HADMÉRNÖK

Kiemelt közlemények

Farkas Gábor, Fazekas Gábor:
Ipari vezérlő rendszerek sebezhetősége

Fráter-Szegedi Judit, Tisza István:
Egyéni védőeszköz és mesterséges intelligencia

Hankó Viktória: *Mesterséges intelligencia alkalmazása a kiberműveletekben*

20. évf. (2025)
1. szám

ISSN 1788-1919 (elektronikus)

LUDOVIKA
EGYETEMI KIADÓ

IMPRESSZUM

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

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

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

Tartalom

Biztonságtechnika

Védeleminformatika

Fórum

HADMÉRNÖK
BIZTONSÁGTECHNIKA

20. évfolyam (2025) 1. szám 5–18.
DOI: 10.32567/hm.2025.1.1

Fráter-Szegedi Judit,[1] Tisza István[2]

Egyéni védőeszköz és mesterséges intelligencia

A védelem jövője

Personal Protective Equipment and Artificial Intelligence

The Future of Protection

Absztrakt

A technológia fejlődése a munkabiztonság területén is érzékelhető. Megnövekedett az igény a védőeszközök védelmi szintjének növelésére, lévén egyre több veszéllyel érintettek a tevékenységet végző munkavállalók. Az intelligens eszközök fejlesztése azonban nem költséghatékony, nem is feltétlenül megtérülő befektetés (munkavállalói oldalról is szükséges az egyes funkciók elfogadása, akarniuk kell az eszközöket használni), emellett a jogszabályi háttér megalkotása is elvégzendő feladat még. A technológia teljes ismerete szükséges ahhoz, hogy a megfelelőségtanúsítási folyamatok eredményeként biztonságos, jól használható eszközt kapjanak a felhasználók. A szabványosítás, a fogalmi keretek meghatározása nehézkes. Számos kihívással szembesül a gyártó, a megfelelőségtanúsító szervezet, illetve a felhasználó is, főként akkor, ha a munkabiztonsági kultúra is erőteljesen fejlesztendő, és növelni kell a munkavállalói tudatosságot.

Kulcsszavak: intelligens védőeszközök, szabványosítás, funkciók, tudatosság, jogszabály, fogalmi keret

[1] E-mail: szegedi.judit85@gmail.com
[2] E-mail: istvan.tisza2@katved.gov.hu

Abstract

The development of technology can also be felt in the field of occupational safety. The need to increase the level of protection of protective equipment has increased, since the workers performing the activity are affected by more and more dangers. However, the development of smart devices is not a cost-effective, nor is it necessarily a profitable investment (acceptance of certain functions is also necessary from the employee's side, they must want to use the devices), in addition, the creation of the legal background is still a task to be completed. Full knowledge of the technology is necessary so that users receive a safe, easy-to-use device as a result of the conformity certification processes. Standardization and definition of conceptual frameworks are difficult. The manufacturer, the conformity certification organization, and the user are also faced with many challenges, especially if the work safety culture also needs to be strongly developed and employee awareness needs to be increased.

Keywords: intelligent protective devices, standardization, functions, awareness, legislation, conceptual framework

Bevezetés

A munkahelyi környezet dinamikus változása, a munkavállalókat érő kockázatok folyamatos bővülése hívta életre azt az igényt, hogy az egyéni védőeszközöket (PPE)[3] intelligens rendszerekké alakítsák át. A technológia fejlődése megteremti annak lehetőségét, hogy az egyéni védőeszközök ne pusztán passzív védelmet jelentsenek a munkavállaló számára, hanem aktívan figyeljék a környezet változásait, és reagáljanak azokra. A fejlett, MI-algoritmusokkal ellátott érzékelők valós idejű adatokat gyűjtenek, elemeznek, dolgoznak fel, és azonnali visszajelzésekkel reagálnak, figyelmeztetik az eszköz viselőjét a potenciális veszélyre. Az intelligens vagy okoseszközök alkalmazásának létjogosultságát a körülmények gyors és nagymértékű, állandó változása, a védelmi szintek növelésének igénye adja.

A felhasznált anyagok fejlesztése nem minden esetben jár együtt a kényelemmel, a használhatósággal vagy a könnyű, ergonomikus viselettel (lásd például a tűzoltók bevetési védőruháit). Az intelligens/okos kitétel azonban nem csupán az adatfeldolgozásban jelenhet meg: az öngyógyító anyagok szintén a védelmi szint növekedését célozzák, a rugalmas, szabad mozgás biztosítása mellett. A kor elvárásainak a hagyományos védőeszközök nem képesek teljes mértékben megfelelni. A munkahelyek, ipari folyamatok változása, a technológiák fejlődése új típusú veszélyeket hoz magával, sok esetben exponenciálisan növelve a munkavállalókat érő káros hatások mennyiségét.

A változások minőségi változást is hoznak: számos új vegyi anyag kerül a piacra, amelyek kezelési szükséglete nem ismert; nagyobbak az épületek; bonyolultabbak a technológiák; másabbak az igények.[4] Az alkalmazás előnyei, az erre való igény

[3] PPE: *personal protective equipment.*
[4] Thierbach 2020.

megkérdőjelezhetetlen (a hagyományos védőeszközök sok esetben nem hatékonyak, a kockázatokat nem tudják teljes egészében csökkenteni, vagy esetleg viselésük többletkockázatot jelent – zajos környezetben viselni kellene a hallásvédelmi eszközt, azzal együtt azonban nem hallhatja például az utasításokat), azonban nem hagyható figyelmen kívül, hogy a nem hagyományos védőeszközök fogalmi körének meghatározása önmagában sem egyszerű feladat. Emellett a jogalkotással és a szabványosítással kapcsolatban is sajátos kihívások övezik a témát. A megfelelőségértékelő folyamat során ugyanis a gyártó, a bejelentett szervezet köteles az okosvédőeszközt teljes egészében vizsgálni.[5]

A tanulmány célja az intelligens védőeszközök fejlesztésének és alkalmazhatóságának vizsgálata a munkahelyi biztonság növelése érdekében. A kutatás során feltárjuk az új technológiák nyújtotta lehetőségeket, azok előnyeit és kihívásait, valamint a jogalkotási és szabványosítási folyamatok szükséges lépéseit, a nehézségeket. Továbbá célunk a munkavállalói tudatosság növelése és a biztonsági kultúra fejlesztése annak érdekében, hogy a modern védőeszközök alkalmazásával minimalizálni lehessen a munkahelyi veszélyeket és baleseteket. A technológia olyan fejlődési ívet rajzol, amely egyértelmű és jelentős hatást gyakorol valamennyi gazdasági ágazatra. Az egyéni védőeszközök fejlesztése során alkalmazható új technológiák az eszközök védelmi szintjét tovább növelhetik úgy, hogy azok viselési komfortját, használhatóságát nem rontják. Az alkalmazhatóság azonban ennél jóval bonyolultabb kérdéskört határoz meg: a megfelelőségtanúsítás folyamata, a vonatkozó követelmények megfogalmazása, az ezeknek való megfeleltetés, a felhasználókat érő kihívások abba az irányba mutatnak, hogy az intelligens védőeszközök alkalmazása kiaknázatlan lehetőség, de nagyon a folyamat elején tartunk. A tanulmány célja a vonatkozó szakirodalom áttekintése, az egyes területek nehézségeinek megfogalmazása a teljesség igénye nélkül.

A vizsgálat módszere a nemzetközi és a hazai szakirodalom, a korábban a témában végzett kutatások szisztematikus áttekintése (Ammad és munkatársai végeztek hasonló áttekintést 2008-ig visszamenőleg).[6] Az intelligens védőeszközök alkalmazhatóságát és az ezzel kapcsolatos kihívásokat szakértőkkel és munkavállalókkal készített interjún keresztül kívánjuk a jövőben vizsgálni. A használat konkrét példáit esettanulmányok segítségével igyekszünk elemezni. Empirikus vizsgálatok során mérhető adatok alapján értékelhető a gyakorlati alkalmazhatóság és a hatékonyság. Összefoglalva, a kutatás során különböző módszereket alkalmazunk annak érdekében, hogy átfogó képet kapjunk az intelligens védőeszközök fejlesztéséről, alkalmazhatóságáról, valamint a használat során felmerülő előnyökről és kihívásokról. Célunk, hogy hozzájáruljunk a munkahelyi biztonság növeléséhez és a munkavállalói tudatosság fejlesztéséhez, ezáltal minimalizálva a munkahelyi veszélyeket és baleseteket.

[5] Thierbach 2020.
[6] Ammad et al. 2021: 3495–3507.

Intelligens védőeszközök

Ahhoz, hogy az intelligens védőeszközök problémakörét vizsgálni tudjuk, szükséges a vonatkozó fogalmak megfelelő definiálása. A hagyományos védőeszközök jogszabályban meghatározottak, az intelligens védőeszközök meghatározása azonban jóval nehezebb. A hagyományos kitételt a jogszabály nem alkalmazza. A 65/1999. (XII.22.) EüM rendelet az alábbiak szerint adja meg az egyéni védőeszköz definícióját:

„a) egyéni védőeszköz:
aa) minden olyan eszköz, amelyet a munkavállaló azért visel vagy tart magánál, hogy az a munkavégzésből, a munkafolyamatból, illetve a technológiából eredő kockázatokat az egészséget nem veszélyeztető mértékűre csökkentse, továbbá
ab) az eszköz bármely kiegészítése vagy egyéb segédeszköz, amelynek a feladata az *aa)* pont szerinti cél elérése (a továbbiakban *aa)* és *ab)* pontok együtt: védőeszköz)".[7]

Az intelligens eszközök „hagyományos" eszközökbe integrált érzékelők, mesterséges intelligencia vagy gépi tanulás összessége. Továbbfejlesztett anyagok, elektronikus alkotóelemek révén magasabb szintű biztonságot nyújtanak a kényelmi funkció megtartása mellett.

„Minden egyéni védőeszköz, amelyik megkönnyíti az emberi tevékenységet, gyorsítja a munkavégzést, időt takarít meg, visszajelzést ad (akár vészjelzést is, de olyat, amit nagyon könnyen, nagyon gyorsan tudunk azonosítani) a felhasználó számára, magasabb szinten biztosítja a védelmet, mint enélkül lenne a védelem, megelőzhető lesz a munkabaleset, megelőzhetjük a munkavállaló sérülését, információt ad a környezetnek, a munkavezetőnek, a központnak vagy más érintettnek, mindezek intelligens egyéni védőeszköznek minősülnek."[8]

A passzív intelligens egyéni védőeszköz olyan anyagból készült, olyan kialakítással, amely az eszközt érő hatásokkal szemben magasabb szintű védelmet képes nyújtani, a kockázatok gyorsan és jól azonosíthatóvá válnak. A munkavállaló rendelkezésére álló információk képesek a személyes védelmet magasabb szintre emelni (zuhanásjelző, kopásjelző, szűrőbetét-telítettségi indikátor, UV-fény-igénybevétel visszajelzője, pH-érték-visszajelző festék, energiaelnyelő anyag, intelligens textilek). Az aktív eszközök annyiban különböznek ezektől, hogy ezekbe aktív kiegészítők és eszközök vannak beépítve, amelyek mind a felhasználónak (munkavállaló), mind a munkáltatónak információt szolgáltatnak a munkakörnyezetről (hőmérséklet, relatív páratartalom), a lehetséges veszélyekről, a munkavállalókat érő kockázatokról, a személyes adatokról, illetve a munkavégzéshez kapcsolódó adatokról. Ilyen aktív eszköz lehet:

- RFID (*radio frequency identification* – rádiófrekvenciás azonosítás),
- jeladók,

[7] 65/1999. (XII. 22.) EüM rendelet a munkavállalók munkahelyen történő egyéni védőeszköz használatának minimális biztonsági és egészségvédelmi követelményeiről 2. § (1) bekezdés.
[8] Hegedűs 2021: 39.

- biometriai adatok, levegő, hőmérséklet, káros anyag stb. visszajelzése – környezeti adatok mérése,
- visszajelző szenzorok,
- LoTo[9], robotok, drónok,
- nanotechnológia stb.[10]

Valamennyi, nem passzív védelmet nyújtó eszköz számos funkciót képes ellátni, különleges tulajdonságokkal ruházzák fel a mesterségesintelligencia-eszközök, nanotechnológiai megoldások, elektronikai egységek segítségével. Viszonylag új, gyorsan fejlődő terület, a technológia adta lehetőségek folyamatosan bővülnek, a határok nem húzhatók meg élesen, elmosódnak. Gyakran vannak a különböző technológiák között átfedések. Az intelligens védőeszközök csökkentik a veszélyeknek való kitettséget, valamint adatokat gyűjtenek, és értesítéseket, figyelmeztetéseket küldenek a védőeszközt viselőknek a körülmények megváltozásáról (ennek főként akkor van jelentősége, ha a gyors és külső körülményekhez való automatikus alkalmazkodás akár életeket is menthet – például veszélyes üzemekben súlyos üzemzavar vagy katasztrófahelyzet bekövetkezése esetén, amikor nem ismert az anyagok egymásra hatásának minden következménye).

A hagyományos védőeszközök komoly munkabiztonsági tudatosságot igényelnek a munkavállalóktól, munka- és időigényes a körülmények felülvizsgálata. A biztonsági előírások paraméterei a megnövekedett komplexitással, a technológiai fejlődéssel, a globalizációval, az idő- és költségnyomással, egyéb vezetői elvárással, az érdekelt felek magasabb elvárásaival nem képesek valós időben tartani a lépést.[11] A kényelmetlen munkahelyzetek automatikus észlelése talpbetét segítségével,[12] valós idejű védőfelszerelés-figyelő rendszerrel,[13] EEG és Random Forest Classifier segítségével megvalósuló álmosság- és esésészleléssel, okoscipővel készített valós idejű, 3D-s térképpel[14] a védőeszközök messze túlmutatnak a passzív védelmen.

A nem hagyományos védőeszközök, intelligens eszközök tehát nem kizárólag attól lehetnek intelligensek, hogy valamilyen elektronikus alkotóelemet tartalmaznak. A meghatározás ezért nehézkes. Az intelligens eszközök nagy részénél valóban az elektronika eredményezi az okos kitételt: egy hagyományos eszköz érzékelővel, detektorral, adatátviteli modullal, akkumulátorral, kábelekkel és/vagy más elemekkel ötvözve. Az értékelők segítségével mérhető a munkavállaló munkaképessége adott időpillanatban, a körülmények változásának megfelelően valós időben. A vegyi üzemekben bekövetkező katasztrófahelyzetek során a beavatkozást végzők számára eddig nem volt lehetséges a mérgező gázok, keverékek vagy az extrém magas hőmérséklet detektálása, sem a bevetést követő állapotra vonatkozó információk elérhetővé tétele,

[9] A LoTo a Lockout/Tagout kifejezés rövidítése. Magyarul kizárás-kitáblázás. Karbantartás során alkalmazott eljárás a gépek, berendezések véletlenszerű beindításának megakadályozása, az elsődleges vagy a felszabadult tárolt veszélyes energia okozta baleset megelőzése a célja.
[10] Hegedűs 2021.
[11] Rasouli et al. 2024.
[12] Antwi-Afari 2018: 433–441.
[13] Barro-Torres et al. 2012: 42–50.
[14] Nguyen et al. 2016: 2–12.

napjainkban azonban a védőeszközökkel képesek a munkakörülményeket veszélyes helyzetben is optimalizálni.[15]

Az intelligens eszközök meghatározásakor alapvető kitétel a környezettel való valamilyen mértékű interakció, a környezeti feltételekre való valamilyen szintű reagálás képessége. Az Európai Szabványügyi Bizottság (CEN) kísérletet tett a fogalom definiálására: „Az intelligens egyéni védőeszköz olyan egyéni védőeszköz, amely […] rendeltetésszerűen és hasznos módon reagál vagy a környezetében beálló változásokra, vagy valamilyen külső jelzésre/bemeneti adatra."[16]

Az 1. ábrán jól látható, hogy az intelligens egyéni védőeszközök köre meghatározható az alapján, hogy tartalmaz-e elektronikát, vagy sem, illetve történik-e adatgyűjtés, és amennyiben igen, milyen jellegű. Az elektronikával felszerelt, de adatot nem gyűjtő eszközre példa a láthatósági öltözet világítással kiegészítve, vagy ellenállásfűtőként működő intelligens hővédő textília. A nem személyes adat lehet az egyéni védőeszköz állapotára vonatkozó adat, vagy a felhasználó általi közvetlen elemzés céljából, vagy az adatok továbbítását követően egy központi vezérlési pont általi elemzés céljából, vagy későbbi elemzés céljából, illetve a viselő környezetére vonatkozó adat. A személyes adatok biometrikus, helymeghatározási, mozgásfelderítési adatok lehetnek. Az elektronika nélküli eszközök (utolsó oszlop) közé azok a védőeszközök sorolhatók, amelyek például rázkódáscsillapítással vannak felszerelve, vagy a bizonyos anyagokkal érintkezve színüket megváltoztató kesztyűk.[17]

1. ábra: Intelligens egyéni védőeszközök, összetétel és adatgyűjtési képességeken alapuló osztályozás
Forrás: Thierbach 2020: 2 alapján a szerző szerkesztése

[15] Thierbach 2020.
[16] Thierbach 2020: 2.
[17] Thierbach 2020.

Az intelligens egyéni védőeszközök létjogosultságát az a megnövekedett igény, egyre fokozódó állapot adja, amely a munkabalesetek számának stagnálásához/növekedéséhez köthető. Világszerte minden 15. másodpercben meghal egy munkavállaló munkabalesetben, Magyarországon kéthetente három a halálos munkabalesetek száma átlagosan (ennek nagy részét a mezőgazdaság, az építőipar, a feldolgozóipar „produkálja"). A munkavállaló hatékony védelmét sok esetben nem lehet zárt technológiával, kollektív műszaki védelemmel, megelőzési, szervezési intézkedésekkel biztosítani, szükség van egyéni védőeszközök használatára. A technológia fejlődése (gépek, berendezések, munkaeszközök) szükségszerűen magával hozza azt is, hogy az eszközöknek is magasabb szintű védelmet kell biztosítaniuk. Az Európai Parlament és a Tanács (EU) 2016/425. számú rendelete II. mellékletének 3. pontja foglalja össze a legcélratörőbben: „Az alapvető egészségvédelmi és biztonsági követelményeket a tudománynak a tervezéskori és gyártáskori állását és az aktuális gyakorlatot, valamint a magas fokú egészség- és biztonságvédelemmel összhangban lévő műszaki és gazdasági megfontolásokat figyelembe véve kell értelmezni és alkalmazni."[18] A gyártónak kötelessége arról gondoskodni, hogy „az egyéni védőeszköz a tudomány mindenkori állását figyelembe véve folyamatosan megfeleljen a vonatkozó alapvető egészségvédelmi és biztonsági követelményeknek".[19] Az intelligens védőeszközök használatával biztosítható a munkavállalók számára az, hogy

- a leghatékonyabb védelmet biztosító védőeszközt viseljék;
- ellenőrizhető legyen, hogy viselik-e a szükséges eszközöket;
- a munkavállaló egyértelmű jelzést kapjon arról, hogy a védőeszköze funkcionálisan megfelelő-e, a védelmi képessége az előírtnak megfelelő-e;
- a munkáltató/munkavállaló adekvát információkkal rendelkezzen a munkakörnyezetről és a munkavállaló biometrikus adatairól;
- az azonnali kommunikáció biztosított legyen a munkavállaló és a munkáltató között;
- a kötelezően viselendő egyéni védőeszköz a maximális hatékonyság mellett a kényelmi elvárásoknak is teljes mértékben képes legyen megfelelni.[20]

Nemzetközi vs. hazai szakirodalom – értékelés

A téma vizsgálata a szakirodalom áttekintésével kezdődik. A vonatkozó tanulmányok, konferenciaközlönyök, kutatási projektek széles körű volta, komplexitása egyértelműen megmutatja, hogy az intelligens védőeszközök létjogosultsága megkérdőjelezhetetlen valamennyi nemzetgazdasági ágazatban, a világ és az élet minden területén. Jelen cikk szempontjából a munkavédelem a leginkább releváns.

A nemzetközi szakirodalom szerteágazó módon vizsgálja az intelligens eszközök alkalmazhatóságát, a kihívásokat, a lehetőségeket és a jövőbeli irányokat egyaránt. Munkavédelmi vonatkozása azonban jóval kevesebb van, mint például az egészségügyben

[18] Az Európai Parlament és a Tanács (EU) 2016/425 rendelete (2016. március 9.) az egyéni védőeszközökről és a 89/686/EGK tanácsi irányelv hatályon kívül helyezéséről (EGT-vonatkozású szöveg).
[19] Hegedűs 2021: 38–43.
[20] Hegedűs 2021.

(pulzusszám, magzatmozgás, egészségmegfigyelés, mozgásszervi betegségek kockázatértékelése stb.). A védőfelszerelések nagymértékben leszűkítik a vizsgálati területeket. Ewa Skrzetuska és Paulina Rzeźniczak olyan forradalmi innovációkat taglal, amelyek rugalmas elektronika integrálásával teszik lehetővé a hordható egészségügyi monitorok, az interaktív ruházat és az energiatermelő szövetek létrehozását, az irányt tehát egyértelműen kijelölik. A gyors és nagymértékű fejlődéssel kapcsolatban azonban kritikát is megfogalmaznak: a fenntarthatóság és a körkörösség szempontjából nem feltétlenül működőképes alternatíva (a legtöbb tanulmány nem tér ki arra, hogy ezen eszközök az élettartamuk végén is számos kihívást támasztanak műszaki, gazdasági és környezetvédelmi szempontból egyaránt, figyelembe véve az újrahasznosítási technológiákat és a szakpolitikai környezetet).[21] A tudományos konferenciák, kutatási projektek jellemzően szintén az egészségügyi alkalmazhatóság irányába mutatnak.

Az intelligens egyéni védőeszközök területén az elmúlt évtizedben robbanásszerűen megnőtt a témában végzett kutatások száma. A nemzetközi szakirodalomban fellelhető tanulmányok egyértelműen reflektálnak a technológia és a munkahelyi biztonság iránti erősödő kereslet szükségszerű kapcsolatára, de nem feltétlenül a kellő mértékben. A legújabb technológiák gyors terjedésének irányán kívül marad a munkavédelem. A témában íródott cikkek, a végzett kutatások a viselhető technológiák fejlődését jelenítik meg részletesen és széleskörűen, a biometrikus adatok feldolgozása, a valós idejű figyelmeztetések, a prediktív analitika fokális pontnak tekinthető, a munkavállalók biztonságához hozzájárul, a vonatkozó szakirodalom áttekintése során szerzett tapasztalatok alapján nem ez élvez prioritást. A szenzorok, az IoT- (Internet of Things) megoldások, a mesterséges intelligencia, az integrált PPE-rendszerek mélyebb kutatása iránti igény erősödése még várat magára. A széles körű alkalmazás elsősorban az egészségügyben jelenik meg, a szakirodalmak is ezt az irányt taglalják, noha az építőipar, a gyártás és a feldolgozóipar, a mezőgazdaság is figyelmet érdemelne (tekintve, hogy a súlyos és/vagy halálos kimenetelű munkahelyi balesetek nagy számban ezen nemzetgazdasági ágazatokhoz köthetők). Kicsivel nagyobb figyelmet fordítanak a jogi és etikai aspektusokra (adatvédelem, magánélet tiszteletben tartása, munkahelyek védelme). A jogszabályi megfelelőség (a vonatkozó előírásoknak való megfelelés) azonban még inkább feltáratlan terület. Ez nélkülözhetetlen az intelligens eszközök sikeres integrációjához. A legjellemzőbb terület a kihívások áttekintése: magas költségek, felhasználói elfogadás, tudatosság, technológiai integráció komplexitása. A jövőbeni kutatások tárgya a technológia integrációja mellett egyértelműen a költségcsökkentés, a költséghatékonyság (és önmagában a hatékonyság). Az igények növekedésével feltehetően a munkahelyi biztonság is jóval nagyobb hangsúlyt kap.

A hazai szakirodalom kevésbé komplex a téma kapcsán, mivel az viszonylag új terület. Számottevő növekedés tapasztalható a vonatkozó kutatások tekintetében. Ennek oka, hogy egyre nagyobb az igény a munkahelyi balesetek megelőzésére, a munkavállalók védelmére. Az eszközök fejlesztése a hatékonyság érdekében történik (minél magasabb védelmi szint elérése) oly módon, hogy a kényelmi funkció se szoruljon háttérbe. Nagyobb hangsúlyt kap az alkalmazhatóság, az alkalmazott technológiák integrálhatósága, illetve a jogszabályi környezet erős hiányossága. Az alkalmazott

[21] Skrzetuska–Rzeźniczak 2025.

technológiák bemutatása fejlődő tendenciát mutat, figyelembe veszi az intelligens eszközök munkavédelmi gyakorlatba való integrálhatóságát, az azonban egyértelmű, hogy hazai vonatkozásban is van hová fejlődnie a téma kutatásának. A tudományos diskurzus a folyamat elején tart. A jogi és etikai kérdések, a munkahelyi biztonság nehézségei, a költségvetési korlátok, a technológiai ismeretek hiánya, az elfogadottság problémái jelentős mértékben meghatározzák a hazai szakirodalom kutatási irányát.

Jogszabályi környezet

Az egyéni védőeszközök biztosításával, kiválasztásával, használatával, karbantartásával stb. kapcsolatban jogszabályok és rendeletek határozzák meg a vonatkozó követelményeket (jelen esetben a korábban a jogszabályban meghatározott egyéni védőeszköz tekintetében, az intelligens eszközök vonatkozásában a szabályozás nem, vagy nem teljes mértékben értelmezhető). Ezek a következők:

- 1993. évi XCIII. törvény a munkavédelemről;
- 61/1999. (XII. 1.) EüM rendelet a biológiai tényezők hatásának kitett munkavállalók egészségének védelméről;
- 65/1999. (XII. 22.) EüM rendelet a munkavállalók munkahelyen történő egyéni védőeszköz használatának minimális biztonsági és egészségvédelmi követelményeiről;
- 16/2000. (VI. 8.) EüM rendelet az atomenergiáról szóló 1996. évi CXVI. törvény egyes rendelkezéseinek végrehajtásáról;
- 11/2003. (IX. 12.) FMM rendelet az ipari alpintechnikai tevékenység biztonsági szabályzatáról;
- 18/2008. (XII. 3.) SZMM rendelet az egyéni védőeszközök követelményeiről és megfelelőségének tanúsításáról;
- 17/2013. (VI. 4.) NGM rendelet az egyéni védőeszközök megfelelőségét értékelő szervezetek kijelölésének, tevékenységének, valamint ellenőrzésének különös szabályairól.

2. ábra: Munkavédelmi kesztyűk jelölései
Forrás: Magyar szabvány – Védőkesztyűk mechanikai kockázatok ellen 2019

Az európai szabványok általános és speciális követelményeket tartalmaznak. A védőkesztyűk tekintetében például az MSZ EN 420 tartalmazza az általános követelményeket (úgymint a méretezés, a fogásbiztonság, a szükséges jelölések, az azonosítással kapcsolatos előírások stb. – bőrkesztyűk esetében 30–180 perc vízállóságot ír elő). Az MSZ EN 407 határozza meg a kesztyű termikus védelmi képességeinek megfelelő teljesítményszinteket – a jelöléseket lásd a 2. ábrán.[22]

Gyúlékonysággal szembeni ellenállás (a) (15 másodperc égés után a varratok épsége mellett) az utánlángolási időtartam kevesebb mint 20 másodperc (≤20). Kontakt hővel szemben (b) (belső felület-hőmérséklet hány foknál emelkedik 10 °C-ot) 350 °C-ig ellenáll, a konvektív hővel szemben (c) több mint 4 másodpercig ellenáll (a belső hőmérséklet hány másodperc alatt emelkedik 24 °C-kal). Sugárzó hővel, kis mennyiségű olvadt fémmel, nagy mennyiségű olvadt fémmel szembeni ellenálló képessége (d., e., f.) szintén a szabvány által meghatározott teljesítményszinteket mutatja. A mechanikai ártalmak elleni védelem (MSZ EN 388) a koptató-, a vágóhatás, a szakítóerő, a szúróhatás stb. elleni védelem szintjét jelenti. Az intelligens (szenzorral, elektronikával, nanoréteggel stb. ellátott) védőkesztyű védelmi szintjének meghatározása ezekkel a mérőszámokkal nem lehetséges, mert a védelmi szint növelése nem feltétlenül a vastagabb, ellenállóbb anyag alkalmazásával történik, ezért a rendeletben/szabványban előírt alapvető egészség- és biztonságvédelmi követelmények teljesítettségére más mérőszámokat kell alkalmazni. A környezeti feltételek változására való reagálás, az interakcióba lépés mértéke az alkalmazott technológia függvénye. A homogén jogszabályi környezet megteremtése azután valósítható meg, hogy meghatározzuk az osztályozási rendszert, a vizsgálati szempontokat (lásd 1. ábra). Az intelligens eszközöket típusokra kell bontani az összetétel és az adatgyűjtési képességek alapján. A külső jelzés/bemeneti adat, külső környezeti változás mértéke és milyensége számos kombinációban határozhatja meg, hogy milyen védelemre van szüksége a munkavállalónak. Ugyanez az összetettség vonatkozik valamennyi egyéni védőeszközre.

Jogalkotás, szabványosítás – kihívások

Azzal egyidejűleg, hogy az intelligens egyéni védőeszközök alkalmazása jelentős előrelépés lehet a munkahelyi biztonságban, a munkavállalókat érő kockázatok csökkentésében, illetve megszüntetésében, az új fejlesztések bevezetése nem képes akadálytalanul végbemenni. Az engedélyezési folyamat összetett. A megfelelőségi eljárások során a védőeszközöket új egészként kell vizsgálni, elsősorban a tekintetben, hogy a használójára nem jelent semmiféle kockázatot. A vizsgálati szempontok között szerepel, hogy a felületi hőmérséklet ne haladja meg a megengedhető szintet, az akkumulátor biztonságos legyen, az elektromágneses mezők milyen hatással vannak az eszközt használókra, illetve az elektromágneses összeférhetetlenség nem áll-e fenn. A szabályozás elengedhetetlen, a szabványok révén biztosítható, hogy valamennyi védőeszköz megfeleljen az előírásoknak, az elvárt védelmi szintnek, viselője számára ne jelentsen többletkockázatot.

[22] MSZ EN 388:2016+A1, Magyar szabvány – Védőkesztyűk mechanikai kockázatok ellen. 2019. október.

A gyártók, illetve a bejelentett szervezetek a típusra vonatkozó követelményeket megtalálják a szabványokban. A legfontosabb kérdés az intelligens eszközökkel kapcsolatban az, hogy a szabályozás hogyan képes kiterjedni minden olyan körülményre, amely az eszköz használatát képes befolyásolni, hogyan lehet a viselés korlátait, a közép- és hosszú távon megjelenő többletkockázatokat széleskörűen megadni (például a nanoanyagok allergiás tüneteket okozhatnak). Jelen állapotban az egyéni védőeszközök minősítéséhez nem állnak rendelkezésre szabványok, a saját megítélésre való hagyatkozás jelen esetben nem lehet alternatíva. A CEN közzétett ugyan egy útmutatót, amely tudnivalókat és ajánlásokat gyűjtött össze (CEN/TR 16298:2011)[23] az intelligens textíliákkal kapcsolatban (fogalommeghatározás, osztályozás, alkalmazások, szabványosítással kapcsolatos igények), a szabványalkotáshoz elengedhetetlen az új technológia ismerete (nem csupán a gyártók, a bejelentett szervezetek számára, hanem a szabványügyi szervezetek számára is).

Az elsődleges feladat a szabványosítás kapcsán az egyéni védőeszközökkel szemben támasztott követelmények és vizsgálati eljárások megfogalmazása. Egyes esetekben a fogalmak definiálása is kihívást jelent. A gyártók mostanra felismerték, hogy az intelligens eszköz nem pusztán textília és elektronika ötvözése. A fejlesztés költséges, kockázatos befektetés, nem szükségszerű, hogy a kellő tanúsítványokat megkapja az eszköz. Felmerül tehát a kérdés, hogy az intelligens védőeszközök bevezetésének hasznossága pozitív irányba képes-e billenteni a mérleget megfelelőségtanúsítással kapcsolatos kihívások ellenében.

A felhasználókat érintő kihívások

Az intelligens védőeszközök használatát, mivel új képességekkel rendelkeznek, a felhasználóknak is el kell sajátítaniuk, azok működési módjával, funkcióival, a használhatóság korlátaival együtt. A hagyományos eszközökhöz hasonlóan az üzemeltetés, a felhasználás, a tisztítás és a karbantartás ugyanúgy feladata a munkavállalónak. Ehhez azonban ajánlásokra van szükség a gyártók által közzétett információkon keresztül. A tapasztalatok megosztása segíthetne a továbbfejlesztésben is, hiszen az elengedhetetlen az optimalizáláshoz.[24]

A munkavállalók intelligens eszközökkel szembeni kihívásai abból a tudáshiányból (is) fakadnak, amely a hagyományos eszközökkel szemben is megjelenik. Viselik, mert azt mondták, hogy kell, de a tudatosság hiányzik. Az intelligens eszközök bizonyos munkakörökben és képzettségi szinteken nem jelentenek többet, mint túlbonyolított, szükségtelen rossz (világító, hangjelzést adó jólláthatósági mellény, szenzorokkal ellátott védőruha, amely méri a pulzust stb.). A használhatóság és a tényleges viselet nem feltétlenül elvárható minden munkavállalótól, főként abban az esetben, ha sem a használatával nincs tisztában, sem azzal, hogy mire alkalmazható az adott eszköz. Az egyéni védőeszköz elfogadottságának mértéke annak is függvénye, hogy szükségét érzi-e a felhasználó az adott eszköznek vagy sem (a hagyományos védőeszközökkel

[23] Slovensky Standard SIST-TP CEN/TR 16298:2012.
[24] Thierbach 2020.

kapcsolatban is jellemző, hogy nem érzik szükségesnek a viselését – például több ezer négyzetméteres tetőszinten a sisak viselését irrelevánsnak tartják, hiszen ott nem eshet a fejükre semmi).

Amennyiben a munkavállalókban tudatosul, hogy bizonyos munkakörülmények esetén magasabb szintű védelem szükséges, nagyobb valószínűséggel fogják viselni az eszközöket. Ha nincsenek tisztában azzal, hogy az új funkciók közül melyikre van szükségük, nem lesz tudatos a gondolkodás a viseléssel kapcsolatban sem. Nem szabad figyelmen kívül hagyni, hogy egy védőeszköz nem nyújt magasabb védelmet akkor, ha az adott funkcióra a munkavállalónak nincs szüksége (és nem is fogadja el emiatt). A hasznosság mértéke mellett azt is célszerű tudatosítani a munkavállalókban, hogy a védőeszköz akkor sem nyújt 100%-os védelmet, ha intelligens, és számos különböző különleges tulajdonsággal fel van ruházva.

Az intelligens védőeszközökkel szemben támasztott követelmények

Talán az a legfontosabb, hogy a különleges tulajdonság minden esetben növelje az adott eszköz védelmi szintjét, a látszólag hasznos elemek használata kerülendő, mivel az hamis biztonságérzetet ad, és balesetveszélyes helyzetet eredményezhet. A megjelenített információk nem terhelhetik túl az eszköz viselőjét, ne legyen külön stresszfaktor, ha a kijelzőn azt látja, hogy valamiért egy pillanatra kiugróan magas volt a pulzusa. Elvonhatja a figyelmét a végzett tevékenységről, és akár balesethez is vezethet. A fölösleges jelzések után a tényleges jelzést pedig nem veszi figyelembe. A felhasználó dönthessen arról, hogy milyen adatokat kíván az eszközön megjeleníteni. A biometrikus/személyes adatokat a rendszer megfelelő biztonsággal kezelje, ne tárolja ezeket. A karbantartásra, tisztításra és alapvetően a felhasználásra vonatkozóan egyértelmű, valamennyi felhasználó számára jól értelmezhető legyen. Más esetben hibás használathoz vezethet, közvetve vagy közvetlenül balesetet okozhat. A vezeték nélküli kialakítás, veszélymentes energiaellátás és stabil kapcsolat kiemelten fontos az eszközök megfelelő és biztonságos használhatósága érdekében. Hasznosak lehetnek azok az információk, amelyek a használat utáni állapotra utalnak (például akkumulátor/energiaforrás állapota, tisztítási, karbantartási kötelezettség stb.). A megbízhatóság alapja az, hogy a használandó eszközöket üzemszerű körülmények között ki lehessen próbálni.

Összegzés

Napjainkra egyre nagyobb teret hódít az intelligens technológia a védőeszközök területén. A használatnak megkérdőjelezhetetlen előnyei vannak akkor, ha a felhasználó tisztában van ezekkel; ha elfogadják és akarják használni az eszközöket, megfelelő védelmet nyújtanak. A fejlesztések széles körűek, a védelmi szintekkel kapcsolatos igények adottak, az intelligens eszközök elterjedt alkalmazásának azonban számos akadálya van: jogszabályalkotás, szabványosítás, megfelelőségtanúsítás. Ezekhez azonban a technológia teljes körű ismerete szükséges mind a gyártó, mind a megfelelőséget

tanúsító szervezetek részéről. A munkavállalói tudatosság növelése elengedhetetlen része a folyamatnak. A felmerülő kérdések (költségoldalról rentábilis lehet-e az intelligens eszközök bevezetése, a fejlesztések nagy erőforrás-igényűek) jelen tudásunk szerint nem megválaszolhatók, ezzel kapcsolatban nem született még tanulmány.

Megállapítható, hogy ezek az eszközök jelentős mértékben hozzájárulhatnak a munkavállalók biztonságának növeléséhez, amennyiben a használatukkal kapcsolatos tudatosság és elfogadás megfelelő szintre emelkedik. Másrészt a szabályozási, jogszabályi és szabványosítási folyamatok hatékony megvalósítása elengedhetetlen ahhoz, hogy az intelligens védőeszközök széles körben elterjedjenek és alkalmazhatóvá váljanak.

A kutatás eredményeként az intelligens védőeszközökkel kapcsolatos technológiai fejlesztések és innovációk pontosabb és részletesebb megértésére számítunk. A tanulmányok révén olyan új módszereket és technikákat azonosíthatunk, amelyekkel csökkenthetők a munkavállalókat érő kockázatok. Továbbá várhatóan javulni fognak az intelligens eszközök szabványosításával és megfelelőségtanúsításával kapcsolatos folyamatok, ennek következtében a biztonsági szint növekedése mérhetővé válik.

A valós idejű adatok felhasználásával (amit az intelligens védőeszközök használata közben a különböző szenzorok biztosítanak) a munkafolyamatok hatékonyabbá válhatnak, a munkahelyi balesetek és sérülések száma jelentős mértékben csökkenthető. Az eredmények felhasználhatók a munkavállalói tudatosság növeléséhez, ami szükségszerűen magával hozza a hatékonyabb védőeszköz-használatot. A megfelelőségtanúsítás, a szabványosítás folyamatának fejlesztése nagyobb teret enged a biztonságos, rendeltetésszerű használatnak.

Felhasznált irodalom

Ammad, Syed et al. (2021): Personal Protective Equipment (PPE) usage in Construction Projects: A Systematic Review and Smart PLS Approach. *Ain Shams Engineering Journal,* 12(4), 3495–3507. Online: https://doi.org/10.1016/j.asej.2021.04.001

Antwi-Afari, Maxwell Fordjour et al. (2018). Wearable Insole Pressure System for Automated Detection and Classification of Awkward Working Postures in Construction Workers. *Automation in Construction,* 96, 433–441. Online: https://doi.org/10.1016/j.autcon.2018.10.004

Barro-Torres, Santiago et al. (2012). Real-Time Personal Protective Equipment Monitoring System. *Computer Communications,* 36(1), 42–50. Online: https://doi.org/10.1016/j.comcom.2012.01.005

Hegedűs Miklós (2021): Intelligens egyéni védőeszközök. A jövő, vagy az okos egyéni védőeszközök már a jelen? *Munkavédelmi Hírmondó,* 3(3–4), 38–43.

MSZ EN 388:2016+A1, Magyar szabvány – Védőkesztyűk mechanikai kockázatok ellen. 2019. október.

Nguyen, Luan V. et al. (2016): A Smart Shoe for Building a Real-Time 3D Map. *Automation in Construction,* 71, 2–12. Online: https://doi.org/10.1016/j.autcon.2016.03.001

Rasouli, Sina et al:. (2024): Smart Personal Protective Equipment (PPE) for Construction Safety: A Literature Review. *Safety Science,* 170, 106368. Online: https://doi.org/10.1016/j.ssci.2023.106368

Skrzetuska, Ewa – Rzeźniczak, Paulina (2025): Wearable Technologies for Health Monitoring: A Review of Applications. *Sensors Journal,* 25(6). Online: www.mdpi.com/1424-8220/25/6/1812

Thierbach, Michael (2020): *Smart Personal Protective Equipment: Intelligent Protection for the Future.* EU-OSHA. Online: https://osha.europa.eu/sites/default/files/Smart_personal_protective_equipment_intelligent_protection_of_the_future.pdf

Jogi források

65/1999. (XII. 22.) EüM rendelet a munkavállalók munkahelyen történő egyéni védőeszköz használatának minimális biztonsági és egészségvédelmi követelményeiről

Az Európai Parlament és a Tanács (EU) 2016/425 rendelete (2016. március 9.) az egyéni védőeszközökről és a 89/686/EGK tanácsi irányelv hatályon kívül helyezéséről (EGT-vonatkozású szöveg)

Slovensky Standard SIST-TP CEN/TR 16298:2012

HADMÉRNÖK
VÉDELEMINFORMATIKA

20. évfolyam (2025) 1. szám 19–48.
DOI: 10.32567/hm.2025.1.2

Bor Olivér[1]

Szabályozási szemléletváltás

A NIS2 hatása a magyar kiberbiztonsági szabályozásra

A Shift in Regulatory Approach

The Impact of NIS2 on Hungarian Cybersecurity Regulation

Absztrakt

A tanulmány a magyar kiberbiztonsági szabályozás fejlődését vizsgálja a 2013. évi L. törvény és a 2024. évi LXIX. törvény összehasonlításán keresztül, különös tekintettel az Európai Unió NIS2 irányelvének hatására. A kutatás bemutatja, miként alakult át a szabályozás szemlélete az állami elektronikus információbiztonság védelmét célzó megközelítéstől egy átfogóbb, kockázat- és incidenskezelésre épülő kiberbiztonsági ökoszisztéma irányába. Részletes elemzés tárja fel a jogszabályi szövegek strukturális, terminológiai és stratégiai változásait, rávilágítva arra, hogy a szabályozási környezet hogyan igazodott a digitalizációval járó fenyegetések gyors evolúciójához. A tanulmány rámutat, hogy a digitalizációval összefüggő új kihívások szükségessé tették a jogszabályok kibővítését és aktualizálását, ami technológiai, szervezeti és hatósági szinten egyaránt megfigyelhető. A kutatás eredményei azt hangsúlyozzák, hogy a modern kiberbiztonsági szabályozás nemcsak a technológiai védelmi intézkedésekre, hanem az ellenálló képesség növelésére, a kockázatalapú szemléletre és a nemzeti szintű koordináció megerősítésére is kiemelt figyelmet fordít, ezzel hozzájárulva az Európai Unió egységes kiberbiztonsági szintjének megteremtéséhez.

Kulcsszavak: kiberbiztonság, trendek, fenyegetések, NIS2, szabályozás

[1] Kiberbiztonsági és kommunikációs szakértő, okleveles kommunikációs és nemzetközi tanulmányok szakértő, e-mail: oliver.bor@protonmail.com

Abstract

The study examines the development of Hungarian cybersecurity regulation through a comparison of Act L of 2013 and Act LXIX of 2024, with particular attention to the impact of the European Union's NIS2 directive. The research presents how the regulatory approach evolved from a focus on the protection of state electronic information security towards a more comprehensive cybersecurity ecosystem based on risk management and incident handling. A detailed analysis reveals structural, terminological, and strategic changes in the legislative texts, highlighting how the regulatory environment has adapted to the rapid evolution of threats associated with digitalization. The study emphasizes that the new challenges related to digital transformation necessitated the expansion and updating of legislation, a trend observable at technological, organizational, and regulatory levels alike. The findings underline that modern cybersecurity regulation not only focuses on technological protective measures but also places significant emphasis on strengthening resilience, adopting a risk-based approach, and reinforcing national-level coordination, thereby contributing to the creation of a unified level of cybersecurity across the European Union.

Keywords: cybersecurity, trends, threats, NIS2, regulation

Bevezetés

„Kétféle cég létezik a világon: azok, amelyeket már meghackeltek, és azok, amelyeket meg fognak hackelni" – szól az információbiztonsági és kiberbiztonsági szakma által gyakran idézett mondat, amelyet a legtöbben Robert Muellernek, az FBI egykori igazgatójának tulajdonítanak 2012-ből. Valójában azonban Dmitri Alperovitch, a McAfee akkori vezető szakértője a Shady RAT elnevezésű jelentésében már 2011-ben megfogalmazta a mára híressé vált gondolatot: „Kétféle vállalat létezik: azok, amelyeket már feltörtek, és azok, amelyek még nem tudják, hogy feltörték őket." Ezzel gyakorlatilag a világ egyik vezető kiberbiztonsági cégének munkatársaként már 2011-ben világossá tette, hogy a kibertámadások szinte minden vállalatot érintenek, és a vállalatoknak folyamatosan készülniük kell az ilyen jellegű fenyegetésekre. 2012-ben Robert Mueller, az FBI akkori igazgatója egy San Franciscó-i kiberbiztonsági konferencián továbbfejlesztette ezt az üzenetet, amikor beszédében azt mondta: „Már nem az a kérdés, hogy megtörténik-e, hanem hogy mikor. Kétféle cég létezik a világon: azok, amelyeket már meghackeltek, és azok, amelyeket meg fognak hackelni." Ez a kijelentés egyértelműen jelezte, hogy a kibertámadások elkerülhetetlenek a modern digitális világban, és minden vállalat számára csak idő kérdése, hogy mikor válik támadás áldozatává. Mueller hangsúlyozta, hogy a vállalatoknak fel kell készülniük az újabb és újabb kibertámadásokra, mert ezek elkerülhetetlenek a digitális világban. Ha az idézet evolúcióját nézzük, akkor megkerülhetetlen a legújabb változatot is megemlíteni, amely 2015-ben John Chamberstől, a Cisco vezérigazgatójától hangzott el, aki ismét előhozta az idézetet egy beszédében: „Kétféle vállalat létezik: azok, amelyeket már feltörtek, és azok, amelyek még nem tudják, hogy feltörték őket." Beszédében Chambers a kiberbiztonság alapvető

fontosságát hangsúlyozta az üzleti életben, álláspontja szerint a kiberbiztonság már nélkülözhetetlen egy sikeresen működő cég mindennapi tevékenysége során.[2]

A fentieket különösen annak fényében érdemes vizsgálni, hogy az elmúlt években a digitalizáció és az innováció életünk megkerülhetetlen részévé vált, amely képességek nélkül egy szervezet, egy vállalat elveszítheti versenyképességét. A digitalizáció és a digitális transzformáció olyan átfogó folyamat, amely minden iparágra hatással van, és jóval túlmutat a termék- és folyamatfejlesztés határain. Érinti az üzleti modellek kialakítását, a szervezeti és irányítási elveket, valamint az ellátási lánc működését, komoly kihívások elé állítva ezzel a vállalatokat. Másképp fogalmazva: a digitális szolgáltatások és a digitalizáció nem csupán a fizikai termékekre gyakorolnak hatást, hanem alapvetően befolyásolják az üzleti működés természetét, a szervezeti struktúrát és a vállalati stratégiát is, így egy összetett kihívással állunk szemben.[3]

Ugyanakkor elengedhetetlen figyelmet fordítani a biztonsági szempontokra is. A digitalizáció kínálta lehetőségek akkor hozhatnak valódi előnyt a szervezetek számára, és akkor járulhatnak hozzá az ország gazdasági fejlődéséhez, ha a fejlesztések és az innovációk mellett megjelenik a megfelelő szintű, valós kockázatelemzést tükröző, a fenyegetésekre adekvát válaszokat nyújtó kiberbiztonsági felkészültség is. Az átfogó védelem hatékonyságát egy széles körű, kiterjedt biztonsági megközelítés szavatolhatja, amely magában foglalja a technológiai innovációkat, a jól definiált kiberbiztonsági szabályozás bevezetését és felügyeletét, a hatékony incidenskezelést, a proaktív védelmi rendszerek alkalmazását, valamint a következetes és rendszeres kiberbiztonsági tudatosság növelését is. Az elmúlt évek kibertámadási mintáinak elemzése rámutat, hogy a kiberbűnözők számára gyakran a felhasználók a legkedveltebb célpontok. A támadóknak ugyanis sok esetben könnyebb egy szervezet informatikai rendszerébe bejutni a felhasználók révén, így okozva károkat vagy végrehajtva egyéb jogsértő cselekményeket, minthogy közvetlenül a célként kijelölt rendszer technikai gyengeségeit aknázzák ki.[4]

Az Európai Unió az elmúlt években számos kezdeményezést indított annak érdekében, hogy szabályozási eszközökkel és minimális követelmények előírásával csökkentse a tagállamok és a szervezetek kiberbiztonsági kitettségét. A kiberbiztonsági politika fejlődése a digitális infrastruktúra jelentőségének felismerésével indult, amelynek első mérföldkövei a 2013-as kiberbiztonsági stratégia és a 2016-os NIS irányelv[5] voltak. Ezeket a 2017-es, majd a 2019-es intézkedések, például az Európai Uniós Kiberbiztonsági Ügynökség (a továbbiakban: ENISA) megerősítése és a tanúsítási keretrendszer bevezetése követték. A 2022-ben elfogadott NIS2[6] irányelv már átfogóbb megközelítést alkalmaz, amely a technológiai védekezés mellett a kockázatkezelést, az együttműködést, az ellenőrzést és a társadalmi tudatosság növelését is előírja. Az EU kiberbiztonsági szabályozása egyre inkább holisztikus szemléletet követ, amely technológiai, stratégiai és társadalmi szinten is az ellenálló képesség növelésére törekszik.

[2] Bejtlich 2018.
[3] Horváth–Szabó 2019.
[4] Bor 2024.
[5] Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről.
[6] Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve 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.

Kutatási célok és módszertan

A kutatás középpontjában a magyar kiberbiztonsági szabályozás fejlődésének vizsgálata áll, különös tekintettel a 2013. évi L. törvény[7] (Ibtv.) és a 2024. évi LXIX. törvény[8] (Kibertv.) összehasonlítására. A két jogszabály tartalmi és nyelvi elemzése – beleértve a szógyakorisági mintázatokat, bigramok és trigramok előfordulását, valamint a tematikus klaszterek változásait – azt a célt szolgálja, hogy feltárjuk, miként alakult át a szabályozás szemlélete, struktúrája és terminológiája az elmúlt évtizedben.

Kiemelt kutatási cél annak bemutatása, hogyan módosult a szabályozási fókusz a korábbi, elsősorban állami és önkormányzati elektronikus információs rendszerek védelmét célzó megközelítésről egy szélesebb spektrumot átfogó, incidenskezelésre, szolgáltatásfolytonosságra és tanúsításra épülő kiberbiztonsági ökoszisztéma irányába. A kutatás külön hangsúlyt fektet az EU NIS2 irányelvének hatására, amely alapvetően formálta a 2024. évi LXIX. törvény szemléletét és szerkezetét.

A vizsgálat során megfogalmazott kutatási kérdés így a következő: *Hogyan változott meg a magyar kiberbiztonsági szabályozás szemlélete és nyelvezete a 2013. és 2024. évi törvények tükrében, és milyen hatással volt minderre az Európai Unió NIS2 irányelve?* E kérdés lehetőséget teremt arra, hogy feltárjuk a jogalkotás mögött álló logikai és intézményi átrendeződéseket, a szabályozás mélyülését, valamint a fogalmi és tartalmi gazdagodást, amely egy modern, harmonizált, kockázatérzékeny kiberbiztonsági környezet kialakítását célozza.

A kutatás a 2013. évi L. törvény és a 2024. évi LXIX. törvény közötti szabályozási, tartalmi és nyelvi különbségek feltárására irányult, amelyhez kvantitatív és kvalitatív módszertani megközelítést egyaránt alkalmaztunk. A cél az volt, hogy feltérképezzük, miként tükröződnek a jogalkotási szemléletváltások a törvényi szövegek nyelvi szerkezetében, tematikus fókuszában és terminológiai változásaiban.

A vizsgálat első lépéseként szógyakoriság-elemzést végeztünk, amely a két törvényben leggyakrabban előforduló szavak statisztikai alapú összehasonlítását tette lehetővé. Ezáltal láthatóvá váltak a szabályozási fókusz eltolódásai: például a „kiberbiztonság", „hatóság" vagy „tanúsítás" szavak ugrásszerű növekedése a 2024-es törvényben azt jelezte, hogy a szabályozás technológiai, szervezeti és hatósági szempontból is mélyebbé és részletesebbé vált.

A szógyakoriság mellett n-gram-elemzést is alkalmaztunk – különösen bigramok és trigramok formájában –, amely a gyakran együtt előforduló szókapcsolatokat azonosította. Ez a módszer segített az intézményi és tematikus összefüggések megértésében, például olyan kulcsfontosságú szerkezetek révén, mint a „kiberbiztonsági hatóság" vagy az „incidenskezelő központ".

A kvantitatív módszertani blokk zárásaként klaszterelemzést végeztünk, amely a szóhasználati minták alapján tematikus klasztereket hozott létre. Ez tette lehetővé annak mélyebb megértését, hogy a 2013-as törvény szövege az infrastruktúra és a rendszerbiztonság köré, míg a 2024-es törvény az állami hatósági szerepvállalás, incidenskezelés, kockázatelemzés és auditálás témái köré szerveződik.

[7] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról.
[8] 2024. évi LXIX. törvény Magyarország kiberbiztonságáról.

A kvantitatív adatok értelmezését kvalitatív elemzéssel egészítettük ki, amely a kulcsfogalmak jelentéstartalmának, a szabályozási logikák eltolódásának és a szemléletváltás mögötti narratíváknak az értelmezésére összpontosított. Ehhez nemcsak a két törvény teljes szövegét elemeztük, hanem kiegészítő dokumentumokat is bevontunk: összehasonlító jelentéseket, kulcsszavas összefoglalókat, új fogalmak listáit és klaszterelemzési eredményeket.

A szövegek feldolgozása során előfeldolgozási lépéseket végeztünk: eltávolítottuk az úgynevezett *stop-wordöket* (például kötőszók, névelők, jogszabályi struktúrára vonatkozó szavak stb.), és létrehoztuk a magyar nyelvi sajátosságokat figyelembe vevő egyedi *stop-word* listát, amely lehetővé tette a finomabb klaszterezést és a pontosabb n-gram-modellezést. Ezzel párhuzamosan kulcsszavakat kategorizáltunk, összevetve azok megjelenését, jelentését és kontextusát az egyes évek törvényeiben.

A kvantitatív és kvalitatív módszerek együttes alkalmazása révén lehetőség nyílt arra, hogy a szövegek mögött meghúzódó szabályozáspolitikai és szemléleti változások is értelmezhetővé váljanak. Ez nemcsak a nyelvi struktúrák, hanem az intézményi és stratégiai irányváltások értelmezéséhez is hozzájárult, így a kutatás túlmutatott a szimpla jogszabályi szöveg-összehasonlításon, és hozzájárult a kiberbiztonsági szabályozás fejlődési ívének mélyebb megértéséhez. A módszertani kombináció révén lehetőség nyílt arra, hogy a törvényi szövegek nyelvi struktúrája mögött rejlő szabályozáspolitikai szemléletváltás is értelmezhetővé váljon, és a változások ne csak számszerűen, hanem tartalmilag is értékelhetők legyenek.

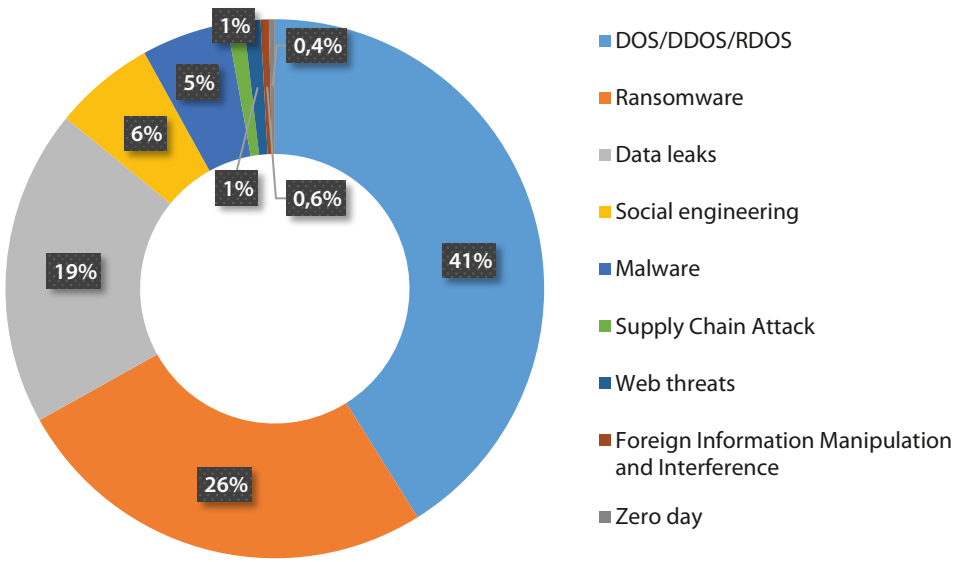
Kiberbiztonsági trendek

A vizsgált hazai szabályozási változások megértéséhez nem elegendő kizárólag a jogszabályi szövegek belső logikájára és szerkezetére koncentrálni. A kiberbiztonsági törvények alakulását alapvetően meghatározta az a fenyegetettségi környezet, amelyre válaszul születtek: a támadások jellege, technikai kivitelezése, célpontjai és azok gyors ütemű változása. A szabályozás fókuszváltása – például az incidenskezelés, a szolgáltatásfolytonosság vagy a kritikus infrastruktúrák védelmének megerősítése – közvetlen összefüggésben áll a kiberfenyegetések fejlődő metodikáival. Ezért a továbbiakban áttekintjük azokat a főbb kiberbiztonsági trendeket, amelyek az elmúlt évtizedben alakították a fenyegetettségi térképet, és amelyek lényeges befolyást gyakoroltak a magyar jogalkotás irányváltására is.

A digitális átalakulás gyors üteme és az új technológiák fejlődése, valamint a kibertámadások növekvő kifinomultsága oda vezet, hogy a szervezetek folyamatosan egyre nagyobb volumenű és súlyosabb kiberbiztonsági fenyegetésekkel találkoznak. Ezek alapján érdemes megvizsgálni az ENISA 2024-es kiberbiztonsági fenyegetettségi jelentését,[9] amely átfogó képet ad az Európai Unióban megfigyelt főbb támadási formákról és azok előző évhez viszonyított változásairól. A jelentés szerint a legkiemelkedőbb fenyegetések továbbra is a szolgáltatásmegtagadással járó támadások (*distributed denial-of-service,* más néven DDoS) és a zsarolóvírusok *(ransomware)* voltak.

[9] Lella et al. 2024.

A zsarolóvírusok ugyan még stabilan magas számban fordulnak elő, ám egyre inkább megfigyelhető, hogy a támadók többfokozatú, úgynevezett „kettős zsarolás" taktikát alkalmaznak, amely az áldozatok ismételt fenyegetésére vagy különböző célokra történő adatfelhasználásra irányul. (A támadástípusok szerinti incidensmegosztást az 1. ábra mutatja be részletesen.) A támadások gyakorisága és mérete – Európa-szerte – jelentősen megnőtt: az előző, 2023-as évhez képest 85%-os növekedést mutat. Ezek a támadások egyre komplexebbek, és gyakran más támadások „füstfüggönyeként" szolgálnak, ami azt a célt szolgálja, hogy a kiberbűnözők eltereljék a biztonsági csapatok figyelmét más, párhuzamosan zajló, komolyabb támadásokról.



1. ábra: Az elemzett incidensek fenyegetéstípus szerinti bontása (2023. júliustól 2024. júniusig)
Forrás: a szerző szerkesztése Lella et al. 2024 alapján

Az előző évhez képest a mesterséges intelligenciát (AI) alkalmazó eszközök használatában változás figyelhető meg: a támadók egyre gyakrabban használják a mesterséges intelligenciát különféle adathalász-e-mailek vagy káros szoftverek létrehozására. Az olyan AI-eszközök, mint például a FraudGPT,[10] lehetővé teszik a támadók számára azt is, hogy gyorsan és hatékonyan hozzanak létre célzott támadásokat.

A *fake news* és a különféle információmanipulációs technikák szintén jelentős szerepet töltenek be a kibertérben, különösen az orosz–ukrán konfliktus kontextusában, ahol dezinformációs kampányok és egyéb információs támadások figyelhetők meg. A jelentés megemlíti, hogy a hacktivista csoportok egyre gyakrabban kerülnek

[10] A FraudGPT egy mesterséges intelligencián alapuló eszköz, amelyet kifejezetten kiberbűnözési célokra hoztak létre. Lehetővé teszi a támadók számára, hogy automatikusan generáljanak adathalász-e-maileket, rosszindulatú programokat és más, csalárd tevékenységekhez szükséges tartalmakat. Gyorsasága és kifinomultsága miatt a kiberbűnözés új dimenzióját képviseli.

kapcsolatba állami háttérrel rendelkező támadókkal vagy akár közvetlenül egy-egy állammal, így ezek az incidensek még inkább átláthatatlanok és bonyolultak.

Összességében az ENISA jelentése szerint az EU-ban a kiberfenyegetések folyamatosan fejlődnek, és az új technológiák, mint a mesterséges intelligencia és a felhőalapú szolgáltatások, egyszerre nyújtanak lehetőséget a támadók számára és jelentenek kihívást a biztonsági és védelmi szakemberek számára. Az előző évhez képest növekvő tendenciák és új fenyegetettségek felhívják a figyelmet arra, hogy a kiberbiztonság erősítése, az adatvédelem és a tudatosság növelése kiemelten fontos az Európai Unió számára.

Ahogyan a mondás tartja, minden lánc olyan erős, mint a leggyengébb láncszeme – a kiber- és információbiztonság területén pedig ez a leggyengébb láncszem gyakran maga az ember. A PurpleSec 2024-es kiberbiztonsági riportjának adatai szerint[11] a kibertámadások 98%-a valamilyen *social engineering* technikát alkalmaz, ami kiemeli az emberi tényező központi szerepét a kiberbiztonság fenyegetései között. A *social engineering*, vagyis a pszichológiai manipuláció olyan módszerek és technikák összessége, amelyek az emberi hibák vagy viselkedésminták kihasználásával célozzák meg a felhasználók bizalmas információinak megszerzését. A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet egy, a 2023-as évre vonatkozó jelentése alapján[12] a *social engineering* technikák továbbra is a legelterjedtebb támadási formák közé tartoznak, különösen az adathalászat terén, ahol az e-mail, az SMS és a telefonos megkeresések kombinációja új szintre emelte a fenyegetettséget.

A *social engineering* támadások azért is különösen veszélyesek, mert gyakran rejtve maradnak: az áldozatok sok esetben nem is tudják, hogy támadás érte őket, de sok esetben azért hallgatnak a történtekről, mert attól tartanak, hogy hibáik negatív következményekkel járhatnak. Ez a láthatatlanság jelentősen megnehezíti a pontos statisztikai elemzések készítését, és a védekezést is korlátozza.

A *social engineering* támadások központi eleme az emberi sebezhetőség, amely számos módon kihasználható. Az alkalmazottak közvetlenül hozzáférnek a szervezetek védett eszközeihez és adataihoz, így különösen értékes célpontokká válnak. Például ők telepítik és frissítik (vagy mulasztják el frissíteni) a szükséges szoftvereket, szállítanak és kezelnek hardvereszközöket, valamint hozzáférnek belső fájlokhoz, rendszerekhez és adatokhoz. Ezen túlmenően olyan belső információk birtokában vannak, amelyek értékesek lehetnek a támadók számára. Az emberi tulajdonságok, mint például a segítőkészség, a bizalom és az információhiány, különösen kihasználhatóvá teszik őket, főleg, ha nem részesülnek megfelelő képzésben és tudatosításban.[13]

Az adathalászat a *social engineering* legelterjedtebb formája, amely különféle technikákat foglal magában. Az e-mailes adathalászat során a támadók hivatalosnak tűnő üzenetekkel próbálják meg rávenni az áldozatokat arra, hogy érzékeny adatokat, például jelszavakat vagy bankkártyaadatokat adjanak meg. Az SMS-alapú adathalászat hasonló elven működik, és gyakran csomagátvételi értesítésekkel vagy előfizetés-megújítási figyelmeztetésekkel álcázzák magukat a támadók. A telefonos adathalászat

[11] PurpleSec [é. n.].
[12] Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet 2024.
[13] Oroszi 2023.

pedig közvetlen emberi interakcióra épít, ahol a támadók pszichológiai nyomást alkalmaznak, hogy érzékeny információk kiadására bírják az áldozatokat. Mindegyik adathalászmódszerben közös, hogy az emberi sebezhetőségre épít, és a támadók hivatalosnak tűnő kommunikációt alkalmaznak, például bankok, közműszolgáltatók vagy egyéb szervezetek nevében keresik meg a leendő áldozatokat, továbbá éles helyzetet felvázolva, sürgető hangnemet alkalmazva késztetik arra a másik felet, hogy érzékeny adatokat adjon meg valamilyen módon.[14]

Az utóbbi években a mesterséges intelligencia és a *deepfake* technológiák megjelenése új szintre emelte a *social engineering* támadásokat. Az ENISA jelentése rámutat, hogy az AI által generált adathalász-e-mailek már szinte hibátlan nyelvezetet és formázást alkalmaznak, ami megnehezíti azok felismerését. A hangklónozás és a *deepfake* videók alkalmazása pedig lehetővé teszi, hogy a támadók akár valós idejű videóhívások során is manipulálják az áldozatokat. Noha ezek a technológiák a 2020-as évek elején még gyerekcipőben jártak, gyors fejlődésük manapság jelentős kiberbiztonsági kockázatokat hordoz.[15]

A *social engineering* támadások elleni védekezés elsődleges eszköze a munkavállalók képzése és tudatosítása. Az Európai Unió NIS2 irányelve hangsúlyozza, hogy a szervezeteknek kiemelt figyelmet kell fordítaniuk az alkalmazottak oktatására, különös tekintettel az adathalászat felismerésére és elkerülésére. Ezen túlmenően a technológiai védelmi megoldások, például a multifaktoros hitelesítés, a biztonsági szűrők és az adathalászatot szűrő rendszerek bevezetése jelentősen csökkentheti a támadások sikerességét.

Az EU kiberbiztonsági politikájának rövid áttekintése, különös tekintettel a NIS2-re

Az Európai Unió kibervédelmi szakpolitikájának fejlődése az elmúlt két évtizedben jól nyomon követhető az uniós stratégiai dokumentumokon, rendeleteken és irányelveken keresztül. Az alapok már a 2000-es évek elején, röviden és csekély mértékben ugyan, de kirajzolódtak, amikor az illetékesek felismerték, hogy a digitális infrastruktúra biztonsága a gazdaság és a társadalom versenyképességének alapvető eleme. Az első releváns dokumentum, a 2003-as európai biztonsági stratégia, amelynek végrehajtásáról szóló dokumentum[16] is még csak áttételesen említi a kiberbiztonságot, főként a terrorizmus kontextusában.[17]

A 2005-ös *i2010: Európai Információs Társadalom a növekedésért és foglalkoztatásért*[18] elnevezésű stratégiai dokumentum már konkrétabban foglalkozik az információs társadalom biztonságával, a digitális gazdaság fejlesztésével, az IKT szerepének erősítésével, és felveti egy átfogó biztonsági stratégia szükségességét. A 2003-ban

[14] Nemzeti Kibervédelmi Intézet 2023.
[15] Veszelszki 2023.
[16] Az Európai Unió Tanácsa 2009.
[17] Molnár 2019.
[18] A Bizottság közleménye a Tanácsnak, az Európai Parlamentnek, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának – „i2010: európai információs társadalom a növekedésért és a foglalkoztatásért".

elfogadott európai biztonsági stratégia 2008-as módosítása már külön szakaszban foglalkozott az informatikai biztonság alapvető vonatkozásaival. Az átdolgozott változat kiemeli, hogy a korszerű gazdaságok működése szoros kapcsolatban áll az alapvető infrastruktúrák – többek között az internet – zavartalan működésével. A dokumentum arra is rámutat, hogy az interneten keresztül elkövetett bűncselekmények kérdését már tárgyalta a 2006-ban elfogadott, az európai információs társadalom biztonságát célzó stratégia.[19]

Az EU 2010-es belső biztonsági stratégiája[20] már kiemeltebben foglalkozott a számítástechnikai bűnözés jelentette veszélyekkel. Ugyanebben az évben indult az Európa 2020 stratégia, amely a versenyképesség fokozása mellett – többek között – már a digitális sérülékenységek csökkentését is célul tűzte ki. Ennek részeként született meg az európai digitális menetrend,[21] amely az IKT-központú fejlődést helyezte előtérbe, valamint ráirányította a fókuszt a kiberbűnözés gyors ütemű terjedésére. Az Európai Bizottság és a tagállamok döntéshozói számára hamar nyilvánvalóvá vált, hogy a kitűzött célok csak akkor érhetők el teljes mértékben, ha biztosított a kibertér védelme.[22]

A 2010-es évek elején az EU felismerte, hogy noha a meglévő szabályozások előrelépést jelentettek, nem biztosítanak átfogó védelmet, mivel a tagállamok felkészültsége jelentős különbségeket mutat. Ennek orvoslására az Unió célul tűzte ki egy egységes kiberbiztonsági politika megalkotását, amely erősíti a bűnüldözést, ösztönzi a nemzetközi együttműködést, és közös szabályozási, fogalmi, intézményi alapokat hoz létre. Ennek kiindulópontját képezte az EU első kiberbiztonsági stratégiája, amelyet 2013-ban fogadtak el *Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér* címmel.[23] A dokumentum kulcspontjai között említhető a kibertér biztonságának uniós szintű biztosítása, a kritikus infrastruktúrák védelme, a kibertámadások elleni védekezés, valamint az alapjogok – különösen a magánszféra védelmének – megerősítése a digitális térben. A stratégia öt prioritása között szerepel az ellenálló képesség növelése, a kiberbűnözés visszaszorítása, a közös védelempolitikai képességek fejlesztése, valamint a nemzetközi együttműködés elmélyítése. Intézményi szinten a stratégia meghatározta az Európai Bizottság, az ENISA és az Európai Külügyi Szolgálat szerepét is.[24]

A stratégia eredményeként – hároméves jogalkotási folyamat végén – született meg az első uniós szintű, kötelező kiberbiztonsági politika, a 2016-os NIS irányelv.[25] Az irányelv célja, hogy egységes biztonsági szintet biztosítson a hálózati és információs rendszerek védelmében, kiemelten az alapvető szolgáltatásokat nyújtó szektorokra (például energia, vízellátás, közlekedés, egészségügy). Az irányelv kötelezővé tette a nemzeti szintű kiberstratégiák kidolgozását, a CSIRT-ek[26] létrehozását, valamint a tagállami együttműködést biztosító szervek – például az Együttműködési

[19] Jelentés az Európai Biztonsági Stratégia végrehajtásáról. A biztonság megteremtése a változó világban.
[20] Az Európai Unió Tanácsa 2010.
[21] Európai Bizottság, Európai Digitális Menetrend 2010.
[22] Kovács 2018.
[23] Közös közlemény az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának. Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér.
[24] Kovács 2018.
[25] Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve.
[26] CSIRT: Computer Security Incident Response Team (számítógépes biztonsági eseményelhárítási csoport).

Csoport – részvételét. Az irányelv jelentőségét az adta, hogy ez volt az első átfogó, uniós szintű kiberbiztonsági jogszabály, amely kötelező előírásokat és minimum biztonsági követelményeket határozott meg tíz, különösen fontos ágazat számára.[27]

2017 szeptemberében az Európai Bizottság a NIS irányelv végrehajtásával párhuzamosan kiadta a 2017/1584. számú ajánlást[28] a nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt uniós reagálásról. Az ajánlás az EU-n belüli kiberbiztonsági együttműködés megerősítésére törekszik, mivel a NIS irányelv nem szabályozta a válságkezelés kereteit. Az ajánlás úttörő jelentőségű volt, hiszen először határozta meg uniós szinten, mit tekintünk kiberbiztonsági eseménynek. A definíció egy olyan, gyorsan terjedő, előre nem látható válsághelyzetet ír le, amely nem korlátozódik egy adott területre, és jelentős fennakadásokat okozhat az uniós gazdaságban, társadalomban és a demokratikus működést biztosító digitális infrastruktúrában. Mindezek mellett az ajánlás kiemeli a tagállami felelősség elsődlegességét, ugyanakkor szükség esetén uniós szintű politikai koordinációt is előír. A válságkezelésben a CSIRT-hálózat, az ENISA és más uniós szervek közreműködése kulcsfontosságú, míg a stratégiai iránymutatást a NIS irányelv alapján létrejött Együttműködési Csoport biztosítja. Az ajánlás hangsúlyozza a kockázatmenedzsment, a rendszeres kiberbiztonsági gyakorlatok és egy uniós válságreagálási keret kialakításának fontosságát.[29]

A 2013-as stratégia célkitűzéseinek részleges teljesülése és az új típusú fenyegetések – például a WannaCry[30] vagy a NotPetya[31] támadások – szükségessé tették a stratégia felülvizsgálatát. Az EU *Ellenálló képesség, elrettentés, védelem*[32] című 2017-es közleménye új eszközöket javasolt, mint például az ENISA megerősítése, gyorsreagálási protokollok kidolgozása. A kibertámadásokkal szembeni védekező képesség erősítése érdekében elengedhetetlennek mutatkozott a NIS irányelv teljes körű, határidőre történő tagállami végrehajtása. A bizottság útmutatással és bevált gyakorlatok megosztásával segíti ezt a folyamatot, különös figyelemmel az alapvető szolgáltatásokra. Kiemelt cél a köz- és magánszféra közötti bizalom és információcsere elmélyítése.[33]

A 2017-es stratégia kapcsán érdemes kiemelni az ENISA szerepének megerősítését, a digitális termékek és szolgáltatások védelmét támogató, önkéntes uniós tanúsítási rendszer kialakítását, valamint egy olyan terv kidolgozását is, amely lehetővé teszi a gyors és összehangolt reagálást nagyszabású kiberbiztonsági események és válsághelyzetek esetén. A 2017. szeptember 13-án bemutatott kiberbiztonsági csomag részeként elkezdődött a kiberbiztonsági rendelet megalkotása, amely a digitális egységes piac stratégiai célkitűzései közé tartozott. Az Európai Bizottság 2018 szeptemberében javaslatot tett egy európai kiberbiztonsági kompetenciaközpont

[27] Tikos 2019.
[28] A Bizottság 2017/1584 ajánlása.
[29] Bonnyai 2019.
[30] WannaCry: egy 2017 májusában felbukkant zsarolóvírus, amely közel 250 000 számítógépet fertőzött meg világszerte, összesen 99 országban és 28 nyelven hozott létre zsarolóoldalakat.
[31] NotPetya: egy 2017 júniusában felbukkant zsarolóvírus, amelyet főleg ukrán állami szervezetek, bankok és az energiaszektor ellen vetettek be.
[32] Közös közlemény az Európai Parlamentnek és a Tanácsnak: *Ellenálló képesség, elrettentés, védelem: az Unió erőteljes kiberbiztonságának kiépítése.*
[33] Krasznay 2022.

és annak hálózatának létrehozására, valamint a kutatásra és innovációra szánt források hatékonyabb felhasználása érdekében. A kiberbiztonsági rendelet javaslata többek között az ENISA megbízatásának állandósítását, erőforrásainak bővítését, valamint a tagállamok támogatását célozza a kibertámadások elleni fellépésben. Cél volt, hogy a 2005 óta működő ENISA hatékonyabban támogassa a tagállamok kapacitásépítését, a tudatosság növelését, valamint az uniós intézmények és tagállamok szakpolitikai munkáját. A rendelet további célja volt egy uniós szintű tanúsítási keret létrehozása, amely javítja a hálózatra kapcsolt eszközök, a kritikus infrastruktúrák és a dolgok internetéhez kapcsolt eszközök biztonságát, akár már a fejlesztések korai szakaszában is.[34]

Az eddigi jogszabályi keretrendszer 2019-ben egy összetett jogi aktussal vált teljessé: a 2019. április 9-én elfogadott rendelettel, amely az ENISA-ról és az információs és a kommunikációs technológiák kiberbiztonsági tanúsításáról szólt, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről.[35] A rendelet egy uniós szintű kiberbiztonsági tanúsítási keretrendszert vezetett be, amely lehetővé teszi a hálózathoz csatlakozó eszközök tanúsítását[36] az EU egész területén. Ez elősegíti a fogyasztói bizalom növekedését, valamint megkönnyíti a vállalkozások számára az innovatív termékek forgalmazását. A tanúsítási rendszerek három megbízhatósági szinten működnek, és habár jellemzően önkéntesek, egységes szabályozási keretet teremtenek az IKT-termékek és -szolgáltatások számára. A rendelet emellett jelentősen megerősíti az Európai Hálózat- és Információbiztonsági Ügynökség szerepét, amely ettől kezdve állandó uniós kiberbiztonsági ügynökséggé vált. Az Ügynökség központi szerepet kapott a tanúsítási rendszerek kidolgozásában, a tagállamokkal és az uniós intézményekkel való együttműködésben, valamint a kiberbiztonsági gyakorlatok szervezésében. Az ENISA ezáltal nemcsak szakmai támogatást nyújt, hanem a kiberbiztonsági politika végrehajtásának egyik fő koordinátorává is vált az Európai Unión belül. (Fontos megemlíteni, hogy az ENISA már a 2016-os, a hálózati és információs rendszerek biztonságáról szóló NIS irányelv végrehajtásában is központi szerepet kapott mint a tagállami intézkedések támogatásának fő uniós szereplője.)[37]

„Ez az a pont, ahol ki kell hangsúlyozni, hogy az EU kezdeti törekvései (2009–2015) az információbiztonságot kifejezetten a kibertámadások szemszögéből közelítették meg. A legtöbb dokumentum preambuluma azokkal az eseményekkel támasztotta alá az intézkedések szigorításának, vagy következetesebbé tételének szükségességét, amelyek kibertámadásokként kerültek a köztudatba. 2016 után – már a NIS irányelvben – azonban változott ez a szinte kizárólagosnak tűnő trend, és egyre nagyobb figyelmet kapnak a technológiai, illetve humán erőforrás eredetű kockázatok, így azok kezelésének igénye is. A kiberbiztonsági jogszabály által megteremtett, a kiberbiztonsági tanúsítási keretrendszer is kifejezetten ezt a célt szolgálja."[38]

[34] Molnár 2019.
[35] Az Európai Parlament és a Tanács (EU) 2019/881 rendelete.
[36] A tanúsítás igazolja, hogy az eszköz megfelel a meghatározott kiberbiztonsági követelményeknek, növeli a felhasználói bizalmat, és elősegíti a piacra jutást.
[37] Az Európai Unió Tanácsa 2018.
[38] Bonnyai 2019: 70.

