ankit – Chauhan, Nidhi (2025): AI-Driven Optimization for Enhancing Performance, Efficiency, and Personalization in Content Delivery Networks. *International Journal of Computer Techniques,* 12(3), 1–9. Online: https://ijctjournal.org/wp-content/uploads/2025/06/AI-Driven-Optimization-for-Enhancing-Performance-Efficiency-and-Personalization-in-Content-Delivery-Networks.pdf

Luong, Phung D. et al. (2025): xOffense: An AI-driven Autonomous Penetration Testing Framework with Offensive Knowledge-Enhanced LLMs and Multi Agent Systems. *arXiv:2509.13021v1.* Online: https://arxiv.org/html/2509.13021v1

Microsoft [s. a.]: What is the Cyber Kill Chain? *Microsoft Security,* s. a. Online: www.microsoft.com/en-us/security/business/security-101/what-is-cyber-kill-chain

Mirsky, Yisroel et al. (2023): The Threat of Offensive AI to Organizations. *Computers & Security,* 124. Online: https://doi.org/10.1016/j.cose.2022.103006

Navigating a New Threat Landscape (2024). Darktrace. Online: www.darktrace.com/resources/navigating-a-new-threat-landscape

Nobles, Calvin (2024): The Weaponization of Artificial Intelligence in Cybersecurity: A Systematic Review. *Procedia Computer Science,* 239, 547–555. Online: https://doi.org/10.1016/j.procs.2024.06.206

Park, Jin H. – Ayati, Seyyed A. – Cai, Yichen (2025): Improving Acoustic Side- Channel Attacks on Keyboards Using Transformers and Large Language Models. *arXiv:2502.09782.* Online: https://doi.org/10.48550/arXiv.2502.09782

Phishing Trends Report (Updated for 2025) [s. a.]. *Hoxhunt,* s. a. Online: https://hoxhunt.com/guide/phishing-trends-report

Potter, Yujin et al. (2025): *Frontier AI's Impact on the Cybersecurity Landscape.* arXiv:2504.05408. Online: https://doi.org/10.48550/arXiv.2504.05408

Rohlf, Chris (2025): AI and the Software Vulnerability Lifecycle. *Center for Security and Emerging Technology,* 8 August 2025. Online: https://cset.georgetown.edu/article/ai-and-the-software-vulnerability-lifecycle/

Salem, Maher – Mrian, Mohammad (2025): *AI-Driven Penetration Testing: Automating Exploits with LLMs and Metasploit-A VSFTPD Case Study.* 2025 International Conference on New Trends in Computing Sciences (ICTCS), Amman, Jordan, 89–96. Online: https://doi.org/10.1109/ICTCS65341.2025.10989363

Schröer, Saskia L. – Pajola, Luca – Castagnaro, Alberto – Apruzzese, Giovanni – Conti, Mauro (2025): Exploiting AI for Attacks: On the Interplay between Adversarial AI and Offensive AI. *arXiv:2506.12519v2.* Online: https://arxiv.org/html/2506.12519

SentinelOne (2025): What is Polymorphic Malware? Examples & Challenges. *SentinelOne,* 20 August 2025. Online: www.sentinelone.com/cybersecurity-101/threat-intelligence/what-is-polymorphic-malware/

Singh, Bhagwant – Cheema, Sikander S. (2024): Emerging Trends in AI-Powered Malware Detection: A Review of Real-Time and Adversarially Resilient Techniques. *Tuijin Jishu/Journal of Propulsion Technology,* 45(4).

Syed, Shoeb A. (2025): Adversarial AI and Cybersecurity: Defending Against AI- Powered Cyber Threats. *Iconic Research and Engineering Journals,* 8(9), 1030–1041.

Usman, Yusuf – Upadhyay, Aadesh – Chataut, Robin – Gyawali, Prashnna K. (2024): Is Generative AI the Next Tactical Cyber Weapon for Threat Actors? Unforeseen Implications of AI Generated Cyber Attacks. *arXiv:2408.12806.* Online: https://doi.org/10.48550/arXiv.2408.12806

Verton, Dan (2025): The 2025 Cybersecurity Pulse Report. *iSMG,* 30 May 2025. Online: https://ismg.io/resource/rsac-2025-pulse/

Yamin, Muhammad M. – Ullah, Mohib – Ullah, Habib – Katt, Basel (2021): Weaponized AI for Cyber Attacks. *Journal of Information Security and Applications,* 57. Online: https://doi.org/10.1016/j.jisa.2020.102722

Yu, Jingru et al. (2024): The Shadow of Fraud: The Emerging Danger of AI-powered Social Engineering and its Possible Cure (Version 1). *arXiv:2407.15912.* Online: https://doi.org/10.48550/ARXIV.2407.15912

Zhu, Yuxuan et al. (2025): CVE-Bench: A Benchmark for AI Agents' Ability to Exploit Real-World Web Application Vulnerabilities. *arXiv:2503.17332v4.* Online: https://arxiv.org/html/2503.17332v4

HADMÉRNÖK
VÉDELEMINFORMATIKA

20. évfolyam (2025) 4. szám 69–85.
DOI: 10.32567/hm.2025.4.5

Pozderka Gábor[1]

A kibervédelmi és a kiberműveleti gyakorlatok rendszerének átalakulása, az aktuális kihívások vizsgálata

The Transformation of Cybersecurity and Cyber Operations Exercises and the Examination of Current Challenges

Absztrakt

A kibertér az elmúlt évtizedben a biztonságpolitika és a katonai műveletek egyik meghatározó dimenziójává vált. A kibervédelmi és kiberműveleti képességek fejlesztése ennek megfelelően stratégiai jelentőségű feladat mind nemzeti, mind nemzetközi szinten. A felkészülés egyik legfontosabb eszközét a kibervédelmi és kiberműveleti gyakorlatok jelentik, amelyek célja a technikai, szervezeti és vezetői képességek fejlesztése valósághű környezetben. A tanulmány bemutatja e gyakorlatok rendszerének átalakulását, elemzi a fejlődést kiváltó tényezőket, valamint vizsgálja azokat az aktuális kihívásokat – különösen a technológiai fejlődés és a nemzetközi együttműködés területén –, amelyek meghatározzák a gyakorlatok hatékonyságát. Az elemzés rámutat arra, hogy a jövőben a komplex, adaptív és multidiszciplináris megközelítés válik meghatározóvá a kibervédelmi felkészítésben.

Kulcsszavak: kibervédelem, kiberműveletek, kibergyakorlatok, NATO, átalakulás

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola, e-mail: pozderka.gabor@hm.gov.hu

Abstract

Cyberspace has become one of the most significant operational domains in modern security and military strategy over the past decade. Consequently, the development of cyber defence and cyber operations capabilities has gained strategic importance at both national and international levels. Cyber defence and cyber operations exercises play a crucial role in preparedness, as they aim to enhance technical, organisational and leadership capabilities in realistic scenarios. This paper examines the transformation of the cyber defence and cyber operations exercise system, analyses the driving factors behind this evolution, and explores current challenges such as rapid technological development and international cooperation. The study highlights that future cyber exercises will increasingly rely on complex, adaptive and multidisciplinary approaches to ensure effective cyber resilience.

Keywords: cyber defence, cyber operations, cyber exercises, NATO, transformation

Bevezetés

A digitalizáció az elmúlt évtizedekben alapvetően átalakította a modern társadalmak működését.[2] Az államigazgatás, a gazdaság, a közlekedés, az energiaszektor, valamint a fegyveres erők működése egyaránt nagymértékben függ az információs és kommunikációs technológiáktól.[3] Az információs rendszerek nem pusztán támogató szerepet töltenek be, hanem sok esetben a működés kritikus feltételét jelentik. Ennek következtében a digitális infrastruktúrák sérülékenysége közvetlen biztonsági kockázattá vált.

A kibertér különlegessége abban rejlik, hogy nem köthető egyetlen ország vagy földrajzi terület határaihoz sem. Emiatt a kibertérben zajló műveletek gyakran rejtve maradnak, az elkövetők kiléte nehezen állapítható meg, miközben a hatásuk szinte azonnal jelentkezik. Egy sikeres kibertámadás nemcsak technikai problémát okozhat, hanem komoly következményekkel járhat az állami működésre, a gazdaságra vagy akár a politikai stabilitásra is. Az ilyen tapasztalatok miatt a kibertér mára a nemzetközi biztonságpolitika egyik meghatározó területévé vált. A kibertér azért is vonzó állami és nem állami szereplők számára, mert viszonylag kevés erőforrással is jelentős hatást lehet elérni benne. Ez különösen azoknak kedvez, akik hagyományos katonai vagy gazdasági értelemben gyengébbek, mégis képesek nyomást gyakorolni fejlett államokra vagy nagy szervezetekre, ennek következtében az erőviszonyok kiegyenlítődhetnek, a konfliktusok jellege is megváltozik, hiszen nem mindig a hagyományos erőfölény lesz a döntő.

A katonai gondolkodásban hagyományosan a szárazföldi, légi, tengeri és később az űrbeli műveletek alkották a hadviselés alapvető doménjeit. A 21. század elejére

[2] A digitális technológiák elterjedése mélyreható változásokat hozott a társadalmak működésében, új módokat teremtett a kommunikációra, a munkavégzésre és az információkezelésre, amelyek alapvetően formálták át a mindennapi életet és az alkalmazott eljárásrendeket.

[3] Kovács 2023.

azonban egyértelművé vált, hogy a kibertér önálló műveleti térként értelmezendő.[4] E felismerést intézményes szinten is megerősítette számos nemzetközi szervezet, különösen a NATO, amely a kiberteret hivatalosan is hadműveleti doménként ismerte el.

A gyakorlatok és felkészülések kiemelt szerepet töltenek be a katonai kiképzések során, mert lehetővé teszik az elméleti ismeretek gyakorlati alkalmazását valósághű körülmények között. Segítenek az érintett állománynak begyakorolni az együttműködést, a fegyelmet és a gyors döntéshozatalt stresszhelyzetekben. A rendszeres felkészülés növeli az egyéni és a csapatszintű teljesítményt, valamint csökkenti a hibák és a félreértések esélyét, illetve a gyakorlatok során feltárhatók a felszerelés, az eljárások vagy a szervezés hiányosságai, amelyeket így időben lehet javítani.

Jelen tanulmány célja a kibervédelmi és kiberműveleti gyakorlatok rendszerének átfogó vizsgálata, különös tekintettel azok átalakulására és az aktuális kihívásokra, ebben a formában kapcsolódik a gyakorlatok hatékonyságértékelési területéhez. A tanulmány bemutatja a gyakorlatok fejlődési ívét, elemzi a technológiai és szervezeti változások hatását, nemzetközi példákon keresztül szemlélteti a különböző megközelítéseket, továbbá ajánlásokat fogalmaz meg a jövőbeni gyakorlatok tervezéséhez. A gyakorlatnak minden esetben összhangban kell lennie a képességfejlesztési célokkal, támogatnia kell azok teljes megvalósulását a DIME[5] minden spektrumában, így direkt módon kapcsolódik a stratégiai döntéshozatali folyamatokhoz és azok kutatási területeihez.

Az összehasonlító elemzés módszertanának alkalmazása a kutatás során biztosítja, hogy a rendelkezésre álló hazai és nemzetközi példákból adekvát következtetéseket lehessen levonni a célok megfogalmazásához, amelyek megfelelő támpontot jelentenek a jövőbeni szervezetek struktúrájának és feladatrendszerének kialakításához.

A kibervédelem és kiberműveletek felértékelődése

A kibertér biztonsági jelentőségének növekedésével párhuzamosan, kezdetben a kibervédelem majd a kiberműveletek szerepe is fokozatosan felértékelődött. A kibervédelem célja nem csupán az informatikai rendszerek védelme, hanem a társadalmi és gazdasági működés folyamatosságának biztosítása is. A kiberműveletek ezzel szemben lehetőséget teremtenek aktív beavatkozásra, elrettentésre és befolyásolásra.[6] Nemzetközi szinten egyre több állam hoz létre dedikált kiberparancsnokságot és fejleszt önálló kiberműveleti doktrínákat. Az Egyesült Államok például az USA Kiberparancsnokság (U.S. Cyber Command) megerősítésével integrálta a kiberműveleteket a hagyományos katonai tervezésbe. Hasonló folyamat figyelhető meg Európában, ahol a legtöbb állam – köztük Észtország, Franciaország, az Egyesült Királyság és Magyarország is – már önálló kibervédelmi és kiberműveleti struktúrákat alakított ki, és folyamatosan vizsgálják azok továbbfejlesztési lehetőségeit.

[4] Clarke–Knake 2019.

[5] A DIME-modell olyan keretrendszer, amely a külpolitikai és stratégiai eszközök négy fő dimenzióját foglalja össze (D – *diplomacy,* I – *information,* M – *military,* E – *economy*), és azt mutatja meg, hogy egy ország vagy szervezet a céljai eléréséhez nemcsak katonai erőt, hanem diplomáciai, információs és gazdasági eszközöket is alkalmazhat, és ezek kombinációja adja a teljes stratégiai hatást.

[6] Haig 2023.

A képességfejlesztés legfontosabb eszközeit a kibervédelmi és kiberműveleti gyakorlatok jelentik. Ezek a gyakorlatok lehetőséget biztosítanak arra, hogy a résztvevők valósághű környezetben teszteljék technikai, szervezeti és vezetési képességeiket, mivel a valós kibertérben ezt csak korlátozottan tehetik meg. A gyakorlatok során nemcsak a technológiai hiányosságok kerülnek felszínre, hanem a döntéshozatali folyamatok, az együttműködés és a kommunikáció gyenge pontjai is. A nemzetközi gyakorlatok különösen fontos szerepet töltenek be, mivel a kibertámadások jellemzően több országot érintenek egyszerre. Az olyan nagyszabású gyakorlatok, mint a NATO által szervezett Cyber Coalition[7] vagy az észt vezetésű, de NATO-képességcélokhoz kapcsolódó Locked Shields,[8] lehetőséget teremtenek az interoperabilitás fejlesztésére és a közös eljárások tesztelésére.

A kibervédelem és kiberműveletek elméleti és fogalmi keretei

A kibervédelem az informatikai rendszerek védelménél jóval komplexebb folyamat. Magában foglalja a technológiai, szervezeti, jogi és humán tényezőket, valamint a stratégiai tervezést. A technológiai komponensek – például tűzfalak, behatolásészlelő rendszerek, titkosítási eljárások – csak a teljes védelem egy részét képezik. A hatékony kibervédelem érdekében szükséges a szervezeti szabályozás, a kockázatkezelés, a tudatosság növelése, valamint a folyamatos oktatás és képzés. A humán tényező kiemelkedő szerepet kap, mivel a felhasználók hibái és a szándékos megtévesztések sokszor nagyobb veszélyt jelentenek, mint a technikai sérülékenységek. Ezért a modern kibervédelemben hangsúlyos a biztonságtudatosság fejlesztése, az incidenskezelési protokollok begyakorlása, valamint a szervezeti kultúra kialakítása, amely elősegíti a gyors és hatékony reagálást.

A kiberműveletek olyan célzott tevékenységek, amelyek a kibertérben fejtenek ki hatást. Ezek lehetnek:

- *védekező műveletek,* amelyek a hálózatok és rendszerek sérülékenységeinek feltárását, a támadások megakadályozását és az incidensek elhárítását célozzák;
- *támadó műveletek,* amelyek a kibertérben a potenciális ellenfél infrastruktúrájára gyakorolnak hatást;[9]
- *befolyásoló műveletek,*[10] amelyek célja a közvélemény, a politikai döntéshozók vagy a szervezeti működés manipulálása.[11]

Fontos megérteni azt, hogy a hagyományos CIS *(communication and information systems)* feladatok főként a katonai kommunikáció és információs rendszerek működtetésére, karbantartására és biztosítására összpontosítanak. Ide tartozik például

[7] A Cyber Coalition a NATO egyik legfontosabb, évente megrendezett kibervédelmi gyakorlata, amelyen a szövetséges és partnerországok vesznek részt. Célja a kibertámadások elleni védekezés, az együttműködés és a döntéshozatali folyamatok gyakorlása valósághű, szimulált környezetben.

[8] A Locked Shields a NATO CCDCOE által szervezett, a világ egyik legnagyobb és legösszetettebb kibervédelmi gyakorlata, ahol a résztvevők valósághű kibertámadások ellen védenek komplex informatikai rendszereket.

[9] Kovács 2021.

[10] AJP 3.20 2020.

[11] Rid 2020.

a rádió- és adatátviteli hálózatok kiépítése, az informatikai rendszerek fenntartása és a megbízható kommunikáció garantálása. Ezzel szemben a kiberszakterület feladatai már nemcsak a rendszerek működtetésére, hanem azok védelmére és az esetleges kibertámadások elleni reagálásra is irányulnak. A kibertevékenységek célja lehet a támadás, a védelem, valamint a sebezhetőségek feltárása és kihasználása. Míg a hagyományos CIS-feladatok statikusabb, inkább működtetési jellegű feladatokat jelentenek, a kiber feladatai dinamikusak és gyorsan változó fenyegetésekkel szembesítenek. A két terület ugyanakkor szoros kapcsolatban áll: a CIS-rendszerek alapozzák meg a kibertevékenységek működését, és azok biztonsága közvetlenül befolyásolja a kiberműveletek sikerét. Összességében a CIS biztosítja a stabil technikai hátteret, míg a kiberszakterület a rendszerek védelmét és az aktív kiberműveletek végrehajtását célozza.

A kiberműveletek során a célok elérése gyakran aszimmetrikus módon történik: kisebb erőforrással rendelkező szereplő is képes jelentős hatást gyakorolni egy fejlettebb rendszerre. Ezért a kiberműveletek alkalmazásának nemcsak technikai, hanem politikai és stratégiai dimenziója is van a korábban hivatkozott DIME minden spektrumában.

Kibervédelmi gyakorlatok: nemzetközi példák

A NATO 2016-os varsói csúcstalálkozóján hivatalosan is elismerte a kibertér mint önálló műveleti domén szerepét.[12] A szövetség tagállamai kötelezettséget vállaltak a kibervédelmi képességek fejlesztésére, valamint az információmegosztás és együttműködés erősítésére.[13] A NATO több nagy léptékű gyakorlatot szervez, például a korábban említett Cyber Coalitiont, amelyben több mint 30 ország vesz részt a védelmi és támadó képességek integrált tesztelésének érdekében. Ezzel összhangban született a NATO felügyelete alatt a Cyber Defence Pledge, amelyben a szövetséges országok elkötelezik magukat a kibervédelmi képességeik fejlesztése és megerősítése mellett. A cél, hogy minden tagállam megfelelő erőforrásokkal és szakértelemmel rendelkezzen a kibertámadások elleni védekezéshez. A kezdeményezés jelentősége abban rejlik, hogy növeli a kollektív védelem hatékonyságát és csökkenti a kibertérből fakadó sebezhetőségeket, emellett elősegíti az együttműködést, a tapasztalatok megosztását és a közös gyakorlatokat a szövetségesek között. Összességében a Cyber Defence Pledge hozzájárul a NATO tagállamai biztonságának és a globális kibertér stabilitásának erősítéséhez.

Az Egyesült Államok 2009-ben hozta létre a U.S. Cyber Commandot, amelynek feladata a nemzeti kiberbiztonsági műveletek koordinálása. A parancsnokság rendszeresen szervez gyakorlatokat, például Cyber Flag néven, ahol a katonai és kormányzati szervezetek komplex kibertámadásokra reagálnak. Ezek a gyakorlatok elősegítik az interoperabilitást a különböző katonai ágak és civil szervezetek között, valamint lehetőséget adnak a döntéshozatali folyamatok tesztelésére.[14]

[12] NATO 2016.
[13] NATO Cyber Defence Pledge.
[14] Libicki 2016.

Észtország 2007-es, ismert kibertámadás-sorozatát követően a szponzor- és partnernemzetek (köztük Magyarország) létrehozták a Locked Shields gyakorlatot, amely a világ egyik legnagyobb valós idejű kibervédelmi gyakorlatává nőtte ki magát. A gyakorlat során a különböző nemzetekből kiválasztott résztvevők valós időben reagálnak szimulált kibertámadásokra, beleértve kritikus infrastruktúrákat, kormányzati hálózatokat és kommunikációs rendszereket. A Locked Shields a stratégiai, taktikai és technikai képességek együttes tesztelését célozza, miközben hangsúlyos a nemzetközi együttműködés.

Izraelben a kibervédelmi gyakorlatok integrált részei a nemzeti biztonsági stratégiának. Az izraeli gyakorlatok során a katonai és polgári szervezetek közösen vesznek részt szimulált támadásokban, amelyek célja a kritikus infrastruktúrák védelme és a gyors reagálás képességének fejlesztése. A gyakorlatok különösen hangsúlyozzák az AI és a prediktív analitika alkalmazását a támadások előrejelzésére.[15]

Japán és Dél-Korea is rendszeresen szervez nagy léptékű kibervédelmi gyakorlatokat, amelyek során a résztvevők valós idejű támadásokra reagálnak. A gyakorlatok során külön figyelmet kap a kritikus infrastruktúrák, például az energia- és közlekedési rendszerek védelme, valamint a kormányzati és katonai kommunikáció folyamatos biztosítása.

Magyarország mind nemzeti, mind kormányzati, mind ágazati szinten több rendszeresen ismétlődő gyakorlat megszervezését is végrehajtotta az elmúlt években, a tapasztalatfeldolgozás eredményeként beépültek a korábbi évek tapasztalatai. A Magyar Honvédség Digitális Csapás nevű többnemzeti kibergyakorlata az állomány technikai felkészültsége mellett a döntéshozatali folyamatok hatékonyságát is rendszeresen teszteli.

A gyakorlatok jellege szerint alapvetően a következő típusokat különböztethetjük meg:

- *Table-top gyakorlatok (TTX).* Szerepjáték-alapú, döntéshozatali folyamatokat vizsgáló gyakorlatok, ahol a résztvevők elméleti forgatókönyvekre reagálnak.[16] Az ilyen jellegű gyakorlatok közelebb hozzák a különböző területeken dolgozó szakembereket, és a kiberbiztonság technikai vetületei mellett annak gazdasági, diplomáciai, politikai, nemzetbiztonsági, vagy akár katonai hatásaira is felhívják a figyelmet. Fontos a valós kibertérben korábban bekövetkezett események ismételt szimulálása, azok továbbgondolása eseményláncok formájában.
- *Red team/blue team gyakorlatok.* A támadó (red) és védő (blue) szerepek elkülönítésével valósághű támadási és védekezési képességeket tesztelnek.
- *Live-fire gyakorlatok.* Valós rendszereken, kontrollált környezetben zajló gyakorlatok, amelyek során a támadások és védekezési mechanizmusok teljes spektruma tesztelhető.
- *Többnemzeti gyakorlatok.* Interoperabilitás és koordináció fejlesztésére irányuló gyakorlatok, ahol különböző országok szervezetei dolgoznak együtt.

[15] Kertész 2023.
[16] Szabó 2018.

A gyakorlatok célja több szinten értelmezhető:

- *technikai szint:* sérülékenységek feltárása, rendszerek megerősítése, incidenskezelési képességek fejlesztése;
- *szervezeti szint:* felelősségi körök tisztázása, kommunikációs folyamatok és koordináció tesztelése;
- *stratégiai szint:* döntéshozatali folyamatok, elrettentési stratégiák és nemzetközi együttműködés erősítése.

Nemzetközi tapasztalatok alapján a rendszeresen végrehajtott gyakorlatok jelentősen növelik a szervezetek felkészültségét, javítják az információmegosztást, és elősegítik a gyors reagálást komplex kibertámadások esetén. Megállapítható, hogy a modern gyakorlatok multidiszciplináris jellegűek, integrálják a technikai, szervezeti és stratégiai szempontokat, valamint hangsúlyozzák a nemzetközi együttműködés jelentőségét. A különböző országok példái azt mutatják, hogy a kibervédelmi gyakorlatok hatékony eszközei a felkészültség növelésének és a kibertérben történő koordinált reagálásnak.[17] A szervezetek saját belső gyakorlatok szervezésével képesek feltárni saját gyengeségeiket, a tapasztalatok alapján javító intézkedéseket bevezetni.

A kibervédelmi gyakorlatok történeti fejlődése és korai szakasza

A kibervédelmi gyakorlatok első generációját elsősorban a technikai problémák megoldására irányuló képzések jellemezték. Az 1990-es évek végén és a 2000-es évek elején a gyakorlatok alapvetően az informatikai szakemberek képzésére koncentráltak, különösen a hálózati biztonság, a tűzfalak konfigurálása, a behatolásészlelés és a sérülékenységek feltárása területén. A gyakorlatok jellemzően izolált környezetben zajlottak, ahol a résztvevők egy előre meghatározott támadási forgatókönyv szerint dolgoztak. Az ilyen gyakorlatok célja elsősorban a technikai hibák és a rendszer-sérülékenységek felismerése volt, ebben a korszakban a szervezeti és vezetési aspektusok kevésbé kaptak hangsúlyt.

Az Egyesült Államokban az 1990-es évek végén és a 2000-es évek elején több kisebb technikai fókuszú gyakorlat zajlott, amelyek célja a katonai hálózatok és a kritikus infrastruktúrák védelmének tesztelése volt. A NATO 2002–2005 között már szervezett kisebb gyakorlatokat, amelyek célja a tagállamok hálózati védelmi képességeinek felmérése és összehangolása volt. Ezek a gyakorlatok fontos alapot teremtettek a későbbi komplexebb rendszerek kialakításához, azonban már a korai tapasztalatok is rámutattak a technikai fókusz korlátaira: az incidensek kezelése gyakran nem volt elég gyors és koordinált, és a szervezeti kommunikáció hiányosságai súlyos problémákat okoztak. Ezen gyakorlatok még jellemzően szeparáltan zajlottak, egy-egy feladat megoldására fókuszáltak, nem vontak be a tervezésbe és feladat-végrehajtásba más műveleti területeket.

[17] Vykopal et al. 2017.

A 2000-es évek közepére egyre világosabbá vált, hogy a kizárólag technikai fókuszú gyakorlatok nem képesek lefedni a kibertér összetett kihívásait.[18] E felismerés nyomán a gyakorlatok komplexebbé váltak, integrálva a szervezeti, vezetői és döntéshozatali dimenziókat. Az újabb gyakorlatok egyik legfontosabb eleme a red team – blue team koncepció bevezetése volt. A red team a támadói szerepet, a blue team a védelmi szerepet testesítette meg. A red team – blue team modellek korai alkalmazása az Egyesült Államokban és az Egyesült Királyságban kezdődött, majd gyorsan átvették más NATO-tagállamok és a szövetség partnerei, ahol a gyakorlatban különböző országok blue teamjei közösen védték a szimulált rendszereket, miközben a red team a támadási technikák széles spektrumát alkalmazta. Kezdetben a nemzetek a red team képességek kialakítását megpróbálták elrejteni többek között a nem egyértelmű, hiányos jogi szabályzói környezet miatt, azonban nyilvánvalóvá vált, hogy ez a narratíva hosszabb távon nem fenntartható, ellehetetleníti a közös feladat-végrehajtást.

A fenti szétválasztás többek között lehetővé tette:

- a támadási módszerek valósághű megértését;
- a védekezési stratégia folyamatos fejlesztését;
- a szervezeti reakciók és döntéshozatali folyamatok tesztelését.

A kibervédelmi gyakorlatok történeti fejlődésében meghatározó jelentőségű volt a kritikus infrastruktúrák bevonása. A 2000-es évek közepén és végén számos országban a gyakorlatok már nemcsak katonai rendszerekre, hanem az energia-, víz-, közlekedési és kommunikációs infrastruktúrákra is kiterjedtek. A korai gyakorlatok egyik fontos hozadéka az volt, hogy lehetőséget adtak az oktatás és tudatosság növelésére. Az oktatási célok mellett a gyakorlatok hozzájárultak a nemzetközi szabványok és protokollok kialakításához, például a NATO és az ENSZ ajánlásainak implementálásához. A gyakorlatok keretében a résztvevők megtanulták felismerni a támadási mintákat, kezelni az incidenseket, koordinálni a szervezeti egységeket és hatékonyan kommunikálni mind belső, mind külső partnerek felé.

A gyakorlatok fejlődésében kulcsszerepet játszott a technológiai fejlődés, amelynek keretében a virtualizáció és szimuláció lehetővé tette a nagy léptékű, valósághű gyakorlatok lebonyolítását anélkül, hogy a tényleges rendszerek veszélybe kerültek volna. Az automatizált támadási szimulációk részeként a mesterséges intelligencia alkalmazása a red team szimulációkban növelte a gyakorlatok komplexitását, valamint a gyakorlatok során keletkező adatok adatgyűjtése és elemzése lehetővé tette a hibák feltárását és a szervezeti tanulás támogatását.

Izrael már a 2000-es évek végén megkezdte a mesterséges intelligencia (AI) integrációját a kibervédelmi gyakorlatokba, különösen a kritikus infrastruktúrák védelmében; ez már előrevetítette egy új korszak érkezését. Az AI-alapú támadásdetektálás és prediktív analitika lehetővé tette a gyors reagálást és a stratégiai döntéshozatal támogatását. A gyakorlatok esetében megfigyelhető, hogy a megkezdett modellek sikere esetén azok igen gyorsan beépülnek a hasonló tematikájú gyakorlatokba. Ennek egyik alapvető oka, hogy a végrehajtó állomány számos esetben átfedéseket mutat,

[18] Bányász–Orbók 2013.

hiszen mind nemzeti, mind nemzetközi téren az anyagi és személyi erőforrások korlátozottan állnak rendelkezésre.

A katonai és állami kibergyakorlatok modern szakasza

A 2010-es évektől a kibergyakorlatok jelentős átalakuláson mentek keresztül.[19] A korai, elsősorban technikai és oktatási célú gyakorlatokat felváltották a komplex, többdimenziós, valós idejű eseményekre reflektáló programok. Az új generációs gyakorlatok célja nem csupán a technikai és szervezeti képességek fejlesztése, hanem a stratégiai döntéshozatal, nemzetközi koordináció és válságkezelés képességének erősítése is. A modern gyakorlatok jellemzője a valós idejű, szimulált támadások komplex integrációja, beleértve a kritikus infrastruktúrákat, a kommunikációs rendszereket, a gazdasági hálózatokat, valamint a kormányzati és katonai irányítási láncokat. A gyakorlatok során a résztvevők különböző szinteken – technikai, operatív és stratégiai – reagálnak az incidensekre, miközben együttműködést gyakorolnak a nemzetközi partnerekkel.

A NATO a 2010-es évekre a kibervédelmi gyakorlatokat már stratégiai eszközként kezelte. A Cyber Coalition gyakorlatok célja a tagállamok közötti interoperabilitás erősítése, a védelmi képességek tesztelése, valamint a döntéshozatali folyamatok gyakorlása volt. A gyakorlatokon a résztvevők valós idejű támadásokra reagáltak, a red team által alkalmazott különböző támadási taktikákra és stratégiákra válaszolva. A Cyber Coalition 2016 már több mint 30 ország részvételével zajlott, fókuszában a kritikus infrastruktúrák védelme és a válságkezelési protokollok tesztelése szerepelt, a Cyber Coalition 2019 gyakorlaton újdonságként a mesterséges intelligencia és automatizált támadási szimulációkat vezették be, a gyakorlat során a résztvevők valós időben reagáltak a komplex kibertámadásokra. A NATO-gyakorlatok jelentősége abban áll, hogy a résztvevők nemcsak technikai készségeiket, hanem stratégiai és koordinációs képességeiket is fejlesztik, ami kulcsfontosságú a többszintű válságkezelésben.

Az Egyesült Államok modern kibergyakorlatainak továbbra is központi eleme a U.S. Cyber Command által szervezett Cyber Flag sorozat. A gyakorlatok célja folyamatos átalakuláson ment keresztül; a katonai és civil kiberműveletek integrációja, a támadó és védelmi képességek tesztelése, valamint a döntéshozatali folyamatok felgyorsítása fontos célok. A gyakorlatok egyik kiemelkedő aspektusa a többszintű koordináció: a helyi katonai parancsnokságok, szövetségi ügynökségek és külső partnerek együttműködésének tesztelése.

Észtország a modern kibervédelmi gyakorlatok esetében is az élvonalban áll, többek között a Locked Shields gyakorlat tapasztalatai révén. A résztvevők valós idejű támadásokra reagálnak, amelyek célja a kritikus infrastruktúrák, a kormányzati hálózatok és a kommunikációs rendszerek védelme. A Locked Shields gyakorlat különlegessége a széles körű nemzetközi részvétel, a gyakorlat során a résztvevőknek interoperábilis módon kell együttműködniük. A gyakorlat során hangsúlyos a red team

[19] Şeker 2019.

által alkalmazott aszimmetrikus támadások kezelése, valamint a gyors döntéshozatal és válságkezelés képessége.[20]

Izrael hosszú ideje kiemelt figyelmet fordít a kibervédelmi képességek fejlesztésére, különösen a kritikus infrastruktúrák védelmére és a stratégiai döntéshozatal támogatására. Az izraeli gyakorlatok során integrálják a katonai és polgári szervezeteket, a red team támadások és blue team védekezések valós idejű koordinációját, valamint a mesterséges intelligencia és prediktív analitika alkalmazását.

Összhangban a korábban megfogalmazottakkal, a 2010-es évektől kezdve több fontos trend figyelhető meg:

- *valós idejű szimulációk:* a gyakorlatok komplexitása nőtt, a résztvevők valós időben reagálnak a támadásokra;
- *AI és prediktív analitika:* a mesterséges intelligencia alkalmazása a támadásdetektálásban és a válságkezelés támogatásában;
- *kritikus infrastruktúrák integrálása:* az energia-, víz-, közlekedési és kommunikációs rendszerek védelme prioritás;
- *többnemzeti együttműködés erősítése:* a gyakorlatok során a résztvevők interoperábilis módon dolgoznak együtt, növelve a nemzetközi felkészültséget;
- *aszimmetrikus támadások kezelése:* a red team komplex és kreatív támadásokat alkalmaz, amelyek aszimmetrikus kihívásokat jelentenek a blue team számára.

A modern katonai és állami kibergyakorlatok komplex, multidimenzionális rendszerek, amelyek integrálják a technikai, szervezeti és stratégiai aspektusokat. A modern gyakorlatok elősegítik a kibervédelmi képességek folyamatos fejlesztését, támogatják a kritikus infrastruktúrák védelmét, és lehetőséget biztosítanak az új technológiák, például az AI integrációjára a kiberműveletekben.

Magyarország mint a NATO tagja aktívan részt vesz a korábban felsorolt nemzetközi kibergyakorlatokban, így biztosítva a szövetséges rendszerből adódó képességfejlesztési célok megvalósulásának tesztelését, finomhangolását.[21]

A kibervédelmi és kiberműveleti gyakorlatok aktuális kihívásai

A 21. század második évtizedében a kibervédelmi és kiberműveleti gyakorlatok nem csupán technikai képzések, hanem komplex stratégiai eszközök is. Az esettanulmányok elemzése lehetővé teszi, hogy a gyakorlatok különböző típusait, célkitűzéseit és eredményeit konkrét példákon keresztül vizsgáljuk. A hivatkozott nemzeti és nemzetközi gyakorlatok jelentősek katonai, állami és kritikus infrastruktúrákat érintő felkészültség szempontjából. A korábban felsorolt példák alapján egyértelműen megállapítható, hogy a modern kibergyakorlatok multidimenzionálisak, és nemzetközileg koordináltan kell megvalósulniuk.

A kibervédelmi gyakorlatok folyamatos fejlődésének egyik legfontosabb aspektusa a folyamatosan változó fenyegetési környezethez való alkalmazkodás. Az új

[20] NATO CCDCOE 2022.
[21] Szöllősi 2024.

típusú kibertámadások, a technológiai innovációk, a globális geopolitikai folyamatok és a kritikus infrastruktúrák komplexitása új kihívásokat jelent a gyakorlatok tervezése és lebonyolítása szempontjából. A modern gyakorlatok tervezése során meg kell hogy jelenjenek a kiberbűnözők és az államilag támogatott csoportok által használt eljárásokra adott válaszok, a résztvevőknek képesnek kell lenniük mindkét típusú támadás kezelésére, figyelembe véve a különböző támadási módszerek komplexitását.

A tapasztalatok elemzése alapján az alábbi szempontok figyelembevétele elengedhetetlen a képességfejlesztés során.

A nemzetközi együttműködés fontossága

A kibertér határokon átnyúló jellege miatt a kibertámadások ritkán érintenek csak egyetlen államot, ezért önálló nemzeti válaszok gyakran nem elegendők. A támadások forrásának azonosítása és a hatások kezelése sokszor több ország információinak és képességeinek összehangolását igényli. A nemzetközi együttműködés a kibergyakorlatok során lehetővé teszi a közös eljárások, kommunikációs csatornák és döntéshozatali mechanizmusok tesztelését. Ennek hiányában válsághelyzetben lassú vagy ellentmondásos reakciók alakulhatnak ki. A közös gyakorlatok során a résztvevők megismerik egymás képességeit és korlátait, ami növeli a bizalmat és a hatékony együttműködés esélyét valós helyzetekben. Az eltérő tapasztalatok és megközelítések megosztása hozzájárul a jobb védekezési módszerek kialakításához is. Mindez összességében erősíti a kollektív kibervédelmet, és csökkenti a kibereseményekeszkalálódásának kockázatát.

A technológiai innovációk integrálása

A kibertérben megjelenő fenyegetések folyamatosan fejlődnek, ezért a védekezési módszereknek is lépést kell tartaniuk ezekkel a változásokkal. Ha a kibergyakorlatok nem építik be az új technológiai innovációkat, akkor nem tükrözik a valós környezetet, és hamis biztonságérzetet kelthetnek. Az új eszközök és megoldások integrálása lehetővé teszi a modern támadási technikák és sérülékenységek valósághű szimulációját. Ennek következtében a résztvevők megtanulják kezelni azokat a kihívásokat, amelyekkel tényleges műveleti helyzetben is szembesülhetnek. A technológiai innovációk alkalmazása segít feltárni a meglévő rendszerek gyenge pontjait, még azelőtt, hogy azokat egy valódi támadás kihasználná. Emellett elősegíti az új védelmi megoldások kipróbálását és finomítását ellenőrzött környezetben. Mindez hozzájárul ahhoz, hogy a szervezetek rugalmasabbá és ellenállóbbá váljanak, és hatékonyabban tudjanak reagálni a gyorsan változó kibertér kihívásaira.

A kritikus infrastruktúrák védelme prioritás[22]

A kritikus infrastruktúrák – például az energiaellátás, a közlekedés, a vízellátás vagy a kommunikációs rendszerek – működése alapvetően meghatározza a társadalom mindennapi életét. Ha ezek a rendszerek kibertámadás következtében megbénulnak, annak azonnali és súlyos következményei lehetnek a lakosság biztonságára és a gazdaság működésére nézve. Éppen ezért a kibergyakorlatok során kiemelt figyelmet kell fordítani ezen rendszerek védelmére, illetve arra, hogy a valós kockázatokat tükröző helyzeteket lehessen modellezni. A gyakorlatok lehetőséget adnak arra, hogy feltárják a kritikus infrastruktúrák sebezhetőségeit és a különböző ágazatok közötti függőségeket; ennek hiányában egy valódi támadás során a reakciók lassúak vagy összehangolatlanok lehetnek, ami tovább növeli a károk mértékét. Mindez hozzájárul a rendszerek ellenálló képességének növeléséhez, és csökkenti annak esélyét, hogy egy kibertámadás társadalmi vagy nemzetbiztonsági válsággá alakuljon.

A red team – blue team módszertan hatékonysága

A red team – blue team módszertan alkalmazása azért elengedhetetlen a kibergyakorlatok során, mert valósághű módon modellezi a támadó és a védekező oldal közötti dinamikát. A red team támadóként folyamatosan új technikákat és megközelítéseket alkalmaz, ami arra kényszeríti a blue teamet, hogy éles helyzetekhez hasonló környezetben reagáljon. Ennek hatására a védekező oldal nemcsak az eszközeit, hanem döntéshozatali folyamatait és együttműködését is fejleszti. A módszertan lehetővé teszi a védelmi rendszerek gyenge pontjainak feltárását még azelőtt, hogy azokat egy valódi támadás kihasználná. A folyamatos támadás-védekezés ciklus miatt a résztvevők azonnali visszajelzést kapnak a stratégiáik hatékonyságáról. Összességében a red team – blue team megközelítés növeli a kibergyakorlatok realizmusát, és hozzájárul a szervezetek hosszú távú kibervédelmi felkészültségének erősítéséhez.

A stratégiai és döntéshozatali képességek fejlesztése

A stratégiai és döntéshozatali képességek fejlesztése fontos feladat a kibergyakorlatok során, mert a kibertámadások gyakran komplex és gyorsan változó helyzeteket teremtenek. Ha a döntéshozók nem tudnak gyorsan és helyesen reagálni, a támadás hatásai elhatalmasodhatnak, és súlyos következményekkel járhatnak a kritikus rendszerekre és a társadalomra is. A gyakorlatok lehetőséget adnak arra, hogy a résztvevők valósághű szimulációkban gyakorolják a döntéshozatalt, a prioritások meghatározását és a kockázatok értékelését, ez elősegíti, hogy a valós helyzetekben a vezetők nyugodtabban és átgondoltabban reagáljanak majd. A stratégiai gondolkodás fejlesztése javítja az erőforrások optimális elosztását és az együttműködést a különböző szervezeti egységek között. Mindez csökkenti a hibák kockázatát, növeli a válsághelyzetek

[22] ENISA 2024.

kezelhetőségét, és erősíti a szervezet ellenálló képességét a kibertámadásokkal szemben. Összességében a stratégiai képességek gyakorlása nélkül a technikai készségek önmagukban nem elegendők a hatékony védekezéshez. A gyakorlatok nemcsak technikai, hanem szervezeti és stratégiai szinten is fejlesztik a résztvevőket.

