HÍRVILLÁM

A NEMZETI KÖZSZOLGÁLATI EGYETEM
Híradó Tanszék szakmai tudományos kiadványa

SIGNAL Badge

Professional journal of Signal Departement
at the University of Public Service

2025

Infokommunikáció 2025

tudományos szakmai konferencia

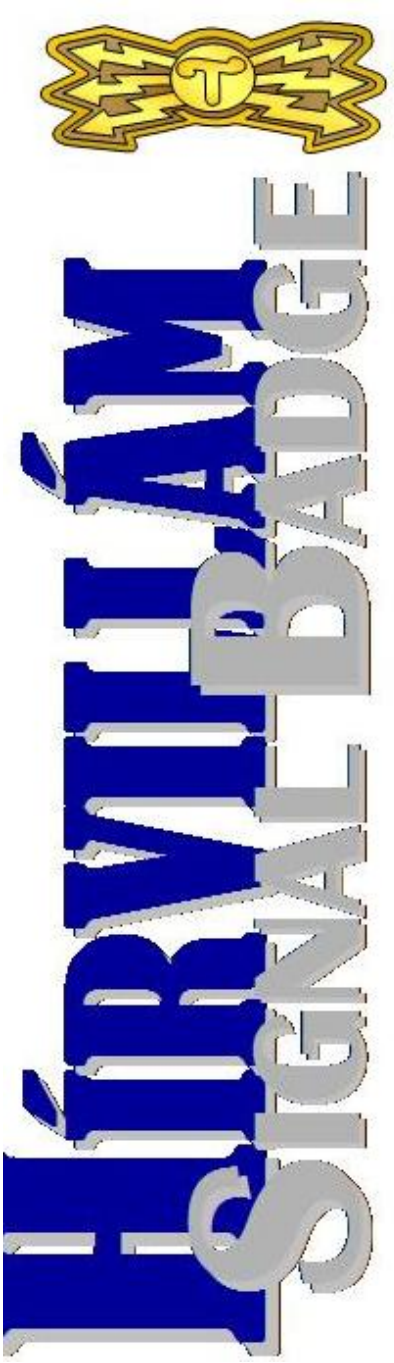
Konferencia kiadvány

2025. november 13.

HÍRVILLÁM
a Nemzeti Közszolgálati Egyetem, Híradó Tanszék tudományos időszaki kiadványa

SIGNAL BADGE
Professional Journal of the Signal Departement at the University of Public Service

Budapest, 2025



Felelős kiadó/Editor in Chief
Dr. Tóth András

A konferencia szervezőbizottsága, illetve a kiadvány szerkesztőbizottsága/Editorial Board

A konferencia szervezőbizottságának társelnökei/ Co-chairs of the conference organising committee
Dr. Tóth András
Dr. Négyesi Imre

Főszerkesztő/Co-ordinating Editor
Dr. Tóth András

Tagok/Members
Dr. habil. Farkas Tibor
Dr. Jobbágy Szabolcs
Dr. Magyar Sándor
Megyeri Lajos
Szűcs Attila
Imhof László
Vilmányi Edina

HU ISSN 2061-9499

.....

NKE HHK KII IIT
1101 Budapest, Hungária krt. 9-11.
1581 Budapest, Pf.: 15
+36 1 432 9000 (29-407 mellék)

Tartalomjegyzék

Köszöntő

Tisztelettel köszöntjük Önt, Kedves Kolléga, Tisztelt Olvasó!

A Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Infokommunikációs és Információbiztonsági Tanszéke, együttműködésben a Honvéd Vezérkar Híradó és Informatikai Csoportfőnökségével, a Nemzeti Média- és Hírközlési Hatósággal, a Hírközlési és Informatikai Tudományos Egyesülettel, illetve a Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Puskás Tivadar Szakkollégiumával, 2025. november 13-án, idén 24. alkalommal rendezte meg nemzetközi tudományos-szakmai konferenciáját.

Az Infokommunikáció konferencia - amely első alkalommal 2000-ben került megrendezésre - célja, hogy átfogó, multidiszciplináris fórumot biztosítson mindazon szakemberek, kutatók, oktatók, egyetemi polgárok és hallgatók számára, akik az információs és kommunikációs technológiák (ICT), valamint azok katonai, kormányzati, ipari és civil alkalmazásai iránt elkötelezettek.

A rendezvény kiemelt küldetése, hogy elősegítse a tudományos párbeszédet és az innovációs együttműködéseket a professzionális és a védelmi szféra között, ezáltal hozzájárulva Magyarország és a közép-európai térség infokommunikációs képességeinek és biztonsági kultúrájának fejlesztéséhez.

A konferencia lehetőséget biztosít arra, hogy a résztvevők megosszák egymással legújabb kutatási eredményeiket, gyakorlati tapasztalataikat, valamint bemutassák az infokommunikációhoz kapcsolódó új trendeket, technológiákat és módszertani megközelítéseket.

A rendezvény a hazai infokommunikációs tudományos élet egyik meghatározó eseménye, amely hozzájárul a kutatás, az oktatás és az innováció összekapcsolásához, valamint a nemzeti és nemzetközi szakmai hálózatok erősítéséhez.

A rendezvény szerves részét képezi a Magyar Tudományos Akadémia által fémjelzett, több évtizedes múltra visszatekintő Magyar Tudomány Ünnepe rendezvénysorozatnak, melyről az akadémia már 1997 óta megemlékezik, és 2003 óta hivatalosan is megünnepeljük minden év november 03-án. Ezzel emléket állítva, és tisztelegve azon momentumnak, amikor is Széchenyi István birtokai egy évi jövedelmét felajánlva hozzájárult a Magyar Tudós Társaság megalapításához, mely a későbbiekben lehetővé tette a Magyar Tudományos Akadémia megalapítását.

A konferencia során az infokommunikációval és az információbiztonsággal kapcsolatos új trendeket és kihívásokat 18 színvonalas előadás keretében érdekesebbnél érdekesebb aspektusokból világították meg az előadók. Az érdekfeszítő előadások mellett, a rendezvény szakmai színvonalát emelte, az együttműködő partnereknek köszönhetően, egy látványos, a

jelenkor technológiai-, technikai- és szolgáltatásszínvonalát felvonultató kiállítás is.

A rendezvény több mint 120 fő regisztrált résztvevőt számlált.

Jelen kiadványban a szerkesztőbizottság a szerzők hozzájárulásával az egyes előadásokból készített korreferátumokat gyűjtötte össze, amelynek eredményeképpen hat előadás került megjelentetésre, amelyeket nagyon nagy örömmel bocsájt rendelkezésre a Kedves Olvasóknak.

Budapest, 2025. november 13.

Dr. Tóth András
a szerkesztőbizottság
elnöke

Infokommunikáció 2025 **Nemzetközi tudományos - szakmai konferencia** *(2025. november 13.)*	
08:50-09:00	**MEGNYITÓ**
Levezető elnök: **Dr. Tóth András** **PANEL I.**	
09:00-09:15	Prof. Dr. Rajnai Zoltán: AI-Cloud egyetemi környezetben
09:15-09:30	Kollár Péter: Az NMHH szerepe a 2G kivezetésben
09:30-09:45	Dr. Orbán József: Reziliens PNT szolgáltatások
09:45-10:00	Dr. Benedek Andor, Klinda Richárd, Kormos László, Dr. Nemcsics Elek, Dr. Vály László: Adaptív mechanizmusok mikrohullámú adatátviteli hálózatokban
10:00-10:15	Marsi Tamás: Kritikus infrastruktúrák elleni kibertámadások
10:15-10:45	**Kávészünet**
Levezető elnök: **Dr. Jobbágy Szabolcs** **PANEL II.**	
10:45-11:00	Kovács Zoltán: Vadászat a vörös attacker-re. Spot and stop the invisible / Meglátni a láthatatlant
11:00-11:15	Gyebnár Gergő: A hálózat sötét oldala, forgalomfigyelés belülről
11:15-11:30	Ceglédi Csaba: A Pro-M kormányzati szolgáltatói szerepe
11:30-11:45	Dr. Prisznyák Szabolcs: Digitális megoldások a büntetés-végrehajtásban
11:45-12:30	**Ebéd**
Levezető elnök: **Dr. Farkas Tibor** **PANEL III.**	
12:30-12:45	Szijártó Zsolt: Izolált régióktól a műveleti tevékenységig – Oracle megoldások a katonai informatikában
12:45:13:00	Imhof László: Orosz-Ukrán konfliktusban megvalósított CIS támogatás, és konklúziói
13:00-13:15	Pál Anita Brigitta: A mesterséges intelligencia és az adatfúzió hatása a katonai döntéshozatalra
13:15-13:30	Bodnár István: Alacsony késleltetésű rendszerek terepi felhasználása

13:30-14:00	**Kávészünet**
Levezető elnök: **Dr. Megyeri Lajos** **PANEL IV.**	
14:00-14:15	Dr. Magyar Sándor: Tudás vagy attitűd? Az emberi tényező fejlesztésének dilemmái a kiberbiztonságban
14:15-14:30	Oláh István: A hálózat gondolatAI?
14:30-14:45	Takács Péter: Narratívaháborúk és percepciós műveletek: a háború politikai természetének újrastrukturálódása az információs térben
14:45-15:00	Szulcsányi Viktor: Támadási felületek minimalizálása IT/OT környezetben
15:00-15:15	Dr. Tóth András: A katonai híradó és informatikai tisztképzés jelene és jövője
15:15-15:20	**A konferencia zárása**

Pál Anita Brigitta: A mesterséges intelligencia és az adatfúzió hatása a katonai döntéshozatalra

A biztonsági architektúrák az elmúlt évtizedben gyökeresen átalakultak a mesterséges intelligencia megjelenésével. Míg korábban a védelem alapját elsősorban a fizikai infrastruktúrák, fegyverrendszerek és erőforrások alkották, ma a stratégiai súlypont egyre inkább az információs térbe, azon belül is az adat értelmezésének dimenziójába helyeződik át. Az adat, amely korábban a döntéshozatal egyik inputja volt, mára önálló és kiemelt stratégiai erőforrássá vált.

Előadásom arra a kérdésre keresi a választ, hogy hogyan konstruálódik a modern katonai valóság a mesterséges intelligencia által működtetett rendszerekben, és milyen kockázatokkal, valamint lehetőségekkel jár az, hogy egyre több döntés előkészítése algoritmikus interpretációra épül.

A modern hadviselésben a helyzetértés már nem pusztán megfigyelés eredménye. A modern rendszerek az adatot feldolgozzák, szűrik, súlyozzák, majd modellalapú értelmezéssé alakítják. Ennek következtében a valóság, amelyet a döntéshozók látnak, egyre inkább mesterségesen előállított konstrukció, amelyet algoritmusok, szoftverrétegek és adatfúziós mechanizmusok formálnak.

Ezen a ponton jelenik meg egy új, meghatározó szereplő: az amerikai Palantir Technologies, amely túlmutat a klasszikus adatkezelési megközelítéseken. A vállalat nem egyetlen alkalmazást

kínál, hanem komplex, egymásra épülő szoftver-ökoszisztémát, amely különböző típusú adatokat, mint a hírszerzési jelentéseket, műholdfelvételeket, pénzügyi tranzakciókat, hálózati aktivitást, híváslistákat képes összekapcsolni, vizualizálni és a műveleti láncokba. A folyamatot a szakirodalom „műveleti ontológiának” nevezi: a valós világ entitásai (személyek, járművek, helyek, események) adatobjektummá alakulnak, majd ezek a rendszerben egy új, digitálisan rekonstruált világot hoznak létre.

Ez a világ azonban nem a nyers valóság tükre, hanem annak szimulált leképezése. Amikor egy elemző, parancsnok vagy döntéshozó egy információs panelt lát, gyakran valóságként tekint rá, holott ez a kép modellek, előfeldolgozási lépések és algoritmikus súlyozások eredményei. A döntést tehát nem az adat hozza meg, hanem az adat értelmezése. Így, ha a modell torzul, a döntés is torzul.

A torzulás veszélye ráadásul nem csupán elméleti. Elég egy apró eltérés egy szenzorértékben, egy félreosztályozott jelben vagy egy módosított prioritási pontszámban és az egész helyzetkép elmozdulhat. Ezért válik az adatintegritás a modern biztonsági környezet egyik legkritikusabb stratégiai célpontjává. A legveszélyesebb támadás ugyanis nem az, amikor egy rendszer leáll, hanem az, amikor a rendszer működik, de rossz valóságot tükröz.

A mesterséges intelligenciát alkalmazó rendszerek ma már nemcsak elemeznek, hanem javaslatokat tesznek, prioritásokat határoznak meg, sőt integrálódnak a katonai műveleti láncba. Ezzel átlépik azt

a határvonalat, ahol az MI nemcsak támogatja, hanem részben helyettesíti is az emberi döntéshozatalt, akár de facto döntéshozóvá válva. Ez új, eddig ismeretlen kérdéseket vet fel az információs szuverenitásról, a felelősségvállalásról és a döntéshozatal etikájáról. E dilemmák nem csupán technológiai kérdéseket vetek fel, hanem mélyen stratégiaiakat is. A valóság újra rekonstruálása az adatfúzión keresztül olyan modellfüggő folyamat, amely érinthet a jövőben NATO-doktrínákat, a közös műveleti elveket és akár nemzetállami adatszuverenitási szabályokat. Amennyiben egy nemzetbiztonság szempontjából kritikus adatértelmező rendszer nemzeti kontrollon kívül kerül, fennáll annak a veszélye, hogy a döntési mechanizmus nem marad teljes mértékben szuverén.

Az előadás arra hívja fel a figyelmet, hogy a 21. században a biztonságpolitika egyik legfontosabb kérdése az, hogy ki birtokolja az adatot, hanem hogy: ki birtokolja a modellt, amely értelmezi az adatot. Mert aki irányítja az értelmezést, az irányítja a döntést is. A modern hadviselésben így a valóság védelme egyben a szuverenitás védelmét is jelenti. Az adatfúzió nem technológiai, hanem stratégiai és filozófiai kérdés. Aki az adatból építi fel a valóságot, az a valóság értelmezését és ezzel együtt a döntések irányítását is birtokolja. A modern katonai és nemzeti döntéshozatal kulcsfogalma tehát a jövőben az értelmezési szuverenitás lesz: annak biztosítása, hogy a modellek, amelyekre döntéseinket építjük, hitelesek, átláthatók és ellenőrizhetők maradjanak.

INFOKUMMINIKÁCIÓ 2025

A mesterséges intelligencia és az adatfúzió hatása a katonai döntéshozatlra

PÁL ANITA
ÓBUDAI EGYETEM
BIZTONSÁGTUDOMÁNYI DOKTORI ISKOLA

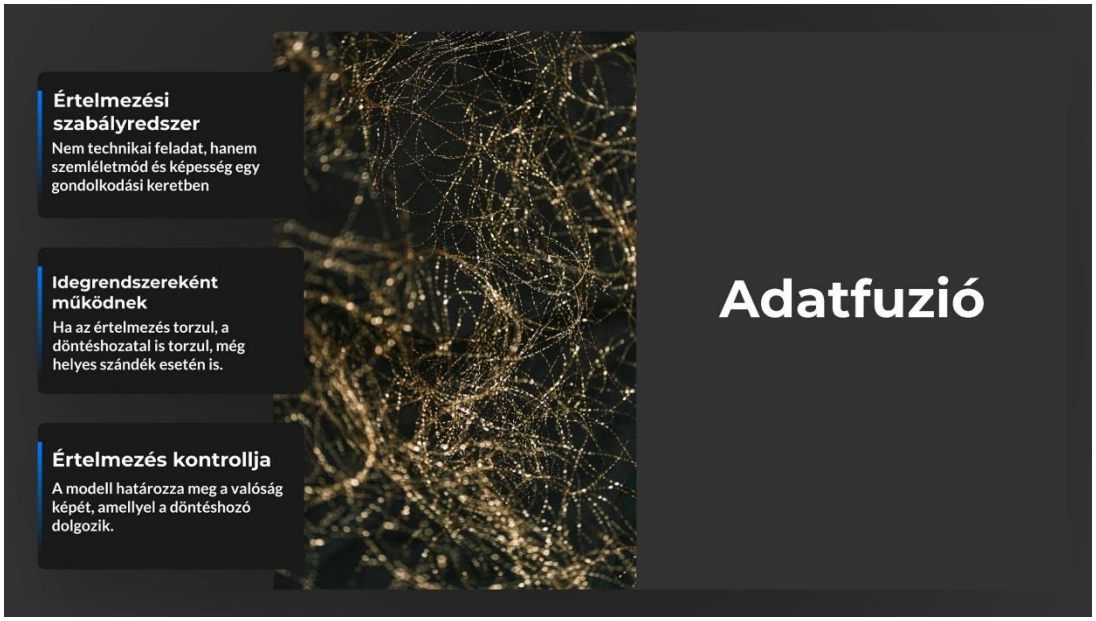
INFOKUMMINIKÁCIÓ 2025

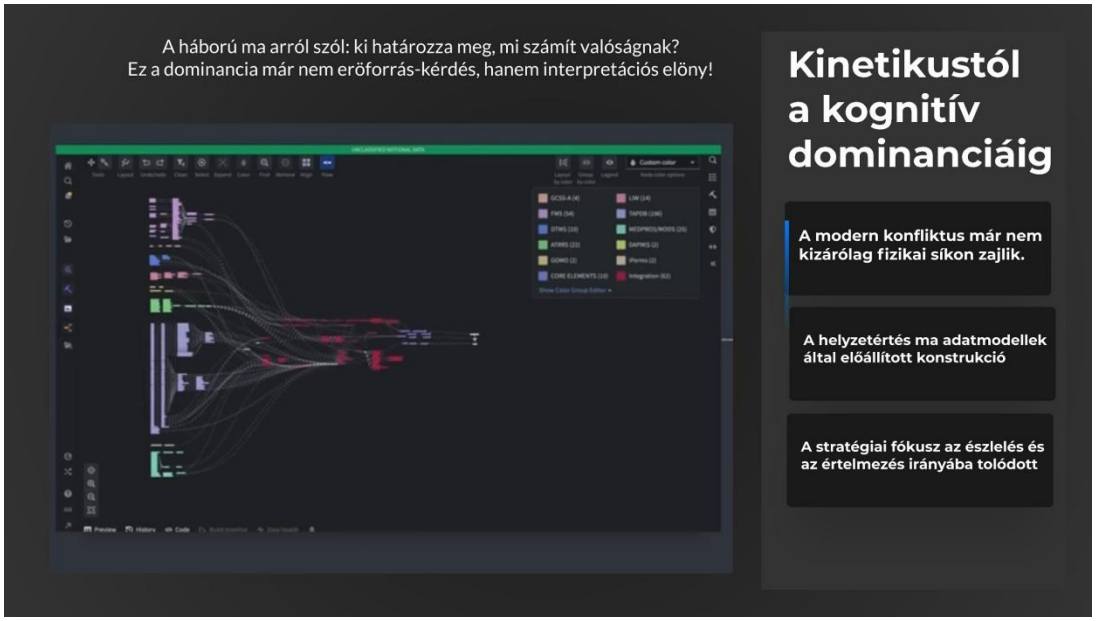
A mesterséges intelligencia és az adatfúzió hatása a katonai döntéshozatlra

PÁL ANITA
ÓBUDAI EGYETEM
BIZTONSÁGTUDOMÁNYI DOKTORI ISKOLA

A katonai döntéshozó nem a valóságot látja, hanem a modell által rekonstruált valóság képletét.

A kérdés az: bízhatunk-e a tükörben?


Értelmezési szabályredszer
Nem technikai feladat, hanem szemléletmód és képesség egy gondolkodási keretben
Idegrendszereként működnek
Ha az értelmezés torzul, a döntéshozatal is torzul, még helyes szándék esetén is.
Értelmezés kontrollja
A modell határozza meg a valóság képét, amellyel a döntéshozó dolgozik.
Adatfuzió

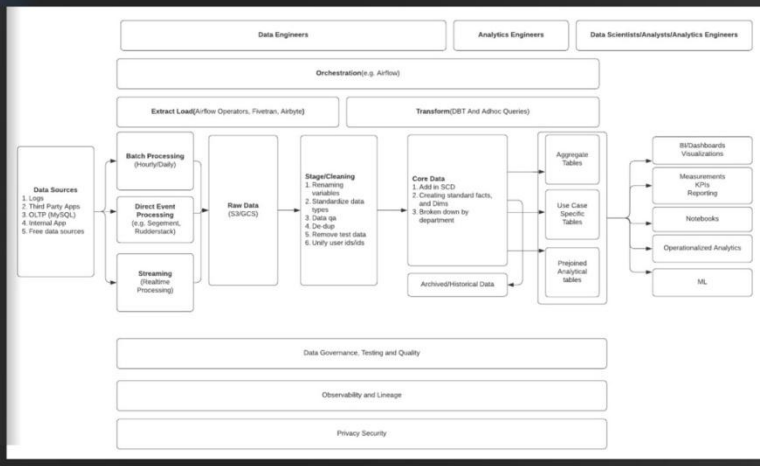

A háború ma arról szól: ki határozza meg, mi számít valóságnak?
Ez a dominancia már nem erőforrás-kérdés, hanem interpretációs előny!
Kinetikustól a kognitív dominanciáig
A modern konfliktus már nem kizárólag fizikai síkon zajlik.
A helyzetértés ma adatmodellek által előállított konstrukció
A stratégiai fókusz az észlelés és az értelmezés irányába tolódott

Az adatintegritás mint stratégiai célpont

Nem a rendszer leállítása a cél, hanem a valóság torzítása

Kis módosítás → nagy stratégiai eltérés

A legveszélyesebb rendszer az, amely jól működik, de rossz valóságot mutat



Gotham: A nemzetbiztonság szolgálatában

A Gotham a nemzetbiztonsági és védelmi szervek számára készült, lehetővé téve a hatalmas, strukturálatlan adatállományok, mint például telefonhívások és mozgási adatok, gyors átvizsgálását és összefüggéseik feltárását.