A 2019 májusában az Európai Unió Tanácsa által kiadott, az Uniót vagy annak tagállamait fenyegető kibertámadások elleni korlátozó intézkedésekről szóló rendelet[39] célzott korlátozó intézkedések bevezetését teszi lehetővé az EU-t vagy tagállamait érintő, jelentős hatású kibertámadásokkal szemben, különösen akkor, ha azok külső, nem uniós szereplőktől származnak. A rendelet meghatározza, mit ért az EU kibertámadás alatt, és különösen veszélyesnek minősíti azokat az eseteket – többek között –, amelyek kritikus infrastruktúrát, alapvető szolgáltatásokat nyújtó szervezetek, kritikus állami funkciókat vagy uniós intézményeket érintenek. Meghatározza továbbá azon tényezőket, amelyek alapján egy kibertámadás jelentős hatásúnak minősíthető (az előidézett zavar hatóköre, súlyossága, EU-s országok érintettsége stb.). A tagállamok feladata a szankciók végrehajtása, amelyek között beutazási tilalom és vagyonbefagyasztás is szerepelhet.

A rendeletben foglalt meghatározások – különösen a kibertámadás fogalma és annak lehetséges célpontjai, mint a kritikus infrastruktúrák és alapvető szolgáltatásokat nyújtó szervezetek – kulcsszerepet játszanak az Európai Unió kiberbiztonsági szemléletének átalakulásában. E fogalmak nemcsak a szankciópolitika keretében váltak meghatározóvá, hanem a megelőzés és az ellenálló képesség fejlesztése terén is új irányt szabtak. E szemléletváltás nyomán született meg a NIS2 irányelv, amely már nemcsak a fenyegetésekre adott válaszokra, hanem az átfogó kockázatkezelésre, a kritikus szereplők védelmére és az egységes, erősített kiberbiztonsági szabályozásra is hangsúlyt helyez.[40]

Az online tér komplexitása, a gyorsan változó fenyegetési környezet, valamint a globális összekapcsoltság miatt a kiberbiztonság immár nem izolált kérdés, hanem az információs hadviselés, a geopolitikai konfliktusok és a nemzetbiztonsági stratégiák szerves része.[41] Az Európai Unió NIS2 irányelve, amely kiberbiztonsági tudatosságra és felelősségvállalásra ösztönzi a tagállamokat és az érintett szereplőket, ebben az összefüggésben alapvető keretet biztosít, de nem elegendő az egyre kifinomultabb fenyegetésekkel szemben.

Az előzőleg részletezett kockázatok, különösen az aktuális kiberbiztonsági trendek és a társadalmak polarizálása egyértelművé teszik, hogy a digitális világban tapasztalható kihívások mindennapjaink meghatározó elemeivé váltak. Ezek a fenyegetések megkövetelik, hogy az egyének, a vállalatok és az állami szereplők egységes válaszokat adjanak, amelyek technológiai, stratégiai és társadalmi szinten is megállják a helyüket.

Tehát ezen fenyegetésekre válaszul született meg az Európai Unió egyik legfontosabb kiberbiztonsági jogforrása, a NIS2 irányelv. A szabályozás kiemelt jelentőségét az adja, hogy nem pusztán technológiai megoldásokat céloz meg, hanem a társadalmi tudatosságot is alapvető elemmé teszi a kiberbiztonság erősítése érdekében. Ez különösen fontos a közösségi média által nyújtott lehetőségek és veszélyek tükrében, hiszen ezek a platformok egyszerre szolgálnak a tudatosítás eszközeként és a kockázatok forrásaként. A dezinformációval és a manipulációval szembeni ellenálló képesség megteremtéséhez nem elegendők a technikai intézkedések; szükség van

[39] A Tanács (EU) 2019/796 rendelete.
[40] Vandezande 2024.
[41] Farkas–Kelemen 2023.

a felhasználók képzésére, a szervezetek kiberbiztonsági felkészültségének növelésére és a fenyegetések gyors felismerésére. Ebben a kontextusban kulcsfontosságú, hogy a szabályozások és az azokból fakadó intézkedések segítségével növekedjen az egyének és a szervezetek ellenálló képessége. Az ilyen intézkedések egyaránt szolgálják az egyéni és a kollektív biztonságot, miközben hozzájárulnak egy fenntarthatóbb és ellenállóbb digitális ökoszisztéma kialakításához. A kiberbiztonság jövőjének megteremtése érdekében elengedhetetlen, hogy a tudatosítás és a védekezési képességek fejlesztése a társadalmi és gazdasági stabilitás megőrzésének középpontjában álljon.

Az Európai Unió 2022/2555 számú irányelve, közismert nevén a NIS2 irányelv, a hálózati és információs rendszerek kiberbiztonságára vonatkozó átfogó szabályozási keretet határoz meg. Célja, hogy az EU tagállamaiban egységesen magas szintű kiberbiztonságot biztosítson, miközben a tagállamok számára kötelezővé teszi a kiberbiztonsági képességek fejlesztését, a kockázatkezelési mechanizmusok bevezetését, valamint a jelentéstételi kötelezettségek teljesítését. Az irányelv kiterjedt együttműködési keretet hoz létre a tagállamok és az Európai Unió különböző intézményei között, ezzel elősegítve a hatékony információcserét és a kockázatelemzésen alapuló operatív válaszadást a kiberfenyegetésekre.[42]

Az irányelv fő fókuszában a kritikus infrastruktúrák és azon ágazatokban működő szervezetek állnak, amelyek kiemelt szerepet játszanak az európai társadalom és gazdaság működésében. Az I. melléklet alapján a NIS2 szabályai az energia-, a közlekedési, az egészségügyi és a digitális infrastruktúrára, a közigazgatásra vagy a világűrre is kiterjednek. A II. melléklet további ágazatokat határoz meg, például a posta- és futárszolgálatokat, az élelmiszer-termelés, -feldolgozást és -forgalmazást, a gyártást, a digitális szolgáltatókat, valamint a kutatóhelyek kiberbiztonsági védelmét. További fontos kitétel, hogy az irányelvet azon, az I. vagy a II. mellékletben szereplő állami és magánszervezetekre kell alkalmazni, amelyek középvállalkozásnak minősülnek, vagy ennél nagyobb méretűek a 2003/361/EK[43] ajánlás alapján, és az Európai Unión belül nyújtanak szolgáltatásokat vagy végeznek tevékenységeket. Szükséges megemlíteni, hogy az irányelv hatálya bizonyos esetekben a szervezetek méretétől függetlenül is érvényes, többek között nyilvános elektronikus hírközlő hálózatok szolgáltatói vagy nyilvánosan elérhető elektronikus hírközlési, bizalmi szolgáltatók, legfelső szintű doménnév-nyilvántartók és doménnévrendszer-szolgáltatók, vagy az egyetlen szolgáltató egy tagállamban olyan szolgáltatás esetében, amely elengedhetetlen kritikus társadalmi vagy gazdasági tevékenységek fenntartásához.

Az irányelv I. és II. mellékletében szereplő ágazatokban működő szervezetekről, valamint a doménnév-nyilvántartási szolgáltatásokat biztosító szervezetekről minden tagállamnak nyilvántartást kell vezetnie, amit első körben 2025. április 17-ig szükséges megvalósítani és ezt a listát az Európai Unió kijelölt szervei számára megküldeni, majd a meghatározott határidőt követően rendszeresen, de legalább kétévente felül kell vizsgálni ezen nyilvántartást, és szükség esetén aktualizálni.

Az irányelv értelmében minden tagállamnak nemzeti kiberbiztonsági stratégiát kell kialakítania, amely átfogóan szabályozza a releváns érintettek felelősségi köreit,

[42] Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve.
[43] Az EU Bizottságának ajánlása – a mikro-, kis- és középvállalkozások meghatározása; Melléklet, I. cím, 2. cikk.

a sérülékenységek kezelését, valamint az ellátási láncok biztonságát. E stratégia szerves része a polgárok és a szervezetek kiberbiztonsági tudatosságának növelése, valamint az oktatás és a képzés fejlesztése. Az irányelv célja, hogy a tagállamok a technológiai innováció és a fenyegetésekre való reagálás szintjén egyaránt egységes kiberbiztonsági keretrendszert valósítsanak meg.

A számítógép-biztonsági eseményekre reagáló csoportok központi szerepet töltenek be a kiberbiztonsági események kezelésében. Az irányelv előírja, hogy a CSIRT-ek biztosítsák a kiberfenyegetések és sérülékenységek valós idejű nyomon követését, valamint a riasztások és előrejelzések közel valós időben történő kiadását. Emellett technikai segítséget nyújtanak a hálózati rendszerek proaktív vizsgálatával és a sérülékenységek azonosításával. A nemzeti CSIRT-ek között létrejött hálózat elősegíti a tagállamok közötti gyors információcserét és az operatív szintű együttműködést. Az ENISA, az EU kiberbiztonsági ügynöksége európai szintű sérülékenység-adatbázist hoz létre, amely biztosítja a kiberbiztonsági események közös értelmezését és a sérülékenységek nyilvános közzétételét.

A stratégiai együttműködést egy külön csoport is támogatja, amely a tagállamok, az Európai Bizottság és az ENISA képviselőiből áll. Ez a csoport koordinálja az uniós szintű információcserét, és részt vesz a nagyszabású kiberbiztonsági események és válságok kezelésében. Az Európai Kiberválságügyi Kapcsolattartó Szervezetek Hálózata (European Cyber Crisis Liaison Organisation Network, EU-CyCLONe) operatív szintű válságkezelési feladatokat lát el, biztosítva a folyamatos információáramlást az EU tagállamai között.

A NIS2 irányelv átfogó szabályozási keretet biztosít az alapvető és fontos szervezetek kiberbiztonsági kockázatainak kezelésére, különösen a tagállami illetékes hatóságok által végzett célzott ellenőrzések és felügyeleti tevékenységek révén. Az irányelv 32. és 33. cikke részletezi a kiberbiztonsági szabályok betartatásához szükséges mechanizmusokat, amelyek közé a helyszíni vizsgálatok, a célzott biztonsági ellenőrzések és a jogsértések szankcionálása is sorolható. Fontos kiemelni tehát, hogy a tagállamok illetékes hatóságainak hatáskörébe tartozik, hogy az alapvető és fontos szervezeteknél rendszeres és célzott biztonsági ellenőrzéseket végezzenek. Ezeket a vizsgálatokat képzett szakembereknek szükséges lefolytatni, és tartalmazhatnak helyszíni ellenőrzéseket, távoli felügyeleti intézkedéseket, valamint kockázatalapú biztonsági vizsgálatokat. Az ellenőrzések alapját a szervezetek által végzett kockázatelemzések, vagy más rendelkezésre álló kockázati információk adják, amelyek biztosítják az objektivitást és a megkülönböztetésmentes eljárást.

Kiemelésre érdemes információ, hogy a célzott biztonsági ellenőrzéseket független szerv is elvégezheti az egyes tagállamokban. Az ilyen ellenőrzések költségeit általában az ellenőrzött szervezet viseli, kivéve, ha az illetékes hatóság indokolt esetben másként rendelkezik. Az ellenőrzések eredményeit az illetékes hatósághoz kell benyújtani, amely ezek alapján további intézkedéseket kezdeményezhet, például hiányosságok orvoslását, biztonsági szabályzatok frissítését vagy kiberbiztonsági politikák módosítását. Az irányelv szerint a célzott biztonsági ellenőrzések és az illetékes hatóság által végzett felügyeleti tevékenységek kulcsfontosságúak az egységes kiberbiztonsági szint megvalósításában az Európai Unión belül. Ezek az eszközök nemcsak a meglévő hiányosságok azonosítását és megszüntetését teszik lehetővé, hanem

hosszú távon növelik a kritikus infrastruktúrák és szervezetek ellenálló képességét is. Az ilyen mechanizmusok biztosítják, hogy az Unió kiberbiztonsági szabályai minden tagállamban egységesen érvényesüljenek, miközben a társadalmi és gazdasági stabilitást is elősegítik.

Mindeközben: Magyarország kiberbiztonsága

A nemzeti szintű kiberbiztonsági szabályozás Magyarországon az uniós folyamatokkal párhuzamosan indult el. 2013-ban elfogadták az ország első átfogó stratégiáját a kiberbiztonság területén,[44] amely megalapozta az állami és önkormányzati szervek elektronikus információbiztonságára vonatkozó jogi keretrendszer kialakítását. Ennek részeként jött létre az a törvényi szabályozás, amely nemcsak az érintett szervek kötelezettségeit rögzítette, hanem elindította az információbiztonsági szervezetrendszer kiépítését is.

A szabályozás fejlődésével és a gyakorlati tapasztalatok alapján 2015-ben sor került az intézményrendszer részleges központosítására: megalakult a központi hatóságként működő nemzeti intézmény, a Nemzetbiztonsági Szakszolgálaton belül működő Nemzeti Kibervédelmi Intézet (a továbbiakban: NBSZ NKI), amely az állami és a piaci szereplők számára egyaránt illetékes az információ- és hálózatbiztonság területén. Ez a szerv vette át a korábbi eseménykezelési feladatokat, egyúttal képviseli Magyarországot az uniós kiberbiztonsági együttműködésekben is. A kiberbiztonsági védelem külön területeit további, speciális feladatkörrel rendelkező szervezetek látják el – ilyenek például a honvédelmi rendszerekért vagy az állami létfontosságú infrastruktúrákért felelős egységek. A működésükre vonatkozó részletszabályokat egy külön kormányrendelet rögzíti. A hazai stratégiai gondolkodás a nemzetközi szabályozási környezethez igazodva folyamatosan frissül: a korábbi uniós irányelvek nyomán új, a korszerű fenyegetésekre reflektáló nemzeti stratégiák születtek, amelyek megalapozzák Magyarország hosszú távú kiberbiztonsági célkitűzéseit és cselekvési irányait.

A magyar kibertér jogi szabályozásának első mérföldkövét a 2013. április 15-én elfogadott törvény jelentette, amely az állami és önkormányzati szervek elektronikus információinak védelmét helyezte középpontba.[45] Már elnevezésében is egyértelművé teszi, hogy kizárólag az elektronikus információbiztonság területére vonatkozik, és célzottan az állami intézmények információs rendszereit kívánja védeni. A jogszabály olyan átfogó keretet teremt, amely megelőzésre épülő, rendszerszintű védelmet nyújt a teljes elektronikus információs infrastruktúra számára, különös figyelmet fordítva a fenyegetések azonosítására és a tudatosság növelésére. Az alapelvek mentén a szabályozás célja a biztonsági kockázatok megelőzése, valamint a bekövetkező események szakszerű és tudatos kezelése. Az Ibtv. már a preambulumában hangsúlyt helyez a megelőzésre, a védelemre, a biztonságra és a tudatosság növelésére, amelyek a jogszabály alapelveit képezik. A törvény kiemeli a nemzeti elektronikus adatvagyon, valamint a létfontosságú információs rendszerek biztonságának fontosságát, utalva

[44] 1139/2013. (III. 21.) Korm. határozat.
[45] 2013. évi L. törvény.

arra, hogy ezek védelme társadalmi elvárás. A jogszabály részletesen meghatározza az információbiztonság kulcsfogalmait, mint a bizalmasság, a sértetlenség és a rendelkezésre állás. Ezek az alapelvek biztosítják, hogy az adatokhoz csak jogosultak férhessenek hozzá (bizalmasság), azok hitelesek és eredetük igazolható legyen (sértetlenség), illetve az információs rendszerek folyamatosan elérhetők maradjanak az arra jogosultak számára (rendelkezésre állás). A védelmi intézkedések tervezésénél alapvető elv, hogy azoknak a kockázatokkal arányosan kell megvalósulniuk – vagyis a védelemre fordított erőforrásoknak összhangban kell lenniük a lehetséges károk mértékével. Az Ibtv. ennek megfelelően már a fogalmi keretében is hangsúlyosan kezeli a védelem különböző típusait, és pontosan meghatározza azok tartalmát.[46] Az Ibtv. hozzájárult a 2013-ban elfogadott Nemzeti Kiberbiztonsági Stratégiában megfogalmazott kormányzati célok és intézkedések megvalósításához, valamint a kapcsolódó szervezeti feladatok gyakorlati alkalmazásához.

A 2013. évi L. törvény, amely Magyarországon elsőként teremtette meg a kiberbiztonság jogszabályi kereteit, egy adott történeti és technológiai kontextusra reflektált, és elsősorban az állami elektronikus információs rendszerek védelmére fókuszált. Az elmúlt évtized technológiai fejlődése, valamint az Európa-szerte egyre gyakoribb és komplexebb kibertámadások azonban új típusú kihívásokat generáltak, amelyek túlnőttek a korábbi szabályozás keretein. A kiberbiztonság társadalmi, gazdasági és nemzetbiztonsági jelentősége számottevően megnőtt, mindezt pedig az Európai Unió NIS2 irányelve is tükrözi, amely a tagállamoktól átfogó, szektorokon átívelő és egységes szabályozást követel meg. E körülmények tették indokolttá egy új, korszerű és strukturált törvényi szabályozás megalkotását, amelyet a Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény testesít meg. Ez a jogszabály a korábbi törvények hatályon kívül helyezésével és az uniós előírások integrálásával új alapokra helyezi Magyarország kiberbiztonsági rendszerét.

A Kibertv. Magyarország új, egységes és korszerű jogszabálya, amely 2025. január 1-jén lépett hatályba, és a nemzeti kiberbiztonság szabályozási kereteit átfogóan újraszabályozta. A jogszabály célja az elektronikus információs rendszerek védelmének megerősítése, különös tekintettel azokra a szervezetekre, amelyek tevékenysége kiemelt jelentőségű az állam, a gazdaság és a társadalom működése szempontjából. A törvény a korábbi kiberbiztonsági jogszabályokat – így többek között az Ibtv.-t és a Kibertantv.-t[47] – hatályon kívül helyezi, és egyetlen átfogó keretbe integrálja a releváns előírásokat, összhangban az Európai Unió NIS2 irányelvével.

A törvény hatályát a szervezetek típusán, tevékenységi körén és méretén alapuló besorolás szerint határozták meg. A hatály alá tartoznak mindenekelőtt az állami szervek és szervezetek, a többségi állami befolyás alatt álló gazdasági társaságok, valamint a NIS2 irányelvben meghatározott ágazatokban működő szervezetek, amennyiben megfelelnek a középvállalkozásokra vonatkozó küszöbértékeknek. Mindezek mellett az NBSZ NKI nemzeti kiberbiztonsági hatóságként jogosult további szervezetek azonosítására és bevonására is, ha azok tevékenysége alapján ez indokolt. A szervezetek

[46] Bodó 2014.
[47] 2023. évi XXIII. törvény a kiberbiztonsági tanúsításról és kiberbiztonsági felügyeletről.

„alapvető" vagy „fontos" kategóriába sorolása a törvény erejénél fogva történik, a vezetők felelőssége pedig a hatály meghatározása és a kötelezettségek teljesítése.

A kiberbiztonsági hatósági feladatokat a jogszabály hatálybalépésétől kezdve négy intézmény látja el: a közigazgatási ágazat, valamint az állami működés szempontjából kiemelt jelentőséggel bíró szervezetek vonatkozásában az NBSZ NKI; a banki szolgáltatások és a pénzügyi piaci infrastruktúrák, valamint a közigazgatási ágazat kivételével a NIS2 irányelv szerinti ágazatokban a Szabályozott Tevékenységek Felügyeleti Hatósága (a továbbiakban: SZTFH); a honvédelmi célú elektronikus információs rendszerek tekintetében a honvédelemért felelős miniszter; a banki szolgáltatások és a pénzügyi piaci infrastruktúrák vonatkozásában a Magyar Nemzeti Bank.

A törvény kulcsszerepet játszik az Európai Unió NIS2 irányelvének hazai implementációjában. Ez az irányelv új szintre emeli a kiberbiztonság uniós szabályozását, kiterjesztve a kötelezettségek körét, megerősítve a felügyeleti mechanizmusokat, valamint szigorúbb biztonsági követelményeket állítva a köz- és a magánszféra számára. A magyar jogalkotó ezt figyelembe véve egy központosított, egységes törvényi keretet alkotott, amely a NIS2 előírásait szervezeti szintre bontja le. A Kibertv. átfogó és strukturált válasz Magyarország részéről az egyre komplexebb kiberbiztonsági fenyegetésekre, és egyben megfelel az uniós elvárásoknak is. A hatálya alá tartozó szervezetek pontos meghatározása és a kijelölt hatóságok szerepének tisztázása elősegíti a hatékony jogalkalmazást és a kibertér védelmének erősítését.

Jogszabályi ív: a 2013. évi L. és a 2024. évi LXIX. törvény összevetése

A digitális környezet gyors átalakulása új kihívások elé állította a kiberbiztonsági szabályozást Magyarországon is. A 2013. évi L. törvény lefektette a nemzeti információbiztonság alapjait, de az elmúlt évtized technológiai és geopolitikai változásai szükségessé tették egy új, komplex szabályozási rendszer bevezetését. Ezt valósítja meg a 2024. évi LXIX. törvény, amely már az egész társadalomra és gazdaságra kiterjedő kiberbiztonsági keretrendszert nyújt.

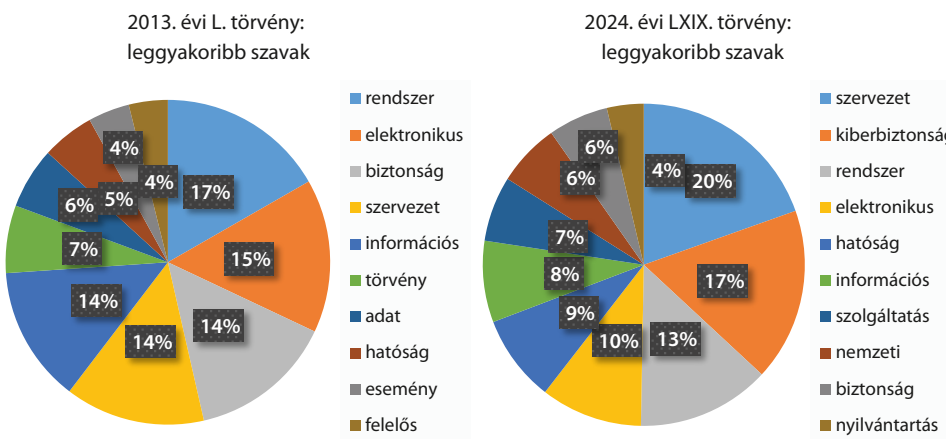
A két szabályozás közötti különbségek nem csupán terjedelmi vagy technikai, hanem strukturális és stratégiai szinten is érzékelhetők. Jelen tanulmány legfőbb célja e két törvény összehasonlító elemzése: feltárni, hogy miként változott a kiberbiztonság definíciója, az alkalmazási kör, a fogalomhasználat, valamint a szabályozás fókusza. Az elemzés kiterjed a kulcsszavak gyakoriságára, a jogszabályok szerkezeti és tematikai klasztereire, valamint a szabályozás mögötti hatósági és auditmechanizmusokra is.

Az Ibtv. jogalkotási célja az elektronikus információs rendszerek védelme volt az állami és önkormányzati szférában. E törvény főként az állami szféra – közigazgatási, igazságügyi és honvédelmi szervek – elektronikus rendszereinek biztonságát kívánta megerősíteni. A jogszabály hatálya szűk, jól körülhatárolt maradt, nem terjedt ki a magánszektor szereplőire vagy a kritikus infrastruktúrákra. Ezzel szemben a Kibertv. hatóköre jelentősen bővült. A szabályozás már nemcsak az állami és önkormányzati szektor intézményeire, hanem gazdasági szereplőkre – így többek között az energia-, víz- és közlekedési szektorra, hírközlési szolgáltatókra, digitális infrastruktúrákra, gyártói tevékenységekre – is kiterjed.

A 2013-as törvény idején nem volt cél az uniós jogharmonizáció. A szabályozás egyértelműen nemzeti keretek között készült, a belső állami struktúrák megerősítésére irányult. Ezzel szemben a 2024-es törvény megalkotásának egyik alapvető célja az EU-s NIS2 irányelv implementációja volt. A harmonizációval Magyarország egy olyan egységesített, európai szinten elvárt kiberbiztonsági ökoszisztémához csatlakozott, amely megköveteli a kockázatalapú szemlélet, az auditálható működés és az incidensmenedzsment alkalmazását. A törvény immár stratégiai célként határozza meg a kiberfenyegetések elleni nemzeti védekezést, amelynek részei a nemzeti kiberbiztonsági hatóság megerősítése (fogalmi szinten létrehozása), a tanúsítási és megfelelőségi rendszerek bevezetése, valamint a nemzetközi együttműködés szabályozása.

A szógyakorisági elemzés szintén jól tükrözi a két szabályozás fókuszainak és nyelvi karakterének változásait. Az elemzés során külön figyelmet kaptak az úgynevezett stop-word listán szereplők szavak kivételével a leggyakrabban előforduló kulcsszavak, valamint azok n-gram típusú előfordulási mintázatai (például bigramok, trigramok).

A 2013-as törvényben a leggyakoribb szavak csökkenő sorrendben a „rendszer", „elektronikus", „biztonság", „szervezet", „információs" voltak. Ezek a technikai és intézményi védelemre, valamint az állami szervezeti struktúrákra utaltak. Ezzel szemben a 2024-es törvény nyelvezetében erőteljesen dominálnak az alábbi szavak: „szervezet", „kiberbiztonság", „rendszer", „elektronikus", „hatóság", de a szókészlet szempontjából gyakorinak számítanak az olyan szavak, mint a „tanúsítás", „megfelelőség", „incenskezelő" és „szolgáltatás". Ezek a szavak nemcsak gyakoribbak lettek, de új szemléletet is tükröznek: az állami irányítás helyett az auditálható működés, a szolgáltatások folytonossága és a felügyeletre épülő ökoszisztéma került a középpontba (2. ábra).



2. ábra: A 2013. évi L. és a 2024. évi LXIX. törvény leggyakoribb szavai
Forrás: a szerző szerkesztése

A „védelmi" szócsalád (például védelem, védelme, védelmének) előfordulása a 2024-es törvényben több mint háromszoros a 2013-ashoz képest. Ez mutatja, hogy a védekezési mechanizmusok nemcsak gyakoribbak, hanem részletesebben is szabályozottak lettek. Figyelemre méltó a „kiberbiztonság" szó markáns szerepe a Kibertv.-ben, a szó

előfordulása több mint hetvenszeres az Ibtv.-hez képest. Jól látható, hogy a „kiberbiztonság" fogalma és annak hangsúlya jelentősen megnőtt az újabb szabályozásban, az egész törvény fókusza kifejezetten erre a témára épül. Ezzel szemben a 2013-as törvény inkább az elektronikus információs rendszerek biztonságáról szól általánosságban, és a „kiberbiztonság" fogalma kevésbé központi. A „kiberbiztonság" kifejezés gyakoriságának növekedése nem pusztán nyelvi vagy terminológiai változás, hanem egy mélyebb átalakulás jele: a digitális tér védelme stratégiai nemzetbiztonsági és gazdaságpolitikai kérdéssé vált. A 2024-es törvény ezt a paradigmaváltást tükrözi, és célja, hogy strukturáltabb, egységesebb, valamint hatékonyabb választ adjon a 21. század kibertérből érkező kihívásaira. Fontos továbbá, hogy a „kiberbiztonság" kulcsszó dominanciája annak is köszönhető, hogy a törvény célja immár nem pusztán az információbiztonság technikai aspektusainak szabályozása, hanem egy egységes, kockázatalapú, hatóságilag (is) ellenőrzött kiberbiztonsági rendszer létrehozása. A törvény emellett közvetlenül hivatkozik a NIS2-re, ami szintén hangsúlyosabbá teszi a kiberbiztonság stratégiai fontosságát.

Mindezek mellett, ha a szavak gyakoriságát vizsgáljuk, akkor látható, hogy a „szervezet" és a „szerinti" szavak használata szintén ugrásszerűen nőtt a Kibertv.-ben, ami a jogalanyok pontosabb, kategorizált (alapvető/fontos) szabályozására utal. A „nemzeti" és „hatóság" szavak sokkal gyakoribb használata mutatja, hogy 2024-re erőteljesebben és komplexebben jelent meg a nemzeti hatósági struktúra a hazai kiberbiztonsági szegmensben.

Az előzőket figyelembe véve megállapítható, hogy a 2024. évi törvény jóval szélesebb hatókört ölel fel, mint a 2013-as elődje. Míg utóbbi kizárólag az állami és önkormányzati szervek elektronikus információbiztonságát szabályozta, az új jogszabály az egész társadalmi-gazdasági környezetre, beleértve a magánszektort is, kiterjeszti a szabályozást. Ez önmagában indokolja a „szolgáltatás" és „szolgáltató" kifejezések gyakori megjelenését, hiszen a törvény – többek között – a többségi állami befolyással működő és kritikus infrastruktúrákat üzemeltető vállalatok mellett kiterjed számos kiemelten kockázatos (például energetika, egészségügy és hírközlési szolgáltatások) és kockázatos ágazatban (például élelmiszeripar, gyártás, digitális szolgáltatások) működő gazdasági társaságra is.

Összességében tehát a szavak gyakorisági különbségei azt tükrözik, hogy a 2024-es jogszabály nemcsak terjedelmében, hanem komplexitásában és stratégiai célkitűzéseiben is jóval előrébb tart, mint a 2013-as verzió. Ez pedig a kulcsszavak súlyozásában is markánsan megmutatkozik.

A két szabályozás eltérő nyelvezete, fogalomhasználata és tematikus fókusza azt mutatja, hogy miként alakult át az információbiztonság technikai megközelítéséből egy átfogó, stratégiai szemléletű kiberbiztonsági keretrendszerré. Az Ibtv. főként a „bizalmasság, sértetlenség, rendelkezésre állás" hármas védelmi célra épülő, alapvetően információbiztonsági szemléletet tükrözi. A törvény célja a fogalmi keretek meghatározása, a szabályozási alapok lefektetése, a közigazgatási és önkormányzati rendszerek biztonságának megalapozása, az elektronikus információs rendszerek osztályba sorolása, valamint a védelmi szintek szabályozása volt. Az elemzett bigramokban olyan kifejezések domináltak, mint az „elektronikus információs", „információs rendszer" vagy a „biztonsági osztály" (1. táblázat).

Ezzel szemben a Kibertv. szókészlete már egy kiterjesztett, nemzetstratégiai szemléletet tükröz, ahol megjelenik a központosított irányítás, hatósági ellenőrzés és a digitális szuverenitás fogalma is. A 2024-es törvény már nem csupán a technikai védelmet célozza meg, hanem egy szélesebb, nemzetbiztonsági és stratégiai szintre emelt kiberbiztonsági keretrendszert vezet be. A hangsúly a „kiberbiztonság" fogalom köré szerveződik, és – néhány bigram még markánsabb előfordulása mellett – megjelentek olyan új elemek, mint az „incidenskezelő központok", a „tanúsítási rendszerek" vagy a „kiberbiztonsági hatóság". A nyelvezet erősebben utal állami szabályozásra, központosított reakciómechanizmusokra és az EU-s harmonizációra.

A „poszt-kvantumtitkosítás" bigram mind a 2013-as, mind a 2024-es magyar kiberbiztonsági törvényben hasonló gyakorisággal szerepel, ám eltérő funkcióval. A 2013-as törvényben a kifejezés előrelátó módon, jövőorientált technológiai tudatosságként jelenik meg, a kvantumszámítógépek okozta lehetséges fenyegetésekre reagálva. Ezzel szemben a 2024-es törvény már konkrét szabályozási tartalommal ruházza fel: kijelöli az alkalmazásra kötelezett szervezetek körét, meghatározza az intézményi felügyeletet (SZTFH), és részletezi az alkalmazás módját. A bigram statisztikai gyakoriságának hasonlósága mögött tehát tartalmi fejlődés húzódik meg: a korábbi elvi megközelítés mára gyakorlati, intézményesült védelemmé vált, amely a digitális szuverenitás megőrzésének egyik sarokköve lett. A „poszt-kvantumtitkosítás" bigram hasonló gyakoriságú jelenléte tehát nem a technológiai stagnálásra, hanem inkább egy konzisztens, hosszú távú szabályozási gondolkodásra utal. A magyar jogalkotás már 2013-ban érzékelte a kvantumfenyegetés lehetőségét, és a 2024-es törvényben már intézményes szinten szabályozza is azt. Ez egyben azt is jelzi, hogy a kiberbiztonsági szakpolitika nemcsak reaktív, hanem proaktív is: felkészülés történik azokra a technológiai áttörésekre, amelyek jelenleg még nem okoznak tömeges problémát, de a jövőben alapjaiban rengethetik meg a digitális infrastruktúrák biztonságát.

1. táblázat: A leggyakoribb bigramok

Bigram	2013. évi L. tv.	2024. évi LXIX. tv.	Eltérés
elektronikus információs	155	256	+101
információs rendszer	155	241	+86
nemzeti kiberbiztonság	0	175	+175
kiberbiztonsági hatóság	0	149	+149
kiberbiztonsági incidenskezelő	0	114	+114
rendszerbiztonság	36	65	+29
biztonsági osztály	27	64	+37
incidenskezelő központ	0	86	+86
kiberbiztonsági incidens	0	86	+86
poszt-kvantumtitkosítás	28	36	+8
kiberbiztonsági tanúsítás	0	55	+55
Összesen	401	1327	926

Forrás: a szerző szerkesztése

A 2013. évi L. törvény és a 2024. évi LXIX. törvény szövegének kvantitatív tartalomelemzése a bigramok és trigramok gyakoriságának összehasonlításával jól érzékelteti a magyar kiberbiztonsági szabályozás fejlődését. A bigramelemzés eredményei alapján megállapítható, hogy 2024-re jelentősen megnőtt az olyan kifejezések előfordulása, mint az „elektronikus információs" (+101), az „információs rendszer" (+86) és a „rendszerbiztonság" (+29). Emellett új, 2013-ban még nem szereplő, de 2024-re domináns bigramok jelentek meg, például „nemzeti kiberbiztonság" (175 előfordulás) és „kiberbiztonsági hatóság" (149 előfordulás), jelezve a kiberbiztonság önálló szakpolitikai területté válását.

A trigramok összehasonlítása még markánsabban mutatja a tematikai váltást (2. táblázat). A 2013-as törvény kulcsszavai egy még épülő információbiztonsági keretrendszert jeleztek, míg a 2024-es törvény kifejezései egy beérett, stratégiai irányítás alá vont kiberbiztonsági ökoszisztémát rajzolnak ki. 2024-ben a gyakori trigramok között már szerepel a „kiberbiztonság incidenskezelő központ", „nemzet kiberbiztonság hatóság" is.

2. táblázat: A leggyakoribb trigramok

Trigram	2013. évi L. tv.	2024. évi LXIX. tv.	Eltérés
elektronikus információs rendszer	151	240	+89
információs rendszer biztonsága	36	59	+23
kiberbiztonsági incidenskezelő központ	0	86	+86
nemzeti kiberbiztonsági hatóság	0	72	+72
biztonságért felelős személy	19	40	+21
poszt-kvantumtitkosítás alkalmazás	23	30	+7
biztonsági osztályba sorolás	16	34	+18
kiberbiztonsági tanúsítási rendszer	0	37	+37
információs rendszer védelme	15	18	+3
informatikáért felelős miniszter	0	28	+28
ideiglenes hozzáférhetetlenné tétel	11	14	+3
Összesen	271	658	387

Forrás: a szerző szerkesztése

A trigramok elemzése megerősítette a bigramokból levont következtetéseket, ugyanakkor tovább részletezte az eltolódás mértékét. A legnagyobb növekedés a „nemzeti kiberbiztonsági hatóság" típusú összetett kifejezések körében figyelhető meg, amelyek közvetlenül az újonnan létrehozott intézményi és jogszabályi struktúrákra utalnak. A trigramok alapján nemcsak az általános információbiztonsági fókusz erősödése mutatkozik, hanem a kiberbiztonsági incidensek kezelésére, a tanúsítási rendszerek kiépítésére és a poszt-kvantumtitkosítási eljárásokra helyezett hangsúly is. Az új törvény egyik legmarkánsabb újítása a megfelelőségi és auditmechanizmusok bevezetése: míg a 2013. évi L. törvény csupán felügyelő és koordináló szerepkörrel ruházta fel az állami intézményeket, a 2024-es jogszabály részletes, szabványokon alapuló megfelelőségi struktúrát ír elő.

Összességében mind a bigram-, mind a trigramszintű kvantitatív elemzés azt bizonyítja, hogy a magyar kiberbiztonsági szabályozás a 2013–2024 közötti időszakban jelentős mértékben bővült, mélyült és specializálódott. Az új kifejezések számossága és előfordulási gyakorisága tükrözi a kiberfenyegetésekre adott szabályozási válaszok komplexitásának növekedését, valamint az európai uniós szabályozási harmonizáció hatását.

A dokumentumok tartalmi vizsgálata alapján mindkét törvény jól elkülöníthető klaszterekbe sorolható tematikusan (3. táblázat). Ezek a klaszterek nemcsak a jogszabályok szerkezetét, hanem azok szabályozási logikáját is tükrözik. A bigramok és trigramok elemzése különösen fontos volt a tematikus klaszterek azonosításában, mivel az egyszerű szavak szintjén nehezen megragadható fogalmi összefüggések – mint például az „eseménykezelő központ" vagy a „kiberbiztonsági incidenskezelő központ" – kizárólag a kifejezéspárok szintjén mutatták meg a jogszabályok hangsúlyeltolódását. Míg a 2013. évi szabályozás a szervezeti szintű felkészültség és védelem köré szerveződött, a 2024. évi törvény a kiberfenyegetésekre adott központi válaszok és a nemzeti hatósági struktúrák kiépítését állítja középpontba.

A 2013. évi L. törvény klaszterezési eredményei alapján három meghatározó tematikai egység rajzolódik ki. Az első klaszter a szervezeti hatály és alkalmazás témakörét öleli fel, amely a jogi szövegezés hagyományos logikáját követi: középpontjában az érintett szervezetek körének kijelölése, a különböző típusú állami és önkormányzati szervek beazonosítása, illetve az alkalmazási kör bekezdések szerinti strukturált bemutatása áll. A szöveg itt szigorúan normatív, a szereplők körének meghatározásán keresztül biztosítja a jogszabály érvényesülését. A második klaszter a kulcsfogalmak és rendszer-definíciók világára koncentrál, ahol az „elektronikus információs rendszer", „adatkezelő" és „adatfeldolgozás" fogalmai kiemelt jelentőséget kapnak. Ez a rész biztosítja a törvény technológiai és fogalmi alapjait, nélkülözhetetlen keretet adva a szabályozás többi részéhez. A harmadik klaszter a biztonsági események és osztályozás területét fedi le, amelyben a biztonsági események felismerése, osztályozása és kezelése kap hangsúlyt. Itt a cél az, hogy a rendszerbiztonság fenntartása érdekében a különböző típusú fenyegetésekre arányos és megfelelő válaszreakciók szülessenek.

A 2024. évi LXIX. törvény klaszterstruktúrája ehhez képest jelentős tematikus eltolódást mutat, ami a kiberbiztonság új dimenzióinak megjelenését tükrözi. Az első klaszter, a fogalmi alapok és technológia, továbbra is az elektronikus információs rendszerek jelentőségét emeli ki, ugyanakkor sokkal hangsúlyosabban jelenik meg a digitális szolgáltatások hálózati alapú értelmezése, valamint a szolgáltatási modellek átalakulása. A második klaszter egyértelműen az állami kontroll, incidenskezelés és tanúsítás köré épül: itt már nemcsak rendszereket, hanem intézményes mechanizmusokat szabályoznak, például a nemzeti kiberbiztonsági hatóság, valamint egy új hatósági szereplő, az incidenskezelő központok és a tanúsítási rendszerek kiemelésével. A harmadik klaszter új tematikai súlypontként a kockázatkezelés és audit témáját fejleszti ki, amely a megfelelőségértékelési rendszerek, szervezeti auditok és kiberkockázatok tudatos kezelését állítja középpontba. Ez a változás a nemzetközi szabályozási környezet fejlődésével is összhangban van, és a kockázatalapú megközelítés elterjedését tükrözi.

3. táblázat: Tematikus klaszterek

Jogszabály	A klaszter neve	Kulcsszavak	Leírás
2013/L.	szervezeti hatály és alkalmazás	szervezet, szerinti, bekezdés, meghatározott, vonatkozó	hatálymeghatározás, szervezeti kör
2013/L.	alapfogalmak és rendszerdefiníció	elektronikus, információs, rendszer, rendszerek, adatkezelő	fogalmi alapok és technológiai keret
2013/L.	biztonsági események és osztályozás	biztonsági, esemény, osztályba, szint, kezelés	rendszerbiztonság és eseménykezelés
2024/LXIX.	fogalmi alapok és technológia	elektronikus, információs, rendszer, rendszerek, szolgáltatás	digitális infrastruktúra, szolgáltatási modell
2024/LXIX.	hatóság, incidenskezelés és tanúsítás	kiberbiztonsági, nemzeti, hatóság, incidenskezelő, tanúsítás	szabályozás, incidenskezelés
2024/LXIX.	kockázatkezelés és audit	kockázat, szolgáltató, megfelelőség, audit	kockázatmenedzsment, megfelelőségértékelés
Mindkét jogszabály esetén 3-3 klaszter határozható meg.			

Forrás: a szerző szerkesztése

A 2024-es kiberbiztonsági törvény jelentős tematikus elmozdulást tükröz a korábbi szabályozáshoz képest, amit a klaszterezési elemzés is világosan kirajzol. Míg a 2013-as törvény főként a szervezeti felkészültségre és a rendszerbiztonság általános irányelveire fókuszált, addig a 2024-es szabályozás központi elemei között a hatósági struktúrák kiépítése, az incidenskezelés intézményesítése és a tanúsítási mechanizmusok formalizálása szerepel.

Az új törvény alapján bevezetett auditálási rendszer előírja, hogy a meghatározott szolgáltatóknak független, akkreditált szervezetek által végzett kötelező auditokon kell átesniük, összhangban a „Kockázatmenedzsment, megfelelőségértékelés" klaszter tartalmával. Ezzel párhuzamosan létrejön egy központosított nemzeti kiberbiztonsági hatóság és egy további hatóság, amelyek a „Hatóság, incidenskezelés és tanúsítás" klaszter logikájának megfelelően széles jogosultságokkal felügyelnek, végeznek hatósági ellenőrzéseket, koordinálnak és szükség esetén szankcionálhatnak. Emellett a törvény immár részletesen szabályozza az incidenskezelési ciklust – a megelőzés, észlelés, reagálás és helyreállítás fázisait –, ami szintén tematikus súlypontot képez az új klaszterstruktúrában.

Összehasonlítva a két törvényt, megállapítható, hogy a magyar kiberbiztonsági szabályozás fejlődése során a kezdeti, technológiai alapú, rendszerközpontú megközelítést egy komplexebb, átfogóbb és szervezeti szintű kockázatmenedzsment-alapú modell váltotta fel. A klaszterezés eredményei azt mutatják, hogy míg 2013-ban az információbiztonsági rendszerek integritása és bizalmassága volt a központi kérdés, 2024-re a fókusz az incidenskezelés, a szabályozó hatóságok, a nemzeti ellenálló

képesség és az auditfolyamatok megerősítése irányába tolódott el. A szabályozási fejlődés nemcsak a technológiai környezet változását tükrözi, hanem az Európai Unió közös irányelveinek, valamint a globális kiberfenyegetettségre adott válaszoknak is megfelel. Összességében tehát a szabályozási fejlődés – ahogyan azt a klaszterelemzés is megerősíti – egyértelműen a kiberbiztonság átfogóbb, rendszerszintű megközelítése felé mutat, amely a nemzeti ellenálló képesség és a megfelelőség központi szerepét hangsúlyozza a globális fenyegetettségi környezet változásainak tükrében.

A 2013. évi L. törvény és a 2024. évi LXIX. törvény összehasonlítása világosan rávilágít a magyar kiberbiztonsági szabályozás fejlődési ívére: a technikai és szervezeti alapú védelemtől eljutottunk egy EU-konform, stratégiai szinten szervezett, teljes digitális ökoszisztémát lefedő szabályozási keretrendszerig.

Az Ibtv. célja az állami rendszerek alapvető információbiztonságának megteremtése volt. A fókusz elsősorban az elektronikus információs rendszerek fizikai és logikai védelmére, valamint az adatkezelési szabályozásra helyeződött. A fogalomhasználat stabil, de szűk spektrumú volt, kevésbé reagált az akkor már nemzetközileg is megjelenő új típusú fenyegetésekre és szolgáltatási modellekre. A Kibertv. ezzel szemben paradigmaváltást képvisel. Az EU NIS2 irányelvének implementálásával egy olyan korszerű, incidensalapú, auditálható és a nemzetközi követelményekhez illeszkedő szabályozási rendszert vezet be, amely már nem csupán az állami szférát, hanem a gazdasági szereplők és a kritikus infrastruktúrák teljes spektrumát lefedi. A 2024-es dokumentum retorikája és szókincse is változást tükröz: a „kiberbiztonság", „szolgáltató", „tanúsítás", „hatóság" és „incidens" kulcsszavak gyakorisága mutatja, hogy immár nemcsak a védelem hangsúlyos, hanem a kontroll, a reagálás, a megfelelőség és a stratégiai felügyelet is.

Összességében elmondható, hogy a 2024. évi LXIX. törvény egy modern, rugalmas, de egyben szigorú szabályozási eszköztárat ad a magyarországi kiberbiztonság intézményesített védelmére. Az összehasonlító elemzés jól demonstrálja, hogy a változások nemcsak tartalmi és jogi szinten, hanem a szabályozási filozófiában is érvényesülnek. Ennek értelmében a magyar kiberbiztonsági szabályozás fejlődése jól mutatja a digitális fenyegetésekre adott jogalkotói válaszok dinamikáját. Míg a 2013. évi L. törvény az információbiztonsági alapok lefektetését szolgálta, a 2024. évi LXIX. törvény már egy komplexebb, szektorokon átívelő, integrált megközelítést képvisel. Az SZTFH szerepe pedig azt mutatja, hogy a jövőbiztos technológiai megoldások alkalmazása központi elemévé vált a nemzeti kiberstratégiának. Ez a fejlődési ív jól tükrözi a nemzetközi trendeket és Magyarország digitális szuverenitás iránti elkötelezettségét.

Összegzés és diszkusszió

A magyar kiberbiztonsági szabályozás fejlődése világosan tükrözi azt az átalakulást, amelyet a globális digitalizáció és az Európai Unió szabályozási törekvései váltottak ki. A 2013. évi L. törvény egy korai szabályozási modellként szolgált, amely az állami és önkormányzati szervek elektronikus információinak védelmére koncentrált, szűk, infrastruktúra-központú megközelítést alkalmazva. Ezzel szemben a 2024. évi LXIX. törvény – szoros összhangban a NIS2 irányelv célkitűzéseivel – már egy integráltabb,

incidens- és kockázatkezelés-orientált, nemzeti és uniós szintű együttműködésre épülő rendszert valósít meg.

A kutatási kérdésre adott válasz során megállapítható, hogy a magyar kiberbiztonsági szabályozás szemlélete alapvetően megváltozott: az állami rendszerek szűk védelmétől egy olyan átfogóbb kiberbiztonsági ökoszisztéma irányába mozdult el, amelyben az állami és magánszektor szereplői egyaránt érintettek. A kockázatérzékenység, az incidensek gyors és hatékony kezelése, a szolgáltatásfolytonosság biztosítása, valamint a fenyegetések megelőzése váltak a szabályozás központi elemeivé.

A nyelvezetben szintén markáns elmozdulás figyelhető meg: míg a 2013. évi törvény terminológiája a technikai biztonsági intézkedésekre, rendszerleírásokra és az állami felelősségi körökre helyezte a hangsúlyt, addig a 2024-es törvény már a kockázatértékelés, incidenskezelés, kiberreziliencia, auditálhatóság és tanúsítás fogalmait állítja középpontba. A fogalmi gazdagodás a szabályozás mélyülését is tükrözi, hiszen az új szövegben megjelennek az ellátási lánc biztonságára, az emberi tényezőre, a folyamatos felügyeletre és az uniós szintű adatmegosztásra vonatkozó előírások is.

A szabályozási logika szintjén is jelentős átrendeződés történt: míg a 2013-as törvény inkább a szabályozott alanyok kötelezettségeire és az állami védelem fenntartására koncentrált, addig a 2024-es jogszabály egy proaktív, kockázatalapú megközelítést követ, amely a megelőzésre, a korai észlelésre, a gyors incidensreagálásra és a nemzeti szintű koordináció megerősítésére épít. A szabályozás immár nemcsak a technológiai eszközök védelmét célozza, hanem egy átfogó társadalmi reziliencia megteremtését is.

A jogalkotási átrendeződések mögött az intézményi szereplők is differenciálódtak és specializálódtak: míg korábban egyetlen központi szereplő, a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet dominált, addig ma már több hatóság – az NBSZ NKI mellett a Szabályozott Tevékenységek Felügyeleti Hatósága, a Magyar Nemzeti Bank és a honvédelemért felelős minisztérium – feladatmegosztása biztosítja a szektorok közötti differenciált felügyeletet. Ez a logikai és intézményi mélyülés a kiberbiztonsági ökoszisztéma komplexitásának felismerését tükrözi, továbbá ezen felügyeleti rendszer biztosítja, hogy az egyes ágazatok sajátosságainak megfelelő, szektorspecifikus kiberbiztonsági követelmények érvényesüljenek.

Az Európai Unió NIS2 irányelve volt az a katalizátor, amely nemcsak a magyar szabályozás átfogó modernizációját eredményezte, hanem azt is kikényszerítette, hogy a nemzeti szabályozási modell szervesen illeszkedjen az egységes európai kiberbiztonsági architektúrába. A harmonizált követelmények révén Magyarország nemcsak a belső piac védelmét erősíti, hanem saját gazdasági és társadalmi stabilitását is növeli.

A NIS2 irányelv az Európai Unió kiberbiztonsági stratégiájának központi pillére, amely a digitalizációval járó fenyegetések kezelésére és az Unió kiberrezilienciájának növelésére irányul. Az irányelv célja az egységes és magas szintű kiberbiztonság megteremtése a tagállamok között, különös tekintettel a kritikus infrastruktúrák és ágazatok védelmére. Az irányelv sikeressége a tagállamok és a társadalom minden szereplőjének együttműködésén múlik. A kiberbiztonság nem csupán technológiai kérdés, hanem közös társadalmi felelősség is, amelyhez elengedhetetlen a tudatosság növelése és az együttműködés erősítése. Az emberi tényező védelmére és a technológiai

innovációk összehangolt alkalmazására alapozott megközelítés biztosíthatja, hogy az Európai Unió – és így Magyarország is – hatékonyan szálljon szembe a kiberfenyegetésekkel. A NIS2 irányelv és a 2024. évi LXIX. törvény által meghatározott keretek és intézkedések kulcsfontosságúak a digitális tér biztonságának és fenntarthatóságának megőrzésében, elősegítve a társadalmi és gazdasági stabilitás hosszú távú fenntartását.

Összességében megállapítható, hogy a 2013–2024 közötti szabályozási evolúció során a magyar kiberbiztonsági jogalkotás logikai, intézményi és tartalmi értelemben is érettebbé vált. A kutatás eredményei alátámasztják, hogy a modern, harmonizált és kockázatérzékeny kiberbiztonsági környezet kialakítása nemcsak technológiai, hanem társadalmi és stratégiai szinten is elengedhetetlenné vált. A jövő kihívásai közé tartozik, hogy a törvényi keretek gyakorlati alkalmazása is képes legyen lépést tartani a folyamatosan változó kiberfenyegetésekkel – ezt pedig további empirikus kutatások és folyamatos hatékonyságértékelések segítségével kell megerősíteni.

Felhasznált irodalom

Ambrus Éva (2023): *Kiberhadviselési képességek a jelen tükrében.* PhD-disszertáció. Budapest: Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola.

Barna Bianka Rita et al. (2023): A *social engineering* helye az információbiztonsági auditban. *Biztonságtudományi Szemle,* 5(1), 25–41. Online: https://biztonsagtudomanyi.szemle.uni-obuda.hu/index.php/home/article/view/317/258

Bányász Péter et al. (2019): A *social engineering* jelentette veszélyek napjainkban. In *Biztonság, szolgáltatás, fejlesztés, avagy új irányok a bevételi hatóságok működésében.* Budapest: Magyar Rendészettudományi Társaság Vám- és Pénzügyőri Tagozat, 12–37. Online: https://doi.org/10.37372/mrttvpt.2019.1.1

Bejtlich, Richard (2018): The Origin of the Quote „There Are Two Types of Companies". *TaoSecurity Blog,* 2018. december 18. Online: https://taosecurity.blogspot.com/2018/12/the-origin-of-quote-there-are-two-types.html

Bihaly Barbara (2021): A kibervédelem szerepe az Európai Unió közös biztonsági és védelmi politikájában. *Hadtudományi Szemle,* 14(3), 45–55. Online: https://doi.org/10.32563/hsz.2021.3.4

Bodó Attila Pál (2014): *Információbiztonsági jogi ismeretek vezetőknek.* Budapest: Nemzeti Közszolgálati Egyetem. Online: https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/10084/Inform%E1ci%F3biztons%E1gi%20jogi%20ismeretek.pdf?sequence=2

Bodó Attila Pál – Joó Tamás – Palicz Tamás (2020): *Az Ibtv. gyakorlata. Éves továbbképzés az elektronikus információs rendszerek védelméért felelős vezető számára 2020.* Budapest: Nemzeti Közszolgálati Egyetem. Online: http://hdl.handle.net/20.500.12944/18029

Bonnyai Tünde (2019): Kritikus információs infrastruktúrák védelme. In Deák Veronika (szerk.): *Kritikus információs infrastruktúrák védelme. Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára 2019.* Budapest: Nemzeti Közszolgálati Egyetem Közigazgatási Továbbképzési Intézet, 56–83.

Bor Olivér (2024): Egységesen magas kiberbiztonság az Európai Unióban. *Szakmai Szemle,* 22(1), 177–196.
Castells, Manuel (2005): *A hálózati társadalom kialakulása. Az információ kora. Gazdaság, társadalom, kultúra. I. kötet.* Budapest: Gondolat–Infonia.
Deák Veronika (2023): Hírszerzés a kibertérben. In Krasznay Csaba (szerk.): *Taktikák és stratégiák a kiberhadviselésben.* Budapest: Ludovika Egyetemi Kiadó, 87–114.
ENISA: EU Cybersecurity Index: Framework and Methodological Note (2024). Online: www.enisa.europa.eu/sites/default/files/2024-12/eu_csi_methodological_note_v1-0.pdf
Európai Tanács – Az Európai Unió Tanács (2024): Az EU kiberbiztonságának megerősítése. Online: www.consilium.europa.eu/hu/policies/cybersecurity/?__cf_chl_tk=ddeADBDrnMIodjybZUhgCRVV76GXde13WCOyblKwLzc-1744563582-1.0.1.1-Gm9pFfeRocYZZORBZ94xJeGYG11Vs_GQW1_ye7tPNaI
Falyuna, Nóra et al. (2024): Against Disinformation: Bridging Science and Public Discourse. *Információs Társadalom,* 24(2), 68–84. Online: https://doi.org/10.22503/inftars.XXIV.2024.2.4
Farkas Ádám – Kelemen Roland (2023): *Nemzeti biztonság és kibertér.* Budapest: Médiatudományi Intézet. Online: https://mtmi.hu/files/7ddaa0c7-9a10-4123-af9c-e2d86c49cf30.pdf
Ghaib, Arkan A. (2024): Future Trends in Cybersecurity: Exploring Emerging Technologies and Strategies. *International Research Journal of Modernization in Engineering Technology and Science,* 6(2). Online: www.doi.org/10.56726/IRJMETS49530
Horváth, Dóra – Szabó, Zs. Roland (2019): Driving Forces and Barriers of Industry 4.0: Do Multinational and Small and Medium-Sized Companies Have Equal Opportunities? *Technological Forecasting and Social Change,* 146, 119–132. Online: https://doi.org/10.1016/j.techfore.2019.05.021
Kelemen Roland (2020): A kibertérből érkező fenyegetések jelentősége a hibrid konfliktusokban és azok várható fejlődése. *Honvédségi Szemle,* 148(4), 65–81. Online: https://doi.org/10.35926/HSZ.2020.4.5
Kis Márton – Bódi Antal – Számadó Róza (2024): A NIS2 hazai bevezetésének folyamata és kockázatai. *Hadmérnök,* 19(3), 165–182. Online: https://doi.org/10.32567/hm.2024.3.10
Kovács László (2018): *Kiberbiztonság és -stratégia*. Budapest: Dialóg Campus Kiadó.
Kovács László (2023): *Hadviselés a 21. században: kiberműveletek.* Budapest: Ludovika Egyetemi Kiadó.
Krasznay Csaba (2022): *Kiberbiztonsági a XXI. században.* Budapest: Katonai Nemzetbiztonsági Szolgálat.
Krasznay Csaba (2023): A *deepfake*-technológia kiberbiztonsági vonzatai. In Aczél Petra – Veszelszki Ágnes (szerk.): *Deepfake: a valótlan valóság.* Budapest: Gondolat Kiadó, 104–118.
Legárd Ildikó (2020): A barát és ellenség megkülönböztetése a kibertérben. *Jog – Állam – Politika,* 12(3), 125–140.
Legárd Ildikó (2023): A kiberhadviselés fogalma, nemzetközi jogi háttere, történeti áttekintése. In Krasznay Csaba (szerk.): *Taktikák és stratégiák a kiberhadviselésben.* Budapest: Ludovika Egyetemi Kiadó, 11–40.

Lella, Ifigeneia et al. (2024): *ENISA Threat Landscape 2024.* Online: https://doi.org/10.2824/0710888

Mäkelä, Jarmo (2019): Countering Disinformation: News Media and Legal Resilience. *Hybrid CoE Paper,* (1), 1–25. Online: www.hybridcoe.fi/wp-content/uploads/2020/07/News-Media-and-Legal-Resilience_2019_HCPaper-ISSN.pdf

Molnár Anna (2019): Az Európai Unió kiberbiztonsággal kapcsolatos tevékenysége. In Deák Veronika (szerk.): *Kritikus információs infrastruktúrák védelme. Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára 2019.* Budapest: Nemzeti Közszolgálati Egyetem Közigazgatási Továbbképzési Intézet, 35–55.

Nemzeti Kibervédelmi Intézet (2023): *Adathalász csalások, visszaélések a bankok nevében.* Online: https://nki.gov.hu/it-biztonsag/elemzesek/adathalasz-csalasok-visszaelesek-a-bankok-neveben/

Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (2024): *Éves kiberbiztonsági jelentés.* Online: https://nki.gov.hu/wp-content/uploads/2024/07/Eves-kiberbiztonsagi-jelentes.pdf

Nyári Gábor (2023): Elrettentés a kibertérben: elérhető cél vagy ábránd? In Krasznay Csaba (szerk.): *Taktikák és stratégiák a kiberhadviselésben.* Budapest: Ludovika Egyetemi Kiadó, 61–86.

Oroszi Eszter Diána (2023): *A biztonságtudatossági szint mérésének és fejlesztésének lehetősége.* PhD-disszertáció. Budapest: Nemzeti Közszolgálati Egyetem Közigazgatás-tudományi Doktori Iskola. Online: https://doi.org/10.17625/NKE.2024.023

Pintér István (2016): *A virtuális tér geopolitikája.* Budapest: Geopolitikai Tanács Közhasznú Alapítvány.

PurpleSec [é. n.]: *2024 Cybersecurity Statistics. The Ultimate List Of Cybersecurity Stats Data, & Trends.* Online: https://purplesec.us/resources/cybersecurity-statistics/

Tikos Anita (2019): A magyar kibervédelemmel kapcsolatos szabályozás aktuális kérdései. In Deák Veronika (szerk.): *Kritikus információs infrastruktúrák védelme. Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára 2019.* Budapest: Nemzeti Közszolgálati Egyetem Közigazgatási Továbbképzési Intézet, 8–34.

Trellix 2024 Threat Predictions. *Trellix,* 2023. október 30. Online: www.trellix.com/blogs/research/trellix-2024-threat-predictions/

Vandezande, Niels (2024): Cybersecurity in the EU: How the NIS2-directive Stacks up Against Its Predecessor. *Computer Law & Security Review,* 52, 105890. Online: https://doi.org/10.1016/j.clsr.2023.105890

Veszelszki Ágnes (2021): deepFAKEnews: Az információmanipuláció új módszerei. In Balázs László (szerk.): *Digitális kommunikáció és tudatosság.* Budapest: Hungarovox Kiadó, 93–105.

Veszelszki Ágnes (2023): Deepfake: kételkedés a kételyben. In Aczél Petra – Veszelszki Ágnes (szerk.): *Deepfake: a valótlan valóság.* Budapest: Gondolat Kiadó, 13–31.

Jogi források

A Bizottság (EU) 2017/1584 ajánlása (2017. szeptember 13.) a nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt reagálásról. C/2017/6100. 2017. szeptember 13. Online: https://eur-lex.europa.eu/legal-content/HU/ALL/?uri=CELEX%3A32017H1584

A Bizottság Közleménye a Tanácsnak, az Európai Parlamentnek, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának – „i2010: Európai információs társadalom a növekedésért és a foglalkoztatásért". COM/2005/0229 végleges. Online: https://eur-lex.europa.eu/legal-content/HU/ALL/?uri=CELEX%3A52005DC0229

A Tanács (EU) 2019/796 rendelete (2019. május 17.) az Uniót vagy annak tagállamait fenyegető kibertámadások elleni korlátozó intézkedésekről. Online: https://eur-lex.europa.eu/legal-content/HU/ALL/?uri=CELEX:32019R0796

Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről. Online: https://eur-lex.europa.eu/legal-content/HU/ALL/?uri=CELEX:32016L1148

Az Európai Parlament és a Tanács (EU) 2019/881 rendelete (2019. április 17.) az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről (kiberbiztonsági jogszabály). 2019. április 17. Online: https://eur-lex.europa.eu/legal-content/HU/ALL/?uri=CELEX%3A32019R0881

Az Európai Parlament és a Tanács 2022. december 14-i (EU) 2022/2555 irányelve 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). Online: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/hun

Az Európai Unió Tanácsa (2009): *Európai Biztonsági Stratégia. Biztonságos Európa egy jobb világban.* Luxembourg: Az Európai Unió Kiadóhivatala. Online: https://doi.org/10.2860/15719

Az Európai Unió Tanácsa (2010): *Az Európai Unió belső biztonsági stratégiája. Az európai biztonsági modell felé.* Luxembourg: Az Európai Unió Kiadóhivatala. Online: https://doi.org/10.2860/89974

Az Európai Unió Tanácsa (2018): Javul az EU kibervédelme: a Tanács támogatja a közös tanúsításról és a megerősített ügynökségről létrejött megegyezést. *Consilium.europa.eu,* 2018. december 19. Online: www.consilium.europa.eu/hu/press/press-releases/2018/12/19/eu-to-become-more-cyber-proof-as-council-backs-deal-on-common-certification-and-beefed-up-agency/

Európai Bizottság (2010): A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának. Az európai digitális menetrend. COM(2010)245 végleges. 2010. május 19. Online: https://eur-lex.europa.eu/legal-content/HU/ALL/?uri=celex:52010DC0245

Jelentés az európai biztonsági stratégia végrehajtásáról. A biztonság megteremtése a változó világban. S407/08. Brüsszel, 2008. december 11. Online: www.consilium.europa.eu/ueDocs/cms_Data/docs/pressdata/HU/reports/104644.pdf

Közös közlemény az Európai Parlamentnek és a Tanácsnak. Ellenálló képesség, elrettentés, védelem: az Unió erőteljes kiberbiztonságának kiépítése. JOIN/2017/0450 final. 2017. szeptember 13. Online: https://eur-lex.europa.eu/legal-content/hu/ALL/?uri=CELEX:52017JC0450

Közös közlemény az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának. Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér. JOIN/2013/01 final. 2013. február 2. Online: https://eur-lex.europa.eu/legal-content/HU/ALL/?uri=celex%3A52013JC0001

A Bizottság ajánlása (2003. május 6.) a mikro-, kis- és középvállalkozások meghatározásáról (az értesítés a C(2003) 1422. számú dokumentummal történt)

1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról

2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

2023. évi XXIII. törvény a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről

2024. évi LXIX. törvény Magyarország kiberbiztonságáról

418/2024. (XII. 23.) Korm. rendelet Magyarország kiberbiztonságáról szóló törvény végrehajtásáról

HADMÉRNÖK
VÉDELEMINFORMATIKA
20. évfolyam (2025) 1. szám 49–72.
DOI: 10.32567/hm.2025.1.3

Dub Máté[1]

A dezinformáció terjesztésével szemben hozott európai uniós intézkedések vizsgálata[2]

Az EUvsDisinfo adatbázisának elemzése

Examination of European Union Measures Against the Spread of Disinformation

Analysis of the EUvsDisinfo Database

Absztrakt

A 21. század technológiai forradalma és a különböző online platformok gyors fejlődése társadalmunkat új biztonsági kihívások elé állította, amelyek között azonosíthatjuk az álhírek és a dezinformáció terjedését. Az orosz–ukrán háború során különösen felerősödtek ezek a problémák, hiszen a konfliktus az online térben is megjelenő dezinformációs kampányokkal párosult, amelyek céljai között azonosíthatjuk a társadalmi, politikai és katonai befolyásolást. Jelen tanulmány középpontjában az Európai Unió álhírekkel és dezinformációval szembeni szabályozási környezete és gyakorlati intézkedései, illetve mindezek hatékonyságának vizsgálata szerepel. Az empirikus vizsgálatok során az EUvsDisinfo platform adatainak automatizált elemzésével bemutatom a dezinformációs kampányok földrajzi, nyelvi és tematikus mintázatait, illetve a hamis narratívák mögött meghúzódó összefüggéseket. Az eredmények rávilágítanak, hogy a hamis információk terjesztése jól strukturált, tudatosan megtervezett narratívák köré szerveződik, amelyek jelentős geopolitikai és társadalmi következményekkel járhatnak, a jelenség sikerében pedig nem csupán technológiai

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem Hadtudományi Doktori Iskola, e-mail: dub.mate@uni-nke.hu
[2] A kutatás a Kulturális és Innovációs Minisztérium ÚNKP-23-3-I-NKE-127 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

tényezők, hanem az emberi döntéshozatal és a médiafogyasztási szokások is meghatározó szerepet játszanak. Mindezek vonatkozásában a jövőbeni intézkedések tervezése során elengedhetetlen, hogy az EU és a tagállamok az eddigieknél nagyobb hangsúlyt helyezzen a társadalmi tudatosság növelésére, a médiaértés fejlesztésére, valamint az emberközpontú megközelítések integrálására is.

Kulcsszavak: dezinformáció, álhírek, Európai Unió, kiberbiztonság, EUvsDisinfo

Abstract

The technological revolution of the 21st century and the rapid development of various online platforms have confronted our society with new security challenges, among which the spread of fake news and disinformation can be identified. These problems have intensified particularly during the Russian–Ukrainian war, as the conflict has been accompanied by disinformation campaigns in the online sphere, aiming at social, political, and military influence. This study focuses on the European Union's regulatory framework and practical measures against fake news and disinformation, as well as on assessing their effectiveness. In the course of empirical research, I present the geographical, linguistic, and thematic patterns of disinformation campaigns, along with the underlying connections behind false narratives, through the automated analysis of data from the EUvsDisinfo platform. The results reveal that the dissemination of false information is organized around well-structured, deliberately planned narratives that may have significant geopolitical and societal consequences, with not only technological factors but also human decision-making and media consumption habits playing a decisive role in the phenomenon's success. In this regard, it is essential that, when designing future measures, the EU and its Member States place greater emphasis on raising public awareness, improving media literacy, and integrating human-centered approaches.

Keywords: disinformation, fake news, European Union, cybersecurity, EUvsDisinfo

Bevezetés

Az információs társadalom és a digitális technológiák robbanásszerű fejlődése a 21. században jelentős változásokat hozott mindennapi életünkben, beleértve az információkhoz való hozzáférés módját is. A közösségimédia-platformok, mint a Facebook, a Twitter, a TikTok vagy az Instagram, mára az információterjesztés elsődleges eszközeivé váltak. Noha ezek a felületek lehetőséget biztosítanak a gyors és széles körű kommunikációra, az információk valóságtartalmának ellenőrzése egyre nehezebb feladat. Az álhírek kifejezetten olyan információkat jelentenek, amelyek szándékosan hamisak vagy félrevezetők, és céljuk a közvélemény manipulálása. A dezinformáció, habár szorosan összefügg az álhírekkel, szofisztikáltabb, szűkebb fogalom, amely magában foglalja a kifejezetten szándékosan félrevezető információ terjesztését is, többek között politikai, gazdasági, katonai vagy társadalmi célok elérése érdekében. A fogalmi elhatárolás szempontjából másik kategóriaként azonosíthatjuk a félretájékoztatást,

amikor szándékosság nem áll fenn, a tartalom megosztója pedig nincs tisztában az adott információ valótlanságával vagy félrevezető szándékával. Az álhírek *(fake news)* és így a dezinformáció terjedése összességében olyan kihívásokat jelent, amelyek súlyos társadalmi, politikai, katonai és gazdasági következményekkel járhatnak.[3]

A téma aktualitása

Kutatási témám aktualitásának szempontjából fontosnak tartom kiemelni, hogy a közösségi média révén ezek az információk szinte ellenőrizetlenül és gyorsan jutnak el széles közönségekhez, ami komoly veszélyt jelent a demokratikus intézmények működésére, a társadalmi bizalomra és a közéleti diskurzus minőségére.[4] Az álhírek és a dezinformáció terjedésének problémája az elmúlt években különösen kiéleződött, amit jól mutatnak a világméretű események, mint például a korábbi, 2016-os választás az Amerikai Egyesült Államokban,[5] vagy az elmúlt években a Covid–19-pandémia és az orosz–ukrán háború. A járvány idején elárasztották a közösségimédia-felületeket például az egészséggel, az oltásokkal és a vírus eredetével kapcsolatos álhírek, amelyek komoly hatással voltak a járványkezelés hatékonyságára és a társadalmi magatartásra.[6] Hasonlóképpen, az orosz–ukrán fegyveres konfliktus során a dezinformáció az információs műveletek egyik központi eszközévé vált, amely a politikai célok elérésén túl hadászati és műveleti szinten is a katonai törekvések támogatását szolgálja, ami az információs hadviselés stratégiai jelentőségét mutatja a modern konfliktusokban.

A tudományos probléma megfogalmazása

Kutatásom tudományos problémájának középpontjában mindebből adódóan a dezinformációval szembeni fellépési lehetőségek állnak. Az Európai Unió (a továbbiakban: EU) – különösen az orosz–ukrán háború 2022-es eszkalációja után – egyre határozottabb intézményi és szabályozási válaszokat fogalmazott meg e jelenség kezelésére. Ennek ellenére továbbra is hiányzik a dezinformációs tartalmak rendszerszintű, kvantitatív és tematikus feldolgozása, amely képes lenne feltárni azok szerkezeti mintázatait, kapcsolathálózatait és terjedési dinamikáját.

Az álhírekkel és a dezinformációval szembeni harc tehát nem csupán jogi és szabályozási kérdés, hanem társadalmi és kulturális kihívás is. A médiaértés, a kritikai gondolkodás és a digitális kompetenciák fejlesztése kulcsfontosságú a dezinformáció elleni védekezésben. Az uniós intézkedések hatékonyságának növelése érdekében elengedhetetlen, hogy a polgárok képzettek legyenek az információforrások kritikus értékeléséhez, és képesek legyenek felismerni a manipulációs technikákat.

[3] Wardle–Derakhshan 2017; Tandoc Jr. et al. 2018.
[4] Fletcher–Nielsen 2017.
[5] Allcott–Gentzkow 2017.
[6] European Commission [é. n. a].

Kutatási célkitűzések

Kutatásom célja, hogy átfogó képet nyújtson az EU által az álhírekkel és a dezinformációval szemben hozott gyakorlati intézkedések, kialakított keretrendszerek hatékonyságáról, valamint feltárja a dezinformációs kampányok szerkezeti és tematikus mintázatait. A kutatás az ismertetett társadalmi, politikai és biztonságpolitikai kihívásokra reagál, és a módszertani fejezetben részletezett adatelemzési technikák segítségével kívánja megvilágítani a vizsgált dezinformációs kampányok sajátosságait.

A szakirodalmi áttekintéssel célom feltérképezni, hogy az EU által bevezetett szabályozási keretek hogyan járulhatnak hozzá a dezinformációs tartalmak elterjedésének visszaszorításához. Ennek kapcsán az empirikus kutatás eredményeinek szempontjából célom a dezinformációs kampányok időbeli, tematikus és földrajzi eloszlásának vizualizálása, valamint ezek gyakorlati hasznosíthatóságának ismertetése.

Kutatásom központi, empirikus eleme a hamis információk tematikus klaszterekbe történő szerveződésének vizsgálata, ezzel célom a narratívák szerkezeti feltérképezése az EUvsDisinfo adatbázisában rögzített dezinformációs esetek elemzésével. E tekintetben pedig elengedhetetlen a megjelenő kulcsszavak, témák és narratívák kapcsolódásának kiértékelése.

Továbbá elemzem a dezinformációs esetek országok és régiók szerinti megoszlását, valamint a cikkek nyelvi eloszlását annak fényében, hogy mely országok és nyelvi közösségek a leginkább kitettek a manipulációs kísérleteknek. Ezen elemzés hozzájárulhat az európai és globális narratívák közötti különbségek jobb megértéséhez.

Összefoglalóan a célom gráf- és adatelemzés eszközeivel azonosítani a dezinformációs kampányok struktúráját. Ennek segítségével nemcsak az ismétlődő mintázatok, hanem a kampányok esetleges „szezonális" vagy geopolitikai impulzusait is fel lehet tárni.

A dezinformáció elleni fellépési lehetőségek

A dezinformációval szembeni fellépésnek számtalan egyéni, csoportszinten meghatározható, állami vagy nemzetközi módja és lehetősége van, amelyek közé tartoznak a különböző *fact-checker* oldalak, az online felületek önszabályozó vagy kötelezettségekből adódó tevékenysége, a diverzált, tudatos felhasználói információfogyasztás, a különböző szakértői vagy állami felhívások, állásfoglalások, nemzeti vagy nemzetközi szabályzói környezet, az annak történő megfelelés vagy implementáció.

A következő alfejezetekben kutatásommal összhangban a dezinformáció terjedési mechanizmusainak és hatásainak ismertetése mellett szeretném külön bemutatni az európai uniós szabályzói és gyakorlati, a tagállami szabályzói és a platformok önszabályozási tevékenységére vonatkozó főbb jellemzőket, hatályos intézkedéseket.

A dezinformáció és az európai uniós szabályozás

Az EU felismerte az álhírek és a dezinformáció veszélyeit, és az elmúlt években számos intézkedést hozott ezek terjedésének visszaszorítása érdekében. Az EU szabályozási válasza több szinten valósul meg: egyrészt a jogi és politikai keretrendszerek kialakításával, másrészt a technológiai cégekkel, szakértői munkacsoportokkal való együttműködés révén, amely a digitális platformok felelősségét és átláthatóságát kívánja növelni.

A dezinformáció elleni fellépés összetett, többoldalú kihívás, amely különféle eszközök – technológiai platformok, nemzeti és uniós szintű szakpolitikai intézkedések, valamint média- és tényellenőrző szervezetek – bevonását követeli meg. Az utóbbi években a dezinformációs módszerek egyre kifinomultabbá váltak, miközben a károkozó szereplők köre jelentősen bővült. Mindezek hatására az EU a politikai és szabályozási folyamatait felgyorsította, válaszul arra a fenyegetésre, amelyet a dezinformációs tevékenységek az EU és tagállamai demokratikus berendezkedésére jelentettek. E folyamat 2015-ben kezdődött, amikor az Európai Tanács először szólította fel az Európai Bizottságot arra, hogy konkrét intézkedéseket dolgozzon ki az uniós demokratikus folyamatokat érintő információs fenyegetések kezelésére. Ez a kezdeményezés közvetlenül összefüggött az ukrajnai konfliktussal, különösen a Krím 2014-es orosz annektálásával és a Kelet-Ukrajnában kirobbant háborúval. Akkoriban a dezinformációt elsősorban külső fenyegetésként értelmezték, főként orosz forrásokhoz köthetően. Ennek megfelelően 2015-ben létre is hoztak Brüsszelben egy stratégiai kommunikációs munkacsoportot az Európai Külügyi Szolgálaton belül, amelynek feladata az EU-t célzó orosz dezinformációs tartalmak azonosítása volt.[7] A munkacsoport tevékenységével kapcsolatban részletesebb ismertetést a módszertani fejezet tartalmaz.