A technikai képességek mellett a szervezeti és stratégiai dimenziók szerepe egyre fontosabb:

- *gyors döntéshozatal:* a valós idejű támadások gyors reagálást igényelnek;
- *koordináció több szervezet között:* a katonai, kormányzati és privát szektorbeli szereplők közötti együttműködés kritikus;
- *kommunikációs kihívások:* a támadások során a belső és külső kommunikáció hatékony kezelése alapvető, a stratégiai kommunikáció szerepe felértékelődik;
- *jogi kihívások:* a jól felkészített technikai állomány mellett a kibertérben végrehajtott műveletek során rendkívül fontosak a jogi és szabályzó környezetet jól ismerő szakemberek. A kibertéri műveletek jogi kereteinek tisztázása kulcsfontosságú;
- *adatvédelmi és adatmegosztási szabályok:* különböző országok eltérő szabályozása nehezíti az interoperabilitást.

A gyakorlatok során várható jövőbeli trendek

A kritikus infrastruktúrák digitalizációja és az IoT-[23] (Internet of Things) alapú rendszerek elterjedése jelentősen növelte a kitettséget és sebezhetőséget. A gyakorlatok abban az esetben lehetnek hatékonyak és sikeresek, amennyiben ezen kihívásokra képesek választ adni, képesek szimulálni a valós környezetet. Ennek megfelelően, a jelenleg végrehajtott gyakorlatok során a résztvevőknek képesnek kell lenniük a hálózatok integrált védelmére, a valós idejű támadásfigyelésre, a rendszerek gyors helyreállítására és a koordinált válságkezelésre.

A jelenlegi tapasztalatok alapján a kibervédelmi gyakorlatok jövőbeni tervezése során az alábbi fontos irányok azonosíthatók és várhatók:

- *integrált szimulációk:* a fizikai és digitális rendszerek együttes védelme;
- *AI és automatizálás fokozása:* az emberi döntéshozatal kiegészítése prediktív analitikával;
- *nemzetközi standardizáció:* protokollok és gyakorlatok összehangolása a globális interoperabilitás érdekében;
- *aszimmetrikus és hibrid fenyegetések kezelése:* állami és nem állami szereplők komplex támadásai;[24]
- *tudatosság és képzés kiterjesztése:* nemcsak a szakemberek, hanem döntéshozók és szervezeti vezetők bevonása.

[23] A dolgok internete (IoT) lényegében olyan különböző, egyértelműen azonosítható elektronikai eszközöket jelent, amelyek képesek felismerni valamilyen lényegi információt, és azt egy internetalapú hálózaton egy másik eszközzel kommunikálni.

[24] Resperger 2018.

A kibervédelmi és kiberműveleti gyakorlatok tehát dinamikusan alkalmazkodnak a változó fenyegetésekhez, és a nemzetközi együttműködés, valamint a technológiai innováció kulcsfontosságú szerepet játszik a hatékonyság növelésében. A fenyegetési környezet komplexitása és a kritikus infrastruktúrák növekvő sebezhetősége új képességeket igényel a résztvevőktől, a szervezeti, döntéshozatali és nemzetközi koordináció kulcsfontosságú a gyakorlatok sikeréhez. A technológiai innovációk új kihívásokat, de egyben lehetőségeket is kínálnak, a nemzetközi együttműködés és jogi harmonizáció elengedhetetlen a globális kibervédelmi képességek fejlesztéséhez.[25] Ezek a gyakorlatok már nem csupán tréningek, hanem komplex, stratégiai szintű eszközök a nemzetközi biztonsági képességek fejlesztésében. A gyakorlatok hatékonyságának értékelése alapvető annak érdekében, hogy a résztvevők ne csak a szimulációkban, hanem a valós rendszerekben is képesek legyenek megfelelően reagálni. A hatékonyság vizsgálata magában foglalja a technikai, operatív és stratégiai szinteket, a szervezeti tanulságokat, valamint az interoperabilitás és döntéshozatal fejlesztését.

A gyakorlatok hatékonyságának értékelésére több módszer létezik (kvantitatív, kvalitatív, kombinált), amelyeket kombináltan célszerű alkalmazni. Példaként említhető, hogy a NATO Cyber Coalition gyakorlatokban a red team támadások sikeressége mérhető, azonban a blue team és a részt vevő országok koordinációs képessége kvalitatív módon értékelhető. A Locked Shields gyakorlaton minden csapat pontozása a támadások elleni védekezés, a válaszidők és a kritikus rendszerek védelmének sikeressége alapján történik, a gyakorlat után a részt vevő országok konkrét biztonsági protokollokat és eljárásokat módosítanak saját nemzeti rendszereikben.[26]

Általános következtetések és jövőbeli ajánlások

A kibervédelmi gyakorlatok nem csupán technikai tréningek, hanem komplex stratégiai eszközök, amelyek javítják a döntéshozatali és válságkezelési képességeket, fejlesztik a nemzetközi interoperabilitást, tesztelik a kritikus infrastruktúrák és kommunikációs hálózatok védelmi képességeit.

A gyakorlatokban egyre nagyobb szerepet kapnak az alábbi technológiák:

- *mesterséges intelligencia (AI):* támadásdetektálás, prediktív analitika, automatizált reagálás;
- *IoT és 5G-rendszerek:* kritikus infrastruktúrák és kommunikációs hálózatok integrált védelme;
- *felhőalapú rendszerek:* decentralizált támadások kezelése, redundancia és reziliencia biztosítása.

Az alábbi szempontok azonosíthatók mint kritikus kihívások és korlátok:

- *fenntarthatóság:* a gyakorlatok költség- és erőforrásigénye magas, különösen a fejlett technológiák alkalmazása esetén;

[25] Menczelesz 2025.
[26] Ertan et al. 2020.

- *szervezeti ellenállás:* az új protokollok és eljárások implementálása gyakran kulturális és szervezeti akadályokba ütközik;
- *jogszabályi korlátok:* a nemzetközi együttműködés során az adatvédelmi és jogi szabályozások eltérései nehezítik az interoperabilitást;
- *technológiai kompatibilitás:* a gyakorlatokon tesztelt innovációk nem mindig kompatibilisek a meglévő rendszerekkel.

A jövőben a gyakorlatok egyre inkább ötvözni fogják a fizikai és digitális rendszereket, a katonai, kormányzati és civil szektort,[27] valamint a valós és szimulált fenyegetéseket, a mesterségesintelligencia-alapú támadásdetektálás,[28] prediktív analitika és automatizált válaszmechanizmusok kulcsfontosságúak a komplex kibertámadások kezelésében. A kibervédelmi és kiberműveleti gyakorlatok stratégiai, technológiai és szervezeti szinten egyaránt kritikus szerepet töltenek be a nemzetközi biztonság és a kritikus infrastruktúrák védelmében. A gyakorlatok értékelése és a tapasztalatok átültetése a valós rendszerekbe javítja a döntéshozatalt, a koordinációt és a technológiai reagálóképességet. A jövőbeli trendek az integrált szimulációk, az AI-alapú automatizált védelem, az IoT-integráció és a nemzetközi standardizáció felé mutatnak. Az ajánlások megvalósítása elősegíti a kibervédelmi képességek folyamatos fejlesztését, a nemzetközi együttműködés megerősítését és a kritikus infrastruktúrák biztonságának növelését.[29] A tanulmányban feldolgozott példák alapján megfogalmazott ajánlások a gyakorlatok fejlesztésére, amelyeknek összhangban kell lenniük a szervezet képességfejlesztési céljaival:

- *Integrált értékelési keretrendszer kialakítása.* Kombinálni kell a kvantitatív és kvalitatív módszereket, figyelembe véve a technikai, szervezeti és stratégiai dimenziókat.
- *Technológiai innovációk folyamatos integrálása.* AI, automatizált támadásdetektálás, felhő- és IoT-rendszerek folyamatos tesztelése és fejlesztése.
- *Nemzetközi együttműködés erősítése.* Közös protokollok, adatmegosztási standardok és interoperabilitás kialakítása.
- *Képzés és tudatosság növelése.* A gyakorlatokba bevonni vezetőket, döntéshozókat és nem csak technikai személyzetet.
- *Kritikus infrastruktúrák védelmének prioritása.* A fizikai és digitális rendszerek integrált védelmének gyakorlása valós idejű támadásszimulációkkal.
- *Jogi és szabályozási harmonizáció.* Az adatvédelmi és jogi keretek egységesítése a nemzetközi gyakorlatok során, valamint közös válságkezelési forgatókönyvek kidolgozása.[30]

A jövőben a gyakorlatok célja egyre inkább az emberi döntéshozatal kiegészítése és a reakcióidő csökkentése, a valós infrastruktúrák valós idejű tesztelése, valamint a gyors helyreállítási és redundanciastratégiák fejlesztése lesz. A gyakorlatok során megszerzett tapasztalatok alapján szükséges a nemzetközi protokollok, szabványok

[27] Kiss 2019.
[28] Zacharis–Katos–patsakis 2024.
[29] NATO 2025.
[30] Schmitt 2017.

és adatmegosztási eljárások harmonizálása, az interoperabilitás javítása révén a többnemzeti válaszok hatékonyabbá válhatnak. Szükséges továbbá, hogy a gyakorlatok eredményei beépüljenek a kibervédelmi és kiberműveleti stratégiákba, válságkezelési és koordinációs eljárásokba figyelembe véve a fenyegetési trendeket.[31]

A Magyar Honvédség a kiberműveleti gyakorlattervezés és végrehajtás során megkezdte a fenti ajánlások implementálását, az eseményláncokat folyamatosan aktualizálja a megszerzett tapasztalatok alapján. A kibervédelemben érintett szervezetek közösen vizsgálják a DIME spektrumában történő feladat-végrehajtás kihívásaira adható válaszokat, ezzel összhangban aktualizálják a szabályzói keretrendszert. Szinte bizonyos, hogy a közeljövőben új, ma még nem azonosított kihívások fognak megjelenni, amelyekre csak akkor adható gyors és hatékony válasz, ha a jelenleg kialakított folyamatok már készségszintűek.

Felhasznált irodalom

2024. évi LXIX. törvény Magyarország kiberbiztonságáról. Online: https://net.jogtar.hu/jogszabaly?docid=a2400069.tv

Bányász Péter – Orbók Ákos (2013): A NATO kibervédelmi politikája és kritikus infrastruktúra védelme a közösségi média tükrében. *Hadtudomány,* 23(E-szám), 188–209. Online: https://ojs.mtak.hu/index.php/hadtudomany/article/view/6705/5304

Clarke, Richard A. – Knake, Robert K. (2019): *The Fifth Domain*. [H. n.]: Penguin Books. Online: www.penguinrandomhouse.com/books/600219/the-fifth-domain-by-richard-a-clarke-and-robert-k-knake/

ENISA (2024): *Cyber Europe 2024: Unveiling Key Insights From the Cyber Exercise That Tested the Cybersecurity of EU's Energy Sector.* Online: www.enisa.europa.eu/news/cyber-europe-2024-unveiling-key-insights-from-the-cyber-exercise-that-tested-the-cybersecurity-of-eus-energy-sector

Ertan, A. et al. szerk. (2020): *Cyber Threats and NATO 2030: Horizon Scanning and Analysis.* Tallinn: CCD COE. Online: https://ccdcoe.org/uploads/2020/12/Cyber-Threats-and-NATO-2030_Horizon-Scanning-and-Analysis.pdf

Haig Zsolt (2023): A kibertéri műveletek fejlődése: a számítógép-hálózati műveletektől a kibertéri befolyásolásig. In Krasznay Csaba (szerk.): *Taktikák és stratégiák a kiberhadviselésben.* Budapest: Ludovika. Online: https://tudasportal.uni-nke.hu/xmlui/handle/20.500.12944/102124?key=Kiberv%C3%A9delem%20%C3%A9s%20nemzetbiztons%C3%A1g%20kiss

Kertész Bence (2023): Kiberműveletek az Izrael és Hamász közötti háborúban. *biztonságpolitika.hu,* 2023. október 30. Online: https://biztonsagpolitika.hu/cikksorozatok/kibermuveletek-az-izrael-es-hamasz-kozotti-haboruban

Kiss Álmos Péter (2019): A hibrid hadviselés természetrajza. *Honvédségi Szemle,* 147(4), 17–37. Online: https://real.mtak.hu/125219/1/HSZ_2019_147_4_Kiss_Almos_Peter.pdf

[31] 2024. évi LXIX. törvény Magyarország kiberbiztonságáról.

Kovács László (2021): Offenzív kiberműveletek II.: Kibererők és képességeik. *Hadmérnök,* 16(3), 119–137. Online: https://doi.org/10.32567/hm.2021.3.7

Kovács László (2023): *Hadviselés a 21. században: kiberműveletek.* Budapest: Ludovika.

Libicki, Martin (2016): *Cyberspace in Peace and War.* Annapolis, MD: Naval Institute Press. Online: https://books.google.hu/books/about/Cyberspace_in_Peace_and_War.html?id=m4f9DAAAQBAJ&redir_esc=y

Menczelesz Adrián (2025): Digitális védelem a 21. században – hazánk kiberbiztonsági stratégiája és annak megvalósítása. *Jogászvilág,* 2025. június 5. Online: https://jogaszvilag.hu/napi/digitalis-vedelem-a-21-szazadban-hazank-kiberbiztonsagi-strategiaja-es-annak-megvalositasa/#

NATO (2016): *Warsaw Summit Communiqué.* Online: www.nato.int/cps/en/natohq/official_texts_133169.htm

NATO (2025): *NATO Cyber Coalition 2025. Advancing Cyber Defence and Strengthening Alliance Resilience.* Online: www.act.nato.int/article/cyber-coalition-2025/

NATO CCDCOE (2022): *NATO Cyberspace Exercises: Moving Ahead CyCon 2022 Workshop Summary.* Online: https://ccdcoe.org/library/publications/nato-cyberspace-exercises-moving-ahead-cycon-2022-workshop-summary/

NATO Cyber Defence Pledge (2016). Online: www.nato.int/en/about-us/official-texts-and-resources/official-texts/2016/07/08/cyber-defence-pledge

NATO Standard Allied Joint Publication-3.20. Allied Joint Doctrine for Cyberspace Operations (2020). Online: https://assets.publishing.service.gov.uk/media/5f086ec4d3bf7f2bef137675/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf

Resperger István (2018): *A válságkezelés és a hibrid hadviselés*. Budapest: Dialóg Campus. Online: https://bit.ly/4sFA7Gx

Rid, Thomas (2020): *Active Measures. The Secret History of Disinformation and Political Warfare.* London: Profile Books. Online: https://books.google.hu/books/about/Active_Measures.html?id=lWltDwAAQBAJ&redir_esc=y

Schmitt, Michael N. szerk. (2017): *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press. Online: https://assets.cambridge.org/97811071/77222/frontmatter/9781107177222_frontmatter.pdf

Şeker, Ensar (2019): The Concept of Cyber Defence Exercises (CDX): Planning, Execution, Evaluation. *arXiv:1906.03184.* Online: https://doi.org/10.1109/CyberSecPODS.2018.8560673

Szabó András (2018): Ajánlás TTX gyakorlatok szervezéséhez. *Hadmérnök,* 13(KÖFOP), 235–251. Online: www.hadmernok.hu/180kofop_14_szabo.pdf

Szöllősi Gergely (2024): Locked Shields 2024: Kimagasló magyar eredmény. *Honvédelem,* 2024. május 21. Online: https://honvedelem.hu/hirek/locked-shields-2024-kimagaslo-magyar-eredmeny.html

Vykopal, Jan et al. (2017): Timely Feedback in Unstructured Cybersecurity Exercises. *arXiv:1712.09424.* Online: https://doi.org/10.48550/arXiv.1712.09424

Zacharis, Alexandros – Katos, Vasilios – Patsakis, Constantinos (2024): Integrating AI-Driven Threat Intelligence and Forecasting in the Cyber Security Exercise Content Generation Lifecycle. *International Journal of Information Security,* 23(4), 2691–2710. Online: https://doi.org/10.1007/s10207-024-00860-w

HADMÉRNÖK
VÉDELEMINFORMATIKA

20. évfolyam (2025) 4. szám 87–102.
DOI: 10.32567/hm.2025.4.6

Tóth Ádám[1]

Zero trust network access az ipari (OT) kiberbiztonságban

Ipari rendszerek távelérésének új megközelítése

Zero Trust Network Access Solutions in Operational Technology Environments

New Approaches of Remote Access in Industrial Environments

Absztrakt

A cikk az ipari rendszerek (OT) távelérésének kiberbiztonsági kihívásait vizsgálja, különös tekintettel a VPN-alapú megoldások sérülékenységeire és a zero trust architektúrára épülő zero trust network access (ZTNA) technológia bevezetésének lehetőségeire. A cikk összehasonlítja a VPN és a ZTNA működését, bemutatva az előnyöket és korlátokat, mint például a legkisebb jogosultság elvének való megfelelés mértéke, az identitásalapú hozzáférés-kezelés és az egyszerűbb szabálykezelés. Emellett vizsgálja a ZTNA OT-környezetbe történő integrációs lehetőségeit a Purdue-modellt is figyelembevéve, kitérve az architekturális megvalósíthatósági lehetőségekre, felhívva a figyelmet az implementáció egyéb kihívásaira. A szakirodalmi áttekintés alapján megállapítható, hogy a ZTNA növelheti az OT kiberbiztonságát, ugyanakkor sikeres bevezetése a megfelelő infrastruktúra-előkészítésen, fokozatos bevezetésen és a költség-haszon arány mérlegelésén is múlik.

Kulcsszavak: ipari rendszerek, OT, távoli elérés, ZTNA, zero trust, zero trust architektúra

[1] Óbudai Egyetem Neumann János Informatikai Kar.

Abstract

The thesis examines the cybersecurity challenges of remote access to industrial systems (OT), with particular emphasis on the vulnerabilities of VPN-based solutions and the potential implementation of zero trust network access (ZTNA) technology built on zero trust architecture. It compares the operation of VPN and ZTNA, highlighting advantages and limitations such as the extent to which the principle of least privilege is enforced, identity-based access management, and simplified policy control. The study also explores the possibilities for integrating ZTNA into OT environments, taking into account the Purdue model and addressing architectural feasibility as well as other implementation challenges. The findings indicate that while ZTNA can enhance OT cybersecurity, its successful deployment depends on proper infrastructure preparation, gradual rollout, and careful consideration of the cost–benefit ratio.

Keywords: industrial control systems, OT, remote access, ZTNA, zero trust, zero trust architecture

Bevezetés

Tudományos problémafelvetés

A Dragos ipari (*operational technology,* OT) kiberbiztonsági szervezet 2025-ös átfogó jelentése[2] szerint 2024-ben a zsarolóvírus-támadás volt az egyik leggyakoribb OT-t érintő támadási módszer. A zsarolóvírusokra specializálódott támadó csoportok (*advanced persistent threat,* APT) az összes támadás 60%-ában vettek célba ipari létesítményeket. Ezen támadásokat nagy részben a távoli elérést biztosító megoldásokon keresztül hajtották végre. A legtöbb támadó csoport által alkalmazott támadási vektorok között szerepel a virtuális magánhálózatok (*virtual private network,* VPN), illetve egyéb távelérést biztosító megoldások sérülékenységeinek kihasználása, és az azokkal kapcsolatos azonosítók, jelszavak *(credential)* megszerzése.

Az Escal Institute of Advanced Technologies (SANS) intézet által összeállított, öt legkritikusabb OT kiberbiztonsági kontrollt tartalmazó listában szintén szerepel a biztonságos távoli elérés biztosítása mint kritikus védelmi intézkedés.[3]

A fentiek alapján azonosítható probléma tehát az OT-környezetek távoli elérésének kompromittációjából adódó támadások bekövetkezése.

Kutatási cél

Az azonosított probléma okán felmerül a kérdés, hogy vajon létezik-e az OT távoli elérésére a jelenleg széles körben alkalmazott megoldásoknál biztonságosabb technológia.

[2] Dragos 2025.
[3] Lee–Conway 2022.

Célom egy modernebb, más megközelítésre épített technológiai megoldás vizsgálata az OT távoli elérésével kapcsolatos biztonságának növelése érdekében.

A cikk szakirodalmi áttekintés útján körbejárja a jelenlegi megoldásokkal kapcsolatos problémákat, és a *zero trust* elvre épített *zero trust network access* (ZTNA) megoldások OT-ban való alkalmazási lehetőségeit vizsgálja.

A vizsgálattal szemben az alábbi kérdéseket fogalmaztam meg:

- Mik a jelenleg alkalmazott megoldások az OT távelérésére? Milyen támadási technikák merülnek fel az OT távoli elérésének esetében?
- Mennyiben nyújtanak nagyobb védelmet a ZTNA-megoldások a VPN-megoldásokkal szemben?
- Mennyire IT-ra szabottak a jelenlegi ZTNA-megoldások, lehetséges-e ZTNA-megoldásokat az OT-ba is implementálni? Milyen kihívások elé állíthatja a szervezeteket egy ilyen implementáció?
- Összességében lehetséges-e ZTNA-megoldás alkalmazása az OT-ban, és ha igen, akkor milyen szempontokat figyelembe véve hozhat felelős döntést a szervezet annak alkalmazásáról?

Hipotézisek

A téma feldolgozása során az alábbi hipotéziseket fogalmaztam meg:

- Általánosságban a ZTNA-megoldások alkalmasak a VPN kiváltására, és nagyobb biztonságot képesek nyújtani a VPN-megoldásoknál.
- Architekturális szempontból lehetséges a ZTNA alkalmazása az OT-ban.
- Az OT rugalmatlansága, technológiai szempontból való lemaradottsága miatt a ZTNA-megoldások OT-ba való integrációja nehézségekkel jár.

Kutatási módszer

A vizsgálat során a releváns szakirodalom, gyártói ajánlások és leírások, publikáció, technológiai megoldások működésének áttekintésén keresztül kaptam válaszokat. A szakirodalom tanulmányozása során olyan naprakész forrásokat kerestem, amelyek a *zero trust* elvnek való megfeleléssel, *zero trust* architektúra kialakításával, a ZTNA-megoldásokkal, OT-architektúramegoldásokkal kapcsolatosak. Továbbá egyéb internetes tartalmakat (tanulmányok, blogbejegyzések, gyártói útmutatók, marketingcélú anyagok stb.) is tanulmányoztam annak céljából, hogy kiderítsem, jelenleg milyen piaci kezdeményezések jelennek meg a ZTNA-megoldások OT-integrációjának kérdése körül, vannak-e konkrét megoldások vagy gyártói javaslatok ZTNA-megoldások OT-környezetbe való implementálásával kapcsolatban.

A fenti vizsgálati kérdésekre adott válaszok alapján a cikk több részre tagolódik:

- A OT-ban jelenleg széles körben alkalmazott és leginkább biztonságosnak tekintett VPN-megoldások alkalmazási lehetőségeinek ismertetése.
- Az OT távoli elérésével összefüggő támadási technikák ismertetése, elsősorban VPN-sérülékenységeken keresztül vizsgálva.

- A ZTNA-megoldások funkcionalitásának ismertetése.
- Összehasonlítás a VPN- és ZTNA-megoldások között a ZTNA által nyújtott magasabb szintű védelem bizonyítására.
- A ZTNA-megoldások implementációjának vizsgálata, architekturális megoldási lehetőségek, a ZTNA Purdue-modellbe való illesztése és az implementáció kihívásai.
- Általános következtetések levonása, a megvalósítás eldöntésének támogatása.

Virtuális magánhálózat (VPN) az ipari irányítási rendszerek távoli elérésére

Az OT-környezetekben is egyre gyakrabban használnak távelérési megoldásokat. Használatuk célja általában a fizikailag messze lévő eszközök elérése, az egyes eszközök, rendszerek külső felek (beszállítók, partnerek, karbantartók) általi támogatásának lehetősége távolról. Az OT-ban népszerű távoli elérést biztosító megoldások közül a VPN-nel foglalkozom, mivel az OT távoli elérésére jelenleg a VPN a leggyakrabban használt és biztonságosnak tekintett megoldás, ezért más megoldásokra (például RDP, VNC stb.) nem térek ki.

A VPN-technológiák megfelelően biztonságos távoli elérést képesek adni. Természetesen sok múlik a megfelelő típus, protokoll kiválasztásán, az architekturális kialakításon, a konfiguráción és egyéb tulajdonságokon, amelyeket a továbbiakban még részletesen érinteni fogok. A felhasználás tekintetében a VPN főbb típusai az alábbiak.

- Kliens-telephely közti/távoli elérésű (client-to-site/Remote access) VPN. A legáltalánosabban használt, egyéni felhasználóknak szánt modell. OT-ban gyakoriak azok a belső és külső karbantartók, akik a szervezet által menedzselt eszközről kívánják elérni az OT-hálózatot. Hasonló célból alkalmazható még a felhőalapú VPN (cloud VPN/VPN as a Service, VPNaaS) is. Ennek előnye, hogy a host oldalon nem szükséges semmilyen infrastrukturális feltételt szabni, hiszen a felhasználó a webes felületen keresztül használja a szolgáltatást, ami egyszerűvé teszi a konfigurációt is. A VPNaaS-megoldások az OT-ban is előfordulhatnak, hiszen a fejlettebb VPN-eszközöket felhős platformon keresztül lehet konfigurálni (platform service). Az általános célú felhős VPN az OT-ban nem fordul elő, mivel az OT nem hosztolja ki az infrastruktúráját a felhőbe.
- Telephelyek közti (site-to-site) VPN. Állandó kapcsolat kialakítására alkalmas megoldás, ahol két hálózat biztonságos összeköttetése valósul meg. Ezt a típust az OT általában egy másik szervezet (például beszállító, partnerszervezet, anyavállalat) hálózatával való összekötése miatt alkalmazhatja.
- Gépek közti (machine-to-machine) VPN. Titkosított, biztonságos adatcsatorna hozható létre gépek, eszközök vagy szolgáltatások között. Egyes szolgáltatók előszeretettel kötik össze a privát felhőjüket az OT-s eszközükkel, ilyen módon menedzselhetővé teszik őket.[4]

[4] Kocsis 2025.

Távelréssel összefüggő támadási technikák

A különböző OT-ra jellemző technikák (*tactics, techniques and procedures,* TTP) megismerésére a MITRE Corporation saját OT-s mátrixszal[5] rendelkezik, amelyben ismerteti az OT-környezetek támadási technikáit. Ezt felhasználva a szervezet megvizsgálhatja a távoli elérésekkel kapcsolatos támadási technikákat, taktikákat és eljárásokat. A mátrix több technikát is tartalmaz, ami közvetlenül a távoli elérést biztosító szolgáltatásokkal, így a VPN-nel is összefüggésbe hozható.

Kezdeti hozzáférés *(initial access)* kategória

Exploitation of remote services. Ebben az esetben a cél, hogy valamilyen sérülékenységet kihasználva a támadó hozzáférjen az OT-környezethez. A technikával kapcsolatban a MITRE zsarolóvírus-támadásokat hoz fel példaként, ahol az eredetileg a szervezet irodai informatikai környezetébe (IT-ba) bejuttatott vírussal, az OT kompromittálása után sikerült megfertőzni az ipari környezetet is, ami egy újabb példa annak igazolására, hogy a legtöbb támadás az IT-zónából szivárog át az OT-ba.[6]

External remote services. A technika lényege, hogy a távelérést biztosító szolgáltatások feltörése útján szereznek hozzáférést a felügyeleti rendszerekhez, és hajtanak végre támadásokat. Erre a MITRE példaként hozza fel a VPN-hozzáférések felderítését és kompromittációját, főként valamilyen külső, a szervezet által nem ellenőrzött gépről való elérés vagy nem megfelelő konfiguráció esetén. Ennek megfelelően a célpontok között felsorolták a VPN-szervert is.[7]

Remote services. A fenti technika a külső távelérésre, ez viszont már a belső hálózaton belüli távelérésre is jellemző, és példaként hozza fel a távoli asztali protokollokat (például *remote desktop protocol,* RDP), a *server message block* (SMB) protokollt, vagy a *secure shell* (SSH) protokollt is. A MITRE példaként hozza fel ezen megoldások kihasználását fájlátvitelre és kódfuttatásra az IT-zónában kompromittált eszközről az OT-környezetbe. A technika egyik fontos tanulsága, hogy ne használjunk olyan *dual-home* megoldást, amelyen keresztül a távelérési megoldást kihasználva támadják az ipari rendszereket.[8]

Discovery kategória

Remote system discovery. A hálózaton lévő eszközök valamilyen (például IP-cím, *hostname*) logikai azonosító alapján felderíthetők, így további eszközök kompromittálódhatnak. A MITRE a statikus hálózati konfigurációt javasolja kockázatcsökkentő

[5] Alexander–Belisle–Steele et al. 2020: 7.
[6] MITRE 2025.
[7] MITRE 2025.
[8] MITRE 2025.

intézkedésként, ami az OT-környezet esetében még egyszerűbben is megvalósítható, hiszen ott gyakoribbak a statikus eszközök.[9]

Remote system information discovery. A távoli elérést biztosító megoldások és azok konfigurációjának feltérképezésével a támadók információt gyűjthetnek a különböző szabályozásokkal, viselkedési mechanizmusokkal kapcsolatban. Ezen keresztül látható a támadó számára, hogy a céljainak megfelelő célpontot talált-e.[10]

Lateral movement kategória

Amikor a támadó érvényes felhasználónévvel és jelszóval (például egy VPN-fiókhoz) bejut a vállalati hálózatba, az elsődleges célja, hogy minél mélyebbre jusson, és minél magasabb jogosultságokat szerezzen. Ezt a folyamatot nevezik oldalirányú mozgásnak *(lateral movement)*. A CrowdStrike 2025-ös Globális Fenyegetettségi Jelentése[11] szerint a támadók rendkívül gyorsak: a kezdeti behatolást követően átlagosan mindössze 48 perc alatt megkezdik az oldalirányú mozgást a hálózaton. A leggyorsabb mért *breakout time* pedig mindössze 51 másodperc volt. Ez a szűk időablak hatalmas nyomást helyez a védelmi csapatokra, hogy a behatolást szinte azonnal észleljék, és megállítsák.[12]

Az oldalirányú mozgás kategóriába eső technikák általánosságban a távelérést biztosító rendszerek kompromittációjának lehetőségeit tartalmazzák, amelyet kihasználva a támadó képes továbbmenni a környezetben, további zónákban lévő eszközök elérése érdekében, ezért a MITRE ICS mátrixában szereplő összes ilyen technikát felsorolom.[13]

Default credentials. Az alapértelemezett jelszavak gyakoriak, főként a programozható logikai kontrollerek (*programmable logic controller,* PLC) és ember-gép interfészek (*human-machine interface,* HMI) esetében. Ezeket a kockázatokat hozzáférés-kezeléssel és jelszószabályok *(policy)* megfelelő kialakításával csökkenteni lehet.

Exploitation of remote services. Azonos az *initial acces* kategóriában lévő azonos nevű technikával.

Hardcoded credentials. A szoftverek vagy *firmware*-ek kódjai tartalmazhatnak olyan alapértelmezett jelszavakat, kriptográfiai kulcsokat, vagy API-kulcsokat *(API-token)*, amelyeket felfedve a támadó jogosulatlanul szerezheti meg a felhasználói munkamenetet *(session)*. Ezeket gyakran az adatgazdák sem ismerik, vagy nehéz módosítani azokat, mert ez rossz hatással lehet az üzemmenetre. Ezek az azonosítók a gyártók, modellek esetében ugyanazok szoktak lenni. Ezért a hozzáférés-menedzsment részévé kell tenni ezen kulcsok, azonosítók kezelését is.

Lateral tool transfer. A támadók a fájlmegosztó-protokollok sérülékenységeit vagy rossz konfigurációt kihasználva képesek fájltranszfereket végezni, amivel támadó

[9] MITRE 2025.
[10] MITRE 2025.
[11] Crowdstrike 2026.
[12] Frész 2025.
[13] MITRE 2025.

kódokat is képesek átültetni további rendszerekbe. Ennek végrehajtására a támadók a távoli elérések sérülékenységeit is kihasználják.

Program download. Protokollsérülékenység kihasználásával a támadó képes programletöltésre vagy -módosításra az eszközökön (például PLC-ken és kontrollereken). Kockázatcsökkentő intézkedés az alkalmazás naplózása, illetve a letöltések és módosítások monitorozása.

Remote services. Azonos az *initial access* kategóriában lévő azonos nevű technikával.

Valid accounts. A támadók valósnak hitt felhasználókként képesek a távoli elérést biztosító megoldáson keresztül bejutni a belső hálózatba. Ennek egyik megelőzési lehetősége többek között a többtényezős hitelesítés (*multi-factor authentication,* MFA), a felhasználói fiókok megfelelő menedzsmentje vagy a hálózati forgalom szűrése is.

A cikk további részében azt is megvizsgálom, hogy a fenti támadási technikák alkalmazhatók-e a ZTNA-megoldások használata esetén.

A ZTNA-megoldások rövid története

A *soha ne bízz, mindig ellenőrizz* (*zero trust,* ZT) elv régóta ismert, gyakorlati megvalósítására számos technológiai megoldás lehetőséget adott az utóbbi évtizedekben. Ezek a technológiák alapvetően egy-egy informatikai terület esetében biztosították ezt az elvet, így számos különálló megoldást kellett párhuzamosan implementálni és üzemeltetni ahhoz, hogy a szervezet a lehető legtöbb területen elérje a *zero trust* elv szerinti működést.

A hálózati szegmentációval a szervezet jelentősen csökkentette annak kockázatát, hogy egy támadó több szervezeti egység gépeit is elérje, például nem jutott át más virtuális helyi hálózatokba (*virtual local area network,* VLAN), így kevesebb kárt tudott okozni. Azonban így is, az adott hálózati szegmensen belüli felhasználói tevékenységek ezzel még nem kontrolláltak, legfeljebb naplózottak.

A *zero trust* architektúra (*zero trust architecture,* ZTA) is egy adott területre összpontosít – a hálózati forgalmon valósítja meg a *zero trust* elvet –, amivel a hálózati szegmentációnál is egy magasabb szintre emeli a biztonságot és az elvnek való megfelelést. A *zero trust* architektúra szerint „semmilyen felhasználó vagy eszköz nem tekinthető alapértelmezetten megbízhatónak, függetlenül attól, hogy a hálózaton belül vagy kívül található. Minden egyes hozzáférési kísérletet szigorúan ellenőrizni és hitelesíteni kell."[14]

A ZTA-elvnek való megfelelést a NIST SP 800-207 számú publikáció[15] is segíti (a továbbiakban, ahol külön nem hivatkozom, ebből a munkából indulok ki), amely meghatározza a ZTA kialakításához szükséges követendő alapelveket. Az alpontokban lévő magyarázatok a távelérések kapcsán is fontos követelmények, akár az OT-ban is.

- Minden adatforrást és szolgáltatást erőforrásként kell kezelni:
  - például a magánkézben lévő vagy külső harmadik félnél, például külső szerződéses karbantartóknál lévő eszközök is ilyen erőforrások, amennyiben

[14] Frész 2025.
[15] Rose et al. 2020: 6.

azokkal szervezeti erőforrások érhetők el. Az OT-ban gyakori a tranziens eszközök használata, amelyek felett a szervezet nem gyakorol kontrollt, nincs nyilvántartva, ezért nem kontrollálandó erőforrásként kezeli, pedig támadási felületet jelent az OT-hálózat számára.

- A hálózattól függetlenül minden kommunikációt biztonságossá kell tenni:
  - attól, hogy egy eszköz a szervezet által menedzselt hálózatban van vagy azon kívül, nem tekinthető megbízhatónak, minden kommunikációs csatornán védeni kell az adatok bizalmasságát és sértetlenségét. Az OT-ban a kommunikációs csatornákkal kapcsolatos legfőbb probléma a titkosítatlan kommunikációs protokollok használata.
- Munkamenet (session) alapon kell megadni a hozzáférést az egyes erőforrásokhoz:
  - a távelérések kapcsán is fontos követelmény a session alapú hozzáférés engedélyezése, ilyenkor a rendszer csak egy adott szolgáltatásához adunk hozzáférést, amivel szintén szűkíthetjük a jogosultságokat.
- Dinamikus szabályokkal kell kezelni az erőforrásokhoz való hozzáféréseket:
  - a dinamikus szabályok esetében (policy) az eszköz olyan tulajdonságait kell figyelembe vennie, mint az idő, szoftververzió, lokáció vagy különböző viselkedési tulajdonságok. Ezek az OT távelérésében is szerepet játszhatnak a külső hálózatokból csatlakozó eszközök tulajdonságainak megfigyelésére.
- Minden eszköznek monitorozni és mérni kell az integritásra, rezilienciára vonatkozó képességeit:
  - a távoli felhasználók esetében más típusú tulajdonságokat lehet szükséges meghatározni, mint a belső hálózaton lévők esetében, például egy, a szervezet által nem menedzselt külső karbantartó eszközéről a végpontvédelmi rendszer frissítéseit is javasolt felülvizsgálni, hiszen az eszközön nem a szervezet kezeli a vírusadatbázis frissítéseit.
- Dinamikus autentikációs és authorizációs folyamatokat kell kialakítani minden erőforrás esetében:
  - ennek megvalósítását segítik az IAM *(identity and access management)* rendszerek és eszközmenedzsment-rendszerek, a többtényezős hitelesítés (MFA), amelyek közül a külső felek távelérése esetében korlátozottak a lehetőségek – a nem menedzselt eszközök a legtöbb esetben nem rendelkeznek a szervezet által használt rendszerek klienseivel.
- Adatgyűjtés és -elemzés:
  - a lehető legtöbb adatot be kell gyűjteni annak érdekében, hogy minél pontosabb szabályokat (policy) lehessen meghatározni, és folyamatosan fejleszteni az egyes erőforrásokra, ami a távoli felhasználók esetében a lokációra vonatkozó tulajdonságok esetében már nehezebben használható.

Zero trust network access (ZTNA)

Az OT fejlődése megköveteli a biztonságának fejlesztését is. Egyre nagyobb az igény a felügyeletre, az adatvezérelt gyártásra (ipar 4.0, IIoT) egyre több IT/OT-kapcsolat

kiépítését követeli meg, a szakértők, karbantartók egyre többször használnak távelérést. Ezek a fejlesztések biztonsági szempontból támadási felületként jelentkeznek, amelyekre egyre több és hatékonyabb védelmi intézkedést kell kialakítani. Az OT számára is egyre fontosabb lesz a jelenleg még inkább csak az IT-ban alkalmazott kiberbiztonsági elvek, gyakorlatok alkalmazása. Ugyanakkor az IT/OT-konvergencia megteremtése segíti a szervezetben összhangba hozni a két terület kiberbiztonsági képességeit is. Ezért fontos vizsgálni a távoli elérések fejlesztési lehetőségeit is az OT-ban, akár egy *zero trust network access* (ZTNA-) megoldás implementációs lehetőségeinek vizsgálatán keresztül.

A *zero trust* architektúra elvére építve a *zero trust network access* (ZTNA-) megoldások gyakorlati megvalósítását kínálják a biztonságos távelérésnek. A ZTNA nemcsak egy szoftveres funkció, hanem architekturális megoldás is, amely megvalósítja a távoli felhasználók beléptetését, validálja azok biztonsági állapotát *(security posture)*, elrejti az erőforrásokat a felderítéstől *(discovery)*, megakadályozza az oldalirányú mozgásokat *(lateral movement)*, kikényszeríti a felügyeleti szabályokat *(policy)*.

A ZTNA-megoldások nem VPN-alapon működnek, hanem a távoli kliens egy felhős vagy helyi *(on-premise)* brókerhez csatlakozik *(trust broker)*, amelyen keresztül megtörténik az autentikáció, a jogosultságok kiosztása, a protokoll kiválasztása, az időintervallum megadása stb. A bróker egy ZTNA-útválasztóval *(gateway)* kommunikál.

A ZTNA tulajdonságai, előnyei

A jelenleg széles körben használt VPN és annak kiváltási lehetőségeként vizsgált ZTNA-megoldások megismerése után vizsgáljuk meg a ZTNA főbb tulajdonságait és előnyeit, illetve vessük össze a VPN funkcionalitásával!

- Míg a VPN perimeter védelmi megközelítésen alapul, és a teljes hálózathoz enged hozzáférést, addig a ZTNA a zero trust elvre építve biztosítja a mikroszegmentációt, illetve a legkisebb jogosultság *(least privilege)* elvnek való megfelelést.[16]
- A VPN IP-alapú autentikációt, a ZTNA identitás alapú autentikációt valósít meg.[17]
- Legkisebb jogosultság elvének való megfelelés: alkalmazásra korlátozva, adott munkamenetre ad jogosultságot a távoli felhasználónak.[18]
- Folyamatos ellenőrzés *(continous verification)* a távoli eszközön is: operációs rendszer (*operating system,* OS) verzió, antivírusprogram utolsó frissítése, titkosítás alkalmazása (például bitlocker), rosszindulató szoftver *(malicious software, malware)* detekció stb.[19]
- Mivel a szervezet által nem felügyelt eszközök esetében nagyobb a kockázata annak, hogy kompromittált eszközről csatlakoznak a szervezet hálózatába, ezért a ZTNA által nyújtott funkcionalitás mellett a szervezet által nem menedzselt (például BYOD, tranziens) eszközök használatának is kisebb a kockázata.