Foundry: Az üzleti szektor támogatása

A Foundry a vállalati szektort célozza, nagyvállalatok és logisztikai hálózatok számára nyújtva megoldásokat az adatok összekapcsolására és az üzleti döntéshozatal támogatására.

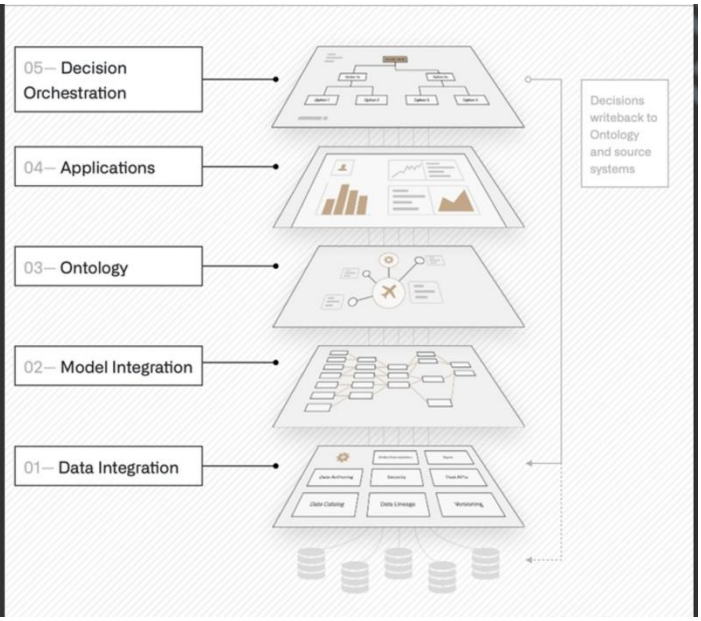
Az értelmezési réteg és a külső MI rendszerek

Számos kritikus rendszer magánfejlesztésű MI-re támaszkodik.

Ezek a rendszerek meghatározzák, mit látunk és hogyan értjük azt.

Ha a modell nem szuverén, akkor a döntés sem feltétlenül az.

Az értelmezés feletti kontroll egyben a cselekvés feletti kontroll.



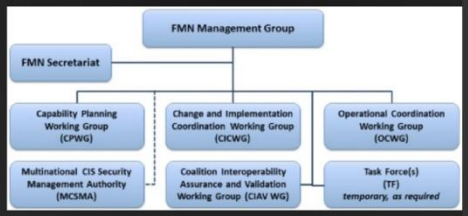
A stratégiai súlypont a kognitív térbe helyeződik át

Az információ hitelessége minden stratégiai döntést befolyásol

A szuverenitás feltétele az adatok és az értelmezés feletti kontroll

A szuverenitás feltétele az adatok és az értelmezés feletti kontroll

NATO - Zero Trust



A bizalom mint nemzetbiztonsági érték


A védelem jövője egyszerre lesz fizikai és kognitív
A „valóság” egyre inkább modelleken keresztül konstruálódik
A védelem jövője egyszerre lesz fizikai és kognitív
Összegzés és következtetések

Bodnár István: Alacsony késleltetésű rendszerek terepi felhasználása

Do you know the story of how the famous Rotschild family became rich? To put it simply, their secret was that the British army at the time of the Napoleonic wars did not yet have low-latency data transmission systems and the Rotchilds' „data transmission system" was faster.

Nowadays in the modern warfare, the speed of decision-making is crucial. In my presentation, I will focus on how technological advances are helping this process: zero-latency systems enable immediate response in data processing and transmission, while low-latency solutions keep critical response times to a minimum. At the same time, predictive analytics and artificial intelligence-enabled models predict situations with mathematical accuracy, optimising operations. In my theoretical framework, I detail the differences between these concepts, their effectiveness, and their synergies.

In the practical applications section, I demonstrate the impact of the technologies through concrete examples. Emphasis will be placed on systems using real-time sensor, which can react almost instantaneously from threat identification to neutralisation. At the same time, I analyse the challenges of low-latency guidance and target prediction for hypersonic weapons, with an indication of future directions for development. The presentation will outline how these innovations are reshaping warfare strategies, while revealing technical limitations and ethical dilemmas.

Ismerik Önök a történetet, hogy a híres Rotschild család hogyan gazdagodott meg? Leegyszerűsítve a választ, az volt a titkuk, hogy a brit hadsereg a napóleoni háborúk idején még nem rendelkezett alacsony késleltetésű adatátviteli rendszerekkel és az Rotchildok „adatátviteli rendszere” gyorsabb volt.

Mára már a modern hadviselésben a döntéshozatal sebessége döntő szerepet játszik. Előadásomban arra fókuszálok, hogyan segítik a technológiai fejlesztések ezt a folyamatot: a nulla késleltetésű rendszerek azonnali reagálást tesznek lehetővé az adatfeldolgozás és -továbbítás területén, míg az alacsony késleltetésű megoldások a kritikus válaszidőket tartják minimális szinten. Ezzel párhuzamosan a prediktív elemzési módszerek és a mesterséges intelligencia által támogatott modellek matematikai pontossággal előre jelzik a helyzetek alakulását, optimalizálva a hadműveleteket. Elméleti keretrendszeremben részletezem e fogalmak közötti különbségeket, hatékonyságukat, valamint azok összefüggéseit.

A gyakorlati alkalmazásokon keresztül bemutatom részben konkrét példákon keresztül a technológiák tulajdonságait. Kezdve olyan egyszerű megoldásoktól, mint a TEMPEST számítógépek videójeleinek valós idejű továbbítása és harctéren való feldolgozása. Összetettebb rendszereket képviselnek a valós idejű szenzorfúzióval működő rendszerek, amelyek a fenyegetések azonosításától a semlegesítésig szinte azonnal reagálnak. Ugyanakkor a hiperszonikus fegyverek esetében az alacsony késleltetésű irányítás és a célpont-előrejelzés kihívásait elemzem, utalva a jövőbeni

fejlesztések irányaira. Előadásomban bemutatom, hogyan alakítják át ezek az innovációk a hadviselés stratégiáit, egyben feltárva a technikai korlátokat és az ilyenkor szokásos kérdésként felmerülő etikai dilemmákat.

Nemzeti Közszolgálati Egyetem Ludovika

nmhh Nemzeti Média- és Hírközlési Hatóság

JUBILEUMI TUDOMÁNYÜNNEP 2025

Field use of low latency systems

OF-2 BODNÁR, István – NUPS MSDS doctoral student

Infocommunication 2025

13.11.2025.

What is the latency?

I wish you a successful and happy New Year in 2020!

MÁV

Low latency refers to the minimum delay between processed input and corresponding output.
Technically speaking, it is the short interval of time during which data travels from its source to its destination.

Source: https://www.maris-tech.com/blog/low-latency-its-impact-on-security-and-commerce-maris-tech/

Historical example

„ Whoever possesses information possesses the world”.
Nathan Rotschild

Napoleonic Wars – message sent via Rothschild's telegraph network.

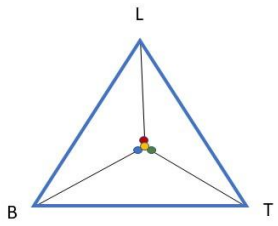
From Waterloo, Belgium, to London, Great Britain. Distance: 400 km.

- June 18, 1815 – British army victorious at Waterloo. **WE WON**
- June 19, 1815 – 6-bit message delivered to London in 1 day
- June 21, 1815 – Official message in London from the royal messenger – three times slower.

This example illustrates that low-latency communication was already a key strategic resource in the 19th century.

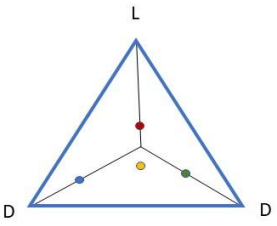
Bandwith, distance, latency

XIX. century and first half of XX. century



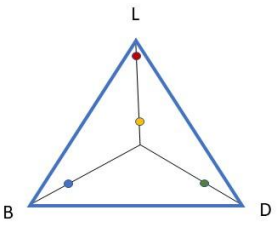
Telegraph equipment, Telephone Herald, Invention of the radio (1895)

Second half of XX. century



Fiber optics for communication purposes (1966), Digitalization, The advent of modern computers

Nowadays



CDN, 5G (URLLC), Edge Computing, Gigabit bandwidth even on the last mile

Why the latency is neccessery?

Highlighted: civil, military, financial sector

Critical infrastructure
- Stock exchange (trading systems)
- Healthcare systems (telemedicine)
- Traffic control (autonomous vehicles)

Industrial applications
- Industry 5.0 – human-machine collaboration
- Computationally intensive tasks
- Predictive maintenance

User experience
- VR/AR applications
- Online games (cloud gaming)
- Real-time video conferencing

Military applications
- Autonomous combat systems
- C4ISR systems
- Battlefield status indication

Classification of the latencies

Low latency
- Machine-human interaction.
- Extreme values: zero latency and the limits of the technology used.

Zero latency
- Machine-machine interaction.
- Maximum (ultra) 50-150 ms (depending on technology) ITU-T 114G – for one-way communication.

Real-time data transfer
- Machine-to-machine interaction.
- Does not exist, physical limit is the speed of light in a vacuum.
- We mean a delay between 0 and 50 ms.
- Mathematical functions, statistics, edge network, AI.

Low latency – from military POV

Theoretical basics → Practical implementation

Zero- and low-latency systems are not just theoretical concepts, but decisive factors in modern warfare.

Predictive methods and hardware innovations (e.g., CPU, GPU, FPGA) enable real-time decision-making.

System integration enables:

- Immediate situation updates
- Accurate threat detection
- Fast and effective responses

Analysis of specific systems:

- Zero latency radar systems (e.g., ELM-2084)
- Zero latency missile control (e.g., NASAMS)
- Real-time video transmission in command systems (PCoIP, BlastExtreme)

Real-time data transfer systems

IT solutions: CDN, edge network devices

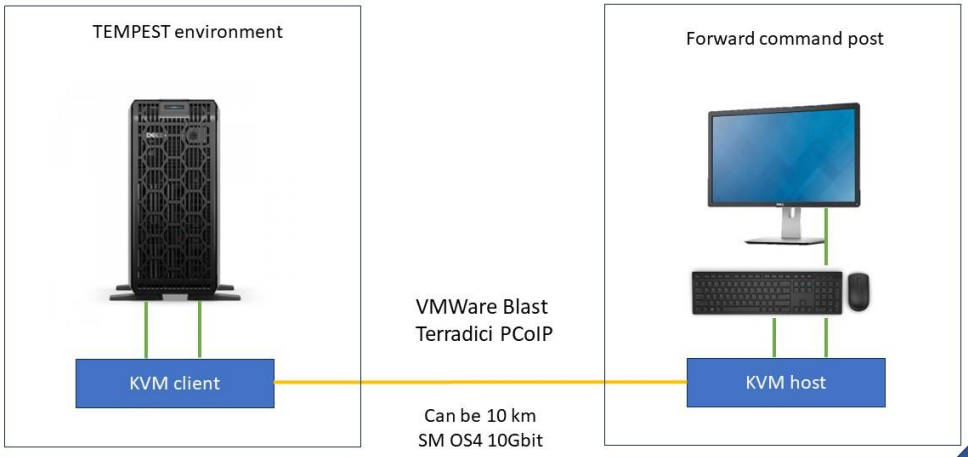
Statistical methods:

- Jitter buffering
- Adaptive bitrate (streaming)
- Algorithm or AI-based prediction – 95% certainty

Mathematical models:

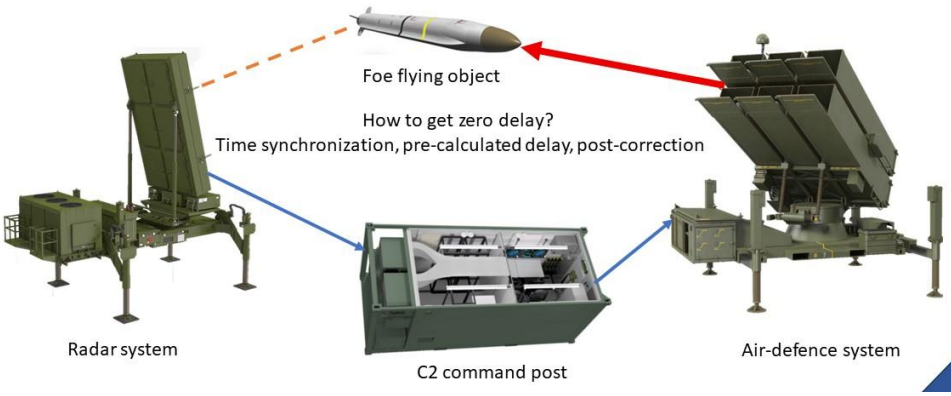
- Time series forecasting (machine learning)
- Network traffic profiling
- FEC (forward error correction)
- Differential coding (change transfer)
- Delay compensation (time transposition)

Simple example from the field



Complex example from the field

Missile interception with radar and destruction with anti-missile



Beyond the technology: the organisational latency

Low Latency (National) Defence (outlook)

The Challenge: Organizational Slowness in an Age of Rapid Threats From Tactics to Strategy

Technology is not everything: Technical delays can be reduced, but decision-making is hampered by bureaucracy and outdated procedures.

Example: The Microsoft Exchange incident (2021) – attacks went unnoticed for weeks because the reporting chain is slow and information gathering is not real-time.

Cultural Barrier: There is resistance even to new technologies (e.g., AI) – preference for old manual processes that seem secure.

Source: Mun Hwa C. (2025). Beyond the Briefing: Building a Zero Latency Defence for the Next Wave of Threats [Post]. https://www.linkedin.com/pulse/beyond-briefing-building-zero-latency-defence-next-wave-mun-hwa-chooi-vuigc/

Beyond the technology: the organisational latency

Low Latency (National) Defence (outlook)

The Solution: Low Latency (National) Defence (LLD)

Goal: Accelerate decision-making and action.

Three key elements:

- Break down data silos: Uninterrupted, automatedinformation flow.
- Mission-oriented leadership: Independent decision-making onsite, without unnecessary approvals.
- AI integration: Real-time threat detection and analysis.

The bottom line: Success is determined by management'scommitment to reviewing traditions and digitaltransformation.


NEMZETI KÖZSZOLGÁLATI EGYETEM
LUDOVIKA
nmhh
Nemzeti Média- és Hírközlési Hatóság
JUBILEUMI
TUDOMÁNYÜNNEP
2025
Thanks you for your attention!
Field use of low latency systems

Dr. Magyar Sándor: Tudás vagy attitűd? Az emberi tényező fejlesztésének dilemmái a kiberbiztonságban

Az előadás az emberi tényező és annak fejlesztésével foglalkozik a kiberbiztonság fókuszában. Kihangsúlyozza, hogy napjainkban ezen a területen már nem elég csak tudást, készséget adni a munkavállalóknak, hanem mindemellett a hozzáállásukat és a szokásaikat is változtatni kell. Sok esetben a biztonsági incidensek nem bonyolult technikai rendszerek hibái miatt keletkeznek, hanem pont a figyelmetlenségből, megszokásból vagy rossz döntésekből fakadóan. Ha valaki ismeri a szabályokat, de nem érzi magáénak őket, vagy nincs belső motivációja betartani azokat, abban az esetben a szervezet továbbra is sérülékeny marad. A biztonságtudatosság ebben az esetben azt jelenti, hogy a mindennapi rutinok, reflexek és döntések is a biztonság felé mutatnak.

Az előadás külön kitér arra, hogy más a biztonságtudatosítás és más a képzés. A képzés aktív tanulást jelent, ahol az emberek gyakorolnak, kérdeznek és visszajelzést kapnak, ezáltal a tudásuk és képességük gyarapodik. A tudatosítás pedig elsősorban felhívja a figyelmet a lehetséges kockázatokra, olyan módon, hogy a résztvevők attitűdje változzon. Ma már sokféle eszköz segítheti ezt. Nemcsak tantermi oktatásról vagy e-learning tananyagról lehet szó, hanem hírlevelekről, rövid figyelmeztetésekről, játékos megoldásokról, például szabadulószobáról, társasjátékról vagy szituációs gyakorlatokról is. Ezek a módszerek közelebb hozzák a

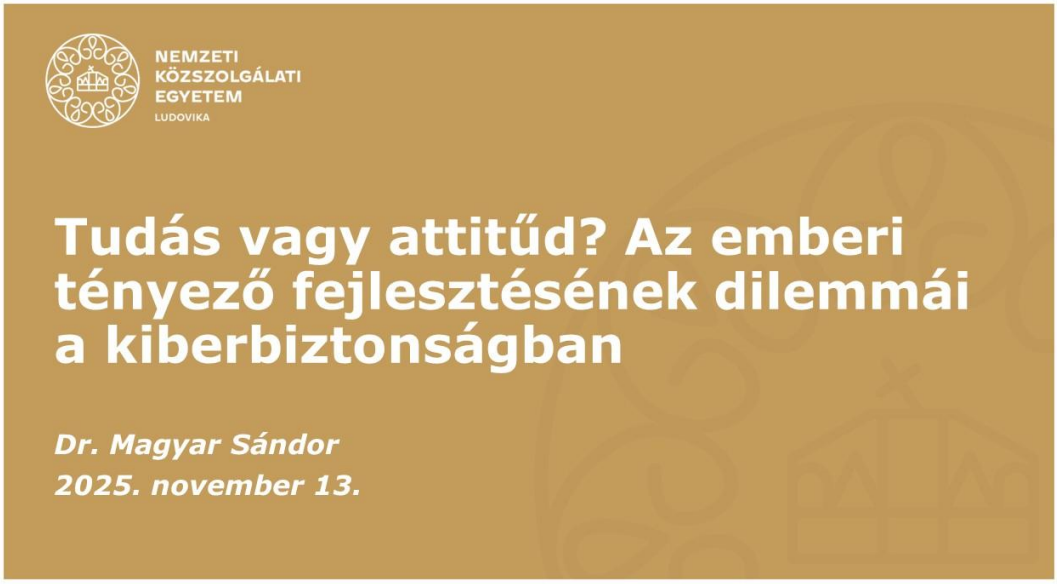
témát a hétköznapi munkához, érthetővé teszik a kockázatokat és élményalapú tanulást adnak, ami jobban hat a viselkedésre. Míg a tudás könnyen fejleszthető tananyagokkal interaktív oktatási anyagokkal, addig a tudatosítás a gyakorlati szituációkkal, esettanulmányok átbeszélésével fejleszthető jobban.

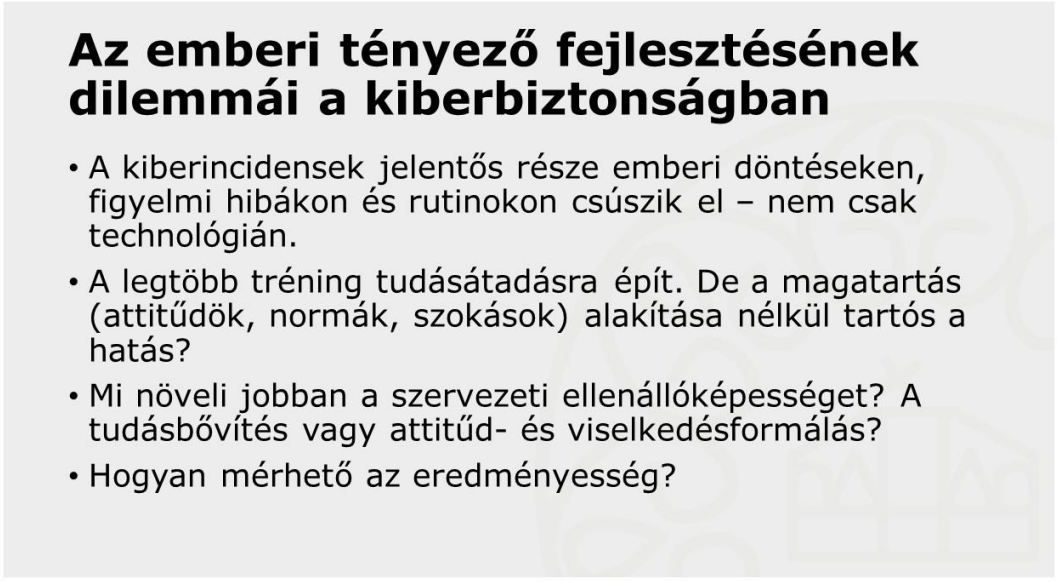
A tudatosítás esetében fontos szerepet kapnak a kibervédelmi gyakorlatok is. Ezek segítenek abban, hogy a szervezetek kipróbálják, hogyan reagálnának egy kibertámadásra vagy válsághelyzetre. Vannak olyan gyakorlatok, amelyek a vezetők döntéshozatali képességét fejlesztik és vannak kifejezetten technikai jellegűek is, amelyek az incidensek kezelésére és a védekezés lépéseire koncentrálnak. A nagyobb, összetettebb gyakorlatok több területet és csapatot vonnak be, és javítják az együttműködést szervezeten belül és szervezetek között. Így nem csak új tudás születik, hanem olyan tapasztalat is, amely valódi helyzetben gyorsabb és biztosabb reakcióhoz vezet.