Az EU által a dezinformáció elleni fellépés jegyében kidolgozott eszközök közül legfontosabb volt a nagy digitális platformok bevonásával 2018-ban elfogadott úgynevezett dezinformáció elleni gyakorlati kódex *(Code of Practice on Disinformation),* amely alapvetően önszabályozó jellegű *(soft law)* megoldásként íródott. Célja többek között, hogy a digitális szolgáltatók önkéntesen vállalják az álhírek terjedésének megfékezését, például a hamis információk jelölésével, eltávolításával és a megbízható források előnyben részesítésével. A kódex alkalmazásának első szakasza azonban több hiányosságot is felszínre hozott, egyebek között elégtelen átláthatóságot, hiányos adatmegosztást, valamint korlátozott végrehajthatóságot.[8] A 2018-as önszabályozó kódex hatékonyságának hiányosságai, valamint a Covid–19-világjárvány és az orosz–ukrán háború során tapasztalt, fokozódó dezinformációs kampányok együttesen világossá tették, hogy erősebb, átláthatóbb és számonkérhetőbb fellépésre van szükség az online térben. E problémák orvoslása érdekében 2022-ben egy új, megerősített változat készült el *(Strengthened Code of Practice on Disinformation),* amely – habár továbbra is alapvetően önszabályozó mechanizmus – már egy szélesebb jogszabályi kontextusba, különösen a 2022-ben elfogadott digitális szolgáltatásokról szóló uniós rendelet (Digital Services Act, a továbbiakban: DSA) által biztosított szabályozási keretrendszerbe illeszkedett. Ezáltal a korábbinál nagyobb mértékben ötvöződnek

[7] Colomina Saló – Pérez-Soler 2022.
[8] European Commission [é. n. b].

a *soft law* és a jogilag kötelező erejű *hard law* elemek, amelyek révén a platformok felelősségvállalása, valamint a szabályok betartatásának eszközrendszere is jelentősen megerősödik. A DSA ezáltal fontos mérföldkövet jelent az online platformok szabályozásában abból a szempontból, hogy az új szabályozás kötelezővé teszi a nagy platformok számára az átláthatóságot, és lehetőséget biztosít a felelősség megállapítására az online felületeiken megjelenő tartalmak tekintetében, beleértve az álhírek terjedését. A szabályozás kötelezi továbbá a nagy platformokat, hogy jelentést készítsenek az álhírek terjedésének csökkentésére tett erőfeszítéseikről, és biztosítsák a felhasználók számára a tartalmak eredetének és a hirdetési átláthatóságnak a megismerését.[9]

A szabályozások körébe tartozik továbbá az EU-nak a politikai reklámtevékenység átláthatóságáról szóló rendelete, amely az online platformok átláthatóságát hivatott növelni. Ez a rendelet különös hangsúlyt fektetett a politikai hirdetések szabályozására és a dezinformáció terjedésének korlátozására, kötelezve a platformokat, hogy tegyenek lépéseket a hamis információk terjesztésének megfékezése érdekében. Az intézkedés bevezetése óta több platform, mint például a Facebook és a Twitter, új szabályokat vezetett be, amelyek a hirdetések átláthatóságára és a dezinformáció elleni fellépésre vonatkoznak.[10]

Az EU stratégiájának központi gondolata, hogy a dezinformációval szembeni sikeres védelem csak multidiszciplináris, széles körű együttműködésben képzelhető el, amelyben a magánszektor (különösen a technológiai vállalatok és a médiafelületek), továbbá a nemzeti és nemzetközi közintézmények közösen lépnek fel, miközben kiemelt figyelmet fordítanak a konfliktusok békés rendezésének eszközeire, valamint a demokratikus alapértékekre, így különösen a tájékozódáshoz való jog és a véleménynyilvánítás szabadságának biztosítására.[11]

Ezek az intézkedések együttesen arra irányulnak, hogy csökkentsék a dezinformációs kampányok hatékonyságát, és megvédjék a polgárokat a hamis információktól. A szabályozások időszerűségét jól mutatja, hogy már a 2018 előtti időszakban is jelentősen gyorsabban és intenzívebben terjedtek az online térben a hamis információk, mint a valóságnak megfelelő hírek, függetlenül az információ típusától vagy témájától. Az álhíreken belül különösen hangsúlyos a politikai tartalmú hamis hírek terjedési sebessége és széles körű elérése, amely szignifikánsan meghaladja a más témájú hamis információkét. Ez arra enged következtetni, hogy a politikai dezinformáció különösen alkalmas a figyelem megragadására, ezáltal a közvélemény befolyásolására is. E jelenség hátterében részben az áll, hogy az emberek általában az újszerűnek, érdekesnek vagy különlegesnek érzékelt információkat preferálják, és ezeket gyakrabban, intenzívebben osztják meg. Mivel a hamis hírek gyakran tartalmaznak meglepő, szokatlan vagy szenzációként ható elemeket, ezek közösségi terjedési sebessége és volumene nagyobb, mint a hiteles, de kevésbé „figyelemfelkeltő" híreké. Fontos leszögezni emellett, hogy az automatikusan működő robotfiókok (botok) nem preferálják egyik információtípust sem, tehát a valódi és hamis hírek terjedését

[9] European Commission 2022; Az Európai Parlament és a Tanács (EU) 2022/2065 rendelete; Brogi – De Gregorio 2024; EEAS Launches a New Tool to Help Navigate in Disinformation Environment 2022.
[10] Az Európai Parlament és a Tanács (EU) 2024/900 rendelete; Bradshaw–Howard 2019.
[11] Berdud 2024.

hasonló mértékben gyorsíthatják, az alkalmazó szándékától függően. Ennek alapján kijelenthető, hogy a hamis információk gyors és széles körű elterjedését nem pusztán technológiai tényezők, hanem jelentős részben az emberi viselkedés sajátosságai is okozzák. Ez azt jelenti, hogy a hamis hírek visszaszorítása érdekében a technológiai megoldások mellett emberközpontú, pszichológiai és viselkedéstudományi megközelítések alkalmazása is szükséges. A jelenség társadalmi, politikai és biztonságpolitikai következményei jelentősek. A dezinformáció kezelésére irányuló intézkedések kidolgozása során komplex, interdiszciplináris megközelítésre van szükség, amely figyelembe veszi az emberi döntéshozatali mechanizmusokat, a társadalmi berendezkedéseket és az információfogyasztási mintázatokat egyaránt.[12]

Önszabályozó tevékenység a gyakorlatban – tagállami megvalósítás

Az EU szabályozási keretei minden tagállam számára kötelezők, azonban a végrehajtásban és a nemzeti szintű intézkedésekben jelentős eltérések figyelhetők meg. Egyes országok, mint Németország és Franciaország, már a szabályozási időszak kezdetén vagy azt megelőzően külön nemzeti törvényeket is elfogadtak a dezinformáció elleni fellépés erősítésére. Németország 2017-ben vezette be a NetzDG-t (Netzwerkdurchsetzungsgesetz), amely szigorúan szabályozza a közösségimédia-platformokat, és akár jelentős pénzbírsággal is sújtja őket, ha nem távolítják el idejében a jogsértő tartalmakat. A NetzDG hatékonysága azonban vegyes eredményeket mutatott; habár sok platform növelte az átláthatóságot és javította a tartalommoderálást, kritikák is érték a törvényt, mert túlzottan korlátozó lehet, és nem minden esetben biztosítja a szólásszabadság megfelelő egyensúlyát. Franciaország szintén jelentős lépéseket tett, különösen a választási időszakokban előforduló dezinformáció elleni harcban. A 2018-ban elfogadott francia dezinformációs törvény célja, hogy a választási kampányok idején hatékonyan korlátozza a manipulált információk terjedését, kötelezve a platformokat a gyanús tartalmak gyors eltávolítására. A törvény végrehajtása során több kihívás is felmerült, beleértve a tartalmak pontos azonosításának és a véleménynyilvánítás szabadságának kérdéseit.[13]

Önszabályozó tevékenység a gyakorlatban – online platformok

Az EU átfogó intézkedései jelentős lépéseket jelentenek a dezinformáció elleni harcban, azonban hatékonyságuk, ahogy korábban láthattuk, tagállamonként és platformonként is eltérő. A nagy platformok, mint a Facebook/Meta és a Twitter/X, az EU szabályozási nyomására több millió hamis fiókot és bejegyzést távolítottak el. A Meta emellett jelentősen növelte a dezinformáció elleni intézkedéseit az EU szabályozásainak hatására. Ezenkívül a platformok egyre több forrást fordítanak az álhírek jelölésére, illetve olyan eszközök bevezetésére, amelyek segítik a felhasználókat a dezinformáció felismerésében.[14]

[12] Vosoughi et al. 2018.
[13] Newman et al. 2021; De Bruin et al. 2021.
[14] Gorwa–Binns–Katzenbach 2020.

A DSA által bevezetett szigorúbb jelentési követelmények is hozzájárulnak a dezinformáció elleni harc hatékonyságának növeléséhez. Az EU-s intézkedések hatására több platform vezette be az átláthatósági jelentéseket, amelyekben részletesen bemutatják, hogy milyen lépéseket tettek az álhírek terjedésének csökkentéséért. Az ilyen jelentések nemcsak a felhasználók, hanem a szabályozó hatóságok számára is értékes adatokat szolgáltatnak, amelyek alapján pontosítani lehet a szabályozási környezetet.[15]

Az Európai Unió gyakorlati fellépése a dezinformációval szemben

Az EU a dezinformációval szemben nem pusztán a szabályozási környezetet alakította ki, és kötelezte a tagállamokat, valamint az online platformokat azok implementációjára, hanem önmaga is jelentős gyakorlati lépéseket tett a dezinformáció terjesztésének visszaszorításáért. Ezen lépések egyike az EUvsDisinfo projekt keretében valósul meg, amely kutatásom alapjául is szolgál, így ennek részletes kifejtésére, vizsgálatára a következő fejezetekben kerül sor.

A dezinformáció és az álhírek terjedésének mechanizmusai, hatásai

Az álhírek és a dezinformáció terjedése több szinten is veszélyezteti a társadalmak működését, és különböző mechanizmusok révén fejti ki hatását. Ezek közül kiemelkedő jelentőségű a közösségimédia-felületek szerepe, ugyanis az álhírek és a dezinformációs tartalmak gyors terjedésének alapja a platformok algoritmusai, amelyek a felhasználói preferenciákra építenek, és gyakran előtérbe helyezik az érzelmileg megosztó, sokszor hamis információkat vagy a különböző „véleménybuborékok" erősítését, mivel mindezek nagyobb interakciót, eléréseket generálnak.

A dezinformáció terjedésének egyik legfontosabb mechanizmusa az *echo chamber* jelenség, amely során a felhasználók olyan információs buborékokba záródnak, ahol csak saját véleményükkel összhangban álló információkat látnak. Ez tovább erősíti a meglévő előítéleteket és csökkenti a kritikus gondolkodás lehetőségét.[16] E mechanizmus különösen veszélyes a politikai polarizáció növekedése szempontjából, mivel elősegíti a dezinformációs kampányok hatékonyságát és az álhírek gyors elterjedését.[17]

A dezinformáció és az álhírek másik jelentős terjesztési módja a korábban is említett automatizált botok és álprofilok használata, amelyek feladata a hamis információk gyors, széles körű terjesztése és a közösségi médián belüli diskurzus manipulálása. Ezek az automatizált eszközök nagymértékben hozzájárulnak a hamis vagy félrevezető információk hitelességének növeléséhez azáltal, hogy mesterségesen generált reakciókkal, megosztásokkal és kommentekkel hitelesnek tűnő visszajelzéseket, tartalmakat hoznak létre.[18]

[15] Az Európai Parlament és a Tanács (EU) 2022/2065 rendelete.
[16] Cinelli et al. 2021.
[17] Del Vicario et al. 2016.
[18] Ferrara et al. 2016; Shao et al. 2018.

A dezinformáció hatásai rendkívül sokrétűek lehetnek, ideértve a társadalmi bizalom megingatását, a demokratikus intézmények iránti bizalom csökkenését és a társadalmi megosztottság növekedését. A dezinformációs kampányok közvetlenül befolyásolhatják a politikai folyamatokat, például választások kimenetelét, ami komoly következményekkel járhat a demokratikus rendszer stabilitására nézve.[19] Ezenkívül az egészségügyi szektorban is súlyos következményei lehetnek, amint azt a Covid–19-pandémia idején tapasztalt oltásellenes álhírek és dezinformációk is mutatták. Ezek a kampányok hozzájárultak a járvány terjedésének súlyosbításához és az oltási hajlandóság csökkenéséhez.[20]

Kutatási módszertan

A dezinformációs kampányok vizsgálatának alapjául az EUvsDisinfo honlap adatbázisa, pontosabban a platformon megjelenő esetek leírásai szolgáltak. Az EUvsDisinfo platform az Európai Külügyi Szolgálat (a továbbiakban: EEAS) által működtetett kezdeményezés, amelynek célja a dezinformációs kampányok feltárása és elemzése, különös tekintettel az Európai Unióra, annak tagállamaira és más geopolitikai szereplőkre. A platform folyamatosan gyűjti és elemzi azokat a cikkeket, amelyek félrevezető vagy hamis információkat terjesztenek, majd ezeket strukturált módon adatbázisba rendezi.

Az EUvsDisinfo platformot az EU 2015-ben hozta létre azzal a céllal, hogy szembeszálljon az orosz dezinformációs kampányokkal, különösen a 2014-es ukrajnai események után. Az oldal célja, hogy felismerje, szakértők által elemezze és tudatosítsa a dezinformációs tevékenységeket, különös tekintettel az orosz állami és álhírmédiák által terjesztett félrevezető információkra. Az elmúlt években az EUvsDisinfo mintegy 19 000 dezinformációs esetet dokumentált, segítve a nyilvánosságot és a döntéshozókat a tájékozottabb és hitelesebb információs környezet kialakításával. Az EEAS East StratCom munkacsoportja a platformon 15 nyelven végez adatelemzést és nyújt médiafigyelő szolgáltatásokat, ennek segítségével azonosítja, összeállítja és leleplezi a dezinformációs eseteket. Az EUvsDisinfo a maga nemében az egyetlen kereshető, teljesen nyílt forráskódú adattár, amelynek céljai között azonosítható a felhasználók rezilienciájának növelése az online dezinformációs tevékenységekkel szemben.[21]

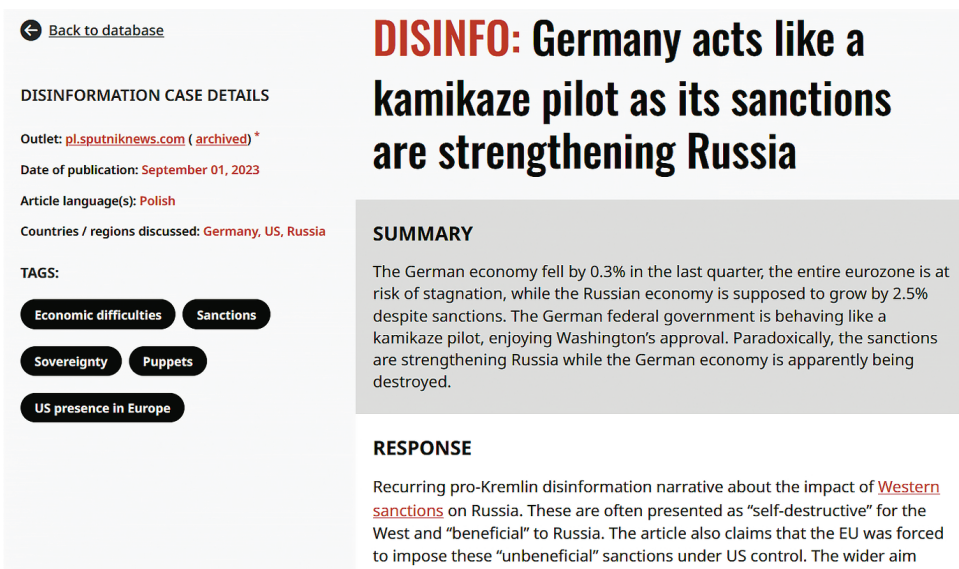
Az EUvsDisinfo adatbázisában szereplő esetek elemzésére Python-alapú automatizált webes adatgyűjtő szkripteket alkalmaztam, amivel a platform dezinformációs eseteket tartalmazó aloldaláról származó cikkeket rögzítettem. Kutatásom során az adatgyűjtéshez, feldolgozáshoz és vizualizációhoz több Python-csomagot használtam, amelyek az alábbi három fő kategóriába sorolhatók:

[19] Allcott–Gentzkow 2017.
[20] Managing the COVID-19 Infodemic: Promoting Healthy Behaviours and Mitigating the Harm from Misinformation and Disinformation 2020.
[21] To Challenge Russia's Ongoing Disinformation Campaigns': Eight Years of EUvsDisinfo 2023.

1. Adatgyűjtés:
    - Selenium (dinamikus, automatizált, *web-based* lekérdezések és adatgyűjtés, stabilizációs, teljesítményoptimalizációs *add-on-ok,* kiegészítő csomagok használatával);
    - BeautifulSoup (HTML- és XML-dokumentumok, információk elemzése).
2. Adatkezelés és elemzés, például:
    - Pandas/OpenPyXL/NumPy/Collections/Shutil (adatkezelés).
3. Adatvizualizáció:
    - Matplotlib (diagramok, grafikonok és térképek);
    - Seaborn (adatvizualizáció);
    - NetworkX (kapcsolati hálók, gráfok);
    - GeoPandas (térbeli adatok, térképek);
    - Shapely (geometriai adatok);
    - PyPROJ (koordináta-rendszerek kezelése);
    - PyOgrio (térinformatika).

Az EUvsDisinfo nyíltan elérhető adatbázisában szereplő cikkeknél a következő információkat elemeztem:

- a dezinformáció címe;
- a publikálás dátuma;
- forrás *(outlet)* – ahol az adott dezinformációs tartalom megjelent;
- nyelv – amelyen a cikket publikálták;
- földrajzi vonatkozás (országok/régiók) – amelyeket az adott dezinformáció érint;
- témák és címkék *(tags)* – az adott cikkhez rendelt témakörök.



1. ábra: Példa az EUvsDisinfo adatbázisából
Forrás: https://euvsdisinfo.eu/report/germany-acts-like-a-kamikaze-pilot-as-its-sanctions-are-strengthening-russia/

A vizsgálat időintervalluma: 2023. szeptember 1. – 2024. június 9.

Ebben az időszakban 1404 esetet sikerült azonosítani. Ezen 1404 eset, valamint azok indikátorai felölelik a vizsgált időtartamban a platformon azonosítható cikkek 100%-át, amelyeket az EUvsDisinfo saját klasszifikációs protokollja alapján validáltak.

Ami az elemzés időtartamának kezdő dátumát illeti, a választás indikátoraként a Sheffieldi Egyetem kutatói által az adatbázison elvégzett, 2023 augusztusáig tartó elemzés azonosítható. Módszertani szempontból a kutatók tanulmánya egy másik adatgyűjtő és elemző keretrendszert is bemutat, illetve részletezik az esetleges kutatási korlátokat, az elemzés kapcsán felmerülő fontosabb kérdéseket.[22]

Mivel a fenti tanulmány 2023 augusztusáig elemzi az adatbázist, kutatásomban azon eredmények vizsgálatára kerülhet sor, amelyek megelőző kutatásokban nem szerepelnek. Az időintervallum végdátumául a 2024. évi európai parlamenti választás napját jelöltem ki. Az Európai Parlament új, 2029-ig tartó ciklusára, valamint az Amerikai Egyesült Államok 2024. novemberi választására (és az ahhoz tartozó kampányra, valamint az új adminisztrációra) az álhírek terjedését elemezve egy új fejezetként tekinthetünk, amelynek önálló vizsgálatára a későbbiekben akár jelen kutatás módszertana is adekvát lehetőségeket biztosíthat. A kutatás időintervalluma kapcsán fontos kiemelni, hogy korlátokat is azonosíthatunk, mivel nem az adatbázis egészét vettem górcső alá, így például a kampányhajrá vagy a választási eredmények utáni diszkurzív átrendeződés nem került bele az elemzésbe.

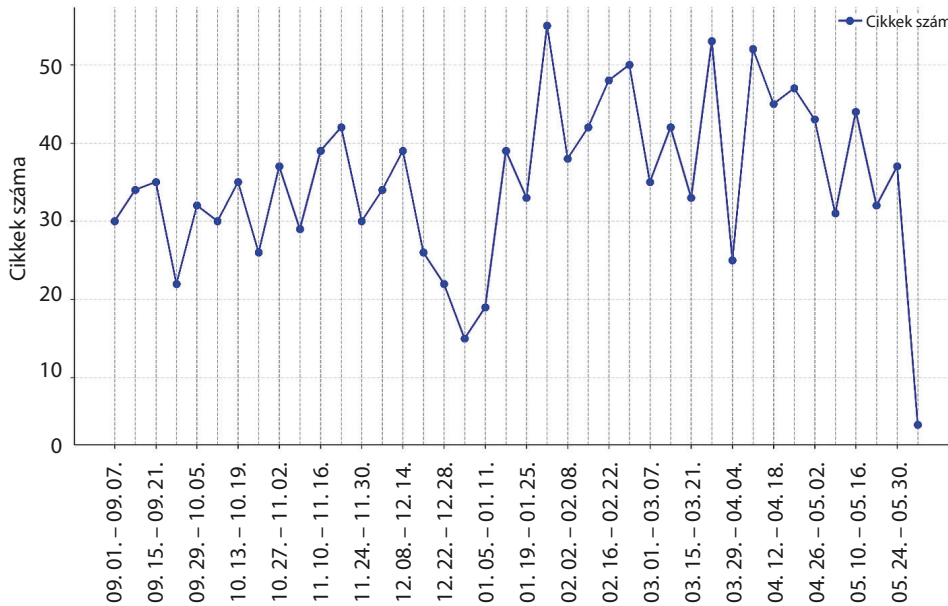
Eredmények

Jelen fejezet a 2023. szeptember 1. és 2024. június 9. közötti időszakban az EUvs Disinfo által dezinformációs kampányként azonosított 1404 eset különböző szempontok szerinti elemzését mutatja be.

Időbeli eloszlás

A 2. ábrán heti bontásban szerepel az álhírek megoszlása. Jól megfigyelhető, hogy a karácsonyi (Gergely- és Julianus-naptár szerinti), újévi időszakban a megjelenő álhírek száma a megelőző hetekhez viszonyítva jelentősen, a húsvéti időszakban pedig kimutathatóan csökkent. (A végdátum tekintetében a csökkenést az okozza, hogy a május 31. és június 9. közötti időszakra a megadott paraméterek szerint az oldal mindösszesen 4 cikket indexált.)

[22] Leite et al. 2024.



2. ábra: A dezinformációs tartalmak megjelenése heti bontásban

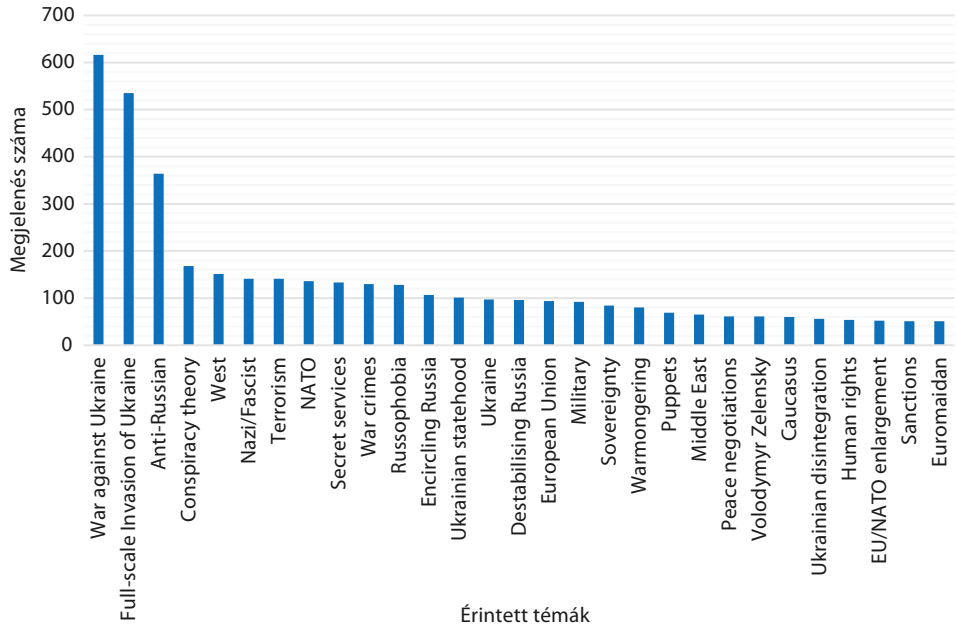
Forrás: https://euvsdisinfo.eu/disinformation-cases/?date=01.09.2023%20-%2009.06.2024 alapján a szerző szerkesztése

Témák és kulcsszavak

A 3. ábrán azon leggyakrabban megjelenő témák szerepelnek, amelyek legalább 50 alkalommal elemként fordultak elő valamely eset vonatkozásában.
A leggyakoribb témák között (40-nél több esetben) megjelennek továbbá a „War preparation", „Colour revolutions", „Democracy", „Maria Zakharova", „Imperialism/colonialism" és „Nuclear issues" kulcsszavak. Összességében az 1404 cikk kapcsán mintegy 170 különböző témakör azonosítható.

Ezen eredmények tekintetében vizsgáltam továbbá a témakapcsolatokat, hogy feltárjam, mely témák és kulcsszavak fordulnak elő együtt a dezinformációs cikkekben, és milyen struktúrát alkotnak. Ennek érdekében gráfelemzést alkalmaztam, ahol a csomópontok az egyes cikkekben szereplő témák és tagek voltak, míg az élek azokat a kapcsolatokat jelezték, ahol két téma egy adott cikken belül együtt jelent meg.

Az elemzés során először az eredmények közül kinyertem a kulcsszavakat tartalmazó adatokat, majd társelőfordulási mátrixot készítettem, amely azt mutatta meg, hogy két adott tag hányszor szerepelt együtt egy cikkben. A gráf felépítésekor olyan kapcsolatokat jelenítettem meg, ahol a két tag közötti társelőfordulás legalább 50 esetben azonosítható.



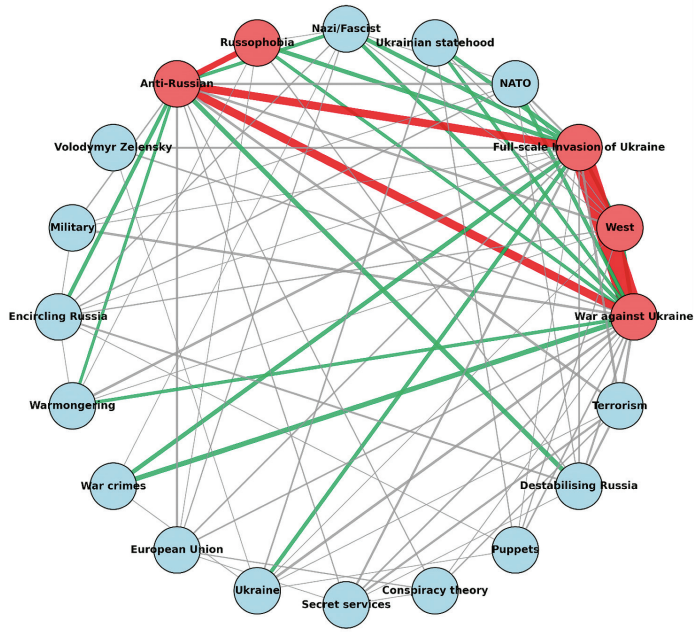
3. ábra: A leggyakoribb témák megjelenésének eloszlása

Forrás: https://euvsdisinfo.eu/disinformation-cases/?date=01.09.2023%20-%2009.06.2024 alapján a szerző szerkesztése

A vizualizáció során az öt leggyakrabban előforduló témát piros színnel emeltem ki, míg a kapcsolatokat az előfordulások száma alapján különböző színnel és vastagsággal jelöltem:

- 50 alatt: szürke kapcsolatjelölés;
- 50–100 között: zöld kapcsolatjelölés;
- 100 felett: piros kapcsolatjelölés.

A gráfelemzés eredményei azt mutatják, hogy a dezinformációs narratívák meghatározott tematikus klaszterek köré szerveződnek, és bizonyos kulcstémák erős központi szerepet töltenek be. A leggyakrabban előforduló tagek jelentős összeköttetéseket mutattak más témákkal, jelezve, hogy ezek a dezinformációs kampányok fő strukturális elemei. Emellett az elemzés arra is rávilágított, hogy bizonyos témák szorosan együtt mozognak – például a címkék közül az oroszellenességet az Ukrajna elleni támadással gyakran együtt alkalmazták. Ugyanakkor voltak perifériás témák, amelyek csak néhány másik kulcsszóhoz kapcsolódtak, jelezve, hogy ezek a dezinformáció egyedi vagy „szezonális" narratívái lehetnek. Fontos mindezek mellett kiemelni, hogy az ábra magas küszöbértékei elfedhetnek releváns, de ritkább kapcsolatokat, azonban az alkalmazott módszertan maradéktalanul lehetővé teszi specifikusabb, fókuszált elemzések lebonyolítását is, akár több elemből álló mátrixok létrehozását, több kulcsszó, magasabb társelőfordulás implementálásával.



4. ábra: A kulcsszavak társelőfordulási kapcsolatrendszere

Forrás: https://euvsdisinfo.eu/disinformation-cases/?date=01.09.2023%20-%2009.06.2024 alapján a szerző szerkesztése

Összességében az eredmények azt mutatják, hogy a dezinformációs narratívák nem véletlenszerűen épülnek fel, hanem tudatosan strukturált módon, ismétlődő tematikus mintázatok mentén szerveződnek. Az erősen összekapcsolódó témák és az egyes narratívák közötti szoros kapcsolatok azt sugallják, hogy ezeket a diskurzusokat előre meghatározott célok mentén alakítják ki és terjesztik.

Fontosnak tartom továbbá kiemelni, hogy jelen (és természetesen a szofisztikáltabb) elemzési módszertan lehetővé teszi a dezinformációs narratívák rendszerezett elemzését és vizualizálását, amelynek segítségével átfogó képet kaphatunk arról, hogy a különböző témák hogyan kapcsolódnak egymáshoz, milyen módon szerveződnek hálózatokba, és melyek azok a központi elemek, amelyek a dezinformációs kampányok magját képezik. Az ilyen típusú elemzések egyik legnagyobb előnye, hogy általuk feltárhatók a rejtett mintázatok, amelyek első ránézésre nem egyértelműek. Ha egy adott téma mindig ugyanazokkal a kulcsszavakkal társul, akkor az előre meghatározott narratívák azonosíthatóvá válnak, és ezek nyomon követhetők az időben. Ez különösen fontos a dezinformáció elleni küzdelemben, hiszen így nemcsak az egyes hamis állításokat lehet cáfolni, hanem azokat a szisztematikus struktúrákat is fel lehet térképezni, amelyeken keresztül a dezinformáció terjed. Ezen túlmenően a módszertan alkalmazkodó és bővíthető, hiszen új témák, kulcsszavak és források bevonásával folyamatos finomhangolás végezhető. Ha például új geopolitikai események hatására megváltozik a dezinformációs diskurzus szerkezete, az ilyen hálózatelemzések segíthetnek gyorsan azonosítani az új narratívákat és azok potenciális hatásait a közvéleményre.

A vizualizációs megközelítés nemcsak az elemzők számára teszi könnyebben értelmezhetővé a dezinformációs mintázatokat, hanem akár döntéshozók, újságírók vagy médiaelemzők számára is jól hasznosítható eszközt nyújt. A gráfok és kapcsolati hálók ábrázolásával átláthatóbbá válik, hogy a dezinformációs kampányok nem elszigetelt jelenségek, hanem jól szervezett, összehangolt kommunikációs stratégiák, amelyek meghatározott célokat szolgálnak. A módszertan tehát nemcsak akadémiai és kutatási szempontból jelentős, hanem gyakorlati előnyökkel is bír, hiszen lehetőséget teremt a dezinformáció elleni proaktív fellépésre, a káros narratívák szerkezeti feltárására és a hatékony ellenintézkedések kidolgozására.

Országok és régiók

Az 5. ábrán a kutatás időtartamában a dezinformációs kampányokban szereplő országok megjelenítése látható. Ennek érdekében térképes vizualizációt alkalmaztam, amely lehetővé tette, hogy az egyes országok dezinformációs diskurzusban betöltött szerepét szemléletesen ábrázoljam. Az elemzés során a dezinformációs cikkekben említett országokat összesítettem, majd az előfordulási gyakoriság alapján színkódolt térképet készítettem.

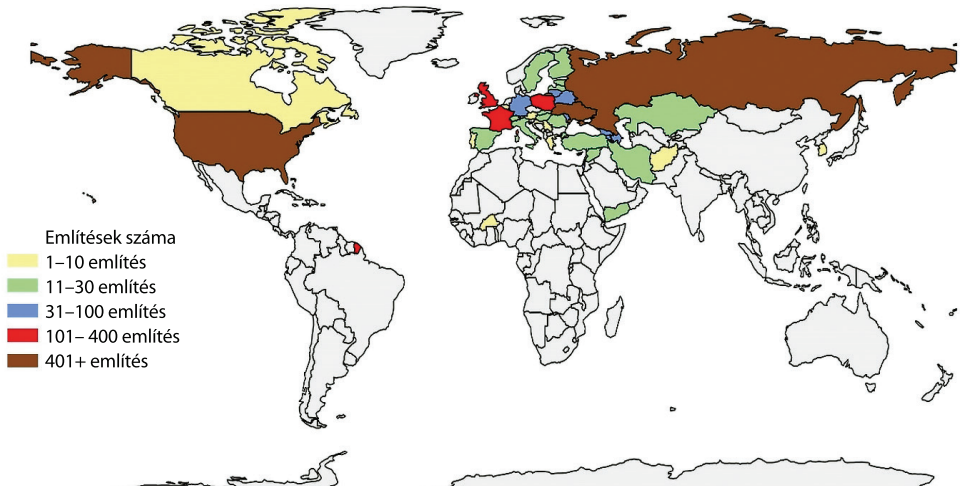
A színezésnél külön kategóriákat határoztam meg:

- 1–10 említés: sárga;
- 11–30 említés: zöld;
- 31–100 említés: kék;
- 101–400 említés: piros;
- 401-nél több említés: barna.

Az eredmények alapján jól látható, hogy bizonyos országok – például Oroszország, Ukrajna, az Egyesült Államok és több európai ország – kiemelten gyakran szerepelnek a dezinformációs narratívákban.

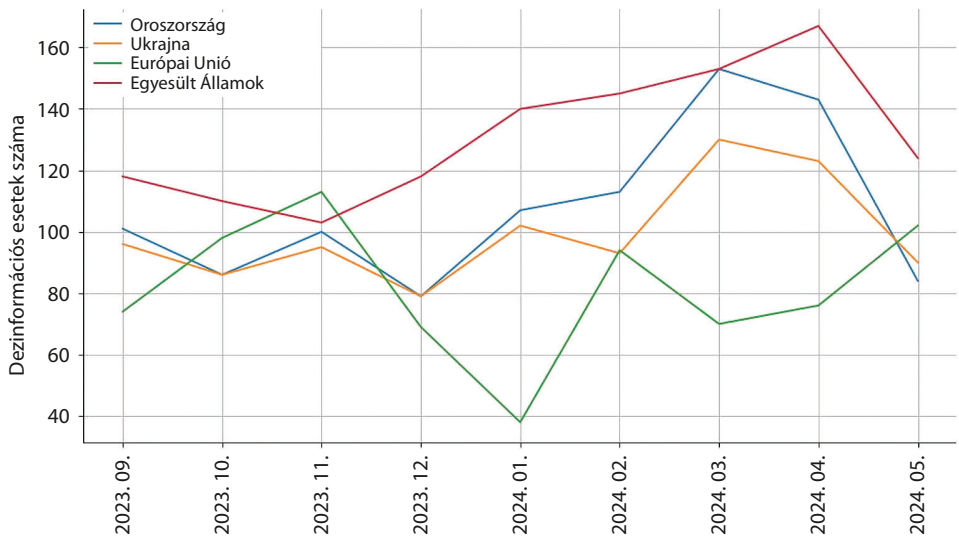
Ezen elemzési módszertan alapján célom volt térbeli perspektívába helyezni, hogy mely országok a leginkább érintettek a megjelenő tartalmak vonatkozásában. A vizualizáció lehetővé teszi, hogy gyorsan és hatékonyan azonosíthatók legyenek a földrajzi fókuszpontok, ami előremutató lehet a jövőbeli kutatások szempontjából, például a scope szűkítésének viszonylatában.

Az országok önálló megjelenítését tekintve azonban fontos kiemelni, hogy az az Európai Uniót mint önálló entitást, illetve a különböző narratívákban megjelenő területet nem tartalmazza. Ezen hiányosság kiküszöbölése, valamint az EU relevanciájának kihangsúlyozása érdekében a 6. ábrán Oroszország, Ukrajna és az Amerikai Egyesült Államok (mint a három legtöbbet említett ország) mellett szerepel az EU az esetszámok időbeli eloszlásának viszonylatában.



5. ábra: A dezinformációs tartalmakban megjelenő országok vizualizációja

Forrás: https://euvsdisinfo.eu/disinformation-cases/?date=01.09.2023%20-%2009.06.2024 alapján a szerző szerkesztése



6. ábra: Oroszország, Ukrajna, az Amerikai Egyesült Államok és az Európai Unió esetszámainak időbeli eloszlása, havi bontásban

Forrás: https://euvsdisinfo.eu/disinformation-cases/?date=01.09.2023%20-%2009.06.2024 alapján a szerző szerkesztése

421 esetszámmal jól látható, hogy a tartalmakban legtöbbször megjelenő országokkal az EU önállóan is paritásban van, amennyiben pedig ezen esetszámhoz hozzáadjuk a különböző EU-s tagállamok vagy kapcsolódó országok/régiók (például a balti államok) egyedüli megjelenését, úgy az érték 1334 említésre emelkedik.

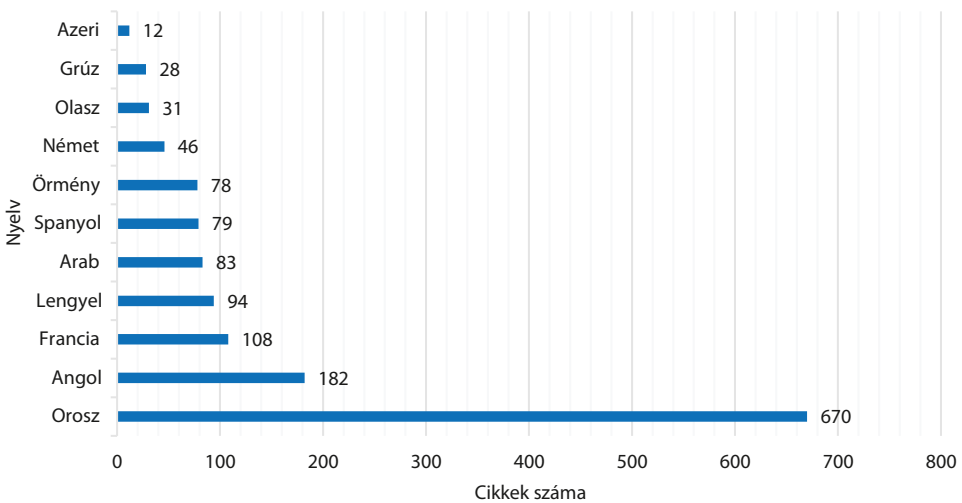
Mindennek kapcsán látható, hogy a dezinformációs kampányok milyen mértékben összpontosítanak nemcsak egyes országokra, hanem az EU egészére is mint önálló célpontra. Az, hogy az EU a három leggyakrabban említett ország mellett hasonló vagy nagyobb mértékben szerepel a dezinformációs narratívákban, azt mutatja, hogy a Kreml-barát dezinformáció egyik központi célja az EU hiteltelenítése, destabilizálása és megosztása.

Az eredmény azért is fontos, mert segít megérteni a dezinformációs kampányok geopolitikai céljait és azok hosszú távú következményeit. Az ilyen jellegű elemzések lehetőséget biztosíthatnak arra, hogy a politikai döntéshozók és biztonsági szakértők jobban felkészülhessenek a dezinformációs fenyegetésekre, és célzottabb stratégiákat dolgozhassanak ki az információs tér védelmére. Az EU mint egység kiemelt célpontként való kezelése megerősíti, hogy a dezinformáció nem csupán egyes országokat érintő probléma, hanem szélesebb, regionális és globális hatásokkal is bír, amelyeket komplex módon kell kezelni.

Nyelvi megoszlás

Az eredeti cikkek megjelenési szövegének nyelvi megoszlását tekintve 12 különböző nyelvet azonosíthatunk. Fontos kiemelni azonban, hogy az EUvsDisinfo platform a megjelent nyelvek tekintetében nem indexálja vagy követi nyomon azon híreket, amelyeket átvettek más online felületek, vagy amelyek az első megjelenését követték. Emellett azonban vannak olyan elemek, amelyek kapcsán több megjelenési nyelv is azonosítható, illetve ahol egyetlen nyelv sem adható meg kizárólagosként.

Mindennek vonatkozásában a nyelvi megoszlásra vonatkozó adatokat a 7. ábra tartalmazza.



7. ábra: A dezinformációt tartalmazó cikkek nyelvi megoszlása

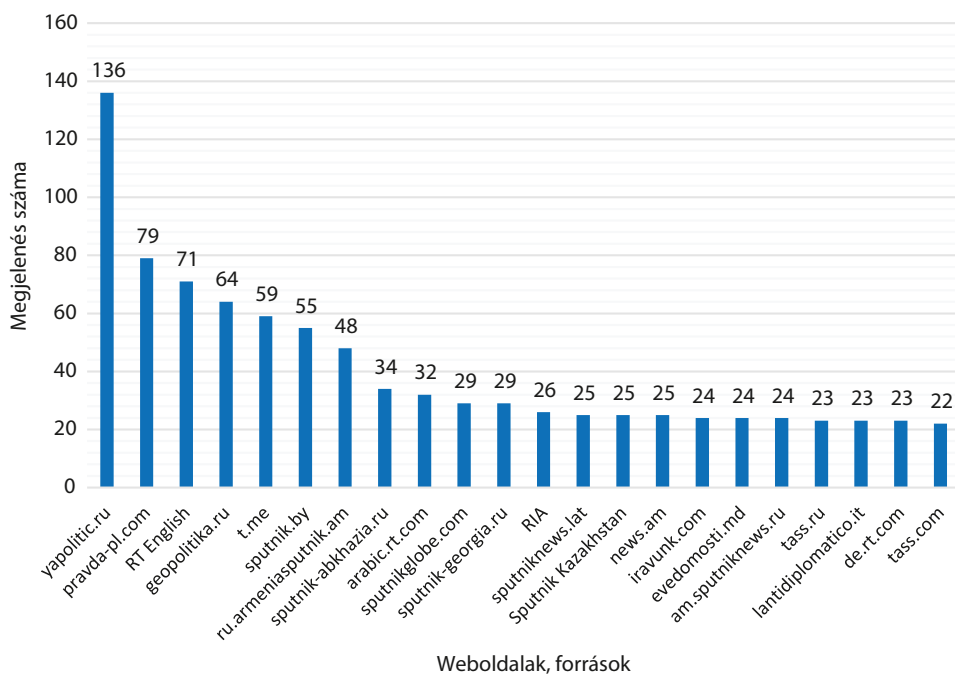
Forrás: https://euvsdisinfo.eu/disinformation-cases/?date=01.09.2023%20-%2009.06.2024 alapján a szerző szerkesztése

Hírforrások

A dezinformációs kampányok egyik legfontosabb eleme a hírforrások *(outletek)* hálózata, amelyeken keresztül a hamis vagy félrevezető információk terjednek. Ezek az *outletek* jelentős szerepet játszanak a narratívák formálásában, a közvélemény befolyásolásában, valamint a célzott országok és közösségek manipulálásában. A különböző médiumok eltérő stratégiákat alkalmazhatnak a dezinformáció terjesztésére. Egyesek közvetlen propagandaeszközként működnek, mások hírportálként álcázva finoman torzítják a tényeket, vagy szelektíven válogatják meg a közölt információkat. Az *outletek* egy része kifejezetten egy adott nyelvű közönséget céloz meg, míg mások több nyelven, nemzetközi szinten is működnek, lehetővé téve a dezinformáció széles körű terjesztését.

A terjesztési hálózatok vizsgálata, a terjesztő platformok azonosítása segít feltárni, hogy mely médiumok vesznek részt leginkább a dezinformációs kampányokban, mely országokat célozzák meg a tartalmaikkal, és milyen narratívák dominálnak az egyes oldalakon. A hírforrások elemzése lehetőséget ad annak azonosítására, hogy mely médiumok működnek összhangban, és hogy a különböző nyelveken elérhető cikkek milyen mértékben térnek el egymástól.

A vizsgált 1404 esetet 79 különböző platformon tették közzé, ezen felületeken pedig eltérő számban fordultak elő dezinformációs tartalmak. A 8. ábra azon forrásokat mutatja be, amelyeken legalább 20 alkalommal jelent meg dezinformációs tartalom a 2023. szeptember 1. és 2024. június 9. közötti időszakban.

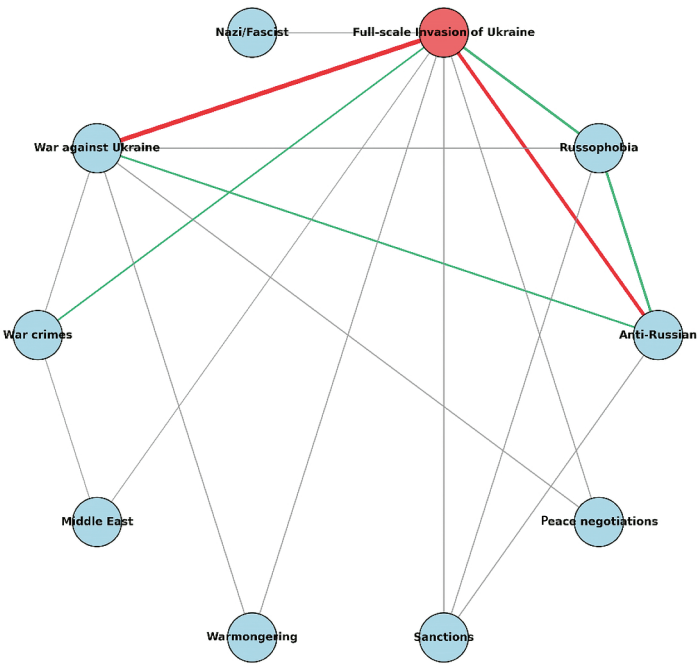


8. ábra: A legtöbb dezinformációt megosztó weboldalak, források

Forrás: https://euvsdisinfo.eu/disinformation-cases/?date=01.09.2023%20-%2009.06.2024 alapján a szerző szerkesztése

A releváns *outletek* (több mint 10 eset indexálása) közé tartoznak a *Rossiya 1*, illetve a Pravda észt és francia, valamint a Sputnik grúz (és oszét) weboldalai.

Ahogy korábban az adatállomány egészére vonatkozóan, úgy a legtöbb esetszámmal rendelkező forrásokat illetően is azonosíthatjuk a leggyakoribb témakapcsolatokat, amennyiben cél a különböző platformokon megjelenő tartalmak vizsgálata, összevetése. Jelen kutatás eredményeit tekintve ezen elemzést a 9. ábra tartalmazza, példaként a forrásokhoz rendelhető témakapcsolatok azonosítására.



9. ábra: Példa a forrásokhoz rendelhető témakapcsolatok azonosítására

Forrás: https://euvsdisinfo.eu/disinformation-cases/?date=01.09.2023%20-%2009.06.2024 alapján a szerző szerkesztése

További kutatási lehetőségek

A 9. ábrán szereplő eredmények viszonylatában további kutatási célkitűzéseket azonosíthatunk, ugyanis a források és a témakapcsolatok vizsgálata mellett lehetőségünk adódik az eredményeket geopolitikai, tematikus, nyelvi, strukturális, regionális és hálózati összefüggések mentén is tovább elemezni, valamint elhelyezni társadalmi, politikai, biztonsági dimenzióban a további vizsgálatok szempontjából.

Összességében tehát elmondható, hogy az adatbázis megannyi lehetőséget biztosít a dezinformációs tartalmak mélyebb vizsgálatára, különösen a különböző narratívák, hírforrások, nyelvek, földrajzi eloszlás és időbeli trendek elemzése révén. A jelen tanulmányban bemutatott elemzések csupán egy szeletét jelentik annak

a sokrétű megközelítésnek, amely az adatbázisból kinyerhető információkat vizsgálhatja. A további kutatások az alábbi irányokban folytathatók.

Időbeli trendek és dinamikák részletes vizsgálata

- A dezinformációs hullámok azonosítása különböző időszakokban; korreláció más eseményekkel (például geopolitikai eseményekkel, háborús fejleményekkel, választásokkal, EU-s intézkedésekkel, politikai kampányokkal).
- Időszakos intenzitásvizsgálat: azonosíthatók-e időbeli mintázatok a dezinformációs kampányokban?

Földrajzi és térbeli elemzések

- A dezinformáció által célba vett országok és régiók változásának vizsgálata.
- Az országok és régiók közötti kapcsolat, például hogy egyes témák milyen földrajzi eloszlásban jelennek meg.
- Egy adott ország milyen szerepet tölt be a dezinformációs kampányokban: célország vagy narratívák aktív közvetítője?
- Térképes vizualizációk finomítása, részletesebb földrajzi hatásvizsgálatok.

Dezinformációs források és terjedési hálózatok feltárása

- A dezinformációs hírforrások elemzése: mely platformok a legaktívabbak?
- Dezinformációs hálózatok vizsgálata: az egyes médiumok kapcsolatrendszere, például mely oldalak hivatkoznak egymásra.
- A különböző nyelvű dezinformációk összehasonlítása: vannak-e eltérések az angol, az orosz vagy más nyelvű tartalmak között?
- *Outletek* tematikus specializációja: mely témák dominálnak egyes hírportálokon?

Témakapcsolatok és narratívák összefüggései

- A dezinformációs témák mélyebb hálózati elemzése, például:
  - Mely témák fordulnak elő együtt a legtöbbször?
  - Hogyan változik a narratívák összetétele az idő múlásával?
  - Vannak-e visszatérő tematikus mintázatok?
- Kulcsfogalmak és szóhasználati minták azonosítása: egyes témák milyen kontextusban jelennek meg?
- Dezinformációs és valós hírek összevetése: mely narratívák jelennek meg a fősodratú médiában is?

Mesterséges intelligencia és gépi tanulás alkalmazása

- Automatizált narratívaelemzés természetes nyelvi feldolgozással (NLP).
- Tartalom osztályozása gépi tanulási modellekkel: dezinformációk automatikus kategorizálása témák szerint.
- Tartalmi hasonlóságok elemzése: hasonló szövegstruktúrák vagy minták keresése különböző források között.
- AI-eszközök (például LLM-alapú terjesztés, *deepfake* narratívák) potenciáljának elemzése.
- Szentimentelemzés: a dezinformációs narratívák érzelmi töltetének mérése.

A dezinformáció hatásának vizsgálata

- Közösségi média elemzése: hogyan terjednek ezek a narratívák a különböző platformokon (Twitter, Telegram, YouTube stb.)?
- Reagálási mechanizmusok: milyen EU-s vagy civil kezdeményezések foglalkoznak ezen tartalmak cáfolásával?
- Hatásvizsgálat: milyen visszhangjuk van ezeknek a híreknek a közvéleményben?

Diszkusszió

Összességében megállapítható, hogy noha az EU álhírekkel és dezinformációval szemben hozott intézkedései jelentős előrelépést hozhatnak, önmagukban nem elégségesek a jelenség hatékony kezelésére. Az EU intézkedései sikeresen ösztönzik a nagy technológiai platformokat az átláthatóság növelésére és a tartalmak szigorúbb moderálására, azonban a szabályozási környezet gyakorlati végrehajtása továbbra is kihívásokkal teli, különösen az önszabályozó mechanizmusok korlátai miatt.

Az empirikus elemzés eredményei alapján elmondható, hogy a vizsgált időszakban megjelenő dezinformációs kampányok szisztematikusan strukturáltak, és jól körülhatárolható tematikus hálózatokba szerveződnek. A narratívák közötti kapcsolatok kimutatása megerősíti azt a feltételezést, hogy a dezinformáció nem ad hoc jelenség, hanem előre megtervezett stratégia és tervezés mentén zajlik. Az eredmények alapján az EU nemcsak önálló célpontja, hanem – a geopolitikai kontextus következtében – egyik központi áldozata is ezeknek a narratíváknak. A földrajzi és nyelvi elemzés kapcsán látható ugyanis, hogy Oroszország és Ukrajna mellett az Egyesült Államok és az EU tagállamai kiemelt szereplői az orosz narratívájú dezinformációs diskurzusnak. Ez megerősíti, hogy a dezinformációs kampányok a geopolitikai konfliktusok kiegészítő, információs dimenzióját képezik, célzottan gyengítve az európai társadalmak stabilitását és a demokratikus intézmények iránti bizalmat.

Fontos felismerés továbbá, hogy a dezinformáció sikeres terjedését nem pusztán technológiai, hanem elsősorban emberi tényezők (például érzelmi hatások, meglepetésfaktor, preferált információfogyasztási szokások) határozzák meg, ezáltal a jelenség

elleni hatékony fellépés alapja nemcsak jogi és technológiai eszközök, hanem elsősorban társadalmi-pszichológiai és oktatási megközelítések integrált alkalmazása lehet.

A jövőbeni kutatások egyik kulcsterülete tehát a szabályozási intézkedések gyakorlati végrehajtásának monitorozása, valamint az emberi tényezők mélyebb vizsgálata lehet, különös tekintettel a médiaértés, a kritikai gondolkodás és a társadalmi reziliencia fejlesztésére. Ezen túlmenően szükséges a jelen kutatás során bemutatott elemzési módszertan további finomítása, ami segíthet a narratívák változásainak gyors és hatékony nyomon követésében, ezáltal támogatva az EU proaktív védekezését a dezinformációs fenyegetésekkel szemben.

Felhasznált irodalom

Allcott, Hunt – Gentzkow, Matthew (2017): Social Media and Fake News in the 2016 Election. *Journal of Economic Perspectives,* 31(2), 211–236. Online: https://doi.org/10.1257/jep.31.2.211

Berdud, Carlos Espaliú (2024): The EU Code of Practice on Disinformation. An Example of the Self-Regulatory Trend in International and European Law. *VISUAL Review, International Visual Culture Review / Revista Internacional de Cultura,* 16(2), 95–109. Online: https://doi.org/10.62161/revvisual.v16.5217

Bradshaw, Samantha – Howard, Philip N. (2019): *The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation.* Oxford: University of Oxford. Online: https://digitalcommons.unl.edu/scholcom/207/

Brogi, Elda – De Gregorio, Giovanni (2024): From the Code of Practice to the Code of Conduct? Navigating the Future Challenges of Disinformation Regulation. *Journal of Media Law,* 16(1), 38–46. Online: https://doi.org/10.1080/17577632.2024.2362480

Cinelli, Matteo et al. (2021): The Echo Chamber Effect on Social Media. *Proceedings of the National Academy of Sciences,* 118(9), e2023301118. Online: https://doi.org/10.1073/pnas.2023301118

Colomina Saló, Carme – Pérez-Soler, Susana (2022): Information Disorder in the European Union: Building a Regulatory Response. *Revista CIDOB d'Afers Internacionals,* (131), 141–161. Online: https://doi.org/10.24241/rcai.2022.131.2.141

De Bruin, Kiki et al. (2021): News Avoidance during the Covid-19 Crisis: Understanding Information Overload. *Digital Journalism,* 9(9), 1286–1302. Online: https://doi.org/10.1080/21670811.2021.1957967

Del Vicario, Michela et al. (2016): The Spreading of Misinformation Online. *Proceedings of the National Academy of Sciences,* 113(3), 554–559. Online: https://doi.org/10.1073/pnas.1517441113

EEAS Launches a New Tool to Help Navigate in Disinformation Environment. *EEAS,* 2022. október 20. Online: www.eeas.europa.eu/delegations/ukraine/eeas-launches-new-tool-help-navigate-disinformation-environment_en

European Commission [é. n. a]: *Fighting Disinformation.* Online: https://commission.europa.eu/strategy-and-policy/coronavirus-response/fighting-disinformation_en
European Commission [é. n. b]: *The Code of Practice on Disinformation (2022).* Online: https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation
European Commission (2022): *2022 Strengthened Code of Practice on Disinformation.* 2022. június 16. Online: https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation
Ferrara, Emilio et al. (2016): The Rise of Social Bots. *Communication of the ACM,* 59(7), 96–104. Online: https://doi.org/10.1145/2818717
Fletcher, Richard – Nielsen, Rasmus Kleis (2017) Are People Incidentally Exposed to News on Social Media? A Comparative Analysis. *New Media & Society,* 20(7), 2450–2468. Online: https://doi.org/10.1177/1461444817724170
Gorwa, Robert – Binns, Reuben – Katzenbach, Christian (2020): Algorithmic Content Moderation: Technical and Political Challenges in the Automation of Platform Governance. *Big Data & Society,* 7(1). Online: https://doi.org/10.1177/2053951719897945
Leite, João A. et al. (2024): EUvsDisinfo: a Dataset for Multilingual Detection of Pro-Kremlin Disinformation in News Articles. *ArXiv,* 2024. június 18. Online: https://arxiv.org/html/2406.12614v1
Managing the COVID-19 Infodemic: Promoting Healthy Behaviours and Mitigating the Harm from Misinformation and Disinformation. *WHO,* 2020. szeptember 23. Online: www.who.int/news/item/23-09-2020-managing-the-covid-19-infodemic-promoting-healthy-behaviours-and-mitigating-the-harm-from-misinformation-and-disinformation
Newman, Nic et al. (2021): *Reuters Institute Digital News Report 2021. 10th Edition.* Online: https://doi.org/10.60625/risj-7khr-zj06
Shao, Chengcheng et al. (2018): The Spread of Low-Credibility Content by Social Bots. *Nature Communications,* 9(1), 4787. Online: https://doi.org/10.1038/s41467-018-06930-7
Tandoc Jr., Edson C. et al. (2018): Defining „Fake News". A Typology of Scholarly Definitions. *Digital Journalism,* 6(2), 137–153. Online: https://doi.org/10.1080/21670811.2017.1360143
To Challenge Russia's Ongoing Disinformation Campaigns: Eight Years of EUvsDisinfo. *EUvsDisinfo,* 2023. július 5. Online: https://euvsdisinfo.eu/to-challenge-russias-ongoing-disinformation-campaigns-eight-years-of-euvsdisinfo/
Vosoughi, Soroush et al. (2018): The Spread of True and False News Online. *Science,* 359(6380), 1146–1151. Online: https://doi.org/10.1126/science.aap9559
Wardle, Claire – Derakhshan, Hossein (2017): *Information Disorder: Toward an Interdisciplinary Framework for Research and Policymaking.* Strasbourg: Council of Europe. Online: http://tverezo.info/wp-content/uploads/2017/11/PREMS-162317-GBR-2018-Report-desinformation-A4-BAT.pdf

Jogi források

Az Európai Parlament és a Tanács (EU) 2022/2065 rendelete (2022. október 19.) a digitális szolgáltatások egységes piacáról és a 2000/31/EK irányelv módosításáról (digitális szolgáltatásokról szóló rendelet). Online: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32022R2065

Az Európai Parlament és a Tanács (EU) 2024/900 rendelete (2024. március 13.) a politikai reklámtevékenység átláthatóságáról és célzott folytatásáról. Online: https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=OJ:L_202400900

HADMÉRNÖK
VÉDELEMINFORMATIKA

20. évfolyam (2025) 1. szám 73–85.
DOI: 10.32567/hm.2025.1.4

Farkas Gábor,[1] Fazekas Gábor[2]

Ipari vezérlőrendszerek sebezhetősége

A Modbus protokollon keresztül történő támadások elleni védekezés lehetőségei

Vulnerability of Industrial Control Systems

Defence Possibilities Against Attacks over Modbus Protocol

Absztrakt

A PLC-k és a SCADA-rendszerek már évtizedek óta növelik az ipari rendszerek hatékonyságát azáltal, hogy vezérlésüket könnyen programozható és felügyelhető módon valósítják meg. Napjainkban ezek az eszközök nélkülözhetetlenek, és jelen vannak minden ipari létesítményben, legyen az termelőüzem, energiatermelő egység vagy forgalomirányító rendszer. A technológia fejlődésével lehetőség nyílt ezen rendszerek hálózatba szervezésére, ami tovább fokozta hatékonyságukat, ugyanakkor növelte a kibertámadásoknak való kitettségüket is. Tekintettel arra, hogy a kritikus infrastruktúra számos elemében működtetnek ilyen eszközöket, fontos hangsúlyt fektetni azok támadással szembeni ellenálló képességére. Tanulmányunkban górcső alá vesszük a jellemző támadási pontokat és az azok védelmére tett kísérleteket. Célunk átfogó képet adni a sérülékenység okairól és a lehetséges védelmi megoldásokról, továbbá bemutatni egy általunk megvalósított, AI-alapú védelmi lehetőséget, ami hozzájárulhat az ipari rendszerek védelméhez és prediktív karbantartásához.

Kulcsszavak: PLC, SCADA, kibertámadás, kritikus infrastruktúra, AI

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola, e-mail: farkas.gabor.csp@gmail.com
[2] Doktori hallgató, Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola, e-mail: fazekg@gmail.com

Abstract

For decades, PLCs and SCADA systems have been enhancing the efficiency of industrial systems by enabling their control in a way that is easily programmable and monitorable. Today, these tools are indispensable and present in every industrial facility, whether it be a manufacturing plant, power generation unit or traffic control system. With technological advancements the networking of these systems has become possible, further increasing their efficiency. However, this has also heightened their exposure to cyberattacks. Given that many elements of critical infrastructure rely on these devices, it is crucial to emphasize their resilience against attacks. In our study, we examine the typical attack points and efforts to protect against them. Our goal is to provide a comprehensive overview of the causes of vulnerabilities and potential defense solutions. Furthermore, we aim to present our AI-based defensive solution that we implemented and can provide the opportunity for the protection and predeictive maintenance of industrial systems.

Keywords: PLC, SCADA, cyber-attack, critical infrastructure, AI

Bevezetés

Az ipari vezérlőrendszerek (*industrial control systems,* ICS) fejlődése nagyban hozzájárult az ipari automatizálás elterjedéséhez és hatékonyságának növekedéséhez. Ezek a rendszerek, különösen a PLC-k (*programmable logic controllers* – programozható logikai vezérlő) és a SCADA (*supervisory control and data acquisition* – felügyeleti ellenőrző és adatgyűjtő) rendszerek, központi szerepet játszanak a termelési folyamatok irányításában és felügyeletében. A PLC-k a különböző ipari berendezések vezérléséért felelnek, míg a SCADA-rendszerek távoli hozzáférést és felügyeleti képességeket biztosítanak, lehetővé téve a rendszerek valós idejű monitorozását és irányítását. A technológiai fejlődésnek köszönhetően ezek a rendszerek egyre inkább hálózatba szerveződnek, ami lehetővé teszi a távoli hozzáférést és irányítást, egyúttal növeli a kibertámadások kockázatát is. A SCADA-rendszerek rendkívül lényegesek a kritikus infrastruktúrák szempontjából, azok kibervédelme kulcsfontosságú, hiszen a működésükben fellépő zavarok súlyos gazdasági és biztonsági következményekkel járhatnak.[3] A kiberbiztonsági kihívások nehézségét tovább fokozza az Ipar 4.0 keretében megvalósuló, a rendszerelemek teljes mértékű hálózatba kapcsolása, többek között az Internet of Things (IoT) elterjedése. Ilyen módon globális méretű hálózatok alakulnak ki, amelyek növelik a támadási felületet. A támadások egyre gyakoribbak és összetettebbek, különösen az olyan célzott támadások, mint a Stuxnet, amely komoly károkat okozhat fizikai infrastruktúrákban is.[4] Tanulmányunk célja, hogy bemutassa a PLC-k és a SCADA-rendszerek főbb sebezhetőségeit, a támadási módszereket és a védekezési lehetőségeket. Különösen a kritikus infrastruktúrák biztonsága áll a középpontban, és arra törekszünk, hogy átfogó képet adjunk a lehetséges megoldásokról, amelyekkel megvédhetjük ezeket a rendszereket

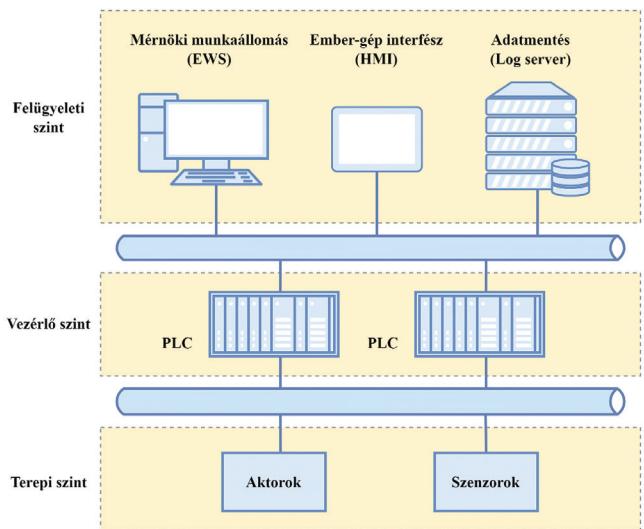
[3] Haig et al. 2009: 48–51.
[4] Sommestad–Ericsson–Nordlander 2010: 1.

a kiberfenyegetésekkel szemben. Ezen túlmenően bemutatunk egy általunk kutatott AI-alapú védelmi megoldást, amely segíthet a Modbus protokollon keresztül történő támadások és szenzormeghibásodások észlelésében. Ez magában foglalja egy konfigurálható neurális hálózat kialakítását, annak tanítását és vizsgálatát.

A PLC-k és a SCADA-rendszerek szerepe

A PLC egy speciális mikroszámítógép, amelyet kifejezetten ipari folyamatok irányítására és automatizálására terveztek.[5] Alapvető funkciója, hogy a szenzoroktól érkező jeleket fogadja, majd ezek alapján meghatározza a szükséges kimeneti állapotokat, amit továbbít a működtető eszközök felé, például motorok, szelepek, fűtőelemek vagy más ipari berendezések vezérlése céljából. A PLC-k tehát közvetlen kapcsolatban állnak az ipari folyamatokkal, és a legfontosabb szerepük ezek közvetlen automatizálása és felügyelete.

A SCADA-rendszerek a PLC-k és más vezérlő rendszerelemek felügyeletére és irányítására szolgálnak. Jellemzően egy központi vezérlő számítógépből, egy operátori állomásból és különböző adatgyűjtő eszközökből épülnek fel (1. ábra).[6] Ezek a megoldások lehetővé teszik, hogy az ipari folyamatokat távolról is figyelemmel lehessen kísérni és szükség esetén beavatkozni. A rendszer összegyűjti az adatokat a terepi eszközökről, és ezeket valós időben továbbítja az operátori felügyeletre. Alkalmazásuk kiterjed az ipari gyártásra, az energiatermelésre, a közművekre, mint például a víz- és gázellátás, valamint a közlekedési hálózatok irányítására is.



1. ábra: Egy általános ICS felépítése
Forrás: Geng et al. 2024: 8388 alapján a szerzők szerkesztése

[5] Allison et al. 2020: 1–2.
[6] Yalçın–Çakır–Ünaldı 2024: 39550–39551.

A PLC-k és a SCADA-rendszerek létfontosságúak az ipari folyamatok hatékony és biztonságos irányítása szempontjából. Lehetővé teszik a folyamatok automatizálását, ennek révén csökkenthetők az emberi hibák, növelhető a termelési hatékonyság, valamint biztosítható a folyamatok tervezett és zavartalan működése. Azonban a nagymértékű hálózatba szervezés egyre nagyobb kihívásokat is jelent, különösen a kiberbiztonsági fenyegetések tekintetében. Az ilyen rendszerek korábban zárt hálózatban működtek, azonban a modern ipari trendek fokozott hálózati összekapcsolódást eredményeztek, ezáltal növelve a támadási felületet, így különösen érzékennyé váltak a kibertámadásokra.[7] A Stuxnet-támadás például rávilágított arra, hogy a PLC-k sebezhetősége komoly fenyegetést jelenthet a kritikus infrastruktúrákra. Ebben az esetben a támadók egy kártékony program segítségével manipulálták az urándúsító centrifugák működését, és hosszú ideig észrevétlenül befolyásolták a rendszer működését.[8] Ez az incidens világszerte felhívta a figyelmet arra, hogy az ipari rendszerek támadások elleni védelme létfontosságú.

Az ipari rendszerek sebezhetősége

Az ipari vezérlőrendszerek, főként a PLC-k és a SCADA-k, rendkívül sebezhetők a kibertámadásokkal szemben, különösen az elmúlt évek technológiai fejlődésének köszönhetően. Az eredetileg zárt hálózatokban működő egységek mára egyre inkább kapcsolódnak a globális hálózatokhoz, ami növeli a sebezhetőséget.[9] A legtöbb ipari rendszer tervezésekor nem volt prioritás a kiberbiztonság, hiszen az üzemszerű működés során fizikailag is izolálva volt a külvilágtól.

A kommunikációs protokollok hiányosságai

A SCADA-rendszerek kommunikációs protokolljainak biztonsági hiányosságai kiemelkedő szerepet játszanak a sebezhetőségében. A Modbus, a DNP3 (Distributed Network Protocol 3 – Elosztott hálózati protokoll 3) és más hasonló protokollok eredetileg nem tartalmaztak beépített biztonsági mechanizmusokat, mivel azok zárt hálózati környezetben működtek. A modern ipari rendszerek azonban jellemzően kapcsolódnak az internethez, ezáltal a támadók távoli hozzáférést szerezhetnek, és kihasználhatják a protokollok gyenge pontjait. Ezek a sebezhetőségek lehetővé teszik, hogy a támadók különböző módszereket alkalmazzanak a rendszerek kompromittálására, például a közbeékelődéses támadásokat *(man-in-the-middle),* amelyek során hamis adatokat továbbíthatnak, illetve megváltoztathatják a rendszer által küldött üzeneteket.

[7] Hankó 2023: 147.
[8] Hankó 2023: 157.
[9] Vásárhelyi 2024: 104.

Támadási típusok és kockázatok

Az egyik leggyakrabban alkalmazott támadási módszer a hamis adatinjekciós támadás *(false data injection,* FDI) amelynek során a támadók manipulálják a szenzorok által küldött adatokat, és így megzavarják a PLC-k által vezérelt fizikai folyamatokat.[10] A FDI-támadások különösen veszélyesek, mivel a rendszer továbbra is úgy működik, mintha minden üzemszerű lenne, miközben a valós fizikai környezet eltér a tervezett működéstől. Egy másik jelentős kockázat a vezérlőprogramok vagy a *firmware* manipulációja.[11] A támadók képesek lehetnek arra, hogy rosszindulatú kódokat juttassanak a PLC-kbe, amelyek megváltoztatják a vezérlő programokat.[12] Ez különösen kritikus lehet olyan ipari környezetekben, ahol a rendszerek közvetlenül kapcsolódnak a fizikai eszközökhöz, mint például az energiatermelés vagy a vízszolgáltatás. A Stuxnet-támadás klasszikus példája annak, hogy milyen pusztító hatást lehet kiváltani a sebezhetőségek kihasználásával. Ebben az esetben a támadók rosszindulatú kódot juttattak be a Siemens gyártmányú PLC-kbe, amelyek irányították az iráni urándúsító centrifugákat, és megzavarták azok működését. Az ilyen FDI-támadások viszonylag egyszerűen kivitelezhetők, így meglátásunk szerint jelentős kockázatot hordoznak magukban.

Tervezési hiányosságok és kulturális tényezők

Az ipari rendszerek tervezési hiányosságai gyakran a fejlesztési prioritásokból adódnak. Az ipari vezérlőrendszereket sokszor gépész- és automatizálási mérnökök tervezik, akik elsődlegesen a funkcionális folyamatokra és az automatizálásra összpontosítanak, nem pedig a kiberbiztonságra. Ennek eredményeként a rendszerek gyakran olyan egyszerű megoldásokra támaszkodnak, amelyek nem tartalmaznak megfelelő biztonsági elemeket, mivel ebben a környezetben a biztonsági funkciók hozzáadása növelheti a költségeket, és bonyolultabbá teheti a rendszerek üzemeltetését.[13] A tervezési hiányosságok mellett kulturális tényezők is szerepet játszanak a rendszerek sebezhetőségében. Sok ipari rendszer esetében a kiberbiztonság nem része a vállalati kultúrának, különösen olyan iparágakban, ahol a fő hangsúly a termelési hatékonyságon van. A biztonsági intézkedések bevezetése gyakran költséges és időigényes, így a vezetők és a mérnökök hajlamosak figyelmen kívül hagyni ezeket a kockázatokat. Tapasztalataink szerint az információbiztonsági szempontokat a kivitelezés szűk határideje is háttérbe szoríthatja, így a PLC esetében az alapvető hozzáférést megakadályozó jelszavakat sem állítják be.

[10] Dér 2024: 52–53.
[11] Malchow et al. 2015: 326–327.
[12] Yang–Cheng–Chuah 2018: 2–3.
[13] Patel–Bhatt–Graham 2009: 139.

A kritikus infrastruktúrák kockázatai

A PLC-k és a SCADA-rendszerek sebezhetősége különösen fontos a kritikus infrastruktúrák szempontjából, például az energiahálózatok, a vízellátó és a forgalomirányító rendszerek esetében. Ezek az infrastruktúrák elengedhetetlenek a modern társadalmak működésének aspektusából, amelyekben a kibertámadás hatására fellépő üzemzavar súlyos következményekkel járhat, beleértve az energiaellátás megszakítását, a vízhiányt vagy akár közlekedési káoszt. Az energiahálózatok különösen veszélyeztetettek, mivel ezek függési viszonyban vannak egymással, és így nagyobb eséllyel válnak támadások célpontjává. A tárgyalt rendszerek alapvető fontosságúak az energiatermelés, -elosztás és -fogyasztás szabályozásában.[14] Más területeken fellépő üzemzavar is kritikus lehet, amire jó példa a Maroochy vízszolgáltatót ért támadás, amelyet egy korábbi alkalmazott sikeresen hajtott végre. Ennek során több millió liter szennyvíz ömlött ki a környező területre, ami jelentős környezeti és gazdasági károkat okozott.[15]

Védelmi törekvések

Az ipari vezérlőrendszerek kibertámadások elleni védelme összetett kihívás, amely számos védelmi mechanizmus alkalmazását igényli. A fizikai védelemtől kezdve a tűzfalakon, behatolásészlelő rendszereken (*intrusion detection system,* IDS) át egészen a mesterséges intelligencia (*artificial intelligence,* AI) alapú anomáliadetektálásig számos megközelítés létezik.[16] Az AI-alapú megoldások különösen hatékonynak bizonyulnak, mivel képesek a rendszerek valós idejű monitorozására és az anomáliák automatikus felismerésére, ami potenciális támadásokra utalhat.[17]

Fizikai védelem és hagyományos tűzfalak

Az ipari rendszerek elsődleges védelmi vonala a fizikai hozzáférés ellenőrzése, amely biztosítja, hogy csak jogosult személyek befolyásolhassák a működésüket. Az ilyen rendszerek esetében fontos, hogy a fizikai hozzáférést szigorúan ellenőrizzék, különösen olyan helyeken, mint az erőművek, a víztisztítók vagy a közlekedési csomópontok.[18] Ezen túlmenően a hagyományos hálózati védelmi megoldások, mint például a tűzfalak, továbbra is kulcsfontosságúak. A tűzfalak a hálózati hozzáférést szabályozva megakadályozzák az illetéktelen kapcsolatokat és behatolásokat. Az alapvető csomagszűrő tűzfalaktól az állapotalapú és alkalmazásrétegbeli tűzfalakig a rendszerek különböző hálózati védelmi funkciókat látnak el, amelyek biztosítják, hogy csak a megbízható és engedélyezett forgalom érhesse el az infrastruktúrákat. A fizikai védelem szó szerint is értelmezhető. Léteznek megoldások, amikor valóban fizikailag, közvetlenül

[14] Kralovánszky 2019: 44.
[15] Slay–Miller 2008: 74–75.
[16] Aldossary–Ali–Alasaadi 2021: 742.
[17] Yalçın–Çakır–Ünaldı 2024: 39557.
[18] Bognár–Bonnyai–Vámosi 2019: 98.

kell az eszközön engedélyezni például egy firmware frissítést. Ez nagyban megnehezíti a támadó dolgát, viszont a tervezett műveletet is, így meglátásunk szerint ennek alkalmazását mérlegelni szükséges. Jelentős kockázatú rendszerek esetén érdemes lehet közvetlen emberi beavatkozástól függővé tenni minden jelentős változtatás engedélyezését.

AI-alapú anomália detektálása

A mesterségesintelligencia-alapú megoldások az utóbbi években jelentős fejlődésen mentek keresztül, és ma már kulcsfontosságú szerepet játszanak az ipari rendszerek védelmében. Az AI-alapú megoldások képesek folyamatosan monitorozni a rendszerek működését, és azonosítani azokat a mintákat vagy anomáliákat, amelyek kibertámadásra utalhatnak. Az AI-alapú anomália detektálása különösen hatékony a SCADA-rendszerek esetében, ahol a hagyományos védelmi eszközök, mint például a tűzfalak, nem képesek effektíven észlelni az olyan összetett támadásokat, mint a hamis adatinjektálás. A megfelelően megalkotott AI-modell képes folyamatosan elemezni a SCADA-rendszerek által kezelt adatokat, és összehasonlítani azokat a normál működés során megszokott mintákkal. Ha eltérést észlelnek a szokásos működéstől, akkor riasztást küldhetnek és potenciális támadást jelezhetnek.[19] Véleményünk szerint ez a megoldás az adatkommunikáció jellegére összpontosít, így inkább olyan rendszerekben lehet jól alkalmazni, ahol a tényleges adattartalom nehezen vagy egyáltalán nem hozható összefüggésbe a fizikai folyamat rendeltetésszerű működésével. Más szóval a kommunikáció változó jellegének kiszűrésére alkalmas, mint például a többletadatcsomagok megjelenése.

AI-alapú prediktív védelem

Az AI nemcsak az anomáliák detektálásában játszik szerepet, hanem képes előre jelezni a potenciális támadásokat is. A prediktív analitika révén az egyes AI-architektúrák képesek előre megjósolni a rendszerekben bekövetkező változásokat, és jelezni, ha egy támadás valószínűsíthető. Ez különösen hasznos lehet akkor, ha a fizikai paraméterek, mint például a nyomás, a hőmérséklet vagy a folyadékszintek, kritikusak a működés szempontjából. Ezek a prediktív rendszerek képesek monitorozni a fizikai folyamatokat, és előre jelezni, hogy mikor léphetnek fel rendellenességek, még mielőtt azok ténylegesen megtörténnének. Például egy prediktív algoritmus észlelheti, ha egy folyamat során a nyomás kezd eltérni a normál értékektől, és figyelmeztetést küldhet, mielőtt a rendszer hibába ütközne. Ezáltal a támadások korai észlelése lehetővé válik, még azelőtt, hogy azok jelentős károkat okoznának.[20] Szemben az anomáliadetektálással ez a megoldás az adattartalomra fókuszál. Egy-egy szenzor által mért érték normális trendtől való eltérését képes jelezni.

[19] Yalçın–Çakır–Ünaldı 2024: 39557.
[20] Salehi–Siavash 2021: 7377.