[16] Mavroudis 2024: 1.
[17] Mavroudis 2024: 3.
[18] Mavroudis 2024: 3.
[19] Mavroudis 2024: 3.

Természetesen VPN-használat esetében is lehetősége van a szervezetnek valamilyen szintű felügyeletre, például ellenőrizheti az eszközön futó legutóbbi vírusellenőrzés dátumát, de ez többletmunkával és feltételekkel jár.[20]

- Auditálhatóság és megfelelés *(compliance):* a központi menedzsmenten keresztül könnyebben és hatékonyabban kezelhetők, felügyelhetők és ellenőrizhetők a szabályok.
- Központi naplógyűjtő- és elemző (*security information and event management,* SIEM) / Műveleti központ (*Security Operational Center,* SOC) integráció: a ZTNA naplói szintén beköthetők központi naplógyűjtő és -elemző (SIEM-) rendszerbe, így hatékonyabbá tehető az incidenskezelés is.
- *Agent* és *agentless* működés is támogatott: a kialakítás lehet felhős vagy *on-prem* is.[21]
- Felhasználóbarát: ZTNA-val nem kell kliensszoftvert telepíteni a gépekre, nem kell kiépíteni a kapcsolatot, mint a VPN esetében, elegendő böngészőn keresztül bejelentkezni a felhős szolgáltatásba.

1. táblázat: A VPN és ZTNA főbb különbségeinek összefoglalása

	VPN	**ZTNA**
Biztonsági funkciók	Biztonságos alagutat biztosít a felhasználó eszköze és a vállalati hálózat között	Testreszabható hozzáférés-vezérlési szabályok
Bizalmi modell	Egyszeri ellenőrzés, perimeter védelem	Dinamikus ellenőrzés, nemcsak a perimeteren, hanem a teljes belső hálózaton belül is
Hozzáférés-biztonsági modell	Az egész hálózathoz való hozzáférés biztosítása	Hozzáférés adott alkalmazásokhoz munkamenetalapon; testreszabhatóság a felhasználói viselkedések alapján (az eszköz állapota és az alkalmazás érzékenysége alapján)
Hitelesítés	Hagyományos módszerek (pl. felhasználónév és jelszó)	A felhasználó hitelesítése hagyományos módszerekkel, az eszközé pedig tanúsítványokkal

Forrás: Fortinet 2025

A ZTNA-architektúra megvalósítási lehetőségei

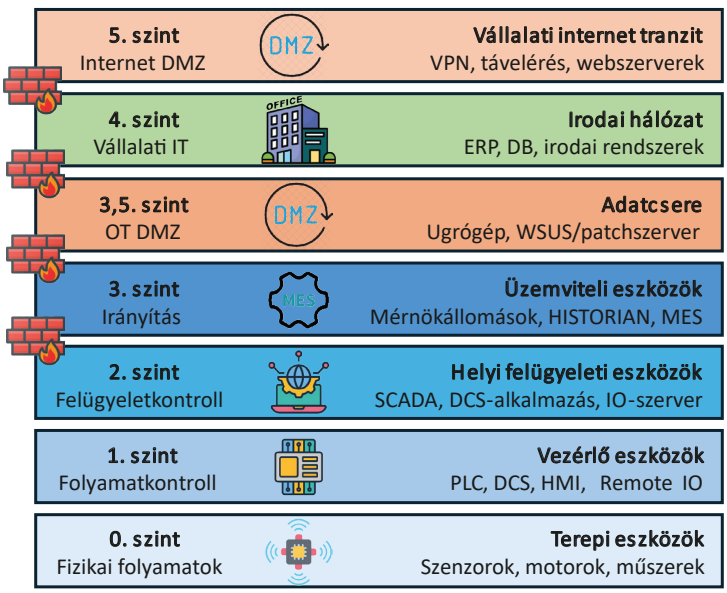
A fejezet egyik célja kideríteni, hogy a jelenleg elérhető, alapvetően IT-infrastruktúrára tervezett ZTNA-megoldások OT-ba való implementálása milyen kihívásokkal járhat, akkor, ha az OT-környezetet valamilyen mértékben a PERA-modell szerint építették ki.

[20] Mavroudis 2024: 7.
[21] Mavroudis 2024: 5.

Implementáció PERA-modell szerint épített architektúrába

Az OT-ban hálózati architektúra kialakításánál követendő modell a *Purdue Enterprise Reference Architecture* (PERA). A *Purdue*-modell szerinti szabályokat az OT-infrastruktúrát távolról elérni kívánó felhasználóra is vonatkoztatni kell. A megvalósítás többféleképpen történhet, de az alapvető szabályok, amelyekre törekedni kell, az alábbiak:

- A távoli elérést közvetlenül az OT-környezetbe végződtetni nem javasolt.
- Zónaátlépések ellenőrzése: a zónák közötti átjárásokat kontrollálni kell.
- Egyet le, egyet fel szabály: egyszerre csak egy zónába lehet fel- vagy lelépni. Ennek vonatkozása a távelérés tekintetében az, hogy a távoli felhasználót nem terminálhatjuk, érkeztethetjük közvetlenül egy alsóbb zónába.



1. ábra: PERA-modell
Forrás: The Claroty Team 2023

A napjainkban javasolt kialakítás demilitarizált zóna (*demilitarized zone,* DMZ) használatával javasolt, ahol a PERA szerinti 3,5. (OT DMZ) és/vagy az 5. zónában (IT-internet DMZ-je) van kialakítva DMZ. A DMZ alkalmazása többféleképpen is történhet, de az alapvető előnye, hogy a távoli elérést ide lehet végződtetni. A két tűzfal között elhelyezett DMZ-be lehet elhelyezni azt az ugrógépet *(jump host)*/terminálszervert, amelyen keresztül a felhasználó az alsóbb zónákba ugorhat. A DMZ tartozhat az OT-hoz, de az IT DMZ-n keresztül is megvalósítható a távelérés. Az alábbi két példa szemlélteti a DMZ kialakításának lehetőségeit:[22]

[22] Andersson 2023: 7.

- OT DMZ: amikor az OT-nak saját DMZ-je van, akár külön a távelérésre dedikáltan *(remote access DMZ).* Javasolt ide végződtetni a VPN-t, és elhelyezni azt az ugrógépet, amelyen keresztül elérhető a hármas zóna. A hármas zónából szintén ugrógéppel javasolt elérni a kettes zónában lévő felügyeleti eszközöket.
- IT (internet) DMZ: ebben az esetben az ötös zónában lévő IT DMZ tölti be az OT DMZ szerepét. Az IT DMZ-t külön tűzfal választja el a hármas zónától, amelyben szintén ugrógépeken keresztül juthatunk le a kettes zónába.

ZTNA-implementációs lehetőségek architekturális szempontból

Természetesen az infrastruktúra adottságaitól függően többféleképpen is megvalósítható az implementáció, az alábbiakban bemutatok néhány szcenáriót.

OT DMZ. Az OT implementáció legvalószínűbb architekturális megvalósítása, hogy a ZTNA *gateway* az OT DMZ-ben (*industrial* DMZ, L3,5) kap helyet, vagyis:

- a felhasználó VPN-n helyett ZTNA-megoldással terminálódik a DMZ-be.
- A DMZ-ből az OT-hálózatba már a megszokott módon, például ugrógépeken keresztül érheti el az alsóbb zónákat.
- Amennyiben az IT-ból való elérést is távoli elérésnek tekintjük, úgy lehetséges a ZTNA gateway-en keresztül elérni az IT-ból is az OT DMZ-t.

Előnyök:

- A VPN helyett egy jobban kontrollált és könnyebben menedzselhető megoldást használhat az OT, miközben az OT-hálózati működés nem változik, így kisebbek a működési és implementációs kockázatok, illetve költségek is.
- Nem szegjük meg a PERA-modell szerinti szabályokat.

Internet DMZ. Amennyiben a szervezet nem rendelkezik OT DMZ-vel, úgy az IT-internet DMZ-jébe is telepíthető a ZTNA *gateway,* ahonnan ugrógépen érhető el a 3. zóna (L3). Ez esetben egyszerre az IT és OT használatra is alkalmazható a megoldás, ami kedvezőbb lehet a szervezet számára.

DMZ-to-DMZ. A szervezet az internet DMZ-ben lévő *gateway-nek* ad elérést az OT DMZ-ben lévő ugrógéphez, vagy egy ott lévő másik *gateway-hez.*

OT belső hálózat. A fenti példák mellett egy másik megközelítés, hogy a *gateway-eket* az OT-hálózatba is implementáljuk: az alsóbb zónákban lévő *gateway-ek* kommunikálnak egymással, így az OT-hálózaton belül az ugrógépeket váltjuk ki ZTNA-eszközökkel. Ehhez hasonló megoldással már rendelkezik a Cisco, amely a saját ipari útválasztóiba *(switch)* integrálta a ZTNA-alkalmazást.[23]

[23] Lobo 2023.

ZTNA-implementációs kihívások az OT-ban, ZTA-implementációs követelményeken keresztül vizsgálva

A NIST SP 800-207 publikáció alapján a ZTA kialakításának támogatásához az alábbi hálózati követelményekkel kell rendelkeznie az OT-nak. A ZTNA-megoldások implementálásának tekintetében az alábbi szempontok szintén fontosak. Az alpontokban az OT sajátosságaiból eredő problémákon keresztül lehet képet kapni a ZTNA implementációjának kihívásairól az OT-ban:

- Az objektumoknak *(enterprise assets)* alapvető hálózati kapcsolattal kell rendelkezniük.[24]
  - Az OT-eszközök hálózati kapcsolataival kapcsolatos probléma lehet, hogy nem képesek TCP/IP-protokoll szerinti *(transmission control protocol)* kommunikációra, például csak ModBUS-protokollon vagy egyéb módon érhetők el, IP-címük nincs.
- A szervezetnek meg kell tudnia különböztetni, hogy mely eszközök tartoznak a vállalathoz, és fel kell mérnie azok biztonsági állapotát.[25]
  - Az OT-nak részletes eszközleltárral kell rendelkeznie, amelynek olyan tulajdonságokat is tartalmaznia kell, amely alapján megállapítható, hogy az eszköz képes-e a ZTNA-megoldással való együttműködésre. Az elavult *(legacy)* eszközök és alkalmazások nem képesek megfelelően kommunikálni a ZTNA-*gateway-jel*.[26]
- A hálózaton le kell tudni követni minden adatforgalmat.[27]
  - A szabályok *(policy)* pontosabb létrehozása érdekében minél több metaadatot ki kell tudni nyerni az eszközökből és a velük történő kommunikációból. Ez OT-ban gondot okozhat a szűkös erőforrásokkal rendelkező eszközök esetében, és növelheti a késleltetést *(latency)* is.[28]
- A vállalati erőforrások nem érhetők el anélkül, hogy szabályokat kikényszerítő megoldáson (*policy enforcement point* [PEP], ami a ZTNA esetében a gateway) keresztül történne a hozzáférés.[29]
  - Ehhez minden távoli felhasználónak a ZTNA-*gateway-en* keresztül kellene haladnia. OT-ban egyes gyártók gyakran saját távoli menedzsmentmegoldást adnak a termékeikhez, *machine-to-machine* VPN-megoldással. Ezek PEP-en keresztüli megvalósítása akadályokba ütközhet.
- Az adatsík és a vezérlési sík logikailag el kell legyen választva.[30]
  - Az OT-menedzsment interfészeket külön menedzsment VLAN-ban kell szeparálni az OT tényleges üzemi rendszereinek interfészeitől.
- Az objektumoknak el kell érniük a PEP komponensét.[31]

[24] Rose et al. 2020: 6.
[25] Rose et al. 2020: 6.
[26] Mavroudis 2024: 7.
[27] Rose et al. 2020: 6.
[28] Mavroudis 2024: 6.
[29] Rose et al. 2020: 6.
[30] Rose et al. 2020: 6.
[31] Rose et al. 2020: 6.

  - A távolról elérni kívánt OT-eszköznek el kell érnie a ZTNA-*gateway-t,* és tudnia kell vele kommunikálni. Ez esetben is problémát okozhat az OT-ban gyakran jelen lévő elavult eszköz, amely nem feltétlenül lesz képes kapcsolatot kiépíteni a *gateway-jel*.
- A PEP az egyetlen komponens, amely hozzáfér a *policy administratorhoz (trust brokerhez)* az üzleti folyamat részeként.[32]
  - A ZTNA-megoldások kialakításukból fakadóan teljesítik a követelményt. Ezért a jelen szempontokat figyelembe véve adott a követelmény teljesítése.
- A távoli vállalati eszközöknek hozzá kell férniük a vállalati erőforrásokhoz anélkül, hogy előbb a vállalati hálózatot kellene használniuk.[33]
  - A ZTNA-megoldások esetében a távoli felhasználónak nem kell először a belső hálózatot elérnie, és onnan elérnie egy felhőszolgáltatást (például e-mail), mintha *full-tunnel* VPN-t használna. Ehelyett a ZTNA-*gateway* hitelesíti a távoli felhasználót, ahonnan egyből a privát felhőbe terminálható, a belső hálózat érintése nélkül.
- A ZTA-hozzáférési döntési folyamatot támogató infrastruktúrának skálázhatónak kell lennie a változó terhelési igényekhez.[34]
  - A ZTNA-megoldást alkotó komponenseket úgy kell tervezni, hogy képesek legyenek kiszolgálni a nagyobb számban érkező kéréseket. Mivel a távoli hozzáférések tekintetében ezek a komponensek szűk keresztmetszetek *(bottleneck)*, ezért biztosítani kell a magas rendelkezésre állásukat.
- Bizonyos esetekben a vállalati eszközök nem érhetnek el bizonyos PEP-eket a szabályzat vagy megfigyelhető tényezők miatt.[35]
  - A ZTNA esetében a szabályok beállítása révén bármilyen feltétel szabható, például külföldi lokáció esetén a *gateway* megszakítja a kommunikációt.

Tehát a fenti szempontok figyelembevételével megállapítható, hogy az OT-környezetbe való implementáció gyakran költséges akadályokba ütközhet, ami miatt a szervezeteknek érdemes átgondolniuk egy ilyen projekt elindítását.

Következtetések

A kutatás alapján megállapítható, hogy az OT távoli elérésére jelenleg biztonságosnak tartott és gyakorlatban gyakran használt megoldás a VPN. Azonban a VPN-megoldások számos sérülékenységgel rendelkezhetnek, amelyekkel támadási felületet adnak a támadók számára, így releváns kérdésként merül fel a VPN kiváltására alkalmas megoldás keresése és vizsgálata.

A ZTNA-megoldások a vizsgálat alapján valóban képesek a VPN-megoldások kiváltására, és nagyobb biztonságot képesek nyújtani a távoli elérés biztosítására.

[32] Rose et al. 2020: 6.
[33] Rose et al. 2020: 6.
[34] Rose et al. 2020: 6.
[35] Rose et al. 2020: 6.

Mindez az OT-környezetben ugyanakkor jelentős kihívásokat tartogathat az OT-környezetben lévő eszközök, és általában az OT technológiai lemaradottsága miatt.

A ZTNA-megoldás bevezetése hatékonyabb szegmentációt, erősebb autentikációt, nagyobb vizibilitást, könnyebb kezelhetőséget jelenthet az OT számára. Azonban a szervezetnek mérlegelnie kell a bevezetéssel kapcsolatos OT-működtetési kockázatokat, költséghatékonyságot. Az alábbiakban összefoglaltam a főbb szempontokat.

Fokozatos bevezetés. Javasolt fokozatosan bevezetni: egyszerre csak egy gyártó egy-két eszközének elérésével javasolt tesztelni az implementációt. Közben pedig fokozatosan le kell építeni a VPN-megoldásokat, törekedni kell arra, hogy a ZTNA-*gateway* legyen az egyetlen bejárat az OT-hálózat felé.

Ár-érték arány. Meg kell vizsgálni, hogy a jelenleg kiépített infrastruktúra milyen kockázatokat rejt magában, és ezeken milyen költségek árán, mennyit segíthet az implementáció. Egy jól kialakított és felügyelt környezet esetében nem biztos, hogy a ZTNA-bevezetés a költségeket is figyelembe véve kockázatarányos döntés lenne.

Az implementációt lehetővé tevő körülmények vizsgálata. A szervezetnek meg kell vizsgálnia, hogy a jelenlegi környezetben működő eszközök/megoldások rendelkeznek-e azokkal a tulajdonságokkal, amelyek lehetővé teszik az implementációt – egy elavult megoldásokat tartalmazó infrastruktúrát nagymértékben fejleszteni kellene ahhoz, hogy képes legyen a ZTNA-funkciók támogatására, ami aránytalanul magas költségeket eredményezhet.

Felhasznált irodalom

Alexander, Otis – Belisle, Misha – Steele, Jacob (2020): *MITRE ATT&CK® for Industrial Control Systems: Design and Philosophy*. Bedford, MA, USA: The MITRE Corporation.

Andersson, Niklas (2023): *The Effect of the IT/OT Gap on the NIS 2 Implementation*. Szakdolgozat. Stockholm: Stockholm University Department of Computer and Systems Sciences. Online: https://su.diva-portal.org/smash/record.jsf?pid=diva2%3A1784461&dswid=5127

CrowdStrike (2026): *CrowdStrike 2026. Global Threat Report.* Online: www.crowdstrike.com/en-us/global-threat-report/

Dragos (2025): *2025 OT. Cybersecurity Action Guide.* Online: https://hub.dragos.com/hubfs/312-Year-in-Review/2025/Dragos_2025_OT_Cybersecurity_Global_Action_Guide.pdf?hsLang=en

Fortinet (2025): *ZTNA vs VPN – What's The Better Cybersecurity Solution?* Online: www.fortinet.com/resources/cyberglossary/ztna-vs-vpn

Frész Ferenc (2025*):* Milliárdnyi kiszivárgott hitelesítő adat. *Substack,* 2025. június 19. Online: https://substack.com/@ferencfresz/p-166319450

Kocsis Tamás (2025): *Ipari (OT) kiberbiztonsági szakember képzés*. Óbudai Egyetem Neumann János Informatikai Kar, prezentáció.

Lee, Robert M. – Conway, Tim (2022): *The Five ICS Cybersecurity Critical Controls.* SANS. Online: https://sansorg.egnyte.com/dl/R0r9qGEhEe

Lobo, Ruben (2023): Zero Trust Network Access (ZTNA) – Revolutionizing Remote Access Security Across OT Environments. *Industrial Cyber,* 2023. december

3. Online: https://industrialcyber.co/zero-trust/zero-trust-network-access-zt-na-revolutionizing-remote-access-security-across-ot-environments/
MAVROUDIS, Vasilios (2024): Zero-Trust Network Access (ZTNA). *arXiv:2410.20611*. Online: https://doi.org/10.48550/arXiv.2410.20611
MITRE Corp. (2025): *ICS Matrix*. Online: https://attack.mitre.org/matrices/ics/
ROSE, Scott et al. (2020): *Zero Trust Architecture*. NIST Special Publication 800–207. Online: https://doi.org/10.6028/NIST.SP.800-207
The Claroty Team (2023): *ICS Security: The Purdue Model.* Online: https://claroty.com/blog/ics-security-the-purdue-model
ZAYTSEV, Alexey (2023): OT Remote Access: Can You Trust Your Technician's Laptop? *Cisco Blogs,* 2023. november 9. Online: https://blogs.cisco.com/industrial-iot/ot-remote-access-can-you-trust-your-technicians-laptop

HADMÉRNÖK
KÖRNYEZETBIZTONSÁG
20. évfolyam (2025) 4. szám 103–123.
DOI: 10.32567/hm.2025.4.7

Horváth János,[1] Horváth Zsuzsa[2]

Bolygóvédelem és NEO-kockázatok

Az Apophis aszteroida helye a Torino-, Palermo- és CIRAS-skálán

Planetary Defence and NEO Risks

The Place of the Apophis Asteroid on the Torino, Palermo, and CIRAS Scales

Absztrakt

A cikk a földközeli objektumok (near earth objects, NEO) becsapódási kockázatának értékelési módszereit mutatja be, különös tekintettel az Apophis aszteroidára, amely a bolygóvédelem egyik aktuális kihívása. Először ismertetjük a hagyományos Torino- és Palermo-skálákat. Majd bevezetni javaslunk egy kozmikus becsapódás kockázatbecslő skálát: a „Cosmic Impact Risk Assessment Scale" (CIRAS) skálát, amely hét kulcsfontosságú tényező – energia, becsapódási valószínűség, hátralévő idő, becsapódási helyszín, atmoszferikus hatás, másodlagos veszélyek és elhárítási nehézség – integrált értékelésével finomítja a kockázat meghatározását. Az Apophis aszteroida 2029-es földközelsége kivételes példaként szolgál, hiszen a kezdeti, bizonytalan pályaadatok magas kockázatot sugalltak, míg a legfrissebb mérések a szinte elhanyagolható ütközési esélyt mutatják. A skálák kombinált alkalmazása nem csupán a kockázatok átláthatóbb kommunikációját teszi lehetővé, hanem támogatja a célzott bolygóvédelmi stratégiák kialakítását is. Az új megközelítés révén megbízhatóbb előrejelzések készíthetők, amelyek hozzájárulhatnak a társadalmi és technológiai felkészültség javításához, valamint a potenciális veszélyek időben történő felismeréséhez. A részletes, többdimenziós kockázatértékelés hozzájárulhat a gyors reagáláshoz és a megelőző intézkedések megtételéhez, így biztosítva a Föld (lakóinak) biztonságát a kozmoszból érkező potenciális veszélyekkel szemben. Ez a megközelítés új távlatokat nyithat a planetáris védelem területén.

[1] Cégvezető, Visionary Tech & Event Solutions, e-mail: horvath_janos@visionarytecheventsolutions.com
[2] Oktató, Nemzeti Közszolgálati Egyetem RTK Katasztrófavédelmi Intézet Tűzvédelmi Műszaki Tanszék, e-mail: horvath.zsuzsanna@uni-nke.hu

Kulcsszavak: bolygóvédelem, földközeli objektumok, Torino-skála, Palermo-skála, kockázatértékelés, ütközési valószínűség, energiafelszabadulás, planetáris védelem, multidimenziós kockázati index

Abstract

The paper introduces evaluation methods for the impact risk of near-Earth objects (NEOs), with a particular focus on the Apophis asteroid – a prime example of the current challenges in planetary defence. The paper explains the workings of the traditional Torino and Palermo scales. Additionally, the Cosmic Impact Risk Assessment Scale (CIRAS) is introduced, which refines risk assessment by integrating seven key factors – energy, impact probability, remaining time until impact, impact location, atmospheric effects, secondary hazards, and mitigation difficulty. The close approach of Apophis in 2029 serves as an exceptional case study. While the initial uncertain orbital data suggested a high risk, the most recent measurements indicate an almost negligible chance of collision. The study emphasises that the combined use of these scales not only allows for clearer communication of risks but also supports the development of targeted planetary defence strategies. This new approach enables more reliable forecasts, contributing to improved social and technological preparedness as well as the timely detection of potential hazards. Overall, the research underlines the importance of detailed, multidimensional risk assessments that facilitate swift responses and the implementation of preventive measures, thereby ensuring Earth's safety against potential cosmic threats. This approach opens new horizons in the field of planetary defence.

Keywords: Planetary defence, Near-Earth Objects, Torino Scale, Palermo Scale, risk assessment, impact probability, energy release, planetary defence, multidimensional risk index

Bevezetés

Az elmúlt évtizedekben a földközeli objektumok (*near-earth objects,* NEO) kutatása[3] a bolygóvédelem és az űrkutatás egyik meghatározó területévé vált. Ezenkívül a földi infrastruktúra és ipari létesítmények védelme[4] is egyre nagyobb figyelmet kap a veszélyes objektumok potenciális becsapódásai kapcsán. A földközeli objektumok közé olyan aszteroidák és üstökösök tartoznak, amelyek pályája a Földhöz veszélyes közelségbe kerülhet, és potenciális ütközés lehetőségét jelenti (1. ábra). A történelem során több példa is bizonyította már a becsapódások katasztrofális hatásait – elég csak a Tunguz-eseményre (1908), a cseljabinszki becsapódásra (2013), vagy akár a dinoszauruszokat kipusztító K-T határhoz tartozó Chicxulub-eseményre gondolnunk.

[3] Lásd: https://cneos.jpl.nasa.gov/; https://neo.ssa.esa.int/; Keresztúri–Sárneczky 2023.
[4] Pallagi 2023; Érces–Vass 2018.

1. ábra: Fantáziarajz aszteroidabecsapódásról
Forrás: a szerzők szerkesztése

Már több olyan skála látott napvilágot, amely a földközeli égitestek becsapódási kockázatát igyekszik számszerűsíteni. A legismertebbek közülük a Torino-skála[5] (0–10) és a Palermo technikai skála[6] (folytonos, logaritmikus index), amelyek a becsapódás valószínűségét és a pusztítás mértékét (energiafelszabadulást) egyszerre kívánják megragadni.

A gyakorlati tapasztalat azonban azt mutatja, hogy a valós kockázatot több tényező is befolyásolja, például:

- a becsapódás valószínűsége (P),
- a felszabaduló energia (TNT-egyenértékben),
- a hátralévő idő (mennyi idő van a figyelmeztetésre),
- a becsapódási helyszín (óceán, partközeli vagy szárazföldi zóna, lakott terület),
- a légköri hatások (magaslégköri robbanás, felszíni becsapódás),
- a másodlagos következmények (cunami [szökőár]), kiterjedt tüzek [tűzvész, tűzvihar], globális klímaváltozás),
- az elhárítási nehézség (technológiai és időbeli korlátok).

E többdimenziós kockázati térben egyetlen skála gyakran nem elég részletes vagy rugalmas ahhoz, hogy mindezt tükrözze. Ezért jelen írásunkban újszerű, bővített módszert vezetünk be, amelyet Cosmic Impact Risk Assessment Scale (kozmikus becsapódás kockázatbecslő skála) (CIRAS) néven javaslunk. A CIRAS hét kulcsparaméter (energia, becsapódás valószínűsége, hátralévő idő, helyszín, atmoszferikus hatás, másodlagos kockázatok, elhárítási nehézség) alapján finoman különbözteti meg a különböző ütközési forgatókönyveket, és egy számba is képes sűríteni a teljes kockázatot.

[5] Binzel 2000.
[6] Chesley et al. 2002.

Az alábbiakban először ismertetjük a hagyományosan használt Torino-skálát[7] és Palermo-skálát,[8] majd az általunk javasolt CIRAS-skálát mutatjuk be részletesen. Ezt követően néhány már lezajlott becsapódást, például a cseljabinszki meteorrobbanást,[9] a Tunguz-eseményt,[10] és a Barringer-krátert,[11] illetve a dinoszauruszok korát lezáró Chicxulub-krátert[12] okozó becsapódást vizsgáljuk a különböző skálák alapján. Végül kitérünk a (99942) Apophis aszteroida[13] 2029-es földközelségére, bemutatva, hogyan változott a kezdeti becslések szerint akár riasztó veszélyhelyzet a legfrissebb megfigyelési adatok tükrében.

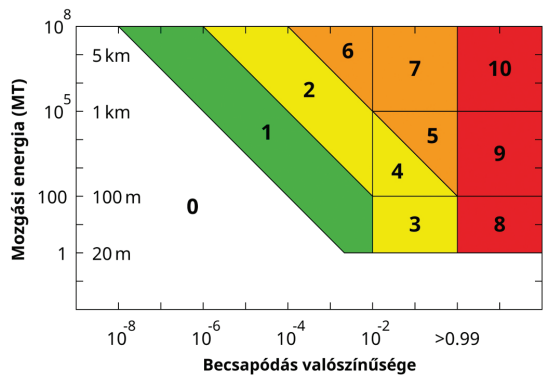
A CIRAS célja, hogy a különböző kockázati tényezőket összehangolva, a szakmai és a laikus közvélemény számára is átláthatóan mutassa be a potenciális ütközésveszélyeket.

Különböző kockázatbecslő skálák

A Torino-skála (Torino Scale)

A Torino-skálát[14] 1999-ben vezették be azzal a céllal, hogy mindenki (a szakemberektől a laikusokig) könnyen megérthesse, milyen mértékű fenyegetést jelent egy-egy újonnan felfedezett égitest és a Föld összeütközésének a lehetősége.[15] A skála 0-tól 10-ig terjedő egész értékekkel osztályozza a kockázatot, egyidejűleg figyelembe véve a becsapódás valószínűségét (P) és a felszabaduló energiát (TNT-egyenértékben, E_{TNT}).

Bár a skálázás végső formája diszkrét (0–10 közötti egész értékek), a háttérben gyakran alkalmaznak folytonos vagy logaritmikus kockázati indexeket, amelyeket aztán lépcsős függvénnyel fordítanak le a Torino-skála egész értékeire. A Torino-skálát mutatja be szemléletesen a 2. ábra.



2. ábra: A Torino-skála
Forrás: Binzel 2000

[7] Binzel 2000.
[8] Chesley et al. 2002.
[9] Borovička 2016; Artemieva–Shuvalov 2016.
[10] Keresztúri–Tóth 2008; Morrison 2018.
[11] Kring 2017; Schmieder–Kring 2020.
[12] Pope et al. 1997.
[13] Apophis ESA [é. n.]; Reddy 2022.
[14] Binzel 2000.
[15] Lásd: https://cneos.jpl.nasa.gov/

Példa egy általános kockázati indexre

Az irodalomban gyakorta használt, leegyszerűsített, úgynevezett logaritmikus modell szerint a becsapódási kockázatot egy I index írja le:

$$I = log_{10}\left(\frac{E_{TNT}}{E_0}\right) + log_{10}\left(\frac{P}{P_0}\right),$$

ahol
$E_{TNT} = a\ robbanás\ energiája\ TNT\text{-}egyenértékben,$
$P = a\ becsapódás\ valószínűsége,$

E_0 és P_0 olyan referenciaértékek, amelyeket a kockázat alapszintjének definiálunk (például $E_0 = 10^6 kt\ TNT$ és $P_0 = 10^{-6}$).

$$\mathrm{TS}(I) = \begin{cases} 0, & \text{ha } I < a_1, \\ 1, & \text{ha } a_1 \le I < a_2, \\ 2, & \text{ha } a_2 \le I < a_3, \\ \vdots & \\ 10, & \text{ha } I \ge a_{10}, \end{cases}$$

Az így kapott I egy folytonos mutató; azonban a Torino-skála (TS) diszkrét besorolás, ezért a két rendszer közötti átmenetet gyakran lépcsős függvénnyel fejezik ki:

ahol $a_1, a_2, \ldots, a_{10}$ az egyes Torino-kategóriák küszöbindexértékei. Ezek megválasztása a történelmi becsapódások gyakoriságán, a fizikai hatások (például légköri robbanás vs. felszíni ütközés) tapasztalatain és a Nemzetközi Csillagászati Unió konszenzusán alapul.

A becsapódás gyakoriságának szerepe

A skála létrehozásakor figyelembe veszik a nagyobb energiájú események ritkaságát is. Gyakorlati becslésekből tudjuk, hogy az E_{TNT} energiával jellemezhető becsapódások átlagos előfordulási gyakorisága (fordított értékük pedig a két esemény közti átlagos időtartam) durván fordított arányosságot követ az energiával vagy a test méretével. Egy leegyszerűsített modellben például:

$$\nu(E_{TNT}) \propto \frac{1}{E_{TNT}^{\alpha}}$$

ahol $\alpha > 0$ valamilyen illesztett paraméter (empirikusan $\alpha \approx 0{,}9 \ldots 1{,}1$). Ez azt jelenti, hogy minél nagyobb energiájú az ütközés, annál ritkább a természetben. A Torino besorolásban a rendkívül ritka, de pusztító erejű objektumok magasabb kategóriát is kaphatnak, még viszonylag alacsony P mellett is.

A Torino-skála kategóriái, 0–10-ig:

- 0 – Az adott objektum ütközési energiája elhanyagolható, vagy az ütközés valószínűsége gyakorlatilag nulla.
- 1 – Rendkívül kicsi a becsapódás esélye; nagy valószínűséggel a további megfigyelések kizárják a veszélyt.
- 2–3 – Kis eséllyel bekövetkező esemény, de már nem teljesen elhanyagolható a kockázat.
- 4–7 – Közepes-magas kockázat; fontos az alaposabb megfigyelés, valamint a lehetséges védelmi stratégiák kidolgozása.
- 8–10 – Magas (vagy közel 100%-os) valószínűségű, globális pusztítást okozó becsapódás.

A skála előnye, hogy a fenti egyenletek (illetve az ezekhez kapcsolódó) számításokat egyetlen, könnyen érthető egész számra redukálja.

A Tunguz-esemény (1908) besorolása a Torino-skálán

A múltbeli nagy erejű becsapódások egyik legismertebb példája az 1908-as Tunguz-esemény.[16] Noha a Torino-skála még akkoriban nem létezett, érdemes megvizsgálni, hogyan illeszkedne, milyen kategóriájú lenne ez a történelemkönyvekbe került esemény.

Becsapódás valószínűsége (P) 1908-ban: a Tunguz-típusú (40–100 méter átmérőjű) objektumok a jelenkori becslések[17] szerint nagyjából 100-200 évente érhetnek el a Föld légkörébe. Ez annyit tesz, hogy egy adott naptári évre vetítve a légkörbe lépés valószínűsége:

$$P \approx \frac{1}{100\ év} = 0{,}01$$

Ez csak nagyon durva becslés, és nem is pontosan a Torino-skálán használt valószínűségi értelemben (hiszen 1908-ban már megtörtént).

Felszabaduló energia (E_{TNT}): egyes becslések szerint a Tunguz-esemény 3–10 megatonna TNT-egyenérték közé tehető robbanási energiával[18] járt. Legyen egy köztes érték, például:

$$E_{TNT} \approx 5{,}0 \cdot 10^6 kt\,.$$

Megfigyelt hatás: a robbanás Szibériában, ritkán lakott területen történt, de körülbelül 2000 km^2 erdőt döntött ki, és a lökéshullám 100–200 km-es körzetben érzékelhető volt. Ha ez lakott terület felett történik, a pusztítás sokkal nagyobb társadalmi-gazdasági kárral járt volna.

[16] Kereszturi–Tóth 2008.
[17] Lásd: https://cneos.jpl.nasa.gov/; https://neo.ssa.esa.int/
[18] Kereszturi–Tóth 2008.

Torino-skála szerinti besorolás: egy több megatonnás légköri robbanás jelentős regionális károkat okozhat, és általában a 8–9 sávba sorolnánk, ha előre tudnánk a bekövetkezését (hiszen egy ekkora energia a lakott területek esetében már katasztrofális lehet). Azonban konkrét valószínűségi besorolást csak előzetes pályaszámítás alapján lehetne adni, ami 1908-ban értelemszerűen nem állt rendelkezésre.

A Tunguz-esemény tehát jól mutatja, miért fontos a Torino-skálán figyelembe venni a robbanási energia nagyságrendjét és a becsapódás valószínűségét egyszerre. Ha egy hasonló objektumot előre észlelnénk, és a számítások alapján lenne reális esély a felszíni vagy légköri robbanásra, legalább 7–8-as (vagy akár magasabb) értéket kaphatna, különösen, ha a várható becsapódás lakott környezetet is érintene.

Összegzés

Összességében a Torino-skála a Földet megközelítő (vagy esetleg eltaláló) égitestek legfontosabb jellemzőit, a pálya adatait, az ütközési valószínűséget és az energiafelszabadulást integrálja. Habár a részletekben gyakran logaritmikus indexeket, sztochasztikus szimulációkat és ritkasági korrekciót is alkalmaznak, a végső kimenet egy könnyen kommunikálható, 0–10 közötti szám, amely a laikus közönség számára is világosan jelzi az esetleges ütközés jelentette veszélyt.

A Palermo-skála (Palermo Technical Scale)

A Palermo-skála a földközeli objektumok becsapódásainak kockázatát egy logaritmikus, folytonos mutatóval fejezi ki. Fő célja, hogy összehasonlítsa a vizsgált becsapódási esemény kockázatát egy úgynevezett háttérkockázattal, vagyis azzal a természetes gyakorisággal, amellyel hasonló vagy nagyobb energiájú égitestek átlagosan ütköznek a Földdel. A Palermo-skála szemléltetése a 3. ábrán látható.

A Palermo-skála matematikai háttere

A Palermo-skála (általános formában) az alábbi módon definiálja az esemény kockázati indexét (PS):[19]

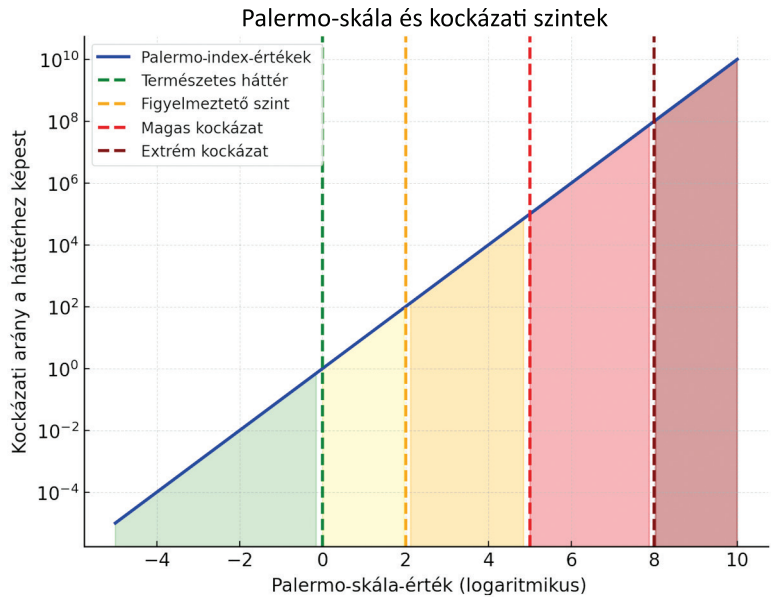
$$PS = log_{10}\left(\frac{P/\Delta t}{f(B)}\right),$$

ahol P a vizsgált esemény (azaz a konkrét becsapódási lehetőség) valószínűsége, Δt a releváns időintervallum, az adott esemény dátumáig hátralevő idő,

[19] Chesley et al. 2002.

f(B) pedig a hasonló vagy nagyobb becsapódási energiájú (vagy pusztító hatású) események évenkénti háttérfrekvenciája a természetes becsapódási statisztikák alapján, B a robbanási/becsapódási energia (TNT-egyenértékben kifejezve).

A PS index logaritmikusan méri, hogy hányszorosára tehető a konkrét esemény kockázata a háttérkockázatnak. A fenti egyenlet egy általános alak, többféle ekvivalens formában is alkalmazzák.



3. ábra: A Palermo-skála
Forrás: a szerzők szerkesztése

A becsapódási energia és a háttérfrekvencia összefüggése

A $f(B)$háttérfrekvencia, vagyis annak a valószínűsége, hogy egy év alatt legalább egy, B vagy annál nagyobb energiájú becsapódás történik, tipikusan egy csökkenő függvény a nagyobb energiák felé. Létezik egy leegyszerűsített, inverz hatványfüggvény-jellegű modell:[20]

$$f(B) \approx \lambda_0 \cdot \left(\frac{B}{B_0}\right)^{-\alpha}$$

ahol λ_0 és B_0 megfelelő normálási konstansok,
α pedig empirikusan meghatározott kitevő (általában 0,8).

[20] Chesley et al. 2002.

A nagyobb energiájú becsapódások egyre ritkábbak, mégpedig közel inverz hatványfüggvény szerint (vagy néha enyhén eltérő lognormális eloszlás alapján).

Ha *B* a becsapódási energia TNT-egyenértékben, tipikusan megajoule vagy kilotonna/megatonna TNT-ben adják meg, majd kiszámítják a rátát, hogy évente átlagosan hányszor fordulhat elő legalább ekkora energiafelszabadulás.

Palermo-index több eseményre

Gyakori, hogy egy adott NEO-nak több különböző Föld-megközelítése is lehet, amelyek mind potenciális ütközési lehetőségeket hordoznak. Ilyenkor a Palermo-indexet az egyes találati valószínűségek, P_i és a hozzájuk tartozó energia, B_i, alapján összegezve vagy maximalizálva is használják. Például, ha k különböző időpontban $(t_1, t_2, \ldots, t_k)$ fennáll a becsapódás lehetősége, az úgynevezett kumulatív Palermo-index[21] lehet:

$$PS_{kumulatív} = log_{10}\left(\sum_{i=1}^{k} \frac{P_i/\Delta t_i}{f(B_i)}\right).$$

Itt: P_i az i-edik potenciális ütközés valószínűsége,
Δt_i az adott ütközés esedékességéig hátralévő idő (évben),
$f(B)$ a megfelelő háttérfrekvencia a B_i energiájú vagy nagyobb eseményekre, a fenti egyenlet szerint.

Megjegyzendő, hogy a valós gyakorlatban a NASA CNEOS (Center for Near Earth Object Studies) vagy az ESA NEOCC (NEO Coordination Centre) saját, szofisztikáltabb sztochasztikus modelljei és a becsapódási valószínűségi függvények *(impact probability density)* alapján számítják a tényleges Palermo-indexeket. A fenti egyenletek szemléltetik a koncepció lényegét, de a végső alkalmazás részletei némileg eltérőek is lehetnek.