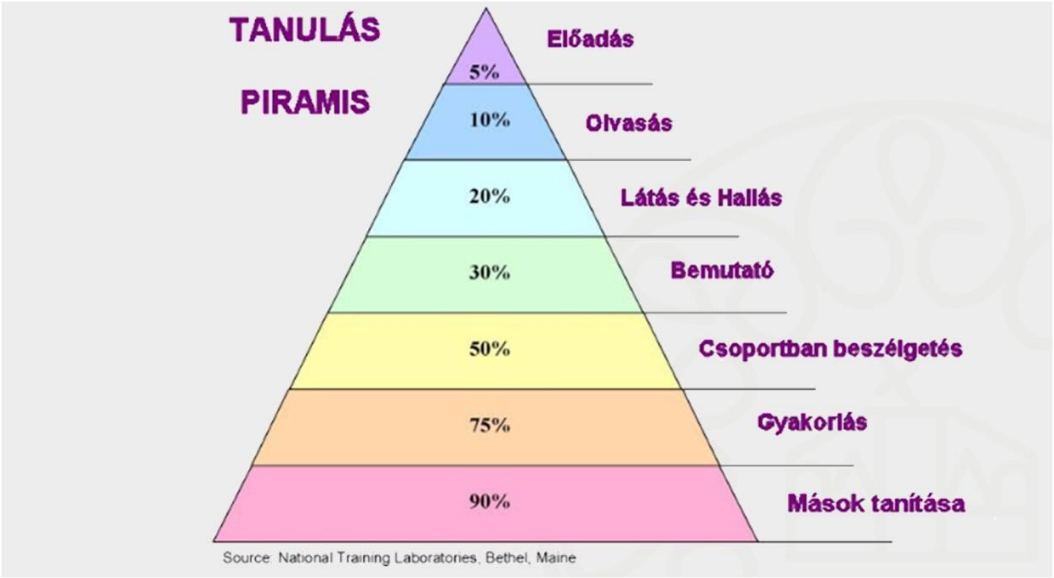
Az előadás modern példát is említ. Egy kiberbiztonsági promptoló versenyt, ahol a résztvevők mesterséges intelligenciának fogalmaznak meg átgondolt, jól felépített utasításokat. Ez egyszerre fejleszti a mesterséges intelligencia biztonságos és hatékony használatát, a kockázatfelismerést a promptok megfogalmazásában, a kreativitást és az együttműködést, és jól mutatja, hogy ma már a tanulás nem csak passzív előadásokból állhat.

Az előadás fő üzenete az, hogy a tudás önmagában kevés, ha nem párosul az attitűd, a szokások és a szervezeti kultúra alakításával.

Aki sikeres akar lenni a kiberbiztonság területén, annak változatos módszereket kell használnia, folyamatosan mérnie kell ezek hatását és nyitottnak kell lennie az új, gamifikált vagy mesterséges intelligencián alapuló eszközök bevezetésére is.


NEMZETI
KÖZSZOLGÁLATI
EGYETEM
LUDOVIKA
Tudás vagy attitűd? Az emberi tényező fejlesztésének dilemmái a kiberbiztonságban
Dr. Magyar Sándor
2025. november 13.


Az emberi tényező fejlesztésének dilemmái a kiberbiztonságban
• A kiberincidensek jelentős része emberi döntéseken, figyelmi hibákon és rutinokon csúszik el – nem csak technológián.
• A legtöbb tréning tudásátadásra épít. De a magatartás (attitűdök, normák, szokások) alakítása nélkül tartós a hatás?
• Mi növeli jobban a szervezeti ellenállóképességet? A tudásbővítés vagy attitűd- és viselkedésformálás?
• Hogyan mérhető az eredményesség?



Tudás

- Olyan ismeret, amelyet tanulással vagy tapasztalatból szerzünk meg.
- Gyakorlati tudás olyan készség, amelyet gyakorlással sajátítunk el.

Biztonságtudatosság

- A munkavállalók hozzáállását, motivációját és hajlandóságát tükrözi a biztonsági szabályok betartására és a biztonságtudatos viselkedésre.

Tudás vagy attitűd

- A kiberbiztonsági kockázatok csökkentéséhez a tudás és az attitűd együttes fejlesztésére van szükség.

Biztonságtudatosság

- A tudatosság nem egyenlő a képzéssel.
- A tudatosságot célzó előadások célja egyszerűen csak a figyelmet a biztonságra irányítani. […] A tudatosságot célzó tevékenységekben a tanuló az információ befogadójának szerepét tölti be, míg a képzési környezetben a tanuló aktívabb szerepet játszik.

Információbiztonsági tudatosítás lehetőségei

- Személyes tudatosító képzések.
- E-learning.
- Hírlevelek.
- Azonnali tájékoztatások (e-mail, üzenet).
- Információbiztonsági szabadulószoba.
- Kiber/információbiztonsági társasjátékok.
- Szituációs játékok.
- Chatbot.
- …

A kibervédelmi gyakorlatok

- Felkészülés a kibertérből érkező fenyegetésekre.
- Készségek fejlesztése.
- A sebezhető pontok felismerése és azonosítása.
- Új eljárások tesztelése.
- Az együttműködés és az információcsere elősegítése:
  - szakmai területek között;
  - szervezetek között;
  - nemzetek között.

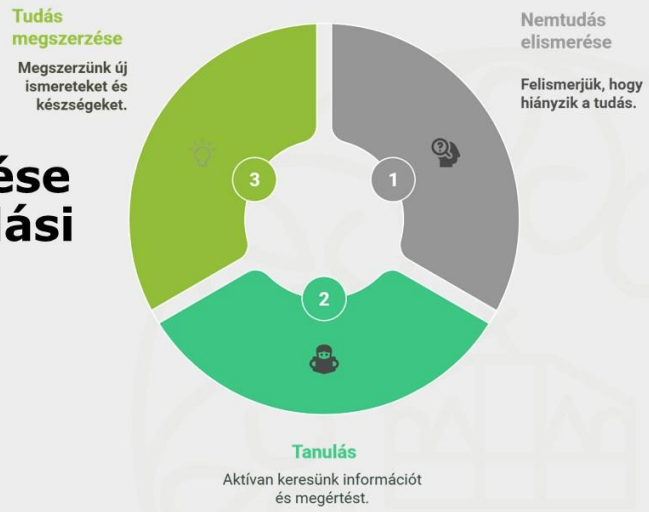
Kibervédelmi gyakorlatok fajtái

- Table Top Exercise.
  - „Asztal mellett” lehetőséget a szakembereknek a forgatókönyv szerinti vészhelyzetek, támadások elleni intézkedések, cselekvési tervek kidolgozására.
- Stratégiai döntéshozatali.
  - Pl. válságkezelési képességek fejlesztése
- Technikai.
  - Eseménykezelési;
  - Nyomrögzítési;
  - Támadó-védekező (Red Team – Blue Team)
  - Stb.
- Komplex.

Kiberbiztonsági promptoló verseny

- A résztvevők együttműködését ösztönző, problémamegoldó gondolkodásra épülő promptoló verseny, amely során egy adott védelmi fókuszú kiberbiztonsági problémára dolgoznak ki megoldásokat.

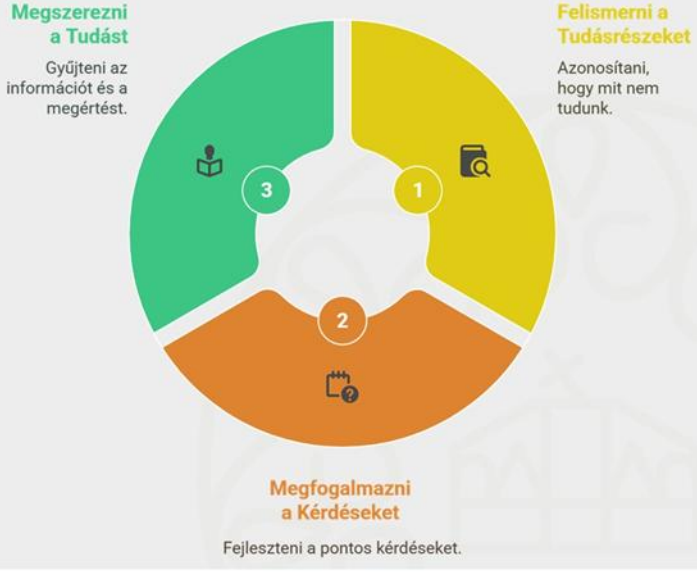
Eredmény elérése régi módi tanulási folyamattal



Promptolás

- A promptolás olyan eljárás vagy módszertan, amelynek során a felhasználó célzott utasításokkal látja el a mesterséges intelligenciát annak érdekében, hogy a kívánt választ vagy tartalmat generáltassa vele.
- A promptolás lényege, hogy strukturált, egyértelmű és célszerű bemenetet adjunk az MI-rendszernek, így befolyásolva annak kimenetét és növelve a válasz minőségét.

Eredmény elérése az módszerrel



Összegzés

- A kiberbiztonsági incidensek jelentős része emberi hibákra vezethető vissza, ezért kulcsfontosságú, hogy a szervezetek megfelelő hangsúlyt fektessenek a munkavállalók képzésére és a biztonságtudatos szemlélet kialakítására.
- A kiberbiztonság területén az emberi tényező fejlesztése folyamatos és komplex feladat.
- Az információbiztonsági tudatosítást nem lehet uniformizáltan kezelni.
- Stratégiai gondolkodás szükséges.

KÖSZÖNÖM A FIGYELMET!

uni-nke.hu

Oláh István: A hálózat gondolatAI?

Előadásomban az infokommunikáció és mesterséges intelligencia (AI) fejlődését, jelenlegi képességeit és a hálózatok biztonsági kockázatait mutattam be, különös hangsúllyal a hálózati megoldásokra, és a jövő kihívásaira.

Az emberiség több ezer éve használ számolóeszközöket, az abakusztól a logarlécen át a programozható gépekig. A 20. század közepén megjelent az első elektronikus számítógép (Colossus, ENIAC), majd a Neumann-elvek szerinti számítógépek. Az ENIAC létrejöttének oka, az emberi számolási képességek meghaladása volt, azaz az első számítógép is egyfajta AI-ként épült meg. Az AI története az 1960-as évektől kezdve folyamatosan fejlődött: LISP nyelv, ELIZA, szakértői rendszerek, majd a gépi tanulás, deep learning és generatív modellek. Mérföldkövek közé tartozik Kaszparov és az IBM Deep Blue párharca (1997), az IBM Watson (2011), valamint a GAN-ok és LLM-ek megjelenése.

Az előadásomban tisztáztam az AI, a gépi tanulás, a deep learning és a generatív AI fogalmait. Az AI képességei ma már kiterjednek a természetes nyelvi chatbotokra, fejlett keresésre, szöveggenerálásra, valós idejű fordításra, képfelismerésre és képgenerálásra. Ugyanakkor az AI képes hackelésre is, valamint az információbiztonsági védekezésben is jelentős szerepet kapott.

Nemzetközi szervezetek (pl. NIST, ENISA) keretrendszereket dolgoztak ki az AI kockázatainak kezelésére. A NIST 2023-ban publikálta az AI Risk Management Framework-öt, amely

iránymutatásokat ad a megbízható AI bevezetésére. A főbb szempontok: megbízhatóság, biztonság, ellenállóság, átláthatóság, adatvédelem és tisztességesség. Az EU AI Act és a GDPR kapcsolódása is kiemelt jelentőségű. Az ENISA szerint a kibertámadások 80%-a már AI-alapú, a leggyakoribb támadások adathalászattal kezdődnek. A nagy nyelvi modellekhez az LLM-ekhez kapcsolódó fenyegetések közé tartozik a prompt injection, training data poisoning, model inversion, evasion attack, model stealing, supply chain attack, hallucination és túlzott autonómia.

Előadásomban bemutattam, hogy az AI már 25 éve jelen van a hálózati védelmekben (proxy, IDS, IPS, sandbox). Ma már GenAI-alapú megoldások is elérhetők, mint tűzfalak, routerek, switchek. Az AI magyarázható működésű lehet, auditálható és verifikálható, ha megfelelően fejlesztik. Az auditok során fontos a külső független ellenőrzés, a konfidencia intervallumok és a biztonsági küszöbök meghatározása. Emiatt olyan AI hálózati megoldások használatát javaslom, amelyek működését, matematikai alapjait, a felhasználók ismerik és értik.

Felhívtam a figyelmet a szingularitás lehetőségére, amikor az emberi és gépi intelligencia teljesen összeolvad. A jelenleg üzemben álló AI megoldások még nem okosabbak az embernél. A jövő architektúrái közül a kvantumszámítástechnikai eszközön alkalmazott AI megoldásokkal vélhetően építhető lesz olyan számítógép, amely már okosabb lesz az embernél. A jövő kulcsterületei közé tartozik a kvantumbiztonság, a

kvantumtechnológia, felhő és AI integrációja, valamint új irányok, mint a biológiai és matematikai processzorok.

Az előadásomban hangsúlyoztam, hogy az AI fejlődése nemcsak lehetőségeket, hanem komoly biztonsági és etikai kihívásokat is jelent a hálózatokban. A jövőben a kvantumtechnológia, a felhő és az AI integrációja új korszakot nyithat, amelyben a szabályozás, az auditálhatóság és a felelős használat kulcsfontosságú lesz a hálózatbiztonság szempontjából.

ÓBUDAI EGYETEM
BÁNKI DONÁT GÉPÉSZ ÉS BIZTONSÁGTECHNIKAI MÉRNÖKI KAR

Egy hálózat GondolatAI

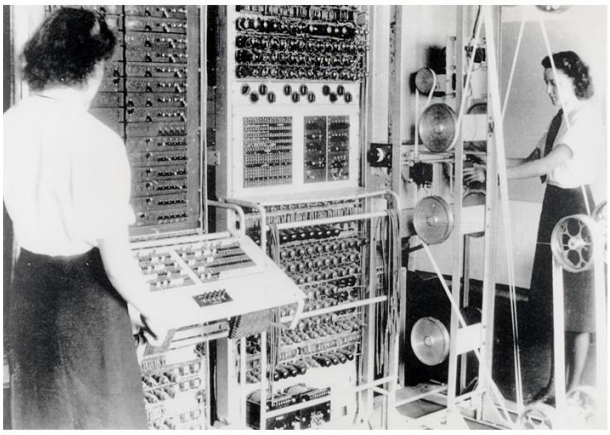
Oláh István doktorandusz

Infokommunikáció 2025 Nemzetközi tudományos-szakmai konferencia
2025. november 13.
NKE Zrínyi Miklós Laktanya és Egyetemi Campus M. Szabó Miklós altábornagy Díszterem, Budapest

ÓBUDAI EGYETEM
BÁNKI DONÁT GÉPÉSZ ÉS BIZTONSÁGTECHNIKAI MÉRNÖKI KAR

A szoftverek (AI) uralják a fizikai eszközöket (embereket?) is !?

- 30 000 éves az első számoló eszköz
- 5.000 éves az abakusz
- 1620 logarléc
- 1623 első számológép
- 1786 TPV=regiszter
- 1812 programozható számlógép, memóriával
- 1820 TPV alapú szövőgép
- 1853 integrált „áramkör” elmélet
- 1887 statisztikai gép USA-népszámlálás
- 1936 elektromechamikus számológép
- 1939 Z1 szabadon programozható gép, No.
- **1943 Colussus Anglia, nem decimális (az AI kezdete)**
- 1944 ENIAC USA
- 1945- Neumann-elvek szerinti gépek USA (előtte Mao?)



ÓBUDAI EGYETEM
BÁNKI DONÁT GÉPÉSZ ÉS BIZTONSÁGTECHNIKAI MÉRNÖKI KAR

AI történelem

- Már az első számítógép is AI machine volt
- 1960 LISP első AI „nyelv” (család)
- **1962 Hazai egyetemeken oktatott tárgyakban benne van az AI**
- 1965 ELIZA-MIT
- 1969 Szakértői rendszerek, MYCIN
- 1985 az első AI appom
- 1990 ML algaritmusok elérhetőek a civil szférában is, elsőre a fordító appok jöttek
- **1997 Garri Kaszparov-IBM Depp Blue**
- 2006 Deep learning új modellek
- 2011 IBM Watson, nyelvi modellek LLM
- 2014 GAN: Generatív Adeversial Networks
- sok az elérhető adat (de tiszta-e?), olcsó=skálázódó feldolgozási technológiák

ÓBUDAI EGYETEM
BÁNKI DONÁT GÉPÉSZ ÉS BIZTONSÁGTECHNIKAI MÉRNÖKI KAR

Alapfogalmak

- **Artifical Intelligence:** a számítástechnika azon területe, amely olyan intelligens gépek létrehozására törekszik, amelyek képesek az emberi intelligenciát megismételni vagy meghaladni.
- **Machine Learning:** a mesterséges intelligencia olyan részhalmaza, amely lehetővé teszi a gépek számára, hogy a meglévő adatokból tanuljanak, és az adatok alapján döntéseket vagy előrejelzéseket hozzanak.
- **Deep Learning:** olyan gépi tanulási technika, amelyben neurális hálózatok rétegeit használják az adatok feldolgozására és a döntések meghozatalára.
- **Generative AI:** új írott, vizuális és auditív tartalmakat hoz létre kérések vagy meglévő adatok alapján

Forrás: Tóth Márton EIVOK-40

ÓBUDAI EGYETEM
BÁNKI DONÁT GÉPÉSZ ÉS BIZTONSÁGTECHNIKAI MÉRNÖKI KAR

Az AI szelleme „is” kiszabadul a palackból....

ÓBUDAI EGYETEM
BÁNKI DONÁT GÉPÉSZ ÉS BIZTONSÁGTECHNIKAI MÉRNÖKI KAR

Amit az AI tud?

- **Természetes nyelvi chatbotok**: az ügyfélszolgálattól kezdve a személyre szabott korrepetáláson át az öngyilkosság-megelőzési tanácsadók képzéséig minden
- **Fejlett keresési képességek**: nem csak linkek, hanem válaszok keresése
- **Szöveggenerálás**: e-mailek, jogszabálytervezetek, szerződések, forgatókönyvek
- **Tartalom** (hang, videó, szöveg) valós idejű fordítása, átírása, elemzése és összefoglalása
- **Képfelismerés és -generálás**. (Smink felismerés, stb.)

Forrás: Tóth Márton EIVOK-40

ÓBUDAI EGYETEM
BÁNKI DONÁT GÉPÉSZ ÉS BIZTONSÁGTECHNIKAI MÉRNÖKI KAR

Amit az AI tud-II?

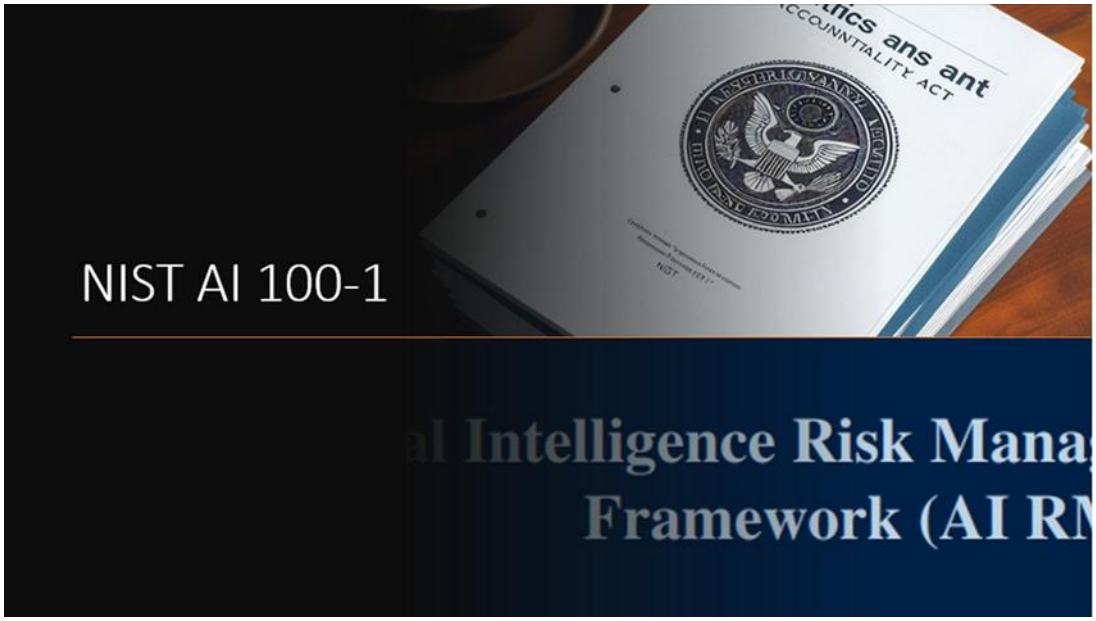
Hack-el, és … védekezik!

https://nki.gov.hu/it-biztonsag-kategoria/mesterseges-intelligencia/
https://nki.gov.hu/wp-content/uploads/2023/03/A-ChatGPT-kiberbiztonsagi-kockazatai_CTI_jelentes.pdf

ÓBUDAI EGYETEM
BÁNKI DONÁT GÉPÉSZ ÉS BIZTONSÁGTECHNIKAI MÉRNÖKI KAR

AI veszélyre felhívó nyilatkozatok

„A mesterséges intelligencia miatti kipusztulás veszélyét az olyan emberiségre leselkedő fenyegetésekkel egyenértékűen kell kezelni, mint a világjárványok vagy az atomháború.”