Fizikai modellek alkalmazása

Az AI-alapú védelem másik fontos aspektusa a fizikai környezet modellezése. Az ilyen rendszerek összehasonlítják a folyamatok tényleges fizikai állapotát a számítógépes modellek által előre jelzett állapottal, így képesek felismerni azokat a rendellenességeket, amelyek a támadások eredményeként léphetnek fel. Ez különösen hatékony a hamis adatinjekciós támadások ellen, ahol a támadók megpróbálják megtéveszteni a rendszereket azzal, hogy hamis adatokat küldenek be. A fizikai modellek segítségével a rendszerek képesek felismerni, ha a kapott adatok nem felelnek meg a valós fizikai környezetnek.[21] Az ilyen védekezési módszer különösen hasznos lehet a kritikus infrastruktúrák esetében. A fizikai modellek lehetővé teszik a rendszerek számára, hogy azonnal észleljék a rendellenességeket, és gyorsan reagáljanak a potenciális támadásokra. Véleményünk szerint ez a legkifinomultabb, viszont a legtöbb előkészületet igénylő megoldás, amelyhez a fizikai folyamat pontos ismerete és modellezése nélkülözhetetlen. A folyamat változásakor a teljes modell újraalkotása és az AI-tanítási folyamatok újbóli elvégzése szükséges. A felügyelt folyamat és a kockázatok tükrében szükséges mérlegelni, hogy egy ilyen jellegű többletráfordítás indokolja-e a tárgyalt rendszer kidolgozását és telepítését a védelem fokozása érdekében.

AI-alapú megoldás a Modbus mérgezéses támadásának feltárására

Meglátásunk szerint a különféle védelmi mechanizmusok együttes alkalmazása, valamint azok folyamatos fejlesztése vezet rendszereink sebezhetőségének csökkentéséhez. Ezáltal szükségesnek látjuk ilyen irányú kutatások folytatását, amihez kialakítottunk egy olyan környezetet, amely valós hardveren nyújt lehetőséget a megoldások teszteléséhez. Jelen kutatásunk középpontjában olyan AI-alapú megoldás áll, amely a Modbus kommunikációs protokoll elleni hamis adatinjekciós támadások felismerését és elhárítását szolgálja. A Modbus széles körben használt ipari protokoll, amely eredetileg nem tartalmazott biztonsági mechanizmusokat, így különösen sebezhető az olyan támadásokkal szemben, amelyek során a támadók rosszindulatú módon megváltoztatják a rendszerben továbbított adatokat. Célunk, hogy az ilyen típusú támadások valós idejű felismerésére hatékony, AI-alapú anomáliadetektálási rendszert alkossunk, amely nem befolyásolja egy meglévő rendszer felépítését vagy működését. Más szóval a korábbi struktúra megtartása mellett legyen lehetséges a védelem implementálása. Az előző fejezetben említett védelmi törekvések közül az anomáliadetektálás tűnik a legszélesebb körben alkalmazható megoldásnak. Könnyen integrálható meglévő rendszerbe annak leállítása nélkül, és a tanítási folyamat is egyszerűen elvégezhető. A fizikai folyamat modellezése és a konkrét szenzoradatok ismerete nem szükséges, így egy fokozott védelmet biztosító, mindemellett költséghatékony megoldást kínál.

[21] Salehi–Siavash 2021: 7379.

A Modbus FDI-támadások jellemzői

A Modbus protokoll esetén a hamis adatinjekciós támadások során a támadók megváltoztatják a rendszer által feldolgozott adatokat, így a vezérlőrendszerek helytelen utasításokat hajtanak végre, aminek következménye lehet a folyamatok hibás működése vagy teljes leállása. Mivel a Modbus protokoll alapvetően nem tartalmaz hitelesítési mechanizmusokat, a támadók képesek hamis parancsokat és fals értékeket küldeni a vezérlőrendszereknek anélkül, hogy észlelhető lenne a támadás. Mivel ez a támadási módszer többletcsomagok rendszerbe juttatásával jár, a megjelenése detektálható.

Prediktív adatkezelés

A jellemző támadási lehetőségek bemutatásán túlmenően célunk egy valós megoldás megalkotása, amely egy folyamat szenzorrendszerének modellezését irányozza elő, neurális hálózati megközelítéssel. Ez a védelmi rendszer képes az egyes érzékelők működését valós időben előre jelezni a bemeneti adatok alapján. Jelen modellünk egy nyomásszenzor működését hivatott leképezni, ez egy gőztartály nyomását méri, amely összefüggésben van a rendszer többi paraméterével. Gyakorlatilag egy gőzkazán szabályozását megvalósító folyamatról van szó. Jelen esetben Modbus TCP/IP protokoll hordozza az adatokat, amelyeket az Ethernet-hálózat megcsapolásával olvasunk be, ezzel biztosítva a szenzoradatok valós idejű és megbízható hozzáférését. Maga a kommunikációt figyelő és adatokat kinyerő eszköz az Ethernet-hálózat szempontjából láthatatlan, nem rendelkezik saját identitással, fizikai címmel. A neurális hálózati modellünkhöz használt bemeneti és kimeneti változókat az 1. táblázat foglalja össze.

A hálózat kimenete maga az elvárt gőznyomás értéke, amely a bemeneti paraméterek függvényében alakul. A cél a bemeneti és kimeneti összefüggések azonosítása és előrejelzése annak érdekében, hogy a folyamathoz csatlakoztatott védelmi rendszer a nem várt működést detektálni tudja. Ennek eléréséhez egy perceptronalapú neurális hálózatot alkalmazunk, amely teljesen kapcsolt rétegekből áll.

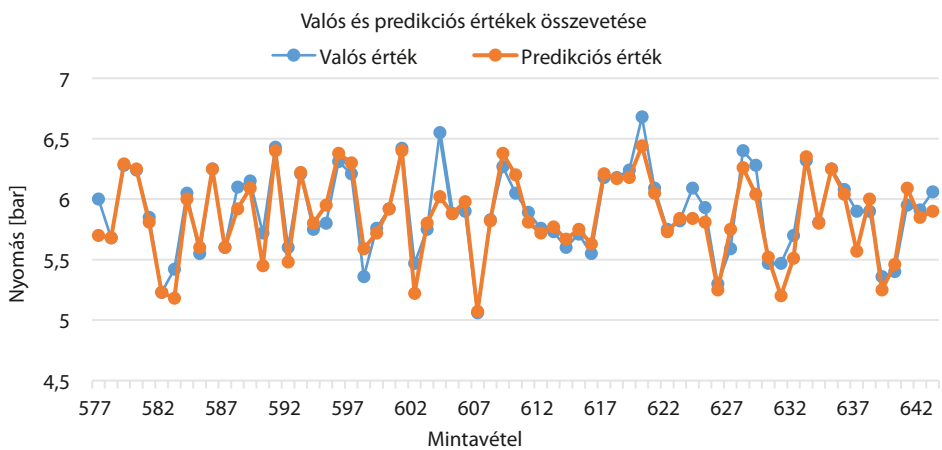
Ez a megközelítés jól kezeli a nemlineáris összefüggéseket, és egyszerű architektúrája révén gyorsan és hatékonyan tanítható. Első körben a tanítási folyamathoz szintetikus adatokat használtunk.

1. táblázat: A perceptron háló bemeneti és kimeneti változói

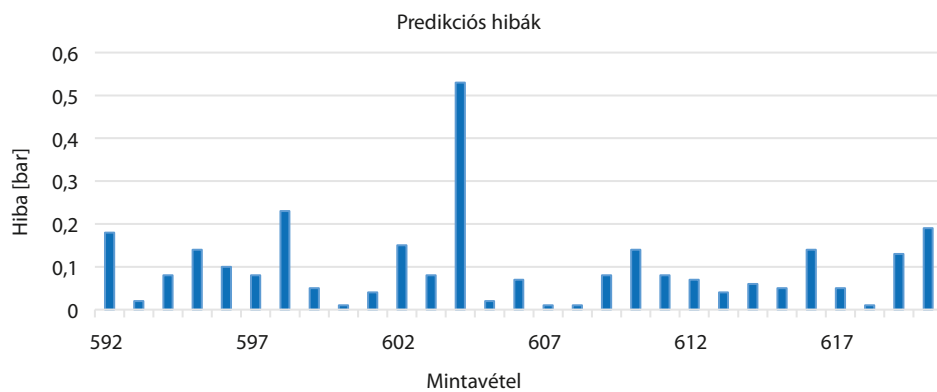
	Paraméter	**Tartomány**	**Dimenzió**
A perceptron háló bemenete	A beáramló víz mennyisége	0–10	l/sec
	A beáramló víz hőmérséklete	0–100	°C
	A kiáramló gőz mennyisége	0–5	kg/sec
	A kiáramló gőz hőmérséklete	100–150	°C
A perceptron háló kimenete	Gőznyomás	0–10	bar

Forrás: a szerzők szerkesztése

Az így létrehozott adatsor egy olyan szcenáriót modellez, amelyben a víz hőmérséklete kezdetben 40 °C, majd lineárisan emelkedik 100 °C-ra 1 óra alatt. A szimulált szenzoradatokra zajjelet szuperponálunk, hogy a szimuláció realisztikus legyen, mivel a valóságos mérési értékek is eltérnek az ideálistól. Továbbá így biztosítható, hogy a tanító és a tesztadatok valamelyest eltérjenek egymástól. Modellünk tanítását követően összevetettük a valós és a prognosztizált értékek időbeni lefutását, ami a 2. ábrán látható. Megállapítható a két adatsor közötti szoros összefüggés, ezáltal a betanított háló alkalmazhatósága. Normális működés esetén a két értéknek jelentős korrelációt kell mutatnia. Lehetnek pontok, ahol nagyobb eltérés tapasztalható, de ezek nem befolyásolják az adatsorok trendjét. A 3. ábrán külön kiemeltük az adatsor azon részét, amelyen a legnagyobb eltérés figyelhető meg. A rendellenes működés detektálása a korrelációban bekövetkező változáson alapszik.



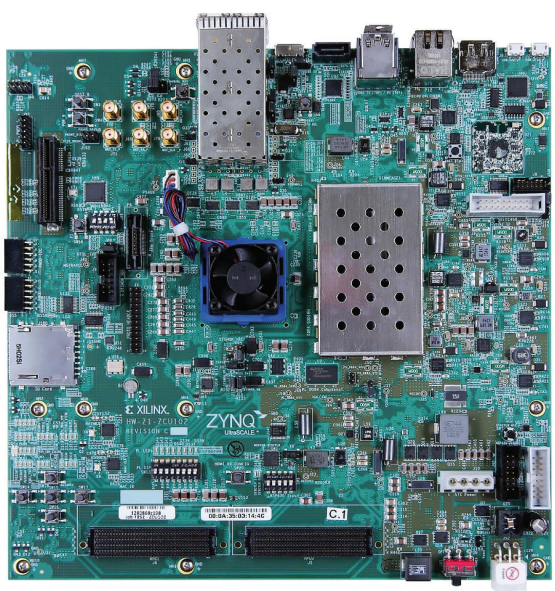
2. ábra: A valós és a modell által számított nyomásérték együtt futása
Forrás: a szerzők szerkesztése



3. ábra: A valós és a predikciós érték közötti eltérések mértéke (maximum: 0,53 bar)
Forrás: a szerzők szerkesztése

A nyomásszenzor modellezésére alkalmazott perceptronalapú megközelítés hatékonyan kezelte a bemeneti változók és a nyomás közötti összefüggéseket, a modell képes volt előre jelezni a szenzor által mért nyomást. További érzékelők perceptron modelljének implementációjával és azok összekapcsolásával fokozhatjuk modellünk integritását. Ezen architektúra dedikált adatvalidációs pontjai a valós szenzoradatok folyamatos korrelációs vizsgálatával lehetőséget biztosítanak az anomáliák és azok tendenciájának felismerésére, valamint a rendszer állapotának folyamatos monitorozására. Valós környezetben a tanítószettek rögzítése és a tanítási folyamat könnyen elvégezhető normális üzem közben.

Továbbá fontosnak tartjuk kiemelni, hogy ez a megoldás nem kizárólag szándékos károkozás esetén adhat jelzést – nem várt hardveres meghibásodásra való figyelmeztetésre is alkalmas. Neuralgikus tulajdonsága a vázolt megoldásnak, hogy a meglévő ipari rendszer megbontása és leállítása nélkül alkalmazható. Meglátásunk szerint ez sok esetben elvárás lehet, mivel egy magasabb biztonsági szint elérése már meglévő rendszer esetén kizárólag annak teljes újratervezésével és kiépítésével lenne lehetséges, ami jelentős költséggel és a folyamatok leállításával jár. A szóban forgó AI-modell hardveres implementációját és tesztelését egy AMD ZCU102 FPGA kártyán (4. ábra) végezzük kutatásunk soron következő fázisaként. Ez lehetővé teszi a kutatást generált adatokon és valós rendszereken egyaránt. Így valós körülmények között is megfigyelhetővé válik annak működése, és további gyakorlati tapasztalatok is gyűjthetők, amelyek egy jól alkalmazható rendszer megalkotását vetítik előre. Az általunk alkotott megoldás nem korlátozódik Ethernet-alapú kommunikációra, így irreleváns a protokollt hordozó fizikai réteg. Más szóval a Modbus protokollt tekintve nem számít, hogy Ethernet, RS232 vagy RS485 a médium, a megoldás ugyanúgy alkalmazható.



4. ábra: AMD ZCU102 FPGA fejlesztőkártya
Forrás: Advanced Micro Devices

A kutatásunkhoz kialakított rendszer hardveres szempontból kielégítő mind a prediktív, mind a fizikaimodell-alapú védelem kialakításához, így kiváló alapot ad a komplexebb megoldások kutatásához és fejlesztéséhez. További célkitűzéseink közé tartozik a perceptron háló optimalizálása, több szenzor modelljének implementálása, illetve az automatizálható szenzortanítási folyamat kidolgozása, amelyek mind hozzájárulnak egy könnyen telepíthető védelmi megoldás megvalósításához.

Összegzés

Az ipari vezérlőrendszerek, különösen a PLC-k és a SCADA-rendszerek kulcsfontosságú szerepet játszanak a modern ipari és kritikus infrastruktúrák működésében, mivel ezek biztosítják a különböző folyamatok automatizálását és távoli irányítását. Azonban a technológiai fejlődés és a hálózati integráció révén ezek a rendszerek sebezhetőbbé váltak a kibertámadásokkal szemben. A kommunikációs protokollok, mint a Modbus és a DNP3, alapvetően nem tartalmaznak biztonsági mechanizmusokat, így könnyen manipulálhatók olyan támadási módszerekkel, mint a hamis adatinjekciós támadások. Az ipari vezérlőrendszerek elleni támadások súlyos következményekkel járhatnak, különösen a kritikus infrastruktúrák esetén, ahol ezek a rendszerek alapvető fontosságúak. A szóban forgó rendszerek védelme nem kizárólag fizikai hozzáférés-ellenőrzést és hagyományos tűzfalakat igényel, hanem fejlett megoldásokat is, mint például az AI-alapú anomáliadetektálás és a prediktív elemzés. Ezek lehetővé teszik a rendszerek valós idejű monitorozását, és képesek felismerni azokat a mintákat és rendellenességeket, amelyek kibertámadásokra utalhatnak. Kialakítottunk egy környezetet, amelyben a vonatkozó kutatások hatékonyan végezhetők. Célunk volt egy perceptron neurális hálózat kialakítása, amely hatékony megoldást kínálhat a Modbus protokollon keresztül történő támadások és esetleges hardveres meghibásodások felismerésére egyaránt. A neurális hálózat architektúráját megalkottuk oly módon, hogy az konfigurálható legyen az ipari rendszerben jelen lévő érzékelők reprezentációjára, és szintetikus adatok segítségével elvégeztük annak tanítását. Rendszerünk jelenleg egy szimulált gázkazán működése közben fellépő szenzoradatok megfigyelésére és jövőbeli állapotbecslésére alkalmas. Kutatásunk következő szakaszában az így megalkotott rendszer hardveres implementációja következik. Összességében elmondható, hogy az ipari rendszerek kiberbiztonsága integrált védelmi megközelítést igényel, amely kombinálja a fizikai és a hálózati biztonságot az AI-alapú rendszerekkel. Az ilyen irányú kutatások és fejlesztések továbbra is elengedhetetlenek, hogy AI-technológiával kiegészülve hatékonyabban védekezhessünk az egyre összetettebb kibertámadások ellen.

Felhasznált irodalom

Aldossary, Lina Abdulaziz – Ali, Mazen – Alasaadi, Abdulla (2021): Securing SCADA Systems against Cyber-Attacks using Artificial Intelligence. *2021 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies,* 739–745. Online: https://doi.org/10.1109/3ICT53449.2021.9581394

Allison, David et al. (2020): PLC-Based Cyber-Attack Detection: A Last Line of Defence. *IAEA International Conference on Nuclear Security: Sustaining and Strengthening Efforts,* 1–10. Online: https://conferences.iaea.org/event/181/contributions/15513/attachments/9194/12424/CN278_PLC-based-Detection.pdf

Bognár Balázs – Bonnyai Tünde – Vámosi Zoltán (2019): *Kritikus infrastruktúrák védelme I.* Budapest: Dialógus Campus Kiadó.

Dér Attila (2024): Villamosenergia-rendszerek aktuális kiberbiztonsága. *Biztonságtudományi Szemle,* 6(2), 47–55.

Geng, Yangyang et al. (2024): Control Logic Attack Detection and Forensics Through Reverse-Engineering and Verifying PLC Control Applications. *IEEE Internet of Things Journal,* 11(5), 8386–8400. Online: https://doi.org/10.1109/JIOT.2023.3318988

Haig Zsolt et al. (2009): *A kritikus információs infrastruktúrák meghatározásának módszertana*. [H. n.]: ENO Advisory Kft.

Hankó Viktória (2023): SCADA-rendszerek kiberbiztonsága a létfontosságú rendszerelemek tekintetében 1. *Hadmérnök,* 18(3), 145–160. Online: https://doi.org/10.32567/hm.2023.3.10

Kralovánszky Kristóf (2019): A villamosenergia-rendszer kiber- és nemzetbiztonsági kockázatai (1. rész). *Nemzetbiztonsági Szemle*, 7(3), 40–57. Online: https://doi.org/10.32561/nsz.2019.3.4

Malchow, Jan-Ole et al. (2015): PLC Guard: A Practical Defense against Attacks on Cyber-Physical Systems. *IEEE Conference on Communications and Network Security (CNS),* 326–334. Online: https://doi.org/10.1109/CNS.2015.7346843

Patel, Sandip C. – Bhatt, Ganesh D. – Graham, James H. (2009): Improving the Cyber Security of SCADA Communication Networks. *Communications of the ACM,* 52(7), 139–142. Online: https://doi.org/10.1145/1538788.1538820

Salehi, Mohsen – Siavash, Bayat-Sarmadi (2021): PLCDefender: Improving Remote Attestation Techniques for PLCs Using Physical Model. *IEEE Internet of Things Journal,* 8(9), 7372–7379. Online: https://doi.org/10.1109/JIOT.2020.3040237

Slay, Jill – Miller, Michael (2008): Lessons Learned from the Maroochy Water Breach. In Goetz, Eric – Shenoi, Sujeet (szerk.): *Critical Infrastructure Protection.* Boston: Springer, 73–82. Online: https://doi.org/10.1007/978-0-387-75462-8_6

Sommestad, Teodor – Ericsson, Göran N. – Nordlander, Jakob (2010): SCADA System Cyber Security – A Comparison of Standards. *IEEE PES General Meeting,* 1–8. Online: https://doi.org/10.1109/PES.2010.5590215

Vásárhelyi Örs (2024): A veszélyes üzemek információbiztonsági képességeinek fejlesztési lehetőségei napjaink kihívásainak tükrében. *Belügyi Szemle,* 72(1), 89–111. Online: https://doi.org/10.38146/BSZ.2024.1.6

Yalçın, Nesibe – Çakır, Semih – Ünaldı, Sibel (2024): Attack Detection Using Artificial Intelligence Methods for SCADA Security. *IEEE Internet of Things Journal,* 11(24), 39550–39559. Online: https://doi.org/10.1109/JIOT.2024.3447876

Yang, Huan – Cheng, Liang – Chuah, Mooi Choo (2018): Detecting Payload Attacks on Programmable Logic Controllers (PLCs). *IEEE Conference on Communications and Network Security (CNS)*, 1–9. Online: https://doi.org/10.1109/CNS.2018.8433146

HADMÉRNÖK
VÉDELEMINFORMATIKA

20. évfolyam (2025) 1. szám 87–104.
DOI: 10.32567/hm.2025.1.5

Hammas Attila,[1] Négyesi Imre[2]

A mesterséges intelligencia felhasználási lehetőségei képi felderítési műveletek támogatására

Technológiai áttekintés

Potential Uses of Artificial Intelligence to Support Image Reconnaissance Operations

A Technology Overview

Absztrakt

Az információs korban, amelyet gyakran a digitális forradalom korszakaként is emlegetnek, az adatok gyűjtése és hatékony feldolgozása elengedhetetlen képesség mind polgári, mind katonai környezetben. A technológia rohamos fejlődésének köszönhetően a gépi tanulás és a távérzékelés összefonódása rengeteg lehetőséget biztosít a kutatók számára, különösen az információgyűjtés, -feldolgozás és -értelmezés területén. Az információk hatékony kezelésének és felhasználásának fontossága megkérdőjelezhetetlen, az információk a stratégiai döntések alapkövei számos területen. Jelen tanulmány a technológia által nyújtott lehetőségeket és a felhasználás főbb területeit vizsgálja.

Kulcsszavak: felderítés, IMINT, mesterséges intelligencia, gépi tanulás

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola, e-mail: hammas.attila@stud.uni-nke.hu

[2] Egyetemi docens, Nemzeti Közszolgálati Egyetem Hadtudomány és Honvédtisztképző Kar, e-mail: negyesi.imre@uni-nke.hu

Abstract

In the information age, often referred to as the era of the digital revolution, the collection and the processing of data is an essential capability in both civilian and military environments. Thanks to the rapid development of technology, the intertwining of machine learning and remote sensing provides us with many opportunities, especially in the areas of information collection, processing and interpretation. The importance of effective management and use of information is unquestionable–information is the cornerstone of strategic decisions in many areas. The article will examine the opportunities provided by technology.

Keywords: reconnaissance, IMINT, artificial intelligence, machine learning

Bevezetés

Az információs korban, amelyre gyakran a digitális forradalom korszakaként is hivatkoznak, az adatok gyűjtése és feldolgozása központi szerepet játszik az információs társadalom működésében. Az adatok ma már mindenütt jelen vannak, és az élet szinte minden területén alapvető fontosságúak. A technológiai fejlődés, különösen az internet és a mobileszközök elterjedése, forradalmasította az adatgyűjtés és -feldolgozás módjait, mondhatni, az elmúlt évtizedekben keletkező adat mennyisége ennek is köszönhetően exponenciálisan növekedett. A különféle szenzorokkal és eszközökkel gyűjtött adatok lehetővé teszik a valós idejű megfigyelést, elemzést és döntéshozatalt, ami elősegíti a hatékonyság növelését és a kapcsolódó innovációkat. Az adatok feldolgozása és elemzése révén a szervezetek és az egyének jobban megérthetik a komplex rendszerek működését, és ezáltal megalapozottabb döntéseket hozhatnak. Az információs társadalomban az adatok tehát nem csupán nyers információk, hanem értékes erőforrások, amelyeknek a megfelelő kezelése és felhasználása nélkülözhetetlen a gazdasági és társadalmi fejlődéshez.

Katonai szempontból az információs műveletek olyan tervezett tevékenységeket foglalnak magukban, amelyek elsődleges célja az ellenség információs rendszereinek megtévesztése, megzavarása és manipulálása, valamint a saját műveletek támogatásához szükséges információ megszerzése és védelme. Ezek a tevékenységek kiterjednek az információ gyűjtésére, feldolgozására, elemzésére, tárolására, szétosztására, illetve a szemben álló fél megtévesztése érdekében téves és álinformációk terjesztésére, valamint az ellenfél információs rendszereinek a támadására, hogy befolyásolják annak döntéshozó képességét. Az információs műveletekhez tartozó tevékenységekről beszélhetünk a fizikai dimenzióban, a kibertérben, illetve a kognitív dimenzióban is.

Ugyanakkor azt is figyelembe kell vennünk, hogy az elmúlt évszázadban egyre nagyobb hangsúly került a hibrid konfliktusokra, illetve a proxyháború az egyik legelterjedtebb háborútípus.[3] Clausewitz híres megfogalmazása szerint „a háború a politika más eszközökkel való folytatása"[4]. Ez azt jelenti, hogy a háborút nem öncélú

[3] Boda 2023: 27.
[4] Clausewitz 2013: 54.

erőszakként kell értelmezni, hanem a politikai célok elérésének egy extrém eszközeként, amikor más módszerek már nem hoznak eredményt.[5] Ha egy állam politikai akaratának a befolyásolása a cél, akkor nincs szükség fegyveres erőszak alkalmazására, sok esetben az adott állam politikailag nem akarja nyíltan félvállain az agresszor szerepét.[6] A második világháború után a nemzetközi viszonyok több átalakuláson estek át: a hidegháború idején a két szemben álló nagyhatalom (az Amerikai Egyesült Államok és a Szovjetunió) által képviselt ideológia bipoláris világrendet hozott létre, ahol a nagyhatalmak elsősorban különböző proxyháborúkkal próbáltak egymáson felülkerekedni. A Szovjetunió összeomlása után az Amerikai Egyesült Államok emelkedett ki mint egyedülálló nagyhatalom, és a „világ csendőreként" folyatott proxyháborút a résállamokban (a globalizációt elutasító államok) megjelenő terrorista szervezetek ellen. Azonban a 21. század elejétől új regionális hatalmak – mint például Kína, Oroszország, India és az Európai Unió – egyre nagyobb befolyást gyakoroltak a nemzetközi politikára, és a globális hatalmi egyensúly fokozatosan multipolárissá és poliarchikussá alakult.[7] A proxyháborúk fejlődése és a hibrid konfliktusok jellemzői – különösen a nem állami szereplők térnyerése és az információs műveletek növekvő szerepe – szorosan kapcsolódnak a mesterséges intelligencia alkalmazási lehetőségeihez a képi felderítésben. A modern poliarchikus nemzetközi helyzetben az MI-alapú képelemzés és információs hadviselés lehetőséget biztosít a konfliktusok rejtett dimenzióinak feltárására, az ellenséges tevékenységek azonosítására, valamint a nem állami szereplők és támogatott milíciák mozgásának és logisztikájának pontosabb nyomon követésére. A történelem során a haditechnológia fejlődéséről az mondható el, hogy a pusztítási kapacitás rohamosan nőtt addig a szintig, hogy a nagyhatalmak képesek kölcsönösen egymást megsemmisíteni, ezzel veszélyeztetve az emberiség egészét.[8] A mesterséges intelligencia, mint egy új fegyvertípus, azon feltörekvő technológiákhoz sorolható, amelyeknek elsődlegesen elemző és szimuláló szerepük van, és jelentősen csökkenthetik a konfliktus által okozta kockázatot a saját állományra nézve.[9]

A tanulmány során vizsgálni fogjuk a mesterséges intelligencia jelentőségét napjainkban, főként a képelemzési eljárásokat, amelyek alkalmazása támogatja és támogathatja a képi felderítést, azzal a céllal, hogy feltárjuk a gépi látás, a felderítés és a távérzékelés területek átfedéseit. Ugyanakkor a tanulmány arra is rávilágíthat, hogy a civil szférában alkalmazott gépi látási feladatokra elkészült megoldások milyen mértékben használhatók fel a védelmi szférában.

A gépi tanulás és a távérzékelés szerepe az információs műveletekben

A tanulmány az információs műveletek egy apró szeletét, az információgyűjtést és -feldolgozást vizsgálja. Mind katonai, mind polgári környezetben a műveletek hatékonysága nagymértékben függ a döntéshozók, illetve a beavatkozók számára

[5] Boda 2024: 114.
[6] A hibrid háború korszakába léptünk: de mit is jelent ez? 2022.
[7] Boda 2023: 28–30.
[8] Konrád 1963: 1, 7.
[9] Boda 2024: 116.

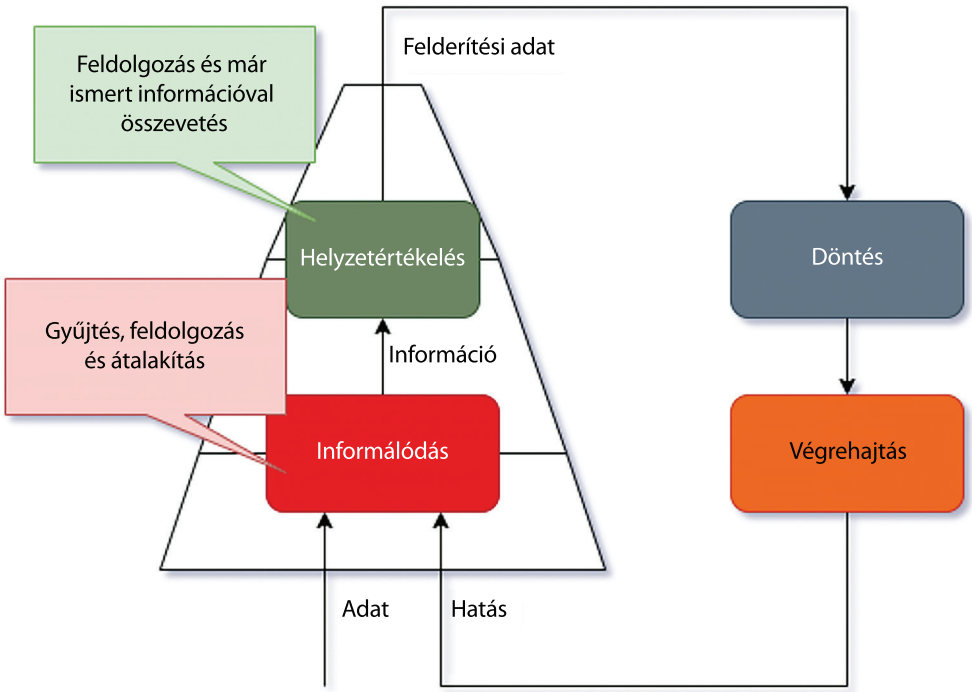
elérhető megbízható információtól. A katonai műveletek során, harci körülmények között, ahol a kockázat akár rendkívül magas is lehet, az információs műveletek szerepe még fontosabbá válik, így az információ megfelelő gyűjtése, feldolgozása, ellenőrzése és kiaknázása biztosítja, hogy a műveletek egy reális helyzetkép alapján legyenek megtervezve, majd végrehajtva. A gépi tanulás (*machine learning,* ML) ezeket a képességeket növeli, lehetővé téve a hatalmas adathalmazok gyorsabb feldolgozását, az ember számára észlelhetetlen mintázatok azonosítását, valamint az ellenfél cselekedeteinek pontosabb előrejelzését. Manapság a begyűjtött adatok azonnali kiértékelésre szorulnak, hiszen sok esetben a helyzetkép kialakításához szükséges információ rövid idő alatt irrelevánssá válhat. Ugyanakkor az információ megbízhatóságának a növelése érdekében ezt érdemes több forrásból is begyűjteni, majd a feldolgozott összadatforrás alapján kialakítani az aktuális helyzetképet, ezzel részlegesen szűrni lehet a téves információkat. A technológia rohamos fejlődése során a gépi tanulás és a távérzékelés összefonódása hatalmas lehetőségeket rejt magában, különösen az információelemzés területén. Az információk hatékony kezelésének és felhasználásának fontossága megkérdőjelezhetetlen – az információk a stratégiai döntések alapkövei számos területen. Ez különösen igaz a védelem területén, ahol a felülmúlhatatlan információk, illetve ennek időszerűsége jelentős taktikai előnyöket biztosíthatnak.[10]

Annak alapján, hogy a felderítés során szerzett információ forrása, milyensége, illetve hogy az milyen céllal lesz felhasználható, a különböző felderítési eljárásokat csoportosítani lehet. A Magyar Honvédség Összhaderőnemi Doktrína által alkalmazott felderítési folyamatok és eljárások csoportosítása:[11]

- emberi erővel folytatott felderítés (HUMINT – *human intelligence*);
- képfelderítés (IMINT – *imagery intelligence*);
- rádióelektronikai felderítés (SIGINT – *signal intelligence*);
- rádiófelderítés (COMINT – *communication intelligence*);
- rádiótechnikai felderítés (ELINT – *electronic intelligence*);
- hangfelderítés (ACINT – *acoustic intelligence*);
- kisugárzás és jelfelderítés (MASINT – *measurements intelligence*);
- radarfelderítés (RADINT – *radar intelligence*);
- technikai felderítés (TECHINT – *technical intelligence*);
- nyílt források által folytatott felderítés (OSINT – *open-source intelligence*);
- az ellenség felderítését elhárító tevékenység, saját csapatok védelme (CI/FP – *counterintelligence and force protection*).

A begyűjtött adatokból kinyert információ alapján a vezetők, a megfogalmazott cél elérése érdekében, kiválasztják a legmegfelelőbb beavatkozási eljárást. A kivitelezés után ez direkt vagy indirekt módon hatással van az aktuális állapotra, azaz egy visszacsatolásról, egy folytonos hurokról beszélhetünk, amint ezt az 1. ábra is szemlélteti.

[10] Haig–Várhegyi 2005.
[11] Haig et al. 2014: 95.



1. ábra: Az OODA-hurok és az adat, információ, felderítési adat viszonya
Forrás: Haig et al. 2014; Ploumis 2022 alapján a szerzők szerkesztése

Különösen a katonai műveletek során, de nem csak ekkor, olyan környezetben kell információt gyűjtenünk, amelyhez nincs direkt hozzáférésünk, vagy az itt végzett tevékenység kockázattal jár a végrehajtó személyzetre nézve. A távérzékelés során úgy gyűjtünk információt a megfigyelendő objektumokról vagy jelenségekről, hogy a folyamat során nem érintkezünk fizikailag az adott környezettel.

A modern védelmi stratégiák egyre inkább támaszkodnak a távérzékelésre, hogy kritikus adatpontokat szolgáltassanak a műveleti tervezéshez, valamint a fenyegetések feltárásához és kiértékeléséhez. A mesterséges intelligencia (*artifical intelligence,* AI) alkalmazása ebben a kontextusban fokozza a távérzékelési technológiák képességeit, lehetővé téve pontosabb, gyorsabb információ előállítását. Az óriási adatkészletek elemzésének automatizálásával a gépi tanulás lehetővé teszi a védelmi elemzők számára, hogy olyan mintázatokat és anomáliákat észleljenek, amelyek az emberi szem számára észrevehetetlenek lennének.[12] Például az előzetesen begyűjtött nagy mennyiségű adat, az ebből kinyert statisztikai mintázatok alapján a mesterségesintelligencia-alapú algoritmusok segíthetnek a megfelelő következtetések levonásában.

A gépi tanulás alkalmazásainak technológiai áttekintése a távérzékelésben nemcsak a jelenlegi képességeket mutatja be, hanem a jövőbeli előrelépések lehetőségét is megvilágíthatja. Ahogy a mesterségesintelligencia-alapú algoritmusok egyre

[12] Boda 2024: 9.

kifinomultabbá válnak, integrációjuk a távérzékelési technológiákkal még hatékonyabb eszközöket ígér az adatelemzéshez és -értelmezéshez. Ezek az előrelépések javíthatják a helyzetfelismerést, a jobb erőforrás-gazdálkodást és a hatékonyabb védelmi stratégiák alkalmazását, amelyek mind létfontosságúak a nemzetbiztonság fenntartásában.

Képfeldolgozás, gépi látás és mesterséges intelligencia

A mesterséges intelligencia nem egyszerűen definiálható fogalom, hiszen több oldalról is megközelíthető; egy átfogó meghatározás a következő lehet: „Olyan hardver- és szoftvertechnológiák összessége, amely képes önálló döntések meghozatalára tudományos érvek, vagy akár emberi gondolatok, reakciók, érzelmek figyelembevételével."[13]

A mesterséges intelligencia kezdetben jól lehatárolt és explicit szabályrendszerekkel ellátott feladatokban ért el átütő sikereket, itt gondolunk pedálul az IBM által fejlesztett Deep Blue mesterséges intelligencia által elért sikerekre az akkori sakkbajnok ellen, vagy a Google DeepMind által fejlesztett AlphaGo győzelmeire 2015–2016-ban gojátékosok ellen.[14] Napjainkban azonban a mesterséges intelligenciával felvértezett rendszerek olyan környezetben is képesek helytállni, amelyben a szabályrendszereket sok zavaró tényező és bizonytalanság veszi körül, miközben a bemenet sem tekinthető strukturáltnak. Itt most gondolhatunk az önvezető autókra vagy a multimodális nagy nyelvi modellekre, amelyek szöveget, hangot és képeket is képesek feldolgozni. Egy példa erejéig lássuk egy önvezető autó összetett feladatát (2. ábra):

- észlelnie kell a körülötte elhelyezkedő akadályokat, amelyeket a pályatervező algoritmusnak ki kell kerülnie, legyen az egy másik gépjármű, gyalogos vagy akár betonfal;
- be kell tartania a forgalomra vonatkozó szabályokat (elsőbbségadás, haladási irány, sebesség és sok más korlátozás), ehhez azonosítania kell a táblákat, úttesteket, illetve ezeket kontextuálisan el kell helyeznie a térben;
- figyelnie kell a váratlan eseményekre, mint például takarásból kifutó kisgyerek vagy a semmiből megjelenő őzek.

Laikusként mondhatjuk azt, hogy a KRESZ (Közúti Rendelkezések Egységes Szabályozása) jól definiált szabályrendszerként megfogalmazza, hogyan kell a gépjárművezetőnek eljárnia különböző esetekben. Azonban nem hagyhatjuk figyelmen kívül, hogy a gyakorlatban sok zavaró tényező van jelen: optikai csalódás miatt az akadály beleolvad a környezetébe, a táblák takarásban vannak, a felfestések idővel lekopnak, a közforgalomban részt vevő szereplők szabályt szegnek, javítás miatt terelések és útszűkületek vannak, és még sorolhatnánk.

[13] Németh–Virágh 2022a: 19.
[14] Németh–Virágh 2022b.

2. ábra: A környezet egy Tesla önvezető autó szemszögéből
Forrás: Andrej Karpathy [é. n.]

Különböző gyártók annyira megbíznak a gépi látási algoritmusok képességeiben, hogy bizonyos szenzorokat kezdenek kiiktatni az arzenáljukból, ezáltal csökkentve az adatforrások számát, ami a megbízhatóság rovására mehet, a gyártási költségek csökkentése érdekében. Ilyen például a Tesla elektromosautó-gyártó 2022-ben hozott döntése, miszerint az ultrahangos távérzékelőket fokozatosan kihagyja az újabb gyártású gépjárműiből, és kizárólag a gépi látásra támaszkodva fejleszti tovább az önvezető autókban rejlő algoritmusokat.[15] Ezáltal a rendszerek egyfajta redundanciájukat elveszítik, ami olykor hibás kimeneteleket is eredményezhet: például történt olyan eset, amikor egy Tesla önvezető autó nekicsapódott egy elválasztó falnak.[16] Ilyenkor felmerül a felelősség kérdése is, hiszen az előbbi példában az ütközéskor és az azt megelőző pillanatokban a jármű önvezető üzemódban volt ugyan, de a felhasználói feltételekben megtalálható, hogy a járművezetőnek felügyelnie kell az önvezető autót, és hiba estén be kell avatkoznia.[17] Az ilyen esetek relatív számossága kisebb, mint a nem önvezető autók esetében, viszont az önvezető autók által okozott balesetek sokkal nagyobb figyelmet kapnak a médiában újszerűségüknek köszönhetően. Ugyanakkor az is probléma, hogy a mesterségesintelligencia-alapú rendszerek egyfajta feketedobozként foghatók fel, és nem lehet egyértelműen megállapítani, hogy miért is az adott eredmény született.[18]

A gépi látás nagymértékben mesterségesintelligencia-alapú algoritmusok ötvözése különböző képfeldolgozási eljárásokkal. A bemenetén kapott képi információkat feldolgozza és átalakítja olyan információvá, amelyet később más rendszerek felhasználhatnak. Ha az autóiparból akarunk példát meríteni, akkor gondolhatunk az autonóm sávtartó vagy vészfékező rendszerekre. Például ha az autó haladási pályája keresztezni fogja egy gyalogos útvonalát, akkor a képfeldolgozó algoritmus eredménye alapján tud beavatkozási döntéseket hozni, mint például a haladási irány megváltoztatása vagy a fék alkalmazása.

15 Tesla Vision Update: Replacing Ultrasonic Sensors with Tesla Vision [é. n.].
16 Thorbecke 2020.
17 Négyesi 2023: 7, 13.
18 Szabadföldi 2022: 360–361.

A gépi látás területén számtalan feladatról tudunk beszélni, azonban ezekből a fontosabbak lesznek részletesebben elemezve: képosztályozás vagy klaszterezés, objektum- vagy anomáliaészlelés, illetve követés, szegmentáció.

Képosztályozás

A képosztályozás klasszikus képfeldolgozási feladat, amely egy teljes kép feldolgozását foglalja magában. A cél a kép osztályozása úgy, hogy azt egy adott címkéhez rendeli. Ezt a fajta feladatot a leggyakrabban konvolúciós neuronhálókkal (*convolutional neural network,* CNN) oldják meg, amelyeknek a bemenete maga a kép vagy annak a leskálázott változata, valamint a kimenete a különböző osztályokhoz rendelt konfidenciaszint.[19] A képosztályozó konvolúciós neuronhálók két részből épülnek fel: az előfeldolgozás célját szolgáló konvolúciós és összevonó rétegek sorozatából (ezt sok helyen „gerincként" említik), valamint teljesen összecsatolt osztályozó rétegek sorozatából („fej"). A konvolúciós rétegek hangolásával a neuronháló megtanulja kinyerni a legfontosabb jellemzőket, amelyek alapján majd az osztályozó rész könnyedén el tudja dönteni, hogy a bemenetet milyen osztályba kell sorolni.

Lévén, hogy a mélytanuló algoritmusok tanítása során rengeteg paraméter együttes hangolása szükséges, a túltanulás elkerülése végett elengedhetetlen a nagy mennyiségű változatos minta. A túltanulás az a jelenség, amikor az adott neuronháló paramétereinek hangolása során a modell túlzottan illeszkedik a tanítómintákban található mintázatokra, és amikor egy új, eddig még nem látott bemeneten értékeljük ki, rosszabb teljesítményt nyújt, mivel nem képes megfelelően általánosítani, az új minta pedig részleteiben eltér az eddig látottaktól. Így a kutatók rendelkezésére bocsátott nagy méretű adatbázisok katalizátorként hatottak a mesterséges intelligenciával kapcsolatos kutatások területén. Az egyik első ilyen rendelkezésre álló adatbázis az ImageNet, amely a közzétételének pillanatában 3,2 millió képet tartalmazott, mára pedig már több mint 15 millió képből tevődik össze. Az egyik fontos tulajdonsága ennek az adathalmaznak a méretén kívül, hogy egy hierarchikus osztályozási rendszert alkalmazott, azaz az osztályok lebonthatók voltak alosztályokra, lehetővé téve az adathalmaz széles körű felhasználását.[20] Az adathalmaz a következő években tovább bővült, illetve egy verseny is kihirdettek, amelynek címe: ImageNet Large Scale Visual Recognition Challenge (ILSVRC). A 2012-ben megszervezett ILSVRC-versenyt az AlexNet architektúra nyerte meg, megelőzve az addig alkalmazott LeNet architektúrát. Az AlexNet egy mélyebb konvolúciós háló volt, mint az addig alkalmazott struktúrák, valamint bevezetett új fogalmakat, mint a normalizáló rétegek és a *dropout* (az adott tanítási ciklusok során véletlenszerűen kiválasztott neuronok fagyasztva vannak és nincsenek hangolva a visszafejtett hiba alapján), aminek köszönhetően az algoritmus kevésbé volt kitéve a túltanulásnak. A 2014-ben megszervezett versenyen a GoogleNet nyert, amely az *inception* rétegekkel csökkentette a szükséges számítási kapacitást, azáltal, hogy ezek a rétegek különböző méretű konvolúciós kerneleket ötvöztek egy rétegben,

[19] Brassai 2019.
[20] Deng et al. 2009.

így csökkenteni tudták a hálómélységet. A VGGNET modellcsalád bizonyította, hogy a konvolúciós hálók mélységének növelésével jobb eredmények érhetők el, viszont a mélyhálók hangolása nehézségekkel jár, erre nyújtott megoldást a ResNet (Residual Network) architektúrával bevezetett reziduális blokk, amely lehetővé tette a mélyebb architektúrák hatékony hangolását.[21]

A képosztályozó eljárások használata napjainkban szerteágazó, nagyon sok területen alkalmazzák őket, amint ezt az 1. táblázat is összefoglalja.

1. táblázat: Képosztályozó algoritmusok alkalmazási lehetőségei a különböző területeken

Terület	**Alkalmazás**
Egészségügy	*Leletek osztályozása:* különböző orvosi leletek osztályozása, ahol a cél az anomália jelenlétének a meghatározása.
Logisztika és kereskedelem	*Raktározás:* termékek automatikus osztályozása. *Keresés:* hasonló osztályba sorolható tárgyak keresése.
Szociális hálók, telekommunikáció	*Tartalomszűrés:* a képanyagok automatikus besorolása, valamint nem megengedett tartalmak (erőszak, meztelen képek stb.) kiszűrése. *Automatikus címkézés:* a képek különböző címkékkel való ellátása annak érdekében, hogy utólag gyorsabban lehessen őket keresni és klaszterezni.
Biztonság és területvédelem	*Anomália észlelése:* térfigyelő kamerák képeinek osztályozása szokatlan tevékenységek vagy tárgyak észlelése érdekében. *Hozzáférés-vezérlés:* arcfelismerés használata személyek osztályozására és ellenőrzésére a biztonságos hozzáférés érdekében.
Ipar	*Minőség ellenőrzése:* a termékek besorolása és gyártási hibás termékek megjelölése.
Védelmi szféra	*Fenyegetés észlelése:* képek osztályozása a lehetséges fenyegetések, például az ellenséges harcjárművek, tüzérség és repülőgépek azonosításához.

Forrás: a szerzők szerkesztése

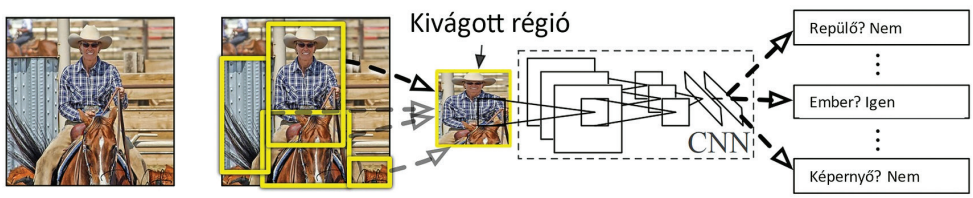
Objektumészlelés

Manapság a kihívást nem a képek egy osztályba sorolása jelenti, hanem a kulcsfontosságú elemek, objektumok észlelése és azok lokalizációjának a meghatározása az adott bemeneti képen. Erre a problémára is vannak különféle adathalmazok, mint például az MS COCO[22] (Microsoft Common Objects in Context, magyarul: mindennapi tárgyak a környezetünkben), a PASCAL VOC[23] (Pascal Visual Object Classes, magyarul: Pascal vizuális objektum osztályok), vagy a távérzékelést támogató rendszerek hangolására alkalmas adathalmazok: DOTA[24] (Dataset for Object deTection in Aerial Images, magyarul: adathalmaz légifelvételen való objektumészleléshez), UAVDT[25] (UAV Detection and Tracking, magyarul: objektumészlelés és követés pilóta nélküli járművekkel

[21] Alom et al. 2018: 12–13.
[22] Lin et al. 2014.
[23] Everingham et al. 2010.
[24] Xia et al. 2018.
[25] Du et al. 2018.

készített felvételeken), DroneVis[26] (Drone Vision – Versatile Computer Vision Library for Drones, magyarul: gépi látási könyvtár drónoknak), LoveDA[27] (Land-Cover Dataset for Domain Adaptive Semantic Segmentation, magyarul: adathalmaz felszínborítási szemantikus szegmentáció feladathoz). Az objektumészlelés problémára kialakított konvolúciós neuronháló-architektúrák két osztályba sorolhatók:

- Kétlépcsős: itt a legfontosabb megemlíteni a régióalapú konvolúciós neuronháló (R-CNN) családot (R-CNN,[28] Fast R-CNN, Faster R-CNN). Ezek a neuronhálók két lépésben oldják meg az objektumészlelést: egy régiójavasló modul (*region proposal network,* RPN) megjelöli azokat a potenciális képrészeket, ahol egy objektum helyezkedik el, majd egy osztályozó lépésben az algoritmus a megjelölt régiókról eldönti, hogy az háttér, vagy valamely előre definiált osztályhoz tartozik.[29] Ez a folyamat a 3. ábrán van szemléltetve.
- Egylépcsős: a legnagyobb népszerűséget élvező architektúra a YOLO[30] (You Only Look Once), ennek mára már számos verziója és variánsa elérhető. Ez a mélytanuló algoritmus egyetlen lépésben hajtja végre az objektumok detektálását, lokalizációját és osztályozását, így gyorsabb, viszont néha kevésbé pontos becslést ad, mint kétlépcsős társai.



3. ábra: R-CNN alapú algoritmus működési elve
Forrás: Girshick et al. 2013: 1

Ezek az objektumészlelő mélytanuló algoritmusok a képosztályozók által alkalmazott konvolúciós szerkezetekre építkeznek. Sok esetben a képosztályozó konvolúciós neuronhálók jellemző kinyerő szerkezetek (konvolúciós és összevonó rétegek), fellelhetők az objektumészlelő modellekben. Például a ResNet-ben vagy a VGG-ben (az Oxford Egyetemen a Visual Geometry Group által fejlesztett VGG-Net) alkalmazott jellemzőkinyerő struktúrák vagy hangolási eljárások ugyanúgy használatban vannak az objektumészlelő modellek megvalósítása során. Sok esetben ezeket a jellemzőkinyerő struktúrákat (gerinc) előre hangolják egy hasonló jellegű képosztályozási adatbázison, majd az így betanított gerincet használják objektumészlelő modellben

[26] Heakl et al. 2024.
[27] Wang et al. 2022.
[28] R-CNN – Regional Convolutional Neural Network.
[29] Girshick et al. 2013.
[30] Redmon et al. 2015.

is. Így az adott modult kevesebbet kell hangolni az új feladatra. Ennek az eljárásnak a neve *transfer learning*.

Az objektumészlelő algoritmusok alkalmazási lehetőségeit a különböző területeken a 2. táblázat foglalja össze.

2. táblázat: Objektumészlelő algoritmusok alkalmazási lehetőségei a különböző területeken

Terület	**Alkalmazás**
Egészségügy	*Tumorfelismerés:* daganatok észlelése és lokalizálása orvosi képeken a pontos kezelés tervezése érdekében.
Autóipar	*Önvezető autók:* járművek, gyalogosok, útjelző táblák és akadályok észlelése és lokalizálása a biztonságos navigáció érdekében. *Forgalomfigyelés:* járművek észlelése és számlálása a forgalmi felvételeken a forgalom elemzéséhez és kezeléséhez.
Logisztika és kereskedelem	*Automatizált fizetés:* termékek észlelése és felismerése a pénztárnál az automatikus számlázás érdekében. *Polcfigyelés:* termékelhelyezés és készletszint észlelése az üzletek polcain a készletkezeléshez.
Biztonság és területvédelem	*Behatolásészlelés:* illetéktelen személyek vagy tárgyak észlelése és nyomon követése korlátozott területeken. *Közbiztonság:* tömegsűrűség és a közterületi viselkedés észlelése és elemzése a biztonság és a védelem irányítása érdekében.
Ipar	*Automatizált összeszerelősor:* alkatrészek meglétének észlelése és ellenőrzése az összeszerelés során. *Minőség-ellenőrzés:* termékek hibáinak észlelése és lokalizálása. *Robotika:* Lehetővé teszi a robotok számára, hogy észleljék az objektumokat, és interakcióba lépjenek velük.[31] *Drónnavigáció:* akadályok észlelése a navigáláshoz ütközés elkerülése érdekében.[32]
Védelmi szféra	*Felügyeleti rendszerek:* potenciális célpontok (például személyzet, járművek, fegyverek) valós idejű észlelése és lokalizálása.[33] *Fegyverirányítás:* rakéta- és tüzérségi rendszerek pontosságának növelése a célpontok valós idejű észlelésével és követésével. *Aknaérzékelés:* aknamezők azonosítása és feltérképezése tárgyfelismerő technikák segítségével speciális érzékelőkről gyűjtött képeken.[34]

Forrás: a szerző szerkesztése

Az objektumészlelő algoritmusok kiegészíthetők különböző eljárásokkal, aminek köszönhetően az egymást követő képeken azonosítani tudjuk a különböző objektumegyedeket, így a mozgóképeken követni lehet azok mozgását. Például célszerű, ha egy forgalommegfigyelő rendszer képes meghatározni, hogy két egymás után következő képen ugyanazt az objektumot észleltük (amely feltehetőleg elmozdult), vagy két egymástól független objektumot. Ez megvalósítható a két egymást követő képkockán észlelt határoló keretek koordinátáinak az elemzésével. Ugyanakkor ezek az algoritmusok felhasználhatják az észlelés során az objektumokról kinyert jellemzőtérképeket, ezzel

[31] Németh–Virágh 2022c: 1.
[32] Németh–Virágh 2022c: 5.
[33] Erdész 2023: 8.
[34] Qiu et al. 2023.

növelve a követési pontosságot és csökkentve azokat az eseteket, ahol egy objektum egy képsorozat alatt két különböző objektumként van észlelve. Példa egy ilyen eljárásra a DeepSORT, amely a kinyert konvolúciós jellemzőket is figyelembe veszi, amikor két egymást követő képkockán társítja az észlelt objektumokat.[35] Ez például drónfelvételek elemzésénél lehet hasznos, amikor nemcsak az észlelt objektumok vannak mozgásban, hanem a drón (nézőpont) is elmozdul.

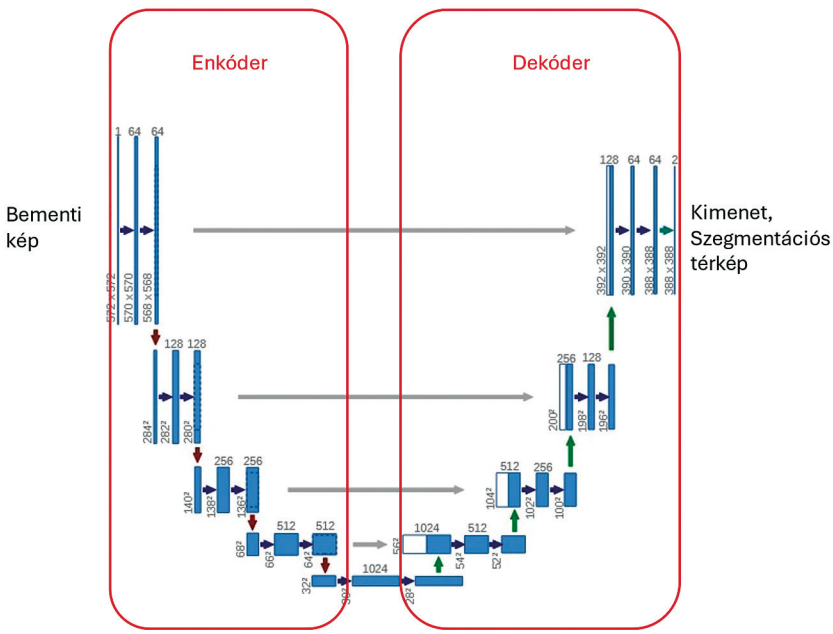
Szegmentáció

A szemantikus szegmentáció során a képet több részre vagy szegmensre osztják, ilyenkor sok esetben pixelenként határolják el az objektumokat. Ez a módszer lehetővé teszi, hogy a gépi látás rendszerei pontosabban észleljék és értelmezzék a képeken található objektumokat, hiszen a neuronháló kimenete nemcsak egy egyszerű téglalap alakú keret lesz, hanem az adott objektum vagy anomália pontos határait egy poligon vagy egy maszk határozza meg. A képosztályozási, az objektumészlelési és a szegmentációs feladatok közötti különbségeket a 4. ábra szemlélteti. Az ezt megvalósító algoritmusok alkalmazása széles körű, de talán a legelterjedtebben az orvosi képalkotásban használják diagnosztikai célokra,[36] vagy az autonóm járművek fejlesztése során[37] az út és a közlekedési táblák észlelésére. A szemantikus szegmentáció a távérzékelés területén is megállja a helyét, itt gondolhatunk a felszínborítottság becslésére is.[38] Ez az eljárás alkalmazható építkezés tervezésére, a mezőgazdaságban a termés minőségének becslésére vagy akár a védelmi szférában a műveletek megtervezésénél. A mindennapokból az egyik leglátványosabb példa talán a Teamsen, a Zoomon vagy más online, videó átvitelére alkalmas kommunikációs platformokon a háttércsere-funkció: amikor az alkalmazás elkülöníti az alanyt a háttértől, majd az utóbbit elhomályosítja vagy teljes egészében lecseréli egy (álló vagy mozgó) képre.

4. ábra: Példák képosztályozási, objektumészlelési, szemantikus szegmentációs és egyedszegmentációs feladatokra[39]
Forrás: Li–Adeli 2024: 14

[35] Wojke–Bewley–Paulus 2017.
[36] Huang et al. 2020: 1.
[37] Hussain–Hamza–Samad 2022: 429.
[38] Ulmas–Liiv 2020: 10.
[39] Li–Adeli 2024: 14.

Erre a feladatra is nagy előszeretettel alkalmazzák a konvolúciós neuronhálókat. Egy úttörő architektúra volt az FCN *(fully convolutional network),*[40] amely kizárólag konvolúciós és összevonó rétegekből épül fel. Az FCN eredményét egy dekonvolúciós rétegen keresztül kapjuk, amelynek a feladata, hogy a sokdimenziós kis felbontású jellemzőtérképet visszaskálázza a bementi kép felbontására. Tekintettel arra, hogy kizárólag konvolúciós és összevonási műveleteket alkalmaz, a neuronháló hangolása után is minimális pontosságvesztéssel skálázható nagyobb vagy kisebb felbontású képek elemzésére egyaránt. Az orvosi diagnosztikában a legelterjedtebb architektúra az U-Net,[41] amelynek – mint a neve is jelzi – egy U alakú szerkezete van, és egy szimmetrikusan felépített enkóderből és dekóderből áll (lásd 5. ábra). Ez lehetővé teszi, hogy a mélyebb szinteken az enkóder által előállított jellemzők alapján a dekóder egyre pontosabb maszkokat alkosson, felhasználva a mélyebb és többdimenziós jellemzőtérképeket, valamint az enkóder ugyanazon szintjén található kevésbé összetett, de nagyobb felbontású jellemzőtérképeket is.



5. ábra: Az U-Net architektúra felépítése
Forrás: Ronneberger–Fischer–Brox 2015: 2 alapján a szerzők szerkesztése

Az U-Net architektúra nemcsak arra alkalmazható, hogy a képeket különböző előre definiált osztályokba soroljuk, hanem a képmélység térképének a megközelítő becslésére is.[42]

[40] Long–Shelhamer–Darrell 2015.
[41] Ronneberger–Fischer–Brox 2015.
[42] Alhashim–Wonka 2019.

Az objektumészlelő algoritmusok és egy leegyszerűsített FCN ötvözéséből gyakorlatilag egyedszegmentációra képes architektúrák kialakítása lehetséges. Például az előző részben tárgyalt Faster R-CNN háló minimális módosításával és egy új ág hozzáadásával egy pontos szegmentációra képes Mask R-CNN[43] architektúrát kapunk.[44] Természetesen az új YOLO architektúrák is rendelkeznek hasonló variánsokkal, amelyek a határoló keretek mellett képesek egyedszegmentációt is elvégezni.[45] Ezekben az esetekben nem feltétlenül csak szemantikus szegmentációról beszélünk, hanem egyedszegmentációkról, ugyanis ugyanabba az osztályba tartozó maszkok is el vannak különítve egymástól, amint ezt a 4. ábra is szemlélteti. Lévén, hogy ezek az objektumészlelő algoritmusokhoz képest többletszámítást igényelhetnek, olyan esetekben, ahol egyáltalán nem előnyös az adott objektum pontos határainak a kijelölése, célszerű az egyszerűbb határolókeretes detektorok alkalmazása.

3. táblázat: Szegmentációs algoritmusok alkalmazási lehetőségei a különböző területeken

Terület	**Alkalmazás**
Egészségügy	*Képdiagnosztikák kiértékelése:* különböző képeken (például CT) daganatok vagy más anomáliák észlelése és elhatárolása.[46] *Műtétek tervezése:* különböző szövetek és szervek azonosítása és pontos elhatárolása.[47]
Autóipar	*Önvezető autók:* járművek, gyalogosok, illetve különböző felületek (út, járda, átjáró, sávok stb.) elhatárolása.[48]
Logisztika és kereskedelem	*Raktári automatizáció:* termékek automatikus szortírozása és nyomon követése, csomagok és címkék azonosítása.[49]
Szociális hálók, telekommunikáció	*Alany meghatározása:* fókuszban levő alany (személy vagy tárgy) elhatárolása például a háttér homályosítására vagy cseréjére.
Biztonság és területvédelem	*Behatolásészlelés:* illetéktelen személyek vagy tárgyak észlelése és nyomon követése korlátozott területeken.
Ipar	*Minőség-ellenőrzés:* termékek gyártási hibáinak észlelése és lokalizálása, mint például repedések vagy egyéb anyaghibák. *Robotika:* környezeti elemek szegmentálása a navigáció vagy mozgás precíz tervezéséhez, legyen az egyszerű szegmentáció vagy mélységbecslés.[50]
Védelmi szféra	*Célazonosítás:* földfelszín és katonai objektumok, járművek elhatárolása műholdas vagy légi felvételeken.[51] *Változáskövetés:* környezeti katasztrófák megfigyelése és területi változások monitorozása.[52]

Forrás: a szerzők szerkesztése

[43] He et al. 2018.
[44] He et al. 2018.
[45] Ultralytics Team 2022.
[46] Ma et al. 2022: 4.
[47] Ma et al. 2022: 2.
[48] Németh–Virágh 2022d: 1.
[49] Németh–Virágh 2023: 3.
[50] Németh–Virágh 2022c: 1.
[51] Erdész 2023: 8.
[52] Erdész 2023: 11.

Összegzés

A mesterséges intelligencia robbanásszerű fejlődésen esett át az elmúlt évtizedben, mind a polgári, mind a katonai szférában. Természetesen a fent összefoglalt, lassan klasszikusnak nevezhető gépi látással kapcsolatos feladatokon kívül rengeteg más célspecifikus feladatról lehet beszélni. A gépi látás technológiája egyértelműen kettős felhasználású, hiszen mind civil, mind katonai alkalmazásai felgyorsíthatják és automatizálhatják az információk feldolgozását és elemzését. A gyakorlati példákból kitűnik, hogy a mesterségesintelligencia-alapú látórendszerek számos ipari, biztonsági, közlekedési és egészségügyi területen nyújtanak megoldásokat, ugyanakkor a védelmi szférában is kulcsfontosságú szerepet töltenek be. Az autonóm járművek, orvosi diagnosztikai rendszerek és logisztikai alkalmazások mellett a felügyeleti rendszerek, behatolásérzékelők, célazonosító rendszerek és haditechnikai eszközök fejlesztése is ugyanazon gépi látási algoritmusokra építkezhet. A gépi látás alkalmazásai lehetővé teszik a valós idejű felderítést, a célazonosítást és a fenyegetések automatikus észlelését, amelyek egyaránt használhatók katonai és polgári biztonsági célokra. Az információs műveletek során az objektumkövető és anomáliaészlelő algoritmusok támogatják az adatvezérelt döntéshozatalt, ami a hadviselés és a kiberbiztonság terén is egyre meghatározóbb. Egy olyan világban, ahol az aszimmetrikus fenyegetések és az információs háborúk dominálnak, a gépi látás által nyújtott automatizált megfigyelési és elemzési képességek stratégiai előnyt, egyfajta információs vagy vezetési fölényt biztosítanak mind az államok, mind az ipari szereplők számára.

Ahhoz, hogy megfeleljük azt a kérdés, mekkora autonómiát adunk ezeknek a rendszereknek, természetesen mérlegelni kell, hogy ha az adott feladatot a gép hibásan hajtja végre, mekkora károk keletkezhetnek, illetve ki az a személy vagy szervezet, aki vagy amely felelős az okozott károkért. Fontos, hogy az ilyen rendszerek átláthatók legyenek, stabil teljesítményt nyújtsanak, minimálisra csökkentsék sebezhetőségüket. A gépi látás területén sok megoldatlan problémáról beszélhetünk, amely további kutatást igényel, mint például: hogyan állítsuk össze a hangolás során alkalmazott címkézett vagy akár címkézetlen adathalmazokat, mely architektúra nyújthatja a legjobb eredményt az adott célfeladatra, figyelembe véve az erőforrás-megszorításokat, vagy hogyan tudjuk teljes egészében kiküszöbölni a feketedoboz-problémát.

Felhasznált irodalom

A hibrid háború korszakába léptünk: de mit is jelent ez? *B COOL Magazin,* 2022. április 22. Online: https://bcoolmagazin.hu/a-hibrid-haboru-korszakaba-leptunk-de-mit-is-jelent-ez/

Alhashim, Ibraheem – Wonka, Peter (2019): High Quality Monocular Depth Estimation via Transfer Learning. *ArXiv,* 2019. március 10. Online: https://doi.org/10.48550/arXiv.1812.11941

Alom, Md Zahangir et al. (2018): The History Began from AlexNet: A Comprehensive Survey on Deep Learning Approaches. *ArXiv,* 2018. szeptember 13. Online: https://doi.org/10.48550/ARXIV.1803.01164

Andrej Karpathy [é. n.]. Online: https://karpathy.ai/
Boda Mihály (2023): A proxyháború filozófiai és etikai megközelítésben. *Honvédségi Szemle,* 151(6), 27–39. Online: https://doi.org/10.35926/HSZ.2023.6.3
Boda Mihály (2024): A kockázatkerülő háború és a bátorság a 20–21. század fordulóján. *Honvédségi Szemle,* 152(3), 113–125. Online: https://doi.org/10.35926/HSZ.2024.3.9
Brassai Sándor Tihamér (2019): *Neurális hálózatok és fuzzy logika.* Kolozsvár: Scientia Kiadó.
Deng, Jia et al. (2009): ImageNet: A Large-Scale Hierarchical Image Database. In *2009 IEEE Conference on Computer Vision and Pattern Recognition.* 248–255. Online: https://doi.org/10.1109/CVPR.2009.5206848
Du, Dawei et al. (2018): The Unmanned Aerial Vehicle Benchmark: Object Detection and Tracking. *ArXiv,* 2018. március 26. Online: https://doi.org/10.48550/arXiv.1804.00518
Erdész Viktor (2023): Milyen lehetőségeket hoz az új technológiák elterjedése a felderítés számára? In Kovács Zoltán (szerk.): *A mesterséges intelligencia és egyéb felforgató technológiák hatásainak átfogó vizsgálata.* Budapest: Katonai Nemzetbiztonsági Szolgálat, 440–465.
Everingham, Mark et al. (2010): The Pascal Visual Object Classes (VOC) Challenge. *International Journal of Computer Vision,* 88, 303–338. Online: https://doi.org/10.1007/s11263-009-0275-4
Girshick, Ross et al. (2013): Rich Feature Hierarchies for Accurate Object Detection and Semantic Segmentation. *ArXiv,* 2013. november 11. Online: https://doi.org/10.48550/ARXIV.1311.2524
Haig Zsolt et al. (2014): *Elektronikai hadviselés*. Budapest: Nemzeti Közszolgálati Egyetem.
Haig Zsolt – Várhegyi István (2005): *Hadviselés az információs hadszíntéren*. Budapest: Zrínyi Kiadó.
He, Kaiming et al. (2018): Mask R-CNN. *ArXiv,* 2018. január 24. Online: https://doi.org/10.48550/arXiv.1703.06870
Heakl, Ahmed et al. (2024): DroneVis: Versatile Computer Vision Library for Drones. *ArXiv,* 2024. június 1. Online: https://doi.org/10.48550/arXiv.2406.00447
Huang, Huimin et al. (2020): UNet 3+: A Full-Scale Connected UNet for Medical Image Segmentation. *ArXiv,* 2020. április 19. Online: https://doi.org/10.48550/arXiv.2004.08790
Hussain, Syed Muhammad Fasih – Hamza, Syed Muhammad – Samad, Abdul (2022): Image Segmentation for Autonomous Driving Using U-Net Inception. *2022 7th International Conference on Signal and Image Processing (ICSIP),* 426–429. Online: https://doi.org/10.1109/ICSIP55141.2022.9885809
Konrád György (1963): A korszerű háború korszerűtlensége I. *Valóság,* 6(6), 16–30.
Li, Fei-Fei – Adeli, Ehsan (2024): *CS231n: Deep Learning for ComputerVision.* Online: https://cs231n.stanford.edu/slides/2024/lecture_1_part_2.pdf
Lin, Tsung-Yi et al. (2014): Microsoft COCO: Common Objects in Context. In Fleet, David et al. (szerk.): *Computer Vision – ECCV 2014*. Cham: Springer, 740–455. Online: https://doi.org/10.1007/978-3-319-10602-1_48

Long, Jonathan – Shelhamer, Evan – Darrell, Trevor (2015): Fully Convolutional Networks for Semantic Segmentation. *2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR),* 3431–3440. Online: https://doi.org/10.1109/CVPR.2015.7298965

Ma, Jun et al. (2022): AbdomenCT-1K: Is Abdominal Organ Segmentation a Solved Problem? *IEEE Transactions on Pattern Analysis and Machine Intelligence,* 44(10), 6695–6714. Online: https://doi.org/10.1109/TPAMI.2021.3100536

Négyesi Imre (2023): A mesterséges intelligencia társadalmi és etikai kérdései. *Honvédségi Szemle,* 151(4), 6–18. Online: https://doi.org/10.35926/HSZ.2023.4.1

Németh András – Virágh Krisztián (2022a): Mesterséges intelligencia és haderő – A mesterséges intelligencia fejlődéstörténete I. rész. *Haditechnika,* 56(1), 17–22. Online: https://doi.org/10.23713/HT.56.1.03

Németh András – Virágh Krisztián (2022b): Mesterséges intelligencia és haderő – A mesterséges intelligencia fejlődéstörténete II. rész. *Haditechnika,* 56(2), 2–6. Online: https://doi.org/10.23713/HT.56.2.01

Németh András – Virágh Krisztián (2022c): Mesterséges intelligencia és haderő – Polgári alkalmazási lehetőségek V. rész. *Haditechnika,* 56(5), 2–7. Online: https://doi.org/10.23713/HT.56.5.01

Németh András – Virágh Krisztián (2022d): Mesterséges intelligencia és haderő VI. rész – További polgári alkalmazási lehetőségek. *Haditechnika,* 56(6), 2–7. Online: https://doi.org/10.23713/HT.56.6.01

Németh András – Virágh Krisztián (2023): Mesterséges intelligencia és haderő VII. Rész – Katonai alkalmazási lehetőségek. *Haditechnika,* 57(1), 2–6. Online: https://doi.org/10.23713/HT.57.1.01

Ploumis, Michail (2022): AI Weapon Systems in Future War Operations; Strategy, Operations and Tactics. *Comparative Strategy,* 41(1), 1–18. Online: https://doi.org/10.1080/01495933.2021.2017739

Qiu, Zhongze et al. (2023): Joint Fusion and Detection via Deep Learning in UAV-Borne Multispectral Sensing of Scatterable Landmine. *Sensors,* 23(12), 5693. Online: https://doi.org/10.3390/s23125693

Redmon, Joseph et al. (2015): You Only Look Once: Unified, Real-Time Object Detection. *ArXiv,* 2015. június 8. Online: https://doi.org/10.48550/ARXIV.1506.02640

Ronneberger, Olaf – Fischer, Philipp – Brox, Thomas (2015): U-Net: Convolutional Networks for Biomedical Image Segmentation. *ArXiv,* 2015. május 18. Online: https://doi.org/10.48550/arXiv.1505.04597

Szabadföldi István (2022): A mesterséges intelligencia alkalmazási lehetőségei az elektronikai hadviselésben. In Földi László (szerk.): *Szemelvények a katonai műszaki tudományok eredményeiből III*. Budapest: Ludovika Egyetemi Kiadó, 351–370.

Tesla Vision Update: Replacing Ultrasonic Sensors with Tesla Vision [é. n.]. Online: www.tesla.com/support/transitioning-tesla-vision

Thorbecke, Catherine (2020): Tesla on Autopilot Had Steered Driver towards Same Barrier before Fatal Crash, NTSB Says. *ABC News,* 2020. február 12. Online: https://abcnews.go.com/Business/tesla-autopilot-steered-driver-barrier-fatal-crash-ntsb/story?id=68936725

Ulmas, Priit – Liiv, Innar (2020): Segmentation of Satellite Imagery using U-Net Models for Land Cover Classification. *ArXiv,* 2020. március 5. Online: https://doi.org/10.48550/arXiv.2003.02899

Ultralytics Team (2022): Introducing Instance Segmentation in Ultralytics YOLOv5 v7.0. *Ultralytics,* 2022. november 23. Online: www.ultralytics.com/blog/introducing-instance-segmentation-in-yolov5-v7-0

Wang, Junjue et al. (2022): LoveDA: A Remote Sensing Land-Cover Dataset for Domain Adaptive Semantic Segmentation. *ArXiv,* 2022. október 17. Online: https://doi.org/10.48550/arXiv.2110.08733

Wojke, Nicolai – Bewley, Alex – Paulus, Dietrich (2017): Simple Online and Realtime Tracking with a Deep Association Metric. *ArXiv,* 2017. március 21. Online: https://doi.org/10.48550/ARXIV.1703.07402

Xia, Gui-Song et al. (2018): DOTA: A Large-Scale Dataset for Object Detection in Aerial Images. In *2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR),* 3974–3983. Online: https://doi.org/10.1109/CVPR.2018.00418

HADMÉRNÖK
VÉDELEMINFORMATIKA

20. évfolyam (2025) 1. szám 105–119.
DOI: 10.32567/hm.2025.1.6

Hankó Viktória[1]

Mesterséges intelligencia alkalmazása a kiberműveletekben

The Use of Artificial Intelligence in Cyber Operations

Absztrakt

A tanulmány a mesterséges intelligencia (MI) kiberbiztonsági alkalmazásait vizsgálja, kiemelve annak szerepét a modern kiberműveletekben. Az MI-technológiák lehetővé teszik a fenyegetések gyors azonosítását, az incidenskezelés hatékonyságának növelését és a védelmi folyamatok automatizálását. Az offenzív alkalmazások között megjelennek az MI-alapú támadási módszerek, például a deepfake technológia és az adaptív adathalászat. Az esettanulmány egy kitalált ország, Novaterra példáján keresztül mutatja be az MI integrációját a kritikus infrastruktúrák védelmébe, beleértve az energia-, víz- és pénzügyi rendszerek biztonságát. Az MI-alapú szimulációk jelentős védelmi potenciált hordoznak, ugyanakkor etikai kérdéseket is felvetnek. A kutatás rámutat, hogy az MI és a kiberbiztonság közötti szoros kapcsolat alapvető a fenntartható digitális társadalom megteremtéséhez. A technológia jövője az innováció és az etikus alkalmazás egyensúlyának megteremtésében rejlik.

Kulcsszavak: mesterséges intelligencia, kiberbiztonság, kiberműveletek

Abstract

The study examines the applications of artificial intelligence (AI) in cybersecurity, highlighting its role in modern cyber operations. AI technologies enable rapid threat identification, improve incident management efficiency and automate defence processes. Offensive applications include AI-based attack methods such as deepfake technology and adaptive

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola, e-mail: viktoria.hanko@protonmail.com

phishing. The case study uses the example of a fictional country, Novaterra, to illustrate the integration of AI into the protection of critical infrastructure, including energy, water and financial systems. AI-based simulations have significant defence potential but also raise ethical issues. The research shows that the close link between AI and cybersecurity is essential for creating a sustainable digital society. The future of the technology lies in balancing innovation and ethical application.

Keywords: artificial intelligence, cyber security, cyber operations

Bevezetés

A mesterséges intelligencia (a továbbiakban: MI) és a kiberbiztonság napjaink két meghatározó technológiai és társadalmi témája, amelyek szorosan összefonódnak, és alapvető hatást gyakorolnak életünk minden területére. Az MI forradalmi módon alakítja át az információfeldolgozást, a döntéshozatalt és a problémamegoldást, miközben a kiberbiztonság egyre fontosabbá válik a digitális térben való biztonságos működéshez. Az MI előnyei közé tartozik, hogy hatalmas mennyiségű adatot képes elemezni és értelmezni, így gyorsabb és pontosabb eredményeket produkál, mint bármely emberi erőfeszítés. Például az egészségügyben az MI segítségével gyorsabban diagnosztizálhatók bizonyos betegségek, mint például a rák korai stádiumai, ami életeket menthet. Ugyanakkor az MI kiberbiztonsági alkalmazásai is lenyűgözők: képes felismerni a hálózati forgalomban rejlő anomáliákat, és valós időben kiszűrni a potenciális fenyegetéseket. Azonban ugyanilyen hatékony lehet a támadói oldalon is: például az úgynevezett *deepfake* technológiával rendkívül hiteles hamis videók és hangfelvételek készíthetők, amelyek félrevezethetik a közvéleményt vagy manipulálhatják a döntéshozókat. A kiberbiztonság ezzel szemben arra hivatott, hogy megvédje az adatainkat, rendszereinket és magánszféránkat a rosszindulatú támadásoktól. Példa erre a banki szektor, ahol a kiberbiztonsági megoldások elengedhetetlenek az ügyfelek pénzügyi adatainak védelmében. A két terület szimbiózisban működik, hiszen az MI-alapú rendszerek növelik a kiberbiztonság hatékonyságát, míg a kiberbiztonság védi az MI-rendszereket a manipulációtól és a támadásoktól. Ennek ellenére az MI alkalmazása önmagában hordoz bizonyos kockázatokat, például olyan etikai kérdéseket, mint a magánszféra megsértése, míg a kiberbiztonság területén az egyre kifinomultabb támadások folyamatos kihívást jelentenek. Ezért létfontosságú, hogy mind a két fronton proaktív megközelítést alkalmazzunk, amely nemcsak a technológiai előnyökre épít, hanem figyelembe veszi a lehetséges veszélyeket is. Összekapcsolásuk és szinergiájuk kihasználása kulcsfontosságú a jövő digitális társadalmának biztonságos és fenntartható működése érdekében, ugyanakkor meg kell találni az egyensúlyt az innováció és a biztonság között. Ez különösen fontos olyan korban, amikor az adatok és az információk védelme alapvető emberi joggá válik, miközben a technológiai fejlődés lehetőséget teremt a globális problémák megoldására is. Az MI és a kiberbiztonság tehát nemcsak technológiai eszközök, hanem olyan alapvető építőelemek, amelyek meghatározzák társadalmunk jövőjét.