A Palermo-index előjele

A Palermo-skálán a 0 szint azt a helyzetet írja le, amikor a kérdéses esemény kockázata megegyezik a „természetes háttérkockázattal" (azaz az átlagos, hasonló energiájú, véletlenszerűen érkező NEO-kkal).

Ha $PS < 0$, akkor az adott esemény kevésbé kockázatos, mint a „háttér", vagyis nagyobb valószínűséggel kerülünk szembe más, véletlenszerű, ismeretlen testtel, mint hogy ez az adott objektum ütközzön velünk. Ha $PS > 0$, akkor a vizsgált égitest kockázata nagyobb, mint amit a „háttér" alapján várnánk. Ez már fokozottabb odafigyelést vagy nyomon követést igényel.

Mindezt képlettel is kifejezhetjük. Tegyük fel, hogy az alapegyenletbeli indexből indulunk ki, és a nevezőt háttéreseménynek tekintjük. Ha $PS > 0$, akkor:

[21] Lásd: https://cneos.jpl.nasa.gov/

$$\frac{P/\Delta t}{f(B)} > 1, \Rightarrow P > f(B)\Delta t,$$

tehát a kérdéses objektum becsapódásának valószínűsége (adott időtartamon belül) magasabb, mint annak az esélye, hogy egy másik, hasonló energiájú égitest ütközne a Földbe.

A Palermo-skála logaritmikus jellege révén minden tízszeres növekedés a valószínűségben vagy az energiában 1 egységet növel az indexen:

$$PS \rightarrow PS + 1 \; ha \; P \rightarrow 10P \; vagy \; E \rightarrow 10E.$$

Hasonlóan, ha a becsapódás valószínűsége a tizedére csökken, a PS értéke 1-gyel csökken. E tulajdonság következtében a skála nagyon jól szemlélteti a kis valószínűségű, de óriási hatású eseményeknél is, hogy mekkora a tényleges kockázat az átlagos, háttérkockázathoz képest.

A Torino- és a Palermo-skála összehasonlítása

Noha a Torino-skála (TS) és a Palermo-skála (PS) hasonló alapgondolaton nyugszik (azaz a becsapódás esélyét és az ütközés energiafelszabadulását veszik főképp figyelembe), a Torino-skála inkább közérthető (0–10 közötti egész érték), míg a Palermo-skála a szakmai igényekre készült, folytonos és finomabb különbségeket is képes megmutatni. A Palermo-skála lehetővé teszi, hogy egy nagyon kicsi, de mégis átlag feletti kockázatot jelentő ütközést (például $PS = +0{,}2$) elkülönítsünk egy egészen elhanyagolható esetűtől (például $PS = -4{,}0$).

Általánosságban, ha az objektum Torino-skálán 0 értéket kap, akkor jó eséllyel a Palermo indexe negatív ($PS < 0$). Ha viszont a TS mondjuk 2–3-as tartományban helyezkedik el, akkor elképzelhető, hogy a PS értéke minimálisan ugyan, de már pozitív (például $PS = +0{,}2$), jelezve, hogy a kockázat kissé meghaladja a háttérszintet.

Összegzés

A Palermo-skála a földközeli objektumok ütközési kockázatát, amelyet a becsapódás valószínűsége és a becsapódás várható energiája határoz meg főképp, egy logaritmikus indexszel méri, figyelembe véve a nagyobb energiájú becsapódások természetes gyakoriságát is.

A Palermo-skála alkalmas arra, hogy finoman rangsorolja a lehetséges földközeli égitestekkel való ütközéseket, és megmutassa, mely objektumok becsapódásának kockázata haladja meg az átlagos háttérkockázatot. Ez különösen fontos olyan eseteknél, ahol a Torino-skála (mivel diszkrét) még nem ad magas értéket, de a szakértőknek már jelezni kell, hogy „ezzel az aszteroidával kicsit többet érdemes foglalkozni".

Cosmic Impact Risk Assessment Scale (CIRAS), egy többtényezős, kozmikus becsapódás kockázatbecslő skála

A CIRAS-skála tényezőinek bemutatása

A Cosmic Impact Risk Assessment Scale (CIRAS) egy többrétű besorolási rendszer a földközeli objektumok becsapódásának kockázatelemzésére. A korábbi skálák (Torino, Palermo) tapasztalataira építve a CIRAS hét kulcstényezőt vesz figyelembe: (E, P, T, L, A, S, M), amelyek a következők:

- E – becsapódási energia (megatonna TNT, log skála),
- P – becsapódási valószínűség (log skála),
- T – hátralévő idő a becsapódásig (log skála),
- L – becsapódási helyszín (diszkrét kategóriák, például óceán, part, szárazföld),
- A – atmoszferikus hatások (diszkrét kategóriák, például légköri robbanás, felszíni becsapódás),
- S – másodlagos veszélyek (diszkrét kategóriák, például tűz, cunamik, globális klímahatás),
- M – elhárítási nehézség (diszkrét kategóriák, például könnyű eltérítés, nukleáris beavatkozás szükségessége).

Az alábbiakban külön bemutatjuk a hét tényező kiszámításának elvi képleteit, majd egy dimenziócsökkentő (összegző) formulát, amellyel a hétténezős eredmény egy számban is összefoglalható.

Becsapódási energia (E)

A CIRAS a becsapódási energiát logaritmikus (Richter-szerű) skálán kezeli. Ha E_{obj} az égitest (aszteroida, üstökös) teljes becsapódási energiája megatonna TNT-ben (Mt TNT), akkor:

$$E_{CIRAS} = log_{10}(E_{obj}/1Mt).$$

Például $E_{obj} = 5Mt$ esetén, $E_{CIRAS} = log_{10}(5) \approx 0.70$.

Becsapódási valószínűség (P)

A Palermo skálához hasonlóan a CIRAS is logaritmikus formában értékeli a becsapódás esélyét:

$$P_{CIRAS} = log_{10}\left(\frac{P_{impact}}{P_{bg}}\right)$$

ahol $P_{impact} \in [0,1]$, a kérdéses objektum ütközési valószínűsége (adott időablakra nézve), míg P_{bg}, az úgynevezett háttér (vagy természetes gyakoriság szerinti) valószínűsége hasonló vagy nagyobb energiájú becsapódásnak ugyanabban az időintervallumban. Ha $P_{CIRAS} > 0$, akkor az esemény kockázata meghaladja a háttérértéket.

Hátralévő idő a becsapódásig (T)

A CIRAS külön tényezőként kezeli, mennyi idő áll rendelkezésre az esetleges ütközés bekövetkeztéig. Legyen Δt_{impact} az években mért hátralévő idő. Ekkor:

$$T_{CIRAS} = log_{10}(\Delta t_{impact})$$

Ha például $\Delta t_{impact} = 50$ év, akkor, $T_{CIRAS} = log_{10}(50) \approx 1.70$

Becsapódási helyszín (L)

A CIRAS diszkrét (0–4) skálán kezeli, hogy az égitest szárazföldön vagy óceánban, illetve lakott vagy ritkán lakott területen csapódna be. Például:

$$L = \begin{cases} 0 & (L0\text{: távoli óceán, minimális közvetlen kár}), \\ 1 & (L1\text{: nyílt óceán, nagyobb cunami}), \\ 2 & (L2\text{: partközeli zóna, súlyosabb cunami}), \\ 3 & (L3\text{: ritkán lakott szárazföld, regionális katasztrófa}), \\ 4 & (L4\text{: városi/metropolisz térség, katasztrofális pusztítás}). \end{cases}$$

Atmoszferikus hatások (A)

A légköri belépés szöge, a sebesség és az anyagszerkezet meghatározza, hogy a test milyen formában fejti ki a pusztító hatását. A diszkrét, 0–4 közötti érték:

$$A = \begin{cases} 0 & (A0\text{: teljes légköri elégés, nincs talajbecsapódás}), \\ 1 & (A1\text{: részleges szétesés, kisebb lökéshullám}), \\ 2 & (A2\text{: magaslégköri robbanás, pl. Tunguz}), \\ 3 & (A3\text{: alacsony légköri robbanás, nagy túlnyomás}), \\ 4 & (A4\text{: felszíni becsapódás, maximális energiaátadás}). \end{cases}$$

Másodlagos veszélyek (S)

A becsapódás következményeit nemcsak a közvetlen robbanás, hanem a másodlagos hatások is befolyásolják,[22] mint például kiterjedt tüzek, szökőárak vagy akár globális klímaváltozás. Különösen ipari területeken egy ilyen esemény másodlagos veszélyeket is jelenthet, például vegyi anyagok szivárgását, robbanásokat vagy tűzterjedést, amelyek ipari biztonsági intézkedéseket[23] igényelnek. A másodlagos (következményes) események közé tartozhat tűzvihar, cunami, globális légköri por és klímaváltozás, vagy akár a biológiai ökoszisztéma összeomlása.

$$S = \begin{cases} 0 & (S0\text{: nincsenek másodlagos hatások}), \\ 1 & (S1\text{: lokális tüzek, kisebb környezeti károk}), \\ 2 & (S2\text{: cunami, nagyobb szeizmikus vagy regionális hatás}), \\ 3 & (S3\text{: globális klímaváltozás, por/aeroszol}), \\ 4 & (S4\text{: ökoszisztéma-összeomlás, kihalási esemény}). \end{cases}$$

Elhárítási nehézség (M)

A CIRAS megkülönbözteti, hogy a test eltérítése mennyire reális (kisebb test, hosszabb felkészülési idő) vagy mennyire reménytelen (nincs elég idő, túl nagy vagy gyors test):

$$M = \begin{cases} 0 & (M0\text{: könnyen eltéríthető, kicsi test, sok idő}), \\ 1 & (M1\text{: közepes erőfeszítés, becsapódó testtel, ütközéssel eltéríthető}), \\ 2 & (M2\text{: nehézkes, nukleáris eszköz is szükséges lehet}), \\ 3 & (M3\text{: rendkívül problémás, kevés idő, hatalmas objektum}), \\ 4 & (M4\text{: szinte lehetetlen, nincs reális védelem}). \end{cases}$$

Egyetlen, összesített CIRAS-index

A CIRAS a fenti hét kategóriával rendkívül részletes képet nyújt. Sokszor azonban szükség lehet egy „összesített" mutatóra, például döntéshozatalnál, amikor a különböző fenyegetések rangsorolása a cél. Ehhez definiálhatunk egy kompozit CIRAS-értéket, vagy CIRAS-indexet:

$$CIRAS_{index} = w_E E_{CIRAS} + w_P P_{CIRAS} + w_T(-T_{CIRAS}) + w_L L + w_A A + w_S S + w_M M,$$

ahol

[22] Keresztúri–Sárneczky 2023.
[23] Pallagi 2023.

E_{CIRAS}, P_{CIRAS}, T_{CIRAS} logaritmikus értékek, $L, A, S, M \in \{0,1,2,3,4\}$ pedig a diszkrét kategóriák.

CIRAS-index súlyozásának indoklása

A CIRAS-index súlyozásának meghatározása kulcsfontosságú annak érdekében, hogy a földközeli objektumok (NEO-k) által jelentett kockázatokat a megfelelő mértékben tükrözze. A következő meggondolások alapján határoztuk meg a súlyokat:

Becsapódási energia (E_{CIRAS}): a robbanási energia fontos tényező, de önmagában nem elegendő a magas kockázat meghatározásához. Közepes súlyt kap.

Becsapódási valószínűség (P_{CIRAS}): a legfontosabb tényező, hiszen a legnagyobb energiájú események is kevésbé aggasztók, ha az ütközési esély elhanyagolható. Ezért ez kapja a legnagyobb súlyt.

Hátralévő idő (T_{CIRAS}): minél kevesebb idő áll rendelkezésre az ütközés előtt, annál sürgetőbbé válik a helyzet. Ezért negatív előjellel szerepel, és viszonylag nagy súlyt kap.

Becsapódási helyszín (L): a lakott területek érintettsége fontos szempont. Egy városi becsapódás jelentősebb kockázatot jelent, mint egy óceánba történő. Mérsékelten magas súlyt kap.

Atmoszferikus hatások (A): a légköri fragmentáció (szétrobbanás) befolyásolhatja az ütközés hatásait, de önmagában nem döntő tényező. Közepes súlyt kap.

Másodlagos veszélyek (S): ha egy becsapódás globális klímaváltozást vagy szökőárt okozhat, az növeli a kockázatot. Magas súlyt kap, de kisebbet, mint a közvetlen ütközési tényezők.

Elhárítási nehézség (M): ha egy objektum eltérítése gyakorlatilag lehetetlen, az növeli a kockázatot. Közepes súlyt kap.

Ezeket figyelembe véve az alábbi súlyozott egyenletet határoztuk meg:

$$CIRAS_{index} = (0.7)E_{CIRAS} + (1.5)P_{CIRAS} + (-1.2)T_{CIRAS} + (0.8)L + (0.6)A + (1.0)S + (0.7)M$$

A fenti egyenlet súlyozási paraméterei fontossági sorrendben:

- $w_P = 1.5$ (becsapódási valószínűség): a legnagyobb súlyt kapja, mivel egy esemény kockázata elsősorban annak bekövetkezési valószínűségétől függ.
- $w_T = -1.2$ (hátralévő idő): minél kevesebb idő áll rendelkezésre, annál nagyobb a kockázat, ezért kap viszonylag nagy, de negatív súlyt.
- $w_S = 1.0$ (másodlagos veszélyek): olyan következmények esetén, mint a szökőár vagy globális klímaváltozás, a hatás jelentős lehet.
- $w_L = 0.8$ (becsapódási helyszín): ha egy objektum lakott területre csapódik be, az jelentősen növeli a kockázatot.
- $w_E = 0.7$ (becsapódási energia): közepes súlyt kap, mivel egy nagy energiájú esemény is kevésbé veszélyes, ha nagyon ritka vagy lakatlan területen történik.

- $w_M = 0.7$ (elhárítási nehézség): ha egy égitest eltérítése nagyon nehéz vagy lehetetlen, az növeli a kockázatot, ezért közepes súlyt kap.
- $w_A = 0.6$ (atmoszferikus hatások): közepes fontosságú tényező, mivel a légköri robbanás bizonyos esetekben csökkentheti, de akár növelheti is a károkat.

A fentiek szerint a CIRAS-index megfelelő egyensúlyt tart fenn a különböző tényezők között, és a lehető legreálisabb kockázatértékelést nyújtja.

Példa: a Tunguz-esemény (1908)

Tegyük fel, hogy egy évvel a becsapódás előtt ismertük volna a Tunguz-objektumot (1908. június 30-án történt a robbanás Szibéria fölött):

Becsült energia: $E_{obj} \approx 5Mt$ (a becslések 3–10 Mt közé esnek). Ekkor:

$$E_{CIRAS} = log_{10}(5) \approx 0.70\,.$$

Ha a felfedezés után egyértelműen látszott volna, hogy *a becsapódás valószínűsége* (egy év távlatában) közel 1, akkor tegyük fel $P_{impact} \approx 1$. Ha a háttér-valószínűség ugyanezen idő alatt $P_{bg} = 10^{-6}$ (példa), akkor:

$$P_{CIRAS} = log_{10}\left(\frac{1}{10^{-6}}\right) = log_{10}\left(10^{6}\right) = 6$$

A hátralévő idő: $\Delta t_{impact} = 1év$, ezért, $T_{CIRAS} = log_{10}(1) = 0$.

(A negatív súly miatt azonban, ha kevesebb idő áll rendelkezésre, például 9 hónap (0,75 év, akkor $\log_{10}0{,}75 = -0{,}125$ közel 0,15-dal növelné az index értékét ⇒ nagyobb kockázat.)

Helyszín: Szibéria ritkán lakott erdős területe, tehát $L = 3$ („ritkán lakott szárazföld, regionális katasztrófa").

Atmoszferikus hatás: magaslégköri robbanás, vagyis $A = 2$.

Másodlagos veszélyek: lokális tűz és erdőpusztítás (2000 km^2), de nem globális klímaváltozás. Legyen S = 2 („regionális" kiterjedés).

Elhárítási nehézség (1908-ban gyakorlatilag semmiféle eltérítési lehetőség sem állt rendelkezésre): $M = 4$ („lehetetlen").

Ekkor a CIRAS-index:

$$CIRAS_{index} = 0{,}7 * (0.70) + 1{,}5 * (6.0) + (-1{,}2) * (-0) + 0{,}8 * (3)$$

$$+ 0{,}6 * (2) + 1 * (2) + 0{,}7 * (4) \approx 18.$$

Ez a feltételezett szám (hiszen 1908-ban nem volt előzetes megfigyelés) mutatja, hogy ha csak 1 év volna hátra, és a becsapódás biztos, a CIRAS-index rendkívül magas lenne (főleg a P_{CIRAS} és az elháríthatatlanság miatt).

Összegzés

A CIRAS hét tényezője (energia, becsapódási valószínűség, hátralévő idő, helyszín, légköri jellemzők, másodlagos hatások, elhárítási nehézség) sokkal árnyaltabban mutatja be a földközeli objektumok jelentette veszélyt, mint a Torino- vagy Palermo-skála. Ugyanakkor a dimenziócsökkentő definíció formula révén egy számmal is összegezhető a kockázat, ha gyorsan kell rangsorolni különböző aszteroidák között.

A Tunguz-esemény (1908) példája megmutatja, hogyan lehetne a CIRAS keretein belül előzetesen felmérni egy regionális, légköri robbanás kockázatát, és miért lenne kiugróan magas az összesített kockázati index, ha a becsapódás gyakorlatilag elkerülhetetlen és időben közel lenne.

A CIRAS tehát a planetáris védelem új útja:

többtényezős elemzés + egydimenziós kockázati index = jobb döntéshozatal és kommunikáció.

Korábbi földi becsapódások és kockázatuk több skála alapján

A Föld történetében számos kisebb-nagyobb becsapódás történt. Híres, már lezajlott eseményeket vetünk össze a Torino-, Palermo- és CIRAS-skálán, fiktív (utólagos) előrejelzésként, mintha a becsapódás előtt ismertek lettek volna a skálák, és pontos pályaadataink lettek volna a becsapódó testekről.

Tunguz-esemény (1908)

Adatok (hipotetikus): $E_{obj} \approx 5Mt,\ P_{impact} \approx 1, \Delta t \approx 1év$.
Torino-skála: 8–9. (Egy ilyen biztos és jelentős energiafelszabadulással járó légköri robbanás regionális-kontinentális pusztítást okozhatott volna.)
Palermo-skála: $PS \approx +5{,}00$
CIRAS-skála: $(E, P, T, L, A, S, M) = (8;\ 9;\ 1;\ 4;\ 4;\ 4;\ 4)$
$CIRAS_{index} \approx 18$.

Cseljabinszki esemény (2013)

Adatok (hipotetikus): $E_{obj} \approx 0{,}5Mt,\ P_{impact} \approx 1, \Delta t \approx 0.0027év \approx 1\ nap$
Torino-skála: 4–5.
Palermo-skála: $PS \approx +7{,}27$
CIRAS-index: $(E, P, T, L, A, S, M) = (-0{,}3;\ 6{,}7;\ -2{,}6;\ 3;\ 2;\ 1;\ 4)$
$CIRAS_{index} \approx 20$

K-T-határ (körülbelül 66 millió évvel ezelőtt)

Adatok (hipotetikus): $E_{obj} \approx 10^8 Mt,\ P_{impact} = 1, \Delta t \approx 10év$
Torino-skála: 10.
Palermo-skála: $PS \gtrsim +9{,}00$
CIRAS-index: $(E, P, T, L, A, S, M) = (8;\ 9;\ 1;\ 4;\ 4;\ 4;\ 4)$
$CIRAS_{index} \approx 30$

Barringer-krátert okozó becsapódás (Arizona, körülbelül 50 ezer éve)

Adatok (hipotetikus): $E_{obj} \approx 10Mt,\ P_{impact} \approx 1, \Delta t \approx 1év$
Torino-skála: 8–9.
Palermo-skála: $PS \approx +5{,}00$
CIRAS-index: $(E, P, T, L, A, S, M) = (1;\ 5;\ 0;\ 3;\ 4;\ 1;\ 4)$
$CIRAS_{index} \approx 17$

Ch'ing-yang esemény (1490, Kína)[24]

Adatok (hipotetikus): $E_{obj} \approx 2Mt,\ P_{impact} \approx 1, \Delta t \approx 1év$
Torino skála: 8–9.
Palermo skála: $PS \approx +4{,}52$
CIRAS-index:
$CIRAS_{index} \approx 15$

Korábbi földi becsapódások kockázatbecslő indexének összehasonlítása több skála alapján

Az 1. táblázatban áttekinthetjük, összehasonlíthatjuk az öt esemény Torino-skála, Palermo-skála és CIRAS-index szerinti értékeit.

1. táblázat: Korábbi földi becsapódások kockázatbecslő indexeinek összehasonlítása

Esemény	**Torino-skála index (TS)**	**Palermo-skála index (PS)**	**CIRAS-index**
Tunguz (1908)	8–9	+5,00	18
Cseljabinszk (2013)	4–5	+7,27	20
K-T-határ (Chicxulub, 66 millió éve)	10	+9,00	30
Barringer-kráter (50 ezer éve)	8–9	+5,00	17
Ch'ing-yang (1490)	8–9	+4,52	15

Forrás: a szerzők szerkesztése

[24] Yau–Weissman–Yeomans 1994.

Összegzés

A fenti példák jól mutatják, hogy a Torino-skála (TS), a Palermo-skála (PS) és a CIRAS-skála egyaránt alkalmas a becsapódási veszély kifejezésére, bár más-más fókuszponttal és részletességgel.

A Torino-skála egyszerű, 0–10-es számot ad a széles nagyközönség számára.

A Palermo-skála (PS) mint folytonos logaritmikus index összeveti a kockázatot a természetes háttérgyakorisággal.

A CIRAS-skála egy komplexebb, többdimenziós értékelési rendszer, amely hét különböző faktort figyelembe véve ad végső besorolást.

Az új megfigyelések alapján esetlegesen megváltoztatott súlyok alkalmazásával a CIRAS-index még árnyaltabb képet adhat a kockázatok rangsorolására. Az eredmények egyértelműen mutatják, hogy a Tunguz-, Barringer-kráter-, illetve Chicxulub-becsapódás rendkívül magas besorolást kapott volna minden rendszerben.

Az Apophis aszteroida

Az első kockázatbecslések (2004-ben)

A (99942) Apophis aszteroidát 2004-ben fedezték fel és körülbelül 340 méter átmérőjűnek, több tízmillió tonnás égitestnek becsülték. A kezdeti megfigyelések bizonytalan pályaadatokat szolgáltattak, és a Földdel való ütközés esélyét akkor még néhány század százalékra tették. Bár ez elsőre igen csekélynek tűnhet, a Naprendszerben tapasztalható perturbációk és hosszú időskálák miatt a kezdeti Torino-skála besorolás átmenetileg elérte a 4-es szintet, ami már komolyabb figyelmet indokolt.

A Palermo-index (PS): $PS = log_{10}\left(\frac{P_{impact}/\Delta t}{f(E_{TNT})}\right)$

ahol P_{impact} az ütközés becsült valószínűsége

Δt az időtáv (például a következő néhány évtized),

$f(E_{TNT})$ a hasonló, vagy nagyobb energiájú becsapódások éves gyakorisága.

A korai számításokban P_{impact} (évtizedes léptékben) volt ugyan kicsi, ám mégis jelentős a háttérhez képest, így a Palermo-index rövid ideig pozitív értékre ugrott, jelezve, hogy a kockázat a természetes háttérnél magasabb.

A CIRAS modellje szerint az Apophis esetében a valószínűség (P) komponens volt a kezdeti időkben magasabb, míg a hátralévő idő (T) és az elhárítási nehézség (M) is közepesen magas értéket kaphatott volna. A pontosított pályaadatok azonban hamar csökkentették mind a valószínűséget, mind a CIRAS-indexet.

Az Apophis 2029. április 13-án, várhatóan mindössze 31 000 km távolságban halad el a Föld felszíne felett. Összehasonlítva a geostacionárius műholdakkal, amelyek körülbelül 36 000 km magasságban keringenek, ez még azoknál is alacsonyabb pályát jelent.

Skálaindexek biztos becsapódás esetén

Az Apophis becsült tömege több tízmillió tonna, ezért egy felszíni becsapódás esetén a felszabaduló energia (mintegy 5×10^4 Mt TNT) regionális vagy kontinentális szintű pusztítást okozhatna.

Torino-skála esetén egy biztos becsapódásnál a 8–10 tartományba került volna, attól függően, mennyire lakott területet érintene. A Palermo-index +5 fölé emelkedne, ha a becsapódás esélye 1–2 éven belül reális lenne.

CIRAS szempontjából az energia (E) $4{,}70$, a becsapódási valószínűség (P) jelenleg alacsony, de ha viszonylag nagy esélye lenne a becsapódásnak, a CIRAS-index 15 vagy annál nagyobb érték is lehetne (nagyban függene a becsapódás helyétől, a másodlagos veszélyektől).

Aktuális besorolás mindhárom skálán

A (99942) Apophis jelenlegi adatai alapján a 2029-es földközelség során a becsapódási valószínűség gyakorlatilag nulla. Bár az aszteroida becsapódási energiája óriási lenne, a kockázati besorolás minden skálán alacsony:

A Torino-skála értéke: TS=0

A Palermo index számítása:

$$PS = log_{10}\left(\frac{P_{impact}/\Delta t}{f(E_{TNT})}\right)$$

Ha $P_{impact} \approx 10^{-8}$ a következő 30 évre, és $f(E_{TNT}) \approx 10^{-8}$ /év, akkor:

$$PS = log_{10}(0.0333) \approx -1.48.$$

CIRAS-index

$$(E, P, T, L, A, S, M) = (4{,}7;\ 0;\ 4;\ 0;\ 0;\ 0;\ 2)$$

Végső CIRAS-index:

$$CIRAS_{index} = 0{,}7 * 4.70 + 0 + 1{,}2 * lg4 + 0 + 0 + 0 + 0{,}7 * 2 = 5{,}41$$

Konklúzió: a Torino-skála, a Palermo-skála és a CIRAS-rendszer egyaránt alacsony kockázatot mutat az Apophis aszteroidára.

Megjegyzés: ha a jövőben az Apophis pályája változna, a besorolások is módosulhatnak, ezért a folyamatos megfigyelés fontos.

Összefoglalás

A földközeli objektumokkal kapcsolatos kutatások és a bolygóvédelmi stratégiák kidolgozása ma már kulcsfontosságú asztronómiai és technológiai kihívás. A Torino-skála 0–10 közötti, közérthető besorolást ad, míg a Palermo-skála folytonos logaritmikus indexével összehasonlítható a kockázat és a természetes háttérbecsapódások gyakorisága. Az újabb CIRAS-rendszer pedig többtényezős megközelítéssel képes számszerűsíteni a veszélyt, és szükség esetén akár egyetlen indexbe sűríteni.

A (99942) Apophis kezdeti besorolása rávilágított, hogy a pályaadatok bizonytalansága milyen nagy hatással lehet egy égitestről alkotott kockázat megítélésekor. Bár az Apophis esetében az ütközés jelenlegi becslése 2029-ben gyakorlatilag nulla, jövőbeli perturbációk és földközeli átvonulások miatt továbbra is kiemelt megfigyelési célpont marad. A 2029-es rendkívüli közelség egyfelől kivételes tudományos lehetőséget biztosít (például radaros felszíntérképezés, gravitációs mérések), másfelől ráirányítja a figyelmet a planetáris védelem szükségességére és a pályapontosítás fontosságára.

Az Apophis esete jól példázza, hogyan változhat a Torino-, Palermo- és CIRAS-skála szerinti értékelés a megfigyelések szaporodásával és a pályabecslések pontosításával.

Felhasznált irodalom

Apophis ESA [é. n.]. *The European Space Agency.* Online: www.esa.int/Space_Safety/Planetary_Defence/Apophis

Artemieva, Natalia – Shuvalov, Valery (2016): From Tunguska to Chelyabinsk via Jupiter. *Annual Review of Earth and Planetary Sciences,* 44, 37–56. Online: https://doi.org/10.1146/annurev-earth-060115-012218

Binzel, Richard P. (2000): The Torino Impact Hazard Scale. *Planetary and Space Science,* 48(4), 297–303. Online: https://doi.org/10.1016/S0032-0633(00)00006-4

Borovička, Jiří (2016): The Chelyabinsk Event. *Proceedings of the International Astronomical Union,* 11(A29A), 247–252. Online: https://doi.org/10.1017/S1743921316002982

Chesley, Steven. R. et al. (2002): Quantifying the Risk Posed by Potential Earth Impacts. *Icarus,* 159(2), 423–432. Online: https://doi.org/10.1006/icar.2002.6910

Érces Gergő – Vass Gyula (2018): Veszélyes ipari üzemek tűzvédelme – ipari üzemek fenntartható tűzbiztonságának fejlesztési lehetőségei a komplex tűzvédelem tekintetében. *Műszaki Katonai Közlöny,* 28(4), 2–22. Online: https://mkk.uni-nke.hu/document/mkk-uni-nke-hu/2018_4_01_Erces%20G%20-%20Vass%20Gy_MKK_cikk.pdf

Keresztúri Ákos – Sárneczky Krisztián (2023): *Célpont a Föld? Kisbolygók a láthatáron.* Budapest: Magyar Csillagászati Egyesület.

Keresztúri Ákos – Tóth Imre (2008): Kisbolygó vagy üstökös? A Tunguz-esemény. *Meteor,* 38(6), 3–9. Online: https://epa.oszk.hu/03000/03054/00358/pdf/EPA03054_meteor_2008_06.pdf

Kring, David A. (2017): *Guidebook to the Geology of Barringer Meteorite Crater, Arizona (a.k.a. Meteor Crater).* [H. n.]: Lunar and Planetary Institute.

Morrison, David (2018): Tunguska Workshop: Applying Modern Tools to Understand the 1908 Tunguska Impact. *NASA/Technical Memorandum* (NASA/TM—220174). Online: https://ntrs.nasa.gov/api/citations/20190002302/downloads/20190002302.pdf

Pallagi András (2023): *Kritikus infrastuktúrák védelmének vizsgálata.* PhD-disszertáció. Budapest: Óbudai Egyetem Biztonságtudományi Doktori Iskola. Online: https://bdi.uni-obuda.hu/wp-content/uploads/2024/06/Doktori-PhD-ertekezes-Pallagi-Andras.pdf

Pope, Kevin O. et al. (1997): Energy, Volatile Production, and Climatic Effects of the Chicxulub Cretaceous/Tertiary Impact. *Journal of Geophysical Research,* 102(E9), 21645–21664. Online: https://doi.org/10.1029/97JE01743

Reddy, Vishnu et al. (2022): Apophis Planetary Defense Campaign. *The Planetary Science Journal,* 3(5), 1–16. Online: https://doi.org/10.3847/PSJ/ac66eb

Schmieder, Martin – Kring, David A. (2020): Earth's Impact Events Through Geologic Time: A List of Recommended Ages for Terrestrial Impact Structures and Deposits. *Astrobiology,* 20(1), 91–141. Online: https://doi.org/10.1089/ast.2019.2085

Yau, Kevin – Weissman, Paul – Yeomans, Donald (1994): Meteorite Falls in China and Some Related Human Casualty Events. *Meteoritics,* 29(6), 864–871. Online: https://adsabs.harvard.edu/full/1994Metic..29..864Y

HADMÉRNÖK
KÖRNYEZETBIZTONSÁG
20. évfolyam (2025) 4. szám 125–147.
DOI: 10.32567/hm.2025.4.8

Kirovné Rácz Réka,[1] Scholtz Emánuel[2]

A mesterséges intelligencia és gépi tanulás algoritmusainak alkalmazása a hidrológiai katasztrófák elleni védekezésben

Application of Artificial Intelligence and Machine Learning Algorithms in Protection Against Hydrological Disasters

Absztrakt

Az elmúlt évtizedekben jelentősen megnőtt a katasztrófák száma, mind a természeti, mind az ember által előidézett katasztrófáké, hazai és nemzetközi viszonylatban is, ezért az előrejelző rendszerek fontossága felértékelődött. Az informatika és a számítástechnika, ezen belül a mesterséges intelligencia, gépi tanulás ugrásszerű fejlődésen ment keresztül az elmúlt időszakban, így lehetővé téve, relatív kevés erőforrással is, nagyon pontos, magas általánosító képességgel rendelkező prediktív modellek megalkotását. A klímaváltozás miatt az időjárás egyre kiszámíthatatlanabbá válik, egyre gyakoribbak a szélsőséges időjárási jelenségek. Ez komoly nehézségek elé állítja az országokat, beleértve Magyarországot is. A hidrológiai katasztrófák hazánkban, a vízrajzi és a domborzati adottságokból adódóan, mindig jellemző katasztrófakockázatot jelentettek. Megemlíthetjük az elmúlt évtizedekből például a 2006-os dunai és tiszai árvizet, a 2013-as dunai árvizet, a 2024-es nagy dunai árhullámot, a 2025-ös áradást a Kaposon, a 2013-as zempléni, a 2020-as dél-zalai villámárvizet, a 2012-es, a 2022-es rendkívüli aszályokat, a 2021-es csapadékhiányt, a 2025-ös aszályos

[1] Egyetemi adjunktus, Nemzeti Közszolgálati Egyetem Rendészettudományi Kar Katasztrófavédelmi Intézet Katasztrófavédelmi Műveleti Tanszék, e-mail: kirovne.racz.reka@uni-nke.hu
[2] Doktori hallgató, Nemzeti Közszolgálati Egyetem Rendészettudományi Doktori Iskola, e-mail: scholtz.emanuel99@gmail.com

időjárást, a 2013-as hókatasztrófát. 2024-ben az előrejelző rendszereknek sikerült időben érzékelni a veszélyt, a rendkívüli összefogásnak és a szakemberek fáradhatatlan munkájának köszönhetően sikerült hatékonyan védekezni az árvíz ellen. Tehát fontos az időbeni cselekvés, új, még pontosabb előrejelző, riasztó rendszerek és védelmi mechanizmusok kialakítása, a lakosság felkészítése. Ebben a cikkben összefoglaljuk a hazai és a nemzetközi kutatásokban használt algoritmusokat és a hazánkban működő előrejelző rendszereket.

Kulcsszavak: mesterséges intelligencia, gépi tanulás, katasztrófavédelem, árvíz, árvízvédelem, településelöntés, villámárvíz, belvíz, aszály, informatika, neurális hálók, support vector machine, decision tree, random forest, fuzzy logic

Abstract

In the last decades, the number of disasters has increased significantly, both natural and man-made, at the national and international level. As a result, the importance of forecasting systems has greatly increased. Information technology and computer science, including artificial intelligence and machine learning, have undergone immense development in recent years, hence making it possible to create predictive models with very high accuracy and great generalisation capability, even having relatively few resources available. Due to climate change, the weather is becoming increasingly unpredictable, with extreme weather becoming more frequent. This is a serious challenge for countries, including Hungary. Unfortunately, hydrological disasters have become quite regular in our country. For example, we can mention the Danube and Tisza floods of 2006, the Danube flood of 2013, the major flood hazard situation on the Danube in 2024, the 2025 flood on the Kapos River, the 2013 Zemplén flash flood, the 2020 South Zala flash flood, the very severe droughts of 2012 and 2022, the moderately severe drought of 2021, the dry weather conditions of 2025, and the snow disaster of 2013. In 2024, forecasting systems successfully detected the danger in time, and thanks to extraordinary cooperation and the tireless work of experts, the country managed to defend effectively against the flood. Consequently, taking action in time is crucial, along with the development of new, even more accurate forecasting and warning systems, as well as defence mechanisms and population preparedness. In this article, I present the algorithms used in domestic and international research, as well as the forecasting systems operating in Hungary.

Keywords: artificial intelligence, machine learning, disaster management, flood, flood protection, urban flooding, flash flood, inland flooding, drought, information technology, neural networks, support vector machine, decision tree, random forest, fuzzy logic

Bevezetés

A mesterséges intelligencia (MI) már nem csupán az adatok alapján tanuló és fejlődő algoritmusok összessége. Egyre inkább képes az emberi megértés, tanulás és problémamegoldás szimulálására, valamint az emberi képességek bizonyos területeinek

leképezésére és hatékonyságának javítására.[3] Ezek a rendszerek meg tudják tanulni az adatokban rejlő mintázatokat, és olyan összefüggéseket is felismernek, amelyeket emberi szemmel csak nagyon nehezen vagy egyáltalán nem lehet észrevenni. Az ilyen rendszereket három kategóriába sorolhatjuk. Az első kategóriába a sekély mesterséges intelligenciával *(artificial narrow intelligence)* bíró rendszerek tartoznak, ezek létrehozása és működtetése olcsó és egy adott feladat témakörben remekül teljesítenek. A második kategóriába az általános célú mesterségesintelligencia-rendszerek *(artificial general intelligence)* tartoznak, megalkotásuk és működtetésük már jóval költségesebb, ilyen rendszereket általában a nagy cégek fejlesztenek. A harmadik kategória a mesterséges szuperintelligencia *(artificial superintelligence),* amely jelenleg még nem létezik, csupán elképzelés, és minden területen felülmúlná az emberi intelligenciát. A mesterségesintelligencia-algoritmusok nagy hátránya, hogy nehéz átlátni őket, sok esetben fekete dobozra hasonlítanak, ezért hibás működés esetén nehéz megtalálni a hiba konkrét okát. A mesterségesintelligencia-algoritmusok pontossága nem mindig tökéletes, ezért kritikus helyzetekben, ahol mások élete múlhat a helyes működésen, különös figyelmet igényelnek. Ilyenkor fontos a megfelelő kockázatkezelés alkalmazása, és a többforrású döntéstámogatás, hogy a rendszer megbízható legyen.[4]

Az árvíz-, belvíz-, villámárvíz- és aszály-előrejelző rendszerek nagy része jelenleg fizikai, hidrológiai modelleket használ, de az elmúlt huszonöt évben több mint 1000 cikk íródott gépi tanulás és mesterséges intelligencia által támogatott árvíz-, belvíz- és villámárvíz-megelőzésről, ezen katasztrófák okozta kár minimalizálásáról, esetleges helyreállítási munkálatokról.[5] Több mint 190 tudományos cikk készült gépi tanulás vagy mesterséges intelligencia által támogatott aszály-előrejelzésről, kárminimalizálásról. A kiadott cikkek mennyisége alapján nyilvánvaló, hogy ez jelenleg fontos kutatási terület.[6] A kutatások jelentős része Kínában, Indiában, Ausztráliában, Iránban, az Egyesült Királyságban és az Amerikai Egyesült Államokban történt. 2010-ig évente csak korlátozott számban jelentek meg publikációk. 2010 és 2015 között jelentősen megnőtt a kiadott cikkek száma. 2015 után a gépi tanulás és mesterséges intelligencia területén történt kutatások és fejlesztések felgyorsultak, ez részben a nagyobb teljesítményű, megfizethető videókártyák elterjedésének köszönhető, így évente már kifejezetten nagyszámú, akár több száz, tanulmány látott napvilágot.[7]

Az AGH University of Science and Technology kutatói, Julia Buszta, Katarzyna Wójcik, Krystian Kozioł és Kamil Maciuk, valamint a Federal University of Paraíba kutatója, Celso Augusto Guimarães Santos az elmúlt 60 év természeti katasztrófáinak előfordulási gyakoriságát térképezték fel, és előrejelzéseket készítettek a következő évekre. Ők is megállapították, hogy mind a szárazságok, földrengések, extrém hőmérsékletek, mind a földcsuszamlások, viharok, árvizek gyakoribbak. Szerintük Európa helyzete jobb Amerika vagy Kína helyzeténél, mivel Európában ritkábbak a természeti katasztrófák. Julia Buszta és társai szerint az elkövetkező időszakban a természeti katasztrófák előfordulásának

[3] *Magyarország Mesterséges Intelligencia Stratégiája 2025–2030* 2025.
[4] Ayyadevara 2018.
[5] OpenAlex lekérdezés.
[6] Buszta et al. 2023.
[7] Tan et al. 2021; Mosavi–Ozturk–Chau 2018; Lu–Huang–Wu 2023.

gyakorisága növekedni fog.[8] Ezért kulcsfontosságú, hogy a lehető legtöbb ember részt vegyen a katasztrófavédelmi feladatokban: legyen szó a katasztrófa megelőzéséről, felkészülésről, beavatkozásról, a károk kialakulása kockázatának minimalizálásáról, helyreállítási, újjáépítési munkálatokról. Kiemelték továbbá, hogy nagyon fontos, hogy ezeket a feladatokat minél többen saját felelősségüknek, kötelességüknek érezzék. Lényeges, hogy az előrejelző rendszerek által adott információkat gyorsan, hatékonyan, időben, pánikkeltés nélkül a lehető legtöbb emberhez könnyen el lehessen juttatni.