ÓBUDAI EGYETEM
BÁNKI DONÁT GÉPÉSZ ÉS BIZTONSÁGTECHNIKAI MÉRNÖKI KAR

National Institute for Standards in Technology (NIST) mesterséges intelligencia-kockázatAI

- 2021-ben a Kongresszus arra utasította a NIST-t, hogy dolgozzon ki egy önkéntes keretet a megbízható mesterséges intelligencia számára
- 2023: Artificial Intelligence Risk Management Framework (AI RMF 1.0)

Célja: olyan iránymutatások és bevált gyakorlatok gyűjteménye, amelyek célja, hogy segítse a szervezeteket a mesterséges intelligencia technológiák bevezetésével és használatával kapcsolatos kockázatok azonosításában, értékelésében és kezelésében

Forrás: Tóth Márton EIVOK-40

ÓBUDAI EGYETEM
BÁNKI DONÁT GÉPÉSZ ÉS BIZTONSÁGTECHNIKAI MÉRNÖKI KAR

Bővebben:

- **Érvényesség és megbízhatóság** – Az AI téves információkat is szolgáltathat, amit a GenAI-ban “hallucinációnak” is neveznek. Fontos, hogy a vállalatok validálni tudják, hogy az általuk alkalmazott mesterséges intelligencia pontos-, és megbízható-e
- **Biztonságosság** – Annak biztosítása, hogy az információkat ne osszák meg más felhasználókkal, mint a hírhedt Samsung ügyben
- **Ellenállóság és biztonság** – A szervezeteknek biztosítaniuk kell, hogy az AI rendszer védett és biztonságos legyen a támadásokkal szemben és sikeresen meg tudja hiúsítani a kihasználására vagy a támadások segítésére irányuló kísérleteket
- **Átláthatóság** – Fontos, szempont az AI működésének a megértése, hisz nincs benne semmiféle fekete mágia
- **Adatvédelem** – Biztosítani kell, hogy a kért információk védettek és anonimizáltak legyenek a felhasználás során
- **Tisztességesség** – A káros előítéletek kezelése (például az AI arcfelismerésben gyakran előfordul elfogultság, a világos bőrű férfiakat pontosabban azonosítják, mint a nőket és a sötétebb bőrszínűeket). Ha például a mesterséges intelligenciát a bűnüldözésben használják, ennek súlyos következményei lehetnek

Forrás: Tóth Márton EIVOK-40

ÓBUDAI EGYETEM
BÁNKI DONÁT GÉPÉSZ ÉS BIZTONSÁGTECHNIKAI MÉRNÖKI KAR

AI és a HACKING

- A klasszikus ITsec megoldásokat AI képessé kell tenni
- Az AI új kihívásaira új ITsec hálózati megoldások szükségesek

ENISA 2025. októberben publikálta a Threat Landsacpe 2025.összefoglalóját. Az Európai Unió 2022/2555 számú irányelve (NIS2) 6 szerinti ágazati besorolás szerint a pénzintézetek szolgáltatásai a hatodik legjobban támadott szolgálatatások a kibertérben jelenleg. A leggyakoribb támadások adathalászattal kezdődnek. Az ENISA szerint ezek

80% már AI alapú.

ÓBUDAI EGYETEM
BÁNKI DONÁT GÉPÉSZ ÉS BIZTONSÁGTECHNIKAI MÉRNÖKI KAR

AI + Large Language Model (LLM)

Az Új TOP

Támadás típusa	Rövid leírás	Főbb példák/hatás	Védekezési stratégia
Prompt Injection	Speciális bemenetekkel manipulált válasz	AI chat szakmai/etikai guardrail megkerülése	Szintaktikus és szemantikus szűrés, input validáció, guardrails, ember-a-hurokban jóváhagyás
Training Data Poisoning	Mérgezett, elfogult vagy rosszindulatú adatokkal tanított modell	Elfogult vagy hibás output, adatvédelmi sérülés	Adatforrás audit, anomaly detection, provenance tracking, adversarial tesztelés
Model Inversion / Membership Inference	Tanítóadatok visszafejtése, PII leak	Személyes adatok kiszivárgása	Differential privacy, likvid lekérdezésszám, titkosítás
Evasion Attack	Finoman módosított inputok, tévesztés céljából	Képfelismerési hibák, azonosítás megkerülése	Adversarial training, input transformation, ensemble modellek
Model Stealing (Extraction)	Modell „lemásolása”, funkcionalitás kisajátítása	IP, tulajdon ellopása	API rate limiting, query log, watermarking
Supply chain attack	Harmadik féltől származó kód, modell vagy dependency támadás	Backdoor/rosszindulatú könyvtár	SBOM, code audit, integrity check, rendszeres függőségfrissítés
Insecure Output Handling	Nem szűrt output, amely downstream rendszerben sérülékenységet okoz	XSS, SQL injection	Output validáció, sandbox, CSP
Hallucination/hamis tartalom	Hihető, de téves vagy veszélyes AI-válasz	Félretájékoztatás, reputációs kár	RAG, fact-check, audit, emberi kontroll
Excessive Agency	AI agent, nem kontrollált autonóm viselkedés	Nem kívánt művelet végrehajtása	Minimális jogosultság, naplózás, felülvizsgálat
Unbounded consumption/denial-of-wallet	Erőforrás (pl. API) túlhasználata/visszaélés	Szolgáltatáskimaradás	Limitálás, throttling, költség-alapú routing

ÓBUDAI EGYETEM
BÁNKI DONÁT GÉPÉSZ ÉS BIZTONSÁGTECHNIKAI MÉRNÖKI KAR

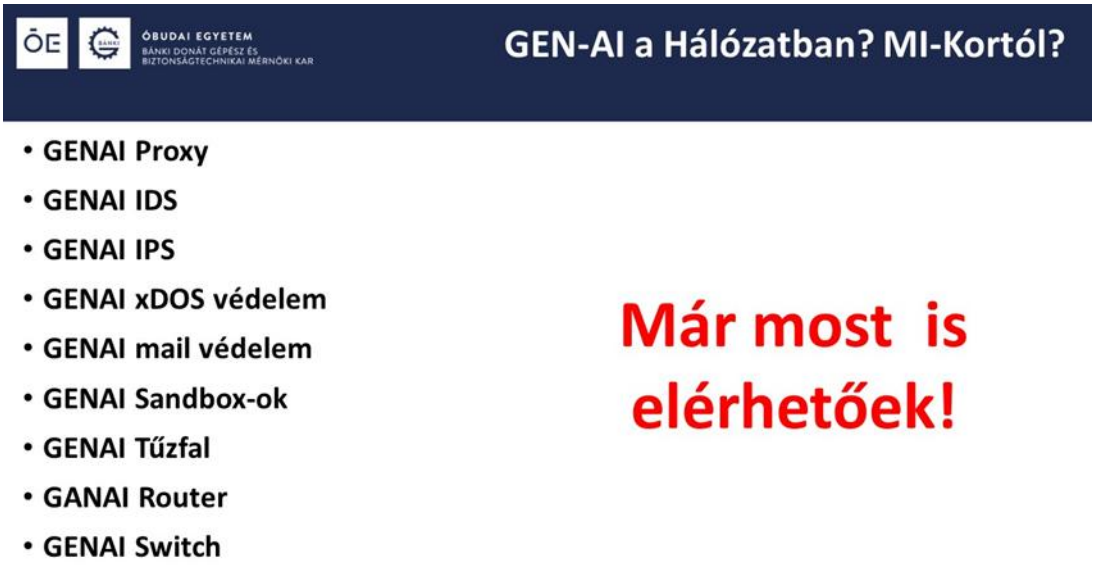
AI a Hálózatban? MI-ÓTA?

- **Hálózati Proxy**
- **Hálózati IDS**
- **Hálózati IPS**
- **Hálózati xDOS védelem**
- **Hálózati mail védelem**
- **Hálózati Sandbox-ok**

Heurisztika alapú működés

25+ éve

Neurális AI !



Ez az MI magyarázható működésű, mert MI fejlesztettük, ezért lehet auditáltatni, és verifikálni is lehet.

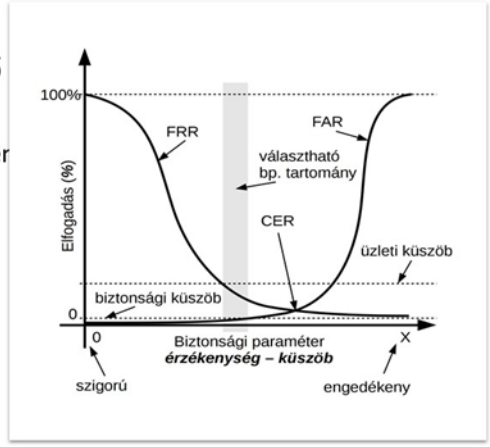
A modell úgy tanul, olyan adaton tanul, és azt tanulja amit MI szeretnénk, és nem azt amit mások!

Forrás: Golda Bence / op EIVOK-59

ÓBUDAI EGYETEM
BÁNKI DONÁT GÉPÉSZ ÉS BIZTONSÁGTECHNIKAI MÉRNÖKI KAR

Audit

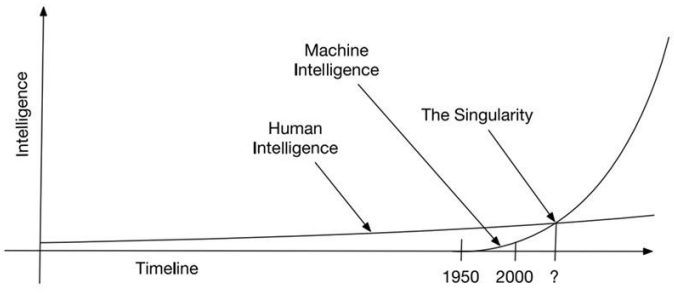
- Külső, független szereplő
- Magyarázható, mérhető, megismerhető az eredmény
  - “Érzésre” mégis más – egyedi esetek, egyén befolyása
- A számítások irreverzibilisek
  - Az eredeti aláírás nem állítható vissza!
- Negatív hipotézis + konfidencia intervallum
  → Elvetésre került → ✅



Forrás: Golda Bence EIVOK-59

ÓBUDAI EGYETEM
BÁNKI DONÁT GÉPÉSZ ÉS BIZTONSÁGTECHNIKAI MÉRNÖKI KAR

Szingularitás?



Forrás: Tóth Márton EIVOK-40

Forrás: Microsoft Copilot

ÓBUDAI EGYETEM
BÁNKI DONÁT GÉPÉSZ ÉS BIZTONSÁGTECHNIKAI MÉRNÖKI KAR

Fókusz a jövőben?

Kvantumbiztonság!

Kvantum+Felhő+AI?

Biológia + Matek processzorok

ÓBUDAI EGYETEM
BÁNKI DONÁT GÉPÉSZ ÉS BIZTONSÁGTECHNIKAI MÉRNÖKI KAR

Felhasznált Irodalom

1 *AI / LLM Biztonsági Szolgáltatások - KPMG Magyarország.* https://kpmg.com/hu/hu/home/services/advisory/technology/cyber-lab/ai-llm-security.html
2 *What Are Adversarial AI Attacks on Machine Learning?.* https://www.paloaltonetworks.com/cyberpedia/what-are-adversarial-attacks-on-AI-Machine-Learning
3 *NIST Identifies Types of Cyberattacks That Manipulate Behavior of AI ....* https://www.nist.gov/news-events/news/2024/01/nist-identifies-types-cyberattacks-manipulate-behavior-ai-systems
4 *NIST Trustworthy and Responsible AI NIST AI 100-2e2025* https://csrc.nist.gov/pubs/ai/100/2/e2025/final
5 *ENISA THREAT LANDSCAPE 2025* https://www.enisa.europa.eu/sites/default/files/2025-10/ENISA%20Threat%20Landscape%202025.pdf
6 *Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.) az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv) (EGT-vonatkozású szöveg) 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)* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555
7 *Megjelent a NIST Mesterséges Intelligencia kockázatkezelési keretrendszere* https://nki.gov.hu/it-biztonsag/hirek/megjelent-a-nist-mesterseges-intelligencia-kockazatkezelesi-keretrendszere/
8 *ISO/IEC 42001:2023 Information technology — Artificial intelligence — Management system* https://www.iso.org/standard/42001
9 *Az Európai Parlament és a Tanács (EU) 2024/1689 rendelete (2024. június 13.) a mesterséges intelligenciára vonatkozó harmonizált szabályok megállapításáról, valamint a 300/2008/EK, a 167/2013/EU, a 168/2013/EU, az (EU) 2018/858, az (EU) 2018/1139 és az (EU) 2019/2144 rendelet, továbbá a 2014/90/EU, az (EU) 2016/797 és az (EU) 2020/1828 irányelv módosításáról (a mesterséges intelligenciáról szóló rendelet) (EGT-vonatkozású szöveg)*
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) (Text with EEA relevance) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689
10 *Bankoknál, biztosítóknál vizsgálta a mesterséges intelligenciát, gépi tanulást az MNB* https://www.mnb.hu/sajtoszoba/sajtokozlemenyek/2023-evi-sajtokozlemenyek/bankoknal-biztositoknal-vizsgalta-a-mesterseges-intelligenciat-gepi-tanulast-az-mnb
11 *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) (Text with EEA relevance)* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679
12 *Survey Shows How Generative AI Puts Organizational AI Maturity to the Test* https://www.gartner.com/en/documents/5373863
13 *A (kiber)biztonság gyakorlatAI: Inspiráló előadások és beszélgetések a jövőhöz vezető úton - EIVOK-59.* https://www.hte.hu/informaciobiztonsagi-szakosztaly-eivok/-/esemeny/1/4975549/eivok-59-a-kiber-biztonsag-gyakorlatai
14 *AI alapú dokumentum hitelesítés a gyakorlatban* www.hte.hu/documents/10180/4963359/I-03_Golda+Bence.pdf
15 *Code security audit based on regulations at a financial institution* https://ieeexplore.ieee.org/document/11030093
16 *AI Governance Framework - AI Governance Framework.* https://ai-governance.eu/
17 *MULTILAYER FRAMEWORK FOR GOOD CYBERSECURITY PRACTICES FOR AI* https://www.enisa.europa.eu/sites/default/files/publications/Multilayer%20Framework%20for%20Good%20Cybersecurity%20Practices%20for%20AI.pdf
18 NIST *AI Risk Management Framework* https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf
19 *REGULATIONS REGULATION (EU) 2022/2554 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011*
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2554
20 13 *Az EU AI Act és a GDPR kapcsolódásai* –https://dmp.hu/adatvedelem/az-eu-ai-act-es-a-gdpr-kapcsolodasai/
21 Megfelelés az AI Act-nek - gyakorlati példák az adatvédelmi feladatokra. https://www.jogiforum.hu/blog-adatvedelem-10/2024/10/11/megfeleles-az-ai-act-nek-gyakorlati-peldak-az-adatvedelmi-feladatokra/
22 *A generatív AI adatvédelmi kockázatai – Jogászvilág.* https://jogaszvilag.hu/vilagjogasz/a-generativ-ai-adatvedelmi-kockazatai/
23 *How to Scale Your Finance AI Pilots* https://www.gartner.com/en/documents/6285783
24 *OWASP Top 10 for Large Language Model Applications* https://owasp.org/www-project-top-10-for-large-language-model-applications
25 *Navigate threats to AI systems through real-world insights* https://atlas.mitre.org/
26 *ML10:2023 Model Poisoning - OWASP Foundation.* https://owasp.org/www-project-machine-learning-security-top-10/docs/ML10_2023-Model_Poisoning
27 *Build a Zero Trust Framework for Secure AI Implementation.* https://www.microsoft.com/en-us/microsoft-365/business-insights-ideas/resources/build-a-secure-zero-trust-secure-foundation-for-ai
28 *How is AI Strengthening Zero Trust? | CSA.* https://cloudsecurityalliance.org/blog/2025/02/27/how-is-ai-strengthening-zero-trust
29 *Take Back Control and Trust Your Enterprise AI with ZeroTrusted.ai's AI Firewall / AI Gateway / AI Health Check* ZeroTrusted.ai. https://www.zerotrusted.ai/
30 *Hogyan segít kezelni az AI az ellátási láncban jelentkező kockázatokat ....* https://logisztika.hu/2024/10/14/hogyan-segit-kezelni-az-ai-az-ellatasi-lancban-jelentkezo-kockazatokat/


ÓBUDAI EGYETEM
BÁNKI DONÁT GÉPÉSZ ÉS BIZTONSÁGTECHNIKAI MÉRNÖKI KAR
Köszönöm megtisztelő figyelmüket!
Óbudai Egyetem
Biztonságtudományi Doktori Iskola

Takács Péter: Narratívaháborúk és percepciós műveletek: a háború politikai természetének újrastrukturálódása az információs térben

Wars of the 21st century are increasingly fought not on physical battlefields, but within the information sphere, where the control of perception and narrative becomes the core objective of conflict. Perception operations, disinformation campaigns and digital narrative warfare fundamentally challenge the Clausewitzian concept of war as an extension of political will through force. Within a fragmented information ecosystem, societies experience divergent “realities” of the same conflict, raising new philosophical questions surrounding sovereignty, responsibility and the construction of the enemy. This presentation explores how reality itself has become the battlespace of modern warfare, and how political decision-making transforms when the ultimate objective is no longer territorial dominance, but the control of meaning.

A 21. század háborúi egyre kevésbé a fizikai csatatéren, sokkal inkább az információs térben zajlanak, ahol a valóságérzékelés és a narratívák uralása válik a hadviselés központi céljává. A percepciós műveletek, dezinformációs kampányok és digitális narratívaháborúk alapjaiban kérdőjelezik meg a Clausewitz-i háborúfogalmat, amely a politikai akarat fegyveres megnyilvánulására épül. A fragmentált információs ökoszisztéma következtében a társadalmak eltérő „valóságokat” élnek meg ugyanazon konfliktusokban, ami új

filozófiai kihívásokat vet fel a szuverenitás, a felelősség és az ellenségkép kategóriáiban. Az előadás bemutatja, hogyan válik a valóság a 21. század haditerévé, és miként alakul át a politikai döntéshozatal, amikor a háború célja már nem terület vagy erőforrás, hanem a jelentés uralása.

Az információs és narratív háborúk paradigmaváltása a 21. században: A háború fogalma a történelem során folyamatosan adaptálódott a technológiai innovációkhoz, politikai rendszerekhez és társadalmi struktúrákhoz. Klasszikus hadtudományi koncepciók, különösen Carl von Clausewitz 19. századi elmélete, a háborút a politika folytatásaként definiálják, amelyben a fegyveres erő alkalmazása az állami akarat érvényesítésének eszköze. A 20. század nagy konfliktusai – az első és második világháború, valamint a hidegháborús szuperhatalmi rivalizálás – megerősítették ezt a modellt: a katonai műveletek, a területellenőrzés és az anyagi erőforrások feletti dominancia volt a háború hagyományos célja, miközben a politikai és stratégiai döntések ezekhez az erőforrásokhoz igazodtak.

A 21. század azonban radikálisan átalakította a háború paradigmáját. A digitalizáció, a globális kommunikációs hálózatok és az információs technológia forradalmi változásokat idéztek elő a hadviselésben. A konfliktusok színtere immár kiterjed az információs és kognitív térre, ahol a cél a valóságérzékelés, a narratívák és a közösségi percepciók uralása. A percepciós műveletek, a dezinformációs kampányok és a digitális

narratívaháborúk előtérbe kerültek, míg a fizikai erő alkalmazása relatív háttérbe szorult.