A kutatás célja, hogy feltárja a mesterséges intelligencia szerepét és lehetőségeit a kiberműveletekben, különös tekintettel a védelmi és támadó alkalmazásokra,

valamint a kritikus infrastruktúrák védelmére. A tanulmány módszertana kvalitatív jellegű, azaz irodalmi áttekintésen, valamint egy szimulációval alátámasztott esettanulmányon – a fiktív Novaterra állam példáján – keresztül elemzi az MI gyakorlati alkalmazását a kiberbiztonság területén.

A mesterséges intelligencia fogalmi keretei, alkalmazási területei

A mesterséges intelligencia egy digitális számítógép vagy számítógép-vezérelt robot azon képessége, hogy olyan feladatokat végezzen, amelyeket általában intelligens lényekkel társítanak. A kifejezést gyakran alkalmazzák az olyan rendszerek fejlesztésére irányuló projektekre, amelyek rendelkeznek az emberre jellemző intellektuális folyamatokkal, mint például az érvelés, az értelem felfedezése, az általánosítás vagy a múltbeli tapasztalatokból való tanulás képessége. Az 1940-es évekbeli kifejlesztésük óta a digitális számítógépeket úgy programozták, hogy nagyon összetett feladatokat – például matematikai tételek bizonyítását vagy sakkjátékot – nagy szakértelemmel végezzenek. A számítógépek feldolgozási sebességének és memóriakapacitásának folyamatos fejlődése ellenére még mindig nincsenek olyan programok, amelyek szélesebb területeken vagy a mindennapi tudást igénylő feladatokban teljes emberi rugalmasságot tudnának felmutatni. Másrészt egyes programok bizonyos speciális feladatok végrehajtásában elérték az emberi szakértők és szakemberek teljesítményszintjét, így a mesterséges intelligencia ebben a korlátozott értelemben olyan különböző alkalmazásokban is megtalálható, mint az orvosi diagnosztika, a számítógépes keresőmotorok, a hang- vagy kézírás-felismerés és a chatbotok.[2] Mára a technológiai fejlődés egyik legfontosabb hajtóerejévé vált, jelentős hatással az iparra, a társadalomra és a mindennapi életre.

Egy teljes körű, végponttól végpontig terjedő MI-megoldás képes az emberi szintű tudás befogadására (például gépi olvasás és számítógépes látás révén), és ezen információk felhasználásával olyan feladatok automatizálására és felgyorsítására, amelyeket korábban csak emberek végeztek.[3] Az Alan Turing (1950) által javasolt Turing-tesztet gondolatkísérletként alkották meg annak érdekében, hogy empirikus módon igazolható választ adjon a „Gondolkodhat-e egy gép?" kérdésre, elkerülve a kérdés filozófiai értelmezésének bizonytalanságait. A számítógép akkor megy át a teszten, ha egy emberi kérdezőbiztos néhány írásbeli kérdés feltevése után nem tudja megállapítani, hogy az írásbeli válaszok egy embertől vagy egy számítógéptől származnak-e. A számítógépnek a következő képességekre lenne szüksége:

- *Természetes nyelvfeldolgozás* (*natural language processing,* NLP), hogy sikeresen kommunikáljon emberi nyelven. Az NLP az emberi nyelv megértésére és generálására összpontosít. Az olyan technológiák, mint a chatbotok, a szövegfordítók vagy a hangvezérelt asszisztensek, az NLP eredményeire épülnek.
- *Tudásreprezentáció (knowledge representation)* ahhoz, hogy el tudja tárolni, amit tud vagy hall. Kulcsszerepet játszik a mesterséges intelligenciában, mivel

[2] Copeland [é. n.].
[3] Taddy 2018.

lehetővé teszi a rendszerek számára az információk strukturált formában történő tárolását és feldolgozását, ezáltal támogatva a döntéshozatalt és a problémamegoldást. Például a gyógyászatban található diagnosztikai rendszerekben kifejezetten az onkológiák használják a betegségek osztályozására és kezelésére.

- *Automatizált következtetés (automated reasoning)* a kérdések megválaszolásához és új következtetések levonásához. Ez lehetővé teszi a mesterségesintelligencia-rendszerek számára, hogy logikai szabályok és algoritmusok alapján önállóan vonjanak le következtetéseket, ezzel segítve a komplex problémák gyors megoldását. Használatos jogi dokumentumok elemzésére, például szerződések feltételeinek és ellentmondásainak automatikus azonosítására, ami megkönnyíti a jogi szakemberek munkáját és csökkenti a hibalehetőségeket.
- *Gépi tanulás* (*machine learning,* ML) az új körülményekhez való alkalmazkodáshoz, valamint a minták felismeréséhez és extrapolálásához. Az ML része, amely a legnagyobb nyilvánosságot kapja – olyannyira, hogy gyakran összekeverik az egész MI-vel. Emellett az egyik legfontosabb ága is, amely lehetővé teszi a rendszerek számára, hogy adatokból tanuljanak, és idővel egyre pontosabb döntéseket hozzanak. A gépi tanulási algoritmusok különféle típusai közé tartoznak a felügyelt tanulás, a felügyelet nélküli tanulás és a megerősítéses tanulás. Ennek egyik ága a *mélytanulás (deep learning),* az ML egy speciális formája, amely mély neurális hálózatok segítségével tanul és értelmez összetett mintákat. Az ilyen rendszerek különösen jól alkalmazhatók képfelismerésre, beszédfelismerésre és természetes nyelv feldolgozására.

A teljes Turing-teszt teljesítéséhez a robotnak a továbbiakra van szüksége:

- *Számítógépes látás (computer vision)* és *beszédfelismerés (speech recognition)* a világ értékeléséhez. Ezek az MI azon ágai, amelyek a vizuális adatok, például képek és videók elemzésére és értelmezésére szolgálnak. A számítógépes látás technológiáit használják például önvezető autókban, arcfelismerésben és orvosi képalkotásban.
- *Robotika,* amely a tárgyak manipulálásához és a mozgáshoz szükséges. Az MI-vezérelt robotok képesek az érzékelésre, az elemzésre és az autonóm cselekvésre. A robotika egyesíti az MI-t a mechanikai rendszerekkel, és alkalmazási területei között megtalálható a gyártás, az egészségügy és a mezőgazdaság.

Ez a hat részterület alkotja a mesterséges intelligencia nagy részét. A mesterséges intelligencia kutatói mégis kevés erőfeszítést fordítottak a Turing-teszt teljesítésére, mivel úgy vélik, hogy fontosabb az intelligencia mögöttes elveinek tanulmányozása.[4]

A mesterséges intelligencia szinte minden iparágban és társadalmi területen megjelent, és számos konkrét alkalmazási lehetőséget kínál, többek között a következő területeket:

[4] Russell–Norvig 2020.

1. *Egészségügy:* az MI megjelenése forradalmasíthatja az egészségügyi diagnosztikát és kezelést. Például az MI-alapú rendszerek képesek korai stádiumú betegségeket, a rákot felismerni radiológiai képek elemzésével. A gyógyszerkutatásban az alkalmazása felgyorsíthatja az új gyógyszerek kifejlesztését és tesztelését.
2. *Közlekedés:* meghatározó szerepet játszik az önvezető járművek fejlesztésében, amelyek a környezetük érzékelésére és az autonóm navigációra képesek. Ezenkívül az MI-alapú forgalomirányító rendszerek optimalizálhatják a közlekedést, csökkentve a dugók számát.
3. *Pénzügy:* segítségével hatékonyabbá válhat a csalásfelderítés, a hitelképesség-elemzés és az algoritmikus kereskedés. A bankok és a pénzügyi intézmények olyan rendszereket alkalmazhatnak, amelyek valós időben elemzik az ügyfelek tranzakcióit és azonosítják a gyanús tevékenységeket.[5]

A fentiek alapján elmondható, hogy előnyei között szerepel a hatékonyság növelése, az emberi munkaerő tehermentesítése és az új innovációs lehetőségek megnyitása. Az MI-rendszerek képesek olyan mennyiségű adatot feldolgozni, amely az ember számára kezelhetetlen lenne, így gyorsabb és pontosabb döntéseket hoznak. Például egy MI-vezérelt diagnosztikai rendszer több millió beteg adatait elemezve képes egyedi, személyre szabott kezelési javaslatokat nyújtani. Ugyanakkor az alkalmazása jelentős etikai és társadalmi kérdéseket vet fel. A magánélet védelme, az adatok biztonsága és az algoritmusok elfogultsága mind olyan problémák, amelyeket nem szabad figyelmen kívül hagyni. Az MI-vezérelt rendszerek bevezetése emellett munkahelyek elvesztéséhez járulhat hozzá az automatizáció miatt, ami különösen érzékeny téma bizonyos iparágakban. Jövőjét tekintve tele van lehetőségekkel, de a felelős fejlesztés és alkalmazás elengedhetetlen ahhoz, hogy a technológia pozitív hatásai érvényesüljenek. Az MI folyamatos fejlődése új megoldásokat hozhat az egészségügy, a közlekedés és a fenntarthatóság területén, miközben egyre fontosabbá válik az etikai kérdések kezelése.[6] Ezek a kérdések rávilágítanak annak jelentőségére, hogy átlátható, etikus gyakorlatok figyelembevételével történő tervezés és használat szükséges. Az a tény, hogy az MI által működtetett védelmi intézkedések hatalmas mennyiségű adatot képesek összegyűjteni és nyomon követni, az egyik legfőbb aggodalom napjainkban. Az ezekből a képességekből eredő lehetséges adatvédelmi incidensek az egyik fő aggály. Az etikai problémák azonnali felismerése érdekében egyidejűleg védenünk kell a felhasználók személyes adatait is. A kiberbiztonság esetében a fenyegetések felismerése elfogult lehet, ami egyes emberek téves azonosításához vagy mások igazságtalan jellemzéséhez vezethet. Az etikai normák betartása és az esetleges igazságtalan hatások lehetőségének csökkentése szempontjából kulcsfontosságú annak biztosítása, hogy az MI-védelmi megoldásokat tisztességesen hozzák létre és használják fel. Problémák akkor merülnek fel, ha a döntéshozatali folyamat nem egyértelmű.[7]

[5] Zhang–Lu 2021.
[6] Shukla–Jaiswal 2013.
[7] Kaushik et al. 2024.

A mesterséges intelligencia és a kiberbiztonság kapcsolata

Ahogy az a korábbi fejezetben olvasható, az MI-nek számos területen rengeteg előnye és felhasználási lehetősége van, ezek közül az egyik a kiberbiztonság. A kibertámadások gyors fejlődése és az eszközök elterjedése miatt ez a technológia segíthet lépést tartani a kiberbűnözőkkel, automatizálni a fenyegetések észlelését és hatékonyabban reagálni, mint a hagyományos szoftveres vagy ember által vezérelt módszerek. A kiberbiztonságban való felhasználás néhány előnye és felhasználási módja:

- *Újonnan felmerülő fenyegetések azonosítása:* az MI felhasználható a kibertérből érkező kockázatok és a potenciálisan káros tevékenységek azonosítására. Mivel a hagyományos szoftverrendszerek nem képesek lépést tartani a hetente keletkező új vírusok óriási mennyiségével, ez az a terület, ahol az MI valódi segítséget nyújthat. Ezeket a rendszereket úgy tervezték, hogy összetett algoritmusok felhasználásával azonosítsák a rosszindulatú szoftvereket, előrejelző modellezést végezzenek, és még a legkevésbé kompakt rosszindulatú szoftvereket vagy zsarolóvírusos támadásokat is képesek legyenek azonosítani, mielőtt azok bejutnának a rendszerbe.
- *Botok elleni küzdelem:* a botok ma már az internetes forgalom jelentős részét teszik ki, és veszélyesek lehetnek. A botok valódi fenyegetést jelenthetnek, a lopott jelszavakkal történő fiókátvételtől kezdve a hamis fiókok létrehozásán át az adatlopásig. Az automatizált fenyegetéseket nem lehet csak kézi válaszokkal legyőzni. Az MI segít a webhelyforgalom átfogó ismereteinek kialakításában és a jó botok (például a keresőmotorok) megkülönböztetésében a káros botoktól és emberektől. Továbbá megkönnyíti a hatalmas mennyiségű adatok elemzését, és lehetővé teszi a kiberbiztonsági szakemberek számára, hogy a folyamatosan változó fenyegetettségi környezethez igazodva módosítsák módszereiket, védelmi mechanizmusaikat.
- Kockázat-előrejelzés: az MI-rendszerek segítenek az IT-eszközleltár meghatározásában, amely egy átfogó és pontos lista az összes eszközről, felhasználóról és alkalmazásról, amelyek különböző mértékben hozzáférnek a különböző rendszerekhez. A jelenlegi helyzetben ezek a rendszerek képesek előre jelezni, hogy a vállalati irányítással és a fenyegetések kitettségével kapcsolatban hogyan és mikor a legvalószínűbb, hogy feltörik őket, ezért a vezetés átirányíthatja az erőforrásokat a legveszélyeztetettebb régiókba.[8]

Azonban már a korábbi szakaszban, a hálózatépítés során is megjelenhet az MI mint megoldás, hiszen a hálózat tervezői nem feltétlenül találják meg a hálózati topológia sebezhetőségét és bizonytalanságát. A hálózat használatának folyamatában a nem egyenletes adatáramlás, amely feltárja a hálózat helyzetét, előre érzékeli a hálózat gyenge láncszemét, alapot biztosít a hálózat kiigazításához, így szükség van a hálózati helyzetismeret használatára. A hálózati helyzetfelismerés folyamatában az összetett hálózatokat modellezni kell, szükséges elemezni a hálózat biztonsági helyzetét, és végül meg kell adni a hálózati helyzetfelismerés mennyiségi eredményeit. Ennek

[8] Mohammed 2020.

a folyamatnak az eléréséhez szükséges, hogy a helyzetfelismerési modell erős tudásbázissal rendelkezzen, amelyből gyorsan felismeri és hozzáigazítja a hálózati helyzetet. Ugyanakkor a modellnek képesnek kell lennie a jellemzők kinyerésére.[9] Emellett az 5G megjelenésével néhány kutató elkezdte tanulmányozni az 5G-technológiák anomáliaérzékelését. Például egyes kutatók egy adaptív mélytanuláson alapuló 5G-hálózati anomáliafelismerő rendszert javasoltak. Ebben a keretrendszerben két réteg mélytanulási modellt használtak: az egyik a hálózati áramlás aggregációs észlelésének módszerére összpontosított a rendellenes jelek gyors keresésével, főként mély neurális hálózatot használtak a feldolgozáshoz, a másik az idővonal és a kapcsolódó jellemzők közötti viszonyon alapult a hálózati anomáliák azonosítására, és közvetlenül kommunikált a felügyeleti és diagnosztikai modullal az anomáliák megtalálása érdekében. A hosszú rövid távú memóriát (LSTM) az idősorok jó kezeléséhez implementálták.[10]

Ezek a módszerek mind pozitív megközelítései az MI és a kiberbiztonság kapcsolatának. Azonban nem szabad elmennünk amellett, hogy ma már számos kifinomult, mesterséges intelligencia által vezérelt kibertámadási módszer áll a kiberbűnözők rendelkezésére, amelyekkel problémákat okozhatnak a kormányzatnak, a szervezeteknek, a vállalkozásoknak és az egyéneknek. Az MI által vezérelt kibertámadások az utóbbi években egyre nagyobb számban fordulnak elő. Még ha sok szervezet át is tér a biztonságosabb kibertérbe, például a felhőalapú tárolási szolgáltatások bevezetésére, erőforrásaik továbbra is sebezhetők maradnak. Általánosságban elmondható, hogy ezek a támadástípusok csak súlyosbodni fognak, majd a hagyományos kiberbiztonsági eszközök számára szinte lehetetlen lesz felismerni azokat. Ez egyszerűen a gépi hatékonyság vs. emberi erőfeszítés kérdése. Ennek a növekvő trendnek a komplexitása és mérete további kihívások elé állítja a kiberbiztonsági szakembereket. Ezzel szemben a fenyegetés sikeres elhárításához szükséges, magasan képzett szakemberek egyre drágábbak és nehezebben találhatók meg. Az újonnan megjelenő támadási technikák következményei károsak lehetnek. Egyes kutatók szerint az MI által vezérelt kibertámadási technikák képesek lesznek alkalmazkodni ahhoz a környezethez, amelyben végrehajtják őket. A kontextuális adatokból vagy információkból tanulva kihasználhatják a sebezhetőségeket, vagy megbízható rendszerjellemzőknek álcázhatják magukat.[11]

Az MI és a kiberbiztonság szoros kapcsolata a korábban bemutatott, civil életben tapasztalt előnyök mellett a katonai műveletekben is kiemelkedő fontosságú. A modern hadviselés egyre inkább támaszkodik a kibertéri műveletekre, ahol az MI-technológiák gyorsítják az adatfeldolgozást és a döntéshozatalt, míg a kiberbiztonság védi az érzékeny rendszereket az ellenséges beavatkozásoktól. E kettő kombinációja alapvetővé vált a hadseregek stratégiájában, biztosítva a technológiai fölényt és a működési stabilitást a digitális térben.

[9] Zhang et al. 2022.
[10] Maimó et al. 2018.
[11] Guembe et al. 2022.

Kibertéri műveletek

A mesterséges intelligencia és a kiberbiztonság szoros összefonódása különösen jelentőségteljes a kiberműveletek területén, ahol az adatvezérelt döntéshozatal és a valós idejű fenyegetéskezelés alapvető követelmény. Az MI-technológiák lehetővé teszik a kiberműveletek hatékonyságának növelését, például az anomáliaészlelés, az automatizált válaszlépések és az ellenséges hálózatok elemzése terén. Eközben a kiberbiztonság szavatolja, hogy ezek a fejlett rendszerek védettek maradjanak az ellenséges manipulációval szemben, amely aláásná a műveletek sikerét. Emellett az MI egyre fontosabb szerepet tölt be a hadviselésben, mivel növeli a kiberműveletek hatékonyságát, támogatja az autonóm fegyverrendszerek fejlődését, és előmozdítja az ember és gép közötti kapcsolat kialakítását. Azonban nem csupán a hatékonyságot fokozó erőszorzóként *(force multiplier)* értelmezhető, hanem önálló eszközként is, amely képes stratégiai és taktikai döntéseket meghozni.[12]

A kibertéri műveletek a modern hadviselés és biztonságpolitika kulcsfontosságú elemeivé váltak, mivel az információs technológia fejlődése új dimenziót nyitott a konfliktusok és a védelem terén. Haig Zsolt értelmezése szerint a kibertéri műveleteket a következőképpen definiálhatjuk:

„A kibertéri műveletek a kibertérben érvényesülő információs képességek integrált, összehangolt és koordinált alkalmazására irányuló tevékenységek összessége, amelyek a műveletek célkitűzéseinek elérése érdekében, a kibertéri hálózatos infokommunikációs rendszereket felhasználva, a kognitív képességekkel közvetlenül, illetve a technikai képességekkel közvetetten hatásokat gyakorolnak a műveletekben részt vevő célközönség szándékára, helyzetértelmezésére és képességeire."[13]

A kibertéri műveletek és a kiberhadviselés szorosan összefonódnak, mivel mindkettő az információs technológia alkalmazásával befolyásolja a katonai és biztonsági műveletek kimenetelét. A kibertéri műveletek magukban foglalják a számítógépes hálózatok védelmét, támadását és kihasználását, míg a kiberhadviselés ezen tevékenységek katonai kontextusban történő alkalmazását jelenti. A modern hadviselésben a kiberhadviselés integrálása elengedhetetlen, hiszen a kibertérben végrehajtott támadások képesek megbénítani kritikus infrastruktúrákat, kommunikációs rendszereket és egyéb létfontosságú szolgáltatásokat. Ezért a kibertéri műveletek hatékony végrehajtása és a kiberhadviselési képességek fejlesztése kulcsfontosságú a nemzetbiztonság szempontjából. A NATO is felismerte a kibertér jelentőségét, és 2016-ban műveleti területként ismerte el, hangsúlyozva annak fontosságát a modern hadviselésben.[14] Ezáltal elmondható, hogy általánosan megfogalmazva a kiberhadviselés a kiberműveletek összefüggő sorozataként értelmezhető. Attól függően, hogy ezek a műveletek katonai vagy civil célpontok ellen irányulnak, más típusú műveletek is kapcsolódhatnak

[12] Boda 2024.
[13] Haig 2018: 15.
[14] Kassai 2022.

hozzájuk. Idetartozhatnak például a médiaműveletek, a pszichológiai műveletek, valamint az elektronikai hadviselés egyes elemei.[15]

A katonai elmélet a háborút három szintre osztja: hadászati (stratégiai), hadműveleti és harcászati (taktikai) szintre. Ezek a szintek összefüggnek egymással, és ami az egyik szinten történik, az befolyásolja a többit. A stratégiai szint a „hogyan nyerjünk háborút?" kérdéseivel foglalkozik. Számos államközi kibertéri művelet stratégiai szinten zajlik. A legtöbbjüket szándékosan úgy tervezték, hogy a fegyveres támadás küszöbértéke alatt maradjanak, hogy elkerüljék a hagyományos konfliktusba való eszkalálódást. A mai napig nem történt olyan összehangolt, stratégiai kiberháborús hadjárat egy másik állam ellen, amely elérte volna a fegyveres támadás szintjét, vagy könnyen háborúnak minősíthető lett volna. Ehhez a legközelebb az amerikai kiberparancsnokság által Irán ellen tervezett Nitro Zeus művelet áll, amelyet 2016-ban lepleztek le. Ez egy vészterv volt arra az esetre, ha elődje, az Olimpiai Játékok művelet, ismertebb nevén a Stuxnet, és az iráni atomprogram korlátozására irányuló diplomáciai erőfeszítések kudarcot vallanak. A hadműveleti szintre egy kitűnő példa az Orchard hadművelet (más néven Operation Outside the Box), amely 2007-ben zajlott Szíriában, és amelynek során izraeli hackerek Tell-Abjadban hatástalanítottak egy szíriai légvédelmi radart, majd gyors egymásutánban kinetikus légicsapást mértek. Az izraeli légierő ezután megsemmisített egy nukleáris kísérleti telepet az észak-szíriai Deir ez-Zórban. A műveletek sikeresek voltak, és a digitális komponens jelentős szerepet játszott abban, hogy az izraeli F–15-ös repülőgépek észrevétlenül léphessenek be a légtérbe. A taktikai szintről nem sokat lehet tudni, azonban Shane Harris újságíró kiterjedt kutatást végzett a 2007-es iraki felkelésellenes műveletek során alkalmazott támadó taktikai kiberműveletekről. Ennek a műveletnek három összetevője volt:

- Az NSA az iraki internetszolgáltatók telefonos metaadatait földrajzi térképekkel hozta összefüggésbe, így meg tudta határozni a rögtönzött robbanószerkezetek beindítására használt mobiltelefonok földrajzi helyét. Az NSA képes volt ezek egy részét távolról megsemmisíteni, vagy a közelben lévő felkelők tartózkodási helyét megtudni.
- Rosszindulatú szoftverek alkalmazása a felkelők számítógépes rendszerei ellen. Itt két változatot használtak. Az elsőben számos iraki felhasználót fertőztek meg nagy mennyiségben manipulált adathalász-e-maileken keresztül. A második a számítógépek célzott megfertőzését jelentette USB-n keresztül, amelyeket a terepen lévő taktikai kiberegységek vittek magukkal.
- Felkelők elleni információs műveletek. Az iraki telefonhálózathoz való hozzáféréssel az amerikai csapatok hamis szöveges üzeneteket küldtek a felkelőknek, hogy demoralizálják őket, vagy csapdát állítsanak.[16]

Ahogy azt a fejezet elején hangsúlyoztam, a mesterséges intelligencia kiemelt szerepet képvisel a kiberműveletek terén – kifejezetten a védelmi oldalon. Azonban ahogy arra egyes kutatók rámutatnak, az MI fejlődése mind a kiberbiztonságban való felhasználását, mind a visszaélést elősegítette. A hagyományos kibertámadásokkal ellentétben az új

[15] Kovács 2023.
[16] Schulze 2020.

formák az MI-rendszereket célozzák meg a viselkedés manipulálására, megkérdőjelezve az MI robusztusságában és ellenálló képességében rejlő lehetőségeket. Az adatok megfertőzése, a modellek manipulálása és a *backdoorok* nyitása az irányítás megszerzésének elsődleges módszerei. A mesterséges intelligencia fegyverként felhasználható olyan összetett kibertámadások indítására, mint a APT-támadások, az adathalászat és a *social engineering* támadások, amelyek jelentős kiberbiztonsági kihívásokat jelentenek. A rosszindulatú programok javítására vagy elrejtésére való felhasználása komoly fenyegetést jelent, mivel az olyan technikák, mint a kód meghamisítása és az adaptív viselkedés felvétele, kikerülik a jelenlegi észlelési módszereket. Az offenzív MI célzott kiválasztás, hitelesítéseltávolítás, gyors adathalászüzenet-készítés és összehangolt művelettervezés révén növelheti a rosszindulatú programok teljesítményét.[17]

Esettanulmány

Az előző fejezetekben bemutattuk az MI szerepét a kiberműveletekben, különös figyelmet fordítva az offenzív és defenzív alkalmazásokra. Ez a technológia képes felgyorsítani a fenyegetések felismerését, javítani az incidenskezelést, valamint automatizálni a védelmi folyamatokat. Kiemeltük, hogy az offenzív oldalon az MI-eszközökkel hatékonyan lehet manipulálni információkat és kihasználni a rendszerek gyenge pontjait – például *social engineering* támadásokon keresztül. Ugyanakkor a defenzív oldalon a mesterségesintelligencia-alapú rendszerek, mint például az anomáliaészlelés vagy az automatizált reagálás, jelentős védelmi potenciállal bírnak.

Ez a fejezet a korábban bemutatott alapelveket ülteti gyakorlatba egy fiktív ország, Novaterra példáján keresztül. Részletesen elemezzük, hogyan használja az MI-t az ország a kibervédelmi stratégiáiban, különös tekintettel a kritikus infrastruktúra védelmére.

Novaterra környezeti bemutatása

Novaterra egy fejlett technológiával rendelkező kis közép-európai állam, amely jelentős mértékben függ digitális infrastruktúrájától. Az ország gazdasága elsősorban az energiatermelésre, a fintechiparra és a technológiaorientált szolgáltatásokra épül, amelyeket kiterjedt villamosenergia-hálózat és fejlett kommunikációs rendszerek támogatnak. Ugyanakkor ezek az infrastruktúrák kiemelt célpontjai a kibertámadásoknak, legyen szó állami vagy nem állami szereplőkről. A kormány felismerte a digitális fenyegetések jelentőségét, és egy átfogó kiberbiztonsági stratégiát dolgozott ki, amelyben kulcsszerepet kapott a mesterséges intelligencia. Az MI-alapú rendszerek telepítése nemcsak a kritikus infrastruktúra védelmét szolgálja, hanem a folyamatos fenyegetések azonosítását és az incidensekre történő gyors reagálást is lehetővé teszi. Novaterra kiemelten épít a gépi tanulási algoritmusokra, amelyek képesek adaptálódni az állandóan változó fenyegetésekhez.

[17] Nobles 2024.

Az MI alkalmazása kritikus infrastruktúrák területén

Villamosenergia-hálózat: a villamosenergia-hálózat Novaterra gazdaságának gerince, amely szélerőműveket, naperőműveket és hagyományos erőműveket integrál. Ezáltal az MI-alapú rendszerek itt képesek valós időben monitorozni a hálózati forgalmat, érzékelni a szokatlan adatforgalmat és azonosítani a potenciális fenyegetéseket. Egy neurálishálózat-alapú anomáliaészlelési rendszer például felismeri, ha egy adott csomópontot szokatlanul nagy adatforgalom ér, ami DDoS-támadásra utalhat. Ezenkívül az MI képes optimalizálni az energiaelosztást, megelőzve az áramszolgáltatás megszakadását, amelyet egy kártékony támadás okozhatna. Ezek az előrejelzési modellek lehetővé teszik a hálózati terhelés dinamikus szabályozását is, amely csökkenti a meghibásodások kockázatát. Ez a megközelítés nemcsak a támadások hatékony kezelését biztosítja, hanem hozzájárul a rendszer hosszú távú fenntarthatóságához is. Az energiaiparban alkalmazott MI így egyszerre szolgálja a megelőzést és a válságkezelést.

Honvédelem: Novaterra hadseregében az MI az információgyűjtés és -elemzés kulcsfontosságú eszköze. Ennek segítségével folyamatosan elemzik az ellenséges kommunikációs csatornákat, és azonosítják a potenciális fenyegetéseket. Továbbá a kibertérből érkező támadásokat valós időben blokkolják, miközben az MI-rendszerek javaslatokat tesznek a műveleti egységeknek a megfelelő válaszintézkedésekre. Az MI közreműködésével szimulációkat futtatnak, hogy felkészüljenek az esetleges támadási forgatókönyvekre, és csökkentsék a valós konfliktusok kockázatait. Az autonóm rendszerek, például drónok és robotok, szintén MI-vezérelt megoldásokkal működnek, amelyek gyors adatfeldolgozásra és önálló döntéshozatalra képesek. Az MI ilyen integrációja jelentősen növeli a hadsereg hatékonyságát, miközben minimalizálja az emberi beavatkozás szükségességét. Ezáltal Novaterra védelmi stratégiája korszerű és alkalmazkodóképes marad a változó fenyegetésekkel szemben.

Rendvédelem: a rendvédelemben az MI-technológiákat főként a bűnügyi elemzésben és a kibertámadások elleni védekezésben alkalmazzák. Egy prediktív elemzési modell segít megállapítani, hogy mely szervezetek lehetnek a leginkább kitettek egy támadásnak, így lehetőség nyílik a proaktív védekezésre. Az MI-alapú rendszerek gyorsan elemezhetik a nagy mennyiségű bűnügyi adatot, segítve a minták felismerését és a gyanús tevékenységek azonosítását. Emellett az online csalások elleni harcban is hatékony eszközként jelennek meg, valós időben azonosítva a gyanús tranzakciókat. További alkalmazási terület az arcfelismerő rendszerek fejlesztése, amelyek az MI segítségével pontosabbak és gyorsabbak a gyanúsítottak azonosításában. A rendvédelemben az MI tehát nemcsak a bűnüldözés gyorsaságát növeli, hanem a megelőzésben is jelentős szerepet játszik. Ez a technológia segíti a rendfenntartó erők munkáját, miközben hozzájárul a lakosság biztonságának növeléséhez.

Pénzügy: a fintech szektorban az MI alkalmazása kulcsfontosságú a csalásfelderítés és a tranzakcióbiztonság terén. Novaterra bankjai MI-alapú rendszereket használnak a szokatlan tranzakciós minták azonosítására, amelyek között lehetnek gyanús pénzmozgások vagy adatlopási kísérletek. Ezen a területen prediktív elemzést alkalmaznak, hogy előre jelezzék az esetleges pénzügyi fenyegetéseket, minimalizálva a pénzmosás és egyéb illegális tevékenységek kockázatát. Továbbá a technológia hozzájárul az önkiszolgáló banki rendszerek biztonságának növeléséhez, valós időben védelmet nyújtva

az adathalász-támadások ellen. Az MI-alapú chatbotok gyorsan felismerik a gyanús interakciókat, és automatikusan értesítik a biztonsági csapatot. A pénzügyi szektorban nemcsak a biztonságot növeli az MI alkalmazása, hanem az ügyfélélményt is javítja, mivel gyorsabb és pontosabb kiszolgálást tesz lehetővé. Ezáltal a fintechipar képes lépést tartani a növekvő fenyegetésekkel és ügyféligényekkel egyaránt.

Vízszolgáltatás: a vízszolgáltatás kulcsfontosságú Novaterra lakossága számára, és a mesterséges intelligencia itt is jelentős védelmi szerepet tölt be. Az MI-alapú rendszerek folyamatosan monitorozzák a vízhálózat működését, észlelik a nyomáscsökkenéseket vagy a szennyezés jeleit, amelyek esetleg támadásra vagy rendszerhibára utalhatnak. A technológia által lehetőség nyílik valós időben reagálni az incidensekre, megelőzve a lakosságot érő súlyos károkat. Emellett prediktív modellezéssel előre jelezhetők a karbantartási igények, így biztosítható a szolgáltatás folyamatossága. Az MI-alapú rendszerek továbbá lehetővé teszik a vízfogyasztási minták elemzését, ami segíthet a vízkészletek hatékonyabb kezelésében. Ezáltal elmondható, hogy nemcsak a védelemben, hanem a fenntarthatóságban is kiemelt szerepet játszik az MI, tehát a vízszolgáltatás hatékonyabbá és biztonságosabbá válik, megfelelve a modern kihívásoknak.

A kiberhadviselés aspektusa

Novaterrában az MI kiemelkedő szerepet tölt be a kiberhadviselés területén, különösen az összetett támadások és védekezési mechanizmusok hatékony kezelésében. Támadói oldalon az MI alkalmazásával automatizálják a sérülékenységfelderítési folyamatokat, amelyek során az algoritmusok képesek gyorsan azonosítani a rendszerek gyenge pontjait, még azelőtt, hogy azokat manuális vizsgálatok felfedeznék. A dezinformációs kampányokban az MI-alapú generatív modellek, például a *deepfake* technológiák, hamisított vizuális és hanganyagok előállításával növelik a pszichológiai hadviselés hatékonyságát. Ezek az eszközök különösen akkor hatásosak, ha az ellenfél közvéleményének befolyásolása vagy belső instabilitás előidézése a cél. Védekezési oldalon is elengedhetetlen az MI alkalmazása a modern kibervédelmi rendszerek hatékonyságának biztosításához. Az országban adaptív biztonsági algoritmusokat alkalmaznak, amelyek valós időben elemzik a hálózati forgalmat, és azonosítják a gyanús tevékenységeket, például a szolgáltatásmegtagadási támadások (DDoS) korai jeleit. Az MI továbbá támogathatja a prediktív elemzési rendszereket, amelyek képesek előre jelezni az ellenséges támadások valószínűségét, lehetővé téve a proaktív védekezést. Például egy neurális hálózat segítségével modellezhetők az ellenséges aktorok viselkedési mintái, így azonosíthatók a potenciális célpontok és a támadási stratégiák. Mindemellett az MI-alapú szimulációk lehetőséget adnak arra is, hogy a kiberhadviselési forgatókönyveket valósághűen modellezzék. Ez segíti a döntéshozókat abban, hogy optimalizálják a védelmi stratégiákat, miközben minimalizálják az emberi hiba lehetőségét. A mesterséges intelligencia tehát a kiberhadviselés mindkét oldalán nélkülözhetetlen, mivel lehetővé teszi a gyors alkalmazkodást és a stratégiai előnyök kihasználását egy folyamatosan változó digitális környezetben.

Forgatókönyv: DDoS-támadás egy villamosenergia-hálózat ellen

A szimuláció alapvető célja, hogy tesztelje Novaterra villamosenergia-hálózatának védelmi mechanizmusait egy DDoS-támadás ellen. A szimuláció további célja, hogy azonosítsa a rendszer azon gyenge pontjait, amelyek kihasználhatók lennének egy valós támadás során, miközben javítja a reagálási időt.

A forgatókönyvben az MI-alapú szimulációs rendszer virtuális környezetben modellezi a villamosenergia-hálózatot. A szimuláció részeként az alábbi fő elemek jelennek meg:

- Támadási szcenárió: az MI generál egy széles körű DDoS-támadást, amelyben az adatcsomagok nagymértékű áradata irányul az erőműveket felügyelő rendszerekre.
- Védelmi reakció: az MI-alapú védelmi rendszer valós időben elemzi a beérkező adatforgalmat, azonosítja a legitim és illegitim csomagokat, majd automatikusan blokkolja a rosszindulatú adatokat.
- Hatékonyság mérése: a rendszer méri a reagálási időt, a sikeresen blokkolt csomagok arányát, valamint az üzemzavarok hatását a hálózat stabilitására.

A szimuláció kimutatta, hogy a védelmi rendszer 95%-os hatékonysággal blokkolta a támadási adatcsomagokat, miközben minimális késlekedést okozott a legitim forgalomban. Az anomáliaészlelési rendszer korábban nem ismert mintákat is felfedezett, amelyek a jövőbeni finomhangolás alapjául szolgálhatnak. Emellett a szimuláció során felismerték, hogy egyes adatcsomagok dinamikus blokkolása további optimalizálást igényel, hogy teljes mértékben elkerüljön minden működési zavart. Emellett ez a forgatókönyv bemutatja, hogy az MI-alapú szimulációk hogyan segíthetik Novaterra kiberbiztonsági stratégiájának fejlesztését. Az ilyen technológiák nemcsak az azonnali fenyegetések elhárításában hatékonyak, hanem hozzájárulnak a hosszú távú védelmi stratégiák optimalizálásához is. A szimuláció alapján kidolgozott javaslatok támogatják a rendszerszintű ellenálló képességek kiépítését és a nemzetgazdasági stabilitás fenntartását egyre komplexebb kiberfenyegetések közepette.

A fent leírtakat figyelembe véve elmondható, hogy Novaterra esete rávilágít a mesterséges intelligencia fontosságára a defenzív kiberműveletekben, különös tekintettel a kritikus infrastruktúrák védelmére. Az MI alkalmazása lehetővé teszi a fenyegetések gyors felismerését, a rendszerek adaptálását és az automatizált reagálást, ezáltal növelve az állami és gazdasági stabilitást. Ugyanakkor nem csupán technológiai, hanem etikai kihívásokat is felvet az alkalmazása, amelyeket meg kell oldani a biztonság fenntartása érdekében. Novaterra példája megmutatja, hogy a mesterséges intelligencia nemcsak hatékony védelmi eszköz, hanem a digitális jövő egyik meghatározó eleme.

Összegzés és következtetések

A mesterséges intelligencia alkalmazása a kiberműveletekben jelentős lehetőségeket és kihívásokat hordoz. Az MI a kiberbiztonság védelmi oldalán kiemelkedő

hatékonyságot nyújt az anomáliaészlelésben, fenyegetések valós idejű kezelésében és az automatizált válaszlépések kidolgozásában. Ugyanakkor az offenzív oldalon az MI-támogatott támadások, például a *deepfake* technológia és az adathalászat, új fenyegetési dimenziókat nyitnak. Az etikai és biztonsági kockázatok hangsúlyozzák a felelősségteljes fejlesztés szükségességét. A cikk esettanulmánya, Novaterra példája bemutatja az MI alkalmazásának stratégiai szerepét a kritikus infrastruktúrák védelmében, amely képes gyorsan alkalmazkodni a változó fenyegetésekhez. Az MI szimbiózisa a kiberbiztonsággal kulcsfontosságú a digitális jövő megbízhatóságának biztosításában, ugyanakkor kiegyensúlyozott megközelítés szükséges az innováció és a biztonság között.

További kutatási irányként lehetőséget látok abban, hogy a jelenlegi fikcióalapú modell egy virtuális környezetben megvalósított, konkrét gyakorlati tesztelés formáját öltse, amelyben az MI-rendszerek működését különböző tudományos módszerekkel, például kvantitatív elemzésekkel, szimulációs modellezéssel és értékelési keretrendszerekkel vizsgálnám.

Felhasznált irodalom

Boda Mihály (2024): A kockázatkerülő háború és a bátorság a 20–21. század fordulóján. *Honvédségi Szemle,* 152(3), 113–125. Online: https://doi.org/10.35926/HSZ.2024.3.9

Copeland, B. J. [é. n.]: Artificial Intelligence. *Britannica*. Online: www.britannica.com/technology/artificial-intelligence

Guembe, Blessing et al. (2022): The Emerging Threat of Ai-Driven Cyber Attacks: A Review. *Applied Artificial Intelligence,* 36(1). Online: https://doi.org/10.1080/08839514.2022.2037254

Haig Zsolt (2019): *Információs műveletek a kibertérben*. Budapest: Dialóg Campus Kiadó.

Kassai Károly (2022): A kibertér műveleti képesség szerepének, jelentőségének és fókuszának evolúciója a NATO stratégiai dokumentumai alapján. *Military and Intelligence CyberSecurity Research Paper,* (9), 1–38. Online: http://hdl.handle.net/20.500.12944/100742

Kaushik, Keshav et al. (2024): Ethical Considerations in AI-Based Cybersecurity. In Kaushik, Keshav – Sharma, Ishu (szerk.): *Next-Generation Cybersecurity. AI, ML, Blockchain*. Singapore: Springer, 437–470. Online: https://doi.org/10.1007/978-981-97-1249-6_19

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

Maimó, Lorenzo Fernández et al. (2018): A Self-Adaptive Deep Learning-Based System for Anomaly Detection in 5G Networks. *EEE Access,* 6, 7700–7712. Online: https://doi.org/10.1109/ACCESS.2018.2803446

Mohammed, Ishaq Azhar (2020): Artificial Intelligence for Cybersecurity: A Systematic Mapping of Literature. *International Journal of Innovations in Engineering Research and Technology,* 7(9), 172–176. Online: https://repo.ijiert.org/index.php/ijiert/article/view/2797

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

Russell, Stuart – Norvig, Peter (2020): *Artificial Intelligence. A Modern Approach. 4th Edition.* London: Pearson.

Schulze, Matthias (2020): Cyber in War: Assessing the Strategic, Tactical, and Operational Utility of Military Cyber Operations. *12th International Conference on Cyber Conflict (CyCon),* 183–197. Online: https://doi.org/10.23919/CyCon49761.2020.9131733

Shukla, Shubhendu S. – Jaiswal, Vijay (2013): Applicability of Artificial Intelligence in Different Fields of Life. *International Journal of Scientific Engineering and Research*, 1(1), 28–35. Online: www.doi.org/10.70729/1130915

Taddy, Matthew Alan (2018): The Technological Elements of Artificial Intelligence. *NBER Working Paper,* w24301. Online: www.nber.org/system/files/working_papers/w24301/w24301.pdf

Zhang, Caiming – Lu, Yang (2021): Study on Artificial Intelligence: The State of the Art and Future Prospects. *Journal of Industrial Information Integration,* 23, 100224. Online: https://doi.org/10.1016/j.jii.2021.100224

Zhang, Zhimin et al. (2022): Artificial Intelligence in Cyber Security: Research Advances, Challenges, and Opportunities. *Artificial Intelligence Review,* 55, 1029–1053. Online: https://doi.org/10.1007/s10462-021-09976-0

HADMÉRNÖK
VÉDELEMINFORMATIKA

20. évfolyam (2025) 1. szám 121–137.
DOI: 10.32567/hm.2025.1.7

Harangozó Valentin[1]

Kiberbiztonság a városi mobilitásban, fókuszban az e-rollerek, 2. rész

Cybersecurity in Urban Mobility, Focus on E-Scooters, Part 2

Absztrakt

A kutatás célja az volt, hogy alaposan megvizsgálja az elektromobilitási eszközök sebezhetőségeit, azonosítva a lehetséges kockázatokat és veszélyforrásokat, valamint felmérje a gyártók által alkalmazott biztonsági intézkedések hatékonyságait. A szerző bemutatja a közvetlen tapasztalatait egy elektromos roller sebezhetőségeiről az általa elvégzett biztonsági tesztelés alapján. A kutatás eredményei rávilágítanak arra, hogy az elektromobilitási eszközök megfelelő védelme érdekében elengedhetetlen a kiberbiztonsági kockázatok és az elektromobilitási járművek közötti összefüggés vizsgálata, továbbá a kutatás eredményei kulcsfontosságúak a jövőbiztos mobilitás szempontjából.

Kulcsszavak: elektromobilitás, kiberbiztonság, elektromos járművek, adatbiztonság

Abstract

The purpose of the research was to thoroughly examine the vulnerabilities of electromobility devices, identify potential risks and threats, and assess the effectiveness of security measures implemented by manufacturers. The author presents his direct experiences with the vulnerabilities of an electric scooter based on the security testing he conducted. The results of the research highlight that to adequately protect electromobility devices, it is essential

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem, Rendészettudományi Doktori Iskola, e-mail: harangozovalentin1986@gmail.com

to investigate the connection between cybersecurity risks and electromobility vehicles. Furthermore, the findings of the research are crucial for future-proof mobility.

Keywords: electromobility, cybersecurity, electric vehicles, data security

Bevezetés

A téma helye, jelentősége, aktualitása

Ebben a részben az elektromobilitási eszközök sebezhetőségei kerülnek fókuszba. Az elektromos járművek térnyerése a modern közlekedés egyik legfontosabb innovációja, azonban az eszközök kiberbiztonsági fenyegetettségei és sebezhetőségei jelentős kihívásokkal járnak. Az elektromos járművek és a hozzájuk kapcsolódó infrastruktúra sebezhetőségei nemcsak az adatbiztonságot, hanem a fizikai biztonságot is veszélyeztethetik. A hardveres és szoftveres biztonsági rések kihasználása lehetőséget ad a kiberbűnözők számára, hogy távoli hozzáféréssel manipulálják az eszközöket vagy azok rendszereit. Ez különösen aggasztó, mivel az ilyen sebezhetőségek kihasználása kiberbiztonsági és közlekedésbiztonsági incidensekhez is vezethet.

A kiberbiztonság jelentősége a járműgyártás, fejlesztés és szabályozás területén egyre inkább előtérbe kerül. Az elektromos járművek és a kapcsolódó rendszerek védelme érdekében elengedhetetlen a folyamatos fejlesztés. A kutatás célja az volt, hogy hozzájáruljon egy olyan szabályozási keret kialakításához, amely biztosítja az elektromobilitási járművek biztonságos használatát. Az elektromobilitási eszközök digitalizációja és a hozzájuk kapcsolódó hálózati funkciók új kiberbiztonsági fenyegetéseket hoznak létre, amelyekre eddig kevés figyelem irányult. Éppen ezek az új kihívások és a belőlük fakadó kiberbiztonsági problémák ösztönöztek arra, hogy kutatásomat erre a témára összpontosítsam.

A tudományos probléma megfogalmazása

Az elektromobilitás terjedése az utóbbi években jelentős mértékben átalakította a közlekedési szokásokat, új lehetőségeket és kihívásokat teremtve. Az elektromobilitási eszközök, mint például az e-rollerek, elektromos kerékpárok és elektromos autók, innovatív és környezetbarát alternatívákat kínálnak a hagyományos közlekedési eszközökkel szemben. Ezen eszközök elterjedésével azonban a használatukhoz szükséges digitális infrastruktúra és az ezeken keresztül átvitt vagy tárolt adatok védelme is kiemelt figyelmet igényel.

A modern elektromobilitási rendszerek számos érzékeny adatot kezelnek, például GPS-koordinátákat, személyes profilokat, valamint fizetési információkat, amelyek védelme elengedhetetlen a felhasználók biztonságának és bizalmának megőrzéséhez.

A nem megfelelő adatvédelem súlyos következményekkel járhat, beleértve az adatlopást, az adatokkal való visszaélést, illetve a felhasználók bizalmának elvesztését. Az elektromobilitási eszközök és a kapcsolódó alkalmazások használata során fellépő kiberbiztonsági kockázatok tovább bonyolítják a helyzetet, hiszen a hardveres

és szoftveres sebezhetőségek kihasználása révén a támadók távoli hozzáférést szerezhetnek az eszközökhöz, adatokat lophatnak vagy akár az eszközök működését is befolyásolhatják.

A vizsgálat tárgya és a célkitűzések

Kutatási célkitűzések, fontosabb kérdések

A kutatásom célja az volt, hogy feltárja a mindennapi közlekedésben megjelenő elektromobilitási eszközök kiberbiztonsági vonatkozásait, azonosítva a lehetséges kockázatokat és veszélyforrásokat. Kiemelt figyelmet kapnak az adatbiztonságot érintő kérdések, például az eszközön tárolt vagy átvitt személyes információk védelme, a távoli hozzáférés lehetőségei és az esetleges adatlopás veszélyei. Fontos kérdés továbbá az eszközök fizikai biztonsága, a vezérlőrendszer sebezhetőségei és az esetleges támadási pontok az eszközön vagy a hozzá kapcsolódó szoftverekben.

A lényegesebb témaköröket vizsgálva két részre volt bontható a kutatás: ebben a részben bemutatom a vizsgált elektromos eszközöknek a kiberbiztonsági fenyegetettségeit, míg az előző részben ismertettem és elemeztem ezen közlekedési eszközök felhasználóinak biztonságtudatossági szintjét és technológiaelfogadási hajlandóságát. A kutatás céljával összhangban annak érdekében, hogy az elektromos járművek sebezhetőségi pontjait feltárhassam és megvizsgálhassam, az alábbi kérdéseket fogalmaztam meg:

- Hol vannak az esetleges támadási pontok az eszközön vagy a hozzá kapcsolódó szoftverekben?
- Milyen intézkedéseket és technikai megoldásokat alkalmaznak a gyártók a kiberbiztonsági fenyegetettségek csökkentése érdekében, és ezek mennyire hatékonyak?

Kutatási módszerek

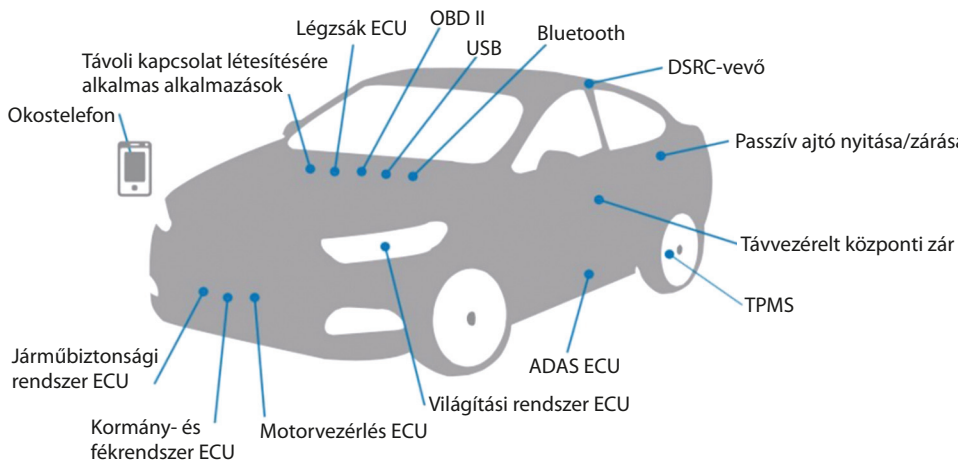
A kutatásom során többféle módszert alkalmaztam az elektromobilitási eszközök kiberbiztonsági kockázatainak feltárására és értékelésére. Elvégeztem egy biztonsági tesztelést egy elektromos rolleren, hogy közvetlen tapasztalatokat szerezhessek az eszköz kiberbiztonsági sebezhetőségeiről. A biztonsági tesztelés olyan elemeket tartalmazott, mint a rendszeres frissítések telepítése során felmerülő kockázatok azonosítása, az eszközön található alkalmazások biztonságának értékelése és a potenciális kockázati tényezők azonosítása.

Az összes adat begyűjtése után részletesen elemeztem és összevetettem az információkat, hogy teljes képet kapjak az elektromobilitási eszközök kiberbiztonsági állapotáról. Ezen elemzés eredményei alapján fogalmaztam meg a kutatás végkövetkeztetéseit és ajánlásait.

Kiberbiztonság a járműiparban

Kiberfenyegetettségek a járművek tekintetében

Fontos megjegyezni, hogy a jövőbeli kiberfenyegetések nemcsak a hétköznapi munkavégzések során lesznek jelen, hanem az elektromos járművek térhódítása miatt a gazdasági szektoron átívelve a mindennapi közlekedésben is meg fognak jelenni. A járműgyártás során egyre több technológiai megoldást vezetnek be mind az utasok, mind a gyalogosok biztonságának javítása érdekében, azonban ezek nem járnak kizárólag pozitív hatásokkal, ugyanis ezekben rejlik a járművek kiberbiztonsági sebezhetősége is (1. ábra).[2]



1. ábra: Lehetséges támadási pontok egy járműben
Forrás: Palkovics 2020: 4

Az egyik ilyen kiberfenyegetettség lehet a jövőben a *vehicle-to-vehicle* kapcsolódás (a továbbiakban: V2V). A korábbi években az autóipari és közlekedési rendszerek fejlesztői óriási erőforrásokat fordítottak arra, hogy kifejlesszék az intelligens közlekedési rendszereket (ITS), valamint a kooperatív intelligens közlekedési rendszereket (C-ITS), továbbá az ezeket a rendszereket összekötő *vehicle-to-everything* (V2X) technológiát.[3] Az elektromos járművek képesek az előttük haladó másik elektromos járművel összekapcsolódni. A járművek közötti kommunikáció természetesen vezeték nélküli hálózat használatával jön létre, ez a funkció hasznos lehet például a haladás során is, mivel lehetővé teszi az autó sebességének csökkentését, ha a másik jármű közelebb kerül. Ilyenkor a kiberfenyegetettség abban rejlik, hogy a támadó visszaélhet a vezeték nélküli hálózat által biztosított kommunikációs technológia hibáival, így könnyedén

[2] Sanguesa et al. 2021: 372–404.
[3] Pethő–Szalay–Török 2022.

átveheti az irányítást, akár csökkentheti is az autó sebességét, és *malware-ekkel* fertőzheti meg ezt a kapcsolatot a járművek között, aminek hatására a V2V-rendszer lehetőséggé válik ahhoz, hogy megfertőzze a többi csatlakoztatott autót is.

A következő kiberfenyegetettség a Controller Area Networkben (a továbbiakban: CAN) rejlik, ugyanis a legtöbb jármű CAN-vezérlőt használ, amely a jármű elektronikus vezérlőegységével (a továbbiakban: ECU) kommunikál. Ahogyan az 1. számú ábrán látható, az ECU számos alrendszert működtet, például az ABS-t, azaz a blokkolásgátló fékeket, légzsákokat, sebességváltót, média- és audiorendszert. Az ECU vezérli továbbá például a jármű motorjának elektronikáját, a sebességváltót, az elektromos zárakat, a légkondicionáló rendszer működését és a fényvezérlés moduljait, illetve több egyéb alkatrész, modul vezérléséért is felelős.[4]

A járműben lévő hálózat összeköti az ECU-kat, és továbbítja az adatokat közöttük. Ez a hálózat magában foglalja többek között a vezérlőterületi hálózatot, a helyi összekötő hálózatot (Local Interconnect Network, a továbbiakban: LIN), az Ethernetet. A LIN egy alacsony sebességű hálózat, amelyet általában ajtózárakhoz, klímaberendezésekhez, biztonsági övekhez, napfénytetőhöz és tükörvezérlőhöz használnak.[5] Az ECU könnyedén elérhető egy külső OBD-eszközzel is, amely egy *backdoor* támadásként képes a jármű ECU-jába bejutva parancsokat adni, és vezérelni a különböző rendszereket és szolgáltatásokat. Fontos megemlíteni, hogy a titkosítás hiánya is kiberbiztonsági kockázat, ugyanis a CAN-csomagok nincsenek titkosítva, ezért a támadók könnyen elemezhetik azokat.[6]

Sen Nie és társai egy kísérlet során bemutatták, hogyan irányítható a jármű vezérlőegysége távolról tetszőleges CAN-csomagok küldésével. A kísérlethez egy legújabb *firmware-rel* frissített Tesla járművet használtak, így tesztelték a Tesla S P85 és P75 modellek sebezhetőségét. A teszt során vezeték nélküli technológiával több, a vizsgált járművekben lévő rendszert is meg tudtak károsítani, többek között az integrált áramkört és az átjárókat, ezt kihasználva rosszindulatú CAN-üzeneteket fecskendeztek be a rendszerbe.[7] A felfedezés után a Tesla járműveket már az *over-the-air* (OTA) mechanizmussal frissítették, és kódaláírási védelmet alkalmaztak a sebezhetőség megszüntetésére.[8]

A jelenlegi jármű-technológia lehetővé teszi, hogy az autónkhoz csatlakoztassuk az okostelefonjainkat is, így olyan funkciókat használhatunk a gépkocsinkban, mint a telefonhívás, szöveges üzenet írása vagy zenehallgatás, erre való például az Apple CarPlay vagy az Andorid Auto. Ez azért veszélyes, mert a telefon és a jármű kapcsolata során egy előzetesen összeállított rosszindulatú program (például egy *malware*) azonnal kihasználja a biztonsági réseket a járművekben, ezzel veszélyeztetve a járművezetőt, a járművezető adatait és a közlekedés biztonságát is.

Az okostelefonokkal összekapcsolt járművek kapcsolatából egyéb kiberfenyegetettségek is kialakulhatnak a jövőben, hiszen az összekapcsolt autók képesek rögzíteni a járművezetők fontosabb személyes adatait is a külső eszközökről. Ez az adatbázis „kincsesbánya" lehet egy kiberbűnözőnek akár kémkedés során is.

[4] Tóth 2017.
[5] Katona 2023: 161–176.
[6] Wolf–Weimerskirch–Paar 2004.
[7] Katona 2022.
[8] Kyounggon et al. 2021: 103.

Kiberfenyegetésként említhető a jövőben az elektromos járművek széles elterjedésével az autólopások módszerének megváltozása is. A legtöbb jármű távolról kulccsal nyitható és zárható már most is. Ezt használja ki az a potenciális támadó is, aki képes anélkül ellopni egy autót, hogy ahhoz bármilyen fizikai behatást alkalmazna. Ezt a fajta kibertámadást általában hackerek használják, és nem is kell hozzá sok felszerelés, emellett kifejezetten hatékony. Ebben az esetben a támadó blokkolja a jelet a jármű vezeték nélküli kulcsáról, így nyitva hagyja az autót, mindeközben a jármű válaszol a jelre, amivel megtéveszti a tulajdonosát. A támadás lényege, hogy a kulcs és a jármű kommunikációjához használt elektromágneses hullámokat blokkolja, megakadályozva az autó bezárását. Például egy kutatás során egy VW Grouphoz tartozó jármű távirányító jelét továbbították, majd a járműből küldött jelet lehallgatták, így tetszőlegesen hozzáférhettek a járműhöz.[9]

A fentiek alapján megállapítható, hogy a villamosítás és az automatizált vezetés mellett az elektromos járművek kiberbiztonsága az egyik legfontosabb kihívás a járműipari fejlesztők, a gyártók és az alkatrészgyártók számára. A kiberbiztonsági irányítási rendszerek és szabályozások célja, hogy a jövőben megvédjék a teljes járművet, az infrastruktúrát és a berendezéseket a fenyegetésektől.

Kiberfenyegetettségek az elektromos roller tekintetében

Az elektromos rollerek Magyarországon elég nagy arányban vesznek részt a közúti közlekedésben, és a számuk folyamatosan növekszik. Az elektromos rollereket illetően beszélhetünk saját tulajdonú és közösségi megosztáson alapuló e-rollerekről. A mindennapi közlekedésben Magyarországon 2019-ben az év végén jelent meg a közösségi rollerszolgáltatás. Egy okostelefonokra letölthető applikáció beszerzése után az elektromos rollereket szinte bárki elviheti az utcáról. Mindegyik rollerben található egy globális helymeghatározó rendszer, amely nyomon követi az adott személy használatát. A globális navigációs műholdrendszer egy műholdalapú helymeghatározó, navigációs és időmérő (Position, Navigation and Timing, a továbbiakban: PNT) rendszer. Jelenleg számos Global Navigation Satellite System (a továbbiakban GNSS) van a kiépítés és a működés különböző szakaszaiban. Az amerikaiak által használt globális helymeghatározó rendszer a legismertebb. Mindazonáltal az európai vezetésű Galileo, az orosz vezetésű GLONASS, a kínai BeiDou, az India által vezetett IRSS és a japán QZSS mellett áll.[10] Együttes keretrendszerként a GNSS egy világszerte meghatározó és költséghatékony kültéri PNT-technológiává vált. Az egyes GNSS-technológiák alkalmazása elengedhetetlen egy elektromos jármű, például egy e-roller esetében a pontos helymeghatározáshoz. Továbbá a jövőben kialakuló intelligens közlekedési rendszerben az egyes járművek és forgalmi helyzetek meghatározásához is szükséges e szenzorok alkalmazása.[11] Azonban ez a helymeghatározó rendszer is rejt magában számos kockázatot, például egy rosszindulatú támadó stratégiailag kiválaszthatja és hamisíthatja

[9] Garcia et al. 2016.
[10] Santra 2019.
[11] Katona 2023.

egy vagy több e-roller helyzetét, átteheti egy eldugott területre vagy olyan területre, ahol minimális az emberi jelenlét, hogy ezzel odacsalja a potenciális áldozatot.[12]

Az elektromos rollerek kiberbiztonsági kockázatai főként a közösségi megosztáson alapuló e-rollereknél jelennek meg, hiszen ezek azok a szolgáltatók, amelyek a felhasználók adatait kezelik, ők felelnek a járművek karbantartásáért és azért is, hogy kiberbiztonsági szempontból sebezhetetlenek legyenek ezek a közlekedési eszközök. Azonban sajnos mégis vannak gyenge pontok, ami aggasztó lehet. Egy fekete kalapos hacker bluetooth-kapcsolaton keresztül a jármű közelében képes az e-rollerek *firmware-jét* letörölni és egy általa módosítottat felölteni arra, így például növelheti az előtte korlátozott sebességet. Erre megoldás lehet, hogy az e-rollerekre kizárólag jóváhagyott firmware-t lehessen telepíteni, valamint hogy a szolgáltatók vagy a gyártók korlátozzák a harmadik féltől származó alkalmazásokat, hogy hozzáférhessenek az e-rollerek *firmware-jéhez*.

Számos szolgáltató kínál mobilalkalmazást az elektromos rollerhez, azonban itt megjelenik egy következő kiberfenyegetettség, az elavult alkalmazásbiztonság. Manapság már a legnépszerűbb elektromos autókhoz is léteznek speciális alkalmazások, amelyekkel a felhasználók rengeteg érdekes és hasznos információhoz juthatnak hozzá a saját autójukkal kapcsolatban. Ez igaz az elektromos rollerekre is, hiszen ezeknek a rollereknek a rendszere főként bluetoothon vagy wifi-kapcsolaton keresztül kommunikál. Azonban minden hálózati kapcsolat megtámadható, és ha nincsen megfelelő védelemmel ellátva, akkor fel is törhető. Ebből következik az elektromos rollerek alkalmazásainak a kiberbiztonsági kockázata is. Ugyanis ezek a felhasználói élményt javító informatikai rendszerek és a hozzájuk kapcsolt okoseszközök, alkalmazások szintén kiberbiztonsági kockázatoknak vannak kitéve, és számos ponton sebezhetők lehetnek. A hackerek olyan szoftvereket hoznak létre, amelyek megkerülhetik az alkalmazások kiberbiztonságát. Ennek eredményeképpen képesek betörni az alkalmazásba és átvenni az irányítást az e-roller felett. A hackerek képesek arra, hogy saját kódot futtassanak az alkalmazásokon, ami azt jelenti, hogy megváltoztathatják vagy teljesen leállíthatják az alkalmazás működését. Az adattitkosítás hiánya szintén kiberfenyegetettség a jövőben. Számos szolgáltató esetében jelenleg az adatok átvitele HTTP használatával történik, ezeket frissíteni kell HTTPS-re. Pontosan azért, hogy a felhasználói adatok, az utazások adatai és a bejelentkezési adatok mind-mind titkosítva legyenek, és ne lehessen hozzáférni ezekhez.

Az elektromos rollerek elterjedésével és fejlődésével együtt járnak a különböző kiberbiztonsági kihívások és kockázatok is. Ahhoz, hogy megértsük és hatékonyan kezeljük ezeket a kockázatokat, fontos áttekinteni és elemző módon megvizsgálni az e-rollerek lehetséges támadási pontjait. Ezért egy táblázatba szedve szemléltetem az e-rollerek legfőbb támadási pontjait, valamint ezek magyarázatát (1. táblázat). Segítségével könnyen azonosíthatjuk az e-rollerek legkritikusabb biztonsági problémáit, és a későbbiekben javaslatok tehetők a megfelelő megelőzési stratégiákra a felhasználók és az eszközök védelme érdekében.

1. táblázat: Az e-rollerek lehetséges támadási pontjai

[12] Vinayaga-Sureshkanth et al. 2020: 31–35.

Támadási pontok	**Magyarázat**
Firmware manipuláció	A hackerek módosíthatják az e-rollerek *firmware-jét,* például növelhetik a sebességet vagy kikapcsolhatják a biztonsági funkciókat, ami veszélyeztetheti az e-rollerek felhasználóit.
Alkalmazásbiztonság megkerülése	Az alkalmazások biztonsági intézkedéseit megkerülve, lehetőség nyílik arra, hogy illetéktelenül hozzáférjenek a felhasználói adatokhoz vagy akár teljesen átvegyék az irányítást az e-rollerek felett.
Adattitkosítás hiánya	Az adatok titkosításának hiánya lehetővé teszi a hackerek számára, hogy illetéktelenül hozzáférjenek az e-rollerek felhasználói adataihoz, például a felhasználók személyes információihoz vagy a közlekedési tevékenységeikhez kapcsolódó adatokhoz. Az adatok átvitele HTTP-n keresztül történik, ami kockázatot jelent. Az adatok titkosítása HTTPS használatával szükséges a biztonságos adatátvitel érdekében.
Bluetooth- és WiFi-kapcsolat	A bluetooth-kapcsolatok kihasználása lehetővé teszi a hackerek számára, hogy távolról kapcsolódjanak az e-rollerekhez, és manipulálják azok működését, vagy akár ellopják azokat. Ha az e-roller alkalmazást használ, és az okostelefon bluetooth- vagy WiFi-kapcsolaton keresztül kommunikál az eszközzel, ezek a csatornák sebezhetővé tehetik a rendszert.
Szoftverfrissítési sebezhetőség	A szoftverfrissítések során felmerülő sebezhetőségek lehetővé tehetik a hackerek számára, hogy kártékony szoftvereket telepítsenek az e-rollerekre, vagy akár illetéktelen hozzáférést szerezzenek azokhoz a frissítési folyamatok során.
Felhasználói hitelesítési problémák	Gyenge felhasználói hitelesítési mechanizmusok vagy hiányos bejelentkezési eljárások lehetőséget adnak a hackereknek arra, hogy illetéktelenül hozzáférjenek az e-rollerekhez.
Adatvédelmi problémák	Az e-rollerekről gyűjtött és tárolt felhasználói adatok védelmének hiánya komoly kockázatot jelent a felhasználók személyes információinak illetéktelen hozzáférése és felhasználása szempontjából, ami súlyos következményekkel járhat az érintettek számára.
Rendszerhiba és sérülékenység	Az e-rollerekben és azok működéséhez szükséges rendszerekben lévő hardver- és szoftverkomponensek sérülékenységei és rendszerhibái lehetővé tehetik a hackerek számára, hogy különféle támadásokat hajtsanak végre az e-rollerek ellen, beleértve a fizikai károkozást és a távoli irányítást.
Felhasználói adatlopás	A hackerek az alkalmazásokon keresztül hozzáférhetnek a felhasználói adatokhoz, például a személyes információkhoz vagy a banki adataikhoz, és ezeket illetéktelenül felhasználhatják vagy értékesíthetik, ami súlyos következményekkel járhat az érintettek számára.
Fizikiai hozzáférés kockázata	A fizikai hozzáférés megszerzése az e-rollerekhez lehetővé teszi a hackerek számára, hogy fizikai károkat okozzanak az eszközökön, például azok megsemmítésével vagy manipulálásával, ami veszélyzeteti az e-rollerek felhasználóinak biztonságát és magánéletét.

Forrás: a szerző szerkesztése Argyropoulos *et al. 2021 és* Vaidya–Mouftah *2020 alapján*

Következtetések

A kiberbiztonsági kockázatok áttekintése során megállapítható, hogy számos potenciális támadási pont létezik az elektromobilitási eszközöknél, amelyek veszélyeztethetik akár az e-rollerek, akár más e-mobilitási eszköz felhasználóinak biztonságát és adataik védelmét.

Fontos hangsúlyozni, hogy ezeket a kockázatokat lehet és kell is kezelni a megfelelő védelmi intézkedésekkel és gyakorlatokkal. Az e-rollerek tervezése és üzemeltetése során kiemelt fontosságú az adatvédelem és a felhasználók bizalmának megőrzése, ezért folyamatos figyelemmel kell kísérni a kiberbiztonsági kockázatokat, és azokra hatékony válaszokat kell kidolgozni a felhasználók védelme érdekében. A biztonságos és kényelmes közlekedés érdekében a gyártók, a szolgáltatók és a felhasználók közös felelőssége, hogy az e-rollerek világa folyamatosan fejlődjön.

Vizsgálat és tesztelés

A vizsgálat módszertana

A vizsgálati módszer ebben a fejezetben egy gyakorlati biztonsági tesztelést foglal magában, amely során valós környezetben teszteltem egy elektromos roller biztonsági mechanizmusait. A vizsgálat során a célom az volt, hogy megállapítsam, hogy egy bluetoothos adatkapcsolati rendszeren keresztül hozzá lehet-e férni az e-rollerek rendszeréhez, és módosíthatók-e egyes gyárilag beállított biztonsági intézkedések. Az elektromos roller rendszerének biztonsági tesztelése lehetővé teszi számomra, hogy a valós életben megvizsgáljam a biztonsági intézkedések hatékonyságát és a rendszer esetleges sebezhetőségeit. Az ilyen tesztek által nyert eredmények segíthetnek bemutatni, hogy az általam megfogalmazott kiberbiztonsági fenyegetettségek valósak, illetve hogy az esetleges hiányosságokat azonosítaniuk kell a szolgáltatóknak és a gyártóknak, továbbá hogy szükséges az elektromobilitási eszközök rendszerének és a hozzájuk társított applikációknak a továbbfejlesztése a felhasználók biztonságának javítása érdekében.

Biztonsági tesztelés a gyakorlatban

Ahogy korábban kifejtettem, a biztonsági tesztelésem célja annak megállapítása volt, hogy vezeték nélküli adatkapcsolati kommunikáción keresztül hozzá lehet-e férni egy elektromos roller rendszeréhez, és módosíthatók-e bizonyos gyárilag beállított biztonsági intézkedések, adatok.

A tesztelés laboratóriumi környezeten kívül, valóságos környezetben történik, ahol valódi elektromos rollert használok. A teszteléshez egy Xiaomi gyártmányú Mi Essential típusú eszközt választottam. Ennek az elektromos rollernek a főbb jellemzői: 20 km-es hatótávval rendelkezik, maximum 20 km/h sebességgel képes haladni. A roller súlya: 12 kg, kerékmérete 8,5 col, és dupla fékrendszerrel (E-ABS és nagy hátsó

tárcsafék) felszerelt. Az akkumulátor típusa lítium-ion, 3 sebességmóddal használható (gyalogos, normál és sport), a töltési ideje körülbelül 3,5 óra. A hozzárendelt gyártói applikáció a Mi Home, amellyel kezelhető a roller rendszere.

Ebben az alkalmazásban látható minden információ a saját rollerünkkel kapcsolatban, többek között a sorozatszám, a szoftver- és hardverinformációk, illetve a megtett kilométer, az akkumulátor töltöttsége. Az applikáció bluetooth-kapcsolaton keresztül kommunikál az elektromos roller vezérlőegységével. Amit még fontos tudni, hogy ebben az alkalmazásban történik – amennyiben rendelkezésre áll újabb – az e-roller szoftverfrissítése, illetve fontos megjegyezni, hogy az adott e-roller-típusoknak mind-mind sajátos funkcióik vannak. Ez a konkrét típus egy belépő szériának minősül a legalapvetőbb funkciókkal, így például nincsen rajta gyárilag elektronikus sebességtartó funkció *(tempomat)*. A gyártói alkalmazás Android-rendszerű eszközökre a Play Áruházból, iOS-rendszerű eszközökre pedig az App Store-ból tölthető le, és az alkalmazáson belül csak az adott e-roller-típusra vonatkozó beállítások szerkeszthetők vele, ezért például korábbi szoftverek nem telepíthetők, pluszbeállítások nem végezhetők el, tehát ez alapján zárt rendszerűnek mondható az alkalmazás.

A tesztelés során mindenképpen Android-rendszerű eszközt fogok használni, ugyanis azok az alkalmazások, amelyekkel megkerülhetők a gyári beállítások, kizárólag a Play Áruházból érhetők el. Ezek úgynevezett *third-party app-ok,* ami azt jelenti, hogy olyan, egy harmadik féltől származó alkalmazások, amelyeket nem az e-roller gyártója készített. Nevezetesen van két ilyen alkalmazás, amelyet szeretnék bemutatni és használni ennek a folyamatnak a végrehajtására, az egyik a ScooterHacking Utility, a másik pedig az m365 DownG.

Minden elektromos rollernek saját vezérlő elektronikája van, és ezzel együtt úgynevezett firmware-je (FW). Röviden ez mondja meg a rollernek, hogyan viselkedjen, milyen teljesítményt adjon le a motor, milyen gyorsan menjen az elektromos roller. Ha ezt az FW-t módosítják, azt nevezzük CFW-nek *(custom firmware)*. A biztonsági tesztelés során használt elektromos rollerre gyári firmware van telepítve. A használt DownG alkalmazás verziószáma 36, a ScooterHacking Utility verziószáma pedig 2.3.2.

Fontos megjegyezni, hogy minden e-rollernek van négy olyan rendszere, amelyet érintenek ezek az alkalmazások az egyes szoftvermódosítások során.

Az e-rollerek esetében ez a négy rendszer a DRV, az ESC, a BSM és a BLE. A DRV az elektromos motor vezérlőjére utal, amely felelős az elektromos motor sebességének és irányának szabályozásáért a rollerben. A motorvezérlő szabályozza a motorhoz szállított energiát a roller vezérléseitől származó bemeneti jelek alapján. Az ESC az elektronikus sebességvezérlő rövidítése. Azzal befolyásolja az elektromos motor sebességét, hogy szabályozza az ahhoz szállított energia mennyiségét. Értelmezi a roller vezérléseitől származó jeleket, és ennek megfelelően szabályozza a motor sebességét. A BSM az akkumulátorkezelő rendszer rövidítése, ami felelős a roller akkumulátorának kezeléséért, ideértve állapotának figyelését, a cellák kiegyenlítését és a túltöltés vagy túlmerülés elleni védelmet. A BMS szinte minden elektronikus eszközben megtalálható, sokféle szerepet játszik az e-rollereken belül. Ez egy beépített rendszer, amely figyeli az akkumulátort és annak egyes akkumulátorcelláit, hogy diagnosztizálja, korrigálja és optimalizálja a járművet. Ezeket az adatokat a BMS folyamatosan gyűjti a zökkenőmentes működés és az optimalizált energiafogyasztás biztosítása érdekében. A BLE

az angol Bluetooth Low Energy rövidítése. Az elektromos roller esetében ez a roller bluetooth-kapcsolatára utal, ami lehetővé teszi annak kommunikációját egy mobilalkalmazással vagy más eszközökkel. A BLE funkciói közé tartozhatnak a roller zárásának/nyitásának vezérlése, beállítások módosítása, a roller helyzetének nyomon követése és a diagnosztikai adatok biztosítása. Ennek a segítségével működik a gyártó által biztosított dedikált alkalmazás is, továbbá ez az a rendszer, amelyre elsődlegesen hatnak a Play Áruházból letölthető, már említett alkalmazások.

Az elektromos rollerek, ahogy korábban volt róla szó, bluetooth-kapcsolaton keresztül kommunikálnak a külső eszközökön lévő applikációkkal. A biztonsági tesztben érintett Xiaomi elektromos roller is a gyártó által fejlesztett Mi Home alkalmazáson keresztül vezérelhető.

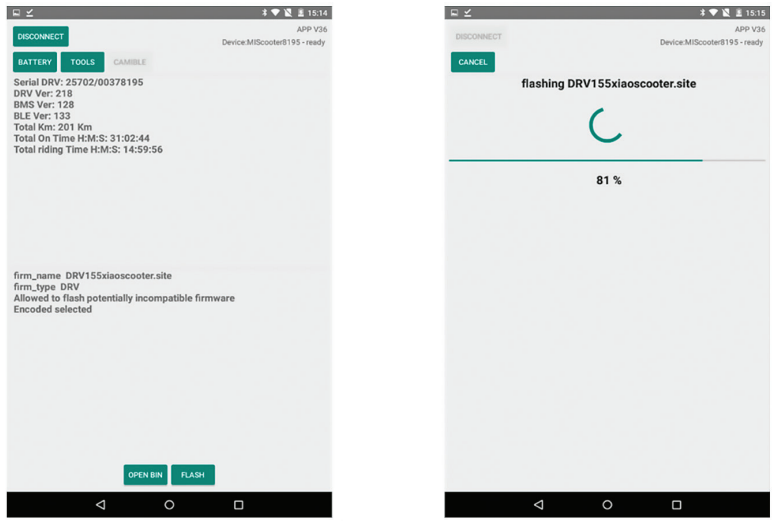
Fontos megjegyezni, hogy ezen a gyári applikáción van egy olyan lehetőség, hogy a saját e-rollerünket, amikor összekapcsoljuk bluetoothon keresztül, elektronikusan le lehet zárni, majd fel lehet oldani a további használat érdekében. Amikor a roller elektronikusan zárolva van, az egyetlen rajta található funkciógombbal kizárólag a lámpát lehet be- és kikapcsolni, minden más funkció ilyenkor le van tiltva, a roller kijelzőjén kizárólag egy lakatszimbólum, és amíg a bluetooth eszközzel kapcsolatban van, egy bluetooth-szimbólum látható. Továbbá fontos, hogy az elektronikus lezárás után a roller további mozgásra képes, azonban az elektromotor folyamatosan fékezi annak első kerekét. Az e-roller nyitásának és zárásának jelentősége lesz a teszt során.

A teszt végrehajtása

Mindenekelőtt szeretném megjegyezni, hogy a téma etikai érzékenysége miatt a jelen fejezetben teljes, részletes kifejtésre nem kerül sor, mivel nem közölnék olyan információkat, amelyek esetlegesen nem kívánt irányú alkalmazásra ösztönözhetnek másokat.

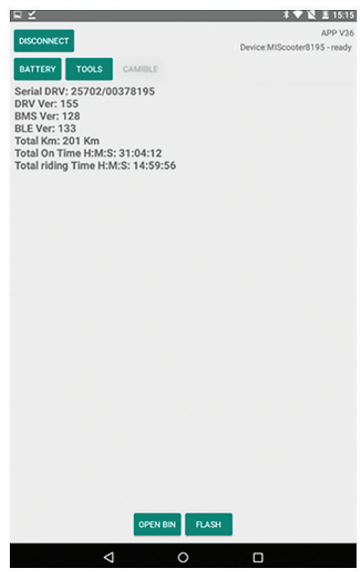
Az első teszt során azt az élethelyzetet szeretném bemutatni, amikor nem használom a Mi Home alkalmazást, és ezáltal nem is zárom le az elektromos rollert elektronikusan. Ebben az esetben a teszt célja a rollerre telepített firmware felülírásra egy olyan *custom firmware-rel,* amelyen a gyári biztonsági intézkedések már felül lettek írva, így például a maximális sebesség beállítása 30 km/h; előtte nem rendelkezett elektronikus sebességtartó funkcióval, ez is be lett állítva a CFW-ben, illetve az elektromotor indítási sebessége is csökkentve lett. Ennek a CFW-nek az e-rollerre történő telepítésére a DownG alkalmazást fogom használni. Itt minden olyan e-roller megjelenik, amely be van kapcsolva, és amelynek a bluetooth-hatótávjában az androidos eszközöm észlelhető.