Kutatási módszerek

A tanulmány módszertanának alapjául az irodalomkutatás szolgált, amely arra irányult, hogy milyen lehetőségeket kínál a mesterséges intelligencia és gépi tanulás a hidrológiai katasztrófák előrejelzésének fejlesztésében. Ennek érdekében figyelmünket a hazai és nemzetközi tudományos eredmények tanulmányozására, összehasonlítására és a hazai rendszerek bemutatására irányítottuk. A témánk szempontjából jelentős szakirodalom feltárásához több, egymást kiegészítő adatbázist használtunk, köztük az MTMT-t, a Google Scholar-t, a Scopus és Web of Science rendszereket, az IEEE Xplore és SpringerLink felületeket, a ScienceDirectet, ResearchGate-et, az OpenAlex bibliográfiai rendszerét, valamint a hazai szakmai folyóiratokat, például a *Hidrológiai Közlöny*t, a *Földrajzi Közlemények*et, a HydroInform kiadványait és a Nemzeti Közszolgálati Egyetem weboldalán elérhető folyóiratokat. Kereséseinket magyar és angol nyelven végeztük.

A kereső kulcsszavak összeállításakor szem előtt tartottuk mind a hidrológiai katasztrófák sajátos témaköreit, mind a mesterséges intelligencia területét. A keresések során a következő főbb kulcsszavakat használtuk a hidrológiára vonatkozóan: árvíz-előrejelzés *(flood prediction),* árvízmodellezés *(flood modelling),* villámárvíz-előrejelzés *(flash flood prediction),* településelöntés *(urban flood modelling),* belvíz-előrejelzés *(inland flood forecasting),* vízhozam-előrejelzés *(streamflow forecasting),* árhullámlefolyás *(hydrograph forecasting),* csapadék-előrejelzés *(precipitation prediction),* aszály-előrejelzés *(drought prediction),* aszályindex *(drought index),* hidrológiai kockázatértékelés *(hydrological risk assessment).* A keresési tartományt nem korlátoztuk kizárólag a hidrológiai katasztrófák előrejelzésére, kiterjesztettük a fókuszt a mesterséges intelligencia tágabb katasztrófavédelmi szerepének vizsgálatára is, olyan kulcsszavakkal, mint mesterséges intelligencia a katasztrófavédelemben *(artificial intelligence in disaster management),* gépi tanulás a katasztrófavédelemben *(machine learning in disaster management),* kockázatbecslés MI-vel *(AI-based risk assessment),* korai előrejelző rendszerek *(early warning systems),* veszélyazonosítás *(hazard identification),* extrém események előrejelzése *(extreme event prediction).* A mesterséges intelligencia és gépi tanulás módszertani oldalának tanulmányozásához technikai kulcsszavakat is alkalmaztunk: gépi tanulás *(machine learning),* mélytanulás *(deep learning),* neurális háló *(neural network),* konvolúciós neurális háló (*convolutional neural network,* CNN), rekurrens neurális háló (*recurrent neural network,* RNN), hosszú-rövid távú

[8] Buszta et al. 2023.

memóriaháló (*long short-term memory,* LSTM), döntési fa *(decision tree),* véletlen erdő *(random forest), gradient boosting,* extrém gradiensnövelés (XGBoost), kategorikus boosting (CatBoost), támasztóvektor-gép (*support vector machine,* SVM), többváltozós regresszió (*multiple linear regression,* MLR), autoregresszív és idősormodellek (AR, ARIMA), fuzzy logika *(fuzzy logic),* genetikus algoritmus (*genetic algorithm,* GA), részecskeraj-optimalizáció (*particle swarm optimisation,* PSO). Munkánkhoz átfogó szakirodalmi áttekintéseket *(literature review, systematic review)* is használtunk, hogy tágabb összefüggésben szemlélhessük a kutatási irányokat és a módszertani változásokat. Mivel nagy figyelmet szenteltünk a magyar nyelvű szakirodalom kutatásának, az MTMT-ben sok keresést végeztünk magyar kulcsszavakkal. Így átláthattuk a hazai kutatási irányokat, modellezési törekvéseket és intézményi gyakorlatokat, illetve a magyar eredményeket a nemzetközi kontextusban értékelhettük.

A kiválasztott publikációk többsége a 2016–2025 közötti időszakból származik, amikor az MI rohamléptekkel fejlődött. Főleg olyan kutatásokat kerestünk, amelyek a vízügyi katasztrófák – árvizek, belvizek, hirtelen áradások, települések elöntése, aszály – előrejelzésével vagy a kockázat felmérésével foglalkoznak. Ezek a tanulmányok MI-algoritmusokat alkalmaznak, vagy ötvözik a hagyományos vízrajzi modelleket és az MI-t. Azokra a publikációkra építettünk, amelyek tudományosan megalapozottak, részleteikben kidolgozottak és logikusak, átláthatóan ismertetik az adatokat és a módszereket, leírják a kutatás menetét, és konkrét, számokkal alátámasztott eredményeket mutatnak be (például RMSE, MAE, R^2, AUC, NSE). Figyelmen kívül hagytuk azokat a tanulmányokat, amelyek nem felelnek meg a tudományos követelményeknek vagy hiányos a módszertani leírásuk.

A jelenlegi predikciós rendszerek hazánkban

Magyarországon a szélsőséges időjárási események mellett a leggyakrabban előforduló természeti katasztrófák az árvizek, villámárvizek és aszályok, ezért ezek előrejelzése rendkívül fontos, mivel így könnyebben megtehetők a szükséges felkészülési intézkedések.

Az OVF (Országos Vízügyi Főigazgatóság) és az OVSZ (Országos Vízjelző Szolgálat) működtet árvíz- és belvíz-előrejelző rendszereket. Előrejelzési információikat nyíltan és ingyenesen elérhetővé teszik az interneten mindenki számára.[9]

A HungaroMet is működtet országos veszélyjelző rendszert, amely kiterjed nagy mennyiségű esőre, zivatarokra, extrém hidegre és melegre, hófúvásra, erős szélre, tartós ködre. Három előrejelzési fokozat van: sárga, narancssárga, piros. A sárga potenciális veszélyt jelent. A narancssárga komolyabb veszélyre figyelmeztet, amikor már veszélyt jelent az emberek testi épségére és anyagi károk is előfordulhatnak, a piros figyelmeztetést komoly veszély esetén, ritkán adják ki, amikor már emberek élete is veszélyben lehet, és nagyon komoly káresemények is előfordulhatnak.[10]

[9] Lásd az Országos Vízügyi Főigazgatóság weblapját: www.vizugy.hu/
[10] HungaroMet vészjelző rendszer.

Az EFAS (European Flood Awareness System) egy árvíz-előrejelző rendszer, amely jelenleg használatban van Magyarországon is, nagyrészt hidrológiai modellekre támaszkodik, a CEMS (Copernicus Emergency Management Service) keretén belül működik, és akár tíznapos hidrológiai predikcióra is képes. Célja a felkészülés elősegítése, és főleg határokon átívelő folyókra koncentrál.

Az Országos Vízügyi Főigazgatóság (OVF) működtet aszálymonitoring-rendszert, amely nyíltan és ingyenesen elérhető mindenki számára. Mérőállomás-hálózat segítségével gyűjtik a csapadék-, páratartalom-, talajnedvesség-, talajhőmérséklet-adatokat és a Global Forecast System (GFS), a European Centre for Medium-Range Weather Forecasts (ECMWF) modellek segítségével előrejelzéseket végeznek.[11]

Az Alsó-Tisza-vidéki Vízügyi Igazgatóság (ATIVIZIG) is foglalkozik árvíz-előrejelzéssel, kifejlesztettek egy LSTM-modellt, amely hétnapos predikciókra képes. A Pálfai-féle aszályindexet (PAI) a 80-as években fejlesztették ki, egyszerű mutató, amely a csapadék-hőmérséklet arányon alapul. Később ennek a továbbfejlesztéséből jött létre a Pálfai Drought Index (PaDI). A Hungarian Drought Indexet (HDI) 2015–2016-ban fejlesztették ki, amely napi időléptékű, kevés bemenetet igénylő, moduláris index, amely objektíven írja le a vízhiány mértékét, figyelembe véve a talajnedvességet és a meteorológiai viszonyokat. Az index kiszámítása három szinten történik, alapul véve, hogy van-e talajnedvesség-adat. Az első szint, a meteorológiai alapindex (HDI_0), nem évszakfüggő, a napi középhőmérsékletet és csapadékmennyiséget használjuk fel, víztartalékot becsülünk a meglévő időszak adataiból. Átlagos időjárás esetén az érték 1 körül lesz, csapadékosabb, hűvösebb időjárás esetén 1 alatt, aszály esetén pedig 1 fölött. Második szint a párolgási hiányt és stressztényezőt is figyelembe vevő index (HDI_S), amelynek az alapparaméterei megegyeznek a HDI_0-val, de a párolgási veszteség teljes mértékben realizálódik, 1,333 alatt nincs vízhiány, 1,333 és 1,5 között enyhe vízhiány, 1,5 és 2,5 között közepes vízhiány, 2 és 3 között erős vízhiány, 3 felett rendkívüli vízhiány van. A harmadik szint a talajnedvességgel súlyozott változat.[12]

A HungaroMet is foglalkozik aszálymonitoringgal, és ezek az információk az Agrometeorológiai menüpontban az Aszály információkra kattintva érhetők el.[13] Az intézet a standardizált csapadékindexet (*standardised precipitation index,* SPI) használja, valamint több különböző műholdas szárazság- és vegetációs indexet, mint például a normalizált differenciált vegetációs indexet (*normalised difference vegetation index,* NDVI), a normalizált differenciált aszályindexet (*normalised difference drought index,* NDDI), a kibővített vegetációs indexet (*enhanced vegetation index,* EVI) és a vegetációs kondícióindexet (*vegetation condition index,* VCI).[14]

Az Alsó-Tisza-vidéki Vízügyi Igazgatóság szintén részt vesz az aszálymonitorozásban, mérőállomásokat üzemeltetnek, fontos szerepet játszottak a HDI_S index kifejlesztésében.[15]

Az elmúlt 20 évben Magyarországon fejlesztések voltak árvízvédelem terén: az árvízvédelmi töltésrendszereket korszerűsítették és kibővítették, és nagy hangsúlyt

[11] Lásd: https://aszalymonitoring.vizugy.hu/ és https://aszalymonitoring.vizugy.hu/index.php?view=info
[12] Fiala et al. 2018; és https://aszalymonitoring.vizugy.hu/index.php?view=info
[13] Lásd: www.met.hu/idojaras/agrometeorologia/aszalyinfo/index.php
[14] Kircsi et al. 2018.
[15] Kozák et al. 2022.

fektettek a karbantartásukra, új védművek és szabályozó műtárgyak épültek, fejlesztették a monitorozó és előrejelző rendszereket. Az elmúlt öt évben figyelmet kapott a modern, korszerű, innovatív vízgazdálkodás.[16]

2025-ben rengeteg fontos intézkedés történt az aszályvédelem területén: létrejött az Aszályvédelmi Operatív Törzs, elindult a Vizet a tájba program, amelynek célja a korábban levezetett, feleslegesnek vélt víz helyben tartása. A gazdák online csatlakozhatnak az önkéntes elárasztási kezdeményezéshez.[17]

Dr. Liptay Zoltán Árpád a Nemzeti Közszolgálati Egyetem Víztudományi Karának kutatója körszimmetrikus és elliptikus bázisfüggvény-hálózatokat alkalmazott 1–6 napos vízszint-előrejelzésre a Dunán, a Tiszán és a Rábán. (A körszimmetrikus és elliptikus bázisfüggvény-hálózatok olyan előrecsatolt neurális hálózatok, amelyek egyetlen rejtett réteggel rendelkeznek, aktivációs függvényük pedig a bázisfüggvény, mint például a Gauss, és nem a ReLU vagy a tanh.) Munkája során felhasználta az OVSZ OPADAT 2010 és 2023 közötti idősoros vízállásadatait. A hálózatokban különféle bázisfüggvényeket, távolságmetrikákat és optimalizálókat hasonlított össze. A Matérn kovariancia, multikvadratikus és multikvadratikus-biharmonikus függvények többnyire jobb RMSE-t adtak a Gaussnál, míg a csapadék hozzáadása csak csekély javulást hozott. A kutató az előrejelzések pontosságát *root mean square error* segítségével értékelte, és összehasonlította klasszikus OVSZ-modellekkel és mesterségesintelligencia-modellekkel is. A Dunán és a Rábán a klasszikus modellek voltak pontosabbak, míg a Tiszán az elliptikus bázisfüggvény-hálózat ért el jobb eredményt.[18]

Blanka-Végi Viktória, Tobak Zalán, Kajári Balázs, Sipos György, Barta Károly, Kovács Ferenc, akik a Szegedi Tudományegyetem Geoinformatikai, Természet- és Környezetföldrajzi Tanszék kutatói és Boudewijn van Leeuwen, aki a Víztudományi és Vízbiztonsági Nemzeti Laboratórium munkatársa a Dél-Alföldön *deep neural network* (DNN), *multi linear regression* (MLR), *eXtreem gradient boosting* (XGBoost) és *support vector machine regression* (SVR) segítségével, Sentinel-1 radarinformációk és Sentinel-2 multispektrális képek, az Országos Vízügyi Főigazgatóság Operatív Vízhiány Értékelő és Előrejelző Monitoring Rendszerének 40 állomásáról származó adatok, és a HU-SoilHydroGrids rendszerből származó adatok felhasználásával talajnedvességet próbáltak előrejelezni. Felhasználtak távérzékelt és terepi talajnedvesség-adatokat, meteorológiai adatokat is, mint például párolgás, napi csapadékmennyiség és hőmérséklet, de még a talaj maximális vízkapacitás-adatait és szabadföldi vízkapacitás-adatokat is. A legjobb eredményt az XGBoost érte el 0,92-es korrelációs együtthatóval. A belvízvizsgálatot Mezőtúrtól északkeletre végezték egy megközelítőleg 1600 km²-es területen a Sentinel-1 és Sentinel-2 adatokból, valamint meteorológiai adatok alapján állítottak elő elöntési térképeket, ahol a belvízborítottság feltérképezésére a *convolutional neural network* (CNN) adta a legjobb eredményt.[19]

Szabó János Adolf, a HYDROinformatikai Kutató, Rendszerfejlesztő és Tanácsadó Bt. kutatója, szakértője, Lucza Zoltán és Szabó-Márku Melinda, a Felső-Tisza-vidéki Vízügyi Igazgatóság szakértői munkájuk során bemutatták a numerikus meteorológiai

[16] *Magyarország 2021. évi árvízkockázat-kezelési terve* 2022; Hegedűs 2020.
[17] Vizet a tájba. Lásd: www.ovf.hu/jobboldali-sav-tartalmai/vizetatajba/vizet-a-tajba
[18] Liptay 2024.
[19] Blanka-Végi et al. 2024.

modellek hibalehetőségeit és korlátait, szerintük ezeket lehetne javítani mesterséges intelligenciával. A cikk nem egy, már meglévő, konkrét rendszert mutat be, hanem az előrejelzés pontosításának lehetőségeit ismerteti. A numerikus modell pontosságának növeléséhez szükség van SAL-ellenőrzésre, amely három tényező alapján vizsgálja az előre jelzett csapadékmezők hibáit: amplitúdó, lokáció és struktúra. A kutatók úgy gondolják, hogy a numerikus modellek előrejelzéseit óránként össze kellene vetni a radarok és földi mérőállomások által jelzett értékekkel, és a gépi tanulási algoritmust az így kapott SAL-értékekkel kellene tanítani. Az algoritmus képes lenne felismerni a numerikus előrejelzések hibamintázatait, és geometrikus transzformációk segítségével tudná korrigálni ezeket.[20]

Mesterséges intelligencia és gépi tanulás az árvízvédelemben nemzetközi szinten

Az árvíz rendszeresen előforduló természeti katasztrófa, a világ sok országát érinti, emberéleteket követelhet és felbecsülhetetlen károkat hagy maga után.

Ling Tan a Nanjing University of Information Science and Technology kutatója, Ji Guo a Nanjing University of Information Science and Technology kutatója, Selvarajah Mohanarajah a University of North Carolina at Pembroke kutatója és professzora, Kun Zhou a Nanjing University of Information Science & Technology kutatója 2020-ban készítettek átfogó tanulmányt, amelyben bemutatják az eddig világszerte elért eredményeket a mesterséges intelligencia és gépi tanulás katasztrófavédelmi felhasználásában. Szerintük a mesterséges intelligenciát és gépi tanulást főleg előrejelzésre használják jelenleg, de folynak kutatások olyan rendszerek előállítására, amelyek a védekezést és a kárelhárítást segítenék. A meglévő megoldásokat két csoportba oszthatjuk: egyszerű megoldások, ezek főleg egy algoritmust használnak, illetve hibrid megoldások, amelyek több módszert, algoritmust használnak a jobb eredmények eléréséhez. Árvíz-előrejelzéshez használatosak az *artificial neural network* (ANN), *support vector machine* (SVM), *decision tree* (DT), *random forest* (RF) algoritmusok. Szintén léteznek más statisztikán alapuló összetett, haladó, modern algoritmusok, mint: *fuzzy logic* (fuzzy logika), *genetic algorithm* (genetikus algoritmus), *particle swarm optimisation* (raj alapú optimalizáció).[21]

A mesterséges neurális hálózat (*artificial neural network,* ANN) olyan népszerű digitális rendszer, amely a kognitív folyamatokat utánozza abban, hogy komplex mintázatokat modellez, előrejelzéseket hoz létre, illetve megfelelő reakciókat ad külső ingerekre. Fő egysége a neuron, amelynek van bemenete, kimenete, nem lineáris aktivációs függvénye, és a neuron bemeneteihez súlyok tartoznak. A mesterséges neurális hálók három típusú réteggel rendelkeznek: bemeneti, kimeneti és rejtett. Általában sok rejtett réteg van. A tanítás során *backpropagation,* vagyis hiba-visszaterjesztés segítségével próbáljuk elérni, hogy a súlyok a megfelelő értékeket vegyék

[20] Szabó – Lucza – Szabó-Márku 2024.
[21] Tan et al. 2021.

fel, ezáltal a háló általánosító képessége a lehető legnagyobb legyen, ami pontosabb predikciókat tesz lehetővé.[22]

A *support vector machine* (SVM), vagyis támasztóvektorgép, egy könnyen használható, felügyelt, relatív egyszerű gépi tanulási modell, amely rugalmasan alkalmazható akár regressziós, akár klasszifikációs feladatokra is. Az algoritmus célja olyan hipersík megtalálása, amely maximalizálja a margót az osztályok között, a legjobban elkülöníti az osztályokat. Abban az esetben, ha a meglévő adatok nem lineárisan szeparálhatóak, akkor a kernel trükk segítségével olyan transzformációt hajtunk végre, amely egy magasabb dimenzióba képezi le az adatokat, ahol már könnyen szétválaszthatóvá válnak.[23]

A döntési fa (*decision tree,* DT) egy felügyelt gépi tanulási algoritmus, amelyet osztályozásra és regresszióra használnak. A cél egy olyan modell létrehozása, amely megjósolja egy célváltozó értékét az adatjellemzőkből kikövetkeztetett egyszerű döntési szabályok megtanulásával. Jól használható regressziós és klasszifikációs feladatokhoz is, kezeli a folytonos és a kategorikus adatokat is. Hátránya, hogy gyakran túlillesztés *(overfitting)* léphet fel, bár ez a jelenség elkerülhető a fa mélységének korlátozásával vagy regularizáció alkalmazásával.[24]

A véletlen erdő *(random forest),* rövidítése RF, közepesen összetett, megbízható, rugalmas klasszifikációs és regressziós modell. Több, egymástól független döntési fát hoz létre, és úgy jut el a végeredményhez, hogy regresszió esetén ezek eredményeit átlagolja, vagy, klasszifikáció esetén, kiválasztja a legtöbb szavazatot kapott eredményt. Változatos adatok esetében is stabil teljesítménnyel rendelkezik, jóval kevésbé hajlamos a túlillesztésre mint a döntési fa.[25]

A *fuzzy logic,* vagyis fuzzy logika a klasszikus igaz-hamis, (1)-(0)-án alapuló logikai rendszer továbbfejlesztése, kibővítése, nem tekinthető gépi tanulási modellnek, ennek ellenére valamilyen szinten az emberi gondolkodásmódot utánozza. Míg a klasszikus logikában csak 0 vagy 1 értéket vehetünk fel, a fuzzy logika lehetővé teszi, hogy a 0 és 1 között lévő tört számokat is felvegyük.[26]

A *genetic algorithm* (GA), vagyis genetikus algoritmus a természetből inspirálódott, modern, heurisztikus optimalizációs eljárás. Központi eleme a „gén" vagy „kromoszóma", amelyeken a következő műveleteket: szelekciót, keresztezést és mutációt addig végezzük, amíg a leállási feltétel nem teljesül. Jól teljesít olyan feladatoknál, ahol a keresési tér extrémen nagy, igaz, hogy nem garantált a legjobb megoldás megtalálása, mivel hajlamos beragadni helyi minimumpontba, de gyakran képes rövid időn belül az optimálishoz közeli megoldást találni.[27]

A *particle swarm optimisation,* azaz raj alapú optimalizáció egy természetből, madárrajok repüléséből, halrajok úszásából inspirálódott, haladó, evolúciós, kevés hiperparaméterrel rendelkező heurisztikus algoritmus, nem gépi tanulási modell, amely jól használható folytonos optimalizálási feladatoknál. Madárrajok esetén nincsen kijelölt vezér, ennek ellenére eljutnak a céljukhoz. Az algoritmus alapeleme az egyed

[22] Ayyadevara 2018.
[23] Ayyadevara 2018.
[24] Ayyadevara 2018.
[25] Ayyadevara 2018.
[26] Ayyadevara 2018.
[27] Ayyadevara 2018.

vagy részecske, amelynek van egy optimuma, a rajnak is van optimuma. Az egyedek a saját és a raj optimumát figyelembe véve mozognak.[28]

Amir Mosavi és Pinar Ozturk a Norvég Műszaki és Tudományos Egyetem (Norwegian University of Science and Technology) Számítástudományi Tanszék (Department of Computer Science) kutatói, gépi tanulási szakértők, Kwok-wing Chau a Hong Kongi Politechnikai Egyetem (Hong Kong Polytechnic University) kutatója, akik által 2018-ban publikált tudományos cikk szerint mind a rövid távú, mind a hosszú távú előrejelző modelleknek fontos szerepük van az árvízkárok megelőzésében. A modellek lehetnek egyszerűek *(single model),* vagy összetettek *(hybrid model)*. A leggyakrabban használt árvíz-előrejelző modell az ANN. Az összetett modellek általában több modell segítségével végeznek predikciókat. Az összetett modellek jóval elterjedtebbek, mint az egyszerűek. Használatosak a következő modellek és algoritmusok, módszerek: *autoregressive moving average* (ARMA), *multiple linear regression, autoregressive integrated moving average* (ARIMA), *quantile regression techniques* (QRT), amelyek célja az árvízgyakoriság előrejelzése (*flood frequency analysis,* FFA). Az ARMA, ARIMA, QRT nem gépi tanulási modellek, de jól használhatók előrejelzésekhez.[29]

A lineáris regresszió a legegyszerűbb gépi tanulási modell, statisztikai módszeren alapul, gyorsan tanítható, kevés erőforrást igényel. Akkor használható jól, ha a bemeneti és a kimeneti adatok között egyszerű lineáris összefüggés van, a valóságban a felhasználása gyakran limitált, mivel a valóságban a bemenet és a kimenet között nem egyszerű lineáris kapcsolat van.[30]

A multiple linear regression már több valóságos helyzetben használható, mint az egyszerű lineáris regresszió, mivel itt a függő változót nem csupán egyetlen tényező, hanem már több független változó magyarázza együttesen. Ez a modell már jóval több kimenetet befolyásoló tényezőt figyelembe tud venni, mint az egyszerű lineáris regresszió, és sok esetben pontosabb predikciókra képes. Akkor ütközhetünk problémába, ha a független változók erősen korrelálnak egymással, vagy bizonyos független változók nem szignifikánsak statisztikailag, ilyen esetekben gyengül a modell általánosító képessége.[31]

Az *adaptive neuro-fuzzy inference systemmel* (ANFIS) Mosavi és társai rövid távú árvíz-előrejelzést végeztek, ez az összetett hibrid rendszer ötvözi a fuzzy logika előnyeit a neurális hálók magas fokú rugalmasságával, ezáltal adaptív előrejelző rendszert hozván létre. A neurális háló komponens tanulás útján optimalizálja a meglévő fuzzy szabályokat, így pontos predikciókat tud végezni.[32]

Alexander Pyayt, az oroszországi Siemens LLC alkalmazottja, Ilya Mokhov, az oroszországi Siemens LLC alkalmazottja, Bernhard Lang, a németországi Siemens AG alkalmazottja, Valeria V. Krzhizhanovskaya, az Amszterdami Egyetem (Universiteit van Amsterdam) kutatója, Robert J. Meijer, a Holland Alkalmazott Tudományos Kutatások Szervezet (Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek) kutatója, munkájuk során töltéseknél mért szenzoradatok alapján próbálnak

[28] Ayyadevara 2018.
[29] Mosavi–Ozturk–Chau 2018.
[30] Ayyadevara 2018.
[31] Ayyadevara 2018.
[32] Mosavi–Ozturk–Chau 2018.

előrejelzéseket végezni. Ilyen adatok a pórusvíznyomás *(pore water pressure),* maghőmérséklet *(core temperature),* dőlésszög *(inclination),* elmozdulások *(displacements),* vízállás *(water level).* Ők *neural cloudsot* (NC) használtak anomáliadetekcióra, amely egy kombinált algoritmus, két fő elemmel. Első eleme az *advanced K-means* (AKM), ez a könnyen használható klaszterező algoritmus, amely meghatározza, hogy milyen értékek számítanak hétköznapinak, normálisnak, és melyek nem. A második eleme a *radial basis function* (RBF) hálózat, amely a meglévő klaszterek középpontjai köré Gauss-görbéket húz, így egy új mérésről könnyedén meg lehet mondani, hogy normális érték-e, vagy anomáliának számít.[33]

A *K-means* egy felügyelet nélkül tanuló modell, célja az adatok klaszterezése (csoportosítása) úgy, hogy a hasonló elemek egy klaszterbe kerüljenek. A modell működtetéséhez előre meg kell adni a k paraméter értékét, vagyis hogy hány klaszterbe szeretnénk csoportosítani az adatokat; bár ez a valóságban gyakran okozhat nehézségeket, az algoritmus sok esetben kimondottan jól működik. Szintén negatívum, hogy olykor megtörténik, hogy beragad egy lokális minimumba, és nem találja meg a globális optimumot. Az algoritmus célja, hogy egy adott klaszteren belül lévő elemek egymáshoz minél közelebb legyenek, úgy, hogy a különböző klaszterek középpontjai pedig egymástól a lehető legtávolabb legyenek. Az algoritmus működése iteratív. Első lépésben általában véletlenszerűen kiválasztunk k darab középpontot. Ezután minden adatot a legközelebbi klaszterközépponthoz rendelünk, aztán a középpontokat újraszámítjuk a klaszterhez tartozó pontok átlagolásával, innen ered az algoritmus neve is. Ezeket a lépéseket addig ismételjük, amíg a klaszterek stabilizálódnak, vagyis már nem változik a pontok besorolása, vagy el nem érünk egy előre megadott iterációszámot.[34]

Advanced K-means (AKM): a *K-means* továbbfejlesztett változata, ahol a klaszterek száma nincs előre rögzítve bemeneti paraméterként, a felhasználó ad meg egy minimális és maximális értéket, és az algoritmus megpróbál az adatokra jól illeszkedő klasztereket találni. Ez úgy valósul meg, hogy választanak egy kezdő klaszterszámot és lefuttatják a hagyományos *K-means* algoritmust. Ezt követően az eljárás iteratív módon módosítja a klaszterközéppontok számát és elhelyezkedését. Új középpontot hoz létre, ha bizonyos adatok túl nagy távolságra esnek a legközelebbi centroidtól, törli azokat a klasztereket, amelyek túl kevés adatpontot tartalmaznak, és összevonja azokat a klasztereket, amelyek középpontjai egy előre megadott távolságküszöbnél közelebb kerülnek egymáshoz. Minden ilyen lépés után ismét lefuttatják a *K-means* lépéseit az aktuális középpontokra, egészen addig, amíg a klaszterszám és a centroidok helyzete nem stabilizálódik, vagy amíg el nem érnek egy maximális iterációszámot. Ez a módszer részben automatizálja a klaszterek számának megválasztását, ugyanakkor az eredmény erősen függ a minimális és maximális klaszterszámtól, a minimális klasztermérettől, valamint a távolságra és összevonásra vonatkozó küszöbértékektől. Az AKM hátrányai közé tartozik, hogy euklideszi távolságra és nagyjából gömb alakú klaszterekre épít, érzékeny az adatok skálázására és a kezdeti középpontválasztásra,

[33] Pyayt et al. 2011.
[34] Ayyadevara 2018.

így nagy dimenziószám vagy zajos, átfedő klaszterek esetén előfordulhat, hogy lokális minimumba ragad, és nem találja meg a globális optimumot.[35]

A települési csapadékvíz által okozott elöntések sok ország számára rendszeres és jelentős problémát okoznak, ami évente felbecsülhetetlenül nagy károkat tud okozni. William Sayers, az Exeteri Egyetem (University of Exeter) kutatója és a HR Wallingford kutatóintézetnél is dolgozik, Dragan Savić és Zoran Kapelan, az Exeteri Egyetem (University of Exeter) kutatói és Richard Kellagher, a HR Wallingford kutatóintézet munkatársa által végzett kutatás célja a beavatkozás hatékonysága és a ráfordítandó összeg közötti egyensúly megtalálása volt. Ők egy ADAPT (A Drainage Analysis and Planning Tool) rendszert egészítettek ki multiobjektív genetikus algoritmussal, konkrétabban *nondominated sorting genetic algorithm II* (NSGA II) és neurális hálóval *(neural network)*.[36]

A multiobjektív genetikus algoritmus (MOGA) egy gyűjtőfogalom, amelybe beletartozik az összes olyan genetikus algoritmus, amely többcélú optimalizációra használható. A hagyományos genetikus algoritmus esetén a cél a legjobb megoldás megtalálása, többcélú optimalizáció esetén ilyen nem létezik, a többcélú optimalizáció esetén kompromisszumos megoldásokat tartalmazó halmaz megtalálására törekszünk, vagyis a Pareto-frontot akarjuk közelíteni. A *nondominated sorting genetic algorithm* II vagyis nemdominált genetikus algoritmus az egyik legelterjedtebb, könnyen használható, gyors, többcélú optimalizációra alkalmazható genetikus algoritmus, amely nemdomináns rendezési stratégiát használ, és kimondottan jól tudja kezelni az egymással ellentétes célfüggvényeket is.[37]

A Google által fejlesztett Google's Flood Hub jól működő árvíz-előrejelző rendszer, amely bárki számára térítésmentesen elérhető, és 2018-tól kezdték használni. A rendszert négy komponens alkotja: adatvalidálás, szakaszos előrejelzés, árvízmodellezés és riasztáselosztás. Két alrendszer gépi tanulásra támaszkodik. A szakaszos előrejelzéshez hosszú rövid távú memória (LSTM) hálózatokat és lineáris modelleket alkalmaznak. Az árvízi elöntést a küszöbérték- és a sokaságmodellekkel számítják ki, ahol az előbbi az árvíz kiterjedését, az utóbbi pedig az árvíz kiterjedését és mélységét is kiszámítja. Az itt elsőként bemutatott sokaságmodell gépi tanuláson alapul. A küszöbértékű modell a Google hagyományos komponense. A rendszer betáplálja a mérőállomásokról, műholdakról kapott adatokat az MI-modellekbe, így végez predikciókat. Jelenleg csak folyami árvizek előrejelzésére képes, de a jövőben elképzelhető, hogy a működést kiterjesztik villámárvizekre is. A történeti adatokon végzett értékelés során minden modell kellően jól működik az operatív használathoz. Az LSTM jobban teljesített, mint a lineáris modell, míg a küszöbértékű és a sokaságmodellek hasonló teljesítménymutatókat értek el az árvíz kiterjedésének modellezésében. A rendszer akár hét nappal előre prediktálni tudja, hogy egy adott folyó ki fog-e lépni a medréből. Ez nagy segítséget jelent, mivel a helyes predikciók segítségével a katasztrófavédelmi szakemberek időben meg tudják hozni a szükséges lépéseket a károk minimalizálása érdekében. Az elmúlt években a projekt rengeteget fejlődött, sok ország csatlakozott

[35] Ayyadevara 2018; Pyayt et al. 2011; Lang et al. 2008.
[36] Sayers et al. 2014.
[37] Deb et al. 2002.

hozzá. A rendszerrel kapcsolatos tervek a lefedettség kiterjesztését, valamint a modellezési képességek és pontosság javítását célozzák.[38]

Az árvizek aránytalanul nagy hatást gyakorolnak a fejlődő és fejletlen országokra, ahol gyakran hiányoznak a sűrű vízhozammérő hálózatok. A világ vízgyűjtőinek csak néhány százalékát mérik, és a vízfolyásmérők nem egyenletesen oszlanak el a világon. Szoros kapcsolat van a nemzeti bruttó hazai termék és az adott országban nyilvánosan elérhető összes vízhozam-megfigyelési adat között, ami azt jelenti, hogy a kiváló minőségű előrejelzések különösen nagy kihívást jelentenek azokon a területeken, amelyek a leginkább ki vannak téve az árvizek pusztító hatásainak. A Flood Hub kutatói kimutatták, hogy a mesterségesintelligencia-alapú előrejelzés megbízhatóan jelzi a szélsőséges folyami eseményeket a nem mért vízgyűjtőkön, akár ötnapos előzetes idővel is, ami hasonló vagy jobb, mint a jelenlegi legmodernebb globális modellező rendszer, a Copernicus Vészhelyzet-kezelési Szolgálat Globális Árvíztudatossági Rendszere (GloFAS) azonnali előrejelzéseinek (nulladik napos előzetes idő) megbízhatósága. A Flood Hub kutatói rávilágítanak, hogy égető szükség van a hidrológiai adatok elérhetőségének növelésére a megbízható árvízi figyelmeztetésekhez való globális hozzáférés további javítása érdekében.[39]

A mesterséges intelligencia és a gépi tanulás a villámárvíz elleni védekezésben nemzetközi szinten

A hirtelen lezúduló csapadék komoly problémákat okozhat, sok ember életét és vagyonát veszélyezteti a hegyvidékeken és dombvidékeken, hiszen villámárvíz kialakulásához vezethet. Az ilyen események előrejelzése nehéz, mivel rendkívül pontos modellekre van szükség, mert a villámárvíz gyorsan alakul ki, és relatív kisebb területre koncentrálódik, pár km-es pontosságú predikció gyakran nem elég.

Ghazi Al-Rawas, Mohammad Reza Nikoo, Malik Al-Wardy és Talal Etri a Sultan Qaboos University kutatói összefoglaló jellegű, 2024-ben publikált cikkükben bemutatják, hogy Iránban SVM, ANN, RNN, CNN és *nearest neighbor classification* (NNC) algoritmusokat, Jordániában ANN, a Fülöp-szigeteken regressziós algoritmusokat, Kínában LSTM, Egyiptomban *light gradient boosting machine* (LightGBM), CatBoost, XGBoost, *multilayer perceptron* (MLP), *logistic regression* (LR) rendszereket használtak villámárvíz-predikcióra.[40]

Az LR, vagyis logisztikus regresszió egyszerű, gyors gépi tanulási modell, amely jól használható kategorikus adatokon. Az algoritmus eredménye gyakran csak két értéket vehet fel: igazat vagy hamisat. Jól használható eldöntendő feladatoknál, például lesz árvíz vagy nem, beteg az illető vagy nem.[41]

[38] Nevo et al. 2022.
[39] Nearing et al. 2024.
[40] Al-Rawas et al. 2024.
[41] Ayyadevara 2018.

RNN, azaz rekurrens neurális hálózat egy speciális verziója a mesterséges neurális hálóknak, rendelkezik, úgymond, beépített memóriával, amely jól kezeli az időben összefüggő, szekvenciális adatokat, ahol kulcsfontosságú a sorrend.[42]

Az RNN-modellek általában jól megtanulják az időbeli mintázatokat, egyszer-egyszer előjön a *vanishing gradient* vagy az *exploding gradient* probléma. Elhaló gradiens *(vanishing gradient)* akkor fordulhat elő, amikor a fontos információval már túl régen találkozott a modell, ilyenkor hajlamos ezt elfelejteni, mivel a tanulás során a régi információ gradiense egyre kisebb lesz, így a súlyfrissítés is egyre kisebb lesz, a régi információ hatása lassan eltűnik, a modell már nem fog emlékezni erre az információra. A robbanó gradiens *(exploding gradient)* probléma akkor fordul elő, amikor bizonyos súlyok túl nagyra nőnek, a modell tanulása instabillá válik, mivel a modell már nem tud konvergálni a helyes súlyok felé azért, mert a frissítések túl nagyok.[43]

Long short-term memory (LSTM), magyarul hosszú rövid távú memória egy komplex modell, amely már kiküszöböli az eltűnő és robbanó gradiens problémát, képes hosszú adatsorozatok esetén is emlékezni a lényeges információkra. Az LSTM működésének legfontosabb eleme a cellamemória: akár egy futószalag, amelyen az információk sok ideig tudnak utazni anélkül, hogy minden lépésnél megváltoznának. Rendelkezik bemeneti kapuval *(input gate),* kimeneti kapuval *(output gate)* és elfelejtő kapuval *(forget gate)*. A fontos információk a cellamemóriában maradnak, a felesleges, kis relevanciával bíró információk pedig elfelejtődnek a felejtő kapun keresztül.[44]

A *bagging* és *boosting* a gépi tanulásban alkalmazott együttes *(ensemble)* tanulási módszerek. Az *ensemble* megközelítés lényege, hogy egyetlen modell helyett modellek csoportját tanítjuk és egyesítjük. A *bagging* és a *boosting* a két legismertebb ilyen technika. A *bagging* (*bootstrap* aggregálás) Leo Breiman statisztikus által 1996-ban bevezetett módszer, amely több változatban létrehozott tanuló modell átlagolásával vagy szavazásával javítja az előrejelzést.[45]

A *bagging* során az eredeti adathalmazból számos *bootstrap* újramintavétellel készült részhalmazt hozunk létre: minden egyes részhalmaz az eredeti mintából véletlenszerűen, visszatevéses mintavételezéssel generálódik, így egy-egy elem többször is szerepelhet vagy kimaradhat egy adott részhalmazból. Minden egyes ilyen *bootstrap* halmazhoz betanítunk egy-egy alapmodellt (úgynevezett alaptanulót, például döntési fát vagy más klasszifikátort), majd az így kapott több modell aggregált előrejelzését adjuk eredményül. Klasszifikáció esetén az egyes modellek osztályba sorolási szavazatait többségi szavazással egyesítjük, regressziónál pedig az átlagukat vesszük. A *bagging* fő hatásmechanizmusa a predikciós modell varianciájának csökkentése azáltal, hogy több, egymástól függetlenül betanított modell átlagát vesszük. Különösen instabil, nagy varianciájú alaptanulók esetén (mint például a döntési fák) hoz jelentős javulást, mivel kiegyenlíti az adatkészlet kis változásaira érzékeny modellek fluktuációit.[46]

[42] Ayyadevara 2018.
[43] Ayyadevara 2018.
[44] Ayyadevara 2018.
[45] Breiman 1996.
[46] Breiman 1996.

Ezzel szemben a *bagging* nem feltétlenül csökkenti a torzítást: az egyes modellek átlagolása a rendszeres hibákat nem szünteti meg, viszont az *overfitting* (túlillesztés) kockázatát csökkenti a variancia mérséklésével. A *bagging* egyszerűsége és hatékonysága miatt hamar népszerű lett; tipikus alkalmazása a *random forest* algoritmus, amely a *bagging* elvét valósítja meg döntési fák esetén, kiegészítve a változók véletlenszerű kiválasztásával minden fa építésekor. A *random forest* így sok, különböző *bootstrap* mintán tanult döntési fa együttesével ér el magas pontosságot és stabilitást. Ebben a kontextusban fontos kiemelni, hogy a *random forest* nem egyenlő a döntési fával: míg a döntési fa egyetlen faalapú modell, addig a *random forest* a *bagging* egy speciális formája, amely sok mély döntési fát tanít különböző *bootstrap* mintákon, és minden egyes *split* során csak egy véletlenül kiválasztott jellemző részhalmazból engedi meghatározni a legjobb osztást. Ez a kétlépcsős véletlenítés – az adatminták és a jellemzők szintjén – jelentősen növeli a modell robusztusságát és általánosító képességét, így a *random forest* működése és célja alapvetően eltér egyetlen döntési fa viselkedésétől.[47]

A *boosting* olyan együttes tanulási módszer, amely szekvenciálisan kapcsol össze több gyenge tanulót annak érdekében, hogy egy erős, nagy pontosságú modellt állítson elő. A *boosting* során az egyes almodelleket egymás után tanítjuk be úgy, hogy minden új modell az előző modell által elkövetett hibákra koncentrál. Ezt tipikusan azzal érik el, hogy a tanulóalgoritmus figyelmét az előző körökben rosszul klasszifikált példákra irányítják – például súlyokat rendelnek az adatokhoz, amelyeket minden iteráció után növelnek a helytelenül besorolt példák esetén.[48]

Kezdetben egy almodell tanul az eredeti adatokon, majd minden további modell az addig rosszul prediktált mintákat nagyobb súllyal veszi figyelembe. Végül az összes almodell előrejelzését egyesítjük, általában súlyozott szavazással vagy összegzéssel, ahol a jobb teljesítményű modellek nagyobb súlyt kapnak a végső döntésben. Ennek eredményeképp a *boosting* iteratív módon csökkenti a modell torzítását: a korábban alulbecsült mintákra fókuszálva egyre pontosabbá teszi a kompozit modellt. A *boosting* elvi alapját Robert Schapire 1990-ben rakta le a gyenge tanulók megerősítésének elméletével, gyakorlati áttörést pedig Freund és Schapire AdaBoost algoritmusa hozott 1996-ban. Az AdaBoost *(adaptive boosting)* volt az első, széles körben alkalmazott *boosting* algoritmus, és máig az egyik legnépszerűbb, mivel viszonylag egyszerű és sokféle gyenge tanulóval jól működik. Az AdaBoost minden iterációban újrasúlyozza a tanító adatpontokat: növeli a rosszul osztályozott példák súlyát, így a következő gyenge modell már ezekre helyez nagyobb hangsúlyt.[49]

Az idők során számos *boosting* variáns született. Jelentős fejlesztés volt Jerome Friedman munkája, aki bevezette a *gradiens boosting* módszert, általánosítva a *boostingot* tetszőleges veszteségfüggvény gradiense mentén történő iteratív javításra – ezzel nemcsak osztályozási, hanem regressziós problémákra is hatékony *boosting* algoritmust adott.[50]

[47] Jansen 2021.
[48] Schapire 1990; Freund 1995.
[49] Freund–Schapire 1996.
[50] Friedman 2001.