A modern információs hadviselés gyökerei a hidegháború propagandatechnikáiban és a médiatér manipulációjában keresendők. Politikai-filozófiai szempontból ezek a jelenségek új dilemmákat vetnek fel: a szuverenitás, a felelősség, az ellenségkép és a jogszerűség klasszikus értelmezései alapjaiban kérdődnek meg. Ha a csata a tudatban és a digitális térben zajlik, az államok és nem állami szereplők legitimációjuk fenntartása és stratégiai céljaik elérése érdekében kénytelenek új, normatív és operatív kereteket kialakítani.

A modern hadviselés paradigmaváltása az erőforrások újra definiálását jelenti. A katonai potenciál mércéje nem csupán a csapatok, fegyverrendszerek és infrastruktúra rendelkezésre állásában, hanem az információs kapacitás, a digitális infrastruktúra és a narratívák kezelési képességében is mérhető. A siker a valóság narratív kontrolljában és a politikai percepciók alakításában nyilvánul meg. A digitális csatatér minden adategysége, története és kommunikációs eleme stratégiai jelentőséggel bír, a konfliktus kimenetele pedig egyre inkább ezen a percepciós színtéren dől el.

A fragmentált információs ökoszisztéma új filozófiai és etikai kihívásokat teremt. A valóság relativizálódása, a filterbuborékok és az „echo-kamrák” következtében a társadalmak eltérő narratívákat tapasztalnak, ami alapjaiban kérdőjelezi meg a politikai szuverenitás, a felelősség és a háborús jog gyakorlati értelmét. A

modern konfliktusok során a hatalom mércéje már nem a fizikai térben, hanem a társadalmi percepciókban és narratívákban mérhető. A jogi és etikai keretek újra értelmezésé nélkül a percepciós műveletek alkalmazása stratégiai, politikai és morális kockázatot hordoz.

A 21. század háborúi: a valóság, mint haditerület: A 21. század háborúi alapvetően átalakították a konfliktus fogalmát. Míg a 20. század háborúi döntően a fizikai csatatereken, terület- és erőforrás-ellenőrzésre épültek, a modern konfliktusok csatatere az információs térbe költözött. A háború célja ma már nem pusztán a fizikai uralom megszerzése, hanem a valóságérzékelés és a narratívák kontrollálása. Ebben az új paradigmában a percepciós műveletek, a dezinformációs kampányok és a digitális narratívaháborúk dominálnak, míg a hagyományos katonai eszközök háttérbe szorulnak. A 21. századi háború alapvetően az információs és narratív térben zajlik, ahol a percepciós műveletek, dezinformációs kampányok és digitális narratívák új definíciót adnak a hadviselésnek és a politikai hatalomnak. A modern konfliktusok célja a valóság kontrollja, amely radikálisan átalakítja a politikai döntéshozatal, a hadtudományi stratégiák és az etikai normák hagyományos logikáját. A győzelem mércéje immár nem a csatatéren, hanem a társadalmi narratívákban és a kollektív percepciók alakításában dől el.

Konvencionális vs. információs háború: A klasszikus hadtudomány, különösen Carl von Clausewitz „A háborúról” című munkája, a háborút a politika folytatásaként, a fegyveres erő alkalmazására építette. Clausewitz szerint a háború instrumentális: a politikai akarat fegyveres kifejeződése. A 21. század digitális és narratív háborúi azonban alapjaiban kérdőjelezik meg ezt a modellt. Ha a csata a tudatban és a digitális térben zajlik, a hagyományos fizikai győzelem mércéje már nem releváns. A modern háború célja a jelentés, a narratíva és a társadalmi percepciók uralása, ahol a győzelem mércéje a valóság narratív kontrollja.

Narratívaháborúk és percepciós műveletek: A percepciós műveletek és narratívaháborúk eszköztára rendkívül széles: célzott közösségi média-kampányok, algoritmusok által vezérelt információáramlás, deepfake-ek, manipulált videók és audioanyagok. Ezek az eszközök lehetővé teszik, hogy az államok és nem állami szereplők új valóságokat alakítsanak ki a társadalmakban, fragmentált módon hatva a különböző közösségekre. A filterbuborékok és echo-kamrák révén ugyanazon eseményekről eltérő „valóságok” jönnek létre, ami alapjaiban kérdőjelezi meg a szuverenitás, a felelősség és az ellenségkép fogalmát.

- Szuverenitás: Ki rendelkezik a valóság feletti kontrollal a globális információs térben?

- Felelősség: Ki vállalja a dezinformáció és a manipuláció következményeit, amikor az információ terjedése transznacionális?
- Ellenségkép: Hogyan definiálható az „ellenség” egy konfliktusban, ahol a percepciók és narratívák sokszor absztrakt, virtuális formában léteznek?
- Jus ad bellum: Ki jogosult a háború megindítására, ha a fegyveres erő alkalmazása helyett a digitális narratívák kontrollja válik stratégiai céllá?

A valóság, mint haditerület és arcvonal: A modern háború célja nem a fizikai dominancia, hanem a jelentés uralása. A politikai döntéshozatal a narratívák mentén formálódik, és a kormányzatoknak képesnek kell lenniük az információs tér folyamatos monitorozására, a manipulációk azonosítására és a társadalmi konszenzus fenntartására. A digitális csatatérben minden adat, minden történet és minden közösségi bejegyzés stratégiai fontosságú; a konfliktusok kimenetele gyakran ezen múlik.

A fragmentált információs ökoszisztéma új filozófiai és politikai dilemmákat hoz: hogyan értelmezhetjük a valóságot, ki vállalja a felelősséget a dezinformációért, és milyen etikai keretek között folytatható a percepciós hadviselés? A modern konfliktusok során a hatalom nem csak a fizikai térben, hanem a tudatokban, narratívákban és közösségi értelmezésekben is mérhető. A politikai-filozófiai diskurzusban így a szuverenitás, a felelősség és a jogszerűség kérdései új megvilágításba kerülnek.

Konklúzió

A 21. századi háború információs és narratív térben zajlik, ahol a percepciós műveletek és narratívák uralása alapvetően új definíciót ad a háborúnak és a politikai hatalomnak. A modern konfliktusok célja a valóság kontrollja, miközben a politikai döntéshozatal és a hadtudományi stratégiák radikálisan átalakulnak. A kérdés immár nem csupán a fizikai erő alkalmazása, hanem az, hogyan lehet ellenőrizni és legitimálni az információt a fragmentált digitális térben, valamint milyen etikai keretek szükségesek a percepciós műveletekhez. A győzelem ma már nem a csatatéren mérhető, hanem a társadalmi narratívákban, a politikai percepciókban és a kollektív valóság alakításában.

Narratívaháborúk és percepciós műveletek: a háború politikai természetének újrastrukturálódása az információs térben

TAKÁCS PÉTER
NEMZETI KÖZSZOLGÁLATI EGYETEM
HADTUDOMÁNYI DOKTORI ISKOLA 2. ÉVFOLYAM

Információs technológia

- A 21. század háborúi nem elsősorban fizikai csatatereken zajlanak.
- Az információs tér vált a modern hadviselés központi színterévé.


A 21. század háborújának jellemzői
A valóságérzékelés és narratívák uralása a cél.
Percepciós műveletek és dezinformációs kampányok dominálnak.
Fizikai erő alkalmazása háttérbe szorul
Konvencionális háború vs.
20. század
Információs háború
21. század


A Clausewitz-i háborúfogalom kihívása
Clausewitz: háború = politikai akarat fegyveres megnyilvánulása.
Digitális és narratív háborúk aláássák ezt a modellt.
Mi a háború célja, ha a csata a tudatban zajlik?"
klasszikus csatatér
vs.
digitális/hálózati „csatatér”

Fragmentált információs ökoszisztéma

- Egy konfliktusról eltérő „valóságok" alakulnak ki különböző társadalmakban.
- Szubjektív narratívák, filterbuborékok, echo-kamrák.

Filozófiai és politikai kihívások

- Szuverenitás: Ki irányítja a valóságot?
- Felelősség: Ki felel a dezinformációért?
- Ellenségkép: Hogyan definiáljuk az „ellenséget"?
- Jus ad bellum: Ki gyakorolja a jogos főhatalmat a 21. századi háborúkban?

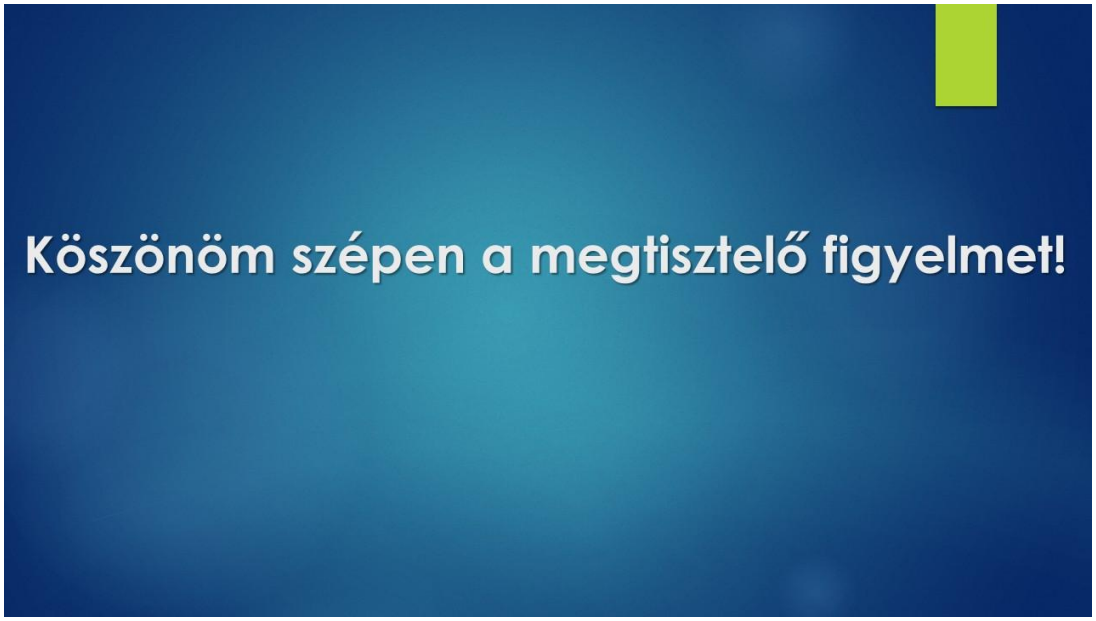
A valóság, mint haditerület

- A modern háború célja nem terület vagy erőforrás, hanem a jelentés uralása.
- Politikai döntéshozatal átalakul a narratívák mentén.
- digitális csatatér, ahol információ és narratívák ütköznek.

Konklúzió

- A 21. századi háború információs és narratív térben zajlik.
- A percepciós műveletek új definíciót adnak a háborúnak és politikai hatalomnak.
- Filozófiai és politikai kérdések: valóság, felelősség, ellenségkép.
- A valóság uralása lett a modern konfliktusok legfőbb célja.


Kérdések
Hogyan lehet ellenőrizni az információt a fragmentált térben?
Milyen etikai keretek kellenek a percepciós műveletekhez?


Köszönöm szépen a megtisztelő figyelmet!

Szulcsányi Viktor: Támadási felületek minimalizálása IT/OT környezetben

In recent years, the exposure of digital systems has increased at a pace that fundamentally reshaped how we think about IT and OT security. With most services, network components, and cloud-based resources now accessible in one way or another, attackers have more opportunities than ever to discover and exploit weak points. The growing interconnection between information technology and industrial environments has opened new operational possibilities, yet it has also introduced attack surfaces that significantly raise the likelihood of cyber incidents. Minimizing this exposure has therefore become a strategic priority, as it directly influences the security of critical infrastructure services and industrial processes.

The attack surface encompasses all network, software, configuration-related and other elements through which unauthorized access may occur. In IT environments, this surface changes constantly: new services, dynamic cloud scaling, APIs, and containerized systems all reshape it on a daily basis. OT environments behave differently. Their components often operate for decades, are difficult to update, lack built-in security controls, and rely on industrial protocols that typically provide neither encryption nor authentication. While IT security generally follows the principles of the CIA triad, OT places physical safety, operational continuity, and availability at the forefront. As IT/OT convergence

accelerates, weaknesses in one domain can have serious consequences in the other.

Recent incidents demonstrate that the attack surface is not an abstract construct but a practical factor with tangible, cross-sector implications when left unmanaged. The mass exploitation of the MOVEit Transfer vulnerability in 2023 illustrates how a widely used, internet-accessible solution handling sensitive data can become the starting point of a large-scale compromise. The 0-day SQL injection flaw was weaponized across government, financial, energy, and corporate sectors, affecting more than 2,500 organizations. Attackers relied on a single exposed component to conduct automated reconnaissance and extract sensitive information — a process made possible by the absence of proper attack surface management. Many affected organizations lacked up-to-date knowledge of where MOVEit was deployed, how it was exposed, or in what configuration it operated. The inability to recognise and monitor external exposure was a direct contributor to the resulting data breaches.

Similarly, investigations in the energy and utilities sectors have revealed tens of thousands of internet-connected OT devices worldwide — PLCs, HMIs, and industrial controllers — operating with inadequate protection, often using default passwords or factory settings. Modern reconnaissance tools, such as Shodan and Censys, map these devices automatically, meaning attackers often notice these exposures sooner than the organizations themselves. This is

particularly alarming in environments where cyber incidents may lead to physical consequences.

Identifying attack surfaces is therefore a critical task that requires different methods in IT and OT systems. In IT environments, a combination of automated and manual techniques — DNS and port discovery, cloud service analysis, API examination, shadow-IT identification, and vulnerability scanning — provides visibility. In OT environments, where active scanning might disrupt operations, passive traffic monitoring, ICS-specific asset discovery, audits of vendor and remote access pathways, and the analysis of network segmentation are safer and more appropriate approaches. Cyber threat intelligence plays a key role in both domains by helping determine which exposures are actively targeted in real-world campaigns and therefore require immediate action.

Reducing the attack surface, however, is a much broader effort. In IT environments, the most effective measures include eliminating unnecessary services, enforcing strong access control, applying Zero Trust principles, accelerating patch management, using micro-segmentation, and monitoring for leaked credentials. In OT systems, the foundation of security lies in restricting direct internet exposure, ensuring secure remote access, managing vendor connections, removing default settings, and maintaining strict IT/OT separation. Although the tools and processes differ, the objective is the same: creating an operational environment where the number of exploitable entry points is kept to a minimum.

Experience shows that managing attack surfaces is not a one-time project but a continuous operational capability. Attackers today can map an organization’s internet-facing presence in minutes using automated tools, which means defenders must operate with comparable speed and awareness. Effective attack surface management relies on real-time monitoring, accurate asset inventories, timely threat intelligence, and rapid decision-making. For modern networked and industrial systems, resilience depends on the ability to detect exposures earlier than the adversary and to respond quickly as the threat landscape evolves.

Overall, this study highlights that minimizing attack surfaces in IT/OT environments is essential for safeguarding critical infrastructure, industrial operations, and sensitive information. Success depends on visibility, proactivity, an understanding of the technological context, and the consistent application of lessons learned from real incidents. Such an approach not only reduces the number of exploitable weaknesses but also strengthens organizational resilience against the challenges of a rapidly changing cyber threat environment.

Az elmúlt években a digitális rendszerek kitettsége olyan ütemben növekedett, amely alapjaiban formálta át az IT- és OT-biztonságról alkotott képünket. Mivel ma már a legtöbb szolgáltatás, hálózati elem vagy felhőkomponens valamilyen módon elérhető, a támadók számára is sokkal könnyebb feltérképezni és kihasználni a gyenge pontokat. Az informatikai és ipari környezetek összekapcsolódása új

lehetőségeket teremt az üzemeltetésben és a folyamatok automatizálásában, ugyanakkor olyan támadási felületet hoz létre, amely korábban nem látott mértékben növeli a kibertámadások bekövetkezésének esélyét. A támadási felület minimalizálása ezért stratégiai jelentőségű feladattá vált, hiszen közvetlen hatással van a kritikus infrastruktúra szolgáltatások és ipari folyamatok biztonságára is.

A támadási felület fogalma magában foglal minden olyan hálózati, szoftveres, konfigurációs vagy egyéb tényezőt, amely lehetőséget adhat illetéktelen hozzáférésre. IT környezetben e felület folyamatosan változik: új szolgáltatások telepítése, felhőalapú erőforrások dinamikus skálázása, API-k és konténerizált rendszerek bevezetése mind folyamatosan hatással lehetnek rá. Ezzel szemben az OT rendszerekben a több évtizedes életciklusú eszközök, a frissítések kihívásai, a beépített biztonsági kontrollok hiánya és az ipari protokollok esetében tapasztalható titkosítás vagy hitelesítés hiánya miatt statikusabb, mégis sérülékenyebb támadási felület figyelhető meg. Miközben az IT környezetben a CIA triádon alapuló információbiztonsági szemlélet a követendő, az OT környezetben a fizikai biztonság, a folyamatok rendelkezésre állása és a működés folyamatossága az elsődleges. Az IT/OT konvergencia következtében azonban a két rendszer gyengeségei mindkét oldalon jelentős negatív következményekkel járhatnak.

A közelmúlt incidensei jól szemléltetik, hogy a támadási felület egy olyan gyakorlati tényező, amelynek hiányos kezelése súlyos,

határokon átívelő következményekkel járhat. A MOVEit Transfer sérülékenységének 2023-as kihasználása jó példája annak, amikor egy széles körben használt, érzékeny adatokat kezelő szoftver internetes elérhetősége és a hibás frissítési folyamatok együtt olyan támadási lehetőséget teremtenek, amelyet a támadók gyorsan és hatékonyan ki tudnak használni. A 0-day SQL injection sérülékenységet széles körben használták kormányzati, pénzügyi, energetikai és vállalati szektorok elleni támadásokban, amelyekben összesen több mint 2 500 szervezet volt érintett. A támadók egyetlen publikusan elérhető komponensre támaszkodva végeztek automatizált felderítést és jutottak hozzá a rendszereken tárolt érzékeny információhoz, amelyet többek között a hiányzó támadási felület menedzsment tett lehetővé. A kompromittálódott rendszerek között olyan szervezetek szerepeltek, amelyek nem rendelkeztek naprakész információval arról, hol fut a sérülékeny szoftver, miként érhető el, illetve milyen konfigurációval került telepítésre. A támadási felület felismerésének és kezelésének hiánya így közvetlenül vezetett nagyléptékű adatszivárgáshoz.

Hasonló tanulságokat hordoznak az energia- és közműszektorban felfedezett, internetre közvetlenül kapcsolt OT eszközökről szóló jelentések is. Ezek szerint világszerte több tízezer PLC, HMI és ipari vezérlő érhető el megfelelő védelem nélkül, sok esetben gyári jelszavakkal vagy alapértelmezett konfigurációkkal. A modern támadóeszközök – mint a Shodan vagy a Censys – automatizált módon térképezik fel ezeket az eszközöket, és a támadók gyakran

előbb ismerik fel a kitettségeket, mint maguk az üzemeltető szervezetek. Ez különösen aggasztó olyan környezetekben, ahol a kibertámadások fizikai következményekkel járhatnak.

A támadási felület azonosítása tehát kiemelten fontos feladat, amely mindkét technológiai területen eltérő módszereket igényel. IT-rendszerek esetében ez különféle automatizált és manuális technikákkal érhető el, mint például a DNS- és portfelderítés, felhőszolgáltatások vizsgálata, alkalmazások és API-k elemzése, shadow IT felderítése, valamint sérülékenységvizsgálat. OT környezetben az aktív szkennelés esetleges veszélyei miatt sokkal inkább passzív hálózatmegfigyelés, ICS-specifikus eszközfelderítés, beszállítói és távoli hozzáférések auditja, valamint a hálózati szegmentáció vizsgálata alkalmazható biztonságosan. Ebben a folyamatban kiemelt szerep jut a kiberfenyegetettségi információknak, amelyek segítenek meghatározni, mely kitettségek képezik ténylegesen a támadói kampányok célpontját, és melyek igényelnek azonnali intézkedést.

A támadási felület minimalizálása ugyanakkor ennél jóval összetettebb folyamat. IT környezetben elsősorban a felesleges szolgáltatások megszüntetése, a jogosultságkezelés, a Zero Trust elvek alkalmazása, a gyors patch menedzsment, a mikroszegmentáció és a kiszivárgott hitelesítési adatok monitorozása jelentik a fő védvonalat. OT rendszerek esetében a biztonságos távoli hozzáférés, a harmadik fél általi hozzáférések kontrollja, a gyártói alapbeállítások kezelése és a közvetlen

internetes kitettség teljes megszüntetése képezik a védelem alapjait. Bár az eszközök és módszerek eltérők, a közös cél olyan védelmi környezet kialakítása, ahol a támadók számára elérhető felületek száma minimálisra csökken.