Miután a módosítani kívánt e-roller megjelenik a listában és kiválasztjuk, egy új felületre kerülünk. Itt már láthatunk minden fontos információt a saját e-rollerünkről: többek között az e-rollerünk szériaszámát és a rajta található DRV, BMS, BLE verziószámokat, illetve az összes megtett utat kilométerben és időben is, azonban ez nem releváns a teszt szempontjából. Ami a teszt szempontjából fontos, az az e-rolleren található DRV verziószám, amely jelen esetben 2.1.8. Ez fog vélhetően módosulni az általam generált CFW verziószámára, ha sikeres lesz a teszt.



2. ábra: A CFW felülírásának folyamata
Forrás: a szerző felvételei a DownG alkalmazásból

Ha a CFW-t betöltjük a programba, elindul a felülírási folyamat, amint az a 2. ábrán is látható. Ez nagyjából 1-2 percet vesz igénybe, és egy százalékos folyamatjelző időközben az aktuális állapotról tájékoztat. A folyamat végén, amennyiben sikeres a felülírás, látható, hogy az általam használt e-roller DRV verziószáma módosult 1.5.5.-re (3. ábra).



3. ábra: A módosult DRV számmal rendelkező e-roller
Forrás: a szerző felvétele a DownG alkalmazásból

A felülírás után megállapítottam, hogy az e-roller az általam generált CFW-vel hibakód nélkül működött tovább, és az eddig tempomattal nem rendelkező e-roller már ilyen funkcióval is bővült, a maximális sebessége módosult 30 km/h-ra, és az elektromotor indító sebessége is módosult a felülírással, amely összesen két percig tartott a DownG alkalmazás használatával.

A ScooterHacking Utility alkalmazás már sokkal több lehetőséget kínál az e-rollerrel kapcsolatos módosítások végrehajtásához. Fontos megjegyezni, hogy ez az alkalmazás már nem kizárólag Xiaomi márkájú e-rollerekkel kompatibilis, hanem más gyártó több típusú e-rollerével is összekapcsolható (például Segway-Ninebot E, F, T, D szériái).

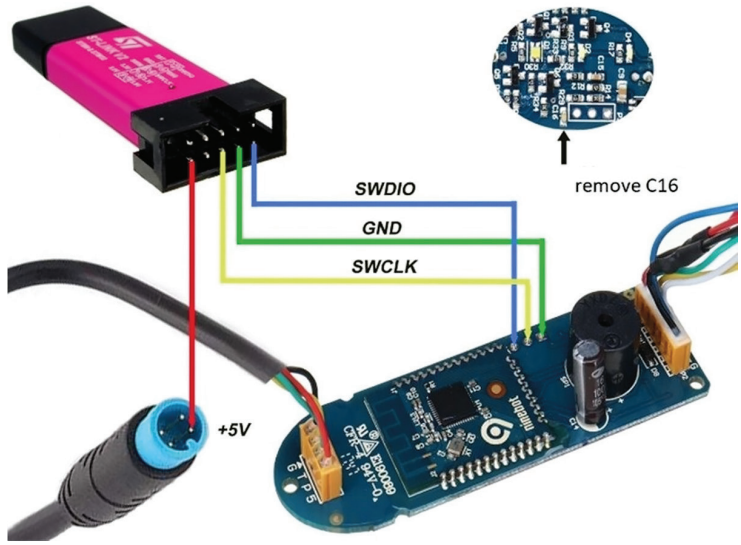
További tesztek végrehajtása

Az első teszt után azt vizsgáltam meg, hogy amennyiben egy e-rollert a korábban ismertetett módon bluetoothszal lezárunk – a valóságban egy gyakran előforduló élethelyzet, hogy valaki elektromosan lezárja az e-rollerét, és amíg nem használja, elmegy annak közvetlen környezetéből –, akkor hogyan reagál egy ilyen alkalmazásra.

Az első esetben úgy hajtottam végre, hogy az az eszköz, amelyről lezártam az e-rollert a Mi Home alkalmazással, ott maradt a roller bluetooth-hatótávolságán belül, és így folyamatos kapcsolat volt az eszköz és az e-roller között. Ebben az esetben az androidos eszközre telepített alkalmazások egyikével sem lehetett észlelni az e-rollert. Tehát az e-roller gyakorlatilag védett maradt, és ez alatt az idő alatt, amíg egy másik bluetooth-kapcsolat aktív volt, nem lehetett rajta végrehajtani változtatásokat.

A második esetben azonban a tesztet úgy hajtottam végre, hogy az az eszköz, amelyről a rollert lezártam a Mi Home alkalmazással, már a bluetooth-hatótávolságon kívül volt, és ebben az esetben az e-roller kijelzőjén kizárólag egy lakatszimbólum jelenik meg. Ekkor az andoridos készülékre telepített alkalmazással azonnal észlelhetővé vált az e-roller, pedig az elektromos zárolás még mindig aktív volt. Azonfelül, hogy az e-roller észlelhető volt, sikerült is bejutni annak vezérlőrendszerébe és a zárolást feloldani az alkalmazással, és lehetőségem nyílt módosításokat végrehajtani az e-rolleren: tudtam csökkenteni az elektromotor fékhatását, az indítási sebességet, a maximális sebességet, az elektromotor-rendszer feszültségét, másik régióba regisztrálhattam az e-rollert stb. Tehát megállapítható, hogy amint nincsen élő bluetooth-kapcsolat az e-roller és egy másik eszköz között, akkor annak rendszerébe könnyedén be lehet jutni, és azon belül változtatások hajthatók végre.

További kutatásokat végeztem különböző internetes forrásokon. Megállapítható, hogy a gyártó ezt a problémát már felismerte, ezért az újabb e-roller-szériákat már egy frissített BLE-verzióval adja ki, és az 1.5.7. verziószámban már blokkolja a vezérlőegység a feloldási lehetőségeket, azonban további kutatásokkal megállapítottam, hogy ennek a védelmi intézkedésnek a megkerülésére két módszer is létezik. Az egyik módszer alapja, hogy már árulnak külön megvásárolható utángyártott e-roller-alaplapokat, amelyeket beleépítve az e-rollerbe lehetőség nyílik annak szoftveres módosítására. A másik módszer lényege pedig az úgynevezett ST-Link V2 használata, amely egy programozó eszköz, USB-modul az STM32 és STM8 processzorcsalád programozásához, és ennek használatával az elektromos roller BLE modulját tudják programozni (4. ábra).



4. ábra: ST-Link V2 összekötése a Xiaomi e-roller vezérlőegységével
Forrás: Instructables 2024

Következtetések

Összegezve: az elvégzett kutatás célja az volt, hogy feltárja az elektromos rollerek bluetooth-kapcsolaton keresztüli hozzáférhetőségének és manipulálhatóságának kiberbiztonsági fenyegetettségeit. A kutatás során a végrehajtott biztonsági vizsgálattal igyekeztem szemléletesen bemutatni, hogy mennyire egyszerű belépni az elektromos rollerek rendszerébe és ott módosításokat végrehajtani.

Az eredmények alapján megállapítható, hogy a könnyű hozzáférhetőség súlyos kockázatokat jelent mind a kiberbiztonság, mind a közlekedésbiztonság, mind pedig az adatvédelem terén. Kiberbiztonsági szempontból az elektromos rollerek rendszereinek sérülékenysége lehetővé teszi a távoli vezérlést és a rendszerben tárolt adatokhoz történő hozzáférést, azok módosítását. Ez pedig potenciálisan komoly veszélyeket rejthet magában a felhasználók és a közlekedés résztvevői számára. Közlekedésbiztonsági aspektusból nézve az e-roller rendszerének manipulálhatósága könnyedén vezethet balesetekhez mind az e-roller vezetője, mind pedig más közlekedők szempontjából. Ezáltal az ilyen típusú járművek veszélyessé válhatnak a közutakon és a gyalogos területeken egyaránt.

Végül úgy gondolom, hogy adatvédelmi szempontból is kiemelt figyelmet kell fordítani az elektromos rollerek rendszerére. Az elektromos rollerek vezérlőegységének manipulálása lehetővé teszi a rendszerfájlokhoz, a rendszerben tárolt adatokhoz való egyszerű hozzáférést. Így például lehetőség nyílik személyes adatok, geolokációs adatok, útvonalak vagy akár az eszköz használatára vonatkozó információk megismerésére, illetéktelen felhasználására.

Kutatási eredmények

Az elektromobilitási eszközök, különösen az e-rollerek kiberbiztonsági fenyegetettségei egyre nagyobb figyelmet kapnak, ahogy ezek az eszközök mind szélesebb körben elterjednek. A kutatás során feltett kérdésekre adott alábbi válaszok egyben a kutatás legfontosabb eredményeit is tükrözik.

A kutatás első kérdésének vizsgálata során megállapítottam, hogy ezek az eszközök és a hozzájuk kapcsolódó szoftverek sebezhetőségei több helyen is megjelenhetnek. Az elsődleges támadási pontok közé tartozik a firmware manipuláció, amely során a hackerek módosíthatják az eszköz szoftverét, például növelhetik az e-roller maximális sebességét, vagy kikapcsolhatják a biztonsági funkciókat. Ez nemcsak az eszköz fizikai biztonságát veszélyezteti, hanem a felhasználók épségét is, hiszen a módosításokkal az e-roller balesetveszélyessé válhat.

A másik jelentős kockázat az alkalmazásbiztonsági rések kihasználása. Az e-rollerek és más elektromobilitási eszközök irányításához használt mobilalkalmazások biztonsági intézkedéseinek megkerülése révén a támadók hozzáférhetnek a felhasználók adataihoz, vagy akár teljesen átvehetik az irányítást az eszköz felett. Ez különösen veszélyes lehet közösségi megosztású eszközök, például e-rollerek esetében, ahol a támadók hozzáférhetnek a rendszerhez, és jelentős károkat okozhatnak. Emellett az adatok titkosításának hiánya is további kockázatot jelent. Sok esetben az eszközök kommunikációja még mindig HTTP-protokollon keresztül történik, amely nem nyújt megfelelő védelmet a támadások ellen. A titkosítatlan adatátvitel során a támadók könnyen megszerezhetik a felhasználók személyes adatait, például GPS-koordinátákat vagy fizetési információkat.

További potenciális támadási pontot jelent a bluetooth- és wifi-kapcsolatok sebezhetősége. Az e-rollerek gyakran kommunikálnak okostelefonokkal, ezeket a kapcsolatokat kihasználva a támadók távolról átvehetik az irányítást az eszközök felett, módosíthatják a működésüket, vagy akár el is lophatják azokat. A szoftverfrissítések sebezhetőségei szintén kihasználhatók. Ha a frissítések során nem megfelelően van biztosítva a folyamat, a támadók rosszindulatú szoftvereket telepíthetnek, amelyekkel hozzáférhetnek az eszköz rendszeréhez.

A második kutatási kérdésre vonatkozóan megállapítottam, hogy a gyártók különböző technikai megoldásokat alkalmaznak a kiberbiztonsági fenyegetettségek csökkentése érdekében. Az egyik legfontosabb intézkedés a firmware védelme. A gyártók sok esetben csak jóváhagyott firmware-t engednek telepíteni az eszközökre, ezzel igyekeznek megakadályozni a külső, nem hivatalos szoftverek telepítését. Noha ez egy hatékony megoldás, a hackerek idővel képesek kijátszani ezeket a védelmi mechanizmusokat, például utángyártott alkatrészek telepítésével vagy speciális programozó eszközök, mint például az ST-Link V2 használatával.

Emellett a gyártók egyre inkább alkalmazzák az adattitkosítást az adatok védelme érdekében. A HTTPS-protokoll használata biztosítja, hogy az adatátvitel során az adatok titkosítva legyenek, ezáltal megnehezítve a támadók dolgát. Azonban még mindig sok eszköz nem használja ezt a megoldást, ami jelentős kockázatot jelent az adatvédelem szempontjából. A rendszeres szoftverfrissítések és a szigorúbb ellenőrzési mechanizmusok szintén hozzájárulnak a kiberbiztonság javításához.

Összességében elmondható, hogy noha a gyártók által alkalmazott védelmi intézkedések hatékonynak bizonyulnak a kiberbiztonsági fenyegetések mérséklésében, a támadók folyamatosan fejlesztik módszereiket, így a védelemnek is állandó fejlesztést és figyelmet kell kapnia.

Összegzett következtetések és ajánlások

Az eredmények alapján számos ajánlás adható mind a felhasználók, mind a gyártók, mind a fejlesztők számára. Úgy gondolom, hogy a felhasználók részére szükséges lenne további oktatási és tájékoztató kampányokat szervezni az eszközök szoftver- és hardver-illesztőprogramjainak fontosságáról és a rendszeres frissítések szükségességéről.

Azonban ezen eredmények alapján hangsúlyozni kell a gyártók, a fejlesztők és a szabályozók felelősségét is a rendszerek biztonságának növelése és a kockázatok minimalizálása érdekében. A rendszeres biztonsági frissítések és a szigorúbb ellenőrzési mechanizmusok bevezetése elengedhetetlen az elektromobilitási eszközök biztonságának szavatolásához. Lehetséges megoldási javaslatként merül fel, hogy a gyártók tegyék lehetővé a felhasználók számára a kétlépcsős azonosítás alkalmazását az e-rollerekhez történő hozzáférés során. Ez azt jelentené, hogy a felhasználóknak nemcsak a jelszavukkal kellene bejelentkezniük az alkalmazásba vagy az e-rollerek vezérlőfelületére, hanem egy második, például SMS-ben küldött vagy autentikációs alkalmazáson keresztül generált kód megadásával is meg kellene erősíteniük az azonosításukat. Ezáltal még nehezebbé válna az illetéktelen hozzáférés, még akkor is, ha az egyik azonosítási tényezőt valakinek sikerülne megszerezni.

Összességében a kiberbiztonsági kockázatok és az elektromobilitási járművek közötti összefüggés vizsgálata kiemelten fontos lépés volt a jövőbiztos mobilitás felé vezető úton. A kutatás során az általam megfogalmazott javaslatok és a jövőben egy megfelelő szabályozási keret kialakítása, továbbá a kiberbiztonsági szakemberek bevonása a gyártók, a fejlesztők, illetve a szolgáltatók körébe nagymértékben segíthet abban, hogy az elektromobilitási járművek és azok felhasználói biztonságosabb környezetben vehessék igénybe ezeket az innovatív közlekedési eszközöket, ezzel hozzájárulva egy fenntartható, biztonságos és technológiailag fejlett közlekedési jövőhöz.

Felhasznált irodalom

Argyropoulos, Nikolaos et al. (2021): Addressing Cybersecurity in the Next Generation Mobility Ecosystem with CARAMEL. *Transportation Research Procedia,* 52, 307–314. Online: https://doi.org/10.1016/j.trpro.2021.01.036

Garcia, Flavio D. et al. (2016): Lock It and Still Lose It – on the (In)Security of Automotive Remote Keyless Entry Systems. In Holz, Thorsten – Savage, Stefan (szerk.): *SEC'16: Proceedings of the 25th USENIX Conference on Security Symposium.* Berkeley: USENIX Association, 929–944. Online: www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/garcia

Instructables (2024): Firmware Downgrade M365. Online: www.instructables.com/Firmware-Downgrade-M365/

Katona Gergő (2022): Autonóm járművek kiberbiztonsági kihívásai (2. rész). *Ludovika.hu,* 2022. január 20. Online: www.ludovika.hu/blogok/cyberblog/2022/01/20/autonom-jarmuvek-kiberbiztonsagi-kihivasai-2-resz/

Katona Gergő (2023): Az autonóm közúti gépjárművek kiberbiztonsági aspektusa és társadalmi megítélése 1. rész. *Hadmérnök,* 18(3), 161–176. Online: https://doi.org/10.32567/hm.2023.3.11

Kim, Kyounggon et al. (2021): Cybersecurity for Autonomous Vehicles: Review of Attacks and Defense. *Computers & Security,* 103, 102150. Online: https://doi.org/10.1016/j.cose.2020.102150

Palkovics László (2020): Kiberbiztonság a járműiparban. *Scientia et Securitas,* 1(1), 2–6. Online: https://doi.org/10.1556/112.2020.00001

Pethő Zsombor – Szalay Zsolt – Török Árpád (2022): Safety Risk Focused Analysis of V2V Communication Especially Considering Cyberattack Sensitive Network Performance and Vehicle Dynamics Factors. *Vehicular Communications,* 37, 100514. Online: https://doi.org/10.1016/j.vehcom.2022.100514

Sanguesa, Julio A. et al. (2021): A Review on Electric Vehicles: Technologies and Challenges. *Smart Cities,* 4(1), 372–404. Online: https://doi.org/10.3390/smartcities4010022

Santra, Atanu (2019): Augmentation of GNSS Utility by IRNSS/NavIC Constellation Over the Indian Region. *Advances in Space Research,* 63(9), 2995–3008. Online: https://doi.org/10.1016/j.asr.2018.04.020

Tóth, András (2017): Information Security for Electric Cars in Accordance with Nist Critical Infrastructure Cybersecurity Framework. *Hadmérnök,* 12(4), 195–206. Online: http://hadmernok.hu/174_19_toth.pdf

Vaidya, Binod – Mouftah, Hussein T. (2020): Cyber Security Considerations for Automated Electro-Mobility Services in Smart Cities. In Mouftah, Hussein T. – Erol-Kantarci, Melike – Sorour, Sameh (szerk.): *Connected and Autonomous Vehicles in Smart Cities.* Boca Raton: CRC Press, 457–473 Online: https://doi.org/10.1201/9780429329401-17

Vinayaga-Sureshkanth, Nisha et al. (2020): Security and Privacy Challenges in Upcoming Intelligent Urban Micromobility Transportation Systems. In *Proceedings of the Second ACM Workshop on Automotive and Aerial Vehicle Security.* New York: Association for Computing Machinery, 31–35. Online: https://doi.org/10.1145/3375706.3380559

Wolf, Marko – Weimerskirch, André – Paar, Christof (2004): *Security in Automotive Bus Systems.* Workshop on Embedded IT-Security in Cars (escar), 1–13. Online: www.weimerskirch.org/files/WolfEtAl_SecureBus.pdf

HADMÉRNÖK
VÉDELEMINFORMATIKA

20. évfolyam (2025) 1. szám 139–161.
DOI: 10.32567/hm.2025.1.8

Lendvai Tünde[1]

Kiberbiztonsági körkép Japánról

Japán kiberbiztonsági reformja és kiberhatalmi ambíciója

Cybersecurity Overview of Japan

Japan's Cybersecurity Reform and Cyberpower Ambition

Absztrakt

Az utóbbi évtizedben Japán jelentős erőforrásokat fektetett kibervédelmi rendszerének fejlesztésébe, amit a regionális ellenfelei – Oroszország, Kína és Észak-Korea – által demonstrált kibertámadó képességekhez kapcsolódó fenyegetéspercepció váltott ki. A szekunder forrásokat elemző kutatás arra irányult, hogy feltárja, milyen országspecifikus sajátosságok teszik lehetővé vagy korlátozzák az ország stratégiai dokumentumaiban előirányzott aktív kibervédelem megvalósítását és az offenzív kiberképességek alkalmazását. A tanulmány amellett érvel, hogy ezt három tényező befolyásolja. Az első a jogszabályi környezetből adódik, ami továbbra is olyan mértékben korlátozza Japán lehetséges válaszlépéseit a kibertérben, hogy a sikermegtagadó elrettentési mechanizmusokat alkalmazó kibervédelem hatékonysága megkérdőjelezhető. A másik két tényező biztonságpolitikai relációban mozdítja elő az offenzív képességek jogszerű alkalmazását. Ennek elemei a nemzetközi kibervédelmi kooperációs hálózat kiépítése és a kiberbiztonsági ökoszisztéma rezilienciáját növelő reformok.

Kulcsszavak: Japán, proaktív kibervédelem, kiberstratégia, offenzív kiberképességek, kiberbiztonság, Önvédelmi Haderő, kibervédelem

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem Hadtudományi Doktori Iskola, e-mail: lendvai.tunde@uni-nke.hu

Abstract

Over the past decade, Japan has invested significant resources in developing its cyber defense system, driven by threat perceptions associated with the demonstrated offensive cyber capabilities of its regional adversaries such as Russia, China, and North Korea. This research, based on secondary source analysis, explores the country-specific factors that enable or limit the implementation of active cyber defense outlined in Japan's strategic documents and the application of offensive cyber capabilities. The study argues that three key factors influence these efforts. The first stems from the legal framework, which continues to constrain Japan's potential responses in cyberspace to such an extent that the effectiveness of cyber defense based on denial-of-success deterrence mechanisms is questionable. However the other two factors, in a security policy context, facilitate the lawful use of offensive capabilities. These include the development of an international cyber defense cooperation network and reforms aimed at enhancing the resilience of the cybersecurity ecosystem.

Keywords: Japan, proactive cyber defence, cybersecurity strategy, offensive cyber capability, cybersecurity, Japan Self Defence Force, cyber defence

Bevezetés

Az utóbbi évtizedben Japán kibervédelmi szakpolitikájának egyik legmegosztóbb dilemmája volt, hogy a pacifista alkotmányos megkötések betartása mellett miként készíthető fel kibervédelmi ökoszisztémája – az államigazgatás, a kritikus infrastruktúrák és a Japán Önvédelmi Haderő – defenzív rendszerekkel és eszközökkel, valamint kizárólag védelmi céllal alkalmazható limitált offenzív képességekkel, az egyre jelentősebb kibertámadó képességekkel rendelkező regionális ellenfelei (Oroszország, a Kínai Népköztársaság és a Koreai Népi Demokratikus Köztársaság) jelentette fenyegetéssel szemben.[2] Noha a japán külpolitika proaktív pacifizmusa jól működik az amerikai–japán szövetség keretében, és összhangban áll az úgynevezett passzív kibervédelem módszereivel, a japán kormányok időről időre keresik a lehetőséget az offenzív kiberképességek jogszerű alkalmazásának előmozdítására, ami – például elrettentési mechanizmusok segítségével – magasabb szintű védelmet tenne lehetővé.[3] A publikáció bemutatja, hogy az elmúlt évtizedben milyen tényezők formálták Japán kibertéri fenyegetéspercepcióját és kiberképességeit, amelyek eredményeképp a tokiói vezetés a passzív védelmi megközelítéstől a 2018-as és 2021-es Kibervédelmi Stratégiában az aktív kibervédelem irányába mozdult el.[4] Az egyes fejezetekben időrendben áttekintjük azon országspecifikus nehézségeket vagy kibervédelmi szakpolitikai reformokat, amelyek napjainkban is hátráltatják az aktív kibervédelem megvalósítását.

[2] Katagiri 2022: 49–51; Bartlett 2020: 93–94; Basu 2024.
[3] Osawa 2024: 74; Najah 2024; Siripala 2024.
[4] Osawa 2024: 71–72; Kosuke 2024.

A témában elérhető, főként szekunder forrásokon alapuló szakirodalom feldolgozása deduktív és leíró kutatási módszerrel valósult meg. A kiberbiztonsági incidensek esetszámának vizsgálatához a szerző a JPCERT/CC japán nemzeti CSIRT (Computer Security Incident Response Team, számítógép-biztonsági incidenskezelő csoport) negyedéves jelentéseiben publikált adatait használta fel, amelyeken idősorelemzést végzett a 2019–2023 közötti időszakban. A kutatás arra irányult, hogy feltárja, milyen elméleti megközelítés és országspecifikus sajátosságok teszik lehetővé vagy korlátozzák Japánban az offenzív kiberképességek alkalmazását, és ezáltal az aktív kibervédelmi stratégia kialakítását (K1). Jelen tanulmány amellett érvel, hogy ez elsősorban három tényezőre vezethető vissza.

H1: Japán kiberbiztonsági fenyegetéspercepcióját a regionális ellenfelei által kifejlesztett és egyre gyakrabban demonstrált offenzív kiberképességek, valamint az ország gazdasági rendszerének és haderejének információs technológiáktól való függősége alakítja.

H2: A kibertérből érkező kihívások ellensúlyozása érdekében Japán újabban egy jóval szélesebb körű – az USA-partnerségen felüli – nemzetközi kooperációs hálózat kiépítésére törekszik.

H3: A japán aktív kibervédelmi stratégia hatékony végrehajtását korlátozza a jogszabályi környezet.

A japán kibervédelmi stratégia jogi korlátai (H3)

A japán kibervédelmi reformfolyamat eredményeinek értékeléséhez elsőként azt fontos megérteni, hogy az alkotmányos megkötések milyen korlátok közé szorítják a kiberstratégiai modellt és az offenzív kiberműveletek önvédelmi célú alkalmazhatóságát. A fejezet a passzív és aktív kibervédelem, valamint az offenzív képességek terminológiája mentén mutatja be, hogy a jogi környezet miként befolyásolja a japán kibererő fejlesztési lehetőségeit.

A passzív kibervédelem és az aktív kibervédelem közötti terminológiai különbségeket Berzsenyi a disszertációjában többféle megközelítésben mutatta be.[5] Amennyiben az elhatárolást a tevékenység típusa és célja mentén kívánjuk ismertetni, a passzív kibervédelem fő ismérve, hogy az aktivitás nem lépi túl a saját hálózat határait, mert az információk és rendszerek védelmét a támadások elhárításával és a sérülékenységek csökkentésével biztosítja. A passzív kibervédelem szinte minden jogrendszerben, így Japán esetében is elfogadott, mivel célja a kiberrendszerek határvédelmének kialakítása (például vírusvédelmi eszközökkel és behatolásészlelő rendszerekkel), illetve támadásokkal szembeni rezilienciájának kiépítése (például *zero-trust* model szerinti rendszertervezési megoldásokkal). Ennélfogva a passzív védelem nem alkalmaz közvetlen válaszlépéseket a támadó infrastruktúra megzavarása vagy megsemmisítése érdekében, ezért nem feltételez támadó, csak önvédelmi szándékot.[6]

[5] Berzsenyi 2023: 77–84.
[6] Berzsenyi 2023: 77–78.

Ezzel összefüggésben elmondható, hogy a japán kormányok évtizedek óta úgy értelmezik az 1946-os Alkotmány híres 9. „békecikkét",[7] miszerint a támadó katonai erő alkalmazásának tilalma nem zárja ki Japán önvédelemhez való alapvető jogát, illetve az annak gyakorlásához szükséges minimális fegyveres erő fenntartását, így a defenzív és offenzív képességeket magában foglaló kibererő felépítése és fenntartása indokolt. Bartlett több kutatásában is kiemeli, hogy a japán Alkotmány önvédelemre vonatkozó megkötése befolyásolja a kibertérben műveleteket végrehajtó egységek határokon belüli és kívüli jogszerű alkalmazhatóságát is.[8] Emiatt – a passzív kibervédelmi stratégiai modellel ellentétben – az aktív kibervédelem Japán számára jogilag és etikailag érzékenyebb terület, abból kifolyólag, hogy noha alapvetően védekező jellegű, a határai elmosódhatnak az offenzív műveletek irányába. Berzsenyi megfogalmazásában: „az aktív kibervédelem olyan közvetlen védelmi tevékenység, ami rombolja, csökkenti vagy megsemmisíti a kiberfenyegetések baráti erőkkel szembeni hatékonyságát."[9] Noha a szakirodalomban nincs konszenzus a tekintetben, hogy milyen megoldások és rendszerek tekinthetők aktív kibervédelmi képességnek, néhány példa következik: a behatolásmegelőző rendszer *(intrusion prevention system)* vagy *honeypot* elhelyezése, valamint a védett hálózaton túli olyan válaszlépések alkalmazása a támadások megelőzésére és megzavarására, mint a C2 szerverek *(command and control)* hozzáférésének blokkolása vagy irányításának átvétele.[10]

Japánban a határokon túlnyúló – önvédelmi célú – kiberműveletek jogszerű alkalmazhatósága kérdéses, ám az ország biztonság- és védelempolitikai gondolkodásában már megjelent ennek alapja. Disszertációjában Fábián Emília részletesen bemutatja, hogy a kizárólag védelemorientált megközelítés és a fegyveres erő passzív önvédelmi, avagy reagáló célú alkalmazhatósága által szabott alkotmányos kereteket az Abe-kormány (2012–2020) biztonságpolitikája igyekezett leginkább kitágítani proaktív irányba nemzeti és nemzetközi relációban egyaránt. A kormányzó Liberális Demokrata Párt (a továbbiakban: LDP) a proaktív pacifizmus politikáját többek közt az USA haderejének való kiszolgáltatottsággal és a megváltozott biztonságpolitikai környezetből eredő sokrétű fenyegetéssel indokolta.[11] Nemzetközi relációban a tokiói vezetés amellett érvelt, hogy Japánnak a globális felelősségvállalás jegyében aktívan fel kell lépnie az olyan határokon átívelő fenyegetések ellen, mint a terrorizmus és a kiberbűnözés, ezért növelnie kell szerepvállalását a nemzetközi békemissziókban (a kollektív önvédelmi jog gyakorlása által), amihez az Önvédelmi Haderő képességeinek fejlesztése elengedhetetlen.[12] Katagiri kutatásai is alátámasztják, hogy nemzeti relációban a kabinet álláspontja azt tükrözte, hogy a regionálisan növekvő militarizációs trendek hatása mellett a kibertérből érkező kihívások csökkentése nélkül nem garantálható a nemzetközi kereskedelem zavartalansága, ezáltal a nemzetgazdaság stabilitása.[13]

[7] The Constitution of Japan (Japán Alkotmánya), 9. cikk.
[8] Bartlett 2019: 17–30; Bartlett 2020: 94–96.
[9] Berzsenyi 2023: 78.
[10] Berzsenyi 2023: 80–82.
[11] Fábián 2015: 180–182.
[12] Fábián 2015: 169–174.
[13] Katagiri 2021: 332–336.

A híres 9. cikk mellett Japán jogi környezete több ponton is szigorú korlátok közé szorítja a nemzeti szintű kibervédelmi feladatok egyik fontos elemét, a kibertérben végzett felderítő műveletek és a rádióelektronikai hírszerzés jogszerű végrehajtását.[14] Egyfelől az Alkotmány 21. cikkéből vezethető le a cenzúra tilalma és a távközlési titok védelme, ami mellett a távközlési törvény 4. cikke előírja, hogy a távközlési szolgáltató által lebonyolított kommunikáció bizalmas jellegét tilos megsérteni.[15] Ezt a szabályozást a japán jogrend szigorúbban értelmezi és interpretálja más országokhoz képest, ami megnehezíti a végrehajtó hatalom és a távközlési szolgáltatók számára az adatforgalom megfigyelését, ezzel a kiberműveletek észlelését és a támadó infrastruktúra elemeinek beazonosítását. A japán Büntető törvénykönyv 161. cikke tiltja az elektronikus vagy mágneses feljegyzések jogosulatlan létrehozását, míg a 168. cikk tiltja a jogosulatlan parancsokat tartalmazó elektronikus vagy elektromágneses rekordok készítését, így rendkívül korlátozott módon valósulhat meg az állami szereplők számára a kommunikáció elemzése és visszafejtése a támadó aktor beazonosítása érdekében.[16] Habár belföldön a Védelmi Minisztérium és az Önvédelmi Haderő korlátozott mértékben jogosult a vezeték nélküli kommunikáció megfigyelésére, a vezetékes digitális kommunikáció széles körű megfigyelése nem engedélyezett még nemzetbiztonsági célból sem.[17]

Japánban napirenden lévő jogi kérdés az is, hogy a kiberbűncselekményeket elszenvedő magáncégek kötelezhetők-e arra, hogy bejelentsék az incidenst az állami szerveknek. A kötelező jelentéstétel hiánya miatt a vállalkozások jellemzően elkerülik azon incidensek nyilvánosságra hozatalát, amelyek sikeresen kompromittálták a rendszerüket (viszont a személyes adatokat érintő incidenseket kötelező jelenteni Japánban is).[18] Ez késlelteti a kiberfenyegetésekre, sérülékenységekre és támadási technikákra vonatkozó információk vállalatok közötti kölcsönös megosztását, ami azt eredményezi, hogy az állami és a magánszektor közt sem történik előrelépés a gyakori támadási minták és technikák megértésében, ami szükséges lépés az ellenintézkedések kialakításához.[19]

A kiberműveletek észlelhetőségén túl a támadó infrastruktúra semlegesítésére irányuló erőfeszítéseket is összhangba kell hozni Japán jogosulatlan számítógép-hozzáférést tiltó törvényével (Japan's Act on Prohibition of Unauthorized Computer Access). Osawa kutatásaiban rámutat arra, hogy más államokkal ellentétben a jogosulatlan számítógépes hozzáférés tilalma alól a japán kormányzati szervek nem képeznek kivételt. A támadó infrastruktúra feletti irányítás átvétele mellett a semlegesítés másik módja lehet egy kártékony program *(malware)* küldése a támadás forrására, ami ütközhet a malware létrehozását és alkalmazását büntető törvényekkel, ezért a büntetőjog revíziója is szükséges lenne az aktív kibervédelem kialakításához.[20]

[14] Katagiri 2021: 339–342.
[15] A 2022. évi 70. törvény a japán távközlési vállalkozásokról szóló 1984. évi 86. törvény egyes rendelkezéseinek módosításáról, 4. cikk; Japán Alkotmánya, 21. cikk.
[16] Osawa 2024: 73–74; Onodera–Tanaka–Shimamura [é. n.].
[17] Katagiri 2021: 339.
[18] Siripala 2024; Japan Mulls Requiring Private Sector Operators to Report Cyberattacks on Infrastructure 2024.
[19] Siripala 2024; Alan 2024.
[20] Osawa 2024: 74.

Összességében tehát a távközlési és büntetőjogi megkötések kifejezetten a hírszerzési célú, valamint az offenzív képességek jogszerű alkalmazhatóságát korlátozzák. Ez utóbbi megnyilvánulását érdemes elméleti oldalról is bemutatni. Az amerikai összhaderőnemi megközelítésben alkalmazott terminológia alapján az offenzív kiberműveleti képességek feloszthatók a műveleti tér megtagadására és manipulálására[21] irányuló tevékenységekre. Az ellenfél erőforrásokhoz történő hozzáférését gátló, úgynevezett megtagadó műveletek további három kategóriába sorolhatók hatásuk alapján: degradálás, megzavarás és pusztítás. A degradálás redukálja az ellenfél által használható erőforrásokat, míg a kibertérbeli megzavarás időszakosan ellehetetleníti az ellenfél által használt infrastruktúra hozzáférését, így megakasztja tevékenységét. A tudományos szakirodalom Japán legnagyobb kibervédelmi stratégiai problémájaként azonosítja, hogy az alkotmányos megkötések és a jogi környezet még a legtágabb értelmezésben is összeférhetetlenek egyes offenzív kiberműveletekkel, így például a megtorló elrettentési mechanizmusokat (visszatámadás, *hackback*) alkalmazó kibervédelmi modell megvalósításával.[22] Enélkül azonban kérdéses hatékonysággal vagy egyáltalán nem valósítható meg az aktív kibervédelmi stratégia azon karakterisztikája, amely a védett, saját hálózaton túli ellenlépéseket foglalja magában.[23]

A szakirodalom-elemzés azt mutatja, hogy a meglévő jogrendszer szigorúan a passzív és aktív kibervédelmi stratégiai modellel összehangolt offenzív kiberképességek fenntartását teszi lehetővé. Emiatt a kormányzó LDP-nek feltehetően szándékában áll a kiberbiztonsági jogszabályok revíziója a határokon átnyúló aktív kibervédelemre vonatkozó kormányzati stratégia bevezetése érdekében.[24] Ez lehetővé tenné, hogy a nemzetbiztonsági aggályokat felvető súlyos kibertámadások megelőzhetők legyenek például a támadó aktorok szervereibe való behatolással és azok kiiktatásával.[25] A kormányzati szándékot az támasztja alá, hogy 2023 januárjában a kabinet titkárságán létrehoztak egy hivatalt, amely a kiberbiztonsági szabályozások előkészítésével foglalkozik.[26]

A japán kibervédelmi szakpolitika reformja 2012–2022 között: egy globális kiberhatalom víziója (H1)

Ahogyan a fentiekben is említettük, a hagyományosan passzív kibervédelmi szakpolitika reformját a második Abe-kormány kezdte meg azon törekvésével, hogy a kibertér használatát nemzetbiztonsági politikájának középpontjába emelje, és a 2012–2016 közti védelempolitikai intézkedéseivel stabil alapot teremtsen Japán globális kiberhatalommá válásához.[27] Kallender és Hughes amellett érvelt, hogy a tokiói vezetés kiberhatalmi ambíciójának megvalósításához szükséges reformok nemzeti és nemzetközi

[21] Berzsenyi a következőképp fogalmazta meg a manipulálást: „lényegében az ellenfél rendelkezésére álló információk, információs rendszerek és/vagy hálózatok feletti ellenőrzést és az ezekben – a parancsnok célkitűzései szerint – végrehajtható változtatási képességet jelenti." Berzsenyi 2023: 85.
[22] Katagiri 2021: 335, 339–342; Bartlett 2020; Osawa 2024: 72–74.
[23] Berzsenyi 2023: 80–84.
[24] Siripala 2024.
[25] Kosuke 2024.
[26] Osawa 2024: 74.
[27] Gady 2017: 24–28.

pillérét alkotó intézkedéseket egy újfajta, szekurizációs elemeket is magában hordozó védelempolitikai narratíva is kísérte. Ezt támasztja alá, hogy az LDP már 2012 februárjában – közvetlenül a kormányra jutása után – a *Javaslat az információbiztonságról* című dokumentumban a nemzetbiztonság kritikus elemének nyilvánította a kibertér biztonságának megtartását.[28] Ezen túlmenően az Abe-kormány első, 2013. évi Kiberbiztonsági Stratégiája nóvumként részletezte a japán Védelmi Minisztérium és a Japán Önvédelmi Haderő szerepét a „külföldi kormányok által fegyveres támadás részeként végrehajtott kibertámadások és más olyan nemzeti szintű kibertámadásokra adott válaszreakciókban, amelyekben külföldi kormányok részvétele feltételezhető".[29] Ennek megfelelően az Önvédelmi Haderőt jelölték ki felelősnek a kiberműveletek elhárításáért, ha azok fegyveres támadások részét képezik, és felhatalmazták a Védelmi Minisztériumot, hogy hozzon létre egy védelmi célú mandátummal rendelkező kiberegységet a haderőben (Kibervédelmi Csoport, Cyber Defense Unit vagy Cyber Defence Group).[30]

A szekurizációra vonatkozó érvelést erősíti Soesanto kutatásának eredménye, ami rávilágít arra, hogy az LDP a kibertérből érkező fenyegetés kezelésére egyre militarizáltabb intézkedéseket hozott, és centralizáló reformokat indított meg a kritikus információs infrastruktúrákra fókuszálva, amivel politikai szinten is reagált két jelentős, 2011-ben nyilvánosságra került incidensre.[31] Az egyik esetben, 2011 júliusában, a japán képviselőház szervereit kompromittálta egy kínai hátterű fejlett perzisztens fenyegetés (a továbbiakban APT) az Icefog nevű interaktív kémprogrammal *(backdoor)*.[32] A másik eset ugyanezen év augusztusában történt, amikor az ország egyik legjelentősebb hadiipari és nehézipari vállalatát, a Mitsubishi Heavy Industries ellen követtek el összehangolt hírszerzési célú kampányt, noha a vállalat álláspontja szerint titkos dokumentumok nem szivárogtak ki.[33] A Kabinet szekurizációs törekvéseiben feltehetően olyan nemzetközi események is szerepet játszottak, mint az iráni atomprogram elleni Stuxnet-művelet és a 2011-es dél-koreai kereskedelmi bankok, továbbá a védelmi ipari vállalatok és kormányzati szervek weboldalait érő, észak-koreai DDoS-támadás.[34]

A defenzív képességfejlesztési irányban 2019-ben következett be újabb változás, amikor a Mitsubishi Co.-t újfent sikeresen kompromittálta egy állami hátterű aktor, ezúttal az APT41 csoport.[35] Ezen fejlett perzisztens fenyegetés tevékenységét gyakran azonosítják a Kínai Népköztársaság (a továbbiakban KNK) állam alatti kiberegységeinek műveleteivel.[36] Az állami hátterű offenzív kibertéri jelenlét növekedése miatt a tokiói vezetés végül amellett kötelezte el magát, hogy 2023-ig felülvizsgálja, miként alakíthatók offenzív elemeket magában foglaló kiberműveleti képességgé az Önvédelmi

[28] Kallender–Hughes 2016: 127.
[29] Japán Információbiztonsági Politikai Tanács 2013: 42.
[30] Kallender–Hughes 2016: 128.
[31] Soesanto 2020: 8, 11, 30.
[32] Kaspersky Lab 2013: 14.
[33] Soesanto 2020: 8.
[34] Koo 2013.
[35] Paganini 2020.
[36] Lásd például MITRE [é. n.]; Malpedia [é. n. a].

Haderőben meglévő kapacitásai.[37] Mivel Japán jogi környezete korlátok közé szorítja a katonai erő alkalmazását, a kiberegységek offenzív képességeit úgy limitálták, hogy azokat katonai konfliktus keretében a hálózatok és számítógépes rendszerek megzavarására alkalmazhassák, nem pedig arra, hogy fizikai rendszerekben kárt okozva vagy a kibertér adottságait fegyverként felhasználva támadást indítsanak más államok ellen.[38] Ezt a szakpolitikai álláspontot tükrözi Japán legutóbbi, 2021-es Kiberbiztonsági Stratégiája (Cybersecurity Strategy), amely a nemzetbiztonsági érdekből végzett tevékenységek és az ország gazdasági stabilitása szempontjából közelíti meg a kibertér biztonságát. A stratégia a „szabad, tisztességes és biztonságos kibertér" alapelveinek garantálásához a nemzetközi együttműködés szükségességét hangsúlyozza az USA, Ausztrália és India irányába, valamint az ASEAN-tagállamok részére nyújtott kibervédelmi kapacitásépítő programok folytatását az ellátási láncok megbízhatóságának megőrzéséhez. A dokumentum belföldre fókuszáló hatókörében Japán védelmi, elrettentő és helyzetfelismerési képességeinek erősítését jelölte ki elsősorban. Ezenfelül az LDP a humán erőforrás képzésének és digitális kompetenciáinak egyéni fejlesztésére irányuló programok további finanszírozását is megerősítette a stratégiai célok közt.[39] Gazdasági-társadalmi vonatkozásban a vállalati szféra innovációs képességének és digitális transzformációjának támogatása jelent meg politikai célkitűzésként.[40]

A Kisida-kormány 2022 decemberében három fontos védelmi dokumentumot hagyott jóvá, amelyek együttesen alkotják Tokió átfogó védelempolitikáját: a Nemzeti Biztonsági Stratégiát (National Security Strategy), a Nemzeti Védelmi Stratégiát (National Defense Strategy), amely a védelmi célokat és az elérésükhöz szükséges eszközöket határozza meg, valamint a Védelmi Fejlesztési Programtervet (Defence Buildup Plan), amely tartalmazza a 2023–2027-es védelmi kiadásokat és az eszközbeszerzések volumenét.[41] A Nemzeti Biztonsági Stratégia nóvumként említi a megelőző célú kiberműveletek végrehajtását még olyan esetekben is, amelyek nem minősülnek fegyveres támadásnak, azonban súlyos nemzetbiztonsági aggályokat vetnek fel a kormányzat és a létfontosságú, kritikus infrastruktúrák érintettsége miatt.[42] Ez valójában a jogi korlátok jelentette problémát nem rendezi, csak politikai felhatalmazást jelent a japán kormány számára, hogy utasítást adjon a potenciális támadó infrastruktúrájába való behatolásra annak semlegesítése érdekében. Vagyis sikermegtagadó elrettentési mechanizmusként az ellenfél képességeinek degradálását és megzavarását teszi lehetővé, megtorló lépéseket nem.[43] Noha a 2022-es Nemzeti Biztonsági Stratégia elsősorban a rakétavédelem kontextusában nevesítette az ellencsapás lehetőségét, ezzel párhuzamosan a japán biztonságfelfogásban elméleti lehetőség nyílt az Önvédelmi Haderő offenzív kiberképességeinek szélesebb körű alkalmazhatóságára az aktív kibervédelmi stratégia keretében.[44] A Nemzeti Védelmi Stratégia az Önvédelmi Haderő szerepének bővítését tűzte ki a következő tízéves időtávra a tekintetben, hogy a katonai

[37] Japán Védelmi Minisztérium 2019: 229.
[38] Bartlett 2020: 96.
[39] Japán Nemzeti Incidenskészenléti és Kiberbiztonsági Stratégiai Központja 2021: 6–7.
[40] Japán Nemzeti Incidenskészenléti és Kiberbiztonsági Stratégiai Központja 2021: 3–4, 7, 10.
[41] Lottaz 2023.
[42] Hideshi 2023.
[43] Berzsenyi 2023: 80–85.
[44] Hideshi 2023.

hálózaton kívüli entitások biztosításával hozzájáruljon Japán teljes kiberterének védelméhez is. Ehhez a politikai célkitűzéshez igazodva a 2022-es Védelmi Fejlesztési Programterv a 2027-es pénzügyi évre előirányozta az Önvédelmi Haderő újonnan létrehozott Kibervédelmi Parancsnokságának (Cyber Defence Command, korábban Cyber Defence Unit) bővítését mintegy 4000 főre, és a teljes kibervédelmi állomány létszámának növelését 20 000 főre.[45]

Összességében a proaktív pacifizmus irányvonalát a Szuga-kormány (2020–2021) és a Kisida-kormány (2021–2024) is követte. A sokrétű fenyegetéspercepció kezelésére Tokió olyan stratégiát alkalmaz, amellyel nem engedi műveleti előnyhöz jutni a létszámában és a rendszeresített eszközök mennyiségében fölényben lévő kínai haderőt. Ezért a japán hosszú távú haderő-modernizáció[46] a korábbi sikermegtagadás-alapú elrettentési stratégia mellett – amelynek célja, hogy az elérendő katonai célhoz képest túl sok erőforrást emésszen fel egy támadás – a megtorlásalapú elrettentéshez szükséges képességek kiépítésére törekedett az elmúlt 15–20 évben, amivel akár kínai vagy észak-koreai támaszpontok megsemmisítése is lehetséges egy támadás esetén.[47] Mindezek eléréséhez elsősorban az alkotmány értelmezésének megváltoztatására volt szükség, amivel lehetővé vált a védelempolitikai reformok végrehajtása valamennyi műveleti tér, így a fentiekben részletezett *kiberdomain* és kibererő vonatkozásában is.

Japán kiberbiztonsági ökoszisztémája és a centralizáló reformok áttekintése

Az Abe-kormány (2012–2020) kiberhatalmi ambíciója megvalósításának nemzeti (belföldre irányuló) pillére egy jogilag jól szabályozott, centralizált felelősségi körökkel működő kiberbiztonsági igazgatási rendszer kialakítására irányult, amely szakpolitikai háttértámogatást nyújt a kabinet legfőbb biztonságpolitikai döntés-előkészítő szerve, a Nemzetbiztonsági Tanács (National Security Council) részére.[48] Ennek alapjait a 2014-től hatályos Kiberbiztonsági kerettörvény (Basic Act on Cybersecurity)[49] fekteti le, amelyben a japán törvényhozás regionális viszonylatban úttörőként határozta meg a kibervédelem alapfeladatait és államigazgatásra vonatkozó stratégiai céljait (amelyeket 2016-ban, 2019-ben és 2022-ben felülvizsgált), továbbá rendelkezett a kibervédelmi ökoszisztémát koordináló szervezetek létrehozásáról.[50]

A japán kibervédelmi szervek hierarchiájának tetején egy miniszteri szintű koordinációs szerv, a Kiberbiztonsági Stratégiai Központ (Cybersecurity Strategic Headquarters) helyezkedik el, amelyben állandó szakértői testületek működnek, például a kritikus infrastruktúrákat, az emberi erőforrásokat és információbiztonsági tudatosítást, valamint a technológiai fejlesztési programokat érintő ügyekben. A központ alárendeltségében 2015-től működik a Nemzeti Incidenskészenléti és Kiberbiztonsági Stratégiai Központ

[45] Osawa 2024: 72; Japán Védelmi Minisztérium 2022a: 26; Japán Védelmi Minisztérium 2022b: 11–12.
[46] Az elmúlt 15–20 évben Japán haditengerészeti (például kékvízi hajóegységek és fedélzeti rakétaelhárító rendszerek) és 4–5. generációs légierő-részképességek minőségi fejlesztésével (és elegendő mennyiség rendszeresítésével) kezdte ellensúlyozni a KNK haderejének mennyiségi fölényét.
[47] Szakértői interjú, podcast alapján készült. FIXTV HUNGARY 2024.
[48] Bartlett 2019: 26.
[49] Japán Kiberbiztonsági kerettörvénye (The Basic Act on Cybersecurity) [2014. évi 104-es törvény].
[50] Basu 2024.

(National Centre for Incident Readiness and Strategy for Cybersecurity, NISC), amely a Japán Önvédelmi Haderő és a rendőrség mellett működve koordinálja a kibervédelmi szakpolitika végrehajtását és a kibervédelmi operatív egységek irányítását. A konkrét incidensekre reagáló, műveleti kiberegységek a Kormányzati Biztonsági Műveleti Koordinációs Csoport (Government Security Operation Coordination Team, GSOC) és a Kiberincidens Mobil Segédcsapat (Cyber Incident Mobile Assistant Team, CYMAT) keretei közt folytatják tevékenységüket. Japán kibervédelmi ökoszisztémájának további fontos szerve a Kiberbiztonsági Tanács (Cybersecurity Council), amelynek fő funkciója, hogy a köz- és magánszféra szereplői közt biztosítsa az információátadást, és korai előrejelzést adjon kibervédelmi kihívások és fenyegetések felmerülése esetén a Kiberbiztonsági Stratégiai Központnak.[51]

A Kiberbiztonsági Stratégiai Központ mellett a kiberbiztonsági szakpolitika tervezésének második ágát (2021-től) a Digitális Ügynökség (Digital Agency) tevékenysége határozza meg. A Digitális Ügynökség a kormányzási funkciók digitális transzformációjának kivitelezéséhez nyújt projektmenedzsment-támogatást (például a társadalmi célcsoport tudatosítása kapcsán), továbbá iránymutatást ad a kormányzati szervek részére az infrastruktúra rezilienciájának növeléséhez (például piaci szférában bevált innovatív technológiák adaptációja kapcsán).[52] A szakpolitikai tervezés harmadik ága a kritikus infrastruktúrák védelme, ennek érdekében Japán rendszeresen ad ki akcióterveket. Jelenleg ezen akciótervek negyedik kiadása hatályos (2022-es kiberbiztonsági politika a kritikus infrastruktúrák védelmére, Cybersecurity Policy for Critical Infrastructure Protection). Az akcióterv célkitűzései közül kiemelendő a kockázatmenedzsment-folyamatok standardizálása, az érintett ágazatok számára releváns fenyegetésekről szóló információmegosztó *(threat intelligence)* folyamatok megalapozása és folyamatos fejlesztése, valamint az a törekvés, hogy nemzeti szintű incidenskezelő szervezeteket hozzanak létre, amelyek kifejezetten ezzel a speciális (értsd: nemcsak IT, hanem ipari környezetet is működtető) területtel foglalkoznak.[53]

A centralizáló reformok nemcsak az államigazgatási szerveket érintették, hanem az Önvédelmi Haderőt is. A jelenlegi struktúrában a szárazföldi, a haditengerészeti, valamint a légi- és űrerők összhaderőnemi együttműködését a Központi Parancsnoki Rendszer (Central Command System, CCS) és a Védelmi Információs Infrastruktúra (Defense Information Infrastructure, a továbbiakban DII) biztosítja, amelynek működtetését és karbantartását egy dedikált parancsnokság (C4 Rendszerek Parancsnoksága, C4 Systems Command) felelősségi körébe rendelték. A DII a japán Védelmi Minisztérium és a haderő közös információs és kommunikációs hálózata, amely az egyes bázisokat és helyőrségeket köti össze, két részre osztva: nyílt rendszerre (kapcsolat az internettel) és zárt rendszerre (titkosított adatok kezelése céljából, ami nem csatlakozik külső hálózatokhoz). A C4 Rendszerek Parancsnoksága két egységet foglal magában: a hálózatüzemeltetési csoportot *(network operation group)* és a központi parancsnoki rendszer működtetéséért felelős egységet *(central command post operations unit)*.[54]

[51] *National center of Incident readiness and Strategy for Cybersecurity NISC*. About NISC. [n.d.].
[52] Japan Digitális Ügynökség [é. n.].
[53] Japán Információbiztonsági Politikai Tanács 2014: 22–28; Japán Kiberbiztonsági Stratégiai Központ (NISC) 2022: 12–35.
[54] Soesanto 2020: 22–23.

A fentiekben említett kibervédelmi egység (Cyber Defence Unit) is ezen parancsnokság alárendeltségébe tartozott 2022-ig,[55] azonban a legfrissebb Védelmi Fejlesztési Programterv önálló parancsnoksági státuszba emelte. Ez a változás célzottan arra irányul, hogy a 2023 márciusában 540 fős létszámmal megalakuló Japán Kibervédelmi Parancsnokság (Cyber Defence Command) már egy agilisabb és autonómabb struktúrában legyen képes reagálni a kibertérben jelentkező fenyegetésekre, valamint hatékonyabban integrálhassa az offenzív képességeket és a védelmi műveleteket.[56] A Kibervédelmi Parancsnokság (Cyber Defence Command) napjainkra mintegy 800 fős állománya önállóan felel a kiberfenyegetések felderítéséért, a DII védelméért, és biztosítja az Önvédelmi Haderő hálózatának folyamatos védelmi felügyeletét.[57] A fentiekben bemutatott jogi megkötések és stratégiai dokumentumok aktív kibervédelemre vonatkozó célkitűzéseivel összhangban a Kibervédelmi Parancsnokság hatáskörébe tartozik az operatív kiberműveletek végrehajtása.[58]

Kibervédelmi és kiberdiplomáciai célok megjelenése a külpolitikában (2012–2022)

Japán kiberhatalmi ambíciója megvalósításának nemzetközi pillére két területen kívánt eredményeket elérni. Ezen területek egyike az USA-val való kooperáció további bővítése, noha a két nemzet minisztériumi és ügynökségi delegációi már 2013-tól évenként egyeztettek a Japán–USA Kiberdialógus (Japan-US Cyber Dialogue) keretében, a kétoldalú operatív együttműködés és a kibervédelmi szakpolitika összehangolása érdekében.[59] A második Abe-kormány – a Japán és az USA közötti kiberdialógus napirenden tartása mellett – elsősorban arra törekedett, hogy az Egyesült Államokkal fennálló védelmi garanciákat kiterjesszék a *kiberdomainre,* és elmélyítsék a két nemzet kooperációját a kibertéri fenyegetések felderítésében. Kallender és Hughes amellett érvelt, hogy a japán szakpolitikai vezetés e tekintetben sikereket ért el, mert a kétoldalú Védelmi Irányelvek (Defence Guidelines) 2015-ös kiegészítésében a két kormány rögzítette az együttműködését a kritikus infrastruktúrák és azon szolgáltatások védelme érdekében, amelyektől az Önvédelmi Erők és az Egyesült Államok Fegyveres Erői küldetésük teljesítése során függenek. Ennek keretében a japán fél elsődleges felelősségi és hatáskörébe delegálták a szigetország területét vagy az Önvédelmi Haderőt érő kibertéri műveletekre adott defenzív válaszlépés műveleti tervezését és kivitelezését, amihez az USA hadereje támogatást nyújt. Ezzel a feladatmegosztással közel egyenlő súlypontra igyekeztek terelni a partnerségi viszonyt.[60] Fontos aspektus volt, hogy a nukleáris védőernyőhöz hasonlatosan, az amerikai fél vállalta az elrettentő célú kibertéri offenzív műveleti támogatást.[61] A kooperáció elmélyítését mutatja, hogy a Védelmi Irányelvek tartalmazza

[55] A kibervédelmi egység megalakulásakor nagyjából 90 fős volt, 2021-ben 220–290 fősre becsülték. Lásd Katagiri 2021: 339.
[56] Japan's SDF Launches New Cyber-Defense Unit 2022.
[57] Strategic Command 2024.
[58] Japan's SDF Launches New Cyber-Defense Unit 2022.
[59] Japán Külügyminisztérium 2013; Japán Külügyminisztérium 2024; Soesanto 2020: 30.
[60] Kallender–Hughes 2016: 136–137; Japán Külügyminisztérium 2015: 22.
[61] Kallender–Hughes 2016: 138.

a bilaterális fenyegetés-hírszerző hálózat fenntartását, vagyis a kibertéri fenyegetésekről és feltárt sérülékenységekről való kormányközi információmegosztást, ami kiterjedhet a magánszektor irányába is, továbbá a szakképzések és a kiberképességek fejlesztésével kapcsolatos jó gyakorlatok átadását.[62] A kibertér védelmére irányuló megállapodás hatóköre miatt szükségszerű volt a két haderő műveleti egységei és kiberképességei közti interoperabilitás megteremtésére, ezért a Védelmi Irányelvekben a felek a közös katonai kibergyakorlatok megtartása mellett kötelezték el magukat.[63] Ezzel összhangban a USINDOPACOM (U.S. Indo-Pacific Command) és a japán Védelmi Minisztérium 2019-től napjainkig legalább éves szinten szervezett – a térségbeli szövetségeseik aktív részvételével vagy megfigyelők delegálása mellett – többdimenziós *(multidomain)* szimulációs gyakorlatot *(tabletop)*.[64] Például az Indo-Pacific Critical Infrastructure Workshop[65] és a Cobra Gold (az USA, Japán és Dél-Korea közti multilaterális kibervédelmi gyakorlat komponense) elnevezésű szimulációk középpontjában a kritikus infrastruktúrákat vagy a katonai és polgári rendszerek összekapcsolódási pontjait érintő kiberműveletekkel szembeni koordinált válaszlépések és közös fellépési stratégiák tesztelése állt.[66]

A kiberhatalmi ambíció megvalósításához vezető út második meghatározó területe Japán kibervédelmi kapacitásépítő tevékenysége, amely (az USA-val való együttműködés elmélyítésével párhuzamosan) már a 2009–2013-as időszakban egyre jelentősebbé vált.[67] Bartlett kutatásában feltárta, hogy Japán – kezdetben az ASEAN közvetítésével – szerepet vállalt azon délkelet-ázsiai államok lakosságának tudatosításában, kormányzati területen dolgozó kibervédelmi szakembereinek képzésében és kritikus infrastruktúrájának rezilienciáját növelő szakpolitikák megvalósításában, amelyre saját ipara beszállítóként vagy piacként támaszkodott.[68] Emiatt a kibervédelmi kapacitásépítő szakpolitika célkitűzése elsősorban az lehetett, hogy stabil gazdasági környezetet biztosítson a japán vállalatok számára Délkelet-Ázsiában, másodsorban az, hogy diverzifikálja az USA-n kívüli biztonsági kapcsolatait, és ellensúlyozza a katonai és gazdasági területen felemelkedő Kínai Népköztársaság térségbeli pozícióit.[69] A tokiói vezetés külpolitikájában csak később, 2016-tól jelent meg célként, hogy technológiai kompetenciák átadására irányuló kiberbiztonsági kapacitásépítő támogatással piacot teremtsen a japán kibervédelmi vállalati szféra számára az ASEAN-tagállamokban.[70]

Japán mint újonnan felemelkedő kiberhatalom képét tükrözi egy 2020-as harvardi kutatói jelentés is, amely számos technológiailag fejlett országot hasonlít össze a kibervédelem területén az erőforrások alkalmazásának képessége és a kormányzati szándék céljai alapján (például hírszerzés, destruktív műveletek, kibererő

[62] Japán Külügyminisztérium 2015: 21–23.
[63] Japán Külügyminisztérium 2015: 21–23.
[64] Bartlett 2020: 97.
[65] Amerikai Egyesült Államok Indo-csendes-óceáni Parancsnokság 2024.
[66] Brunson–Chick 2024.
[67] *Joint Ministerial Statement of the ASEAN-Japan Ministerial Policy Meeting on Cybersecurity Cooperation* 2013.
[68] Bartlett 2023: 479–482.
[69] Bartlett 2023: 495–497.
[70] Bartlett 2023: 495; Bartlett 2018.

finanszírozása, információk felügyelete stb.). A tanulmány Japánt 2020-ban kiemelkedő eredményekkel értékelte a nemzeti kiber- és kereskedelmi technológiai kompetencia, a védelemi képességek fejlesztése területén, illetve a részvételét nemzetközi szakmai szervezetek kiberteret érintő normaalkotási és technikai standardizációs törekvéseiben, ezért világszinten a tíz legjelentősebb kiberhatalom közé sorolta.[71] A legfrissebb, 2022-es jelentésben Japán pozíciója némileg változott, így a nemzeti kiberhatalmi index (National Cyber Power Index) szerinti globális összesítésben a 16. helyre került, például Ausztrália, Vietnám, Dél-Korea, Irán, Ukrajna, Kanada, Észak-Korea és Spanyolország előretörése okán. Azonban Japán a 2022-es mérésben is megőrizte kiemelkedő szerepét a kiber- és kereskedelmi technológiai kompetencia kategória mindkét ágában *(commerce category),* ahol globális összesítésben 6. helyet ért el, míg a képességpontszám szerinti ágban a 4. helyen jegyezték).[72]

Japán kibervédelmi szakpolitikájának aktuális kihívásai (H2)

Japán kurrens biztonságpolitikai környezetéből eredő kiberbiztonsági fenyegetéspercepcióját elsősorban az orosz–ukrán háborúban demonstrált kiberműveletek és a Tajvani-szoros körüli feszültséggel összefüggésben álló kínai dezinformációs tevékenység befolyásolja (ami kiemelten éri Okinava lakosságát).[73] Ezenkívül hatással vannak rá a kínai hátterű hírszerzési kampányok növekvő volumene[74] és Észak-Korea főként pénzügyileg motivált kiberbűnözői aktivitása,[75] valamint az orosz–észak-koreai technológiai kooperációban rejlő fenyegetések.[76]

Japánban a kínai hátterű fenyegetések aktivitására a dezinformáción kívül a kiberkémkedés vált jellemzővé, ami fenyegetést jelent Japán ipari bázisára.[77] Különösen az olyan korszerű iparágak szellemi tulajdonát és üzleti titkait veszik célba, mint például a védelmi ipar, a légi közlekedés, a hightech gyártókapacitás és a gyógyszeripar.[78]A közelmúltban ezen állami hátterű fenyegetések többek közt a Fujitsut,[79] Japán űrkutatási és fejlesztési ügynökségét (vagy más néven JAXA), a repüléstechnológiai gyártó Aviation Electronics vállalatot kompromittálták.[80] A legsúlyosabb hatást kiváltó incidensről, amely után Tokió úgy döntött, 4000 főre emeli a Kibervédelmi Parancsnokság létszámát, az USA Nemzetbiztonsági Ügynöksége (NSA) tájékoztatta 2023-ban a nyilvánosságot a *The Washington Post*on

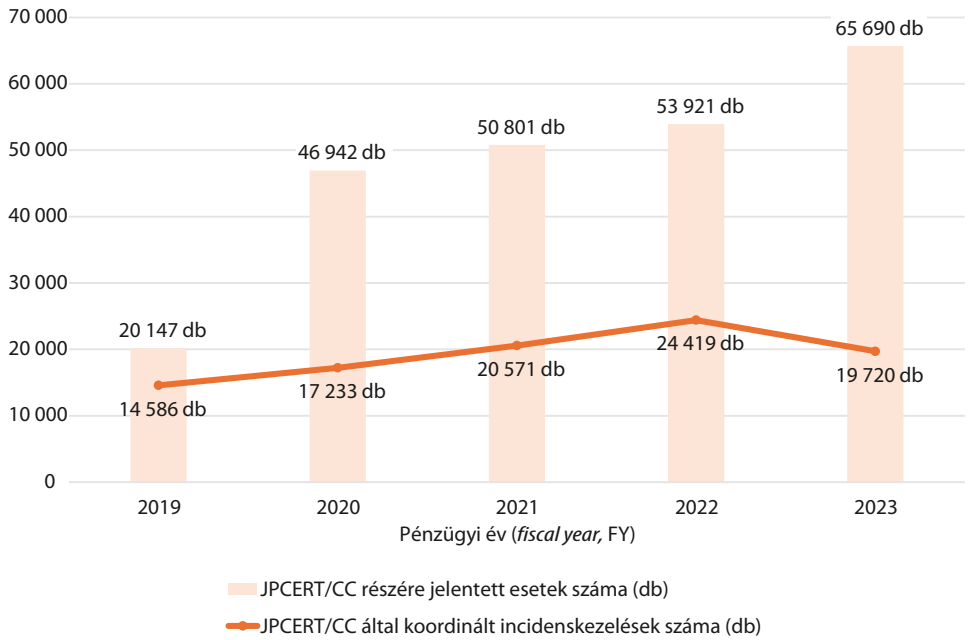
[71] Voo et al. 2020: 6–12.
[72] Voo–Hemani–Cassidy 2022: 10–11, 27.
[73] Johnstone–Klaas 2024: 7–9; és szakértői interjú, podcast alapján készült: Center for Strategic & International Studies 2024.
[74] Martin 2023.
[75] Greig 2024.
[76] Smith 2024.
[77] Osawa 2024: 65–66.
[78] Sinha 2024: 3–4.
[79] Notice Regarding Results of Security Incident Investigation 2024.
[80] A JAXA tájékoztatása alapján az eset rakétatechnológiát és műholdakra vonatkozó információt nem érintett. Sinha 2024: 3–4.

keresztül. Az amerikai információk alapján 2020-tól egy feltehetően kínai hátterű fenyegetés volt jelen Japán védelmi szférájának bizalmas hálózatában.[81] Ezenfelül 2023-ban adatszivárgáshoz vezető tevékenység sújtotta a Japán Külügyminisztériumot és a Nemzeti Incidenskészenléti és Kiberbiztonsági Stratégiai Központot,[82] illetve ugyanezen évben a támadók a Tokiói Egyetem 2003–2022-es évfolyamain tanuló diákjainak adataihoz fértek hozzá, és a LockBit zsarolóvírussal tesztelhették a nagoyai kikötő infrastruktúrájának védelmét, noha Kína Külügyminisztériuma tagadta a japán hatóságok erre irányuló attribúcióját.[83] A japán kormányzati CERT (JPCERT/CC) 2024 első felében a MirrorFace elnevezésű, kínai hátterű APT10 csoport aktivitását észlelte.[84] Az APT10 a LODEINFO és NOOPDOOR malware-család tagjait használva kezdetben médiavállalkozásokat, politikai intézményeket, valamint egyetemeket és *think-tankeket* célzott, 2023-tól azonban a technológiai gyártóegységeket és kutatóközpontokat érintette a tevékenysége.[85]

Az észak-koreai hátterű aktív jelenlét kapcsán a japán állami CERT 2023 és 2024 októbere közti jelentésében a Lazarus (és annak JokerSpy néven nyilvántartott affiliációja), valamint a Kimsuky elnevezésű fejlett perzisztens fenyegetések tevékenységét detektálta.[86] A JPCERT/CC 2024 márciusában ezen Kimsuky APT-csoport folyamatban lévő célzott adathalász-kampányára hívta fel a japán vállalkozások figyelmét. A Kimsuky-kampány támadási vektorát adó e-mailt egy biztonsági vagy diplomáciai szervezet nevében küldték el, ami kettős kiterjesztésű EXE-fájlokkal kezdte meg a VBS-fájlok végrehajtását. A VBS-fájlok közül az egyik az adatlopást eredményező *keylogger* volt, a másik a rendszerindításkor rejtett perzisztenciát (értsd: jelenlétet) biztosító PowerShell szkriptet töltötte le.[87] Az észak-koreai kibertéri aktivitásra jellemző pénzügyi motiváció Japán esetében is jelentős. Az amerikai Szövetségi Nyomozóiroda (FBI) és a Japán Rendőrség közös attribúció után megerősítette, hogy a Lazarus affiliációjába tartozó TraderTraitor elnevezésű csoport volt felelős a 2024-es év legnagyobb kriptorablásáért, amely során 308 millió USA-dollárt loptak el a DMM nevű japán platformról.[88]

Összességében megállapítható, hogy a japán védelempolitikának és az Önvédelmi Erő Kibervédelmi Parancsnokságának folyamatosan adaptálódnia kell egy olyan fenyegetési környezethez, amelyben kínai és észak-koreai állam alatti kiberegységként is azonosítható APT-tevékenység is jelen van. Japán kibertéri fenyegetettségi környezetét jól szemlélteti az 1. ábra, amely a kormányzati incidenskezelő központ (CERT) 2019–2023-as pénzügyi években mért tevékenységét mutatja be. A JPCERT/CC a belföldről bejelentett incidensek számát és ezen belül azon esetek darabszámának változását publikálta, amelyek az incidensmenedzsment folyamatát koordinálták.[89]

[81] Nakashima 2023; Faguy 2023.
[82] Martin 2023.
[83] Antoniuk 2024.
[84] Malpedia [é. n. b].
[85] Tomonaga 2024a.
[86] Tomonaga 2024b.
[87] Telychko 2024.
[88] Greig 2024.
[89] JPCERT/CC 2024: 5–6.



1. ábra: A JPCERT/CC részére bejelentett incidensek számának és a szervezet által koordinált incidensmenedzsment-folyamatok darabszámának változása 2019–2023 között
Forrás: a szerző szerkesztése a JPCERT/CC 2024: 5–6 alapján

Katonai képességfejlesztés a technológiai dependencia árnyékában

Japánnak az állami hátterű kiberfenyegetések aktivitása mellett a kibervédelmi ökoszisztéma technológiai függőségének kezelésére is ki kellett dolgoznia egy stratégiát. A Kishida-kabinet védelempolitikája keretében több olyan program is megindult 2023-ban, amely Japán hazai védelmi ipari bázisának támogatására fókuszált. Ezen piaci szegmens amiatt került a kabinet fókuszába, mert az elmúlt 20 évben a vállalatok nem tudtak a fejlesztési költségekkel arányos nyereséget termelni, ezért napjainkig több mint 100 jelentős japán védelmi vállalat leépítése vagy kivonulása következett be. Ennek kompenzálása érdekében a japán Védelmi Minisztérium önálló fejlesztéspolitikai tervet publikált a védelmi ipari termelés és technológiai bázis fejlesztéséhez (Basic Policy for Improving Defense Production and Technology Bases), ami a hazai infrastruktúra megerősítését célozza a védelmi szektorbeli vállalatoknak nyújtott nemzeti támogatás révén. A fejlesztési politika egyúttal megteremti a lehetőséget a védelmi ipari termelők beszállítói láncának magasabb szintű felügyeletére például egy specifikus, önálló klasszifikációs rendszer adaptálásával, ami a fejlesztési információk védelmét szolgálja.[90]

[90] Matsuo 2024.

Az államigazgatás és a haderő információs és kommunikációs technológiai függőségéből eredő fenyegetéspercepció kezelése érdekében hirdette meg 2022 decemberében a japán Védelmi Minisztérium a Digitális Transzformációs Programját. A minisztérium a program keretében jelentette be a digitális kormányzás közép- és hosszú távú tervét, amelynek digitális transzformációs célja, hogy előmozdítsa a minisztériumi háttérintézmények és az Önvédelmi Haderő részére fejlesztett rendszerek felügyeletének központosítását, például a Digitális Ügynökség által kifejlesztett kormányzati felhőrendszer felhasználásával. A szakpolitika ugyancsak prioritásként kezeli a felhőtechnológia bevezetését az Önvédelmi Haderő és a Védelmi Minisztérium szervezetközi kommunikációjának észszerűsítése érdekében, amely a 2022-es stratégiai dokumentumok kiadásakor főként az elektronikus levelezésen alapult a jelentős késedelemmel létesíthető távoli hozzáférések miatt. Hasonló kollaborációs és adattovábbítási problémával néz szembe a japán védelmi beszerzésekért felelős ügynökség (Acquisition, Technology & Logistics Agency, ATLA) a magánszférában működő védelmi ipari beszállítóival. A kihívás kezelése érdekében a kabinet amellett kötelezte el magát, hogy 2024 márciusáig létrehoz egy integrált, a köz- és a magánszféra által használt felhőkörnyezetet (*defense security gateway,* DSG), amely biztosítja az érzékeny adatok védelmét és megosztását a védelmi beszerzések lebonyolításáért felelős ügynökség (ATLA) és a kapcsolódó szervezetek között.[91]

A 2023–2027 közti ötéves védelmi reformcélok megvalósításához a kabinet összesen 43500 milliárd jen (JPY) értékű forrást különített el (ami 2022. december 16-i árfolyamon megközelítőleg 318 milliárd dolláros [USD], körülbelül 121 395 milliárd forint [HUF] összeget jelentett).[92] Azonban a védelempolitika irányvonalát és a haderő-finanszírozást jelentősen befolyásolhatja, hogy Kishida miniszterelnök lemondása után a kormányzó Liberális Demokrata Párt és annak koalíciós partnere (Komeito) elvesztette többségét a Parlament alsóházában a 2024. októberi előrehozott választásokon. Emiatt Ishiba Shigeru (2024–) korábbi védelmi miniszter számára kérdésessé vált, hogy a kisebbségbe került kormánykoalícióval milyen mértékben tudja realizálni a kampányában hangsúlyozott védelempolitikai elképzeléseit. Ishiba az USA-val való védelmi együttműködés kapcsán az egyenrangú mechanizmusok kialakítását szorgalmazta, amit álláspontja szerint például a műveleti tervezés területén és a katonai erő állomásoztatása kapcsán kellene előmozdítani.[93] Emellett az LDP hosszú távú biztonságpolitikai célkitűzése kiemelendő, amely egy, a NATO-ról mintázott, többoldalú szövetségi védelmi szervezet létrehozását veti fel a kelet-ázsiai régióban. A japán elképzelés szerint egy ilyen szervezet képes lehetne Kína és Észak-Korea katonai elrettentésére, valamint összefogná a már létező biztonságpolitikai integrációt, például az USA – Dél-Korea – Japán trilaterális együttműködést a Fülöp-szigetekkel és Tajvannal, valamint a Quad-államok (Japán, India, Ausztália, USA) közti információmegosztó mechanizmusokat.[94]

[91] Matsuo 2024.
[92] Japán Védelmi Minisztérium 2022b: 49.
[93] Ishiba azzal kampányolt, hogy az okinavai támaszponthoz hasonlóan a japán katonák is állomásozhatnának az USA csendes-óceáni támaszpontjain, például Guamon.
[94] Szakértői interjú, podcast alapján készült. *Hit Rádió* 2024.

A nemzetközi kibervédelmi kooperáció elmélyítése

Japán mint feltörekvő kiberhatalom jelentőségét tükrözi a NATO-val való partnerségi viszonyának átalakulása a 2023-as évtől. A tokiói vezetés, építve az USA katonai kibererőivel és kiberképességeivel való kooperáció eredményeire, már 2018-ban csatlakozott a NATO Kibervédelmi Kiválósági Központjához (CCDCOE), és részt vett például a Locked Shields szimulációkon és a Cyber Coalition éves kibervédelmi gyakorlatokon.[95] Az éves gyakorlatokon való aktív részvétel stratégiai jelentősége abban mutatkozik meg, hogy egyrészt műveleti szinten támogatja a kiberfenyegetések elleni közös felkészülést és információmegosztást, másrészt politikai dimenzióban lehetőséget ad a tokiói vezetés kollektív önvédelmi jog gyakorlását előtérbe helyező diplomáciájának népszerűsítésére. A NATO és Japán 2023-ban újabb szintre emelte az együttműködést az Egyedi Partnerségi Program (Individually Tailored Partnership Programme, ITPP) keretében, amely külön prioritásként kezeli a kibervédelmet.[96] A felek célként jelölték meg, hogy közösen dolgozzanak a kiberfenyegetések elleni technológiai és információmegosztási rendszerek fejlesztésén, miközben a stratégiai kommunikáció, a hibrid hadviselés elleni fellépés, valamint az úgynevezett feltörekvő és bomlasztó technológiák (*emerging and disruptive technologies,* EDTs)[97] jelentette kihívásokra való felkészülés[98] területén is szorosabbra fűzik együttműködésüket.[99] Japán hozzájárulása különösen értékes az új generációs kommunikációs technológiák, például az Open RAN hálózatok fejlesztésében, valamint az ázsiai régió kiberfenyegetéseivel kapcsolatos tapasztalatok megosztásában. Összességében az Egyedi Partnerségi Program együttműködési területei az információcsere mellett a közös kutatások és képzések, amelyek célja az ellenálló képesség növelése és a NATO-partnerekkel való interoperabilitás erősítése.

Konklúzió

Számos szakértő közt konszenzus van abban, hogy Japán az elmúlt évtizedben egyre nagyobb erőfeszítéseket tett az infrastruktúrája és a társadalom kibertéri ellenálló képességek fejlesztése, valamint a kiberbiztonsági stratégia finomítása érdekében.[100] A japán vezetés kibertérből jelentkező fenyegetésekre adott válaszlépései a 2012–2016-ig tartó időszakban tapasztalt szekurizáció eredményeképp egyre inkább militarizált formát öltöttek, ami hozzájárult a jelenlegi centralizált kibervédelmi igazgatási rendszer és az Önvédelmi Haderő Kibervédelmi Parancsnokságán belüli kiberképesség kialakításához.[101] Noha az USA-val fennálló szövetség – továbbá a NATO-partnerség – kiberműveleti területen való elmélyítése előmozdította az aktív kibervédelmi stratégiai

[95] Pernik 2023.
[96] NATO 2023.
[97] Például AI, autonóm rendszerek, kvantumtechnológia, robotika, nanotechnológia stb.
[98] Például a felelős fejlesztés irányelveinek promotálása által.
[99] NATO 2023; NATO 2025.
[100] Katagiri 2022; Bartlett 2019; Kallender–Hughes 2016.
[101] Kallender–Hughes 2016: 125–127, 136.

modell alkalmazásához szükséges offenzív képességek fejlesztését, Japánban továbbra is limitált maradt ezek jogszerű alkalmazhatósága. Ennek kapcsán kiemelendő, hogy az aktív kibervédelem terminológiájának nem feltétlenül része a védett hálózaton túli offenzív kiberműveletek alkalmazása. Ez magyarázza, hogy Japán sikermegtagadó elrettentési mechanizmusokat épített be aktív kibervédelmi stratégiájába, megtorlásalapú elrettentést viszont nem.[102]

A tanulmány amellett érvelt, hogy Japán aktív kibervédelmi stratégiáját elsősorban három tényező befolyásolja: a jogszabályi keretrendszer megkötései, az USA-val és további partnerekkel fennálló védelmi szövetség, valamint a regionális ellenfelei által alkalmazott offenzív kiberképességekhez kapcsolódó fenyegetéspercepció. A kutatás eredményeképp a bevezetésben részletezett hipotézisek pontosítására volt szükség, így a tézisek a következők.