A gradiens alapú *boosting* keretrendszer számos modern megvalósítás alapja; ilyen például a széles körben használt XGBoost algoritmus is. Ugyanakkor a *boosting* hajlamos lehet a túlillesztésre, ha túl sok iterációt használunk, vagy ha jelentős zaj van az adatokban. Empirikus vizsgálatok kimutatták, hogy míg zajmentes adatokon a *boosting* gyakran pontosabb, addig zajos adatkörnyezetben a *bagging* stabilabbnak bizonyul. A *boosting* modell ugyanis felerősítheti a zajt vagy a kimeneti változóban lévő véletlenszerű hibákat azzal, hogy megpróbál minden apró hibát kijavítani, ami túlillesztéshez vezethet. Ezzel szemben a *bagging,* mivel átlagolással dolgozik, jóval robusztusabb a zajjal szemben, és ritkábban fordul elő, hogy teljesítménye zaj hatására jelentősen romlik.[51]

Categorical boosting (CatBoost), azaz kategorikus boosting algoritmus egy relatív új, 2017-ben megalkotott, rugalmas *gradiens boosting* algoritmus, amely nagyon hatékonyan tudja kezelni a nagy mennyiségű kategorikus bemeneti adatot. Képes számokká alakítani a kategorikus adatokat *one-hot encoding* felhasználása nélkül.[52]

Mohamed Wahba, aki az Egyiptom–Japán Tudományos és Technológiai Egyetem (Egypt-Japan University of Science and Technology, E-JUST) Környezetmérnöki Tanszékének (Environmental Engineering Department) kutatója, Mustafa El-Rawy, aki a Miniai Egyetem (Minia University) Építőmérnöki Karán (Civil Engineering Department, Faculty of Engineering) a Vízgazdálkodási Mérnöki tanszék professzora és kutató, Nassir Al-Arifi, aki a Szaúd-Arábiai Király Szaúd Egyetem (King Saud University) Geológiai és Geofizikai Tanszékének (Department of Geology and Geophysics) kutatója, Mahmoud M. Mansour, aki az Egyiptomi Menoufia Egyetem (Menoufia University) Mérnöki Kar Építőmérnöki Tanszékének (Department of Civil Engineering, Faculty of Engineering) kutatója, akik által végzett tudományos munka során, amelynek célja új módszerek kifejlesztése volt, amivel Japánban földcsuszamlások és villámárvízek kockázatát lehet becsülni, LASSO Regression modell segítségével generáltak *landslide hazard map* (LHM), *flood hazard map* (FHM), *composite hazard map* (CHM) eredményeket. A kapott eredményeket *receiver operating characteristic* (ROC) és *area under the curve* (AUC) segítségével mérték. Az LHM és a FHM 99% fölötti ROC- és AUC-értéket értek el.[53]

Khaula Alkaabi, az Egyesült Arab Emírségek Egyetem (United Arab Emirates University), Uzma Sarfraz, a Government College University Lahore és Saif Al Darmaki, az Egyesült Arab Emírségek Nemzeti Meteorológiai Központjának (National Center of Meteorology) kutatói közösen végzett munkájuk során az Egyesült Arab Emírségek területén prediktálták a villámárvíz valószínűségét egy hibrid mélytanulási keretrendszerrel, amely integrálja a CNNs-t, RNNs-t és a *neural ordinary differential equations* (Neural ODEs) megoldásait, amelyek R^2 0,98 RMSE = 2,87 × 10^6, MAE = 1,13 × 10^6, PBIAS = –8,38 értékeket értek el.[54]

A következőkben összefoglaló táblázatban (1. táblázat) mutatjuk be a különböző országokban alkalmazott mesterségesintelligencia-alapú villámárvíz-előrejelző modelleket, valamint azok teljesítményét.

[51] Kotsiantis–Kanellopoulos 2012; Opitz–Maclin 1999.
[52] Jansen 2021.
[53] Wahba et al. 2023.
[54] Alkaabi – Sarfraz – Al Darmaki 2025.

1. táblázat: Villámárvíz-előrejelző modellek összehasonlítása

Modell	Modell célja, felhasználása	Elért eredmények
Least Absolute Shrinkage and Selection Operator (LASSO) regresszió	Villámárvíz előrejelzése	AUC *(area under the curve):* 99,36% Átlagos abszolút hiba (MAE): 0,208
DeepLabv3 (konvolúciós neurális hálózat, CNN)	Villámárvíz detektálása	Szegmentálási pontosság: 87%
Neurális differenciálegyenlet (Neural ODE)	Villámárvíz detektálása	Átlagos abszolút hiba (MAE): $1{,}85 \times 10^6$ Root mean square error (RMSE): $3{,}41 \times 10^6$ R^2: 0,97 Nash–Sutcliffe-hatékonyság (NSE): 0,97 Percent bias (PBIAS): –25,48%
Konvolúciós neurális hálózat (CNN) + Rekurrens neurális hálózat (RNN)	Villámárvíz előrejelzése	Átlagos abszolút hiba (MAE): $1{,}66 \times 10^6$ Root mean square error (RMSE): $3{,}74 \times 10^6$ R^2: 0,96 Nash–Sutcliffe-hatékonyság (NSE): 0,96 Percent bias (PBIAS): –13,73%
Konvolúciós neurális hálózat (CNN) + Rekurrens neurális hálózat (RNN) + neurális differenciálegyenlet (Neural ODE)	Villámárvíz előrejelzése	Átlagos abszolút hiba (MAE): $1{,}13 \times 10^6$ Root mean square error (RMSE): $2{,}87 \times 10^6$ R^2: 0,98 Nash–Sutcliffe-hatékonyság (NSE): 0,98 Percent bias (PBIAS): –8,38%
U-net alapú detektálás	Veszélyértékelés és erőforrás-allokáció támogatása	F1-pontszám: 0,92

Forrás: Wahba et al. 2023; Alkaabi – Sarfraz – Al Darmaki 2025; Zhou 2025

A mesterséges intelligencia és a gépi tanulás az aszály elleni védekezésben nemzetközi szinten

Az aszály mint hidrológiai katasztrófa jóval lassabban alakul ki, mint az árvíz, de jelentősen tovább is tart, és nagyobb területeket érint. Fontos, hogy minden országnak legyen modern, pontos aszálymonitorozó és -előrejelző rendszere, és létezzenek akciótervek arra nézve, hogyan lehet elkerülni az aszályt, vagy legalább a hatását csökkenteni. Az aszályok előrejelzése kulcsfontosságú a gazdasági stabilitás érdekében. Az időben előrejelzett aszályra sokkal könnyebb felkészülni, és megtenni a szükséges intézkedéseket.

Ali Mokhtar, a Kairói Egyetem Mezőgazdasági Mérnöki Tanszék (Cairo University Faculty of Agriculture) kutatója, akinek publikációs területei a vízgazdálkodás, a mesterséges intelligencia és az éghajlatváltozás, és társai Kínában CNN, LSTM és XGB algoritmusokkal végeztek aszály-előrejelzést, felhasználva az 1980 és 2019 között gyűjtött meteorológiai adatokat. A predikciókhoz felhasználták a csapadékmennyiségi és hőmérsékletátlagot, minimum- és maximumhőmérséklet-, szélsebesség- és páratartalom-adatokat.[55]

Jelenleg nincs általános, világszerte használható aszályindex. Mhamd Saifaldeen Oyounalsoud, Abdullah Gokhan Yilmaz, Mohamed Abdallah és Abdulrahman Abdeljaber kutatásuk során, amelynek célja az aszály-előrejelzés volt Ausztráliában, DT, *generalised linear model* (GLM), SVM, ANN és RF modellek segítségével új aszályindexeket fejlesztettek ki, amelyek jobban teljesítettek a meglévő indexeknél.[56]

Kavina Dayal a School of Agriculture and Environmental Science intézmény kutatója, amely a University of Southern Queensland része, Ravinesh Deo a University of Southern Queensland School of Agricultural, Computational & Environmental Sciences kutatója és Armando A. az Apan University of Southern Queensland School of Civil Engineering and Surveying kutatója, munkájuk során a SPEI-t *(standardised precipitation-evapotranspiration index)* prediktálták ANN segítségével, és ezáltal végeztek aszály-előrejelzést Ausztrália két különböző éghajlati régiójában, egy mérsékelt területen és egy füves pusztai részen. A modell bemenetei idősoros meteorológiai adatok voltak, mint csapadékmennyiség, minimum és maximum hőmérséklet. A modell jól teljesített, az R^2 megközelítően 0,99 volt.[57]

Tadele Melese, a Bahir Dar Egyetem (Bahir Dar University) Természeti Erőforrás Menedzsment Tanszékének (Department of Natural Resource Management) kutatója és társai több gépi tanulási modellt is kipróbáltak aszály-előrejelzés céljából Etiópiában, és arra a következtetésre jutottak, hogy az együttes tanulási modellek *(ensemble learning models)* kimondottan jól teljesítenek ebben a helyzetben. A *random forest* teljesítménye volt a legjobb, 71,18%-os pontosságot és 0,9 AUC-t értek el. Kutatásuk arra is rávilágított, hogy kulcsfontosságú az adatok kiegyensúlyozottsága, ezért hibrid mintavételezést alkalmaztak, amely ötvözi a manuális újra-mintavételezést és a *synthetic minority oversampling technique* (SMOTE) technikát. Munkájuk során, a túlilleszkedés elkerülése érdekében, *grid search-öt* és keresztvalidációt használtak.[58]

A következőkben összefoglaló táblázatban (2. táblázat) mutatjuk be a különböző országokban alkalmazott mesterségesintelligencia-alapú aszály- és aszályindex-előrejelző modelleket, valamint azok teljesítményét.

[55] Mokhtar et al. 2021.
[56] Oyounalsoud et al. 2024.
[57] Dayal–Deo–Apan 2017.
[58] Melese et al. 2025.

2. táblázat: Aszály-előrejelző modellek összehasonlítása

Modell	Modell célja	Elért eredmények
Extreme gradient boosting (XGB)	SPEI aszályindex előrejelzése éghajlati változókból	SPEI-3: Átlagos abszolút hiba (MAE): 0,26–0,35 Négyzetes átlag hiba (RMSE): 0,09–0,17 Nash–Sutcliffe-hatékonyság (NSE): 0,84 SPEI-6: Négyzetes átlag hiba (MSE): 0,16 Korrelációs együttható (R): 0,95
Random forest (RF)	SPEI aszályindex előrejelzése éghajlati változókból	SPEI-3: Átlagos abszolút hiba (MAE): 0,36 Nash–Sutcliffe-hatékonyság (NSE): 0,86 SPEI-6: Négyzetes átlag hiba (MSE): 0,11 Korrelációs együttható (R): 0,95
Konvolúciós neurális háló (CNN)	SPEI előrejelzése különböző időskálákon	SPEI-3: Négyzetes átlag hiba (MSE): 0,29 Korrelációs együttható (R): 0,82 SPEI-6: Négyzetes átlag hiba (MSE): 0,36 Átlagos abszolút hiba (MAE): 0,49 Korrelációs együttható (R): 0,77
Long short-term memory (LSTM)	SPEI előrejelzése	SPEI-3: Négyzetes átlag hiba (MSE): 0,37 Átlagos abszolút hiba (MAE): 0,56 Korrelációs együttható (R): 0,78 SPEI-6: Négyzetes átlag hiba (MSE): 0,46 Korrelációs együttható (R): 0,77
Mesterséges neurális háló (ANN)	SPEI havi előrejelzése	Determinációs együttható (R^2): 0,9839 Nash–Sutcliffe-hatékonyság (NSE): 0,9838 Négyzetes átlagos hiba gyöke (RMSE): 0,1338 Átlagos abszolút hiba (MAE): 0,0882
Gradiens boosting	PDSI – Palmer-féle aszály-súlyossági index osztályozása	Pontosság: 0,61 AUC (area under the curve): 0,8982 F1-pontszám: 0,60
Támogató vektorgépek (SVM)	PDSI – Palmer-féle aszály-súlyossági index osztályozása	Pontosság: 0,67 AUC (area under the curve): 0,8681 F1-pontszám: 0,66
Random forest (RF)	PDSI – Palmer-féle aszály-súlyossági index osztályozása	Pontosság: 0,72 AUC (area under the curve): 0,9000 F1-pontszám: 0,71
Döntési fa (decision tree, DT)	PDSI – Palmer-féle aszály-súlyossági index osztályozása	Pontosság: 0,56 AUC (area under the curve): 0,55 F1-pontszám: 0,7456

Forrás: Mokhtar et al. 2021; Oyounalsoud et al. 2024; Dayal–Deo–Apan 2017; Melese et al. 2025

Összefoglalás

Láthatjuk, hogy az elmúlt húsz év alatt a mesterséges intelligencia felhasználása nagyon elterjedt lett a különböző hidrológiai katasztrófák előrejelzésében, sok esetben pontosabb predikciókat ér el, mint a régi fizikai modellek. Hidrológiai katasztrófák predikciójánál leggyakrabban artificial neural network (ANN), convolutional neural network (CNN), decision tree (DT), random forest (RF), support vector machine (SVM), extreme gradient boost (XGBoost), long short-term memory (LSTM) eszközöket használnak. A fentebb leírtak alapján azt is kijelenthetjük, hogy csak mesterséges-intelligencia-alapú módszerek használata árvíz-, belvíz-, villámárvíz-, településelöntés-, aszály-előrejelzéshez a legtöbb esetben nem lesz elegendő. A tudomány jelen állása szerint a régebbi klasszikus hidrológiai módszerek kombinálása több gépitanulás- és mesterségesintelligencia-modellel hozza a legjobb eredményt. Hazánk rendelkezik jól működő árvíz- és aszály-előrejelző rendszerrel, de jelenleg a mesterséges intelligencia és a gépi tanulás alkalmazása még nem jellemző a hidrológiai katasztrófák predikciós rendszereiben, viszont több egyetem és intézmény, mint a Nemzeti Közszolgálati Egyetem, Szegedi Tudományegyetem, Felső-Tisza-vidéki Vízügyi Igazgatóság, is folytat kutatást ebben a témakörben.

Felhasznált irodalom

Al-Rawas, Ghazi et al. (2024): A Critical Review of Emerging Technologies for Flash Flood Prediction: Examining Artificial Intelligence, Machine Learning, Internet of Things, Cloud Computing, and Robotics Techniques. *Water,* 16(14). Online: https://doi.org/10.3390/w16142069

Alkaabi, Khaula – Sarfraz, Uzma – Al Darmaki, Saif (2025): A Deep Learning Framework for Flash-Flood-Runoff Prediction: Integrating CNN-RNN with Neural Ordinary Differential Equations (ODEs). *Water*, 17(9), 1283. Online: https://doi.org/10.3390/w17091283

Ayyadevara, V. Kishore (2018): *Pro Machine Learning Algorithms: A Hands-On Approach to Implementing Algorithms in Python and R.* New York: Apress. Online: https://doi.org/10.1007/978-1-4842-3564-5

Blanka-Végi Viktória et al. (2024): Gépi tanulási módszerek az aszály és belvíz monitoring és előrejelzés fejlesztésében. *Földrajzi Közlemények,* 148(2), 175–181. Online: www.foldrajzitarsasag.hu/downloads/reviews/2024/FK_2024_02_175_181_Blanka_etal.pdf

Breiman, Leo (1996): Bagging Predictors. *Machine Learning,* 24, 123–140. Online: https://doi.org/10.1007/BF00058655

Buszta, Julia et al. (2023): Historical Analysis and Prediction of the Magnitude and Scale of Natural Disasters Globally. *Resources,* 12(9), 106. Online: https://doi.org/10.3390/resources12090106

Copernicus Emergency Management Service. Online: https://emergency.copernicus.eu/

Dayal, Kavina – Deo, Ravinesh – Apan, Armando A. (2017): Drought Modelling Based on Artificial Intelligence and Neural Network Algorithms: A Case Study in

Queensland, Australia. In Leal Filho, Walter (szerk.): *Climate Change Adaptation in Pacific Countries*. Cham: Springer, 177–198. Online: https://doi.org/10.1007/978-3-319-50094-2_11

Deb, Kalyanmoy et al. (2002): A Fast and Elitist Multiobjective Genetic Algorithm: NSGA-II. *IEEE Transactions on Evolutionary Computation*, 6(2), 182–197. Online: https://doi.org/10.1109/4235.996017

European Flood Awareness System. Online: https://european-flood.emergency.copernicus.eu/en

Fiala Károly et al. (2018): Operatív aszály- és vízhiánykezelő monitoring rendszer. *Hidrológiai Közlöny,* 98(3), 14–24 Online: https://real.mtak.hu/156046/1/Fiala_et_al2018HidrologiaiKozlony.pdf

Freund, Yoav (1995): Boosting a Weak Learning Algorithm by Majority. *Information and Computation,* 121(2), 256–285. Online: https://doi.org/10.1006/inco.1995.1136

Freund, Yoav – Schapire, Robert Elias (1996): Experiments with a New Boosting Algorithm. *Machine Learning: Proceedings of the Thirteenth International Conference, 1996.* Online: https://cseweb.ucsd.edu/~yfreund/papers/boostingexperiments.pdf

Friedman, Jerome Harold (2001): Greedy Function Approximation: A Gradient Boosting Machine. *The Annals of Statistics,* 29(5), 1189–1232. Online: https://doi.org/10.1214/aos/1013203451

Hegedűs Gergely (2020): Újabb mérföldkőhöz érkezett Magyarország árvízvédelme. *Magyar Építők,* 2020. szeptember 24. Online: https://magyarepitok.hu/vizgazdalkodas/2020/09/ujabb-merfoldkohoz-erkezett-magyarorszag-arvizvedelme

Jansen, Stefan (2021): *Machine Learning for Algorithmic Trading.* Birmingham: Packt.

Kircsi Andrea et al. (2018): *Drought Monitoring in Hungary.* Interreg – OMSZ. Online: https://drmkc.jrc.ec.europa.eu/portals/0/Innovation/SupportSystem/12_Hungary/Documents/thursday/Andrea_Kircsi_final_Hungary20181108.pdf

Kotsiantis, Sotiris – Kanellopoulos, Dimitris (2012): Combining Bagging, Boosting and Random Subspace Ensembles for Regression Problems. *International Journal of Innovative Computing, Information and Control,* 8(6), 3953–3961. Online: www.ijicic.org/ijicic-11-02046.pdf

Kozák Péter et al. (2022): Az aszály monitoring hálózat és az aszálykezelés gyakorlata a 2022. évi aszály tükrében. *Vízügyi Közlemények,* 104(3), 113–130. Online: https://library.hungaricana.hu/en/view/VizugyiKozlemenyek_2022/?pg=458

Lang, Bernhard et al. (2008): Neural Clouds for Monitoring of Complex Systems. *Optical Memory and Neural Networks,* 17(3), 183–192. Online: https://doi.org/10.3103/S1060992X08030016

Liptay Zoltán Árpád (2024): Hidrológiai előrejelzés körszimmetrikus bázisfüggvény hálózatokkal. *Hidrológiai Közlöny,* 98(3), 1–33. Online: www.hidrologia.hu/vandorgyules/41/word/0606_liptay_zoltan_arpad.pdf

Lu, Shuang – Huang, Jianyun – Wu, Jing (2023): Knowledge Domain and Development Trend of Urban Flood Vulnerability Research: A Bibliometric Analysis. *Water,* 15(10). Online: https://doi.org/10.3390/w15101865

Magyarország 2021. évi árvízkockázat-kezelési terve (2022). Online: https://vizeink.hu/wp-content/uploads/2022/10/akk/Arvizkockazat-kezelesi_terv.pdf

Magyarország Mesterséges Intelligencia Stratégiája (2025–2030) (2025). Online: https://cdn.kormany.hu/uploads/document/c/c0/c0d/c0dfdbd37cfa520a-e37361a168d244c85e7295af.pdf

Melese, Tadele et al. (2025): Machine Learning-based Drought Prediction Using Palmer Drought Severity Index and TerraClimate Data in Ethiopia. *PLoS One,* 2025. június 18. Online: https://doi.org/10.1371/journal.pone.0326174

Mokhtar, Ali et al. (2021): Estimation of SPEI Meteorological Drought Using Machine Learning Algorithms. *IEEE Access,* 9, 65503–65523. Online: https://doi.org/10.1109/ACCESS.2021.3074305

Mosavi, Amir – Ozturk, Pinar – Chau, Kwok-wing (2018): Flood Prediction Using Machine Learning Models: Literature Review. *Water,* 10(11). Online: https://doi.org/10.3390/w10111536

Nearing, Grey et al. (2024): Global Prediction of Extreme Floods in Ungauged Watersheds. *Nature,* 627, 559–563. Online: https://doi.org/10.1038/s41586-024-07145-1

Nevo, Sella et al. (2022): Flood Forecasting with Machine Learning Models in an Operational Framework. *Hydrology and Earth System Sciences,* 26(15), 4013–4032. Online: https://doi.org/10.5194/hess-26-4013-2022

OpenAlex lekérdezés – flood prediction. Online: https://explore.openalex.org/works?page=1&filter=title_and_abstract.search:flood+prediction,type:types/article,primary_topic.id:t11490

OpenAlex lekérdezés – 2000–2025, drought prediction. Online: https://explore.openalex.org/works?page=1&filter=publication_year:2000-2025,title_and_abstract.search:drought+prediction,primary_topic.id:t11490,type:types/article&view=api,report,list

Opitz, David – Maclin, Richard (1999): Popular Ensemble Methods: An Empirical Study. *Journal of Artificial Intelligence Research,* 11, 169–198. Online: https://doi.org/10.1613/jair.614

Oyounalsoud, Mhamd Saifaldeen et al. (2024): Drought Prediction Using Artificial Intelligence Models Based on Climate Data and Soil Moisture. *Scientific Reports,* 14. Online: https://doi.org/10.1038/s41598-024-70406-6

Pyayt, Alexander et al. (2011): Machine Learning Methods for Environmental Monitoring and Flood Protection. *World Academy of Science, Engineering and Technology,* 54, 118–123. Online: www.researchgate.net/publication/254762064

Sayers, William et al. (2014): Artificial Intelligence Techniques for Flood Risk Management in Urban Environments. *Procedia Engineering,* 70, 1505–1512. Online: https://doi.org/10.1016/j.proeng.2014.02.165

Schapire, Robert Elias (1990): The Strength of Weak Learnability. *Machine Learning,* 5, 197–227. Online: https://doi.org/10.1023/A:1022648800760

Szabó János Adolf – Lucza Zoltán – Szabó-Márku Melinda (2024): Mesterséges Intelligencia (MI) alkalmazásának lehetőségei az árvízi előrejelzések pontosításában. In Dobó Kristóf et al. (szerk.): *A Magyar Hidrológiai Társaság által rendezett XLI. Országos Vándorgyűlés dolgozatai.* Budapest: Magyar Hidrológiai Társaság. Online: https://hidrologia.hu/vandorgyules/41/word/0607_lucza_zoltan.pdf

Tan, Ling et al. (2021): Can We Detect Trends in Natural Disaster Management with Artificial Intelligence? A Review of Modeling Practices. *Natural Hazards,* 107, 2389–2417. Online: https://doi.org/10.1007/s11069-020-04429-3
Vizet a tájba. Online: www.ovf.hu/jobboldali-sav-tartalmai/vizetatajba/vizet-a-tajba
Wahba, Mohamed et al. (2023): A Novel Estimation of the Composite Hazard of Landslides and Flash Floods Utilizing an Artificial Intelligence Approach. *Water,* 15(23). Online: https://doi.org/10.3390/w15234138
Zhou, Shuyan (2025): Application of AI in Urban Flash Flood Risk Assessment: From Real-time Warning to Resilience Planning. *Applied and Computational Engineering,* 150(1), 9–14. Online: https://doi.org/10.54254/2755-2721/2025.22398

HADMÉRNÖK
KÖRNYEZETBIZTONSÁG

20. évfolyam (2025) 4. szám 149–159.
DOI: 10.32567/hm.2025.4.9

Sibalin Iván,[1] Kátai-Urbán Maxim,[2] Cimer Zsolt[3]

Az energiaipari-biztonság és a környezeti fenntarthatóság egyes összefüggéseinek értékelése, 1. rész

Assessment of Certain Interrelations between Industrial Safety in the Energy Sector and Environmental Sustainability, Part 1

Absztrakt

A veszélyes anyagokkal foglalkozó üzemek biztonságos működését célzó iparbiztonsági szempontok hatékony érvényesülése a fenntartható fejlődési stratégia sikerének alapvető feltétele. Jelen kutatás fő célja az energiaipari-biztonság és a környezeti dimenzió közötti összefüggések feltárása. A cikksorozat első része az iparbiztonság fenntartható fejlődésben betöltött stratégiai jelentőségét megalapozó elméleti és gyakorlati érvek meghatározását követően értékeli az energiaágazat üzembiztonsága kérdésének a környezeti fenntarthatósági diskurzusban elfoglalt helyét.

Kulcsszavak: iparbiztonság, energiaágazat, környezeti fenntarthatóság, baleset, veszélyhelyzeti kibocsátás

[1] Óraadó, Nemzeti Közszolgálati Egyetem Katasztrófavédelmi Intézet, e-mail: sibalin4@gmail.com
[2] Osztályvezető, Semmelweis Egyetem Biztonságtechnikai Igazgatóság Biztonságszervezési Osztály, e-mail: katai.urban.maxim@semmelweis.hu
[3] Dékán, Nemzeti Közszolgálati Egyetem Víztudományi Kar, e-mail: cimer.zsolt@uni-nke.hu

Abstract

Ensuring the safe operation of hazardous facilities through the effective implementation of industrial safety measures is a fundamental prerequisite for achieving sustainable development. The primary objective of the present study is to explore the interrelations between the industrial safety in the energy sector and the environmental dimension. Following the identification of theoretical and practical arguments supporting the strategic importance of industrial safety in sustainable development, the first part of this article series evaluates the position of industrial safety in the energy sector within the discourse on environmental sustainability.

Keywords: industrial safety, energy sector, environmental sustainability, accident, emergency release

Bevezetés

Az iparosodás, túlfogyasztás és egyéb antropogén eredetű tevékenységek környezetre gyakorolt káros hatásainak felismeréséből fakadóan a 20. század 70-es évei elején vette kezdetét az a napjainkban is zajló globális szintű stratégiai tervező munka, amely meghatározó a fenntarthatóság megvalósításának folyamatában. A fenntartható fejlődést a Környezet és Fejlődés Világbizottságának 1987-es, *Our Common Future* (Közös jövőnk) című Brundtland-jelentésében olyan fejlődésként fogalmazták meg, „amely kielégíti a jelen szükségleteit anélkül, hogy veszélyeztetné a jövő nemzedékek esélyét arra, hogy ők is kielégíthessék szükségleteiket".[4] Összhangban a nemzetközi gyakorlattal, a fenntarthatóság Magyarországon is stratégiai jövőképként értelmezendő. A hazai Nemzeti Fenntartható Fejlődési Keretstratégia a fenntartható fejlődés négy úgynevezett dimenzióját azonosítja: a környezetit, a gazdaságit, a társadalmit és az emberit.[5] Bár az e szempontok közötti közvetlen vagy közvetett kapcsolatok, kölcsönhatások fennállása nyilvánvaló tény, hasznos részkutatások végezhetők célzottan egy-egy konkrét dimenzió vonatkozásában is. A környezeti dimenzió jelentőségének szemléltetésére alkalmas lehet a Világgazdasági Fórum (WEF) 2025-ös globális kockázatjelentésének az elkövetkező tíz évre vonatkozó – 1. táblázatba foglalt – kockázati rangsora, amelyben az öt legnagyobb mértékű kockázat közül az első négy környezeti, az utolsó pedig technológiai jellegű.

1. táblázat: A WEF 2025-ös jelentése által a következő tíz évre meghatározott öt legnagyobb globális kockázat

Ssz.	Globális kockázatok rangsora
1.	Szélsőséges időjárási események
2.	Biodiverzitás csökkenése és az ökoszisztémák összeomlása
3.	Föld rendszereiben bekövetkező kritikus változások
4.	Természeti erőforrások hiánya
5.	Félretájékoztatás és dezinformáció

Forrás: World Economic Forum 2025: 8

[4] Our Common Future 1987.
[5] Nemzeti Fenntartható Fejlődési Tanács 2012.

A téma fontosságát és hosszú távú aktualitását alapul véve ugyancsak időszerű az energiaágazat üzembiztos és balesetmentes működésének, azaz az energiaipari-biztonság kifejezetten a környezeti fenntarthatóságban betöltött szerepének értékelése. Definíció szerint energiaipari-biztonság alatt az iparbiztonsági szakterület azon része értendő, „amelynek célja az energetikai rendszerek és rendszerelemek biztonságos működésének – műszaki, jogi és hatósági eszközök útján történő – szavatolásával az energiaellátás baleset- és üzemzavarmentességének a biztosítása, valamint az energiaágazat területén a súlyos ipari balesetek és üzemzavarok kockázatának minimálisra csökkentése".[6] Erre tekintettel mindenekelőtt azt célszerű megvizsgálni, hogy a tágabb, iparbiztonság szakterületi sajátosságai miként kamatoztathatók a fenntartható fejlődés környezeti dimenzióját célzó stratégiaalkotás keretében.

Iparbiztonság: a fenntartható fejlődés stratégiai jelentőségű szakterülete

Általános értékelés

Magától értetődő, hogy az ipari balesetek megelőzése, az azokkal szembeni védekezés, valamint – bekövetkezésük esetén – következményeik elhárítása a környezetvédelem szempontjából kulcskérdés. Ugyanakkor tágabb, fenntarthatósági perspektívából vizsgálódva feltételezhető, hogy az iparbiztonság stratégiai jelentőségű. Ennek bizonyításához lényeges kiindulópont, hogy meglehetősen széles körű azon tevékenységek köre, amelyek az iparbiztonság szakterületi feladatai közé sorolhatók. Definíció szerint ide tartozik „a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezéssel, a veszélyes áruszállítással, a nukleáris balesetek elhárításával, valamint a létfontosságú rendszerek és létesítmények biztonságával kapcsolatos üzemeltetői, hatósági és önkormányzati feladatok teljesítése". Mindez pedig „a lakosság életének és egészségének, a környezetnek és a létfenntartáshoz szükséges anyagi javaknak és szolgáltatásoknak a magas szintű védelmét szolgálja".[7] Az iparbiztonság fogalmából jól látható, hogy a szakterület a fenntartható fejlődésnek mind a négy dimenziójában szerepet játszik. Különös hangsúly helyeződik ebből a szempontból a létfontosságú rendszerek védelemére, amelyek sérülése, esetleges megsemmisülése az emberek élete és a (természetes, épített) környezet szempontjából egyaránt súlyos következményekkel jár, kiesésük hatásai elérhetik a társadalom jelentős részét vagy egészét, gazdasági instabilitást, környezeti és egészségügyi károkat idézhetnek elő.[8] Ugyancsak külön kiemelendő a nukleáris, valamint súlyos ipari balesetekkel szembeni védelem, amelyek szintén kiterjedt, akár visszafordíthatatlan környezeti, gazdasági, illetve társadalmi károkat okozhatnak.

A következő két alpontban olyan érveket vázolunk fel, amelyek az iparbiztonság környezeti dimenzióban betöltött stratégiai jelentőségének alátámasztását célozzák (2. táblázat).

[6] Sibalin 2022: 57.
[7] Kátai-Urbán 2014: 94–105.
[8] Teknős–Kóródi 2016: 83–96.

Elméleti érvek

Egy szakterület adott stratégiai tervezőmunkában történő alkalmazhatóságának megítéléséhez indokolt megvizsgálni, hogy azt a korábban elfogadott releváns stratégiák egyáltalán nevesítik-e a jövőkép megvalósításának mérvadó kontextusában. Civilizációs és természeti kihívásokkal teli világunkban a biztonság hosszú távú fenntartása komplex rendszerré vált,[9] az iparbiztonságnak pedig, katasztrófavédelmi szakterületként, az egyik legfőbb rendeltetése éppen a közbiztonság, illetve a lakosság fizikai biztonságának megőrzése, amely elvárások sokszor stratégiai szinten is visszaköszönnek. Hazai példát alapul véve, a jelenlegi magyar kormányzati stratégiai rendszerben a biztonságpolitika alapdokumentumának számító – így a részstratégiák kialakításakor is szem előtt tartandó – *Nemzeti Biztonsági Stratégiá*ban (NBS) (ipar) biztonsági és fenntarthatósági szempontok egyaránt megjelennek. A dokumentum megállapítja, hogy „Magyarország és a magyar állampolgárok mindenoldalú – politikai, gazdasági, pénzügyi, társadalmi, technológiai, környezeti, egészségügyi, katonai, rendészeti, információs és kibertérbeli – biztonsága alapvető érték. Biztonságunk megteremtése, fenntartása és erősítése olyan követelmény, amely minden további kormányzati célkitűzés teljesülésének előfeltétele." Rögzíti továbbá, hogy

„Magyarországnak rendelkeznie kell olyan képességekkel, amelyek komplex megelőzési és katasztrófakockázat-csökkentési rendszert alkotnak, és természeti vagy ipari katasztrófák, valamint egészségügyi válsághelyzetek és tömeges sérülésekkel és rombolással járó támadás esetén hatékonyan reagálnak a lakosság életének, egészségének, anyagi javainak védelme és a károk minimalizálása érdekében".

A fenntarthatóságra több különböző aspektusból is utal az NBS. A dokumentum értelmében

„[n]emzeti biztonsági érdekünknek tekintjük […] a fenntartható fejlődés elősegítését", valamint, hogy „[a] fenntartható társadalmi és gazdasági fejlődés, továbbá a természeti katasztrófák megelőzésének egyik kritikus feltétele az éghajlatváltozás hatásainak mérséklése, a gazdaság fosszilis energiahordozó-igényének csökkentése érdekében a környezettudatos és karbonszegény életmód népszerűsítése".[10]

Az NBS hivatkozott rendelkezései alapján megállapítható az iparbiztonsági és a fenntarthatósági szempontok megléte a hatályos hazai biztonságpolitikai stratégiai keretrendszerben. Mindazonáltal a szakterületnek a környezeti fenntarthatósági stratégiai tervezésben való elméleti relevanciája az *ökológiai válság* kifejezés elterjedtsége, valamint a tudományági besorolás alapul vételével is megerősíthető. A helyes és hatékony válságkezelés fontosságát a 2020-ban kialakult koronavírus-pandémia idején voltaképpen az egész világ megtapasztalhatta. Akkor emberek milliárdjai érzékelhették közvetlenül egy olyan krízis hatásait, amely teljes országok és társadalmak működését,

[9] Érces–Vass–Ambrusz 2023: 117–130.
[10] 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról. 1. melléklet. 8., 83., 131., 174.

illetve a lakosság mindennapjait volt képes megváltoztatni. A válságok megelőzéséhez és kezeléséhez a biztonság- és védelemtudományok eszköztára hasznos – sok esetben megkerülhetetlen – eligazítást ad. Ezzel összefüggésben lényeges megállapítani, hogy számos tudományos munka használja korunk környezeti problémái vonatkozásában az *ökológiai válság,* illetve *ecological crisis* meghatározást. A Google Scholar keresőmotor 2025. augusztus 30-i keresés során a magyar nyelvű meghatározásra nagyjából 613, míg az angol nyelvű verzióra mintegy 142 000 találatot ajánlott fel. Az eredmények is arra engednek következtetni, hogy az akadémiai szféra egy meghatározó része gyakorlatilag „válságosnak" értékeli a környezet jelenlegi állapotát. E szemantikai megközelítés bizonyos értelemben hivatkozási alapként szolgálhat a válságokat vizsgálati tárgyként értelmező és egyúttal az ökológiai problémák kezeléséhez is hozzájáruló biztonság- és védelemtudományok – így az azok rendszerébe illeszkedő iparbiztonsági szakterület – alkalmazásának kiterjesztésére a fenntartható fejlődés környezeti dimenziójával kapcsolatos tudományos kutatómunka során.[11] Annak ténye pedig, hogy a különböző stratégiai dokumentumok alkalmasak lehetnek arra, hogy egyfajta hidat képezzenek a tudományos eredmények és a jogi normák között,[12] a kutatásba bevont szakterületek stratégiai jelentőségének erősödését vetíti előre.

A stratégiaalkotásban kiemelt szerepe van a multi- és interdiszciplináris szemléletmódnak, illetve kutatásnak is. Példaként említve: Magyarország kutatási, fejlesztési és innovációs stratégiája felhívja a figyelmet, hogy „[a] bölcsészet- és társadalomtudományok szerepe szintén fontos a modern technológiák befogadásában, a nemzeti és emberi identitás erősítésében egy globalizálódó és technicizálódó világban, a technika humanizálásában, az áltudományok, a tudományellenesség kivédésében, a hagyományőrzés és progresszió összehangolásában". A dokumentum emellett a tudásáramlás specifikus céljai között említi a tudományágak, illetve a különböző szektorok közötti kutatói mobilitás erősítését is.[13] Az Egyesült Nemzetek Nevelésügyi, Tudományos és Kulturális Szervezete (UNESCO) *Oktatás a fenntartható fejlődésért 2020–2030* című stratégiájából – amely a fenntarthatóság oktatásba való minél szélesebb körű integrálását célozza – ugyancsak kiolvasható az interdiszciplináris és projektalapú tanulás és cselekvés fontossága.[14] Tekintettel arra, hogy az iparbiztonság szakterülete több tudományág – köztük reál-, természet- és társadalomtudományok – releváns ismereteit is magában foglalja, ötvözi, ezért alkalmas a holisztikus, átfogó kutatások végzésére is, ami a stratégiai tervezőmunkának elengedhetetlen feltétele.

Gyakorlati érvek

Az iparbiztonság környezeti fenntarthatóságban betöltött gyakorlati szerepének igazolásához a katasztrófavédelem megelőzésre, védekezésre, valamint helyreállításra irányuló feladatrendszeréből célszerű kiindulni.[15]

[11] Sibalin 2022: 36–37.
[12] Baranyai–Csernus 2018: 243.
[13] ITM – Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal 2021: 27., 43.
[14] United Nations Educational, Scientific and Cultural Organization 2020: 28.
[15] Sibalin 2022: 38.

Ennek megfelelően az iparbiztonság feladata kiterjed az üzemzavarok és súlyos ipari balesetek kialakulásának a megelőzésére, amelynek célja az Országos Katasztrófavédelmi Főigazgatóság honlapja szerint „a különböző veszélyek, kockázatok bekövetkezésének elkerülése, a károsító hatások megszüntetése vagy csökkentése, valamint az eseménykezelés feltételeinek biztosítása".[16] A katasztrófavédelmi szakemberek már több esetben tapasztalhatták meg testközelből a súlyos, havériajellegű környezetszennyezések természetkárosító hatásait.[17] E veszélyhelyzeti kibocsátások rövid időn belül képesek kiterjedt és nemritkán maradandó környezetkárosodást okozni.[18] A kisebb havériaesemények azonban szintén relevánsak lehetnek a környezeti fenntarthatóság szempontjából: a veszélyes anyagok gyártásával, szállításával, tárolásával és felhasználásával összefüggő kevésbé súlyos balesetek, üzemzavarok tulajdonképpen mindennapos események, amelyek során környezetre káros anyagok kerül(het)nek a külvilágba.[19] Mind a súlyos pusztítást okozó, mind az alacsonyabb mértékű kibocsátással járó balesetek, üzemzavarok megelőzésével az iparbiztonsági szakterület gyakorlatilag újabb környezeti problémák kialakulását akadályozza meg, illetőleg csökkenti bekövetkezésük kockázatát, amivel érdemben járul hozzá a fenntarthatósághoz.[20]

A védekezés katasztrófavédelmi feladata környezeti fenntarthatósági stratégiai szempontból lényegében az alkalmazkodással áll összefüggésben. A természet és az emberiség közötti egyensúly felborulásából[21] fakadó környezeti problémák – köztük a szélsőséges időjárási viszonyok, klímazavarok – ugyanis veszélyeztethetik az ipari létesítmények és rendszerelemeik épségét, üzemszerű működését, ami extrém esetben akár súlyos katasztrófák kiváltó oka is lehet. E megváltozott feltételekhez tehát az ipari infrastruktúráknak, illetve azok üzemeltetőinek is alkalmazkodnia kell, annak részeként pedig védekezni is szükséges az újszerű környezeti problémákkal szemben.[22]

Végül a már megvalósult, veszélyes anyagokkal kapcsolatos balesetek esetén a helyreállítás katasztrófavédelmi feladata keretében az iparbiztonság szakemberei – többek között – a sérült infrastruktúrák javítását, mentesítési feladatok végrehajtását,[23] a környezetbe került szennyeződések semlegesítését, illetve kivonását végzik, amivel érdemben járulnak hozzá a globális környezeti egyensúly helyreállításához is.[24]

16 BM–OKF [é. n. a.].
17 BM–OKF [é. n. b.].
18 Sibalin 2022: 39.
19 Szakál et al. 2020.
20 Sibalin 2022: 39.
21 Vidékfejlesztési Minisztérium 2011.
22 Sibalin 2022: 41.
23 Hoffmann et al. 2015.
24 Sibalin 2022: 42.