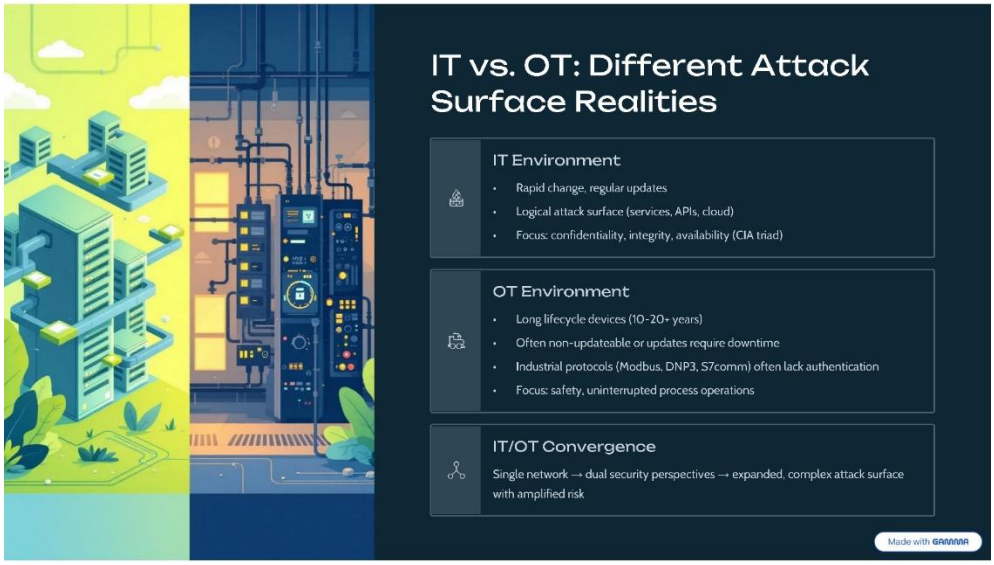
A tapasztalatok alapján kijelenthető, hogy a támadási felületek menedzsmentje nem egyszeri projekt, hanem folyamatosan fenntartandó képesség. Az ellenfelek ma már automatizált eszközökkel, percek alatt képesek feltérképezni egy szervezet internetes jelenlétét, így a védelem csak akkor lehet hatékony, ha proaktív megközelítésen, valós idejű felügyeleten és naprakész fenyegetési információkon alapul. A modern hálózati és ipari rendszerek rezilienciájának alapfeltétele, hogy a szervezetek hamarabb ismerjék fel saját kitettségeiket, mint a támadók, és képesek legyenek gyorsan reagálni a változó fenyegetésekre.

Összességében ez a tanulmány rámutat, hogy az IT/OT környezetek támadási felületének minimalizálása alapvető jelentőségű a kritikus infrastruktúrák, ipari folyamatok és érzékeny adatok védelmében. A siker kulcsa a felügyelet, a proaktivitás, a technológiai sajátosságok megértése és a valós incidensekből levont tanulságok következetes alkalmazása. Egy ilyen megközelítés nemcsak csökkenti a támadók által kihasználható sebezhetőségeket, hanem megerősíti a szervezet ellenállóképességét is, amely a jövő fenyegetéseivel szemben elengedhetetlen.


Minimizing Attack Surfaces in IT/OT Environments
Viktor Szulcsányi
Doctoral School on Safety and Security Sciences, Óbuda University
Made with GAMMA


Presentation Agenda
Introduction: Why This Matters
IT vs. OT Differences
Case Studies
Attack Surface Identification Methods
Mitigation Strategies
Conclusion
Made with GAMMA


Why This Matters in 2025
The Challenge
Digital transformation has dramatically expanded the attack surface across both IT and OT systems. In 2024, attacks targeting operational technology with physical consequences reached record levels across energy, water utilities, and manufacturing sectors.
Central question: "What can attackers see in our systems?"
Network Exposure
Open ports, reachable services, and public endpoints
Credential Access
Stored passwords, API keys, and token leaks
What can attackers see in our systems?
Data Visibility
Databases, files, and backups accessible or misconfigured
Configuration & Logs
Exposed configs, debug endpoints, and log information
Internet-Connected OT
Rapid spread of OT devices with direct internet access
Remote Access Standard
Remote connectivity becoming default operational model
Supply Chain Risks
Exponentially growing vulnerabilities in service chains
Made with GAMMA


IT vs. OT: Different Attack Surface Realities
IT Environment
Rapid change, regular updates
Logical attack surface (services, APIs, cloud)
Focus: confidentiality, integrity, availability (CIA triad)
OT Environment
Long lifecycle devices (10-20+ years)
Often non-updateable or updates require downtime
Industrial protocols (Modbus, DNP3, S7comm) often lack authentication
Focus: safety, uninterrupted process operations
IT/OT Convergence
Single network → dual security perspectives → expanded, complex attack surface with amplified risk
Made with GAMMA

Why Minimizing Attack Surface Is Critical

OT systems were never designed for internet connectivity. Each misconfiguration can halt entire operations.

→ **Common Weak Points**

Default passwords, outdated firmware, remote maintenance access, public admin interfaces

→ **Attacker Tools (2023-2024)**

Shodan, Censys, leaked credentials, open GitHub repositories, legacy VPNs without MFA

→ **Direct Impact**

Lack of attack surface management leads directly to operational disruptions with physical consequences

Case Study: Internet-Exposed OT Devices

The Discovery

Between 2023-2024, Microsoft, Dragos, and CISA issued alerts: tens of thousands of OT devices accessible directly from the internet across water utilities and energy sectors.

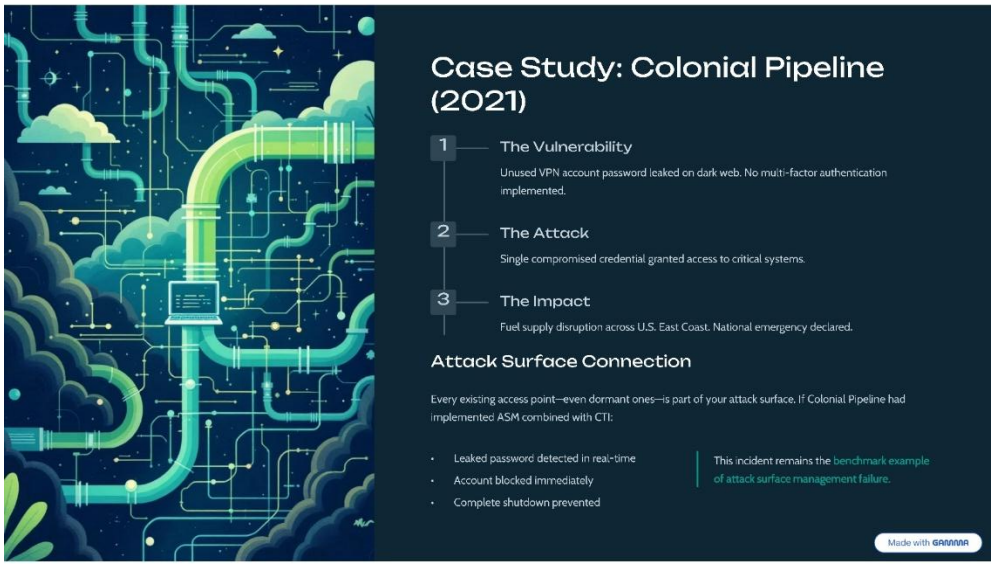
Critical Problems Identified

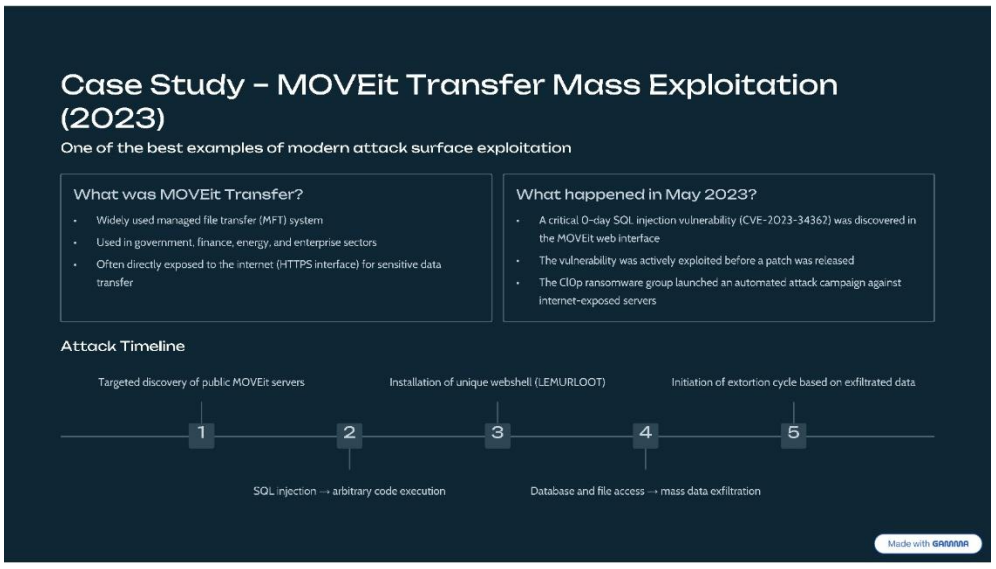
- Internet-connected PLCs without protection
- No firewall or VPN implementation
- Open remote access (RDP) ports
- Factory default passwords maintained

Key Lesson: Without active ASM, attackers have better visibility into your infrastructure than you do.

Data Manipulation | Operation Disruption | Physical Damage Potential

Made with GAMMA


Case Study: Colonial Pipeline (2021)
1
The Vulnerability
Unused VPN account password leaked on dark web. No multi-factor authentication implemented.
2
The Attack
Single compromised credential granted access to critical systems.
3
The Impact
Fuel supply disruption across U.S. East Coast. National emergency declared.
Attack Surface Connection
Every existing access point—even dormant ones—is part of your attack surface. If Colonial Pipeline had implemented ASM combined with CTI:
Leaked password detected in real-time
Account blocked immediately
Complete shutdown prevented
This incident remains the benchmark example of attack surface management failure.
Made with GAMMA


Case Study – MOVEit Transfer Mass Exploitation (2023)
One of the best examples of modern attack surface exploitation
What was MOVEit Transfer?
Widely used managed file transfer (MFT) system
Used in government, finance, energy, and enterprise sectors
Often directly exposed to the internet (HTTPS interface) for sensitive data transfer
What happened in May 2023?
A critical 0-day SQL injection vulnerability (CVE-2023-34362) was discovered in the MOVEit web interface
The vulnerability was actively exploited before a patch was released
The ClOp ransomware group launched an automated attack campaign against internet-exposed servers
Attack Timeline
Targeted discovery of public MOVEit servers
1
SQL injection → arbitrary code execution
2
Installation of unique webshell (LEMURLOOT)
3
Database and file access → mass data exfiltration
4
Initiation of extortion cycle based on exfiltrated data
5
Made with GAMMA

Case Study – MOVEit Transfer Mass Exploitation (2023)

Affected Organizations and Consequences

- Over 2,500 organizations affected worldwide
- Tens of millions of personal data records compromised
- Affected sectors: government, banking, financial services, airlines, energy, healthcare and educational institutions
- Examples: BBC, British Airways, Shell, US government agencies

Why is this important from an attack surface perspective?

Attackers exclusively exploited publicly accessible services

Many organizations didn't know if they were using MOVEit or how it was accessible

Key success factors: public, discoverable services; automatable 0-day exploit; missing ASM visibility; slow detection and response

The MOVEit incident clearly demonstrated that a single internet-exposed service is sufficient to cause a global-scale data breach affecting thousands of organizations within days. Attackers discover exposure before organizations realize it exists.

Made with GAMMA

Identifying IT Attack Surface with ASM Tools

DNS & Port Discovery

Subdomain enumeration and open port identification across all domains

Cloud Resources

Public cloud asset analysis (S3, Azure Blob, storage buckets)

Shadow IT Discovery

Unauthorized devices, services and applications identification

Vulnerability Scanning

Version analysis, configuration review (Nessus, OpenVAS, Qualys)

API Exposure

Public and private API endpoint security assessment

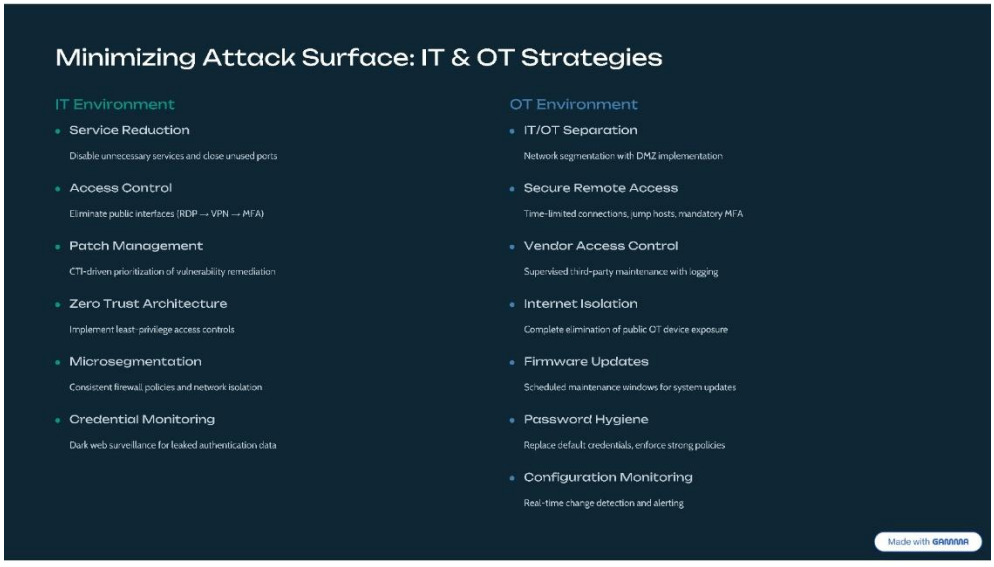
Third-Party Services

Outsourced provider security posture evaluation

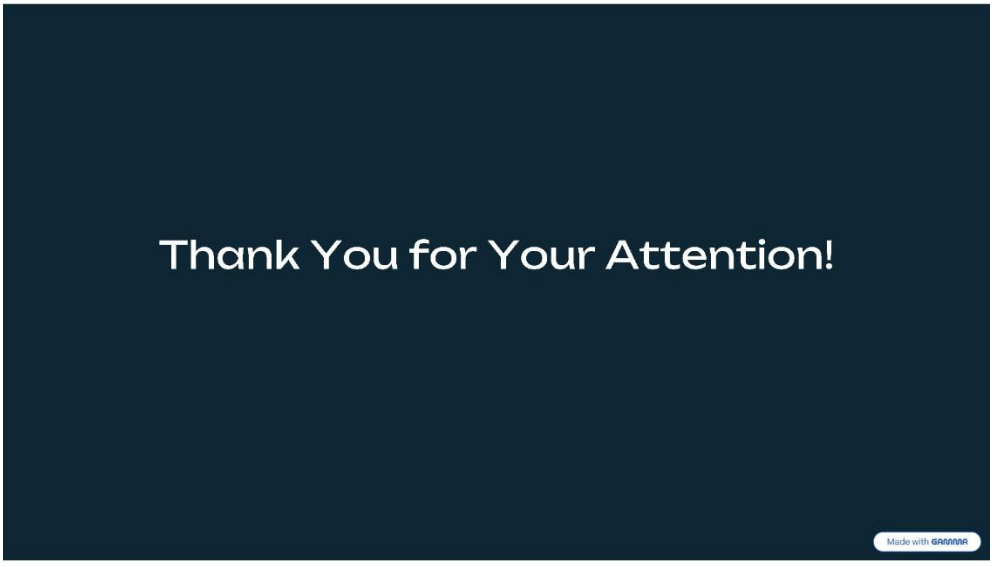
Common Tools: Shodan, Censys, SecurityTrails, Nmap | **ASM Platforms:** Randori, Palo Alto Cortex Xpanse, Microsoft Defender EASM

Made with GAMMA


Identifying OT Attack Surface
Critical Difference: Active port scanning on OT devices can be prohibited or dangerous. Passive methods are essential.
01
Passive Network Observation
SPAN/TAP implementations for non-intrusive monitoring
02
ICS-Specific Asset Discovery
Specialized tools can help in automating asset discovery in a non-intrusive way
03
Remote Access Inventory
Complete cataloging of all remote connectivity points
04
Vendor Relationship Audit
Third-party maintenance access review and control
05
Legacy Access Points
Old network devices and legacy IP gateways identification
06
Network Segmentation Mapping
OT network zone documentation and boundary verification
Made with GAMMA


Minimizing Attack Surface: IT & OT Strategies
IT Environment
Service Reduction
Disable unnecessary services and close unused ports
Access Control
Eliminate public interfaces (RDP → VPN → MFA)
Patch Management
CTI-driven prioritization of vulnerability remediation
Zero Trust Architecture
Implement least-privilege access controls
Microsegmentation
Consistent firewall policies and network isolation
Credential Monitoring
Dark web surveillance for leaked authentication data
OT Environment
IT/OT Separation
Network segmentation with DMZ implementation
Secure Remote Access
Time-limited connections, jump hosts, mandatory MFA
Vendor Access Control
Supervised third-party maintenance with logging
Internet Isolation
Complete elimination of public OT device exposure
Firmware Updates
Scheduled maintenance windows for system updates
Password Hygiene
Replace default credentials, enforce strong policies
Configuration Monitoring
Real-time change detection and alerting
Made with GAMMA


Conclusion - Strengthening Our Digital Defenses
Holistic Attack Surface Management
Effective security requires a comprehensive approach to identifying and mitigating vulnerabilities across both IT and OT domains. Continuously monitor and reduce potential entry points for attackers.
Tailored IT vs. OT Strategies
Recognize the fundamental differences between IT and OT environments. Implement distinct, yet integrated, security measures that respect operational criticality and unique technical challenges.
Lessons from Real-World Incidents
Case studies highlight the devastating impact of successful attacks. Learning from these incidents is crucial for refining defense strategies and preventing similar breaches.
Proactive & Continuous Security
A reactive stance is no longer sufficient. Prioritize proactive measures, continuous monitoring, and regular updates to stay ahead of evolving threats and ensure resilience.
Minimizing attack surfaces is not a one-time task but an ongoing commitment to safeguarding critical infrastructure and sensitive data in an increasingly connected world.
Made with GAMMA


Thank You for Your Attention!
Made with GAMMA

Busa Attila József: Kritikus infrastruktúrák a digitális tűzvonalban

A technológiai fejlődés és a digitalizáció térnyerése elkerülhetetlenül érinti a kritikus infrastruktúrákat is. A tanulmány célja bemutatni az informatikai (IT) és az üzemeltetési technológia (OT) konvergenciájából fakadó biztonsági kockázatokat. Különös figyelmet fordít az ipari vezérlőrendszerek (ICS) sérülékenységeire, valamint az ukrán energiahálózatot érintő Industroyer kártevőcsalád működését. A cikk rámutat a hálózati szegmentálás és a megfelelő védelmi stratégiák fontosságára a jövőbeli támadások kivédése érdekében.

1. Bevezetés

A technológiai fejlődés és a digitalizáció gyorsuló üteme miatt a kritikus infrastruktúrák – mint például az energiaellátás vagy a közlekedés – mára elválaszthatatlanul integrálódtak a kormányzati digitális infrastruktúrába. Ez a konvergencia új biztonsági kockázatokat teremt, hiszen a fizikai folyamatokat irányító rendszerek immár a kibertámadások elsődleges célpontjaivá váltak. A hatékony védekezés alapfeltétele ezért az aktuális fenyegetések és támadási trendek naprakész ismerete.

2. A tisztán informatikai és az ipari informatikai rendszerek (IT/OT) konvergenciája

A biztonság fogalma eltérő hangsúlyokat kap az IT és az OT területeken. Az információbiztonság (InfoSec/ITSec) elsődleges célja a CIA-elv (Confidentiality, Integrity, Availability), azaz a bizalmasság, sértetlenség és rendelkezésre állás biztosítása. Ezzel szemben az ipari rendszerek biztonsága (OTSec) esetében a legfőbb kritérium az állandó rendelkezésre állás és az üzembiztonság (safety).

A korábbi éles határvonal az IT és OT rendszerek között mára megszűnőben van. Az egyre gyakoribb összekapcsolódás lehetővé teszi, hogy egy IT rendszert érő kompromittálás után a támadó az OT hálózatba is behatolhasson, ami fizikai következményekkel is járhat.

3. Kritikus infrastruktúrák és sérülékenységeik

Kritikus infrastruktúrának tekintjük azokat a létfontosságú rendszereket, amelyek elengedhetetlenek a társadalmi vagy gazdasági folyamatok fenntartásához. Ide soroljuk többek között az energiaellátást, az ivóvízellátást, az élelmiszeripart, a pénzügyi szektort, az egészségügyet, a honvédelmet és a közlekedést is. Ezeket a szektorokat ipari vezérlőrendszerek irányítják.

Az OT területek sérülékenysége több tényezőre vezethető vissza:

Elavult rendszerek: Számos OT-rendszer évtizedekig működik frissítés nélkül, gyakran támogatás nélküli operációs rendszereket (pl. Windows XP, Windows 7) futtatva.