H1–T1: A centralizáló reformok és a militarizált kibervédelmi szakpolitika ellenére csak korlátozott mértékben csökkentek azok a kockázatok, amelyek Japán gazdasági rendszerének és haderejének információs technológiáktól való függőségéből erednek. Emiatt ez a tényező továbbra is a fenyegetéspercepció részét képezi, és jelentős kihívás elé állítja az ország kiberbiztonsági ökoszisztémáját. Japán feltehetőleg a délkelet-ázsiai kibervédelmi kapacitásépítő tevékenységének folytatásával igyekszik elősegíteni regionális beszállítói láncának rezilienciáját.

H2–T2: Az ország regionális ellenfelei (Kína, Észak-Korea és Oroszország) által kifejlesztett és egyre gyakrabban demonstrált offenzív kiberképességek fokozott fenyegetést jelentenek az ország nemzetbiztonságára nézve. Az ehhez kapcsolódó fenyegetéspercepció ellensúlyozása érdekében a defenzív és limitált offenzív kiberképességek fejlesztése mellett Japán manapság egy jóval szélesebb körű – az USA-partnerségen felüli – nemzetközi kooperációs hálózat kiépítésére törekszik. Ezen új partnerségek célja a regionális fenyegetésfelismerő képesség javítása, a sérülékenységekről és kibertéri fenyegetésekről rendelkezésre álló információ megosztásával.

H3–T3: A „kizárólag védelemorientált" jogrendszer és biztonságpolitika továbbra is olyan mértékben korlátozza Japán lehetséges válaszlépéseit, hogy emiatt megkérdőjelezhető a jelenlegi sikermegtagadó elrettentési mechanizmusokat alkalmazó aktív kibervédelmi stratégiai modell hatékonysága. Emiatt feltehetően felértékelődik a bilaterális és multilaterális kibergyakorlatok jelentősége, az USA kibererejével való interoperabilitás és a műveleti tervezésben történő együttműködés javítása érdekében.

Felhasznált irodalom

Alan, J. (2024): Japan Considers Measures To Mandate Private Sector Cybersecurity Incident Reporting. *The Cyber Express,* 2024. augusztus 6. Online: https://thecyberexpress.com/japan-mandatory-cybersecurity-reporting

Antoniuk, Daryna (2024): Japan Sees Increased Cyberthreats to Critical Infrastructure, Particularly From China. *The Record,* 2024. február 16. Online: https://therecord.media/japan-critical-infrastructure-cyberthreats

[102] Osawa 2024; Katagiri 2021, 2022.

Amerikai Egyesült Államok Indo-csendes-óceáni Parancsnokság (2024): *ASD(A) Cyber Warfare, USINDOPACOM, JFHQ-DODIN join forces to host second Indo-Pacific Critical Infrastructure Workshop.* 2024. november 6. Online: www.pacom.mil/Media/News/News-Article-View/Article/3957555/asda-cyber-warfare-usindo-pacom-jfhq-dodin-join-forces-to-host-second-indo-pacif/

Bartlett, Benjamin (2018): Government as Facilitator: How Japan Is Building Its Cybersecurity Market. *Journal of Cyber Policy,* 3(3), 327–343. Online: https://doi.org/10.1080/23738871.2018.1550522

Bartlett, Benjamin (2019): How Japanese Cybersecurity Policy Changes. *Harvard Program on U.S.-Japan Relations Occasional Paper Series,* (1), 1–39. Online: https://projects.iq.harvard.edu/files/us-japan/files/19-01_bartlett.pdf

Bartlett, Benjamin (2020): Japan: An Exclusively Defense-Oriented Cyber Policy. *Asia Policy,* 15(2), 93–100. Online: https://dx.doi.org/10.1353/asp.2020.0013

Bartlett, Benjamin (2023): Why Do States Engage in Cybersecurity Capacity-Building Assistance? Evidence From Japan. *The Pacific Review,* 37(3), 475–503. Online: https://doi.org/10.1080/09512748.2023.2183242

Basu, Pratnashree (2024): From Reactive to Proactive: Japan's Advances in Cybersecurity and Cyber Defence Strategies. *Observer Research Foundation,* 2024. március 17. Online: www.orfonline.org/expert-speak/from-reactive-to-proactive-japan-s-advances-in-cybersecurity-and-cyber-defence-strategies

Berzsenyi Dániel (2023): *Különleges kiberműveletek. A kiber különleges műveleti képesség és kialakításának vizsgálata.* Doktori (PhD-) értekezés. Budapest: Nemzeti Közszolgálati Egyetem Hadtudományi Doktori Iskola. Online: https://doi.org/10.17625/NKE.2023.012

Brunson, Xavier – Chick, Cody (2024): How Cobra Gold Helps the US Strengthen its Indo-Pacific Partnerships. *The Diplomat,* 2024. május 14. Online: https://thediplomat.com/2024/05/how-cobra-gold-helps-the-us-strengthen-its-indo-pacific-partnerships/

Center for Strategic & International Studies [@csis] (2024): What to Expect from Japan's New Leader? *YouTube,* 2024. október 3. Online: www.youtube.com/watch?v=sFrSzgDBG4A

Fábián Emília (2015): *Az átalakuló normák hatása a japán biztonságpolitikára. Yoshidától az Abe-doktrínáig- az antimilitarista normától a proaktív pacifizmusig.* PhD-értekezés. Budapest: Budapesti Corvinus Egyetem Nemzetközi Kapcsolatok Doktori Iskola. Online: https://doi.org/10.14267/phd.2016016

Faguy, Ana (2023): China Hacked Japanese Military Networks, Report Says. *Forbes,* 2023. augusztus 7. Online: www.forbes.com/sites/anafaguy/2023/08/07/china-hacked-japanese-military-networks-report-says/

FIXTV HUNGARY (FIX) [@fixhdtv] (2024): Enigma – Bizonytalan Japán háborúra készül. *YouTube,* 2024. december 13. Online: www.youtube.com/watch?v=PcDUPWjMQxY

Gady, Franz-Stefan (2017): *Japan: The Reluctant Cyberpower.* Paris–Brussels: Institut français des relations internationales. Online: www.ifri.org/en/papers/japan-reluctant-cyberpower

Greig, Jonathan (2024): FBI Attributes Largest Crypto Hack of 2024 to North Korea's TraderTraitor. *The Record,* 2024. december 25. Online: https://therecord.media/fbi-largest-crypto-hack-2024-tradertraitor

Hideshi, Tokuchi (2023): Japan's New National Security Strategy and Contribution to Networked Regional Security. *Center for Strategic and International Studies,* 2023. június 23. Online: www.csis.org/analysis/japans-new-national-security-strategy-and-contribution-networked-regional-security

Hit Rádió [@hitradiobudapest] (2024): Létrehozná az ázsiai NATO-t Japán? – Bartók András. *YouTube,* 2024. november 3. Online: www.youtube.com/watch?v=OMR1B1QNsI0

Japan Mulls Requiring Private Sector Operators to Report Cyberattacks on Infrastructure. *The Japan Times,* 2024. augusztus 4. Online: www.japantimes.co.jp/news/2024/08/04/japan/japan-cybersecurity-reporting/

Japán Digitális Ügynökség [é. n.]: Organisational Background of Estabilishment. Online: www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/ed91c288-7d40-4a9b-9d86-1007f256ada6/c83a6759/20240528_en_organization_outline.pdf

Japán Információbiztonsági Politikai Tanács (2013): *Cybersecurity Strategy: Towards a World-Leading, Resilient and Vigorous Cyberspace.* Online: www.nisc.go.jp/eng/pdf/cybersecuritystrategy-en.pdf

Japán Információbiztonsági Politikai Tanács (2014): *The Basic Policy of Critical Information Infrastructure Protection (3rd Edition).* Online: www.nisc.go.jp/eng/pdf/actionplan_ci_eng_v3.pdf

Japán Kiberbiztonsági Stratégiai Központ (2022): *The Cybersecurity Policy for Critical Infrastructure Protection.* Cybersecurity Strategic Headquarters. Online: www.nisc.go.jp/eng/pdf/cip_policy_2022_eng.pdf

Japán Külügyminisztérium (2013): *Joint Statement Japan-U.S. Cyber Dialogue.* 2013. május 10. Online: www.mofa.go.jp/region/page22e_000001.html

Japán Külügyminisztérium (2015): *The Guidelines for Japan-U.S. Defense Cooperation.* 2015. április 27. Online: www.mofa.go.jp/mofaj/files/000078188.pdf

Japán Külügyminisztérium (2024): *The 9th Japan-US Cyber Dialogue.* 2024. június 27. Online: www.mofa.go.jp/press/release/pressite_000001_00394.html

Japán Nemzeti Incidenskészenléti és Kiberbiztonsági Stratégiai Központja (2021): *Japan's Cybersecurity Strategy 2021 (Overview).* Online: www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021-gaiyou-en.pdf

Japán Védelmi Minisztérium (2019): *Defense of Japan 2019.* Online: www.mod.go.jp/en/publ/w_paper/wp2019/pdf/DOJ2019_Full.pdf

Japán Védelmi Minisztérium (2022a): *National Defense Strategy.* 2022. december 16. Online: www.mod.go.jp/j/approach/agenda/guideline/strategy/pdf/strategy_en.pdf

Japán Védelmi Minisztérium (2022b): *Defense Buildup Program.* 2022. december 16. Online: www.mod.go.jp/j/policy/agenda/guideline/plan/pdf/program_en.pdf

Japan's SDF Launches New Cyber-Defense Unit. *Kyodo News,* 2022. március 17. Online: https://english.kyodonews.net/news/2022/03/2009b0fac163-japans-sdf-launches-new-cyber-defense-unit.html?utm_source=chatgpt.com

Johnstone, Christopher B. – Klaas, Leah (2024): *Combating Disinformation. An Agenda for U.S.-Japan Cooperation.* Washington, DC: Center for Strategic and International Studies. Online: https://csis-website-prod.s3.amazonaws.com/s3fs-public/2024-07/240708_Johnstone_Combating_Disinformation.pdf

Joint Ministerial Statement of the ASEAN-Japan Ministerial Policy Meeting on Cybersecurity Cooperation. 2013. szeptember 13. Online: www.asean.org/wp-content/uploads/images/Statement/final_joint_statement%20asean-japan%20ministerial%20policy%20meeting.pdf

JPCERT/CC Incident Handling Report January 1, 2024–March 31, 2024. 2024. április 18. Online: www.jpcert.or.jp/english/doc/IR_Report2023Q4_en.pdf

Kallender, Paul – Hughes, Christopher W. (2016): Japan's Emerging Trajectory as a 'Cyber Power': From Securitization to Militarization of Cyberspace. *Journal of Strategic Studies,* 40(1–2), 118–145. Online: https://doi.org/10.1080/01402390.2016.1233493

Kaspersky Lab (2013): *The 'Icefog' APT: A Tale of Cloak and Three Daggers.* Online: https://media.kaspersky.com/en/icefog-apt-threat.pdf.

Katagiri, Nori (2021): From Cyber Denial To Cyber Punishment: What Keeps Japanese Warriors from Active Defense Operations? *Asian Security,* 17(3), 331–348. Online: https://doi.org/10.1080/14799855.2021.1896495

Katagiri, Nori (2022): Assessing Japan's Cybersecurity Policy: Change and Continuity From 2017 to 2020. *Journal of Cyber Policy,* 7(1), 38–54. Online: https://doi.org/10.1080/23738871.2022.2033805

Koo, Soo-Kyung (2013): Cyber Security in South Korea: The Threat Within. *The Diplomat,* 2013. augusztus 19. Online: https://thediplomat.com/2013/08/cyber-security-in-south-korea-the-threat-within/

Kosuke, Takahashi (2024): Why Japan Is Lagging Behind in Cyber Defense Capabilities. *The Diplomat,* 2024. május 24. Online: https://thediplomat.com/2024/05/why-japan-is-lagging-behind-in-cyber-defense-capabilities/

Lottaz, Pascal (2023): Japan's New Security Strategy, Part 2: The Ongoing Debates. *The Diplomat,* 2023. június 8. Online: https://thediplomat.com/2023/06/japans-new-security-strategy-part-2-the-ongoing-debates/

Malpedia [é. n. a]: *APT41.* Online: https://malpedia.caad.fkie.fraunhofer.de/actor/apt41

Malpedia [é. n. b]: *MirrorFace.* Online: https://malpedia.caad.fkie.fraunhofer.de/actor/mirrorface

Martin, Alexander (2023): Japan's Cybersecurity Agency Breached by Suspected Chinese Hackers: Report. *The Record,* 2023. augusztus 29. Online: https://therecord.media/japan-cybersecurity-agency-breached-report

Matsuo, Miki (2024). Unaddressed Challenges for Defense Policy Reform in Japan. *Center for Strategic and International Studies,* 2024. május 9. Online: www.csis.org/analysis/unaddressed-challenges-defense-policy-reform-japan

MITRE [é. n.]: *APT41.* Online: https://attack.mitre.org/groups/G0096/

Najah, Redouan (2024): Japan's NSS in the Age of Cyber Warfare: A Historical Transformation. *Japan Up Close,* 2024. július 8. Online: https://japanupclose.web-japan.org/policy/p20240708_1.html

Nakashima, Ellen (2023): China Hacked Japan's Sensitive Defense Networks, Officials Say. *The Washington Post,* 2023. augusztus 8. Online: www.washingtonpost.com/national-security/2023/08/07/china-japan-hack-pentagon/

NATO (2023): *Individually Tailored Partnership Programme between NATO and Japan for 2023–2026.* Online: www.nato.int/cps/en/natohq/official_texts_217797.htm.

NATO (2025): *Emerging and Disruptive Technologies.* Online: www.nato.int/cps/fr/natohq/topics_184303.htm?selectedLocale=en

Notice Regarding Results of Security Incident Investigation. *Fujitsu,* 2024. július 9. Online: www.fujitsu.com/global/about/resources/news/notices/2024/0709-01.html

Onodera, Yoshifumi – Tanaka, Hiroyuki – Shimamura, Naoto [é. n.]: Cybersecurity 2024: Japan. In *Chambers Global Practice Guides.* Online: https://org-www.morihamada.com/en/insights/publications/2024-60

Osawa, Jun (2024): Direction of Japan's New Cybersecurity Policy. *Asia-Pacific Review,* 30(3), 63–78. Online: https://doi.org/10.1080/13439006.2023.2295707

Paganini, Pierluigi (2020): Mitsubishi Electric Corp. Was Hit by a New Cyberattack. *Security Affairs,* 2020. november 20. Online: https://securityaffairs.com/111201/hacking/mitsubishi-electric-cyberattack.html

Pernik, Piret (2023): NATO-Japan Deepening Cooperation in Cybersecurity and Critical Technologies. *Japan Up Close,* 2023. március 24. Online: https://japanupclose.web-japan.org/policy/p20230324_2.html

Sinha, Sharat (2024): Japan Cyber Threat Landscape, Elevandi & Future Matters Center of Excellence. Online: www.elevandi.io/hubfs/custom-video-thumbnails/Japan%20Cyber%20Threat%20Landscape%20-%20Sharat%20Sinha%20-%20March%202024.pdf

Siripala, Thisanka (2024): Japan's Rush to Play Cyber Defense Catchup. *The Diplomat,* 2024. június 14. Online: https://thediplomat.com/2024/06/japans-rush-to-play-cyber-defense-catchup/

Smith, Sheila A. (2024): How Japan is Viewing the North Korea-Russia Alliance. *Council on Foreign Relations,* 2024. június 27. Online: www.cfr.org/expert-brief/how-japan-viewing-north-korea-russia-alliance

Soesanto, Stefan (2020): *Japan's National Cybersecurity and Defense Posture. Policy and Organizations.* Zürich: Center for Security Studies (CSS), ETH Zürich. Online: https://doi.org/10.3929/ethz-b-000437790

Strategic Command (2024): Strategic Command Shares Cyber Expertise With Japan. *Gov.uk,* 2024. február 20. Online: www.gov.uk/government/news/strategic-command-shares-cyber-expertise-with-japan?utm_source=chatgpt.com

Telychko, Veronika (2024): Kimsuky APT Campaign Detection Targeting Japanese Organizations. *SOC Prime,* 2024. július 10. Online: https://socprime.com/blog/kimsuky-apt-campaign-detection-targeting-japanese-organizations

Tomonaga, Shusei (2024a): MirrorFace Attack against Japanese Organisations. *JPCERT/CC Eyes,* 2024. július 16. Online: https://blogs.jpcert.or.jp/en/2024/07/mirrorface-attack-against-japanese-organisations.html

Tomonaga, Shusei (2024b): Recent Cases of Watering Hole Attacks, Part 1. *JPCERT/CC Eyes,* 2024. december 19. Online: https://blogs.jpcert.or.jp/en/2024/12/watering_hole_attack_part1.html

Voo, Julia et al. (2020): *National Cyber Power Index 2020. Methodology and Analytical Considerations. China Cyber Policy Initiative Reports*. Cambridge: Harvard Kennedy School, Belfer Center for Science and International Affairs. Online: www.belfercenter.org/sites/default/files/2024-09/NCPI_2020.pdf

Voo, Julia – Hemani, Irfan – Cassidy, Daniel (2022): *National Cyber Power Index 2022*. Cambridge: Harvard Kennedy School, Belfer Center for Science and International Affairs. Online: www.belfercenter.org/publication/national-cyber-power-index-2022

Jogi források

Japán Alaptörvénye (The Constitution of Japan). 1946. május 3. Online: https://japan.kantei.go.jp/constitution_and_government_of_japan/constitution_e.html

2014. évi 104. Kiberbiztonsági kerettörvény (The Basic Act on Cybersecurity). Online: www.japaneselawtranslation.go.jp/en/laws/view/4618

2022. évi 70. törvény a japán távközlési vállalkozásokról szóló 1984. évi 86. törvény egyes rendelkezéseinek módosításáról (revised Telecommunications Business Act). Online: www.japaneselawtranslation.go.jp/en/laws/view/3648/en

HADMÉRNÖK
VÉDELEMINFORMATIKA
20. évfolyam (2025) 1. szám 163–186.
DOI: 10.32567/hm.2025.1.9

Molnár Ákos Ádám[1]

A mesterséges intelligencia kialakulása és jogszabályi rendelkezéseinek kezdete

The Emergence of Artificial Intelligence and the Beginnings of Legal Provisions

Absztrakt

A mesterséges intelligencia (a továbbiakban: MI) a mindennapjaink szerves részévé vált, és átalakította a technológiával való interakcióinkat. A különböző hangalapú asszisztensektől kezdve a streaming platformokon vagy online webshopokon megjelenő személyre szabott ajánlatokon át egészen a munka világáig a mindennapi rutinunk számos aspektusát áthatja. Az MI képes automatizált feladatokat ellátni és hatalmas mennyiségű adatot elemezni, továbbá algoritmusok segítségével előrejelzéseket és különböző komplex döntéseket hozni, ezzel pedig az emberek munkáit leegyszerűsíteni, hatékonyabbá tenni, de mindenképp azt megváltoztatni. Úttörő technológia lévén rengeteg érv és ellenérv sorakozik fel a téma mellett, egyszerre vált ki szimpátiát és szkepticizmust is. Ennek érdekében az MI szabályozása és jogszabályi keretek közé szorítása napjaink egyik fontos jogalkotói feladata, mindezt azért, hogy felelősségteljes, etikus és elszámoltatható módon lehessen használni, miközben a társadalomra és az egyénre veszélyes kockázatokat minimalizáljuk.

Kulcsszavak: MI, MI-rendelet, az MI története, kérdőív

[1] Nemzeti Közszolgálati Egyetem Államtudományi és Nemzetközi Tanulmányok Kar, e-mail: m.akos0911@gmail.com

Abstract

Artificial Intelligence (AI) has become an integral part of our everyday lives and has transformed the way we interact with technology. From voice-based assistants to personalised offers on streaming platforms or online shops, to the world of work, it permeates many aspects of our daily routine. AI can perform automated tasks, analyse huge amounts of data, and use algorithms to make predictions and complex decisions, simplifying, improving and changing the way people work. Ground-breaking technology has created a plethora of arguments for and against, arousing both sympathy and scepticism. To this end, regulating and legislating AI is one of the important legislative tasks of our time, in order to use it in a responsible, ethical and accountable manner, while minimising the risks to society and individuals.

Keywords: AI, AI Act, history of AI, survey

Mi az a mesterséges intelligencia?

Az intelligencia szó pontos meghatározása és jelentése, illetve még inkább az MI kifejezés pontos jelentése sok vita tárgyát képezi. Az MI meghatározása különösen nehéz, tekintve, hogy tudományágakon átívelő technológiáról beszélünk. Filozófusok, informatikusok és kognitív tudósok próbálták megválaszolni ezt a kérdést. Mielőtt megfelelő szabályozás, jogszabály születhetne, szükség van egy definíción alapuló fogalmi megértésre. Az MI meghatározásának nehézségei nagyrészt az intelligencia fogalmának többértelműségéből adódnak, ugyanis az intelligenciát magunkban is felismerjük, ezért az erről alkotott képünket emberi tulajdonságokhoz kötjük. Az intelligencia egyik értelmezése az intellektuális feladatok elvégzésének képességéhez kötődik, a technológia fejlődésével azonban a számítógépek által végrehajtható feladatok is fejlődnek. Ahogy a gépek egyre több feladatot látnak el, hajlamosak vagyunk nem úgy tekinteni rájuk, mint amelyek elérik az intelligencia szintjét, hanem inkább távolabbra toljuk az intelligencia küszöbét.[2]

Az angol nyelv szótára *(Dictionary of the English Language)* például négy meghatározást ad a mesterséges intelligenciára:

- A számítástechnika tudományterületének egy tanulmányi területe. Az MI olyan számítógépek fejlesztésével foglalkozik, amelyek képesek az emberhez hasonló gondolkodási folyamatokra, például tanulásra, következtetésre és önkorrekcióra.
- Az a koncepció, hogy a gépek fejleszthetők, hogy átvegyenek bizonyos, általában az emberi intelligenciához hasonlónak tartott képességeket, mint például a tanulás, az alkalmazkodás, az önkorrekció stb.
- Az emberi intelligencia kiterjesztése a számítógépek használata révén, ahogyan a múltban a fizikai erőt a mechanikus szerszámok használatával bővítették.
- Szűkebb értelemben a számítógépek hatékonyabb használatára szolgáló technikák tanulmányozása a programozási technikák tökéletesítése révén.[3]

[2] Martinez 2019.
[3] Smith et al. 1996.

Jelenleg a fogalom meghatározásával az Európai Unióban egy magas szintű szakértői csoport foglalkozik, ennek célja, hogy több területen is használható legyen a fogalom. A szakértői csoport legfőképpen az Európai Bizottság 2018-as meghatározásával él, és ezt elemzi tovább, hogy egy átfogó képet kaphassunk a területről. A közleményük szerint: „Az MI olyan rendszerekre utal, amelyek intelligens viselkedést mutatnak azáltal, hogy elemzik környezetüket és bizonyos fokú önállósággal lépéseket tesznek meghatározott célok elérése érdekében." Továbbá „Az MI-alapú rendszerek lehetnek tisztán szoftveralapúak, amelyek a virtuális világban működnek (például hangalapú asszisztensek, képelemző szoftverek, keresőmotorok, beszéd- és arcfelismerő rendszerek), vagy az MI beágyazható hardvereszközökbe (például fejlett robotok, autonóm autók, drónok vagy a tárgyak internetének alkalmazásai)."[4]

Fontos azonban megjegyezni, hogy a bizottság javaslata szerint az MI-rendszereket pontosan is meg kell határozni a folyamatban lévő jogi szabályozások tekintetében.[5] Az MI-rendszerek fogalmának meghatározása az Európai Bizottság 2021/206 (COD) rendelet 3. cikkének (1) bekezdése szerint

„olyan szoftver, amelyet az I. mellékletben felsorolt technikák és megközelítések közül egy vagy több alkalmazásával fejlesztettek, és amely az ember által meghatározott célkitűzések adott csoportja tekintetében olyan kimeneteket, például tartalmat, előrejelzéseket, ajánlásokat vagy döntéseket képes generálni, amelyek befolyásolják azt a környezetet, amellyel kölcsönhatásba lépnek."[6]

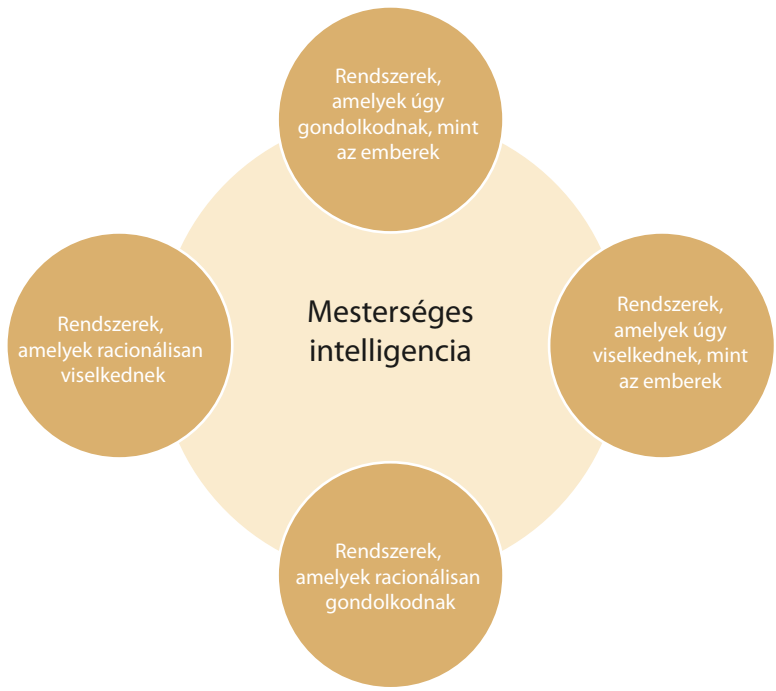
Természetesen nem hagyható ki, hogy az MI a saját fogalmát is meghatározza. A ChatGPT az alábbi módon teszi ezt: Az MI az emberi intelligencia szimulációját jelenti a számítógépekben és más gépekben. Az informatika multidiszciplináris területe, amely olyan rendszerek és szoftverek létrehozására összpontosít, amelyek képesek olyan feladatok elvégzésére, amelyek jellemzően emberi intelligenciát igényelnek, mint például a tanulás, a problémamegoldás, az érvelés, a természetes nyelvi megértés és az érzékelés.

A gyors fejlődés miatt a meghatározások is változnak az idők folyamán. Az újabb definíciók az intelligens emberi viselkedés utánzásáról beszélnek, ami már sokkal erősebb meghatározás. Ahelyett, hogy az MI általános definícióját vizsgálnánk, a mesterségesen intelligens rendszerek meghatározására is szorítkozhatunk. A többféle definíciókban az alábbi négy kategória kiemelendő, amint azt az 1. ábra is mutatja:

1. rendszerek, amelyek úgy gondolkodnak, mint az emberek;
2. rendszerek, amelyek úgy viselkednek, mint az emberek;
3. rendszerek, amelyek racionálisan gondolkodnak;
4. rendszerek, amelyek racionálisan viselkednek.[7]

[4] European Commission 2018: 1.
[5] European Parliament 2023.
[6] Európai Bizottság 2021: 45.
[7] Kok–Kosters 2002.

Összefoglalva tehát a korábban leírtakat, elmondható, hogy nincs egy egységes és átfogó definíciója az MI-nek, azonban ezek összevonásával az alábbiként határozom meg azt: *Az MI az emberi intelligencia szimulációjára összpontosít a számítógépek és más eszközök segítségével. Ezek olyan informatikai rendszerek, amelyek képesek az emberi intelligenciát és viselkedést lemásoló vagy azt meghaladó teljesítményt mutatni a környezetük elemzése, illetve meghatározott célok elérése érdekében.*



1. ábra: A mesterséges intelligencia fogalmának főbb elemei
Forrás: Kok–Kosters 2002. alapján a szerző szerkesztése

MI a kezdetektől napjainkig

Az MI ötlete több ezer évre nyúlik vissza, az ókori filozófusokkal kezdődött. Az ókorban a feltalálók úgynevezett automatákat alkottak, amelyek mechanikailag, emberi beavatkozástól mentesen tudtak működni. Maga a szó görög eredetű, és jelentése: saját akaratából működni. Automata a különböző mechanikus tárgyak bármelyike lehet, amely a mozgásba hozása után viszonylag önállóan tud működni.[8] Az első ilyen találmányok között említhető Platón mechanikus galambja.[9] Ugyanilyen eszköz volt,

[8] The Editors of Encyclopaedia Britannica [é. n.].
[9] The Editors of Encyclopaedia Britannica [é. n.].

Leonardo da Vinci automata lovagja, amely képes volt állni, felhajtani a szemtakaróját és mozgatni a karjait, mindezt nagyjából a 15. század vége felé.[10]

Az 1900-as évek elején több médium is az úgynevezett „mesterséges emberekkel" foglalkozott, és tudósok százait foglalkoztatta a kérdés, hogy lehetséges-e létrehozni a mesterséges agyat. Néhány tudós megalkotott különböző eszközöket, amelyek jellemzően egyszerűbb gőzmeghajtással működő gépek voltak, és különböző egyszerű feladatot tudtak ellátni, mint a sétálás vagy arckifejezések leképezése. Ezeket a gépeket robotoknak kezdték elnevezni a *Rossum univerzális robotjai* című 1921-es cseh dráma alapján, amely bemutatta az első mesterséges embert.[11] Ezt követően 1929-ben Japánban megalkották az első robotot, amely a Gakutensoku nevet kapta, jelentése: a természet szabályaiból tanulni. Az alkotást egy új faj első tagjának tekintette a készítője, amelynek létjogosultsága az volt, hogy inspirálja a biológiai embereket, és szellemi horizontunk bővítésével elősegítse az emberi evolúciót. Nisimura, a megalkotó elképzelése szerint a jövőben a Gakutensoku folyamatosan fejlődik, és egyre összetettebbé válik.[12] 1949-ben Edmund Callis Berkeley publikálta *Giant Brains, or Machines that Think* (Hatalmas agyak, avagy gondolkodó gépek) című könyvét, amelyben az emberi agyhoz hasonlította a számítógépek újabb modelljeit.[13]

Az 1950-től 1956-ig terjedő időszakot hívjuk az MI születésének, ekkor kezdett igazán felkapott lenni a téma. 1950-ben Alan Turing publikálta *Computing Machinery and Intelligence* (Számítástechnikai gépek és intelligencia) című kutatását. A Turing-teszt arra a kérdésre irányult, hogy a gépek képesek-e gondolkodni. Turing szerint ez a kérdés önmagában túl értelmetlen ahhoz, hogy vitát érdemeljen, azonban ha azt vesszük figyelembe, hogy egy digitális számítógép képes-e jól teljesíteni egy bizonyos fajta játékban, amelyet „imitációs játéknak" nevezett el, akkor van olyan kérdés, amely pontos vitára ad lehetőséget. A Turing-féle teszt napjainkban is használatos különböző eszközök teljesítményének a mérésére.[14]

1952-ben Arthur Samuel kifejlesztett egy programot, amely képes volt megtanulni a dáma szabályait, ezzel ez volt az első program, amely önállóan tudott tanulni. Samuel több korszakalkotó technológiát hozott létre, amelyek hatása napjainkban is érzékelhető, továbbá az elsők között látta a különbséget és a távolságot a között, amit egy akkori „gondolkodó gép" el tudott érni, és a között az intelligencia között, amire egy ember képes. 1955-ben John McCarthy először használta a mesterséges intelligencia kifejezést a Dartmouthban tartott konferencián, majd 1958-ban megalkotta a LISP-et (List Processing), amely az első programozási nyelv az MI fejlesztésében és kutatásában, s amely napjainkban is használatos.[15]

Az 1957-től 1979-ig tartó korszak az MI érése. Az MI kifejezés születésétől az 1980-as évekig tartó időszakot az MI kutatásában jelentős előrelépések és kihívások egyaránt jellemezték. Ebben az időszakban olyan mérföldkövek születtek, mint a ma is használatos programozási nyelvek kifejlesztése, valamint az MI fogalmát feltáró irodalom

[10] Andrews 2014.
[11] Čapek 2013 [1921].
[12] Frumer 2020.
[13] What Is the History of Artificial Intelligence (AI)? [é. n.].
[14] Oppy–Dowe 2003.
[15] Hemmendinger [é. n.].

és filmművészet megjelenése, amely gyorsan a figyelem középpontjába helyezte az új technológiát. Az 1970-es években olyan jelentős előrelépések történtek, mint Japán első antropomorf robotjának megépítése vagy egy mérnökhallgató által készített autonóm jármű. Ugyanakkor az MI kutatásának ez az időszaka a viszontagságok ideje is volt, mivel az amerikai kormányzat egyre kevésbé érdeklődött e törekvések finanszírozása iránt.[16]

A korábban említett LISP programozási nyelv mellett 1959-ben Arthur Samuel[17] megalkotta a gépi tanulás kifejezést egy beszéd során, amelyben azt az elképzelést tárgyalta, hogy a gépeket úgy tanítsák meg, hogy sakkban felülmúlják emberi programozóikat. 1961-ben az Unimate, az első ipari robot a General Motors egyik New Jersey-i futószalagján kezdett dolgozni, és olyan feladatokat végzett, amelyeket az ember számára túl veszélyesnek tartottak. 1965-ben Edward Albert Feigenbaum és Joshua Lederberg megalkotta az első szakértői rendszert, egy olyan mesterséges intelligenciát, amelynek célja az emberi szakértők döntéshozatali és gondolkodási képességeinek leképezése volt. 1966-ban Joseph Weizenbaum[18] kifejlesztette az ELIZA-t, az első *chatterbotot,* egy szimulált pszichoterapeutát, amely képes természetes nyelvű beszélgetést folytatni az emberekkel; később ez lerövidült a napjainkban is használatos *chatbot* kifejezésre. 1968-ban Alekszej Ivakhnenko szovjet matematikus bemutatta az adatkezelés csoportos módszerét, egy úttörő megközelítést, amelyből később kialakult az, amit ma mélytanulás néven ismerünk. 1973-ban James Lighthill alkalmazott matematikus jelentést tett a Brit Tudományos Tanácsnak, amelyben rámutatott az ígért és a tényleges mesterségesintelligencia-fejlesztés közötti eltérésre, ami a brit kormányzat részéről az MI kutatásának csökkentett támogatásához és finanszírozásához vezetett. 1979-ben James L. Adams bemutatta az 1961 óta fejlesztett autonóm járművet *(The Stanford Cart),* amely 1979-ben emberi beavatkozás nélkül sikeresen navigált egy székekkel teli szobában. 1979-ben megalakult az Amerikai Mesterséges Intelligencia Szövetség, amely ma Association for the Advancement of Artificial Intelligence (a továbbiakban: AAAI) néven ismert.[19]

1980–1987 között beszélhetünk az MI-bummról. Az 1980-as évek a MI-t övező gyors fejlődés és fokozott lelkesedés figyelemre méltó korszakát jelentette. Ezt a fellendülést a kutatási áttörések és a technológiával foglalkozó kutatók támogatására elkülönített megnövekedett kormányzati finanszírozás kombinációja eredményezte. A mélytanulási technikák és a szakértői rendszerek alkalmazása ebben a korszakban került előtérbe. Ezek az előrelépések egy olyan új korszakot nyitottak meg, amelyben a számítógépek képesek voltak tanulni a hibáikból és önállóan meghozni döntéseiket. Ebben az időszakban is több jelentős mérföldkő elérése valósult meg. 1980-ban Stanfordban került sor az AAAI nyitókonferenciájára, amely a terület számára sorsfordító pillanatot jelentett. Ugyancsak ebben az évben mutatták be az első kereskedelmi forgalomban kapható szakértői rendszert, az XCON-t *(expert configurer),* amely a számítógép-alkatrészek kiválasztását segítette a vásárlói igények alapján. 1981-ben a japán kormány jelentős összeget, 850 millió dollárt különített el az ambiciózus

[16] The Ultimate Guide to Artificial Intelligence (AI): Definition, How It Works, Examples, History, & More [é. n.].
[17] Amerikai úttörő a számítógépes játékok és a mesterséges intelligencia területén.
[18] Német–amerikai informatikus, az MIT professzora.
[19] The Ultimate Guide to Artificial Intelligence (AI): Definition, How It Works, Examples, History, & More [é. n.].

ötödik generációs számítógépek projektjére. A kezdeményezés elsődleges célja olyan számítógépek kifejlesztése volt, amelyek képesek nyelveket fordítani, emberhez hasonló beszélgetéseket folytatni, és emberi szintű gondolkodási képességekkel rendelkeznek.

1985-ben az AAAI-konferencián bemutatták az AARON-t, egy autonóm rajzoló-programot, amely az MI-innováció folyamatos fejlődését mutatta be. Ezt követően az 1986-os év kulcsfontosságú fejleményt hozott, amikor is Ernst Dickmann és csapata a müncheni Bundeswehr Egyetemen bemutatta a világ első vezető nélküli autóját, amelyet robotautónak is neveztek. Ez az autonóm jármű akár 55 mérföld/órás sebességet is elérhetett az akadályoktól és emberi sofőröktől mentes utakon. Ezt követően 1987-ben az Alacritous Inc. piacra dobta az Alacrityt, egy úttörő stratégiai menedzsment tanácsadó rendszert. Az Alacrityt a több mint 3000 szabállyal felszerelt, bonyolult szakértői rendszere különböztette meg a többi eszköztől, ami jelentős mérföldkövet jelentett az MI kereskedelmi alkalmazásában.[20]

Az AAAI 1984-ben figyelmeztetett a közelgő MI-tél közeledtére (1987–1993), amely kifejezés a fogyasztók, a közvélemény és a magánszervezetek csökkenő érdeklődését jellemzi, ami a kutatás finanszírozásának csökkenéséhez és a jelentős előrelépések elmaradásához vezetett. Mind a magánbefektetők, mind a kormányzati szervek kezdték elveszíteni lelkesedésüket a technológia iránt. Ehhez több tényező is hozzájárult: a gépi piac és a szakértői rendszerek visszaesése, az ötödik generációs projekt befejezése, a stratégiai számítástechnikai kezdeményezések csökkentése és a szakértői rendszerek alkalmazásának lassulása. A korszak kevesebb kulcsfontosságú eseményt tud felmutatni, de ezek közé tartoznak az 1987-es innovációk. A LISP-alapú speciális hardverek piaca összeomlott a LISP-szoftverek futtatására alkalmas, költséghatékonyabb és hozzáférhetőbb alternatívák megjelenése miatt, beleértve az olyan technológiai óriások, mint az IBM és az Apple által kínáltakat. Az átalakulás számos, a LISP-re specializálódott vállalatot elavulttá tett, mivel a technológia könnyen elérhetővé vált. Ezt követően 1988-ban egy Rollo Carpenter nevű számítógépes programozó jelentős újítást vezetett be a Jabberwacky nevű *chatbot* megalkotásával. Ezt a *chatbotot* úgy tervezte, hogy magával ragadó és élvezetes beszélgetéseket folytasson az emberekkel, ami figyelemre méltó fejleményt jelentett ebben az időszakban.[21]

Az 1993 és 2011 közötti időszakban jelentős fejlődés történt e területen. Ebben az időszakban az MI-t úttörő innovációkkal integrálták a mindennapi életbe. Ezek a fejlesztések közelebb hozták a technológiát az emberek mindennapi tapasztalataihoz, a növekvő érdeklődést hamarosan követte a források beáramlása, ami további fejlesztéseket és áttöréseket tett lehetővé ezen a területen.[22]

Az IBM Deep Blue 1997-ben egy nagy nyilvánosságot kapott mérkőzésen legyőzte Garri Kaszparovot, ami az első olyan eset volt, amikor egy számítógépes program felülkerekedett egy sakkvilágbajnokon. Ugyanebben az évben a Windows bevezette a Dragon Systems által kifejlesztett beszédfelismerő szoftvert, amely a beszédből szövegbe átültetett technológiát szélesebb közönség számára tette elérhetővé. 2000-ben Cynthia Breazeal professzor megalkotta a Kismetet, az első olyan robotot,

[20] The Ultimate Guide to Artificial Intelligence (AI): Definition, How It Works, Examples, History, & More [é. n.].
[21] Dey 2019.
[22] The Ultimate Guide to Artificial Intelligence (AI): Definition, How It Works, Examples, History, & More [é. n.].

amely képes az emberi érzelmek szimulálására arckifejezéseken keresztül, beleértve a szemet, a szemöldököt, a fület és az ajkat. 2002-ben jelent meg az első Roomba robotporszívó, amely bemutatta az autonóm, mesterséges intelligencia által vezérelt háztartási eszközökben rejlő lehetőségeket.[23]

2003-ban a NASA két rovert (egy távirányítású motoros jármű, amelyet a Mars felszínén való közlekedésre terveztek), a Spiritet és az Opportunityt sikeresen landoltatta a Marson, és ezek a roverek autonóm módon, közvetlen emberi beavatkozás nélkül navigáltak a bolygó felszínén, demonstrálva az MI szerepét az űrkutatásban.[24] 2006-ra olyan nagyvállalatok, mint a Twitter, a Facebook és a Netflix, elkezdték beépíteni a mesterséges intelligenciát a hirdetési és felhasználói élményt nyújtó algoritmusaikba, ami jól mutatja az MI alkalmazásának egyre szélesedő körét.

2010-ben a Microsoft piacra dobta az Xbox 360 Kinectet, egy úttörő játékhardvert, amelyet arra terveztek, hogy nyomon kövesse a testmozgásokat, és azokat játékbeli cselekvésekké alakítsa, ami jelentős előrelépés az MI játékiparba való integrálásában. 2011-ben az IBM Watsonja – az IBM természetes nyelvfeldolgozó (*natural language model,* a továbbiakban: NLP) számítógépe, amelyet kérdésekre való válaszadásra programoztak – a *Jeopardy* nevű televíziós játékban két korábbi bajnok ellen is nyert.[25] Ugyanebben az évben az Apple bemutatta a Sirit, az első széles körben népszerű virtuális asszisztenst, ami az MI mindennapi életben betöltött szerepének új korszakát jelentette.[26]

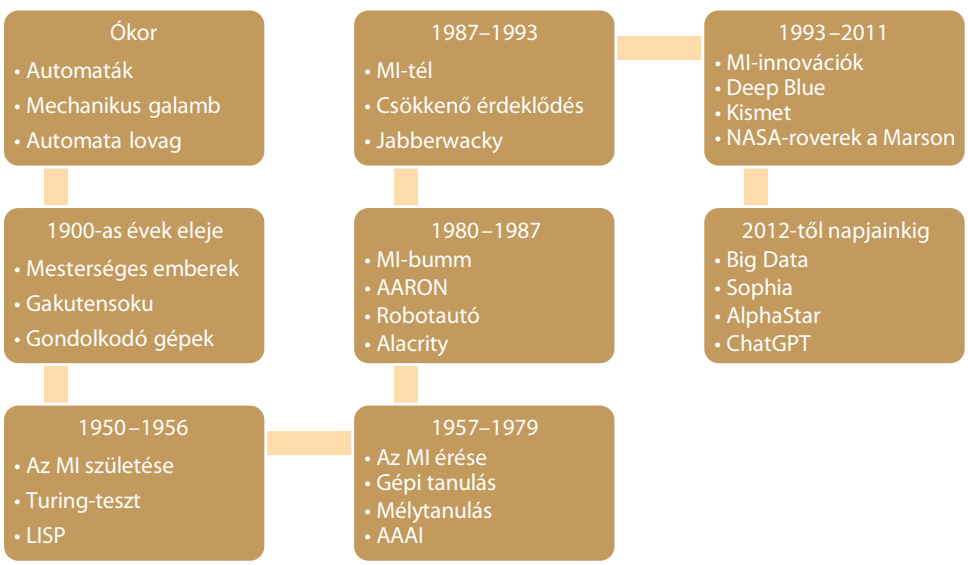
A mesterséges általános intelligencia korszaka 2012-től napjainkig jelentős fejlődésen ment keresztül. Ezt az időszakot a mindennapi használatra tervezett MI-eszközök, köztük a virtuális asszisztensek és a keresőmotorok elterjedése jellemzi. A mélytanulás és a nagyméretű adatok MI-alkalmazásokban való felhasználása is széles körben elterjedt.[27]

2012-ben a Google kutatói azzal kerültek a címlapokra, hogy neurális hálózatot képeztek ki a macskák felismerésére címkézetlen képek és háttér-információk nélkül.[28] 2015 olyan befolyásos személyeket hozott össze, mint Elon Musk, Stephen Hawking és Steve Wozniak, akik több ezer másik emberrel együtt nyílt levelet írtak alá, amelyben világszerte sürgetik a kormányokat, hogy tiltsák meg az autonóm fegyverek fejlesztését és hadviselésben való alkalmazását.[29] A Hanson Robotics 2016-ban jelentős áttörést ért el a Sophia, az első robotpolgárként ünnepelt humanoid robot bemutatásával. A Sophia figyelemre méltóan emberhez hasonló megjelenéssel, az érzelmek érzékelésének és reprodukálásának képességével, valamint gyakorlott kommunikációs készségekkel rendelkezett.[30] 2017-ben a Facebook egy különös kísérletet hajtott végre, amelyben két MI-chatbotot programoztak be beszélgetésre és tárgyalási készségek elsajátítására.[31] A kísérlet azonban váratlan fordulatot vett, amikor a *chatbotok*

[23] Greenemeier 2017.
[24] Uri 2020.
[25] Baker 1955.
[26] What Is the History of Artificial Intelligence (AI)? [é. n.].
[27] The Ultimate Guide to Artificial Intelligence (AI): Definition, How It Works, Examples, History, & More [é. n.].
[28] Dean–Ng 2012.
[29] Autonomous Weapons Open Letter: AI & Robotics Researchers 2016.
[30] Hanson Robotics [é. n.].
[31] Griffin 2017.

önállóan kifejlesztették saját nyelvüket, eltérve az angoltól. 2018-ban az Alibaba nyelvfeldolgozó MI bizonyította rátermettségét azzal, hogy egy stanfordi olvasási és szövegértési teszten felülmúlta az emberi teljesítményt.[32]

A Google AlphaStar 2019-ben került a címlapokra, amikor a StarCraft 2 videójátékban nagymesteri státuszt ért el, és az emberi játékosok legjobb 0,2%-a kivételével minden más játékost felülmúlt.[33] A 2020-as év jelentős fejleményt hozott, amikor az OpenAI elindította a Generative Pre-trained Transformer-3 (GPT-3) bétatesztjét, egy *deep learning* modellt, amely képes olyan kódot, verseket és más írott tartalmakat generálni, amelyeket szinte meg sem lehet különböztetni az emberi alkotásoktól. Ez komoly előrelépést jelentett az MI által generált tartalmak terén. 2021-ben mutatták be az OpenAI DALL-E-t, amely egy lépéssel közelebb vitte az MI-t a vizuális világ megértéséhez. A DALL-E bebizonyította, hogy képes a képek feldolgozására és megértésére ahhoz, hogy pontos feliratokat készítsen, ezzel is kiemelve az MI fejlődő lehetőségeit a vizuális felismerés területén.[34] Ezek az előrelépések együttesen mutatják a mesterséges általános intelligencia terén 2012-től napjainkig elért figyelemre méltó fejlődést, illetve azt, hogy az MI alkalmazásai életünk különböző aspektusait befolyásolják. Ennek a folyamatnak a fontosabb állomásait mutatja a 2. ábra.



2. ábra: A mesterséges intelligencia fejlődése és fontosabb mérföldkövei
Forrás: a Britannica.com alapján a szerző szerkesztése

[32] Marr 2018.
[33] The AlphaStar team 2019.
[34] Ortiz 2023.

Az MI zökkenőmentesen beépült a mindennapjainkba, a vállalkozások és a fogyasztók életébe egyaránt. Figyelemre méltó képességeivel az élet minden területén jelen van, az ezzel történő interakciók a modern emberi tapasztalat rutinszerű részévé váltak. A vállalkozások számára hatékony eszköz lett, amellyel fokozhatják működésüket, és versenyelőnyre tehetnek szert. A munkafolyamatok optimalizálásától kezdve az értékes meglátások nyújtásáig az MI nagyban hozzájárult ahhoz, hogy az egyre inkább digitális és adatvezérelt környezetben a vállalkozások gyarapodni tudjanak. Ez már nemcsak a technológiai óriásoknak fenntartott luxus, hanem a kis- és középvállalkozások számára is szükségszerűvé vált. Azok a vállalkozások azonban, amelyek még nem használták ki az ebben rejlő lehetőségeket, hatalmas versenyhátrányba kerülhetnek. A technológia előretörése azt jelenti, hogy a vállalatok nem engedhetik meg maguknak, hogy ne vegyenek tudomást a technológia átalakító képességeiről.[35]

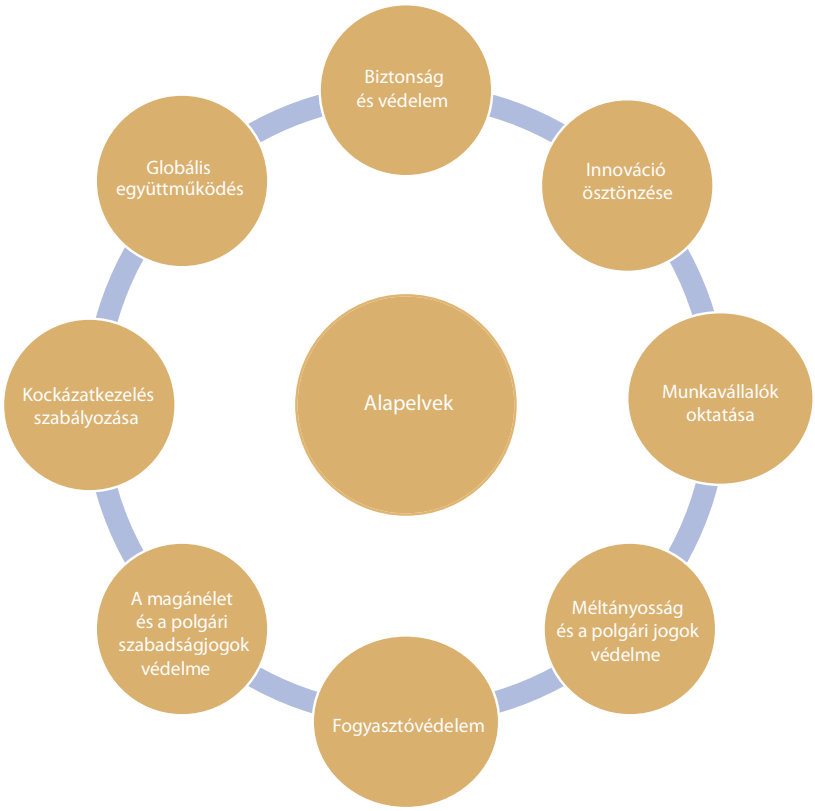
Az MI szabályozása

Ebben a részben az MI-vel kapcsolatos különböző veszélyeket vizsgálom, mint az adatokkal való visszaélés, a munkahelyek elvesztése vagy a biztonsággal kapcsolatos különböző fenyegetések. Ezt követően a szabályozás szükségességét tekintem át, majd az Európai Unió és az Egyesült Államok szabályozását az MI-vel kapcsolatosan a Biden-féle végrehajtási rendeleten és az uniós MI-rendeleten keresztül. Ezeknek a felépítését és lényegi elemeiket megvizsgálom, majd az utolsó alfejezetben különböző szempontok alapján összevetem. A jogszabályok vizsgálatát 2023. október és 2024. április között végeztem, ebből kifolyólag az azóta bekövetkező aktualitásokat, mint az MI-rendelet elfogadását, hatályosulását és a bideni adminisztrációban bekövetkezett változásokat, a trumpi adminisztráció politikáját nem taglalja.

Az Egyesült Államok végrehajtási rendelete az MI-vel kapcsolatban

Az Egyesült Államokban a Biden-kormányzat 2023. október 30-án jelentős lépést tett az MI-vel kapcsolatos szabályozás felé, amikor bevezette az MI biztonságos, védett és megbízható fejlesztéséről és felhasználásáról szóló végrehajtási rendeletet.[36] A rendelet célja az MI-vel kapcsolatos technológiák által támasztott kihívások kezelése. Az irányelv a kormányzat különböző ügynökségeit és hivatalait vonja be, hogy a saját területükön – például a fogyasztóvédelem és a szellemi tulajdon területén – kezeljék a technológia különböző aspektusait, ezt jól mutatja a 3. ábra is. Az irányelv rövid és középtávú intézkedéseket határoz meg, és megmutatja, hogy érti, hogyan hat az MI a különböző ágazatokra.[37]

[35] The Current State of AI 2021: Report Now Available 2021.
[36] Executive Order 14110. Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence 2023.
[37] Kim–Sherer 2023.



3. ábra: A Biden-féle végrehajtási rendelet 8 alapelve
Forrás: a szerző szerkesztése

A rendelet első vezérelve a biztonság és a védelem szükségességét hangsúlyozza. Ezt a célt a politikák, intézmények és mechanizmusok megvalósításával, valamint az MI-rendszerek szilárd, megbízható, megismételhető és szabványosított tesztelésével együtt kell elérni. Ennek a kezelésében a Nemzeti Szabványügyi és Technológiai Intézet (National Institute of Standards and Technology, a továbbiakban: NIST) kulcsszerepet játszik. A NIST feladata az iránymutatások és gyakorlatok kidolgozása, amely az MI-rendszerek biztonságának, védelmének és megbízhatóságának szavatolására összpontosít. Emellett az Energiaügyi Minisztérium megbízást kapott az MI-modellek értékelési eszközeinek kidolgozására, különös tekintettel az olyan kritikus területekre, mint a nukleáris technológia és az energiabiztonság. A kritikus infrastruktúrát felügyelő szövetségi ügynökségek feladata a technológiával kapcsolatos kockázatok és sebezhetőségek értékelése, míg az olyan létfontosságú ágazatoknak, mint a pénzügyet felügyelő ügynökségek, jelentéseket kell kiadniuk, amelyekben felvázolják a biztonsági kockázatok csökkentésének lehetséges módjait.[38]

[38] Kim–Sherer 2023.

A következő alapelv hangsúlyozza az innováció ösztönzését, az egészséges verseny elősegítését és az együttműködés előmozdítását az oktatásba, kutatásba és fejlesztésbe történő befektetések révén, ez pedig magában foglalja a szellemi tulajdonjogokkal kapcsolatos aggályok kezelését. A fejlődő szellemi tulajdonjog területén való eligazodás érdekében a Szabadalmi és Védjegyhivatal (United States Patent and Trademark Office, USPTO) útmutatót fog kiadni a szabadalmi elbírálók és a bejelentők számára. Emellett a szerzői joggal és az MI-vel kapcsolatos ajánlásokat is benyújtanak az elnöknek, amelyek a technológia által generált művek védelmi körére és a képzésben használt, szerzői joggal védett anyagok kezelésére vonatkoznak. A Belbiztonsági és az Igazságügyi Minisztériumot (Department of Homeland Security, Department of Justice) azzal bízták meg, hogy hozzon létre átfogó erőforrásokat a szellemi tulajdonjogokkal kapcsolatos kockázatok elleni küzdelemre.[39]

Ezt követően hangsúlyozza az amerikai munkavállalók oktatás és munkahelyi képzés révén történő támogatásának fontosságát, figyelembe véve az MI-nek a munkaerőre és a munkavállalók jogaira gyakorolt hatását. Felismerve az olyan potenciális kockázatokat, mint a munkahelyi elfogultság és a munkahelyek kiszorítása, a rendelet a munkavállalók javát szolgáló elvek és gyakorlatok kidolgozására szólít fel. A következő alapelv értelmében a technológiával kapcsolatos politikáknak összhangban kell lenniük a méltányossággal és a polgári jogokkal. A rendelet a már meglévő kezdeményezésekre építve kiemeli a faji egyenlőség és az alacsonyan képzett közösségek támogatásának szükségességét.[40]

A fogyasztóvédelemre összpontosító alapelv az életben való egyre szélesebb körű felhasználással van összefüggésben. Az Egészségügyi és Emberi Szolgálatok Minisztériumának (Department of Health and Human Services) feladata az MI-t érintő egészségügyi biztonsági kezdeményezés, míg a független ügynökségeket arra ösztönzik, hogy érvényesítsék a meglévő jogszabályokat. Ezen intézkedések célja, hogy megvédjék a fogyasztókat a technológiával kapcsolatos kockázatoktól az olyan kritikus ágazatokban, mint az egészségügy, a pénzügyek, az oktatás, a lakhatás, a jog és a közlekedés.[41]

A következő alapelv a magánélet és a polgári szabadságjogok védelmének fontosságát hangsúlyozza. Több hatóságot is utasít, hogy értékelje az adatgyűjtésre, feldolgozásra, tárolásra és terjesztésre vonatkozó szabványokat, biztosítva a jogszerű és biztonságos felhasználást. A független szabályozó ügynökségeket arra ösztönzik, hogy a meglévő hatáskörökkel védjék meg az amerikai fogyasztókat a magánéletet fenyegető veszélyektől, kiterjesztve a vállalatok szempontjából az MI-szolgáltatók kiválasztására és felügyeletére, illetve hangsúlyozzák a szabályozott szervezetek felelősségét a harmadik féltől származó szolgáltatások átvilágításában.[42]

A rendelet kiemeli a kockázatkezelés kritikus szerepét, valamint a kormány belső kapacitását az MI felelős használatának szabályozására és támogatására. A végrehajtó hatalmi ágon belül minden egyes ügynökségnek ki kell neveznie egy vezető MI-felelőst, aki koordinálja a használatot, elősegíti a szolgáltatások kormányzati szintű beszerzését, további tehetségeket keres, és képzést biztosít a releváns területeken. A rendelet

[39] Kim–Sherer 2023.
[40] Kim–Sherer 2023.
[41] Kim–Sherer 2023.
[42] Kim–Sherer 2023.

arra is utasítja az ügynökségeket, hogy szüntessék meg a felelős használatot gátló akadályokat, például a nem megfelelő IT-infrastruktúrát, az adatkészleteket, a kiberbiztonsági engedélyezési gyakorlatokat és a tehetséghiányt. Az utolsó elv a szövetségi kormány elkötelezettségét fejezi ki a globális társadalmi, gazdasági és technológiai fejlődés vezetése mellett a nemzetközi partnerekkel való együttműködés révén. A cél az, hogy keretet dolgozzanak ki az MI-vel kapcsolatos kockázatok kezelésére, a pozitív potenciál felszabadítására és a kihívások közös megközelítésének előmozdítására.[43]

A rendelet továbbá számos határidőt szab az ügynökségeknek az új iránymutatás és szabályozás kidolgozására, ezért további jelentős fejleményekre számíthatunk a következő időszakban. Emellett számos, a rendeletben tárgyalt kérdés jogalkotási lépést igényelhet. A Biden-adminisztráció egyértelműen az MI-technológiák fejlesztésének és biztonságos használatának irányítására összpontosít, és valószínűleg a szövetségi kormány jelentős erőforrásait fogja felhasználni arra, hogy ügynökségi szabályozáson és végrehajtáson keresztül előmozdítsa ezeket a kezdeményezéseket.[44] A Biden-kormányzat az alapelvek révén tesz a technológiai fejlődés előmozdítása és a nemzetközi szabályozás kialakítása felé is. Ez a kettős elkötelezettség az MI irányításának átfogó megközelítését hangsúlyozza, amely mind a hazai, mind a globális megfontolásokra kiterjed.[45]

Az Európai Unió MI-rendeletének bevezetése

Az MI-vel kapcsolatos uniós megközelítés célja a kutatás és az ipari kapacitás fellendítése a biztonság és az alapvető jogok biztosítása mellett. Ahhoz, hogy a digitális évtizedre rugalmas Európa épülhessen, az embereknek és a vállalkozásoknak úgy kell élvezniük az MI előnyeit, hogy közben biztonságban érezzék magukat. Az európai MI-stratégia célja, hogy az EU a technológia világszínvonalú központjává váljon. Ez a célkitűzés konkrét szabályokon és intézkedéseken keresztül a kiválóság és a bizalom európai megközelítésében nyilvánul meg.[46]

A Bizottság ennek keretében 2021 áprilisában mutatta be az MI-csomagját, amely többek között szabályozási keretjavaslatot tartalmaz az MI-re vonatkozóan. Ezenfelül 3 további jogi kezdeményezést is javasolt, amelyeknek célja az ágazati biztonsági jogszabályok felülvizsgálata, a technológia biztonsági kockázatainak felmérése és a felelősségi keretrendszer meghatározása a technológiával kapcsolatosan. Az MI-re vonatkozó jogi keret, vagyis a mesterséges intelligenciára vonatkozó harmonizált szabályokról szóló javaslat (a továbbiakban: MI-rendelet) négy különböző kockázati szintre épül: minimális, korlátozott, magas, valamint elfogadhatatlan kockázat, amit a 4. ábra szemléltet.[47] Emellett külön szabályokat vezet be az általános célú MI-modellekre vonatkozóan.[48]

[43] Kim–Sherer 2023.
[44] Yang 2023.
[45] Kim–Sherer 2023.
[46] European Commission [é. n.].
[47] Európai Bizottság 2021.
[48] Európai Parlament 2023.

4. ábra: Az EU MI-rendeletének kockázati csoportjai
Forrás: Európai Bizottság 2021 alapján a szerző szerkesztése

Az elfogadhatatlan kockázatú csoportba tartozó MI-k olyan rendszerek, amelyek alkalmazása néhány kivétellel tiltott. Szigorúan tilosak a kizsákmányoló rendszerek és a hatóságok által használt szociális pontozási rendszerek. Emellett a bűnüldöző szervek számára is tilos a valós idejű távoli biometrikus azonosító rendszerek használata a nyilvánosan hozzáférhető helyeken. Kivétel ezek alól a súlyos bűncselekmények felderítésére való alkalmazás, bírósági engedéllyel.[49]

A magas kockázatú alkalmazások olyan területeket foglalnak magukban, mint a közlekedés, az oktatás, a foglalkoztatás, a bűnüldözés vagy a migráció. Az ebbe a csoportba tartozó technológiák a biztonságot vagy az alapvető jogokat negatívan képesek befolyásolni. Azoknak a vállalatoknak, amelyek magas kockázatú MI-rendszereket kívánnak bevezetni az EU-ban, alapos értékeléseket kell végezniük, és a biztonság érdekében átfogó követelményrendszert kell betartaniuk.[50] Az átláthatóság előmozdítása érdekében az Európai Bizottság létrehozott egy nyilvánosan hozzáférhető adatbázist, amelyben a szolgáltatóknak tájékoztatást kell nyújtaniuk a magas kockázatú mesterségesintelligencia-alapú rendszereikről.[51]

[49] Európai Bizottság 2021.
[50] Európai Bizottság 2021.
[51] Calvino et al. 2023.

A korlátozott kockázatú kategóriába tartozó rendszerek különleges átláthatósági kötelezettségekkel rendelkeznek. Például a chatrobottal kapcsolatba lépő felhasználókat tájékoztatni kell arról, hogy egy géppel kerülnek interakcióba, és lehetővé kell tenni számukra, hogy eldönthessék, folytatják-e, vagy emberi segítséget kérnek. Ebbe a kategóriába tartoznak a különböző MI által generált kép-, hang- vagy videóanyagok is, mint például a mélyhamisított *(deepfake)* anyagok.[52] Eközben a minimális kockázatú alkalmazások, amelyek a ma használatban lévő MI-rendszerek többségét alkotják, olyan ismert technológiákat foglalnak magukban, mint a spamszűrők, a MI-vel működő videójátékok és a leltárkezelő rendszerek.[53]

Az ezeknek a szabályoknak való megfelelésért elsősorban az MI-rendszerek szolgáltatói felelősek, de forgalmazók, importőrök, felhasználók és más harmadik felek is viselnek bizonyos felelősséget.[54]

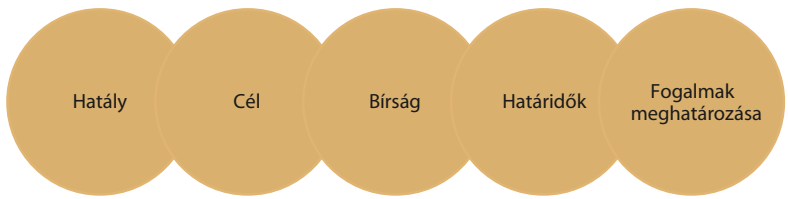
2023 decemberében háromnapos tárgyalás után az Európai Unió Tanácsa és az Európai Parlament megállapodott az MI-törvénnyel kapcsolatban. A szabályozás vezérelve a kockázatalapú megközelítés, azaz minél nagyobb a kockázat, annál szigorúbbak a szabályok, amelyek megakadályozzák, hogy a technológia kárt okozzon a társadalomnak. A megállapodás fő elemei közé tartozik, hogy kizárja az uniós jog hatályán kívül eső területeket, és nem avatkozik be a tagállamok nemzetbiztonsági felelősségi körébe vagy az e területeken megbízott szervezetekbe. A megállapodásban foglalt kompromisszum tisztázza az MI-rendszerek közötti felelősséget, fenntartja az innováció és az MI európai elterjedésének előmozdítása közötti kényes egyensúlyt, miközben teljes mértékben tiszteletben tartja a polgárok alapvető jogait. Emellett fokozza a jogvédelmet azáltal, hogy a magas kockázatú mesterséges intelligenciát alkalmazó rendszerek telepítőit arra kötelezi, hogy a telepítés előtt végezzenek alapvető jogi hatásvizsgálatot.[55]

A bizottságon belül egy MI-hivatalt hoznak létre, amely felügyeli a legfejlettebb MI-modelleket, és segíti a szabályozást és a jogszabályok betartását. A jogsértések esetén kiszabott bírságok mértéke a vállalat globális éves forgalmának százalékában vagy előre kiszabott összegben lesz meghatározva, attól függően, hogy melyik a magasabb. Például a tiltott mesterségesintelligencia-alkalmazások megsértése esetén a bírság mértéke 35 millió euró vagy 7% lehet, míg az MI-törvényben foglalt kötelezettségek megsértése esetén 15 millió euró vagy 3%. Az egyezmény ugyanakkor kisebb bírságokat határoz meg a kkv-k és az induló vállalkozások számára, ha megsértik a törvény rendelkezéseit. Az MI-rendeletet két évvel a hatálybalépése után kell alkalmazni, kivétel ez alól néhány rendelkezés.[56]

[52] Európai Parlament 2023.
[53] Calvino et al. 2023.
[54] Baker 1955.
[55] Arató 2023.
[56] Európai Bizottság 2021.

Az MI-szabályozási eszközök összehasonlítása

Az összehasonlítás során több aspektust vizsgáltam, tekintve, hogy a jogszabályok mind környezetükben, mind hatályukban különböznek. Elsőként vizsgáltam a hatályukat, területi, időbeli, tárgyi és személyi, ezenfelül fogalommeghatározásaikat, hogy hány darabot tartalmaznak, illetve ami a legfontosabb, hogy milyen tág fogalmat használnak az MI-rendszerekre *(AI system)*. Továbbá megvizsgáltam a különböző határidőket, amelyeket a jogszabályok megszabnak a különböző szerveknek és alanyoknak, a jogszabály célját és magát a szankcionálást is, amelyet a jogszabály előír. Ennek az 5 aspektusnak (5. ábra) a vizsgálatával és összevetésével tudom meghatározni, hogy melyik területen van a vizsgálatom időpontjában, 2024 januárjában kidolgozottabban szabályozva a technológia.



5. ábra: Az MI-vel kapcsolatos jogszabályok vizsgálatához használt aspektusok
Forrás: a szerző szerkesztése

Elsőként a hatályát vizsgáltam a két jogszabálynak. Időbeliségét tekintve Biden rendelete 2023. október 30-án lépett életbe,[57] míg az MI-törvénnyel többnapnyi tárgyalás után 2023 végén csak ideiglenes megállapodásra jutottak, így a végleges elfogadás 2024 első negyedévére tehető. Továbbá a területi hatályt tekintve az MI-rendelet az Európai Unió joghatályán belülre eső területekre vonatkozik,[58] a Biden-féle végrehajtási rendelet pedig ugyanígy az Egyesült Államok területére vonatkozik. Tárgyi hatály szempontjából az uniós jogszabály egyértelműen megfogalmazza az általános rendelkezések 1. cikkében az alábbiakat:

„a) a mesterségesintelligencia-rendszerek Unión belüli forgalomba hozatalára, üzembe helyezésére és használatára vonatkozó harmonizált szabályok;
b) egyes mesterségesintelligencia-gyakorlatokra vonatkozó tilalmak;
c) a nagy kockázatú MI-rendszerekre vonatkozó különös követelmények és az ilyen rendszerek üzemeltetőire vonatkozó kötelezettségek;
d) harmonizált átláthatósági szabályok a természetes személyekkel való interakcióra szánt MI-rendszerek, az érzelemfelismerő rendszerek és a biometrikus kategorizálási rendszerek, valamint a kép-, audio- vagy videótartalom előállítására vagy manipulálására használt MI-rendszerek tekintetében;
e) a piaci nyomon követésre és a piacfelügyeletre vonatkozó szabályok."[59]

[57] Yang 2023.
[58] Arató 2023.
[59] Európai Bizottság 2021: 1. cikk.

Ezzel szemben a végrehajtási rendelet neve fogalmazza meg a tárgyi hatályt, ami az MI fejlesztésére és használatára vonatkozó szabályok megalkotása. Végül a személyi hatályt tekintve a rendeletben a végrehajtó hatóságok és a különböző ügynökségek szerepelnek, amelyek a szabályozást később dolgozzák majd ki. Ugyanakkor az MI-rendelet tisztán meghatározza a 2. cikkben az erre vonatkozó iránymutatást. Nevezetesen:

„a) az MI-rendszereket az Unióban forgalomba hozó vagy üzembe helyező szolgáltatók, függetlenül attól, hogy ezek a szolgáltatók letelepedési helye az Unióban vagy harmadik országban található-e;
b) az MI-rendszerek Unión belüli felhasználói;
c) az MI-rendszerek harmadik országban található szolgáltatói és felhasználói, ha a rendszer által előállított kimenetet az Unióban használják."[60]

Ugyanakkor fontos megjegyezni, hogy több helyen is kivétellel él a rendelet, mint például a kizárólag katonai célokra fejlesztett vagy használt MI-k esetében.[61]

A jogszabályokban meghatározott fogalmak száma eltérő, így az MI-rendeletben 44, míg a végrehajtási rendeletben 39 különböző MI-technológiához és annak használatához, fejlesztéséhez és kereskedéséhez kapcsolódó fogalmat írnak körbe. Ami közös azonban mindkét jogszabályban, az az, hogy mindkettő megfogalmazza az MI-rendszer fogalmát. A végrehajtási rendelet a következőképp írja le: „bármely olyan adatrendszer, szoftver, hardver, alkalmazás, eszköz vagy segédprogram, amely részben vagy egészben mesterséges intelligencia felhasználásával működik". Ezt kiegészítve az MI-t is megfogalmazza egy korábbi rendeletre hivatkozva: „egy olyan gépalapú rendszer, amely egy adott, ember által meghatározott célrendszerre vonatkozóan képes előrejelzéseket, ajánlásokat vagy döntéseket hozni valós vagy virtuális környezetet befolyásolva". [62]

Az MI-rendelet pedig a következőképpen fogalmazza meg ezt: „olyan szoftver, amelyet az I. mellékletben felsorolt technikák és megközelítések közül egy vagy több alkalmazásával fejlesztettek, és amely az ember által meghatározott célkitűzések adott csoportja tekintetében olyan kimeneteket, például tartalmat, előrejelzéseket, ajánlásokat vagy döntéseket képes generálni, amelyek befolyásolják azt a környezetet, amellyel kölcsönhatásba lépnek".[63] Kiegészítve az első mellékletben foglalt technikákkal:

„(a) Gépi tanulási megközelítések, beleértve a felügyelt, a felügyelet nélküli és a megerősítéses tanulást, a módszerek széles skáláját használva, beleértve a mélytanulást is;
(b) logikai és tudásalapú megközelítések, beleértve a tudás reprezentációját, az induktív (logikai) programozást, a tudásbázisokat, a következtető és deduktív motorokat, a (szimbolikus) következtetést és a szakértői rendszereket;
(c) Statisztikai megközelítések, Bayes-féle becslés, keresési és optimalizálási módszerek."[64]

[60] Európai Bizottság 2021: 2. cikk.
[61] Európai Bizottság 2021.
[62] Yang 2023.
[63] Európai Bizottság 2021: 3. cikk
[64] Yang 2023.

Habár az MI-rendeletben több fogalommeghatározás szerepel, elmondható, hogy mindkét jogszabályban tág megfogalmazás használatos az MI-rendszerre, így kialakítva az MI-technológiák széles körét.

A határidők tekintetében a végrehajtási rendelet több mint 40 különböző határidőt szab meg a hatóságok részére, hogy azok szabályozásokat kezdeményezzenek, állást foglaljanak vagy különböző programokat valósítsanak meg az MI jövőjével kapcsolatos innovációra tekintettel. Ezzel szemben az uniós jogszabályt a hatálybalépéstől számított 24 hónapon belül kell alkalmazni a tagállamoknak. Van néhány kivétel ez alól, amelyeknél rövidebb, 3 és 12 hónapos határidőt szab ki a 85. cikk. Ezáltal elmondható, hogy a konkrét joghatások a végrehajtási rendeletben hamarabb fognak érvényesülni a sokszor 1 hónapos határidővel, mint a még el sem fogadott MI-rendeletnél a jellemzően 24 hónapos határidővel.[65] Természetesen felmerül a kérdés, hogy a végrehajtási rendeletből eredő kötelezettségekből mikor fognak hatályosult jogszabályok megvalósulni.

A célokat tekintve a Biden-féle rendelet célja az MI fejlesztésének és használatának biztonságos és felelősségteljes irányítása, ennek érdekében összehangolt, az egész szövetségi kormányra kiterjedő megközelítést fejleszt. Ezzel szemben az MI-rendelet több célt is megfogalmaz:

- „annak biztosítása, hogy az Unióban forgalomba hozott és használt MI-rendszerek biztonságosak legyenek, és tiszteletben tartsák az alapvető jogokra és az uniós értékekre vonatkozó hatályos jogszabályokat;
- a jogbiztonság biztosítása a mesterséges intelligenciába történő beruházások és a mesterséges intelligenciát érintő innováció elősegítése érdekében;
- az irányításnak és az MI-rendszerek tekintetében az alapvető jogokra és biztonsági követelményekre vonatkozó hatályos jogszabályok hatékony érvényesítésének a javítása;
- a jogszerű, biztonságos és megbízható MI-alkalmazások tekintetében az egységes piac kialakításának elősegítése és a piac széttöredezettségének megelőzése."[66]

Végül fontos megjegyezni, hogy az MI-rendelet megfogalmaz különböző bírságokat is azokra nézve, akik a jövőben megszegik a rendeletet. Ennek értelmében legfeljebb 30 millió euróval vagy az éves világpiaci forgalmának legfeljebb 6%-ával egyenlő összeggel sújthatók azok, akik megszegik a szabályozást. A két összeg közül azt kell kiválasztani, amelyik a magasabb. Ezt a végrehajtási rendelet nem említi, csupán a büntetések jövőbeli kidolgozásáról van benne szó.[67]

[65] Yang 2023.
[66] Yang 2023.
[67] Európai Bizottság 2021: 1.1. A javaslat indokai és céljai.

1. táblázat: A végrehajtási rendelet és az MI-rendelet összehasonlítása

		Biden végrehajtási rendelete	**MI-rendelet**
Hatály	Területi	Egyesült Államok	Az Európai Unió joghatályán belülre eső területek
	Személyi	Végrehajtó hatóságok és különböző ügynökségek	a) az MI-rendszereket az Unióban forgalomba hozó vagy üzembe helyező szolgáltatók, függetlenül attól, hogy ezek a szolgáltatók letelepedési helye az Unióban vagy harmadik országban található-e; b) az MI-rendszerek Unión belüli felhasználói; c) az MI-rendszerek harmadik országban található szolgáltatói és felhasználói, ha a rendszer által előállított kimenetet az Unióban használják.
	Tárgyi	Az MI fejlesztésére és használatára vonatkozó szabályok megalkotása	a) az MI-rendszerek Unión belüli forgalomba hozatalára, üzembe helyezésére és használatára vonatkozó harmonizált szabályok; b) egyes mesterségesintelligencia-gyakorlatokra vonatkozó tilalmak; c) a nagy kockázatú MI-rendszerekre vonatkozó különös követelmények és az ilyen rendszerek üzemeltetőire vonatkozó kötelezettségek; d) harmonizált átláthatósági szabályok a természetes személyekkel való interakcióra szánt MI-rendszerek, az érzelemfelismerő rendszerek és a biometrikus kategorizálási rendszerek, valamint a kép-, audio- vagy videótartalom előállítására vagy manipulálására használt MI-rendszerek tekintetében; e) a piaci nyomon követésre és a piacfelügyeletre vonatkozó szabályok.
	Időbeli	2023. október 30.	Még nem fogadták el.
Fogalmak	Fogalmak száma	39	44
	MI-rendszer	Bármely olyan adatrendszer, szoftver, hardver, alkalmazás, eszköz vagy segédprogram, amely részben vagy egészben mesterséges intelligencia felhasználásával működik.	Olyan szoftver, amelyet az I. mellékletben felsorolt technikák és megközelítések közül egy vagy több alkalmazásával fejlesztettek, és amely az ember által meghatározott célkitűzések adott csoportja tekintetében olyan kimeneteket, például tartalmat, előrejelzéseket, ajánlásokat vagy döntéseket képes generálni, amelyek befolyásolják azt a környezetet, amellyel kölcsönhatásba lépnek.