2. táblázat: Az iparbiztonság (környezeti) fenntarthatóságban betöltött stratégiai jelentőségének szemléltetése

Általános fenntarthatósági értékelés	**Környezeti fenntarthatóság**	
	Elméleti érvek	**Gyakorlati érvek**
Emberélet és egészség védelme (humán dimenzió)	Stratégiaalkotási alapok megléte	Környezeti problémák megelőzése
Környezet védelme (környezeti dimenzió)	Ökológiaiválság-kezelési szempont	Környezeti problémákkal szembeni védekezés
Anyagi javak és szolgáltatások védelme (gazdasági és társadalmi dimenzió)	Multidiszciplináris jelleg	Környezeti egyensúly helyreállítása

Forrás: Sibalin Iván szerkesztése

Az energiaipari-biztonság helye a környezeti dimenzió jövőképéhez vezető folyamatban

A fenntarthatósági stratégiai gondolkodásban az energiaágazat legtöbbször jellemzően a környezetvédelem – kiváltképpen éghajlatváltozás elleni küzdelem – és a normálüzemi kibocsátások kontextusában jelenik meg, míg az energetikai rendszerek és rendszerelemek sérüléseiből eredeztethető szennyezésekre kevesebb hangsúly helyeződik. Ezzel összhangban a hazai és nemzetközi szintű fenntartható fejlődési és egyéb környezetvédelmi stratégiák lényegi eleme az energiatermeléssel és -felhasználással kapcsolatos környezetszennyezés problémája, különösen a fosszilis energiahordozók elégetését kísérő hatalmas mennyiségű szén-dioxid-kibocsátás üvegházhatása, és az ennek kezelését szolgáló stratégiai célok, részcélok, szakpolitikai eszközök meghatározása. Tipikusan ilyen célként említhető a karbonsemlegesség elérése, ennek részeként a fosszilis energiát fokozatosan felváltó megújulóenergia-termelésre való áttérés, a szén-dioxid-kvóták előírása, az erdősítési programtervek ütemezése stb.

A környezeti fenntarthatóság stratégiai jövőképével kapcsolatos diskurzusban a normálüzemi és veszélyhelyzeti kibocsátások között tapasztalható aránytalanságnak több magyarázata is lehet. Egyrészt kétségtelen, hogy az energetikai létesítmények normálüzemi kibocsátásával összefüggő legfőbb aggály a környezet, illetve a légkör szennyezése, amelynek folyamata lényegesen könnyebben prognosztizálható, számszerűsíthető és modellezhető, mint a számos bizonytalanságtól függő, rendkívüli és nemritkán véletlenszerű veszélyhelyzeti működés károsanyag-kibocsátása. Másrészt a haváriaesemények során – a baleset jellegétől és súlyosságától függően, nem mellékesen az emberi élet, egészség károsodása és az anyagi javak sérülése miatt – jelentős mértékben felerősödhetnek a humán és a társadalmi, illetve a gazdasági dimenziót érő hatások, negatív következmények miatti aggodalmak, háttérbe szorítva a környezetvédelmi megfontolásokat. Harmadrészt az ipari balesetek és üzemzavarok megelőzésének, az azokkal szembeni védekezésnek és következményei helyreállításának

sokszor szűk fókuszú, csupán operatív-technikai feladatokként történő értelmezése nehezen illeszthető a stratégiák tág, filozófiai-politikai jellegű narratíváiba (3. táblázat).

3. táblázat: A veszélyhelyzeti működés környezeti fenntarthatósági stratégiai tervezésbe való bevonásának korlátai

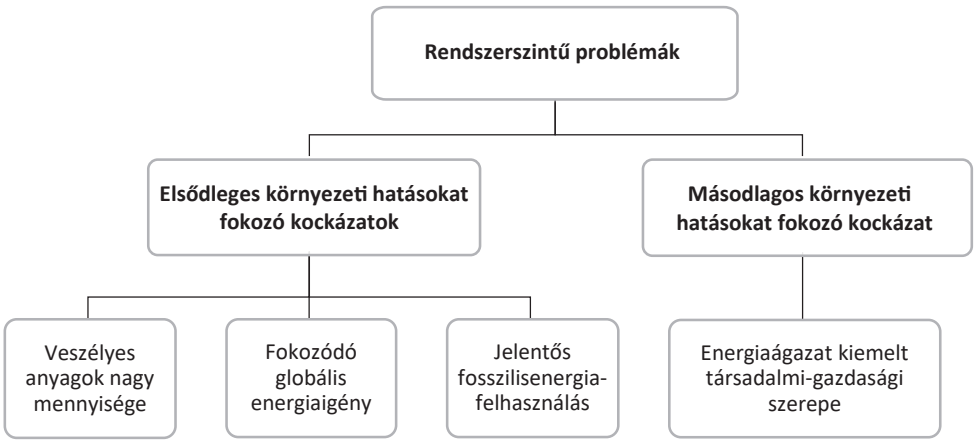
1.	Előrejelezhetőség és modellezhetőség korlátozottsága
2.	Humán, társadalmi, gazdasági hatások dominálhatnak
3.	Operatív-technikai és filozófiai-politikai megközelítés közötti feszültség

Forrás: Sibalin Iván szerkesztése

Mindazonáltal tényként konstatálható – egyebek mellett történeti tapasztalatok alapján – az is, hogy a súlyos energiaipari katasztrófák képesek rendszerszintű, azaz stratégiai keretek között értelmezhető problémákat okozni, és ezek részeként negatív hatásokat gyakorolni a természeti környezetre. A balesetek károsanyag-kibocsátásai tipikusan elsődleges környezeti hatásokkal járnak. Bekövetkezésük kockázatát erősíti, hogy az energiaágazat működtetése hatalmas mennyiségű veszélyes – köztük gyúlékony, robbanékony, ózonréteget károsító – anyag használatával jár napjainkban is. Ezzel párhuzamosan az emberiség energiaszükséglete folyamatosan nő: a Nemzetközi Energiaügynökség 2025-ös jelentése szerint a globális energiakereslet 2024-ben 2,2%-kal nőtt az előző évhez képest, ami közel 1%-kal meghaladja a 2013 és 2023 közötti időszak 1,3%-os éves átlagos növekedési szintjét.[25] Bár a biztonsági szempontból lényegesen alacsonyabb kockázattal járó megújuló energia felhasználását célzó stratégiai irányok nyilvánvalóan mérsékelik az energiaigény növekedését kísérő energiaipar-biztonsági aggályokat, a kifejezetten balesetveszélyes fosszilisenergia-felhasználás a globális energiamixnek továbbra is jelentős hányadát teszi ki (2024-ben 86,7%-át).[26]

A rendszerszintű problémákat illetően további lényeges szempont az energiaágazat más ágazatokhoz viszonyított kiemelt társadalmi és gazdasági jelentősége. Nem túlzás ugyanis azt állítani, hogy a kritikus szervezetek ellenálló képességéről szóló 2024. évi LXXXIV. törvény 1. mellékletében nevesített valamennyi ágazat funkcionálása lényegében az energetikai rendszerek és rendszerelemek épségétől, működésének minőségétől függ. Az energiaellátás korlátozottsága vagy átmeneti kiesése tulajdonképpen az összes többi ágazat működését is akadályozza, illetve szélsőséges esetben akár el is lehetetlenítheti. Az energiaágazat társadalmi szerepe különösen azon alágazatok kapcsán válik szembeötlővé, amelyek akár rövid időre történő kiesésével elemi életfeltételek ellátása szűnhet meg, mint például az ivóvíz-szolgáltatás.[27] A más ágazatok energiahiány miatti korlátozottsága – minden közvetlen és közvetett társadalmi, gazdasági következménye mellett – bizonyos esetekben másodlagos környezeti hatásokat is generálhat (1. ábra).

[25] International Energy Agency 2025: 8.
[26] Neufeld 2025.
[27] Sibalin 2022: 29.



1. ábra: Energiaipari katasztrófákkal kapcsolatos rendszerszintű (stratégiai keretek között értelmezhető) aggályok egyes példái
Forrás: Sibalin Iván szerkesztése

Az energetikai létesítmények veszélyhelyzeti működése témakörének a fenntartható fejlődés környezeti dimenzióját érintő stratégiai tervezésbe való bevonásával kapcsolatos korlátok ellenére, az említett rendszerszintű aggályok mind azt bizonyítják, hogy az energiaipari-biztonságnak helye van a környezeti fenntarthatóság jövőképével összefüggő stratégiai gondolkodásban.

Befejezés

Napjaink technológiai és egyéb globális szintű kihívásai közepette konstans és hosszú távú aggályként vannak jelen bolygónk életében a természeti környezettel kapcsolatos kockázatok, amelyek kezelése egyre sürgetőbb, és sokrétű beavatkozást igényel. A fenntartható fejlődés (környezeti dimenzió) tekintetében az iparbiztonság is stratégiai jelentőségű szakterületként értelmezhető, ugyanis annak elhanyagolása, illetve a releváns stratégiai tervezésből való kiiktatása minden bizonnyal meghiúsítaná vagy jelentősen megnehezítené a környezeti fenntarthatóság jövőképének megvalósítását. Az iparbiztonság ebbéli funkciója elméleti és gyakorlati érvekkel is alátámasztható. Az előbbiek közé sorolható a fenntarthatósági és ipari biztonsági szempontok egyidejű megléte a hatályos stratégiai keretrendszerben, az iparbiztonság absztrakt ökológiai válságkezelési szerepe, valamint a szakterület multidiszciplináris jellege. Az utóbbiak közé tartozik az iparbiztonságnak a környezeti problémák megelőzésében, a már meglévő környezeti problémákkal szembeni védekezésben, valamint a környezeti egyensúly helyreállításában betöltött rendeltetése.

Kifejezetten az energiaipari-biztonságnak a környezeti fenntarthatósághoz való viszonyulását illetően megállapítható, hogy az azzal kapcsolatos diskurzusban e részszakterület csupán korlátozottan jelenik meg. Így a fenntartható fejlődést célzó stratégiai tervezésben is a normálüzemi kibocsátások témaköre dominál, szemben

az energetikai rendszerek veszélyhelyzeti működésével. Ennek konkrét okai között említhető a rendkívüli események, illetve az azokból fakadó károsanyag-kibocsátások előrejelezhetőségének és modellezhetőségének korlátozottsága, a már megvalósult katasztrófák, súlyos balesetek nem környezeti – azaz humán, társadalmi és gazdasági – hatásai, valamint a veszélyhelyzeti működéssel összefüggő feladatok „stratégiaidegen" megközelítése. Ugyanakkor az is megállapítható, hogy az energiaágazat haváriajellegű eseményei mégis csak stratégiai szinten értelmezhető problémákat generálhatnak. A katasztrófák elsődleges környezeti hatása a havária következtében előállt szennyezés. Ennek kockázatát fokozza annak ténye, hogy az energiaágazat hatalmas mennyiségű veszélyes anyaggal működik, az energiaigény globális szinten növekszik, valamint, hogy a balesetveszélyes fosszilisenergia-felhasználás továbbra is számottevő mértékű. Emellett az energiaágazat kulcsfontosságú szerepet tölt be a többi szektor funkcionálásában is, ezért az ellátásbiztonsági akadályok – a társadalmi és gazdasági mellett – akár másodlagos környezeti hatásokat is előidézhetnek.

A cikksorozat következő része már megtörtént balesetek következményeinek bemutatásán keresztül vizsgálja és értékeli az energiaipari-biztonság és a környezeti fenntarthatóság egyes összefüggéseit, az iparbiztonság stratégiai jelentőségét megalapozó gyakorlati érvek mentén.

A jelen cikkel kapcsolatos kutatómunka 2025. szeptember 30-án zárult.

Felhasznált irodalom

Baranyai Gábor – Csernus Dóra Ildikó szerk. (2018): *A fenntartható fejlődés és az állam feladatai.* Budapest: Dialóg Campus. Online: https://vtk.uni-nke.hu/document/vtk-uni-nke-hu/webXS_PDF_ATMA_Fenntarthato_fejlodes.pdf

BM – Országos Katasztrófavédelmi Főigazgatóság [é. n. a.]: *Lakosságfelkészítés.* Online: www.katasztrofavedelem.hu/62/lakossagfelkeszites

BM – Országos Katasztrófavédelmi Főigazgatóság [é. n. b.]: *Környezetvédelem és kéménysepréss.* Online: https://kemenysepres.katasztrofavedelem.hu/tajekoztatok/kornyved

Érces Gergő – Vass Gyula – Ambrusz József (2023): Épületek károsító hatásokkal szembeni rezilienciájának jellemzői. *Polgári Védelmi Szemle,* 15(különszám), 117–130. Online: https://kvi.uni-nke.hu/document/kvi-uni-nke-hu/%C3%96sszerakott%20PV%20Szemle%20cikkek_02_24_Szerkesztett.pdf#page=117

Hoffmann Imre et al. (2015): Iparbiztonság Magyarországon. *Védelem Online: Tűz- és Katasztrófavédelmi Szakkönyvtár,* 22(1). Online: www.vedelem.hu/letoltes/anyagok/549-dr-hoffmann-imre-dr-levai-zoltan-dr-katai-urban-lajos-dr-vass-gyula.pdf

International Energy Agency (2025): *Global Energy Review 2025.* Online: https://iea.blob.core.windows.net/assets/5b169aa1-bc88-4c96-b828-aaa50406ba80/GlobalEnergyReview2025.pdf

ITM – Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal (2021): *Magyarország kutatási, fejlesztési és innovációs stratégiája 2021–2030.* ITM. Online: https://nkfih.gov.hu/hivatalrol/strategia-alkotas/kutatasi-fejlesztesi-innovacios-strategia

Kátai-Urbán Lajos (2014): Súlyos ipari balesetek megelőzését és a felkészülést célzó jogintézmények egységes rendszerbe foglalása. *Hadmérnök,* 9(4), 94–105. Online: www.hadmernok.hu/144_10_katai_urbanl_1.pdf

Nemzeti Fenntartható Fejlődési Tanács (2012): *Nemzeti Fenntartható Fejlődési Keretstratégia 2012–2024. A 18/2013. (III. 28.) OGY határozat melléklete.* Online: https://njt.hu/jogszabaly/2013-18-30-41

Neufeld, Dorothy (2025): Chart: What Powered the World in 2024? *Visual Capitalist,* 2025. augusztus 22. Online: www.visualcapitalist.com/what-powered-the-world-in-2024/

Report of the World Commission on Environment and Development: Our Common Future (1987). http://www.un-documents.net/our-common-future.pdf

Sibalin Iván (2022): *Az energetikai rendszerek fenntartható működésével kapcsolatos iparbiztonsági tevékenységek stratégiai célú kutatása és fejlesztése.* PhD-disszertáció. Budapest: NKE Katonai Műszaki Doktori Iskola. Online: https://tudasportal.uni-nke.hu/xmlui/bitstream/handle/20.500.12944/19565/sibalin_ivan_doktori_ertekezes.pdf

Szakál Béla et al. szerk. (2020): *Módszertani kézikönyv a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezéssel foglalkozó gyakorló szakemberek részére.* Budapest: Hungária Veszélyesáru Mérnöki Iroda.

Teknős László – Kóródi Gyula (2016): A vízzel kapcsolatos veszélyeztetettség éghajlatváltozással kapcsolatos aspektusainak katasztrófavédelmi szempontú elemzése és kiértékelése II. *Hadmérnök,* 11(3), 83–96. Online: http://hadmernok.hu/163_07_teknos.pdf

United Nations Educational, Scientific and Cultural Organization (2020): *Education for Sustainable Development: a Roadmap.* Paris: UNESCO. Online: https://doi.org/10.54675/YFRE1448

Vidékfejlesztési Minisztérium (2011): *Nemzeti Környezettechnológiai Innovációs Stratégia 2011–2020. 1307/2011. (IX. 6.) Korm. határozat melléklete.* Online: http://njt.hu/cgi_bin/njt_doc.cgi?docid=140750.204955

World Economic Forum (2025): *The Global Risks Report 2025.* 20th Edition. Geneva. Online: https://reports.weforum.org/docs/WEF_Global_Risks_Report_2025.pdf

Jogi forrás

1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról. 1. melléklet. Online: https://njt.hu/jogszabaly/2020-1163-30-22

HADMÉRNÖK
VÉDELEMGAZDASÁG

20. évfolyam (2025) 4. szám 161–180.
DOI: 10.32567/hm.2025.4.10

Szöllősi Annamária[1]

Az innováció mint stratégiai fegyver

Az amerikai és a kínai technonacionalista megközelítések összehasonlítása

Weaponising Innovation

A Comparative Analysis of U.S. and Chinese Techno-Nationalist Approaches

Absztrakt

A kortárs geopolitikai versengésben a technológia, az innováció és a nemzetbiztonság szoros összefonódása a technonacionalizmus fogalmában nyer elméleti keretet. E folyamatok középpontjában az Egyesült Államok és a Kínai Népköztársaság nagyhatalmi stratégiai versengése áll, amely a védelmi innovációt és a technológiai fölény megszerzését a nemzetbiztonság és a gazdasági versenyképesség alapfeltételeként értelmezi. A védelmi innovációs ökoszisztémák összehasonlító elemzése rávilágít a nemzeti kutatás-fejlesztési modellek szerkezeti eltéréseire, valamint a finanszírozási mechanizmusok és a stratégiai irányítás eltérő logikáira. A tanulmány áttekinti a technonacionalizmus kialakulását és elméleti alapjait, valamint feltárja annak gyakorlati megnyilvánulásait a nagyhatalmi versengésben. Az elemzés rámutat, hogy a technológiai önállóság és a stratégiai szuverenitás iránti törekvések a geopolitikai, gazdasági és tudományos dinamika központi mozgatórugóivá váltak, és a 21. század világrendje egyre inkább a technonacionalista törekvések mentén formálódik.

Kulcsszavak: feltörekvő és diszruptív technológiák, védelmi innováció, védelmi kutatás-fejlesztés, stratégiai verseny, technonacionalizmus

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem Hadtudományi Doktori Iskola, e-mail: szollosi.annamaria@outlook.hu

Abstract

In contemporary geopolitical competition, the close interconnection between technology, innovation, and national security is theoretically framed by the concept of techno-nationalism. At the core of these processes lies the great-power strategic rivalry between the United States and the People's Republic of China, in which defence innovation and the pursuit of technological superiority are regarded as prerequisites for both national security and economic competitiveness. The comparative analysis of defence innovation ecosystems highlights structural differences in national research and development models, as well as the divergent logics of financing and strategic governance. The study further reviews the emergence and theoretical foundations of techno-nationalism and explores its practical manifestations in the context of great-power competition. The analysis demonstrates that efforts toward technological autonomy and strategic sovereignty have become central drivers of geopolitical, economic, and scientific dynamics, shaping the 21st-century global order increasingly along techno-nationalist lines.

Keywords: emerging and disruptive technologies, defence innovation, defence research and development, strategic competition, techno-nationalism

Bevezetés

A 21. század biztonsági környezetét a hibrid hadviselés komplex formái jellemzik, amelyek a katonai és nem katonai – politikai, gazdasági, technológiai és információs – eszközök integrált alkalmazásán alapulnak. Céljuk nem kizárólag a katonai fölény megszerzése, hanem a politikai nyomásgyakorlás, a gazdasági befolyás erősítése, az állami működés destabilizálása, valamint a döntéshozatali mechanizmusok torzítása.[2] A jövőbeli, előre nem látható fenyegetések következtében az anticipatív fenyegetéskezelés került a biztonsági racionalitás középpontjába. Ezzel párhuzamosan a biztonság fogalma is kitágult, a hagyományos katonai fenyegetések mellett egyre nagyobb hangsúlyt kapnak a gazdasági, ökológiai, digitális és társadalmi kockázatok.[3] Az államközi hibrid konfliktusok egyik sajátos formáját képezi a védelmi innovációk terén kibontakozó versengés, amely a technológiai fölény megszerzését geopolitikai céllá emelte. Ez a tendencia szorosan összefügg a globális rend átalakulásával, amelyet egyre inkább a poliarchikus világrend jellemez. Ebben a struktúrában a hatalom több központban koncentrálódik, és már nem kizárólag állami szereplők, hanem technológiai vállalatok, kutatóintézetek és más transznacionális szereplők is folyamatos versengésben és részben együttműködésben formálják a globális erőviszonyokat.[4] A poliarchikus világrend decentralizált hatalmi viszonyai és a többpólusú verseny bonyolult és kiszámíthatatlan biztonsági környezetet eredményeztek, amely a stratégiai tervezést, valamint a nemzeti érdekérvényesítést is új alapokra helyezte.

[2] Boda 2022; Boda 2025; Háber 2022.
[3] Remek 2023; Szöllősi 2025: 170–171.
[4] Boda 2022; Boda 2025.

A Nemzetközi Stratégiai Tanulmányok Intézete (International Institute for Strategic Studies, IISS) a védelmi innovációt tudatos technológiai és stratégiai megújulásként értelmezi, amelynek révén az államok a változó világrendre reagálnak, hogy megőrizzék vagy megszerezzék hatalmi pozíciójukat. Az IISS szerint a védelmi innovációs politikák prioritásait négy, egymással kölcsönhatásban álló tényező alakítja:

- a fenyegetettség és sebezhetőség percepciója;
- a politikai, katonai és társadalmi támogatás együttes megléte;
- az innovációt irányító szervezeti és kormányzási struktúrák;
- az innovációba irányuló beruházások volumene és jellege.[5]

Az innováció nem csupán technológiai újításként értelmezhető, hanem a biztonságpolitikai gondolkodásmódot is alakítja, aminek felfogása fokozatosan elmozdult a gazdasági alapú kutatás-fejlesztés-innováció (K+F+I) paradigmájától a társadalmi és politikai diskurzusok irányába. Az *innovatív biztonság* mára stratégiai kényszerré vált, amely meghatározza a globális erőviszonyokat és formálja a biztonsági kormányzás logikáját. A biztonság és innováció viszonya ugyanakkor rávilágít a jelenség összetett és ellentmondásos természetére is: az innováció egyszerre szolgálhatja a bizonytalanság csökkentését, miközben új biztonsági kockázatokat is teremthet. Válsághelyzetekben a biztonsági nyomás ösztönzi a technológiai fejlesztéseket, míg stabil környezetben épp a biztonsági megfontolások szabhatnak határt az innovációnak.[6]

A tanulmány kvalitatív elemzési megközelítést alkalmaz, amely ötvözi a szakirodalmi áttekintést és a dokumentumelemzést. Elsődleges forrásként a nemzetközi szakirodalom, vezető kutatóintézetek jelentései, politikai és kormányzati dokumentumok, valamint nyilvánosan elérhető statisztikai adatok szolgáltak. Mivel a technonacionalizmus témaköre a magyar szakirodalomban szinte teljesen feldolgozatlan, a tanulmány a nemzetközi szakirodalom áttekintése és elemzése révén a hazai tudományos diskurzushoz kíván hozzájárulni.

A védelmi innováció globális trendjei és strukturális átalakulása

A fegyveres erők és a katonai tervezési rendszerek világszerte strukturális átalakuláson mennek keresztül annak érdekében, hogy lépést tudjanak tartani a modern hadviselés gyorsaságával és az információtechnológiai környezet kihívásaival, ugyanakkor a technológiai fölény megőrzése is alapvető fontosságú a katonai erő szempontjából. A változás középpontjában a feltörekvő és diszruptív technológiák[7] (*emerging and disruptive technologies,* EDT) állnak, amelyek a katonai modernizáció hajtóerejét jelentik. Az EU 2021/697 rendeletének meghatározása szerint a *forradalmi védelmi technológia (disruptive technology for defence)* „olyan továbbfejlesztett vagy teljesen új technológia, amely gyökeres változásokat eredményez, ideértve a védelmi kérdések

[5] Soare–Pothier 2021: 5.
[6] Haddad – Vorlíček – Klimburg-Witjes 2024.
[7] A tanulmány a diszruptív kifejezést a mindent felforgató értelemben használja, utalva arra, hogy ezen technológiák potenciálisan rendszert átalakító, a geopolitikai és nemzetbiztonsági viszonyokat radikálisan befolyásoló hatásúak.

tekintetében az elméleti és gyakorlati síkon történő paradigmaváltást is, többek között azzal, hogy felváltja vagy elavulttá teszi a meglévő védelmi technológiákat."[8] A digitális, autonóm, mesterséges intelligencián (AI) alapuló és hálózatalapú rendszerekre épülő technológiai fejlődés új alapokra helyezi a hadviselést. Az új képességek megjelenése érdemben módosíthatja a konfliktusok lefolyását, és kikényszeríti a hadseregek stratégiai gondolkodásának és tervezési elveinek újradefiniálását.[9] Az e területeken megszerzett technológiai fölény stratégiai előnyt jelent, amely túlmutat a hagyományos katonai dominancián,[10] és a következő években várhatóan átalakítja a nemzetközi biztonsági környezetet, egyre meghatározóbb szerepet játszva a globális hatalmi egyensúly átrendeződésében.[11]

A védelmi innovációs dinamika átalakulása

A globális biztonsági környezet és a haditechnika gyors ütemű fejlődése új dimenziókat nyitott a védelmi innováció terén. A modern hadviselés már nem csupán a hagyományos fegyverrendszerekre és katonai doktrínákra épül, hanem egyre szorosabban kapcsolódik a civil szektor technológiai eredményeihez és K+F+I-tevékenységéhez. A tudományos és technológiai fejlesztések súlypontja fokozatosan áthelyeződött a hagyományos állami védelmi szektorból a civil innovációs központokba.[12] A kettős felhasználású *(dual-use)* technológiák térnyerése komplex stratégiai környezetet eredményezett. A fejlett védelmi rendszerek és új generációs fegyverek kifejlesztésének elsődleges forrása továbbra is a védelmi célú K+F+I-költségvetés, amely azonban egyre inkább kölcsönhatásban áll a civil szektor innovációs folyamataival. A K+F+I-ráfordítások hatása kétirányú: egyrészt a növekvő katonai költségvetések közvetlenül ösztönzik a haditechnikai fejlesztéseket, másrészt a civil szektorban létrejövő technológiák kettős felhasználhatósága alapvetően befolyásolja a katonai képességek fejlődését.

A Stockholmi Nemzetközi Békekutató Intézet (Stockholm International Peace Research Institute, SIPRI) adatai szerint már tizedik éve folyamatos a globális katonai kiadások emelkedése, amely 2015 és 2024 között összességében 37%-kal nőtt. A 2024-es év történelmi csúcsot jelentett, amikor a kiadások elérték a 2,718 milliárd dollárt, ami éves szinten 9,4%-os növekedést jelent, és a világ GDP-jének 2,5%-át tette ki. A SIPRI adatai szerint a világ öt legtöbbet költő állama – sorrendben az Egyesült Államok, Kína, Oroszország, Németország és India – együttesen a globális katonai kiadások mintegy 60%-át fedezi. Az Egyesült Államok a világ legnagyobb védelmi költségvetésével rendelkezik: a 2024-es 997 milliárd dollár védelmi kiadás több mint háromszorosa a második helyen álló Kína hivatalosan közzétett 314 milliárd dolláros védelmi büdzséjének.[13] Ugyanakkor a hivatalos kínai védelmi költségvetés évek óta

[8] Az Európai Parlament és a Tanács (EU) 2021/697 rendelete (2021. április 29.).
[9] Fetter–Sankaran 2024: 254; Vuk 2025: 15.
[10] Reding–Eaton 2020: 7.
[11] Soare–Pothier 2021: 3.
[12] Vuk 2025: 14.
[13] Liang et al. 2025: 1.

viták tárgyát képezi, mivel vélhetően nem fedi le a teljes katonai kiadási spektrumot.[14] Az amerikai Védelmi Minisztérium (Department of Defense, DoD) becslése szerint a teljes kínai védelmi költségvetés akár 40–90%-kal is meghaladhatja a hivatalosan közölt adatokat, és elérheti a 330–450 milliárd dollárt.[15]

A globális K+F-beruházások és technológiai erőviszonyok átrendeződése

A globális K+F-beruházások és a technológiai innovációk élmezőnyében fokozatos átrendeződés figyelhető meg. Az Egyesült Államok az 1960-as években még 69%-os részesedéssel uralta a globális K+F-piacot, azonban ez az arány 2016-ra mindössze 28%-ra esett vissza.[16] Az amerikai technológiai dominancia visszaszorulása összefügg a globális technológiai verseny kiéleződésével, valamint a feltörekvő gazdaságok – elsősorban Kína – növekvő súlyával. Kína K+F kiadásai évtizedek óta folyamatosan növekednek, ezért a két listavezető ország ráfordításai közötti különbség egyre szűkül. A technológiai önállóság elérése érdekében az 1990-es évektől folyamatos, jelentős beruházások révén Kína a 2000-es évekre már a globális K+F-tér meghatározó szereplőjévé vált.

A technológiai átrendeződés folyamatát az Ausztrál Stratégiai Politikai Intézet (Australian Strategic Policy Institute, ASPI) a tudományos publikációk száma, idézettségi mutatói és a kutatóintézetek dominanciája szerint értékelte. Az ASPI 21 évet (2003–2023), valamint 64 technológiai területet felölelő kutatása hasonló következtetésre jutott: az elmúlt két évtizedben jelentős átalakulás ment végbe a globális technológiai erőviszonyokban. A legmarkánsabb tendencia az Egyesült Államok fokozatos visszaszorulása, és ezzel párhuzamosan Kína gyors és tudatos technológiai felemelkedése. A 2000-es évek elején az Egyesült Államok még szinte minden vizsgált szektorban vezető szerepet töltött be, azonban 2019 és 2023 között a tendencia megfordult, és a vizsgált 64 technológiai területből 57-ben Kína szerzett vezető pozíciót.[17]

A Szellemi Tulajdon Világszervezete (World Intellectual Property Organization, WIPO) Globális Innovációs Indexe a vezető nemzetközi referencia az innovációs teljesítmény mérésére és összehasonlítására. A 2025-ös adatok alapján mindkét ország a globális innovációs élvonalban szerepel, bár erősségeik eltérő innovációs területekre koncentrálódnak. Az USA a 3. helyét megőrizve továbbra is stabil vezető pozíciót tölt be, ugyanakkor innovációs növekedési üteme – különösen a K+F-befektetések terén – lassul. Az országban működnek a világ legnagyobb K+F-befektető vállalatai, és kiemelkedően erős a San Francisco – San José-térség technológiai központja, a Szilícium-völgy. Kína esetében a trendek dinamikus növekedést mutatnak, különösen a technológiai teljesítmény és az innovációs régiók fejlődése terén. 2025-ben először került be a tíz leginnovatívabb ország közé, amit többek között a szabadalmi aktivitás, a technológiaexport, valamint az ország innovációs és technológiai központjának,

[14] Beaver 2025; Kisvári 2024: 209.
[15] DoD 2024a: 148.
[16] Reding–Eaton 2020: 30.
[17] Wong Leung – Robin – Cave 2024: 7.

a Sencsen–Hongkong–Kanton régió (Shenzhen – Hong Kong – Guangzhou) gyors fejlődésének köszönhet. Ugyanakkor a WIPO értékelése rámutat Kína innovációs profiljának kiegyensúlyozatlanságára is: a kiemelkedő kutatási és technológiai teljesítmény erős kontrasztban áll az intézményi minőség, jogbiztonság és kormányzati hatékonyság terén mutatott gyengébb mutatókkal.[18]

Az Egyesült Államok védelmi innovációs ökoszisztémája

Az Egyesült Államok védelmi innovációs ökoszisztémája a nemzeti hatalom és a technológiai fölény fenntartásának egyik legfontosabb pillére, amely a katonai képességek fejlesztését, az innováció ösztönzését és a gyors technológiai adaptációt szolgálja. A fejezet e rendszer felépítését, működési logikáját és stratégiai jelentőségét vizsgálja, kiemelve, hogy miként járul hozzá az Egyesült Államok globális katonai-technológiai vezető szerepének fenntartásához.

Védelmi K+F+I-modell

Az Egyesült Államok decentralizált és többpólusú tudományos és technológiai irányítási rendszerében az állam, az akadémiai szféra és a magánszektor egyaránt aktív szerepet játszik. A rendszert a versenyalapú K+F+I jellemzi, amelyben a magánvállalatok vezető szerepet töltenek be, míg az állam elsősorban finanszírozóként, szabályozóként és koordinátorként működik. A köz- és magánszféra szoros együttműködése az amerikai technológiai fölény egyik alapvető tényezője. A vezető technológiai vállalatok, mint a Google, az IBM, a Microsoft vagy a Meta, meghatározó szerepet játszanak az AI, a kvantumtechnológia, valamint a nagy teljesítményű számítástechnika területén. Ezek a cégek jelentős K+F+I-kapacitásokkal rendelkeznek, és gyakran vesznek részt kormányzati programokban is. A szövetségi kutatóintézetek és nemzeti laboratóriumok – például a NASA – szintén jelentős szerepet játszanak, különösen az űrkutatás és a műholdas technológiák fejlesztése terén.[19]

A Nemzeti Tudományos Alap (National Science Foundation, NSF) kulcsszerepet tölt be a magas szintű tudományos kutatás előmozdításában. Elsősorban az alapkutatások támogatásáért felel, pályázati úton, versenyalapú elbírálás alapján. Az országos szintű K+F-programok koordinációját a Tudomány- és Technológiapolitikai Hivatal (Office of Science and Technology Policy, OSTP) végzi, amelynek vezetője az amerikai elnök tudományos főtanácsadója. Az OSTP feladatai közé tartozik a szövetségi K+F-prioritások meghatározása, valamint a stratégiai technológiai területeken az Egyesült Államok vezető szerepének biztosítása.[20] Az OSTP munkáját kiegészíti az 1993-ban létrehozott Nemzeti Tudomány- és Technológiai Tanács (National Science and Technology Council, NSTC), amely a végrehajtó hatalom szintjén intézményesíti a tudományos

[18] WIPO 2025: 55–56.
[19] Wong Leung – Robin – Cave 2024: 5.
[20] The White House [é. n.].

és technológiai döntéshozatal koordinációját. Az NSTC célja a szövetségi ügynökségek K+F-tevékenységeinek összehangolása az elnöki prioritásokkal, különös tekintettel a gazdasági versenyképesség és a nemzetbiztonság erősítésére.[21]

A védelmi innováció egyik legfontosabb intézményi pillére a Fejlett Védelmi Kutatási Projektek Ügynöksége (Defense Advanced Research Projects Agency, DARPA),[22] amelyet 1958-ban Dwight D. Eisenhower elnök hozott létre válaszul a Szputnyik-1 felbocsátására. Ez az esemény a hidegháborús technológiai verseny egyik fordulópontját jelentette, és az amerikai innovációs rendszer stratégiai újraszervezését is kiváltotta. Az ügynökség célja azóta is változatlan: „megelőzni és előidézni a technológiai meglepetéseket", és stratégiai előnyt biztosítani az amerikai haderő számára. A Hadügyminisztérium (Department of War, DoW) alá rendelt, önálló költségvetéssel rendelkező szervezet éves forrásait a Kongresszus hagyja jóvá. A DARPA 2024. évi költségvetése mintegy 4,12 milliárd dollár volt, amely 1,5%-os növekedést jelentett az előző évhez képest.[23] A DARPA ösztönzi a nagy kockázatú, magas megtérülésű projekteket, amelyek célja „nem a fokozatos előrelépés, hanem az átalakító változás elérése". Működési modellje eltér a hagyományos kutatóintézetekétől: nem rendelkezik saját laboratóriumokkal, fejlesztéseit teljes mértékben külső – akadémiai és ipari – partnereken keresztül valósítja meg. A programok kidolgozását és irányítását mintegy száz, nagy fokú autonómiával rendelkező programmenedzser végzi. A decentralizált és célorientált DARPA-modell a technológiai fejlődés üteméhez és irányváltásaihoz illeszkedő dinamikus reagálást tesz lehetővé.[24]

A védelmi innovációs stratégia

A *Peace Through Strength*[25] doktrína régóta az amerikai védelmi gondolkodás meghatározó eleme. Alapelve, hogy a katonai erő és a technológiai fölény demonstrálása megelőzi a konfliktusokat, ezáltal biztosítva a stratégiai elrettentést és a nemzetközi stabilitást. A doktrína jelentős szerepet kapott a Reagan-korszakban, és a második Trump-adminisztrációban ismét hangsúlyos elemmé vált.[26] Bár az új *Nemzeti Védelmi Stratégia* még előkészítés alatt áll, várhatóan megerősíti a *Peace Through Strength* és az *America First* elvére épülő megközelítést, az ipari bázis modernizációját, valamint a nagyhatalmi verseny – különösen Kína – jelentette kihívásokra adott válaszokat.[27] Ezt a törekvést szimbolizálja az a 2025 szeptemberében kiadott elnöki rendelet is, amely a DoD másodlagos megnevezéseként visszaállította a történelmi Hadügyminisztérium elnevezést. Az intézkedés nem pusztán a katonai erődemonstrációt kifejező retorikai

[21] Sargent–Shea 2020: 7.
[22] Az eredetileg Advanced Research Projects Agency (ARPA) néven létrehozott ügynökséget a védelmi ügyekre való összpontosítás hangsúlyozása érdekében 1972-ben nevezték át Defense Advanced Research Projects Agency (DARPA) névre.
[23] Mosley 2024.
[24] Gallo 2021.
[25] Magyarul: béke erő révén.
[26] O'Hanlon 2025; The White House 2025a.
[27] DoW 2025a.

aktus, hanem a stratégiai kommunikáció tudatosan alkalmazott eszköze, amelynek elsődleges célja az erő és az elszántság globális színtéren való kivetítése.[28]

Az Egyesült Államok védelmi innovációs stratégiája közvetlenül szolgálja a technológiai dominancia fenntartását. A technológiai vezető szerep megőrzése kiemelt stratégiai cél, különösen a katonai és nemzetbiztonsági alkalmazások terén.[29] 2023-ban a K+F+I-szegmens a védelmi költségvetés legnagyobb arányú növekedését mutatta (+9,4%), és elérte a 151 milliárd dollárt. A 2014-ben megkezdett stratégiai átalakulás középpontjában a fejlett haditechnikai rendszerek fejlesztése és a nagyhatalmi konfliktusokra való felkészülés áll. Ennek megfelelően a védelmi prioritások fokozatosan eltolódtak a felkelések és aszimmetrikus hadviselés elleni műveletektől a konvencionális, technológiaintenzív katonai képességek fejlesztése irányába.[30] Ugyanakkor az Egyesült Államok globális biztonságpolitikai kötelezettségei megkövetelik, hogy párhuzamosan képes legyen hagyományos fegyverrendszerek nagy volumenű gyártására is. A DoW így kettős stratégiai nyomás alatt áll: miközben proaktívan fejleszti a következő generációs technológiákat, fenn kell tartania és bővítenie kell a meglévő hagyományos fegyverrendszerek gyártási kapacitásait is.[31]

Az elmúlt öt évtizedben az Egyesült Államok szövetségi K+F+I-kiadásainak közel felét a DoW kapta. A minisztérium számos innovációs és kutatási programot működtet, és meghatározó szerepet játszik a katonai technológiai fejlesztésekben. A Digitális és Mesterséges Intelligencia Főhivatal (Chief Digital and Artificial Intelligence Office, CDAO) központi szerepet tölt be az AI, az adattudomány és a digitális technológiák integrációjában.[32] Az AI-alapú megoldások védelmi célú adaptációjának felgyorsítását szolgálja a 2024-ben mintegy 100 millió dolláros induló költségvetéssel létrehozott AI Gyors Képességfejlesztő Egység (AI Rapid Capabilities Cell, AI RCC). Az egység célja az AI hadviselési és műveleti alkalmazásainak előmozdítása, különös tekintettel a parancsnoki és irányítási rendszerekre, az autonóm rendszerek fejlesztésére, a hírszerzésre, valamint a kiberhadviselésre.[33] A DoW egyik legújabb innovációs kezdeményezése a Thunderforge projekt, amely a kereskedelmi AI-rendszerek katonai alkalmazásának lehetőségeit vizsgálja. A vezető technológiai vállalatokkal (Scale AI, Microsoft, Anduril) együttműködésben megvalósuló projekt célja az operatív és stratégiai döntéshozatal felgyorsítása emberi felügyelet mellett, különösen az információs és időbeli nyomás alatt zajló hadműveletekben.[34] A DoW innovációs motorjaként a DARPA feladata, hogy előre jelezze és alakítsa a jövő hadviselését meghatározó technológiai trendeket.[35] Az ügynökség fontos szerepet játszik a kettős felhasználású technológiák fejlesztésében, különösen az információs rendszerek, a kommunikáció, a kvantumtechnológia és az AI terén. A DARPA által irányított programok – mint például a Hypersonic Air-breathing

[28] The White House 2025b.
[29] DoD 2022: 2.
[30] Tian et al. 2024: 3.
[31] DoD 2023: 8; DoD 2024b: 66.
[32] DoW 2023.
[33] DoW 2024.
[34] Vigliarolo 2025; DoW 2025b.
[35] Nature 2020.