Protokollok hiányosságai: Az ipari hálózati protokollok (pl. Modbus, SCADA) gyakran titkosítás és autentikáció nélkül működnek, így az adatforgalom lehallgatható vagy manipulálható.
Emberi tényező: A gyenge vagy alapértelmezett jelszavak használata továbbra is jelentős kockázatot jelent.
Magas kockázat: Az esetleges leállások kritikus következményekkel járhatnak, ami megnehezíti a karbantartást és frissítést.

4. Esettanulmány: Az Industroyer kártevőcsalád

Az ipari környezetek elleni támadások egyik legjelentősebb példája az Industroyer, amelynek első verziója 2016-ban az ukrán energiahálózatot célozta meg.

4.1. Az Industroyer működési mechanizmusa (2016, Ukrajna)

A kártevő képes közvetlenül irányítani az elektromos alállomások kapcsolóit és megszakítóit, amelyek az analóg kapcsolók digitális megfelelői. Ez a képesség az áramelosztás lekapcsolásától a berendezések fizikai károsodásáig terjedő hatásokat válthat ki.

I. A célpont és az időzítés A támadás 2016-ban történt, és az ukrán energiahálózat volt a célpont. Ez volt az egyik legelső olyan széles körben ismert eset, amelyet kifejezetten ipari vezérlőrendszerek (ICS) elleni szabotázsra terveztek.

II. A támadás menete (IT-ből az OT-be)
A kártevő egy hátsó kaput (backdoor) telepített, és egy helyi proxy segítségével hitelesítette magát a belső hálózaton.

A kommunikációhoz HTTP-csatornát nyitott a külső vezérlő (C2) szerver felé, majd a belső proxyn keresztül tartotta a kapcsolatot, elrejtve a tevékenységét.
A perzisztencia (állandó jelenlét) érdekében a kártevő egy futó szolgáltatáshoz (service) kapcsolódott, amely előre meghatározott időközönként újranyitotta a kapcsolatot a támadók szervere felé, így az újraindítások után is működőképes maradt.

III. A fizikai hatás (A "lekapcsolás")
Miután a támadók elérték az OT szintet, a kártevő képes volt közvetlenül átvenni az irányítást a fizikai eszközök felett.
Az Industroyer képes volt közvetlenül vezérelni az elektromos alállomások kapcsolóit és megszakítóit (amelyek az analóg kapcsolók digitális megfelelői).
Ennek következménye az áramelosztás egyszerű kikapcsolásától kezdve a berendezések súlyos károsodásáig terjedhetett.
A támadás végül tényleges áramkimaradást okozott, bizonyítva, hogy a digitális behatolás képes fizikai infrastruktúrát megbénítani.

Miképpen lehetséges ez?
A fő kockázati tényező az IT és OT konvergenciája:
A két terület közötti szétválasztás megszűnt, az összekapcsolódás egyre gyakoribb.
Sok OT rendszer elavult, frissítés nélküli operációs rendszereket futtat (pl. Windows XP, 7), amelyek sérülékenyek az IT felől érkező támadásokkal szemben.

Az ipari protokollok gyakran titkosítás és hitelesítés nélkül működnek, így a hálózatra bejutó támadó könnyen manipulálhatja az adatforgalmat.

4.2. Industroyer 2 és a Sandworm csoport

2022-ben a támadók a kártevő új verzióját, az Industroyer 2-t vetették be, ismét egy ukrán energetikai vállalat ellen. A támadást 2022. április 8-ra időzítették, de az előkészületek már hetekkel korábban megkezdődtek. Az újdonság az volt, hogy az ICS-specifikus kódok mellett Windows, Linux és Solaris rendszerekre írt adattörlőket (wiper) is alkalmaztak. A Sandworm csoport több pusztító kártevőt, köztük a CaddyWiper-t is felhasználta a művelet során.

5. Jövőkép és védekezési stratégiák

A jövőben a kritikus infrastruktúrákat célzó kibertámadások számának növekedése várható, különös tekintettel a törlőautomatizmussal kiegészített Industroyer-jellegű fenyegetésekre.

A védekezés hatékonysága növelhető az alábbi intézkedésekkel:

Hálózati szegmentálás: Az IT és OT hálózatok szigorú elkülönítése minimalizálja a támadások terjedését.

Biztonsági mentés és visszaállítás: Rendszeres mentések és kidolgozott visszaállítási tervek szükségesek a működési szünetek minimalizálására.

Elemzés és AI: A nyilvánosságra került támadókódok elemzése alapján kell frissíteni a védelmi szabályokat. Hosszú távon a mesterséges intelligencia is segítséget nyújthat a támadások időben történő megállításában.

6. Összefoglalás

Az előrejelzések szerint a kritikus infrastruktúrákat célzó támadások száma a jövőben tovább fog növekedni, és számítani kell az automatizált, pusztító hatású kódok szélesebb körű megjelenésére. A védekezés érdekében elengedhetetlen a hálózati szegmentálás alkalmazása, amely elszigeteli az IT és OT rendszereket, megakadályozva a támadások átterjedését. Emellett kulcsfontosságú a rendszeres biztonsági mentések készítése és a visszaállítási tervek (DRP) kidolgozása a működési szünetek minimalizálására. A jövőbeli védekezésben a nyilvánosságra került támadókódok folyamatos elemzése, valamint a mesterséges intelligencia által támogatott, valós idejű észlelés játszhat döntő szerepet.

Az ipari rendszerek biztonsága nem csupán technológiai kérdés, hanem a nemzetbiztonság és a gazdasági stabilitás alapköve. Mivel az IT és OT rendszerek konvergenciája visszafordíthatatlan, a szervezeteknek proaktív védelmi stratégiákat kell alkalmazniuk, figyelembe véve a legújabb kiberfenyegetéseket és a technológiai fejlődés irányait.

Infokommunikáció 2025

KRITIKUS INFRASTRUKTÚRÁK A DIGITÁLIS HARCMEZŐN

Busa Attila József
MH KIMK, Képzési Osztály
osztályvezető
BRU Infosec Kft.
ügyvezető
Óbudai Egyetem, Biztonságtudományi Doktori Iskola,
3. éves doktorandusz hallgató

VÁZLAT

- InfoSec vs. ITSec vs. OTSec
- Mik lehetnek kritikus infrastruktúrák?
- Miért sérülékenyebbek az OT területek?
- Van-e megoldás?
- Mit hoz a jövő?

INFOSEC VS. ITSEC VS. OTSEC

Information Security

„Információ Biztonság”

Magának az információnak (digitális vagy kézzel fogható) a védelme.

Bizalmasság (**C**onfidentiality), sértetlenség (**I**ntegrity), rendelkezésre állás (**A**vailablity) elve.

Information Technology Security	**Operational Technology Security**
„Informatikai Rendszerek Biztonsága”	„Ipari vezérlőrendszerek Biztonsága”
security	safety
Igyekeznek a CIA mindhárom alapelvét betartani.	Alapvetően az állandó rendelkezésre állás a fő kritérium ezeknél a rendszereknél.

MIK LEHETNEK KRITIKUS INFRASTRUKTÚRÁK?

Kritikus Infrastruktúra

LÉTFONTOSSÁGÚ RENDSZER, AMELY ELENGEDHETETLEN A LÉTFONTOSSÁGÚ TÁRSADALMI VAGY GAZDASÁGI FOLYAMATOKHOZ.

Energia

Ivóvízellátás

Banki szolgáltatások

Élelmiszeripar és mezőgazdaság

Közbiztonság védelem

Digitális infrastruktúra

Közlekedés

Pénzügyi Piaci Infrastruktúrák

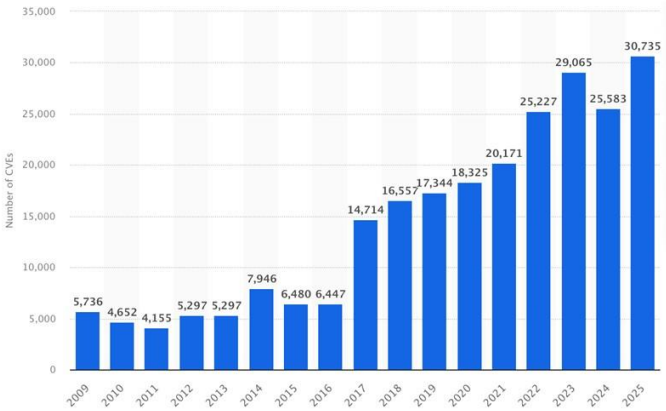
Egészségügyi ellátó létesítmények

Ezeket vezérlik az ipari vezérlőrendszerek!

MIÉRT SÉRÜLÉKENYEBBEK AZ OT TERÜLETEK?

- Sok OT-rendszer évtizedekig működik frissítés nélkül, így gyakran futnak rajtuk támogatás nélküli régi operációs rendszerek (pl. Windows XP, Windows 7).
- A szétválasztás az IT és OT rendszerek között megszűnt, egyre gyakoribb az összekapcsolódás, ami lehetővé teszi, hogy az IT rendszer kompromittálása után a támadó az OT hálózatra is beléphessen. (Hogyan kapcsolódhat ide az IoT Sec?)
- Az ipari hálózati protokollok (pl. Modbus, ION, DCS, SCADA) gyakran autentikáció és titkosítás nélkül működnek, így lehallgatható vagy manipulálható az adatforgalom.
- Az esetleges leállások magas kockázatot jelentenek.
- Gyenge, vagy alapértelmezett jelszavak használata, elavult belépési protokollok alkalmazása szintén kockázatot jelent az ipari környezetek számára.
- Helytelen felsővezetői gondolkodás?

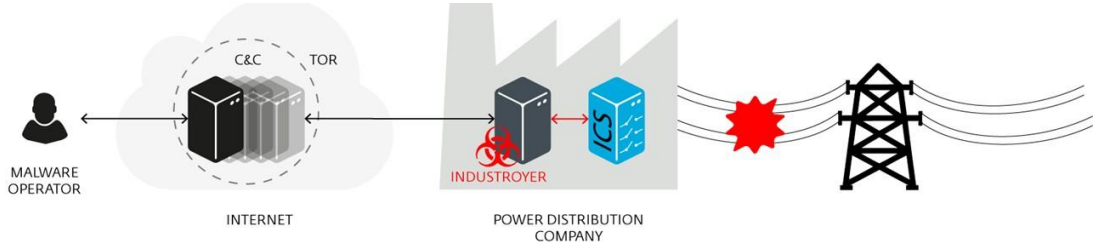
AZ ELMÚLT NÉHÁNY ÉV „FELFEDEZETT” SÉRÜLÉKENYSÉGEINEK STATISZTIKÁJA.



INDUSTROYER

- Célpont: 2016, ukrán energiahálózat

Képes közvetlenül irányítani az elektromos alállomások kapcsolóit és megszakítóit. Ezek a kapcsolók és megszakítók az analóg kapcsolók digitális megfelelői. Így a potenciális hatás az áramelosztás egyszerű kikapcsolásától kezdve a tényleges meghibásodásokon át a berendezések súlyosabb károsodásáig terjedhet.



INDUSTROYER TECHNIKAI HÁTTERE

- Helyi proxyval hitelesíti magát a belső hálózaton keresztül a backdoor telepítése előtt.
- A hitelesítés után HTTP-csatornát nyit a külső a C2 szerver felé. A későbbi kommunikáció ezt követően a belső proxyn zajlik.
- Létrehoz egy fertőzött fájlt a helyi rendszeren (melyen keresztül életben tartja a kapcsolatot), amely egy futó szerviz szolgáltatáshoz kapcsolódik.
- A megfertőzött szolgáltatás folyamatosan nyitva tartja a backdoor-t, úgy, hogy előre meghatározott időközönként újranyitja a kapcsolatot a támadó szerver felé, így a rosszindulatú program továbbra is fut az újraindítások után is.

JAVASOLT VÉDELMI INTÉZKEDÉSEK

- **Hálózati szegmentálás:** Az ipari irányító rendszerek és hálózatok szegmentálása, vagyis elkülönítése, segíthet minimalizálni a támadó terjedését, ha az egyik területet érinti.
- **Biztonsági mentés és visszaállítási terv:** Rendszeres biztonsági mentéseket kell készíteni a kritikus rendszerekről, és visszaállítási terveket kell kidolgozni. Ez lehetővé teszi a gyors helyreállítást és a működési szünet minimalizálását, ha egy támadás vagy károsítás történik.

INDUSTROYER 2

Célpont: az ukrán energetikai vállalat.

Támadás időpontja: A beavatkozást 2022.04.08-ra tervezték, de a jelek arra utalnak, hogy a támadást legalább két héttel előtte előkészítették.

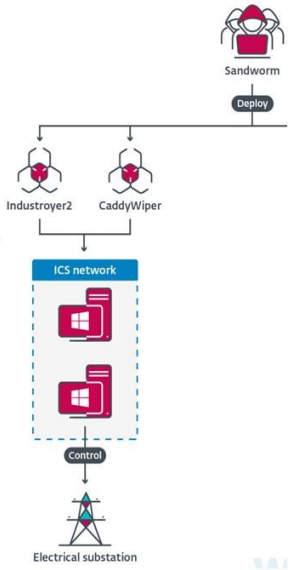
A támadásban ICS-képes rosszindulatú szoftvereket és Windows, Linux és Solaris operációs rendszerekhez alkalmazható lemeztörlőket használtak. Nagy valószínűséggel a támadók az Industroyer rosszindulatú szoftver új verzióját használták, amelyet 2016-ban az ukrajnai áramkimaradáshoz használtak.

INDUSTROYER 2

Az Industroyer2 mellett a Sandworm több pusztító kártevő családot is használt, köztük a CaddyWiper-t.

A CaddyWiper-t először 2022.03.14-én fedezték fel, amikor egy ukrán bank ellen használták.

A CaddyWiper egy változatát 2022.04.08 ismét felhasználták a korábban említett ukrán energiaszolgáltató ellen.



MIT HOZ A JÖVŐ?

- A jövőben várható, hogy a kritikus infrastruktúrákat célzó kibertámadások elszaporodnak. A törlőautomatizmussal kiegészített új Industroyer jellegű támadásokra nagy eséllyel számíthatunk a jövőben is.
- A védekezés módja (az eddig említetteken felül) talán az lehet, hogy a nyilvánosságra került támadókódokat át kell elemezni és hozzájuk kell igazítani a védelmi rendszerek biztonsági szabályait.
- Idővel nagy eséllyel a mesterséges intelligencia is sikeresen besegíthet majd az ilyen típusú támadások időben történő megállításához.

ÖSSZEFOGLALÁS

A technológiai fejlődés és a digitalizáció folyamatosan növekszik. Az ipari irányító rendszerek, az energiaellátás, a víz- és hulladékkezelés, a közlekedés és más kritikus infrastruktúrák szorosan kapcsolódnak a digitális technológiákhoz. Ezért nagyon fontos, hogy a védelem oldaláról is tisztában legyünk az aktuális támadási trendekkel a sikeres védekezésre való felkészülés érdekében.

FORRÁSOK

- CyberArk Blog Team: The Anatomy of the SolarWinds Attack Chain https://www.cyberark.com/resources/blog/the-anatomy-of-the-solarwinds-attack-chain (letöltve: 2025.10.23.)
- Industroyer: Biggest threat to industrial control systems since Stuxnet https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/ (letöltve: 2025.10.23.)
- MalPedia for win.industroyer https://malpedia.caad.fkie.fraunhofer.de/details/win.industroyer (letöltve: 2025.10.23.)
- How Kaspersky Industrial CyberSecurity deals with an APT based on Industroyer malware https://www.kaspersky.com/enterprise-security/mitre/industroyer (letöltve: 2025.10.23.)
- WIN32/INDUSTROYER A new threat for industrial control systems https://web-assets.esetstatic.com/wls/2017/06/Win32_Industroyer.pdf (letöltve: 2025.10.23.)
- CRASHOVERRIDE Analysis of the Threat to Electric Grid Operations https://www.dragos.com/wp-content/uploads/CrashOverride-01.pdf (letöltve: 2025.10.23.)
- ENISA Threat Landscape 2023 https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023 (letöltve: 2025.10.23.)
- Threat Landscape for Supply Chain Attacks https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks (letöltve: 2025.10.23.)
- Kiberbűnözők célpontja lett az energiaszektor https://greendex.hu/kiberbunozok-celpontja-lett-az-energiaszektor/ (letöltve: 2025.10.23.)
- Kibertámadás is okozhatta a pakisztáni áramszünetet https://nki.gov.hu/it-biztonsag/hirek/kibertamadas-is-okozhatta-a-pakisztani-aramszunetet/ (letöltve: 2025.10.23.)
- WeLiveSecurity by ESET: Industroyer2 Industroyer reloaded https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/ (letöltve: 2025.10.23.)

Köszönöm a figyelmet!

Imhof László: Orosz-Ukrán konfliktusban megvalósított CIS támogatás és konklúziói

The Russian-Ukrainian conflict has become one of the most striking examples of the further development of the digitalization of warfare in the 21st century, where kinetic operations are closely linked to the activities taking place in cyberspace, information space and the everyday activities of the armed forces practicing network-based warfare. The presentation will demonstrate how and with what technical means the CIS technology used in the conflict is being transformed – including radio and satellite systems, drone-control military telecommunications ecosystems, big data analysis, AI-based decision support and digital communication infrastructure – and operational and strategic thinking is being reshaped in this light. It analyzes new technologies emerging in conflict, such as the military adaptation of commercial technologies, the intertwining of civilian and military information systems, and communication platforms used in psychological and disinformation operations based on a rapidly changing information environment. The results show that the digitalization of war means not only the introduction of new tools, but also a transformation of the basic logic of warfare, where the acquisition of digital superiority has become a strategic factor on par with physical resources.

Az orosz–ukrán konfliktus a 21. századi hadviselés digitalizációjának továbbfejlesztési irányainak kijelöléséhez az egyik legmarkánsabb

példájává vált, ahol a kinetikus műveletek szorosan összekapcsolódnak a kibertérben, az információs térben és a hálózat alapú hadviselést gyakorló haderők mindennapjaiban zajló tevékenységekkel. Az előadás bemutatja, hogyan és milyen technikai eszközök használatával formálódik át a konfliktusban használt híradó-informatikai technológia – többek között a rádió-, a műholdas rendszerek, a drónvezérlő katonai távközlési ökoszisztémák, a big data elemzés, az AI-alapú döntéstámogatás és a digitális kommunikációs infrastruktúra –, illetve ennek tükrében rajzolódik át a hadműveleti és stratégiai gondolkodás. Elemzi a konfliktusban megjelenő új technológiákat, így a kereskedelmi technológiák katonai adaptációját, a civil és katonai információs rendszerek összefonódását, valamint a gyorsan változó információs környezetre épülő pszichológiai és dezinformációs műveletekben használt kommunikációs platformokat. Az eredmények rámutatnak, hogy a háború digitalizációja nem csupán új eszközök bevezetését jelenti, hanem a hadviselés alaplogikájának átalakulását is, ahol a digitális fölény megszerzése a fizikai erőforrásokkal egyenrangú stratégiai tényezővé vált.

Tartalom

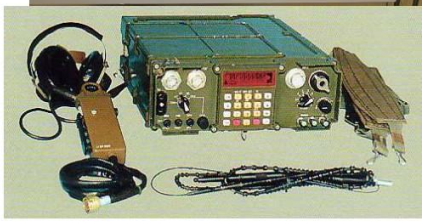
- Rádióhíradásban használt eszközök,
- Műholdas és mikrohullámú átviteli eszközök,
- Informatikai háttér,
- Okostelefonhasználat,
- Tartalékos regisztrációs app,
- Következtetések és javaslatok,
- Összegzés.

2

Orosz rádióeszközök: R-168 „AKVEDUK”

Képességek:

- fix frekvencia (egyfrekvenciás szimplex, kétfrekvenciás szimplex);
- frekvenciaugrás (FH) (egyfrekvenciás szimplex);
- pásztázás vétel 8 előre beállított frekvencián;
- manuális vagy automatizált rádiós adatrögzítés rádiós adatbeviteli eszközről (optikai interfészen keresztül) vagy külső számítógépről;
- vészhelyzeti rádióadatok törlése;
- konferencia-, cím- és hanghívások fogadása/továbbítása;
- távirányító telefonról;
- működés vezérlése külső számítógépről az RS-232C interfészen keresztül;
- hangos bejelentő a kezelő tevékenységeiről;
- párbeszéd mód;
- automatizált beépített tesztelés.



Főbb technikai adatok:

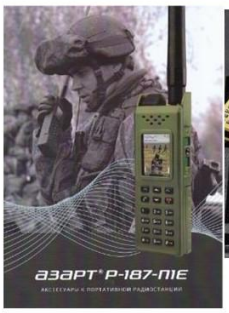
- Frekvencia tartomány, MHz: 30,0…107 975
- Frekvenciatávolság, kHz: 25
- Frekvencia ugrás FH módban, ugrás/s: 100
- FH módban használt frekvenciák száma: ±256
- Információátviteli sebesség, kbps: 1,2…16
- Adó kimeneti teljesítménye, W: 0,25; 2,0; 8,0
- Kommunikációs hatótáv (TShDA antenna), km:
  analóg információ (fix frekvencián minden üzemmódban): ±12 km
  digitális információ (minden üzemmódban): ±10 km

3

Orosz rádióeszközök: R-187 „AZART”

Főbb technikai adatok, Kézi rádió R-187-P1E

- Frekvencia tartomány, MHz: 27,0…520
- FH módban használt frekvenciák száma: 20000
- Információátviteli sebesség, kbps: 256
- Adó kimeneti teljesítménye, W: 4,0
- Kommunikációs hatótáv: minden üzemmódban ±4 km
- Tömeg: 0,5 kg
- Használható külső hőmérséklet intervallum: -40C --- +50C



Főbb technikai adatok, Beépített (és légideszant) rádió R-187-VE

- Frekvencia tartomány, MHz: 1,5 ---- 2500
- FH módban használt frekvenciák száma: (HF)100 – (VHF) 20000
- Információátviteli sebesség: 9,6 --- 33000 kbps
- Adó kimeneti teljesítménye: HF 100 W, VHF 40 W
- Kommunikációs hatótáv: minden üzemmódban HF 500 km *(ha ideálisak a körülmények)*, VHF 20 km
- Használható külső hőmérséklet intervallum: -40C --- +50C

4

Orosz (?) rádióeszközök:

KÍNAI BAOFENG

Wagner csoport

ÉSZAK KOREA: K1

Vihar hadtest

Ukrán rádióeszközök:

L3HARRIS család

A NATO Type-1 kriptoalgoritmust nem tartalmazzák a rádiók, így NATO kulcs sem tölthető fel. Ezen típusok a NATO-ban nem használt Citadell kulcsrendszert használják, vagy a Type-3-at.

Ukrán rádióeszközök:

aselsan

ASELSAN

Az ASELSAN V/UHF rádióit 2016 óta vásárolja az ukrán hadsereg. Az ukrán védelmi minisztériummal kötött szerződések alapján több ezer ASELSAN terméket szállítottak az Ukrán Fegyveres Erőknek, elsősorban a Szárazföldi Erők dandárjai számára, különösen a 30-512 MHz V/UHF sávban stabil kommunikációt biztosító rádiókat.

A VRC-9661 (10 W és 50 W), a PRC-9651 (5 W) és a PRC-5712 (125 mW) katonarádió. Mindegyiket a NATO-szabványoknak megfelelően tervezték, és biztosítják a titkosított hangkommunikációt és egyidejű adatátvitelt a felhasználók részére.

Főbb jellemzők:

- 1,77 hüvelykes színes RGB TFT kijelző 128 x 160 felbontással
- Magas szintű EHV (COMSEC és TRANSEC) - Beépített hardver alapú titkosítás - Frekvencia ugrás - Vészhelyzet törlése - Felhasználói hozzáférés
- Egyidejű hang- és adatkommunikáció
- Beépített GNSS vevő
- Beépített kamera (13 megapixel)
- Beépített memória (8 GByte)

7

Ukrán rádióeszközök:

ELBIT

E-LynX™ Vehicular Single Channel (V/UHF 1x50W)

E-LynX™ Vehicular Dual Channel (V/UHF 2x50W)

AES-256 kódolású kulcsalgoritmus: ***VÉDETT!***

E-LynX™ Tactical Router

E-LynX™ Intercom.

G-10N Key fill device

8

Ukrán rádióeszközök:

SILVIUS

A hadműveleti és harcászati szint támogatása érdekében szélessávú nagysebességű rádiórendszereket alkalmaznak a polgári mobil bázisállomások kommunikációs erőforrásaiba (Internet erőforrás), amely biztosítja a megfelelő cellákon belüli adattovábbítást a katonai oldalnak, valamint átjátszókat hoz létre a közellégtérben történő adattovábbításhoz. A MIMO technológiát haditechnikai híradó segédeszközként és kisegítő szolgáltatásként kívánja az ukrán haderő felhasználni.

Silvius 4400

Az adattovábbításhoz tervezett kiegészítő technológia:
SILVUS 4400 radió –7600 db,
SILVUS 4200 radió – 11000 db,

Sávszélesség 20 Mbit/sec
Kódolás: DES56, és AES256
Teljesítmény: 1 W
Csatorna sávszélesség: 1,25 – 2,5 – és 5 MHz
Frekvencia tartomány:
- *L band (139)--------1350-1440 MHz*
- *S Band (235)--------2200-2500 MHz*
- *Federal C-I (467)--4400-4940 MHz*

Silvius 4200

9

Ukrán civil rádióeszközök:

MOTOROLA SLR5500 ÁTJÁTSZÓ

Technikai adatok:
- VHF (136-174MHz); UHF1 (400-470MHz); 300R1 (300-360MHz)
- 64 programozható csatorna
- 1-50W állítható teljesítmény

Funkciók:
- Átjátszó
- Trönkölt központként lefedettségbővítés

MOTOROLA MOTOTRBO DM4600 MOBIL URH RÁDIÓ

Technikai adatok:
- VHF (136-174MHz); UHF1 (403-470MHz); UHF2 (450-527MHz)
- 64 programozható csatorna
- 1-25W/25-40W állítható teljesítmény

Funkciók:
- A rádió jelszóval is programozható
- vészhívás

MOTOROLA DP-4800/4400

VHF: 136-174MHz között programozható
- 1000 programozható csatorna
- Nagyméretű, színes, 5 soros LCD kijelző és teljes alfanumerikus billentyűzet
- 5 programozható gomb, egyszerű kezelhetőség
- Digitális MotoTRBO TDMA üzemmód
- Ipari felhasználásra kialakított ház és bevonat
- Különböző digitális csatornahozzáférési és hívási módok
- Maximum 5W RF kimenő teljesítmény
- IP57-es szabványnak megfelelő por és vízállóság

10

Rádióeszközök a fronton

- Orosz:

R-123/173
R-168 „AKVEDUR”
R-178 „AZART”
Kínai „noname” ipari rádióeszközök (*Baofeng*)

- Ukrán:

Motorola:
- MotoTrbo DP4801;
- SLR-5500;
- DM-4600;
- DP-4800/4400

- Harris (US)
- Aselsan (TR)
- Elbit (IL)
- Silvius, (US)

11

Orosz műholdas eszközök:

holdas katonai terminál rendszer,

- R-438M Belozer, (LEO)

- Katonai távközlési műholdak (harcászati és stratégiai):
  - Strela,
  - Raduga,
  - Meridian,
  - Rodnik.

12

Ukrán műholdas eszközök: Starlink

- Műholdalapú internetszolgáltatás, 32 országnak van hozzáférése
- Május végéig kb. 12 000 vevő terminált szállítottak le Ukrajnába
- Védett és biztos Internethozzáférés
- Polgári felhasználás: EÜ rendszerek (590 kórház és rendelő) + közig. és oktatás
- Katonai felhasználás:
  - drónok
  - ISTAR
  - adatmegosztás

VSAT: KA sáv 2000 db
KU sáv 600 db

13

Orosz mikrohullámú eszközök:

- Mikrohullámú katonai gerinchálózat,
  - R-416GM,

14

Ukrán mikrohullámú eszközök:

- Új mikrohullámú stacioner cellarendszer,
  - AirFiber rendszer,

1700 db állomás + aktív eszközpark (router, switch, hálózati elemek)

Jellemzők	Ubiquti AirFiber
Frekvencia sáv	5150-5250 MHz
Adatátviteli sebesség	1 Gbit/s
Sugárzási teljesítmény	29 dBm (790 mW)
Hatótávolság	100 km alatt
Antenna fejsúlya	1,5 kg

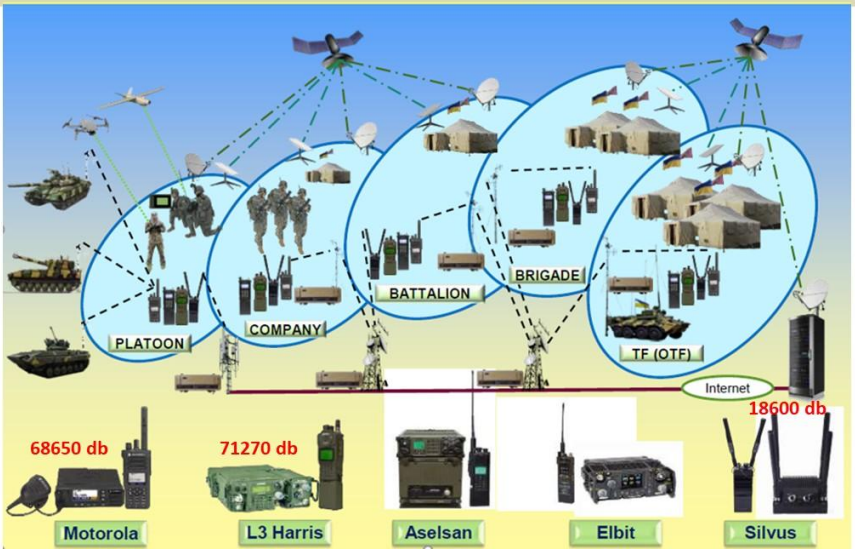
- COMET (US) troposzféra relé (BLOS):

200+ db állomás + aktív eszközpark (router, switch, hálózati elemek)

Jellemzők	COMET
Frekvencia sáv	4400-5000 MHz
Adatátviteli sebesség	5-60 Mbit/S
Sugárzási teljesítmény	10 W
Hatótávolság	60 km -ig
Hordsúly	25 kg

15

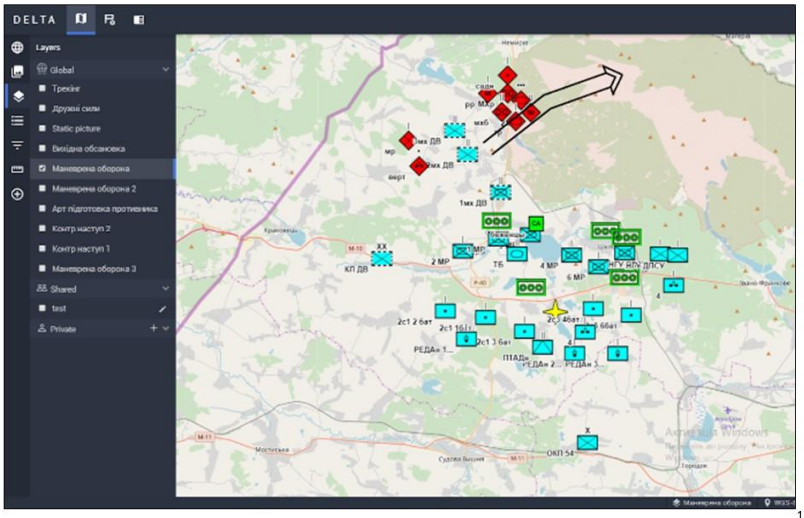
Híradó informatikai támogatás - Ukrajna



16

Ukrán valós idejű informatika:

DELTA



17

Ukrán valós idejű informatika:

A DELTA BMS szoftverrendszer

- egy web böngésző alapú **valós idejű térkép alapú vezetés-irányítási szoftverrendszer**
  (felhő - adatközpontok(hírközpontok) – applikáció, drón alkalmazás)
- a **rendszert az ukrán védelmi minisztérium fejlesztette ki a NATO és ukrán programozók segítségével**, így egy olcsó megoldás született, amit először 2017-ben tesztelték a Tide Sprint gyakorlaton, jelenlegi fejlesztési fázisban már NATO MIP4-IES kompatibilis,
- a Delta háromdimenziós képet nyújt a harctérről valós időben, **digitális térképen integrálja a különböző szenzorokból és forrásokból**, köztük a hírszerzéstől származó, az ellenségről szóló **információkat**,
- A rétegek lehetőséget adnak az aktuális csatatér objektumok rendszerezésére és logikai gyűjteményekre való felosztására, hogy megosztják a hozzáférésüket az egyes felhasználókkal vagy felhasználói csoportokkal
- a katonai csapatok, a civil tisztviselők (és még az ellenőrzött járókelők is) használhattak arra, hogy **nyomon kövessék és megosszák** egymással az **orosz erőkre vonatkozó részletes információkat**.
- nem igényel további beállításokat, és **bármilyen digitális eszközön** működőképes.
- A rendszerhez kapcsolódik a távirányítású elektromos járművek fejlesztése is.

18

Ukrán valós idejű informatika:

KROPYVA

19

Ukrán valós idejű informatika:

KROPYVA

20

Okostelefonhasználat - Ukrajna

Mobil/ okos eszközök alkalmazása:

Okostelefonok kiemelkedő szerepet játszanak az orosz-ukrán háborúban taktikai szinten döntő hatást tesznek lehetővé Ukrajnában

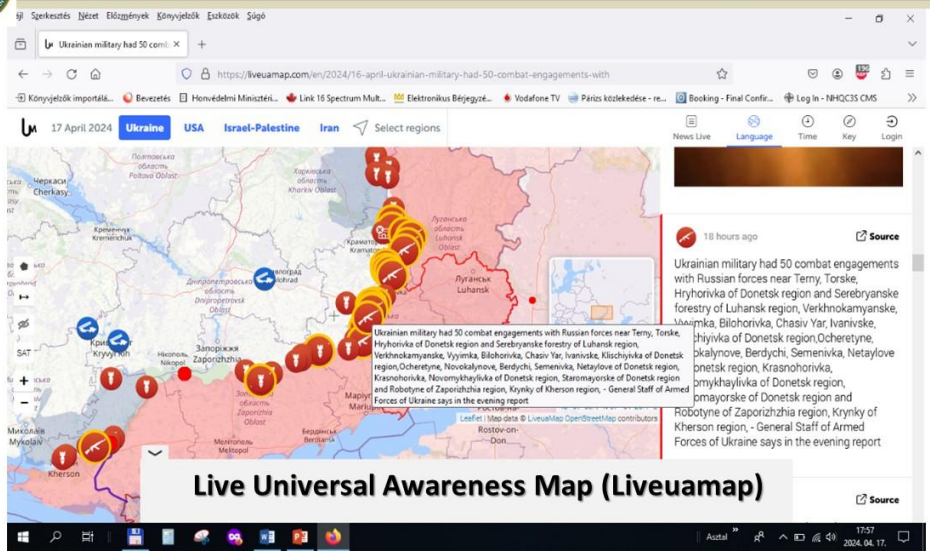
- Sebezhetőség *versus* javított helyzetfelismerés és agilis reagáló képesség

Az okos telefonok biztosítják a „nagy képet”.

- https://liveuamap.com/en/2024/16-april-ukrainian-military-had-50-combat-engagements-with
- Térinformatikai krízisfigyelés az AI támogatásával
- Üzleti modellre alapozott közös intelligencia kép és működési kép (CIP-COP)

21

Okostelefonhasználat - Ukrajna



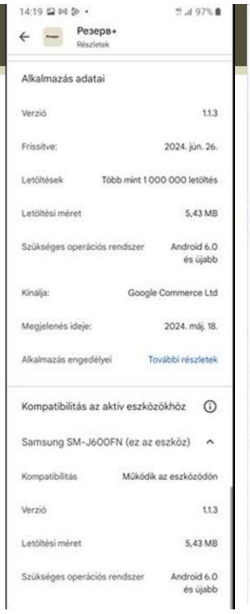
22

Tartalékos regisztráció

Rezerv+:

Hadrafoghatósági adategyeztetési app

- Több mint egymillió ukrán frissítette az adatait,
- Több ezer fő Ukrajnán kívülről is,
- IoS app nem fellelhető, csak Android



23

Következtetések és javaslatok:

- **Az ukrán hadsereg felhő alapon** szervezik az **adatkommunikáció**t, ---- ennek a megoldásnak a vizsgálata és megvalósítása folyik az MH-ban….
- **Az ukrán fél a stacioner adatközpontja mellett, még 4 db mobilt tervez** (mozgó kamionban), ----- szükséges az MH *Low Profile* mozgó adatközpontjaimnak kialakítása,
- Még **50000 db TETRA** (trönkölt, EDR) terminált szereznek be. (Az orosz zavarás nem hatékony a rendszerre),
- A **Területvédelmi Ezredek esetében** megfontolandó, hogy a méregdrága harcászati rádiók helyett a tervezett EDR rádiók beszerzése mellé szükséges beilleszteni az olcsó, **ipari kivitelű** polgári **rádiók** beszerzését.
- A civil **térfigyelő kamerákat rendszerbe szervezték**, AI (MI) fut rajta, korai előrejelzési rendszerben,
- Lakossági jelentő chat szobák kerültek kialakításra, ---- Kialakítása a nemzeti reziliencia érdekében szükséges,
- **Drónok** használata kiemelt jelentőséggel bír a konfliktusban, ---- a haderőfejlesztési program végére nem lehet olyan fegyvernem vagy támogató erő melynek nincs szakterületi drón- vagy autonóm eszköz képessége (MH Drónstratégia)

24

További szakterületi javaslatok:

- A **HUNTACCIS interoperabilitási képességének** és a szolgáltatásainak bővítése a mielőbbi **Egységes Műveleti Helyzetkép (COP)** stabil alkalmazása érdekében.
- A mobilizálható infokommunikációs képességek kialakítása, továbbá a **műhold alapú hírközlés vitális**. Az MH vonatkozásában tovább kell **növelni a műholdas képességet**, és a tervezett módon beindítani az MH VSAT programot.
- Aktívabb részvétel az **FMN** munkacsoportokban, szükséges beépíteni a híradó rendszerbe a munkacsoportban alkotott irányvonalakat, és implementálni a *Spiral 4* követelményrendszert.
- A híradó-informatikai eszközökkel alkotott hálózatok legyenek **redundánsak, illetve lehallgatás és zavarás ellen védettek.**
- A digitalizált manőver erők híradó-informatikai rendszerei egy **robosztus, magas sávszélességű** és megbízható átviteli transzportinfrastruktúrát (vegyes tábori és stacioner rendszer) követelnek meg.

25

ÖSSZEGZÉS

- **A Műveleti Digitalizáció felpörgetése,**
- **Több és pontosabb rendszerintegráció,**
- **Az MH VSAT program beindítása,**
- **Szakmai szinten kezelt decentralizált K+F projektek,**
- **A teljes állomány digitális kompetenciájának a növelése.**

- Mesterséges intelligencia (AI) bevezetése

- Konstruktív szimulációs térben,
- Drónvezérlésben,
- Hálózatmenedzsment helyzetfüggő módosítása érdekében,

27

Szerzőink figyelmébe

Kiadványunk lehetőséget biztosít max. 40 ezer leütés (egy szerzői ív) terjedelemben – *elsősorban: távközlés, híradás, informatika, információvédelem, illetőleg hadtudományi és természettudományi témakörökben* – tanulmányok, szakcikkek magyar és idegen nyelvű megjelentetésére.

A cikknek tartalmaznia kell egy 2-5 soros absztraktot magyar és/vagy idegen nyelven.

A cikkek beküldése e-mailen a hhk_hirado_szakcsoport@uni-nke.hu címre lehetséges. A cikkek leadási határideje: folyamatos (megjelenés évente kétszer).

A megjelentetésre szánt cikkek csak a szerző(k) eddig máshol még meg nem jelent, saját önálló (társszerzők esetében közös) írásműve(i) lehetnek. Az írásművekben lévő idézeteknek meg kell felelniük a szerzői jogról szóló hatályos jogszabályoknak. A megjelentetésre szánt írásművek csak nyílt (nem minősített) információkat és adatokat tartalmazhatnak. Ezek minősített voltát a szerkesztőbizottság nem vizsgálja, ennek felelőssége a cikk szerzőjét terheli.

A szerkesztőbizottság a megjelentetésre szánt írásműveket lektoráltatja. A szerkesztőbizottság fenntartja a jogot, hogy a megjelentetésre szánt és megküldött írásművet – *külön indoklás*

nélkül - megjelenésre alkalmatlannak ítélje. Az ilyen cikkeket nem küldi vissza, és nem őrzi meg.

A kiadványban lehetőség van idegen nyelvű cikkek megjelentetésére. Az idegen nyelven megjelentetésre szánt írásművek nyelvi lektorálása a szerzőt terheli.

Minden kézirathoz elektronikusan is mellékelni kell egy kitöltött "Kéziratbeküldési űrlap"-ot, és egy "Copyright átruházási űrlap"-ot. Mindkét űrlapot ki kell nyomtatni és alá kell írni (többszerzős cikk esetében minden szerzőnek!), majd a kinyomtatott és aláírt űrlapokat faxon (fax szám: +36-1-432-9025), vagy postai úton levélben (levélcím: Hírvillám Szerkesztőség, 1581. Budapest Pf.: 15.) is meg kell küldeni a szerkesztőségnek. Ezek hiányában a cikkeket a szerkesztőség nem lektoráltatja és nem jelenteti meg!

Az űrlapok a szerkesztőségnél szerezhetők be.

Megjelent az NKE HHK KII Infokommunikációs és Információbiztonsági Tanszék gondozásában

www.comconf.hu
www.puskashirbaje.hu

HU ISSN 2061-9499

***

NKE HHK KII IIT
1101 Budapest, Hungária krt. 9-11.
1581 Budapest, Pf. 15.
+36 1 432 9000 (29-407 mellék)