Weapon Concept[36] vagy a Next-Generation Microelectronics Manufacturing[37] – egyszerre szolgálják a katonai elrettentés erősítését, a hadműveleti rugalmasság fokozását, valamint az Egyesült Államok technológiai vezető szerepének megőrzését.

A Kínai Népköztársaság védelmi innovációs ökoszisztémája

Kína védelmi innovációs ökoszisztémája dinamikusan átalakult, hogy erősítse technológiai önállóságát és támogassa a katonai modernizációt. A fejezet bemutatja, hogyan használja Kína központosított innovációs és védelmi rendszerét hosszú távú nemzeti stratégiája részeként a képességek gyors fejlesztésére, és miként válik mindez a globális hatalmi verseny meghatározó eszközévé, különösen az Egyesült Államokkal szemben.

A védelmi K+F+I-modell

Kína K+F-költségvetését a korlátozott nyilvános átláthatóság miatt *fekete doboznak* nevezik, amiről nehéz hiteles, összehasonlítható adatokat találni.[38] A hivatalos kínai statisztikák szerint az ország teljes K+F-ráfordítása 2024-ben 3,613 milliárd jüant tett ki, ami megközelítőleg 500 milliárd dollárnak felel meg, és 8,3%-kal haladja meg az előző évi szintet.[39] A kínai állam centralizált innovációs rendszerében a kormány stratégiai irányítóként és finanszírozóként lép fel. A technológiai fejlődést hosszú távú nemzeti stratégiák mentén alakítja, különösen olyan prioritásként kezelt, magas hozzáadott értékű szektorokban, mint a félvezetőipar, az AI és a kvantuminformatika.[40] Az állam célzott eszközökkel – például irányított befektetési alapokon, részleges vagy vegyes tulajdonosi struktúrákon és közpolitikai beavatkozásokon keresztül – formálja a magán- és félig állami vállalatok innovációs tevékenységét.[41]

A tudományos-technológiai stratégia közvetlen pártfelügyelet alatt áll, irányítását a Kínai Kommunista Párt látja el. A szektor politikai koordinációjáért a 2023-ban létrehozott Központi Tudományos és Technológiai Bizottság (Central Science and Technology Commission, CSTC) felel. A bizottság célja a nemzeti innovációs rendszer egységesítése és a technológiai önállóság erősítése. A CSTC átfogó hatáskörrel rendelkezik a K+F, az oktatás, a szellemi tulajdon kezelése, valamint az állami technológiai beruházások területén egyaránt.[42] A Kínai Tudományos Akadémia (Chinese Academy of Sciences, CAS) élen jár a hazai tudományos, technológiai és innovációs képességek

[36] Az Amerikai Légierővel (USAF) közös program levegőbelégzéses hajtóművű hiperszonikus cirkálórakéta kifejlesztését célozta, amely több sikeres repülési demonstráció után 2023-ban lezárult, és technológiai eredményei beépültek az USAF jelenleg is zajló Hypersonic Attack Cruise Missile (HACM) programjába. Vigliarolo 2022; GAO 2024.

[37] A program a Moore-törvény fizikai korlátainak megkerülésére törekszik a hagyományos 2D-chipek helyett 3D heterogén integráció (3DHI) révén különböző anyagokból és funkciókból álló chipek egymásra rétegzésével. DARPA 2022.

[38] Clapp 2022: 1.

[39] NBS 2025.

[40] Kania 2019: 85; Silk Road Hungary 2025.

[41] zhang–Lan 2022.

[42] Mok 2023; Lee 2024.

fejlesztésében. A 113 intézetet koordináló szervezetet a világ legnagyobb kutatóintézeti hálózataként tartják számon. A CAS központi, állami irányítás alatt áll, és 2023-ban 23,8 milliárd dolláros költségvetéssel gazdálkodott. Meghatározó szerepet tölt be a hosszú távú technológiai stratégia kialakításában és az innovációs erőforrások koncentrálásában, továbbá koordinálja a nemzeti technológiai célkitűzések megvalósítását. A hazai kutatásokra épülő idézési hálózat útján autonóm, belső tudományos struktúrát alakított ki, amely számos területen a világ élvonalába tartozó publikációkat tesz közzé.[43] A Kínai Nemzeti Természettudományi Alap (National Natural Science Foundation of China, NSFC) a legjelentősebb kutatásfinanszírozó szervezet az országban, különösen az alapkutatás területén, amelyet versenyalapú pályázati rendszeren keresztül támogat. Ugyanakkor a nagy méretű AI-modellek fejlesztésének felgyorsítása érdekében a kínai kormány egyre inkább a *big science* megközelítést alkalmazza, így olyan államilag támogatott kutatóintézetek és laboratóriumok, mint a Beijing Academy of Artificial Intelligence, a Zhejiang Lab vagy a Peng Cheng Lab, a hagyományos pályázati struktúrát megkerülve közvetlen kormányzati forrásokat kapnak.[44]

Kína katonai-technológiai innovációs rendszerének meghatározó elemei közé tartoznak azok a műszaki egyetemek, amelyek szoros kapcsolatban állnak a védelmi szektorral. Ezek közül is kiemelkedik a Nemzetvédelem Hét Fia (Seven Sons of National Defence) néven ismert egyetemcsoport,[45] amely szoros együttműködésben dolgozik a Kínai Népi Felszabadító Hadsereggel (People's Liberation Army, PLA) és a védelmi iparral. Ezek az egyetemek az Ipari és Informatikai Minisztérium (Ministry of Industry and Information Technology, MIIT) irányítása alatt működnek, és jelentős állami támogatásban részesülnek. Kulcsszerepet játszanak az AI, a hiperszonikus technológia, a kiberhadviselés, az űrkutatás és a kvantuminformatika fejlesztésében. A Hét Fiú tevékenysége szervesen illeszkedik a katonai-polgári fúzió kínai stratégiájába, és jól példázza, hogyan épül be a felsőoktatás és a tudományos kutatás a védelmi kapacitások erősítésébe.[46]

A védelmi innovációs stratégia

Kína politikai retorikája saját fejlődésére koncentrálva a békés fejlődés útját hirdeti, amelynek központi eleme a *kínai nemzet nagyszerű megfiatalításának* víziója. Ennek teljes körű megvalósítását 2049-re, az államalapítás századik évfordulójára tűzte ki célul.[47] Kína egyre transzparensebben törekszik globális szerepének megerősítésére és nemzetközi befolyásának kiszélesítésére. Új nemzeti biztonsági stratégiáját 2025 májusában tette közzé *Kína nemzetbiztonsága az új korszakban* címmel. A dokumentum hangsúlyozza, hogy „a közös nemzetközi biztonság előmozdítása Kína, mint jelentős

[43] Wong Leung – Robin – Cave 2024: 19.
[44] Ding–Xiao 2023: 8.
[45] Név szerint: Harbin Institute of Technology, Nanjing University of Science and Technology, Northwestern Polytechnical Institute, Beijing Institute of Technology, Harbin Engineering University, Beijing University, Nanjing University of Aeronautics and Astronautics.
[46] McFaul–Bresnick–Chou 2025; DoD 2024a: 29, 155.
[47] Sullivan 2024: 15–16.

ország nemzetbiztonsági felelőssége" – ez összhangban áll a multipoláris világrendre és a multilaterális együttműködésre épülő külpolitikai narratíváival. A Globális Biztonsági Kezdeményezés Kína válasza az USA által vezetett nyugati biztonsági modellekre, amely alternatívát kíván nyújtani egy új nemzetközi rend megteremtésére. Az ország párhuzamos intézményrendszert és alternatív normákat épít, politikai feltételektől mentes finanszírozási és technológiai együttműködési modelleket ígérve, amelyek fokozatosan erodálják az Egyesült Államok szövetségi előnyét. A dokumentumból kirajzolódó megközelítés világosan tükrözi Kína szándékát a külső technológiai függőség csökkentésére, valamint a létfontosságú ágazatokban való önellátás megerősítésére. Ebben a stratégiai keretben a technológiai innováció és a katonai modernizáció nem csupán a belső fejlődést szolgálják, hanem a geopolitikai verseny eszközeivé is válnak, amelyek Kína globális pozíciójának megerősítését és a fennálló világrend átalakítására irányuló törekvéseit támogatják.[48]

Kína hosszú távon a globális technológiai vezető szerep megszerzésére törekszik, ezért jelentős erőforrásokat fordít a technológiai fejlődés előmozdítására. A csúcstechnológiákban való autonómia megszerzése a nemzeti fejlesztési stratégia középpontjában áll: az AI területén 2030-ra globális vezető szerepet kíván elérni.[49] A célzott állami támogatások, a stratégiai iparpolitikai és kutatási programok, valamint az intenzív nemzetközi tudományos együttműködések útján fokozatosan a globális innováció meghatározó szereplőjévé vált. A technológiai fejlődés nemcsak az alapkutatások szintjén jelentős, hanem az alkalmazott kutatásban, a termékfejlesztésben és az ipari gyártásban is meghatározó. Különösen jelentős eredményeket ért el az AI, a kvantumszámítás, az űrtechnológia, a hiperszonikus fegyverek és az új generációs kommunikációs rendszerek területén. Több stratégiai iparágban – így a hajóépítés, a mikroelektronika és a kritikus nyersanyagok területén – olyan mértékű ipari fölényt ért el, amely már az Egyesült Államok és szövetségesei összesített kapacitását is meghaladja.[50]

Kína védelmi-technológiai stratégiájának központi mechanizmusa a polgári-katonai fúzió, amely a negyedik ipari forradalom civil szektorban elért eredményeinek katonai célú adaptációja és integrációja útján igyekszik elősegíteni a haderő fejlesztését.[51] A katonai modernizációban kiemelt szerepet kapnak a kettős felhasználású technológiák, a kiber- és űrbeli képességek, valamint az AI katonai alkalmazása.[52] A modernizáció első szakasza 2027-re, a PLA megalapításának centenáriumára tervezi az alapvető modernizációs célok elérését. A második fázis 2035-re tűzte ki célul a haderő modernizációjának lényegi befejezését. A 2049-ben esedékes kínai állami centenáriumra ütemezett befejező szakasz célja pedig a 21. századi hadviselési követelményeknek történő teljes mértékű megfelelés.[53] A 2025. szeptemberi katonai parádén Kína nyilvánosan is bemutatta modernizált, technológiailag fejlett haderejét.

[48] CASI 2025.
[49] Chan et al. 2025.
[50] DoD 2023: 8.
[51] Soare–Pothier 2021: 22–23; Horowitz–Kahn 2021; Kania et al. 2021.
[52] Sullivan 2024.
[53] Panyue 2022.

A hiperszonikus rakéták, drónok, AI-alapú rendszerek látványosan demonstrálták technológiai önállóságát és elrettentő képességeit.

Technológia + innováció + nemzetbiztonság = technonacionalizmus

A technológiai fejlesztések és a nemzetbiztonság egyre szorosabban összefonódnak. A korábban elsősorban gazdasági ösztönző tényezőként kezelt technológia mára a geopolitikai verseny egyik elsődleges színterévé vált. A nagyhatalmak közötti rivalizálás, a szankciós politikák és az ellátási láncok stratégiai újragondolása arra ösztönzi az államokat, hogy a nemzetbiztonsági és szuverenitási szempontból érzékeny ágazatokat ismét nemzeti ellenőrzés alá vonják.[54] Egyre több ország tekinti stratégiai prioritásnak a technológiai önállóság elérését, a külföldi függőségek csökkentését, valamint a kritikus infrastruktúrák hazai kézben tartását. Ez a folyamat a technonacionalizmus eszméjét tükrözi, amely napjaink globális geopolitikai és geoökonómiai versengésének legmeghatározóbb tendenciája.

A technonacionalizmus fogalmát elsőként Robert B. Reich definiálta 1987-ben, és a japán gazdasági felemelkedésre reagálva olyan nemzetállami technológiai stratégiaként határozta meg, amely önellátás révén törekszik autonómiára és gazdasági versenyelőnyre.[55] Paul Stoneman értelmezésében a technonacionalizmus már a technológiai innováció, a nemzetbiztonság és a gazdasági fejlődés metszéspontjában jelenik meg. Véleménye szerint a technológia a nemzetbiztonság alappillére, és egy ország csak akkor válhat tartósan versenyképessé, ha képes a technológiai kapacitások lokalizálására.[56]

A nemzeti érdekek mentén szervezett K+F+I-politikában a kutatás-fejlesztési ökoszisztémák is geopolitikai eszközzé váltak. A technonacionalizmus több elemző szerint is gátolja a globális tudományos együttműködést és az innovációs dinamizmust. A technológiai széttagolódás *(technological decoupling)* megbontja a korábban integrált nemzetközi kutatási hálózatokat, és egymással inkompatibilis technológiai rendszerek kialakulásához vezet.[57] A technológiai fejlesztések és a nemzetbiztonság egyre szorosabb összefonódása következtében az Egyesült Államokban megerősödtek azok a szabályozási keretek, amelyek célja a külföldi befolyás és tudástranszfer kockázatainak csökkentése. A kapcsolódó szabályozások körébe tartozik a külföldi finanszírozási források és együttműködések közzétételi kötelezettsége, egyes külföldi tehetségprogramokban való részvétel tilalma, kutatásbiztonsági képzések előírása, az egyetemek számára kötelező biztonsági programok működtetése, vagy a szövetségi szervek információmegosztási és kockázatértékelési feladatai. A kutatásbiztonsági politikák *(research security policies)* két fő kockázattípust azonosítanak:

- a külföldi befolyásgyakorlás veszélyét az amerikai kutatási ökoszisztémán belül;
- a hazai kutatási eredmények külföldi ellenfelek általi kihasználásának kockázatát.[58]

[54] Lee–Han–Zhu 2022.
[55] Goreczky 2024.
[56] Yan 2023: 10.
[57] Feakin–Segal 2025.
[58] Blevins 2025.

A technonacionalizmus globális felerősödése egyre világosabban kirajzolódó technológiai blokkok kialakulásához vezet. Glenn Snyder *alliance halo* elmélete szerint a szövetségesek között kimondatlan normaként működő elvárás, hogy egymás érdekeit a formális szerződéses kötelezettségeken túl is támogassák. A technonacionalista logika ezen normát a technológiai kérdésekre is kiterjeszti, így lojalitást vár el a szövetségesektől például a Huawei-hez vagy TikTokhoz hasonló ügyekben is. Ha egy szövetséges eltérően ítéli meg a technológiai fenyegetéseket, az a kimondatlan elvárások megsértését jelenti, ami komoly politikai és bizalmi feszültséghez vezethet, és akár a szövetségi kapcsolatok meggyengülését is eredményezheti – ahogyan azt a Huawei-ügy is jól példázza.[59] A kisebb és közepes hatalmak – például Japán, Dél-Korea vagy India – ebben a stratégiai környezetben kénytelenek egyensúlyozni technológiai szuverenitásuk megerősítése és a nagyhatalmi technológiai normákhoz való alkalmazkodás között. Miközben a nagyhatalmak technonacionalista törekvései erős normatív nyomást helyeznek ezekre az államokra, egyre több ország keresi az autonóm technológiai fejlődés útjait, például a beszállítói láncok diverzifikálásával vagy a hazai innovációs kapacitások bővítésével.[60]

A technonacionalizmusban a gazdaságfejlesztési célokat háttérbe szorítva elsősorban nemzetbiztonsági megfontolások érvényesülnek, amelyek a hazai technológiai kapacitások megerősítésére és a riválisállamok technológiai fejlődésének akadályozására irányulnak.[61] A technonacionalista politikák támadó eszközként, például a K+F+I-beruházások útján a nemzeti gazdasági és biztonsági dominancia céljait szolgálják ki. A defenzív intézkedések (export- és importellenőrzések, vízumtilalmak, pénzügyi szankciók, technológiatranszfer elleni fellépés) a riválisnemzettel szembeni védelmi reakciókat foglalják magukba.[62] A technonacionalista megközelítés értelmében a stratégiai jelentőségű technológiák birtoklása és fejlesztése nem csupán gazdasági versenyelőnyt, hanem geopolitikai dominanciát is biztosít. E logika szerint a technológiai függőség nemzetbiztonsági kockázatot jelent, míg a hazai fejlesztés és technológiai önellátás olyan nemzeti érdek, amely kulcsszerepet játszik az állam hatalmának, szuverenitásának és biztonságának fenntartásában.[63]

Számos elemző szerint ezek a tendenciák legerősebben az Egyesült Államok és Kína közötti technológiai versenyben tükröződnek.[64] A nyugati biztonságpolitikai szemlélet Kína politikai rendszerét és hosszú távú stratégiáját a fennálló világrenddel szembeni strukturális kihívásként értelmezi. Eszerint Kína technológiaalapú katonai modernizációja a globális geopolitikai erőegyensúly átrendezésének eszköze, amely közvetlen kihívást intéz a jelenlegi, szabályalapú, Nyugat-központú biztonsági architektúrával szemben.[65] Ezt tükrözi a 2022-es amerikai nemzeti biztonsági stratégia is, amely a Kínai Népköztársaságot jelöli meg az Egyesült Államok egyetlen olyan versenytársaként, amely „egyszerre rendelkezik a nemzetközi rend átalakításának

[59] Lee–Han–Zhu 2022: 489–490; Krach – Chiang – Ashley Ford 2020.
[60] Feakin–Segal 2025.
[61] Goreczky 2024.
[62] Bateman 2022: 2–3.
[63] Chan et al. 2025; Fang–Hwang 2023; Lee 2024.
[64] Feakin–Segal 2025; Fang–Hwang 2023; Bateman 2022.
[65] Soare–Pothier 2021: 13, Kisvári 2024.

szándékával és – egyre inkább – az ehhez szükséges gazdasági, diplomáciai, katonai és technológiai erővel is".[66] Kína szabja meg a verseny dinamikáját, ezzel folyamatos adaptációra kényszerítve az Egyesült Államokat – a dokumentum ezt stratégiai ütemet meghatározó kihívásként *(pacing challenge)* azonosítja. A kihívás komplex és többdimenziós: nem korlátozódik a katonai szférára, hanem kiterjed a védelmi képességek modernizálására, a globális befolyásért folytatott versengésre, valamint a technológiai dominancia megszerzéséért zajló küzdelemre is.[67]

A technonacionalizmus keretében mindkét nagyhatalom saját technológiai ökoszisztémájának megerősítésére törekszik, miközben kölcsönösen igyekeznek korlátozni egymás hozzáférését a kulcsfontosságú technológiákhoz és piacokhoz – különösen a félvezetők, ritkaföldfémek, 5G/6G, AI[68] és kvantumszámítás terén.[69] Az Egyesült Államok elsődleges célja technológiai hegemóniájának megőrzése,[70] míg Kína egyre nagyobb volumenű beruházásokkal törekszik a stratégiai ágazatok dominanciájára.[71] Az USA világelső a csúcstechnológiás chipgyártásban, amely az AI és a modern hadiipar alapja, míg Kína ritkaföldfémek terén elért stratégiai fölénye a chipgyártáshoz és számos katonai alkalmazáshoz nélkülözhetetlen. A versengés egyik legszemléletesebb terepe ezért a félvezetőipar és a ritkaföldfémek piaca, ahol az egyik fél stratégiai előnye a másik fél strukturális hátrányát jelenti. Az amerikai félvezetőfölény éppen ott válik sebezhetővé, ahol Kína erős, míg a kínai ritkaföldfém-dominancia az amerikai technológiai függés miatt korlátozott. A kölcsönösen alkalmazott korlátozási mechanizmus az erőviszonyok ellensúlyozása érdekében az exportkorlátozásokra a nyersanyagkivitel szigorításával reagál. A két megközelítés alapjaiban alakítja át a globális geopolitikai egyensúlyt, amelynek gyakorlati következményei az aktuális konfliktusokban is jól megfigyelhetők. Az Egyesült Államok az orosz–ukrán háború kapcsán szigorította az Oroszországgal szembeni exportkontrollt, míg Kína a Tajvan körüli feszültségek nyomán felgyorsította a hazai félvezetőipar fejlesztését.

Az Egyesült Államok és Kína technonacionalista stratégiája eltérő intézményi és ideológiai alapokra épül. Az amerikai modell a *nyitott innováció – zárt hozzáférés* elvén alapul: nyitott a szövetségesek felé, de korlátozza a riválisokat. Az USA szövetségi együttműködéssel és protekcionizmussal ötvözi stratégiai céljait, ami egyszerre erősíti a technológiai pozíciót és védi a stratégiai iparágakat. A decentralizált, piac- és versenyalapú rendszerben a civil–katonai együttműködés és az alulról építkező dinamika a meghatározó. A kínai modell ezzel szemben a *zárt önellátás – nyitott tanulás* elvén alapul, vagyis a belső technológiai önellátást ötvözi a nemzetközi tudástranszferrel. Kína példája azt mutatja, hogy a technológiai transzfer kontroll alatt tartása mellett is lehet a nyitott technológiai kapcsolatokból gazdasági és nemzetbiztonsági előnyöket kovácsolni. A kínai technonacionalizmus a technológiai fejlődés tudatos politikai és ideológiai irányítását is magában foglalja. Ez a megközelítés a hazai technológiák preferálásában, a nyugati modellekhez való hozzáférés korlátozásától való félelemben,

[66] The White House 2022: 23.
[67] DoD 2022; DoD 2024a.
[68] Chan et al. 2025.
[69] Fang–Hwang 2023.
[70] The White House 2025c.
[71] Chan et al. 2025.

valamint a legkorszerűbb modellekben – például a Zuchongzhi szupravezető kvantumszámítógépek, a Chang'e-6 holdszonda vagy a Meng Hsziang mélytengeri fúróhajó – elért nemzeti büszkeségben is testet ölt.[72]

Konklúzió

A technológiai önállóság és a nemzetközi együttműködés közötti feszültség alapvetően meghatározza a 21. század geopolitikai, technológiai, gazdasági és tudományos viszonyrendszerét, és komoly hatást gyakorol a nemzetközi rend átalakulására. A globális hatalmi egyensúly egyik meghatározó tényezője a védelmi technológiákban és innovációban elfoglalt pozíció. A vezető szerep hosszú távon is formálja a globális hatalmi viszonyok alakulását, csakúgy, mint az innovációban való lemaradás, ami tartós stratégiai hátrányt eredményezhet. A versengés központi célja az innováció uralása és a K+F vezető szerep megszerzése vagy fenntartása, amely egyaránt biztosít tudományos, gazdasági, politikai és katonai befolyást.[73]

A katonai képességek fejlődésének a globális hatalmi egyensúly átalakulására gyakorolt hatása nemzetbiztonsági szempontból is meghatározó, amelyben az EDT-k jelentősége messze túlmutat a tudományos és gazdasági dimenziókon. A katonai célú EDT-k fejlesztése eltérő regionális intenzitással, de világszerte fegyverkezési versenyhez vezetett, amely magával vonja a védelmi K+F+I-kiadások folyamatos növekedését.[74] Az EDT-k körüli globális diskurzus gyakran zéró összegű logikát követ, amely szerint az egyik fél technológiai előnye a másik stratégiai veszteségét jelenti.[75] Ez a versengő logika legmarkánsabban az AI területén rajzolódik ki, de egyre inkább áthatja a kvantumszámítást, a félvezetőipart és a biotechnológiát is, alakítva azok nemzetközi megítélését és versenyét.

Napjainkra a védelmi K+F+I geopolitikai tétté vált, amely meghatározza, mely országok lesznek képesek befolyásolni a jövő világrendjének alakulását. A nagyhatalmak a nemzetközi együttműködés rovására a technológiai szuverenitást egyre inkább stratégiai és biztonsági kérdésként kezelik. Ez a megközelítés intézményesíti a stratégiai jelentőségű technológiákhoz való hozzáférés nemzeti szintű védelmét. A globális technológiai verseny egyre inkább militarizálódik és a hidegháborús időszakot idéző nagyhatalmi rivalizálás formáját ölti,[76] amelynek a technonacionalizmus egyszerre tünete és eszköze. A technonacionalizmus szűrőjén keresztül a technológiai szuverenitás nemzeti szuverenitássá, az innovációs fölény geopolitikai fölénnyé, a technológiai függőség pedig stratégiai sebezhetőséggé alakul. Bár a jövőbeli kimenetek bizonytalanok, a jelenlegi élmezőny várhatóan évtizedekre meghatározza a globális gazdasági, politikai és biztonsági struktúrák szerkezetét.

[72] Ding–Xiao 2023: 10; CASI 2025.
[73] Bickell et al. 2024: 15.
[74] Liang et al. 2025: 8; Clapp 2022: 1.
[75] Fang–Hwang 2023.
[76] Sherman 2019; Soare–Pothier 2021: 3.

Felhasznált irodalom

Az Európai Parlament és a Tanács (EU) 2021/697 rendelete (2021. április 29.) az Európai Védelmi Alap létrehozásáról és az (EU) 2018/1092 határozat hatályon kívül helyezéséről. Online: https://eur-lex.europa.eu/eli/reg/2021/697/oj?eliuri=eli%3Areg%3A2021%3A697%3Aoj&locale=hu

Bateman, Jon (2022): *U.S. – China Technological "Decoupling": A Strategy and Policy Framework.* Washington, D.C.: Carnegie Endowment for International Peace Publications Department. Online: https://carnegieendowment.org/research/2022/04/us-china-technological-decoupling-a-strategy-and-policy-framework?lang=en#the-evolution-of-us-thinking-and-policy

Beaver, Wilson (2025): China's Defense Budget Is Bigger Than You Think. *The Heritage Foundation,* 2025. április 17. Online: www.heritage.org/china/commentary/chinas-defense-budget-bigger-you-think?utm_

Bickell, Eleni G. et al. (2024): *Federal Research and Development (R&D) Funding: FY2025. CRS Report*. Online: www.congress.gov/crs-product/R48307?utm=

Blevins, Emily G. (2025): Federal Research Security Policies: Background and Issues for Congress. CRS Report. Online: www.congress.gov/crs-product/R48541

Boda Mihály (2022): A hibrid háború etikája: az igazságos hibrid háború elmélete. In M. Szabó Miklós (szerk.): *A hadtudomány aktuális kérdései napjainkban I.* Budapest: Ludovika, 95–108. Online: https://doi.org/10.36250/00973_06

Boda Mihály (2025): *A multipoláris nemzetközi rendtől a poliarchikusig – a „hadszíntérháború"-tól a hibrid háborúig*. Kézirat.

Chan, Kyle et al. (2025): Full Stack: China's Evolving Industrial Policy for AI. *RAND Expert Insights,* 2025. június 26. Online: https://doi.org/10.7249/PEA4012-1

China Aerospace Studies Institute (CASI) (2025): *In Their Own Words: 2025 China's National Security in the New Era*. [H. n.]: China Aerospace Studies Institute. Online: https://bit.ly/46AGWk4

Clapp, Sebastian (2022): *Emerging Disruptive Technologies in Defence.* European Parliamentary Research Service. Online: www.europarl.europa.eu/thinktank/en/document/EPRS_ATA(2022)733647

Defense Advanced Research Projects Agency (DARPA) (2022): *DARPA Seeks Proposals to Forge the Future of U.S. Microelectronics Manufacturing*. Online: www.darpa.mil/news/2022/future-microelectronics-manufacturing

Ding, Jeffrey – Xiao, Jenny W. (2023): *Recent Trends in China's Large Language Model Landscape*. Centre for the Governance of AI. Online: https://cdn.governance.ai/Trends_in_Chinas_LLMs.pdf

Fang, Tianyu – Hwang, Tim (2023): *The Rise of Techno-Nationalism.* Online: www.newamerica.org/oti/reports/the-rise-of-techno-nationalism/

Feakin, Tobias – Segal, Adam (2025): Brave New Techno-Nationalist World. *Foreign Policy,* 2025. június 4. Online: https://foreignpolicy.com/2025/06/04/trump-tech-policy-techno-nationalism/?utm_

Fetter, Steve – Sankaran, Jaganath (2024): Emerging Technologies and Challenges to Nuclear Stability. *Journal of Strategic Studies,* 48(2), 252–296. Online: https://doi.org/10.1080/01402390.2024.2433766

Gallo, Marcy E. (2021): Defense Advanced Research Projects Agency: Overview and Issues for Congress. *CRS Report*. Online: https://sgp.fas.org/crs/natsec/R45088.pdf
Goreczky Péter (2024): Nyitottnak maradni, de mennyire – erősödő techno-nacionalizmus a világban. *Világgazdaság,* 2024. július 29. Online: www.vg.hu/velemeny/2024/07/nyitottnak-maradni-de-mennyire-erosodo-techno-nacionalizmus-a-vilagban?utm=
Haddad, Christian – Vorlíček, Dagmar – Klimburg-Witjes, Nina (2024): The Security-Innovation Nexus in (Geo-) Political Imagination. *Geopolitics,* 29(3), 741–764. Online: https://doi.org/10.1080/14650045.2024.2329940
Háber Péter (2022): A hibrid hadviselés elméletének tömör összefoglalása a hazai szakirodalom alapján. *Felderítő Szemle,* 21(4), 72–94. Online: https://hhk.uni-nke.hu/document/hhk-uni-nke-hu/2022_4_Felder%C3%ADt%C5%91%20Szemle.pdf
Horowitz, Michael C. – Kahn, Lauren (2021): *DoD's 2021 China Military Power Report: How Advances in AI and Emerging Technologies Will Shape China's Military*. Council on Foreign Relations. Online: www.cfr.org/blog/dods-2021-china-military-power-report-how-advances-ai-and-emerging-technologies-will-shape
Kania, Elsa B. (2019): Minds at War. China's Pursuit of Military Advantage through Cognitive Science and Biotechnology. *PRISM,* 8(3), 82–101. Online: www.jstor.org/stable/pdf/26864278.pdf?refreqid=fastly-default%3A246290d30dc0d9c005b36c4079a51dd5&ab_segments=&initiator=&acceptTC=1
Kania, Elsa B. et al. (2021): How Should the U.S. Respond to China's Military-Civil Fusion Strategy? *ChinaFile,* 2021. május 22. Online: www.chinafile.com/conversation/how-should-us-respond-chinas-military-civil-fusion-strategy
Kisvári Tamás (2024): Kína hosszú távú stratégiája. In Görbe Attiláné – Zán Krisztina (szerk.): *Kína – A Középső Birodalom*. Budapest: Katonai Nemzetbiztonsági Szolgálat, 204–225. Online: https://bit.ly/4uaMWdC
Krach, Keith – Chiang, Mung – Ashley Ford, Christopher (2020): *Briefing on Taiwan Semiconductor Manufacturing Corporation's Intent To Invest $12 Billion in the U.S. and on the CCP's Ability To Undermine U.S. Export Controls*. Online: https://bit.ly/4bjlxOW
Lee, Ji-Young – Han, Eugeniu – Zhu, Keren (2022): Decoupling from China: How U.S. Asian Allies Responded to the Huawei ban. *Australian Journal of International Affairs,* 76(5), 486–506. Online: https://doi.org/10.1080/10357718.2021.2016611
Lee, Lizzi C. (2024): China's Big Fund 3.0: Xi's Boldest Gamble Yet for Chip Supremacy. *The diplomat,* 2024. június 6. Online: https://thediplomat.com/2024/06/chinas-big-fund-3-0-xis-boldest-gamble-yet-for-chip-supremacy/
Liang, Xiao et al. (2025): Trends in World Military Expenditure, 2024. *SIPRI Publications,* 1–12. Online: https://doi.org/10.55163/AVEC8366
McFaul, Cole – Bresnick, Sam – Chou, Daniel (2025): *Pulling Back the Curtain on China's Military-Civil Fusion. How the PLA Mobilizes Civilian AI for Strategic Advantage.* CSET, 2025. szeptember. Online: https://cset.georgetown.edu/wp-content/uploads/CSET-Pulling-Back-the-Curtain-on-Chinas-Military-Civil-Fusion.pdf
Mok, Charles (2023): The Party Rules: China's New Central Science and Technology Commission. *The Diplomat,* 2023. augusztus 23. Online: https://thediplomat.

com/2023/08/the-party-rules-chinas-new-central-science-and-technology-commission/
Mosley, Brian (2024): FY24 Budget Update. *CRA News,* 36(4). Online: https://bit.ly/40GNXwe
National Bureau of Statistics of China (NBS) (2025): *China's Expenditure on Research and Experimental Development (R&D) Exceeded 3.6 Trillion Yuan in 2024*. Online: www.stats.gov.cn/english///PressRelease/202502/t20250207_1958579.html?utm
Nature (2020): Editorial: DARPA 'Lookalikes' Must Ground Their Dreams in Reality. *Nature,* 579, 173–174. Online: https://doi.org/10.1038/d41586-020-00690-5
O'Hanlon, Michael E. (2025): Achieving "Peace through Strength" in the 2020s. *Brookings,* 2025. február 21. Online: www.brookings.edu/articles/achieving-peace-through-strength-in-the-2020s/?utm
Panyue, Huang szerk. (2022): *Xi's Vision Leads to Success*. Online: http://eng.mod.gov.cn/xb/News_213114/TopStories/4923634.html?utm
Reding, D. F. – Eaton, J. (2020): *Science & Technology Trends 2020–2040.* Brussels: NATOScience & Technology Organization Office of the Chief Scientist NATO-Headquarters. Online: https://apps.dtic.mil/sti/pdfs/AD1131124.pdf
Remek Éva (2023): Változó biztonság, változó biztonságfelfogás. In Zachar Péter Krisztián – Barna Attila (szerk.): *Titkos cikkek az örök békéhez. Ünnepi tanulmányok a 70 éves Fülöp Mihály tiszteletére*. Budapest: Ludovika, 337–349. Online: https://doi.org/10.36250/01132_27
Sargent, John F. – Shea, Dana A. (2020): *Office of Science and Technology Policy (OSTP): History and Overview.* Online: www.congress.gov/crs-product/R43935
Sherman, Justin (2019): *Essay: Reframing the U.S.China AI „Arms Race"*. Online: www.newamerica.org/cybersecurity-initiative/reports/essay-reframing-the-us-china-ai-arms-race/introduction
Silk Road Hungary (2025): *Kína tudományos és technológiai fejlődése új lendületet ad az ipari innovációnak.* 2025. július 28. Online: https://silkroadhungary.hu/2025/07/kina-tudomanyos-es-technologiai-fejlodese-uj-lenduletet-ad-az-ipari-innovacionak-2/
Soare, Simona R. – Pothier, Fabrice (2021): *Leading Edge: Key Drivers of Defence Innovation and the Future of Operational Advantage.* International Institute of Strategic Studies Research Papers. Online: https://www.iiss.org/research-paper/2021/11/key-drivers-of-defence--innovation-and-the-future--of-operational-advantage/
Sullivan, Ian M. (2024): Three Dates, Three Windows, and All of DOTMLPF-P. *Military Review,* 104(1), 14–25. Online: www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/January-February-2024/Sullivan/Journals/Military-Review/utm/
Szöllősi Annamária (2025): A reziliencia a biztonság kontextusában. *Hadtudományi Szemle,* 18(2), 161–177. Online: https://doi.org/10.32563/hsz.2025.2.10
The White House (2022): *National Security Strategy.* Online: https://bidenwhitehouse.archives.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf

The White House (2025a): *President Trump is Leading with Peace Through Strength.* Online: www.whitehouse.gov/articles/2025/03/president-trump-is-leading-with-peace-through-strength/?utm
The White House (2025b): *Fact Sheet: President Donald J. Trump Restores the United States Department of War.* Online: www.whitehouse.gov/fact-sheets/2025/09/fact-sheet-president-donald-j-trump-restores-the-united-states-department-of-war/
The White House (2025c): *President's Council of Advisors on Science and Technology.* Online: www.whitehouse.gov/presidential-actions/2025/01/presidents-council-of-advisors-on-science-and-technology/
The White House [é. n.]: *Office of Science and Technology Policy.* Online: www.whitehouse.gov/ostp/?utm
Tian, Nan et al. (2024): Trends in World Military Expenditure, 2023. *SIPRI Fact Sheet,* 2024. április. Online: www.sipri.org/sites/default/files/2024-04/2404_fs_milex_2023.pdf
U.S. Department of Defense (2022): *National Defense Strategy of the United States of America*. Online: https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF
U.S. Department of Defense (2023): *National Defense Industrial Strategy*. Online: www.govinfo.gov/content/pkg/GOVPUB-D-PURL-gpo234254/pdf/GOVPUB-D-PURL-gpo234254.pdf
U.S. Department of Defense (2024a): *Military and Security Developments Involving the People's Republic of China*. Online: https://media.defense.gov/2024/Dec/18/2003615520/-1/-1/0/MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA-2024.PDF
U.S. Department of Defense (2024b): *National Defense Industrial Strategy Implementation Plan for FY2025*. Online: www.govinfo.gov/content/pkg/GOVPUB-D-PURL-gpo234260/pdf/GOVPUB-D-PURL-gpo234260.pdf
U.S. Department of War (2023): *Chief Digital & Artificial Intelligence Office Celebrates First Year*. Online: www.war.gov/News/Releases/Release/Article/3464012/chief-digital-artificial-intelligence-office-celebrates-first-year/
U.S. Department of War (2024): *CDAO and DIU Launch New Effort Focused on Accelerating DOD Adoption of AI Capabilities*. Online: www.war.gov/News/Releases/Release/Article/3996199/cdao-and-diu-launch-new-effort-focused-on-accelerating-dod-adoption-of-ai-capab/
U.S. Department of War (2025a): *Statement on the Development of the 2025 National Defense Strategy*. Online: www.war.gov/News/Releases/Release/Article/4172735/statement-on-the-development-of-the-2025-national-defense-strategy/
U.S. Department of War (2025b): *DIU's Thunderforge Project to Integrate Commercial AI-Powered Decision-Making for Operational and Theater-Level Planning*. Online: www.diu.mil/latest/dius-thunderforge-project-to-integrate-commercial-ai-powered-decision-making
U.S. Government Accountability Office (GAO) (2024): *Hypersonic Weapons: DOD Could Reduce Cost and Schedule Risks by Following Leading Practices. Report to Congressional Committees.* Online: www.gao.gov/assets/880/870416.pdf

Vigliarolo, Brandon (2022): Darpa Says US Hypersonic Missile Is Ready for Real World. *The Register,* 2022. április 6. Online: www.theregister.com/2022/04/06/darpa_hypersonic_missile/

Vigliarolo, Brandon (2025): It Begins: Pentagon to Give AI Agents a Role in Decision Making, Ops Planning. *The Register,* 2025. március 5. Online: www.theregister.com/2025/03/05/dod_taps_scale_to_bring/?utm

Vuk, Pavel (2025): Editorial: Disruptive Technologies. *Contemporary Military Challenges,* 27(1), 13–18. Online: https://doi.org/10.2478/cmc-2025-0002

Wong Leung, Jennifer – Robin, Stephan – Cave, Danielle (2024): *ASPI's Two-Decade Critical Technology Tracker: The Rewards of Long-term Research Investment*. Barton ATC: ASPI. Online: https://bit.ly/4rPT6hE

World Intellectual Property Organization (WIPO) (2025): *Global Innovation Index 2025: Innovation at a Crossroads*. Genf: WIPO. Online: https://doi.org/10.34667/tind.58864

Yan, Ming (2023): How Techno-Nationalism Affects Technological Decoupling Between China and the U.S. *International Journal of Education and Humanities,* 10(3), 10–13. Online: https://doi.org/10.54097/ijeh.v10i3.11782

Zhang, Lin – Lan, Tu (2022): The New Whole State System: Reinventing the Chinese State to Promote Innovation. *Environment and Planning A: Economy and Space,* 55(1), 201–221. Online: https://doi.org/10.1177/0308518X221088294

Tartalom

VÉDELEMINFORMATIKA

Gábor Farkas: *Electronic Warfare Framework* 5

Károly Kassai: *Cybersecurity Challenges of the Integration of Artificial Intelligence (AI) Solutions* 17

Zoltán Kovács: *The Use of Artificial Intelligence in Cyberattacks, Part 1* 39

Zoltán Kovács: *The Use of Artificial Intelligence in Cyberattacks, Part 2* 53

Pozderka Gábor: *A kibervédelmi és a kiberműveleti gyakorlatok rendszerének átalakulása, az aktuális kihívások vizsgálata* 69

Tóth Ádám: *Zero trust network access az ipari (OT) kiberbiztonságban* 87

KÖRNYEZETBIZTONSÁG

Horváth János, Horváth Zsuzsa: *Bolygóvédelem és NEO-kockázatok* 103

Kirovné Rácz Réka, Scholtz Emánuel: *A mesterséges intelligencia és gépi tanulás algoritmusainak alkalmazása a hidrológiai katasztrófák elleni védekezésben* 125

Sibalin Iván, Kátai-Urbán Maxim, Cimer Zsolt: *Az energiaipari-biztonság és a környezeti fenntarthatóság egyes összefüggéseinek értékelése, 1. rész* 149

VÉDELEMGAZDASÁG

Szöllősi Annamária: *Az innováció mint stratégiai fegyver* 161