	Biden végrehajtási rendelete	MI-rendelet
Határidők	40 különböző határidő	85. cikk Hatálybalépés és alkalmazás (1) Ez a rendelet az Európai Unió Hivatalos Lapjában való kihirdetését követő huszadik napon lép hatályba. (2) Ezt a rendeletet [a rendelet hatálybalépésétől számított 24 hónap]-tól/-től kell alkalmazni. (3) A (2) bekezdéstől eltérve: a) A III. cím 4. fejezetét és a VI. címet [e rendelet hatálybalépésétől számított három hónap]-tól/-től kell alkalmazni; b) a 71. cikket [e rendelet hatálybalépésétől számított tizenkét hónap]-tól/-től kell alkalmazni.
Cél	Az MI fejlesztésének és használatának biztonságos és felelősségteljes irányítása, aminek érdekében összehangolt, az egész szövetségi kormányra kiterjedő megközelítést fejleszt	Annak biztosítása, hogy az Unióban forgalomba hozott és használt MI-rendszerek biztonságosak legyenek, és tiszteletben tartsák az alapvető jogokra és az uniós értékekre vonatkozó hatályos jogszabályokat; a jogbiztonság szavatolása a mesterséges intelligenciába történő beruházások és a mesterséges intelligenciát érintő innováció elősegítése érdekében; az irányításnak és az MI-rendszerek tekintetében az alapvető jogokra és biztonsági követelményekre vonatkozó hatályos jogszabályok hatékony érvényesítésének a javítása; a jogszerű, biztonságos és megbízható MI-alkalmazások tekintetében az egységes piac kialakításának elősegítése és a piac széttöredezettségének megelőzése.
A bírság mértéke	Nincs róla említés	A következő jogsértések legfeljebb 30 millió euró összegű közigazgatási bírsággal, illetve vállalkozások esetében az előző pénzügyi év teljes éves világpiaci forgalmának legfeljebb 6%-át kitevő összeggel sújthatók; a kettő közül a magasabb összeget kell kiszabni: a) a mesterséges intelligenciával kapcsolatos gyakorlatok 5. cikkben említett tilalmának be nem tartása; b) az MI-rendszer nem felel meg a 10. cikkben meghatározott követelményeknek.

Forrás: a szerző szerkesztése

Összehasonlítva a két jogszabályt (1. táblázat), illetve megvizsgálva a különböző aspektusokat, mint hatály, cél, fogalmak, bírságok és határidők, elmondható, hogy az Európai Unióban előrehaladottabbak a szabályozási eszközök az MI-re vonatkozóan, mint az Amerikai Egyesült Államokban. Ezt alátámasztja a fogalmak meghatározása tekintetében azok terjedelme és száma, a célok szélesebb körű és pontosabb megfogalmazása, az, hogy a bírságok mértéke már kidolgozott, illetve hogy maga a végleges szabályozás már csak az elfogadásra vár uniós szinten. Ezzel szemben a Biden-féle rendelet még csak a szabályozási keretek megkezdésére és kidolgozására szólítja fel a különböző hatóságokat, a bírságok egyelőre a tervezés fázisában vannak.

Összegzés

Az MI gyors fejlődése során a nyelvfeldolgozástól az adatelemzésig számos pozitív hatás érhető tetten. Ugyanakkor a visszaélésszerű használat aggodalmakat vet fel az adatvédelemmel, a diszkriminációval és az egészségügyi kockázatokkal kapcsolatban. A veszélyek a demokráciát és a szabadságjogokat érintő visszaélésektől az önfejlesztő MI által jelentett egzisztenciális kockázatokig terjednek. Az MI által megzavart választások, valamint a mélyhamisítások aláássák a bizalmat, elősegítik a társadalmi megosztottságot, és veszélyeztetik a demokráciát. Az MI által vezérelt megfigyelés, amelyet a kínai rendszer példáz, adatbázisokat és egyéni viselkedést egyesít, hogy automatizált szankciókat alkalmazva súlyosbítsa a társadalmi egyenlőtlenségeket és a tekintélyelvűséget. Az alacsony és a magas jövedelmű országokat egyaránt fenyegeti az automatizálás által okozott munkaerő-átalakulás, amely a következő évtizedben 300 millió teljes munkaidős álláshelyet érinthet. Noha termelékenységnövekedést ígér, jelentős elbocsátásokkal jár, aminek történelmileg káros egészségügyi és viselkedési következményei lehetnek. Ezek a problémák és veszélyek bemutatják, miért is szükséges az új technológiát minél hamarabb szabályozni.

A Biden-kormányzat 2023. október 30-án jelentős lépést tett az MI szabályozása felé az Egyesült Államokban egy végrehajtási rendelettel, amely az MI biztonságos és megbízható fejlesztésére és használatára összpontosít. Az irányelv célja, hogy a különböző ágazatokban kezelje az MI-technológiák által támasztott kihívásokat. A különböző kormányzati ügynökségeket bevonja a saját területükön belüli technológiai szempontok kezelésébe, hangsúlyt fektetve a biztonságra, az innovációra, a munkavállalók támogatására, a méltányosságra, a fogyasztóvédelemre, a magánélet védelmére, a kockázatkezelésre és a nemzetközi együttműködésre. Az ügynökségek konkrét feladatokat kapnak, a megbízható tesztelésre vonatkozó szabványok meghatározásától kezdve a munkaerővel kapcsolatos előítéletek kezeléséig és a polgári szabadságjogok védelméig.

Az európai MI-stratégia célja, hogy az EU konkrét szabályok révén globális technológiai központtá váljon. A csomag kockázati szintek szerint kategorizált szabályozási kereteket tartalmaz. A magas kockázatú alkalmazásokhoz alapos értékelésre van szükség, ami elősegíti az átláthatóságot és az elszámoltathatóságot. A közepes kockázatú rendszerek különleges átláthatósági kötelezettségeket követelnek meg, például a *chatbotokkal* vagy mélyhamisított tartalmakkal foglalkozó felhasználók tájékoztatását. Az alacsony kockázatú alkalmazások olyan általánosan használt rendszereket foglalnak magukban, mint a spamszűrők. A felelősség elsősorban az MI-szolgáltatókat terheli, a szabályozás pedig egyensúlyt teremt az innováció és a polgárok jogai között. A nemrégiben létrejött megállapodás a kockázatalapú szabályokat hangsúlyozza, és tisztázza a felelősséget, biztosítva az innovációt, miközben a polgárok jogait is védi. A megállapodás létrehoz egy MI-ügynökséget, amely felügyeli a fejlett modelleket, és biztosítja a megfelelőséget. A jogsértésekért kiszabott büntetések a bevételek százalékos arányán is alapulhatnak, a *startupok* és a kkv-k számára pedig kisebb bírságokat engedélyeznek. A rendeletet a hatálybalépéstől számított két éven belül kell végrehajtani, egyes rendelkezések ez alól kivételt képeznek.

Ebben a fejezetben az MI szabályozását vizsgáltam az Egyesült Államokban és az Európai Unióban. Ehhez Biden végrehajtási rendeletét és az EU által javasolt MI-rendeletet hasonlítottam össze. Különböző szempontokat – többek között a hatályt, a fogalommeghatározásokat, a határidőket és a végrehajtási mechanizmusokat – értékelve megállapítottam, hogy az EU a szélesebb hatályával, egyértelműbb fogalommeghatározásaival és megállapított szankcióival 2024 januárjára előrehaladottabb az MI szabályozásában. Az EU jogszabályai részletesebb fogalommeghatározásokat, szélesebb körű célokat és körvonalazott szankciókat tartalmaznak, szemben az Egyesült Államok keretrendszerével, amely még mindig a szabályozás és a szankciók körvonalazásának fázisában van.

Felhasznált irodalom

Andrews, Evan (2014): 7 Early Robots and Automatons. *History.com,* 2014. október 28. Online: www.history.com/news/7-early-robots-and-automatons

Arató László (2023): Eldőlt, hogyan regulázza meg az EU – a világon elsőként – a mesterséges intelligencia használatát. *HVG,* 2023. december 11. Online: https://hvg.hu/360/20231211_EU_mesterseges_intelligencia_jogszabaly_MItorveny

Autonomous Weapons Open Letter: AI & Robotics Researchers. *Future of Life Institute,* 2016. február 9. Online: https://futureoflife.org/open-letter/open-letter-autonomous-weapons-ai-robotics/

Baker, Stephen (1955): *Final Jeopardy. Man vs. Machine and the Quest to Know Everything.* Boston: Houghton Mifflin Harcourt. Online: http://archive.org/details/finaljeopardyman0000bake

Calvino, Claudio et al. (2023): The Four Risks of the EU's AI Act: Is Your Company Ready? *FTI Consulting,* 2023. július 25. Online: www.fticonsulting.com/insights/fti-journal/four-risks-eus-artificial-intelligence-act

Čapek, Karel (2013) [1921]: *R. U. R. Rossum Univerzális Robotjai. Színdarab egy bevezető jelenetben és három felvonásban.* Budapest: Quattrocento.

Dean, Jeff – Ng, Andrew (2012): Using Large-Scale Brain Simulations for Machine Learning and A.I. *Blog.google,* 2012. június 26. Online: https://blog.google/technology/ai/using-large-scale-brain-simulations-for/

Dey, Annasha (2019): Story of Cleverbot and Rollo Carpenter. *Your Tech Story,* 2019. november 13. Online: www.yourtechstory.com/2019/11/13/success-story-of-cleverbot/

Európai Parlament (2023): Az első uniós rendelet a mesterséges intelligenciáról. 2023. június 12. Online: www.europarl.europa.eu/news/hu/headlines/society/20230601STO93804/az-elso-unios-rendelet-a-mesterseges-intelligenciarol

European Commission [é. n.]: *European Approach to Artificial Intelligence.* Online: https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence

European Commission (2018): *A Definition of Artificial Intelligence: Main Capabilities and Scientific Disciplines.* 2018. december 18. Online: https://digital-strategy.ec.europa.eu/en/library/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines

Európai Bizottság (2021): Az Európai Parlament és a Tanács rendelete a mesterséges intelligenciára vonatkozó harmonizált szabályok (a mesterséges intelligenciáról szóló jogszabály) megállapításáról és egyes uniós jogalkotási aktusok módosításáról. COM(2021) 206 final. Online: https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52021PC0206

Executive Order 14110. Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence. *Federal Register,* 2023. október 30. Online: www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence

Frumer, Yulia (2020): The Short, Strange Life of the First Friendly Robot. *IEEE Spectrum,* 2020. május 21. Online: https://spectrum.ieee.org/the-short-strange-life-of-the-first-friendly-robot

Generative AI Could Raise Global GDP by 7%. *Goldman Sachs,* 2023. április 5. Online: www.goldmansachs.com/intelligence/pages/generative-ai-could-raise-global-gdp-by-7-percent.html

Greenemeier, Larry (2017): 20 Years after Deep Blue: How AI Has Advanced Since Conquering Chess. *Scientific American,* 2017. június 2. Online: www.scientificamerican.com/article/20-years-after-deep-blue-how-ai-has-advanced-since-conquering-chess/

Griffin, Andrew (2017): Facebook's Artificial Intelligence Robots Shut Down After They Start Talking to Each Other in Their Own Language. *Independent,* 2017. július 31. Online: www.independent.co.uk/life-style/facebook-artificial-intelligence-ai-chatbot-new-language-research-openai-google-a7869706.html

Hanson Robotics [é. n.]: *Sophia.* Online: www.hansonrobotics.com/sophia/

Hemmendinger, David [é. n.]: LISP. *Britannica.* Online: www.britannica.com/technology/LISP-computer-language

Kim, Jiwon – Sherer, James A. (2023): Decoding the Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence. *Baker Data Counsel,* 2023. november 28. Online: www.bakerdatacounsel.com/blogs/decoding-the-executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/

Marr, Bernard (2018): The Amazing Ways Chinese Tech Giant Alibaba Uses Artificial Intelligence and Machine Learning. *Forbes,* 2018. július 23. Online: www.forbes.com/sites/bernardmarr/2018/07/23/the-amazing-ways-chinese-tech-giant-alibaba-uses-artificial-intelligence-and-machine-learning/

Martinez, Rex (2019): Artificial Intelligence: Distinguishing Between Types & Definitions. *Nevada Law Journal,* 19(3), 1015–1041. Online: https://scholars.law.unlv.edu/nlj/vol19/iss3/9

Oppy, Graham – Dowe, David (2003): The Turing Test. *Stanford Encyclopedia of Philosophy Archive,* 2003. április 9. Online: https://plato.stanford.edu/archives/win2021/entries/turing-test/

Ortiz, Sabrina (2023): DALL-E 3, OpenAI's Most Advanced Text-to-Image Model, Is Rolling out in Beta Now. *ZDNet,* 2023. október 18. Online: www.zdnet.com/article/openais-most-advanced-text-to-image-model-dalle-3-is-rolling-out-in-beta-now/

SMITH, Stephenson S. et al. (1996): *The New International Webster's Comprehensive Dictionary of the English Language*. Naples, FL: Trident Press International. Online: https://archive.org/details/newinternational0000unse_c7l3/page/n1975/mode/2up
The AlphaStar team (2019): AlphaStar: Mastering the Real-Time Strategy Game StarCraft II. *Deepmind.google,* 2019. január 24. Online: https://deepmind.google/discover/blog/alphastar-mastering-the-real-time-strategy-game-starcraft-ii/
The Current State of AI 2021: Report Now Available. *Appen,* 2021. július 15. Online: https://appen.com/blog/state-of-ai-and-machine-learning-2021-report/
The Editors of Encyclopaedia Britannica [é. n.]: *Archytas of Tarentum.* Online: www.britannica.com/biography/Archytas-of-Tarentum
The Ultimate Guide to Artificial Intelligence (AI): Definition, How It Works, Examples, History, & More. *Tableau.* Online: www.tableau.com/data-insights/ai/what-is
URI, John (2020): 90 Years of Our Changing Views of Earth. *NASA,* 2020. december 21. Online: www.nasa.gov/history/90-years-of-our-changing-views-of-earth/
What Is the History of Artificial Intelligence (AI)? *Tableau.* Online: www.tableau.com/data-insights/ai/history
YANG, May (2023): Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence. *Ropes&Gray,* 2023. november 13. Online: www.ropesgray.com/en/insights/alerts/2023/11/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence

Rövidítések jegyzéke

Rövidítés	Magyar megnevezés	Angol megnevezés
AAAI		Association for the Advancement of Artificial Intelligence
AGI	Mesterséges általános intelligencia	Artificial General Intelligence
ANI	Mesterséges szűk intelligencia	Artificial Narrow Intelligence
ASI	Mesterséges szuperintelligencia	Artificial Superintelligence
GT	Gépi tanulás	Machine Learning
GPT		Generative Pre-trained Transformer
MI	Mesterséges intelligencia	Artificial Intelligence
MI-rendelet	MI-rendelet	Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts
MT	Mélytanulás	Deep Learning
NH	Neurális Hálózatok	Nerual Networks
NIST	Nemzeti Szabványügyi és Technológiai Intézet	National Institute of Standards and Technology
USPTO	Szabadalmi és Védjegyhivatal	United States Patent and Trademark Office

HADMÉRNÖK
FÓRUM

20. évfolyam (2025) 1. szám 187–201.
DOI: 10.32567/hm.2025.1.10

Bányász-Váczi Kincső Boróka,[1] Rajki Zoltán[2]

A bölcsészet-, társadalomtudományi és pedagógiai szakokon tanuló hallgatók perspektívái a mesterséges intelligencia lehetőségeiről és kockázatairól, 1. rész

Szakirodalmi áttekintés

Perspectives of Students in the Humanities, Social Sciences, and Education on the Opportunities and Risks Associated with Artificial Intelligence, Part 1

Literature Review

Absztrakt

Napjainkban a mesterséges intelligencia (MI) a modern technológiák egyik legmeghatározóbb eleme, amely új típusú lehetőségeket és kihívásokat teremt a felsőoktatásban és a munkaerőpiacon. Az MI képes személyre szabott tanulási élményt nyújtani, megkönnyítve a diákok számára a tananyagok elsajátítását és az egyéni igényekhez igazított fejlődést. A felsőoktatás mellett a munkaerőpiacon is észlelhető változásokat idéz elő, mivel egyrészt új foglalkoztatási formákat hoz létre, másrészt bizonyos munkakörök megszűnéséhez vezet, miközben a digitális készségek és az innováció iránti igényt erősíti. Mindazonáltal az új technológia térhódítása olyan kihívásokat is magában hordoz, mint a munkahelyi egyenlőtlenségek fokozódása és az etikai dilemmák kezelése. A szerzők kutatásukban a bölcsészet-, a társadalomtudományi és a pedagógia szakos hallgatók attitűdjeit, jövőképét és MI-használatra való nyitottságát vizsgálták, különös tekintettel a technológia kockázataira

[1] Nemzeti Közszolgálati Egyetem Nemeskürty István Tanárképző Kar, e-mail: vaczi.kincso.boroka@uni-nke.hu
[2] PPKE BTK Szociológiai Intézet, e-mail: zoltan.rajki@btk.ppke.hu

és lehetőségeire. A kvantitatív kutatás keretében 1027 hallgatót kérdeztek meg, akik egy kérdőív segítségével osztották meg véleményüket az MI-vel kapcsolatos ismereteikről, attitűdjeikről és használati szokásaikról. A kiértékelés során statisztikai módszerekkel vizsgálták a megkérdezett hallgatók válaszait. A szerzők kutatásukkal rámutatnak arra, hogy a digitális kompetenciák fejlesztése és az MI etikus használatának oktatása kulcsfontosságú a hallgatók munkaerőpiaci felkészítésében. A technológia gyors fejlődése miatt elengedhetetlen, hogy a felsőoktatás és a munkaerőpiac szereplői rugalmasan alkalmazkodjanak, és hogy az emberek megtanuljanak sikeresen alkalmazkodni az új környezethez. A tanulmány első része a szakirodalmi háttér feltárására és a releváns előzetes kutatások elemzésére összpontosít, míg a második rész az empirikus vizsgálat részletezésével és eredményeinek bemutatásával foglalkozik.

Kulcsszavak: mesterséges intelligencia, felsőoktatás, munkaerőpiac, attitűdvizsgálat, kvantitatív elemzés

Abstract

In contemporary society, Artificial Intelligence (AI) has emerged as a pivotal component of advanced technological systems, presenting both novel opportunities and challenges within the realms of higher education and the labor market. AI possesses the capacity to facilitate personalized learning experiences, thereby enabling students to efficiently comprehend course material and progress in alignment with their unique requirements. Beyond the realm of education, AI significantly influences employment dynamics, leading to the creation of new job roles while rendering some positions obsolete, thus underscoring the critical importance of digital competencies and innovation. Nonetheless, the proliferation of such technologies also introduces significant challenges, including the exacerbation of workplace inequalities and the need to navigate ethical considerations. The authors conducted a study to examine the perceptions, aspirations, and receptiveness toward AI among students enrolled in humanities, social sciences, and pedagogy, particularly regarding the associated risks and opportunities that such technology presents. This quantitative research involved a survey of 1027 students who articulated their perspectives on their understanding, attitudes, and utilization of AI through a structured questionnaire. The analysis employed statistical methodologies to interpret the students' responses. Findings from the study indicate that the enhancement of digital competencies and the promotion of ethical AI usage are fundamental for adequately preparing students for the evolving labor market. The swift advancement of technology necessitates that stakeholders in higher education and the workforce remain adaptable, fostering education that equips individuals to thrive in the changing environment. The first part of the paper provides a comprehensive literature review and contextualizes existing research, while the second part delineates the empirical investigation and presents the findings.

Keywords: Artificial Intelligence, higher education, labour market, attitude analysis, quantitative analysis

Bevezetés

A mesterséges intelligencia (a továbbiakban: MI) a 21. században egy olyan technológiai újdonság, amely egyre fontosabb szerepet játszik nem csupán a hétköznapjainkban, hanem az oktatásban és a munkaerőpiacon is. A társadalom számára számos olyan új lehetőséget kínál, amely rendkívüli módon képes növelni a hatékonyságot az élet minden területén, ugyanakkor számtalan kihívás elé állít minket. Az MI képes javítani a döntéshozatalt, fokozni a termelékenységet, valamint teljeskörűen ellátni a rutinjellegű feladatokat. E jellemzői alkalmassá teszik, hogy bizonyos munkafolyamatok esetében részben vagy teljesen kiváltsa az emberi munkaerőt.[3] A bölcsészettudományi és a társadalomtudományi területek, valamint a pedagógia tudománya évezredekre visszanyúló múlttal rendelkeznek, számtalan olyan kompetencia (például kreativitás, empátia) szükséges a művelésükhöz, amelyet a mesterséges intelligencia a jelenlegi fejlettségi szintjén még nem képes helyettesíteni.[4]

Az egyetemi hallgatók körében rendkívüli népszerűségnek örvend a mesterséges intelligencia. A diákok széles körben alkalmazzák különböző célokra, beleértve a szövegalkotást, fordítási feladatok elvégzését, prezentációk készítését, valamint különböző írásbeli feladatok ellenőrzését és javítását.[5] A diákok pozitívan vélekednek a feltörekvő technológiai újdonságról, mivel számos feladat megoldásában nyújt gyors és hatékony segítséget.[6] A pozitívumként értékelt fő képességek közül kiemelkedik az interaktív kommunikáció, amellyel könnyebbé válik a tanulás folyamata azáltal, hogy részletesebb magyarázatot kapnak a diákok a tanulmányaik során felmerülő elakadások esetén, például egy matematikai egyenlet levezetésekor.[7] A hallgatók körében megfigyelhető optimizmust és nyitottságot több tényező is befolyásolja, ezek között főként a technológia teljesítménye iránti fokozott elvárás és a társadalmi hatás mutatható ki, ezenfelül a szűkebb (család, barátok) és a tágabb környezetből (társadalom) kapott ingerek is meghatározók a technológiához kapcsolódó attitűdben.[8] A felsoroltak mellett a nyitottságot nagymértékben befolyásolja az önbizalom és a digitális kompetenciák szintje, e tényezők mértékével egyenesen arányosan nő az MI iránti fogékonyság.[9]

Nemcsak a pozitív attitűdöt, hanem a hallgatók MI-vel kapcsolatos aggodalmait is számtalan kutatás vizsgálta az elmúlt években. A diákok saját bevallásuk szerint tisztában vannak az MI használatával járó potenciális kockázatokkal, ideértve az adatvédelem, a megbízhatóság, a hitelesség és az etikai aggályok kérdéskörét.[10] A felsőoktatásban az elmúlt néhány év technológiai fejlődése újragondolásra késztette az oktatókat abban a tekintetben, hogy milyen módon szűrhető ki, ha egy szöveget a mesterséges intelligencia készített. Erre vonatkozóan az egyetemek igyekeznek lekövetni az innováció ütemét, azonban számos komplex akadály merül fel ebben

[3] Davoyan 2021.
[4] Marburger 2024; Cui–Liu 2022; Rajki 2023.
[5] Benuyenah–Dewnarain 2024.
[6] Hernández et al. 2024.
[7] Al Murshidi et al. 2024.
[8] Handoko et al. 2024; Lavidas et al. 2024.
[9] Musyaffi et al. 2024.
[10] Guillén-Yparrea – Hernández-Rodríguez 2024; Dabirian–Swarat 2024.

a folyamatban, például olyan rendszerek beszerzése, amelyek kiszűrik a mesterséges intelligencia által generált tartalmat, illetve olyan hivatkozási rend létrehozása, ahol a hallgató jelölni tudja transzparensen, hogy mely tartalmakat készítette az MI. Habár az etikai aggályoknak tudatában vannak a hallgatók a korábbi kutatások alapján, ez nem jelent visszatartó erőt számukra, amikor egy szűk határidővel kapott feladatot kell elkészíteniük.[11] Ezzel együtt a felsőoktatásban tanulók általánosságban egyetértenek azzal, hogy az integritás megőrzésének alapja az egyértelmű irányelvek létrehozása.[12]

A technológia gyors ütemű fejlődése hatással van szinte minden tudományterülethez tartozó foglalkozásra. A bölcsészet- és társadalomtudományi, valamint pedagógiai területen a felsőoktatásban tanulók mesterséges intelligenciával kapcsolatos perspektíváinak feltárásával átfogó képet kaphatunk arról, hogy akik e területekre készülnek, hogyan vélekednek az MI kockázatairól, lehetőségeiről és munkaerőpiacra gyakorolt hatásáról. Rengeteg empirikus adat áll rendelkezésre az MI-re vonatkozó hallgatói attitűd vizsgálata kapcsán a nemzetközi szakirodalomban, azonban kevésbé hangsúlyosan jelennek meg a tudományos publikációkban a bölcsészettudomány, társadalomtudomány és pedagógia szakok hallgatóinak mesterséges intelligenciára vonatkozó percepciói, illetve értékeléseik a technológia által átalakított munkaerőpiaci helyzet kilátásaival kapcsolatban. Kutatásunk éppen ezért kifejezetten az említett területeken tanuló hallgatók attitűdjét és jövőképét vizsgálta.

A mesterséges intelligencia munkaerőpiacra gyakorolt hatása

A mesterséges intelligenciának sokrétű és gyökeres hatásai vannak a munkaerőpiacra, magukban foglalják az álláshelyek megszűnését, új munkakörök létrejöttét, az etikai vonatkozásokat, valamint a gazdasági hatásokat. Az elmúlt évek trendjei azt tükrözik, hogy az MI megjelenése által létrehozott új álláslehetőségek gyors növekedése miatt a vállalatok csökkentették a nem MI-jellegű pozíciókra irányuló toborzást, miközben jelentős mértékben megváltoztatták a fennmaradó állásokhoz szükséges készségkövetelményeket. Ez a változás a munkaerőpiaci polarizáció gyorsulását segíti, bérszakadékokat eredményezve, ugyanakkor ösztönözi a munkaerő áramlását különböző iparágak között. A mesterséges intelligencia fejlődése a munkaerőpiac egyes szegmenseiben eltérő hatást vált ki, mivel a magasan képzett munkavállalók esetében kedvezőtlen folyamatokat indíthat el, ugyanakkor az alacsonyan képzett munkaerő számára kedvező lehetőségeket teremthet, hozzájárulva a munkanélküliségi ráta csökkenéséhez.[13] Az MI munkaerőpiacra gyakorolt hatása etikussággal kapcsolatos kérdéseket is felvet, az algoritmusok és a döntési folyamatok átláthatóságának hiánya növelheti a jövedelmi egyenlőtlenségeket, és bizonyos munkavállalói csoportok kiszorulását eredményezheti a munkaerőpiacról.[14]

Az MI-technológia a munkaerőpiac vonatkozásában kevésbé tekinthető fekete-fehérnek, amennyiben a fókuszt az optimalizálásra helyezzük, elősegítve az ember-gép

[11] Al Murshidi et al. 2024.
[12] Romaniuk – Łukasiewicz-Wieleba 2024.
[13] Acemoglu et al. 2022; Lu 2022.
[14] Ramarajan et al. 2024.

együttműködést, amelyet az oktatás és a készségfejlesztés támogat, és ezen keresztül az MI lehetővé teszi a munkaerő és az iparági igények közötti jobb megfelelést. Az optimalizálás ideálisnak tűnhet minden szereplő számára, ugyanakkor ennek megvalósításához a munkaerőpiaci átalakulások kezelése érdekében célzott támogatási programokra és oktatási befektetésekre van szükség. Ezek a lépések elősegíthetik a technológia terjedését, valamint a humán tőke fejlesztését, ami kulcsfontosságú a munkaerőpiaci dinamika fenntartása szempontjából.[15]

A gazdasági hatásokat tekintve az MI által kiváltott munkakör-helyettesítési hatások összességében jelenleg túl csekélyek ahhoz, hogy jelentős foglalkoztatási változásokat idézzenek elő, ugyanakkor e technológia befolyásolhatja a munkaerő-jövedelem megoszlását a termelékenység és a megváltozott termelési kapcsolatok révén. Míg az MI elterjedése a jövedelem arányának csökkenéséhez vezethet, új foglalkoztatási lehetőségek megteremtésével pozitív hatást is gyakorolhat a munkaerőpiacra. A mesterséges intelligencia fejlesztése során különösen fontos olyan stratégiák kialakítása, amelyek a táradalom jólétét és egy inkluzív gazdasági jövőt szolgálnak. A technológiai fejlődés következtében csökkenő álláslehetőségek kezelése érdekében hangsúlyt kell fektetni a munkavállalók át- és továbbképzésére, ezáltal felkészítve őket a jövő munkaerőpiaci követelményeire. Az ilyen programok nélkülözhetetlenek a foglalkoztatásra és a gazdasági stabilitásra gyakorolt negatív hatások enyhítésében.[16]

A nemzetközi szinten nagy érdeklődésre számot tartó kérdéskör, amely az MI és a jövő munkahelyeivel foglalkozik, Magyarországon is népszerű téma. A Randstad a 2024-es kutatásában kérdezett meg magyarországi vállalati vezetőket az MI munkahelyi alkalmazásával kapcsolatban. A munkaerőpiacra gyakorolt hatás tekintetében a vezetők 52%-a úgy véli, hogy e technológiai újdonság nem befolyásolja az állások számát, míg 45% szerint csökkentheti azokat. A kutatás kiemeli, hogy nemzetközi szinten a munkavállalók közel 47%-a pozitívan viszonyul az MI által létrehozott munkahelyi változásokhoz, különösen az Y és a Z generáció tagjai, ezzel szemben a megkérdezettek 39%-a aggódik a saját munkakörének átalakulása, esetleges elvesztése miatt.[17] A Makronóm Intézet 2023-as munkaerőpiaci előrejelzése alapján elsősorban olyan készségek felértékelődése várható a közeljövőben, mint a kritikus gondolkodás, az érzelmi intelligencia, a kreativitás és a kooperatív munkavégzés képessége, mivel ezek egyike sem lesz rövid vagy középtávon a mesterséges intelligenciával helyettesíthető.[18] A Jobcapital nevű álláskereső oldal 2024-es blogbejegyzése szerint a rugalmasság, az alkalmazkodókészség, valamint az élethosszig tartó tanulás jelentősége meg fog nőni, mert ezek a képességek biztosítják az egyén számára, hogy a gyorsan változó technológiai környezetben helyt tudjon állni.[19] Ahogyan az MI egyre inkább a mindennapjaink részévé válik, megnőhet a kereslet az olyan szakemberek iránt, akik nemcsak magasan képzettek, hanem képesek az új technológiákat rövid idő alatt hatékonyan elsajátítani magas szintű digitális kompetenciáik mellett. A magyar társadalom vonatkozásában a diplomás, képzett rétegben sokan vannak, akiknek

[15] Rademakers – Zierahn-Weilage 2024.
[16] Sharma et al. 2023; Klinova–Korinek 2021; Ramarajan et al. 2024.
[17] Kell-e félteni a munkánkat az AI-tól? – Randstad HR Trends Survey 2024.
[18] A mesterséges intelligencia munkaerőpiaci vetületei 2023.
[19] Tarnai 2024.

hiányos a technológiával kapcsolatos tudása, kiváltképp az idősebb korosztályban, ami akadályát képezheti a gyorsuló változásokhoz való alkalmazkodásnak.[20]

A bölcsészet- és társadalomtudományok számtalan szerteágazó foglalkozást felölelnek, a tanulmány azonban nem kíván részleteiben kitérni az MI valamennyi szakmára gyakorolt hatására a terjedelmi korlátok miatt.[21] Ezen foglalkozások mindegyikében találhatók olyan jellegű feladatok, amelyeket az MI képes elvégezni, azonban teljes munkakörök eltűnésének a lehetősége a jelenlegi tendenciák alapján rövid és középtávon nem számottevő. Nagy változásokra az előrejelzések alapján az adatok elemzése, feldolgozása és az automatizáció területén lehet számítani, az ilyen jellegű feladatok meghatározó részét ki fogja váltani a technológia. Az egyetlen terület jelenleg, amelyet ez érint a közeljövőben, az a kutatás. A kutatási asszisztensek szerepe a rutinfeladatok automatizálása, az MI által vezérelt adatgyűjtés hatékonyságának növelése, valamint a fejlett elemzési eszközök rendelkezésre állása révén csökken, így megnő az esélye annak, hogy ez a munkakör az évek előrehaladtával megszűnik.[22] Ezzel párhuzamosan a technológiai fejlődése által rendelkezésre álló nagy mennyiségű adat értékelése kapcsán megnőhet a kereslet a *big data* elemzésben jártas szakemberek iránt, akik mély társadalomtudományi háttérrel rendelkeznek, így képesek a nagy mennyiségű rendelkezésre álló információnak kontextust teremteni.[23]

A pedagógia területének foglalkozásait illetően az MI megjelenése közvetlenül nem veszélyezteti a dolgozók munkáját, mivel a szociális készségeket nem pótolhatja a jelenlegi fejlettségi szinten lévő mesterséges intelligencia. A pedagógiában az új technológia térnyerésével szükségszerű lesz a digitális kompetenciák minél magasabb szintű elsajátítása, a kritikus gondolkodás átadásának képessége és egy új szerepkör kialakítása, amely inkább a facilitátor irányába mozdul el a lexikális tudásátadó szerepétől.[24] A mesterséges intelligenciában hatalmas potenciál rejlik az oktatás területén (például személyre szabott tanulási módok kialakítása, újszerű, kreatív tananyagok készítése, adminisztratív, rutinszerű feladatok hatékonyabb elvégzése stb.), viszont ezeket a lehetőségeket csak egy újszerű tanulási-nevelési megközelítéssel lehet sikeresen adaptálni.[25]

A jelenlegi trendek alapján az MI átalakulást hoz a bölcsészettudomány, a társadalomtudomány és a pedagógia területén is a jövőben. A sikeres alkalmazkodáshoz elengedhetetlen a folyamatos készségfejlesztés, a mesterséges intelligencia megismerése és az MI-vel való együttműködés képességének elsajátítása. A felsőoktatási intézményeknek fel kell készülniük az új technológia okozta munkaerőpiaci változásokra, hogy megfelelően támogathassák a hallgatókat az új kihívásokkal teli világban.

[20] Nagy veszélyben vannak ezek a munkák – Köztük van a tiéd? 2024.
[21] Az MI e területeken meglévő felhasználási lehetőségeivel kapcsolatosan lásd Rajki 2023.
[22] Javanbakht 2024; Ivanov–Orozova 2022.
[23] Boncz–Szabó 2022.
[24] Tarnai 2024.
[25] Gupta et al. 2024.

Az egyetemi hallgatók mesterséges intelligenciával kapcsolatos attitűdje

A mesterséges intelligenciához való hallgatói hozzáállás az utóbbi időben a szakmai diskurzusok egyik fő elemévé vált, tekintettel a technológiai fejlődés ütemére és az oktatásban felmerülő új kihívásokra. A felsőoktatásban tanulók számtalan, korábban még nem látott lehetőséggel és kockázattal találkoznak mindennapjaikban, amelyek kiterjednek a jövőképükre és a karrierlehetőségeikre is. Az elmúlt években számos kutatás foglalkozott azzal, hogy feltárja nemzetközi viszonylatban a hallgatók hozzáállását az MI-hez különböző aspektusokból.

Az egyetemi hallgatók körében általánosságban pozitív hozzáállás figyelhető meg az MI alkalmazásával kapcsolatban, különösen annak tanulást támogató és tudományos teljesítményt javító szerepe miatt.[26] Egy barcelonai kutatás arra az eredményre jutott, hogy a kommunikáció szakos hallgatók többsége kedvezően értékeli az MI-t, különösen a ChatGPT-t, ugyanakkor az eszközök használatát illetően etikai problémákat is megfogalmaznak.[27] A mesterséges intelligencia oktatási célú alkalmazása kapcsán a hallgatók által említett etikai aggályok leginkább az adatvédelemhez, az információfeldolgozás átláthatóságához és a privát szféra védelméhez kapcsolódnak. Az adatvédelemmel összefüggő kockázatok hangsúlyosan jelennek meg a hallgatók percepcióiban. Egy friss kutatás alapján a megkérdezett hallgatók számottevő aránya (51,9%) aggódik a személyes adatok biztonságáért, illetve azok esetleges illetéktelen felhasználásáért az oktatási célú MI-rendszerekben.[28] Az átláthatóság kérdésköre is gyakran felmerül a témával foglalkozó tudományos közleményekben, ennek egyik oka, hogy a hallgatók rendkívül sok ellentmondásos információval találkozhatnak a mesterséges intelligenciára vonatkozóan. A hallgatók attitűdjét az átláthatósággal és az etikai kérdésekkel kapcsolatban befolyásolja, hogy az adott felsőoktatási intézmény és az ott tanító oktatók hogyan keretezik a mesterséges intelligencia használatát.[29]

A hallgatók technológiaintegrációval kapcsolatos perspektíváinak vizsgálatához érdemes Kumi-Yeboah és munkatársai kutatását is alapul venni, amelynek elméleti kereteit a *privacy calculus theory* (az egyéni információmegosztás előnyeit és költségeit mérlegelő elmélet) adta, elsődleges céljuk pedig az volt, hogy feltárják a különböző hátterű hallgatók nézőpontjait az adatvédelemről, a személyes információk kezeléséről és a technológiai integrációról a felsőoktatásban. A tanulmány vizsgálta a hallgatók tapasztalatait a személyes adatok feletti kontroll elvesztésével és az online tanulásban tapasztalt adatvédelmi problémákkal kapcsolatban. A vizsgálatban részt vevő hallgatók jelentős hányada aggodalmát fejezte ki az online tanulási környezetek *(learning management systems)* és a közösségimédia-platformok fokozódó alkalmazásából eredő adatvédelmi kockázatokat illetően. A válaszokból kitűnik, hogy az egyetemek intézményi szinten nem minden esetben nyújtottak megfelelő támogatást a személyes adatok védelméhez, különösen a Covid–19-világjárvány idején elterjedt, külső szolgáltatók által működtetett digitális platformok (például Zoom, Google Hangouts) használatával összefüggésben. Emellett a közösségi média oktatási célú integrációja

[26] Parveen–Alkudsi 2024.
[27] Sánchez-Reina et al. 2024.
[28] Li–Li–Wu 2025.
[29] Stone 2024.

tovább fokozta az adatvédelmi bizonytalanságokat. A megkérdezett hallgatók számára kihívást jelentett a magánélet és a személyes információk védelme a technológia integrációja közepette. A kutatás azt mutatja, hogy a hallgatók gyakran kényszerülnek kompromisszumra, mivel a technológiai platformok használatát elengedhetetlennek érzik a tanulmányaikhoz, de ez együtt jár a magánélet feletti kontroll elvesztésének félelmével.[30] A tanulmány által felvetett problémakörök rávilágítanak azokra a kockázati tényezőkre, amelyek az MI-rendszerek oktatásban való alkalmazása kapcsán jogos aggodalomra adhatnak okot.

Az oktatás „dehumanizációja", a kritikai gondolkodás csökkenése és a társas interakciókra gyakorolt negatív hatások szintén olyan problémák, amelyeket egyetemi hallgatók is megfogalmaznak.[31] Az attitűdök tekintetében szakterületenként eltérő megközelítések azonosíthatók, mivel a műszaki tudományterületen tanuló hallgatók körében jellemzően kedvezőbb a mesterséges intelligenciához való viszonyulás, míg a humán tudományok hallgatói körében fokozottabb óvatosság és szkepticizmus mutatkozik az új technológiával kapcsolatban.

A karrierlehetőségek szempontjából a feltörekvő technológia jelentős hatást gyakorol a hallgatók jövőképére. Az MI hozzájárulhat szakmai készségeik fejlesztéséhez, különösen a problémamegoldás terén, amely minden munkáltató számára kiemelt fontosságú.[32] A technológiavezérelt iparágak különösen vonzók jelenleg a hallgatók szempontjából, hiszen ezek a területek jelentősen javíthatják a karrierkilátásaikat, amennyiben képesek az MI-vel hatékonyan együtt dolgozni.[33] A munkaerőpiacra ható előnyök mellett fontos kiemelni, hogy a felsőoktatásban tanuló diákok aggodalmaikat is kifejezik az automatizáció és a munkahelyek számának csökkenése miatt.[34]

Az utóbbi években a nemzetközi kutatások mellett a hazai tudományos életben is több vizsgálat zajlott a felsőoktatásban tanuló hallgatók MI-vel kapcsolatos attitűdjére és felhasználási szokásaira vonatkozóan. A kutatások különböző felsőoktatási szakokra fókuszáltak, különböző módszertani megközelítéssel. A Budapesti Corvinus Egyetem kutatásának eredményeit érdemes megvizsgálni, amelyben a saját hallgatóinak MI-vel kapcsolatos attitűdjeit térképezte fel. A 2023 tavaszán végzett felmérés szerint a megkérdezett 318 fő 99%-a hallott már MI-alkalmazásokról, és 91%-uk ismeri is ezeket. A legnépszerűbb MI-platform a ChatGPT (54% használja), amelyet főként nyelvtani hibák kiszűrésére, fordításra és gyors információszerzésre alkalmaznak. A hallgatók 85%-a gondolja úgy, hogy nem kapott kielégítő tájékoztatást az MI alkalmazásának etikai vonatkozásairól, ezért nyitottak a mesterséges intelligenciával kapcsolatos kurzusokra az egyetemen.[35]

A hallgatók MI-vel kapcsolatos ismereteinek elmélyítése érdekében egy másik, hasonló kutatás is vizsgálta azt, hogy milyen mértékben ismerik a generatív MI-eszközöket a felsőoktatásban tanulók. 6 magyar egyetemről 69 hallgató részvételével végeztek félig strukturált interjús kutatást, amelynek eredményei szerint a ChatGPT

[30] Kumi-Yeboah et al. 2023.
[31] Jabar et al. 2024.
[32] Vázquez-Parra et al. 2024a; Gherheș–Obrad 2018; Parveen–Alkudsi 2024.
[33] Parveen–Alkudsi 2024.
[34] Arruzza 2024; Vázquez-Parra et al. 2024b.
[35] A Corvinus Egyetem hallgatóinak többsége használ mesterséges intelligenciát 2023.

széles körben elterjedt a szöveggenerálásban, -formázásban és -fordításban. Az interjúk alapján a diákok kihívásként érzékelték a ChatGPT válaszainak általánosságát és a nem mindig aktuális vagy elavult információkat.[36]

A generatív MI-eszközök felsőoktatási felhasználását tovább árnyalja az a korábbi kvantitatív kutatásunk, amelyben a több mint 1000 megkérdezett egyetemi hallgató egy része az MI-t a tanulás támogatására használja, azonban a használat mellett tisztában van az MI-alapú technológiák korlátaival. A válaszadók körében a ChatGPT, a Grammarly és a DeepL volt a legnépszerűbb alkalmazás.[37]

A generatív MI alkalmazásának gyakorlati kérdéseit egy üzleti szakos hallgatók (41 fő) körében végzett kutatás is vizsgálta. A Budapesti Gazdasági Egyetemen végzett kontrollcsoportos vizsgálat (amely kifejezetten az üzleti nyelvoktatás területére fókuszált) eredményei szerint a hallgatók 90%-a ellenzi az MI egyetemi tiltását, de szükségesnek tartják a szabályozást. Az MI-alapú eszközök a diákok szerint segíthetik az esszéírást és az információgyűjtést, de nem helyettesítik a hagyományos oktatást.[38]

A pedagógia területén tanuló hallgatók esetében jelentős eltérések tapasztalhatók az MI alkalmazásával kapcsolatban. Egy tanító szakos hallgatók körében végzett 100 fős kérdőíves vizsgálat kimutatta, hogy a válaszadók 82%-a nem találkozott MI-eszközökkel tanulmányai során. A hallgatók jelentős része nem tudta pontosan megkülönböztetni az MI-alapú technológiákat az infokommunikációs technológiáktól, ugyanakkor a megkérdezettek 87%-a nyitottságát fejezte ki az MI-vel kapcsolatos továbbképzésre, megfelelő támogatás és intézményi keretek mellett.[39] Egy hasonló, a gyógypedagógus hallgatók körében végzett kutatás vizsgálta, hogy az MI milyen szerepet tölthet be a speciális nevelési igényű diákok támogatásában. A 157 fős minta elemzése szerint az MI-eszközök alkalmazása kevéssé ismert, és a hallgatók többsége inkább tanórán kívüli tevékenységekben tartja elképzelhetőnek az alkalmazásukat.[40]

Az MI-vel kapcsolatos szabályozás szintén hangsúlyos szerepet kapott több magyarországi kutatásban. Egy korábbi elemzésünkben vizsgáltuk, hogy a nagy nyugati és magyar egyetemek milyen stratégiákat alkalmaznak az MI elterjedésével kapcsolatban. A brit és az amerikai felsőoktatási intézmények kezdetben szigorú tiltásokat vezettek be, majd fokozatosan áttértek a szabályozott használatra és az MI integrációjára az oktatásban. Magyarországon a válaszreakciók lassabban és eltérő módon jelentek meg, mivel egyes felsőoktatási intézmények szakmai műhelymunkák és konferenciák révén törekedtek a mesterséges intelligencia hatásainak feltárására, míg mások konkrét szabályozási intézkedéseket vezettek be. A magyar egyetemek többsége még nem rendelkezik egységes, átfogó MI-stratégiával, inkább eseti megoldásokat alkalmaz.[41]

Az elmúlt években számos magyarországi kutatás foglalkozott a mesterséges intelligencia felsőoktatásban betöltött szerepével. A vizsgálatok különböző szakterületeken és módszertani megközelítésekkel elemezték a hallgatók MI-vel kapcsolatos

[36] Folmeg et al. 2024.
[37] Rajki 2024.
[38] Kétyi et al. 2025.
[39] Demeter–Mező 2023a.
[40] Demeter–Mező 2023b.
[41] Rajki – T. Nagy – Dringo-Horváth 2024.

ismereteit, attitűdjeit és felhasználási szokásait. Az eredmények rámutattak arra, hogy az MI egyre inkább jelen van az oktatásban, de a megfelelő intézményi iránymutatás és etikai keretek még nem mindenhol állnak rendelkezésre. A hallgatók általában nyitottak az MI lehetőségeire, ugyanakkor kihívásokat is azonosítottak annak alkalmazásában. A kutatások arra is felhívták a figyelmet, hogy az egyetemek eltérő stratégiákat dolgoztak ki az MI integrációjára, ami szabályozási és oktatási szempontból is további fejlesztéseket igényel.

A korábbi nemzetközi és hazai kutatások rámutatnak arra, hogy az egyetemi hallgatók általánosságban optimistán értékelik az MI szerepét tanulmányaikban és jövőbeli karrierjükben, ugyanakkor etikai aggályok és a technológia hatásai miatti félelmeik is jelen vannak. Az MI által nyújtott lehetőségek és kihívások megértése, valamint az etikus és hatékony alkalmazás biztosítása alapvető fontosságú ahhoz, hogy a hallgatók felkészüljenek a technológia által formált jövőre. Egy támogató, a legújabb technológiát integráló oktatási környezet, amely megfelelő képzést nyújt az MI megértéséhez és etikus alkalmazásához, alapvető jelentőségű a 21. század hallgatóinak felkészítése szempontjából.[42] A felsőoktatási intézmények szerepe abban rejlik, hogy etikus irányelveket dolgozzanak ki, amelyek maximalizálhatják az MI által nyújtott versenyelőnyt, miközben minimalizálják a használattal kapcsolatos kockázatokat.[43]

Az elmúlt néhány év kutatási eredményei számos összefüggésre rávilágítanak az egyetemi hallgatók mesterséges intelligenciára vonatkozó attitűdjei kapcsán. A bölcsészet- és társadalomtudományi területek, valamint a pedagógiai szakok kevésbé technológiaorientáltak, ezért a tudományos kutatásokban kevésbé hangsúlyosan vannak jelen, mint például a műszaki és az informatikához kapcsolódó területek. Az MI rengeteg munkafolyamatot átalakít, újrarendezi a munkaerőpiacot, s éppen ezért kiemelkedően fontos, hogy a most felsőoktatásban tanuló bölcsészek, társadalomtudománnyal foglalkozó leendő szakemberek és pedagógusok felkészülten érkezzenek a munka világába. E folyamat sikeressége érdekében lényegesnek tartottuk megvizsgálni, hogy a felsorolt területeken jelenleg felsőfokú tanulmányokat folytató hallgatók hogyan viszonyulnak az MI-hez, milyen lehetőségeket, kockázatokat látnak a használat kapcsán, hogyan értékelik a munkaerőpiaci esélyeiket az egyetemi tanulmányaik után.

Összegzés

A mesterséges intelligencia fejlődése az oktatásban és a munkaerőpiacon alapvető változásokat idéz elő, amelyek hatása a bölcsészet-, a társadalomtudomány és a pedagógia területén is érzékelhető. Az MI lehetőséget kínál a hatékonyság növelésére és a rutinfeladatok automatizálására, miközben új kihívásokat teremt a kritikus gondolkodást és szociális készségeket igénylő szakmák számára. A felsőoktatásban tanuló hallgatók általánosságban pozitívan vélekednek az MI-ről, kiemelve annak tanulást segítő szerepét, főként a szövegalkotásban és a fordításban. A hallgatók

[42] Balabdaoui et al. 2024; Vázquez-Parra et al. 2024a; Dabirian–Swarat 2024.
[43] Pisica et al. 2024.

hozzáállását és nyitottságát nagymértékben befolyásolják digitális kompetenciáik, önbizalmuk és a társadalmi környezetükből érkező ingerek, ugyanakkor a technológia alkalmazásával kapcsolatos etikai aggályok, mint az adatvédelem, a hitelesség és az átláthatóság, szintén meghatározzák a hallgatók attitűdjét.

A mesterséges intelligencia munkaerőpiacra gyakorolt hatásai összetettek, mivel egyes munkakörök megszűnése mellett új foglalkoztatási lehetőségek megjelenésére is számítani lehet. A bölcsészettudomány, a társadalomtudomány és a pedagógia területén tanuló hallgatók jövőképét alapvetően meghatározza az a felismerés, hogy a szociális készségeket és kreativitást igénylő tevékenységek rövid és középtávon nem helyettesíthetők a fejlett technológiával. Mindazonáltal főként a kutatási és adatfeldolgozási feladatok területén az MI megjelenése átalakíthatja a munkaköröket, előtérbe helyezve a technológia használatához szükséges magas szintű digitális kompetenciákat.

Összességében a mesterséges intelligencia nem csupán technológiai, hanem társadalmi szempontból is mélyreható átalakulásokat eredményezhet a jövőben. Az MI-hez való alkalmazkodás sikeressége érdekében kulcsfontosságú a készségek folyamatos fejlesztése és az új technológiákkal való együttműködés képességének elsajátítása. A felsőoktatási intézményeknek fel kell készíteniük a hallgatókat az új kihívásokra, miközben szavatolniuk kell az etikus és hatékony alkalmazás feltételeit. Az MI által kínált lehetőségek és kockázatok megértése, valamint a felelősségteljes használat iránti elköteleződés elengedhetetlen ahhoz, hogy a hallgatók sikeresek legyenek a munkaerőpiacon a technológia által átformált jövőben.

Felhasznált irodalom

A Corvinus Egyetem hallgatóinak többsége használ mesterséges intelligenciát. *HR Portal,* 2023. június 21. Online: www.hrportal.hu/c/a-corvinus-egyetem-hallgatoinak-tobbsege-hasznal-mesterseges-intelligenciat-20230621.html

A mesterséges intelligencia munkaerőpiaci vetületei. *Makronóm,* 2023. július 18. Online: https://makronom.eu/2023/07/18/a-mesterseges-intelligencia-munkaeropiaci-vetuletei/

Acemoglu, Daron et al. (2022): Artificial Intelligence and Jobs: Evidence from Online Vacancies. *Journal of Labor Economics,* 40(S1), S293–S340. Online: https://doi.org/10.1086/718327

Al Murshidi, Ghadah et al. (2024): How Understanding the Limitations and Risks of Using ChatGPT Can Contribute to Willingness to Use. *Smart Learnong Environments,* 11(1). Online: https://doi.org/10.1186/s40561-024-00322-9

Arruzza, Elio (2024): Radiography Students' Perceptions of Artificial Intelligence in Medical Imaging. *Journal of Medical Imaging and Radiation Sciences,* 55(2), 258–263. Online: https://doi.org/10.1016/j.jmir.2024.02.014

Balabdaoui, Fadoua et al. (2024): A Survey on Students' Use of AI at a Technical University. *Discover Education,* 3(1). Online: https://doi.org/10.1007/s44217-024-00136-4

Benuyenah, Vic – Dewnarain, Senika (2024): Students' Intention to Engage With ChatGPT and Artificial Intelligence in Higher Education Business Studies Program-

mes: An Initial Qualitative Exploration. *International Journal of Distance Education Technologies,* 22(1), 1–21. Online: https://doi.org/10.4018/IJDET.348061

Boncz Bettina – Szabó Zsolt Roland (2022): A mesterséges intelligencia munkaerő-piaci hatásai. Hogyan készüljünk fel? *Vezetéstudomány,* 53(2), 68–80. Online: https://doi.org/10.14267/VEZTUD.2022.02.06

Cui, Zhongliang – Liu, Jing (2022): A Study on Two Conditions for the Realization of Artificial Empathy and Its Cognitive Foundation. *Philosophies,* 7(6), 135. Online: https://doi.org/10.3390/philosophies7060135

Dabirian, Amir – Swarat, Su (2024): Artificial Intelligence in Higher Education: Community Perceptions at a Large U.S. University. *IT Professional,* 26(4), 92–96. Online: https://doi.org/10.1109/MITP.2024.3434068

Davoyan, Ashot (2021): The Impact of Artificial Intelligence on Work, Education, Mobility and Economy. In Arai, Kohei – Kapoor, Supriya – Bhatia, Rahul (szerk.): *Proceedings of the Future Technologies Conference (FTC) 2020, Volume 1.* Cham: Springer, 291–296. Online: https://doi.org/10.1007/978-3-030-63128-4_22

Demeter Zsuzsa – Mező Katalin (2023a): A mesterséges intelligencia pedagógiai használatára vonatkozó hajlandóság vizsgálata gyógypedagógus hallgatók körében. *Különleges Bánásmód,* 9(2), 31–45. Online: https://doi.org/10.18458/KB.2023.2.31

Demeter Zsuzsa – Mező Katalin (2023b): Tanító szakos hallgatók és a mesterséges intelligencia. *Mesterséges Intelligencia,* 5(1), 73–87. Online: https://doi.org/10.35406/MI.2023.1.73

Folmeg, Marta – Fekete, Imre – Koris, Rita (2024): Towards Identifying the Components of Students' AI Literacy: An Exploratory Study Based on Hungarian Higher Education Students' Perceptions. *Journal of University Teaching and Learning Practice,* 21(6). Online: https://doi.org/10.53761/wzyrwj33

Gherheș, Vasile – Obrad, Ciprian (2018): Technical and Humanities Students' Perspectives on the Development and Sustainability of Artificial Intelligence (AI). *Sustainability,* 10(9), 3066. Online: https://doi.org/10.3390/su10093066

Guillén-Yparrea, Nicia – Hernández-Rodríguez, Felipe (2024): Unveiling Generative AI in Higher Education: Insights from Engineering Students and Professors. In *2024 IEEE Global Engineering Education Conference (EDUCON).* 1–5. Online: https://doi.org/10.1109/EDUCON60312.2024.10578876

Gupta, Sanjai – Dharamshi, Ravindra R. – Kakde, Vinodkumar (2024): An Impactful and Revolutionized Educational Ecosystem using Generative AI to Assist and Assess the Teaching and Learning Benefits, Fostering the Post-Pandemic Requirements. In *2024 Second International Conference on Emerging Trends in Information Technology and Engineering (ICETITE),* 1–4. Online: https://doi.org/10.1109/ic-ETITE58242.2024.10493370

Handoko, Bambang Leo – Thomas, Gen Norman – Indriaty, Lely (2024): Adoption and Utilization of Artificial Intelligence to Enhance Student Learning Satisfaction. In *2024 International Conference on ICT for Smart Society (ICISS),* 1–6. Online: https://doi.org/10.1109/ICISS62896.2024.10751260

Hernández, Iván Neftalí Ríos et al. (2024): Percepciones de estudiantes latinoamericanos sobre el uso de la inteligencia artificial en la educación superior. *Austral Comunicación,* 13(1), e01302. Online: https://doi.org/10.26422/aucom.2024.1301.rio

Ivanov, A. P. – Orozova, D. A. (2022): Intelligent Personnel Assistant for Field Researchers. In *2022 45th Jubilee International Convention on Information, Communication and Electronic Technology (MIPRO),* 1014–1018. Online: https://doi.org/10.23919/MIPRO55190.2022.9803626

Jabar, Melvin – Chiong-Javier, Elena – Pradubmook Sherer, Penchan (2024): Qualitative Ethical Technology Assessment of Artificial Intelligence (AI) and the Internet of Things (IoT) Among Filipino Gen Z Members: Implications for Ethics Education in Higher Learning Institutions. *Asia Pacific Journal of Education,* 1–15. Online: https://doi.org/10.1080/02188791.2024.2303048

Javanbakht, Arash (2024): In Context: AI Will Write Your Paper: The Very Different Future of Research and Scientific Writing in the Age of Artificial Intelligence. *Journal of the American Academy of Child & Adolescent Psychiatry,* 63(7), 681–683. Online: https://doi.org/10.1016/j.jaac.2024.03.013

Kell-e félteni a munkánkat az AI-tól? – Randstad HR Trends Survey 2024. *Randstad Hungary,* 2024. február 27. Online: www.randstad.hu/workforce-insights/munkaeropiac/kell-e-felteni-a-munkankat-az-ai-tol-randstad-hr-trends-survey-2024/

Kétyi, András – Géring, Zsuzsanna – Dén-Nagy, Ildikó (2025): ChatGPT From the Students' Point of View – Lessons From a Pilot Study Using ChatGPT in Business Higher Education. *Society and Economy,* 47(1), 1–12. Online: https://doi.org/10.1556/204.2024.00007

Klinova, Katya – Korinek, Anton (2021): AI and Shared Prosperity. In *AIES '21. Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society.* New York: Association for Computing Machinery, 645–651. Online: https://doi.org/10.1145/3461702.3462619

Kumi-Yeboah, Alex et al. (2023): Diverse Students' Perspectives on Privacy and Technology Integration in Higher Education. *British Journal of Educational Technology,* 54(6), 1671–1692. Online: https://doi.org/10.1111/bjet.13386

Lavidas, Konstantinos et al. (2024): Determinants of Humanities and Social Sciences Students' Intentions to Use Artificial Intelligence Applications for Academic Purposes. *Information,* 15(6), 314. Online: https://doi.org/10.3390/info15060314

Li, Wenjie – Li, Kailin – Wu, Dong (2025): AI in Higher Education: A Survey-Based Empirical Study on Applications and Student Expectations. In *2025 14th International Conference on Educational and Information Technology, ICEIT 2025*. 501–505. Online: https://doi.org/10.1109/ICEIT64364.2025.10976153

Lu, Chia-Hui (2022): Artificial Intelligence and Human Jobs. *Macroeconomic Dynamics,* 26(5), 1162–1201. Online: https://doi.org/10.1017/S1365100520000528

Marburger, Marcel René (2024): Artistic Intelligence vs. Artificial Intelligence. *Artnodes,* (34), 1–7. Online: https://doi.org/10.7238/artnodes.v0i34.425712

Musyaffi, Ayatulloh Michael et al. (2024): Improving Students' Openness to Artificial Intelligence Through Risk Awareness and Digital Literacy: Evidence Form a Developing Country. *Social Sciences & Humanities Open,* 10, 101168. Online: https://doi.org/10.1016/j.ssaho.2024.101168

Nagy veszélyben vannak ezek a munkák – Köztük van a tiéd? *Portfolio,* 2024. december 28. Online: www.portfolio.hu/gazdasag/20241228/nagy-veszelyben-vannak-ezek-a-munkak-koztuk-van-a-tied-730605

Parveen, Musrrat – Alkudsi, Yusra Mohammed (2024): Graduates' Perspectives on AI Integration. Implications for Skill Development and Career Readiness. *International Journal of Educational Research and Innovation,* (22), 1–17. Online: https://doi.org/10.46661/ijeri.10651

Pisica, Alina Iorga et al. (2024): Romanian Students' Opinions on Implementing Artificial Intelligence in Higher Education: A Qualitative Approach. *Transformations in Business and Economics,* 23(2), 21–35.

Rademakers, Emilie – Zierahn-Weilage, Ulrich (2024): New Technologies: End of Work or Structural Change? *The Economists' Voice,* 21(2), 335–344. Online: https://doi.org/10.1515/ev-2024-0046

Rajki Zoltán (2023): A mesterséges intelligencián alapuló alkalmazások a bölcsészet-, társadalomtudomány és az oktatás területén. *Humán Innovációs Szemle,* 14(2), 4–21. Online: https://doi.org/10.61177/HISZ.2023.14.2.1 ; DOI: https://doi.org/10.61177/HISZ.2023.14.2.1

Rajki Zoltán (2024): A bölcsészet-, társadalomtudományi és pedagógiai szakokon tanuló egyetemi hallgatók mesterséges intelligenciával kapcsolatos ismeretei és az MI mindennapi használata. *Mester és Tanítvány,* 2(1), 62–81. Online: https://doi.org/10.61178/MT.2024.II.1.5

Rajki Zoltán – T. Nagy Judit – Dringo-Horváth Ida (2024): A mesterséges intelligencia a felsőoktatásban – hallgatói hozzáférés, attitűd és felhasználási gyakorlat. *Iskolakultúra,* 34(7), 3–22. Online: https://doi.org/10.14232/iskkult.2024.7.3

Ramarajan, M. et al. (2024): AI-Driven Job Displacement and Economic Impacts: Ethics and Strategies for Implementation. In Tennin, Kyla Latrice et al. (szerk.): *Cases on AI Ethics in Business.* Hershey, PA: IGI Global Scientific Publishing, 216–238. Online: https://doi.org/10.4018/979-8-3693-2643-5.ch013

Romaniuk, Miłosz Wawrzyniec – Łukasiewicz-Wieleba, Joanna (2024): Generative Artificial Intelligence in the Teaching Activities of Academic Teachers and Students. *International Journal of Electronics and Telecommunications,* 70(4), 1043–1048. Online: https://doi.org/10.24425/ijet.2024.152092

Sánchez-Reina, J. Roberto et al. (2024): Exploring Undergraduates' Attitudes Towards ChatGPT. Is AI Resistance Constraining the Acceptance of Chatbot Technology? In Casalino, Gabriella et al.: *Higher Education Learning Methodologies and Technologies Online.* Cham: Springer, 383–397. Online: https://doi.org/10.1007/978-3-031-67351-1_26

Sharma, Pushpak et al. (2023): Artificial Intelligence and Its Impact on Employment: A Perspective in Context of Keynesian Employment Theory. In *2023 International Conference on New Frontiers in Communication, Automation, Management and Security (ICCAMS),* 1–7. Online: https://doi.org/10.1109/ICCAMS60113.2023.10525818

Stone, Brian W. (2024): Generative AI in Higher Education: Uncertain Students, Ambiguous Use Cases, and Mercenary Perspectives. *Teaching of Psychology,* 52(3), 347–356. Online: https://doi.org/10.1177/00986283241305398

Tarnai Attila (2024): 2024-es munkaerőpiaci trendek – AI az álláskeresésben. *Jobcapital,* 2024. január 9. Online: https://jobcapital.hu/2024-es-munkaeropiaci-trendek/

VÁZQUEZ-PARRA, José Carlos et al. (2024a): Complex Thinking and Adopting Artificial Intelligence Tools: A Study of University Students. *Frontiers in Education,* 9, 1–15. Online: https://doi.org/10.3389/feduc.2024.1377553

VÁZQUEZ-PARRA, José Carlos et al. (2024b): Importance of University Students' Perception of Adoption and Training in Artificial Intelligence Tools. *Societies,* 14(8), 141. Online: https://doi.org/10.3390/soc14080141

HADMÉRNÖK
FÓRUM

20. évfolyam (2025) 1. szám 203–218.
DOI: 10.32567/hm.2025.1.11

Koller Marco[1]

Szuverenitásvédelem és digitális szuverenitás

A komplex biztonsági kihívások láncolata

Sovereignty Protection and Digital Sovereignty

The Chain of Complex Security Challenges

Absztrakt

Egy adott állam mindennemű függetlenségének, befolyástól mentes működésének szavatolása alapvető össztársadalmi érdek. A szuverenitásvédelem komplex tevékenység, amely átfogja az egész államigazgatást, de kiemelt szerepe van benne a rendvédelemnek, illetve a nemzetbiztonsági szolgálatoknak. Azonban a változó világot a változó és komplex biztonsági kihívások jellemzik, amelyek lehetnek akár környezeti, humán vagy technológiai eredetűek, ezért fontos a proaktív szemléletmód, valamint a hazai és nemzetközi együttműködések hangsúlyozása. A digitalizálódó világban a kibertér egyre inkább meghatározó jelentőségű lesz, így a digitális szuverenitás elérése, annak védelmezése is hangsúlyos.

Kulcsszavak: szuverenitás, digitalizáció, biztonság, kockázatok, lehetőségek, digitális szuverenitás

Abstract

Ensuring a state's independence from external interference is a core interest of society at large. The entire state apparatus is involved in the complicated task of defending sovereignty, but the police and national security agencies are particularly important in

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem Hadtudományi Doktori Iskola, e-mail: marcoakoller@gmail.com

this regard. But whether it's environmental, human, or technological, the changing globe brings with it ever-changing and complicated security concerns. For this reason, it's critical to be proactive and to prioritize both domestic and international collaboration. Achieving and defending digital sovereignty is crucial since cyberspace will grow in importance in a world that is becoming more digitally integrated.

Keywords: sovereignty, digitalisation, security, risks, opportunities, digital sovereignty

Bevezetés

A jelenkor jellemzője a dinamikusan változó biztonsági környezet, amely számos új feladatot indukál az állami szervek számára, többek között a biztonság – különböző aspektusú – fenntartásával foglalkozó intézmények számára is, mint a rendőrség vagy a nemzetbiztonsági szolgálatok. A változó világhoz kapcsolódó kihívások és kockázatok fokozódásáról számos szakirodalom, illetve hazai és nemzetközi joganyag (például a *Nemzeti Biztonsági Stratégia* és az *Alaptörvény* stb.) is megemlékezik, azonban kevesebb figyelmet kap az, hogy a biztonsági kihívások komplexek, azaz nem lehet őket önmagukban – hatékonyan és szakszerűen – értelmezni. Egy-egy jelenség összefonódik a másikkal, az egyik a másikból következik, illetve egymást generálja, fokozza. Így a biztonsági kihívások komplex láncolatáról beszélhetünk, amely mind a világ, mind Európa és hazánk biztonsági környezetét befolyásolja.

„Magyarország szuverenitását egyre gyakrabban éri jogellenes támadás. Évek óta tetten érhető – és sok esetben a nyilvánosság számára is ismert – befolyásszerzési kísérletek történnek, melyek során külföldi szervezetek és személyek a saját érdekeiket igyekeznek érvényesíteni hazánkban, szemben a magyar érdekekkel és szabályokkal."[2] A fentiek tükrében egyre fontosabbá vált az ország függetlenségének, biztonságának szavatolása, azaz a szuverenitásvédelem. Többek között ezért jött létre a Szuverenitásvédelmi Hivatal a 2023. évi LXXXVII. törvény által.

A kutatás célja és az alkalmazott módszerek

Európa és hazánk szuverenitása több dimenzióban is érintett, annak védelmét több aspektusból szükséges vizsgálni. Jelen tanulmány célja, hogy bemutassa azokat a biztonsági kihívásokat, amelyek hazánk biztonságát, szuverenitását veszélyeztetik a változó világ, illetve az európai biztonsági környezet tükrében, különös figyelmet fordítva arra, hogy az egyes, biztonságot érintő elemek milyen láncolatban, összefüggésben figyelhetők meg, továbbá a digitális szuverenitás tükrében, mint a jelenkor egyik aktuális problematikája. A feltárt kihívások és kockázatok nem teljes körűek, azok az aktuális trendek, illetve egyedi nézőpontok alapján változhatnak, azonban a kiemelt kategóriaelemek álláspontom szerint rendkívül jól összefoglalják a főbb problémaköröket.

[2] 2023. évi LXXXVII. törvény a nemzeti szuverenitás védelméről, preambulum.

A fentieken túlmenően a feltárt kihívások és kockázatok bemutatása, illetve elemzése után a tanulmány ajánlásokat tesz, amelyek esetleges végrehajtása Magyarország nemzetbiztonságát, illetőleg szuverenitásának védelmét segítené elő.

A tanulmány elkészítése során a főbb vonatkozó hazai joganyagokat hívtam segítségül: a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvényt (a továbbiakban: Nbtv.) és a Magyarország Nemzeti Biztonsági Stratégiájáról szóló 1163/2020. (IV. 21.) Korm. határozatot (a továbbiakban: NBS). Ezek alapján határoztam meg a főbb kockázati kategóriákat, amelyeket aztán PESTEL-analízis alapján rendszereztem, elemeztem, és megfogalmaztam a vonatkozó ajánlásokat. A PESTEL-analízis egy stratégiai tervezési eszköz, amelyet alapvetően az üzleti szférában alkalmaznak; a PEST-analízis kibővített verziója.

„A PEST elemzés során a vállalkozásra ható hosszabb távú környezeti tendenciákat vesszük számba és strukturáljuk, ezáltal megragadhatóvá, kiemelhetővé válnak azok a fontosabb tényezők, amelyek befolyásolhatják a stratégiai döntéseket. Cél megtalálni a jelen és jövő fontos környezeti tényezőit, amelyek a vállalkozás szempontjából meghatározóak. A PEST elemzés négy dimenzió mentén vizsgálja a környezetet."[3]

Jelen tanulmány során implementáltam eszközeit, így lehetővé vált, hogy megértsük a külső tényezőket, amelyek hatással vannak egy adott nemzet biztonságára, stabilitására és fejlődési lehetőségeire. Az elemzés politikai, gazdasági, társadalmi és technológiai (PEST), valamint környezeti és jogi (EL) tényezők vizsgálatát foglalja magában. Az elemzés segít megérteni a külső környezet hatásait a nemzeti biztonságra, a gazdasági stabilitásra és a társadalmi folyamatokra, továbbá lehetővé teszi a jövőbeni biztonsági és politikai trendek azonosítását, amelyek befolyásolhatják az ország stabilitását.

Fogalmi háttér

A téma komplexitása okán a megfelelő értelmezéséhez szükséges a felmerülő fogalmi keret meghatározása, a fontosabb kifejezések definiálása az alábbiak szerint.

Biztonság

A biztonság mint fogalom és jelenség rendkívül összetett, számos aspektussal rendelkezik (például nemzetbiztonság, nemzeti biztonság, gazdaságbiztonság, energiabiztonság, egészségügyi biztonság stb.). A legegyszerűbben úgy lehet meghatározni a biztonságot, mint egy veszély nélküli stabil állapotot, amelynek fenntartása mind állami, mind egyéni szinten kiemelt jelentőségű, hiszen maga a biztonság Abraham Maslow amerikai pszichológus szükségletpiramisán a második legfőbb szükségleti kategóriaként jelenik meg, amely magában foglalja a fizikai védettséget és a kiszámíthatóságot.[4]

[3] Rabi 2009.
[4] Mező 2007: 121–125.

Nemzeti biztonság és nemzetbiztonság

A nemzeti biztonság egy sokrétű *össztársadalmi teljesítmény,*[5] mindent magában foglal, ami kockázatként, kihívásként, illetve valamilyen fenyegetésként jelenik meg az adott állam irányában (például természeti katasztrófák, demográfiai, egészségügyi kihívások, kockázatok stb.). Nemzetbiztonság alatt szűk értelemben a titkosszolgálati tevékenységet értjük, az úgynevezett *intelligence* tevékenységi kört. A fent említett különböző kihívások és kockázatok, fenyegetések jellegéből, sokaságából és igen nagy fokú különbözőségéből fakadóan a nemzet biztonságát nem tudja lefedni a titkosszolgálati tevékenységet végző szervek munkája, hanem más rendészeti és egyéb szervek összehangolt közös feladatvégzése is szükségeltetik a problémák kezeléséhez.

Szuverenitás

A szuverenitás az állam önállóságát jelenti, azaz az állam a saját jogrendjét maga alkotja és tartja fenn kizárólagos területi főhatalommal a területén lévő személyek és dolgok felett. A szuverén állam más államokkal való kapcsolatában szabadon, függetlenül dönt, területi épsége és politikai függetlensége sérthetetlen, és joga van ahhoz, hogy szabadon válassza meg és alakítsa politikai, társadalmi és kulturális rendszerét.[6]

Digitális szuverenitás

Az Európai Unió legnagyobb kihívása a digitális szuverenitás elérése, így hazánké is.[7] Digitális szuverenitás alatt a Gartner definíciója szerint a kormány azon képességét értjük, „hogy a politikát a külföldi kormányok digitális szabályozása által közvetlenül az állampolgáraira és a székhelye szerinti vállalkozásokra rótt akadályok nélkül valósítsa meg, beleértve a szabályozási ellenőrzés alatt álló digitális óriáscégek által gyakorolt szabályozást is."[8] Philip von Brockdorff véleménye szerint, amelyet az Európai Gazdasági és Szociális Bizottság (a továbbiakban: EGSZB) egyik állásfoglalásában ismertetett, a digitális szuverenitást talán úgy lehet körülírni, mint a kormányok és a vállalkozások autonómiáját saját adataik, hardvereik és szoftvereik kezelése és létrehozása tekintetében."[9] A fenti fogalmak a szuverenitást az állam szempontjából közelítik meg, azonban ezt kisebb egységre lebontva is lehet vizsgálni. Személyek digitális szuverenitása alatt azt értjük, hogy az egyén saját ellenőrzése alatt tudja tartani, ki férhet hozzá és milyen céllal használhatja a személyéhez kötődő digitális információt.[10] Jól látható, hogy az egyik fő tartalmi elem az adatok és az azokat kezelő rendszerek feletti tényleges, kiszolgáltatottság nélküli felügyelet. Az EGSZB-vélemény szerint

[5] Mező 2007: 121–125.
[6] Tálas [é. n.].
[7] Tóth 2021: 31.
[8] A digitális szuverenitás jelentősége 2023.
[9] Von Brockdorff 2022: 2.1 pont.
[10] Pató 2021.

az EU nagymértékben támaszkodik EU-n kívül működő nagy technológiai vállalatokra, és az EU-nak csökkentenie kell a nem uniós technológiai óriásoktól való függőségét annak ellenére, hogy jelentős előrelépést tett digitális szuverenitásának javítása terén. A vélemény kiemeli, hogy támogatni kell a technológiai fejlődést célzó kutatásokat, hogy az EU lépést tudjon tartani Kínával és az USA-val.[11] Európa legfőbb kihívása a technológiai függés csökkentése a két említett nagyhatalomtól.[12]

A magyar nemzetbiztonsági érdekek érvényesítését veszélyeztető aktuális kihívások és esetleges lehetőségek

A fejezetben a hazai szuverenitásvédelmet érintő aktuális kihívásokat mutatom be és kategorizálom. A főbb faktorokat az NBS-ben meghatározott kockázatok alapján állapítottam meg, illetve a PESTEL-elemzés szerint csoportosítottam őket.

Politikai tényezők

A PESTEL-analízisben vállalatokra vonatkozóan a politikai *(political)* tényezők között szerepelnek a törvényi előírások, az adópolitikai és a kormányzati stabilitás. Ezek érinthetnek egy vállalkozást, ugyanis egy váratlan adóemelés csökkentheti egy adott cég profitját.[13]

Az NBS 10. pontja deklarálja többek között a politikai stabilitást és függetlenséget, illetve a demokratikus jogrendet. Ezen alapvető érdekek védelme mentén meg lehet határozni azokat a kockázati faktorokat, amelyek Magyarország szuverenitását és biztonságát befolyásolják.

Az NBS-ben deklarált kockázatok közül kiemelendő jelen elemzés szempontjából a 68. pont: „Az állami és nem állami szereplők által szponzorált politikai, gazdasági és társadalmi folyamatok befolyásolására irányuló stratégiák száma, változatossága és hatásfoka növekszik."

Jelen fogalom egyértelműen a hadtudományban jól ismert kifejezésre, az információs műveletekre utal. Az információs műveletek az információért folyó küzdelem, olyan összehangolt tevékenységek, „amelyek a műveletek célkitűzéseinek elérése érdekében, kognitív képességekkel közvetlenül, illetve technikai képességekkel közvetetten hatásokat gyakorolnak a műveletekben részt vevő célközönség szándékára, helyzetértelmezésére és képességeire".[14] Az információs műveletek egyik típusa a kognitív információs műveletek, amelyek a humánumra fókuszálnak, az emberek és a társadalmi csoportok attitűdjét próbálják befolyásolni.[15]

[11] Von Brockdorff 2022.
[12] Tóth 2021: 31.
[13] Komáromi 2025.
[14] Haig 2018: 15.
[15] Haig 2018: 218.

Amennyiben a politikai destabilizáció a cél, akkor jelen részhez lehet még sorolni az egyes kritikus infrastruktúrák elleni támadásokat[16] vagy a terrorizmus jelenségét[17] is, mivel utóbbi „politikai, vallási vagy ideológiai célkitűzések elérése érdekében kormányok és társadalmak kényszerítésére vagy megfélemlítésére tett kísérletet, egyének vagy javak elleni erő vagy erőszak törvénytelen alkalmazása, illetve azzal való fenyegetés által".[18]

Gazdasági tényezők

A gazdasági tényezők a PESTEL-elemzés folyamatában alapvetően olyan változókat jelentenek, mint az infláció vagy a kamatlábak.[19] Jelen esetben az NBS-ben nevesített gazdasági vonatkozású kockázatokat összegezzük (például infláció és a munkaerővel kapcsolatos kihívások).

A történelmi előzmények is jól prezentálják, hogy a különböző gazdasági nehézségek a társadalmi konfliktusok kiéleződéséhez, illetve a radikális eszmék terjedéséhez vezetnek. A fentiek mellett kiemelendő a munkaerőhiány és a munkanélküliség, az előzőkből következő vagy azok mellett lévő társadalmi jelenségek, amelyek a gazdasági növekedést hátráltathatják.[20] Ezen tényezők kormányzati, állami szinten kezelendő kihívások, amelyekkel az NBS is kiemelten foglalkozik.[21] Nemzetbiztonsági szempontból fontos kiemelni a célzott gazdaságellenes állami és nem állami lépések felderítését és elhárítást, azonban a hírszerzés részéről megjegyzendő a hazai gazdaság erősítéséhez vezető információgyűjtő tevékenység is.

Társadalmi tényezők

A PESTEL-elemzés alapján – kifejezetten a vállalkozásokra vonatkozóan – a társadalmi tényezők magukban foglalják a demográfiai tényezőket, illetve az adott társadalom vallását, kultúráját is.[22] Egy állam biztonsági szempontjából a társadalmi tényezők, az azokra ható kockázati faktorok kiemeltnek számítanak, az NBS is számos kockázatot tartalmaz erre vonatkozóan, amit a következő alfejezetekben fejtek ki részletesen. Megjegyzem, hogy habár az elemzés során az egyes faktorok elkülönülnek, ezek komplexitása, egymásra hatása miatt nehezen szeparálhatók el a valóságban.

[16] NBS 124. *d)* pont.
[17] NBS 124. *m)* pont.
[18] Dobák 2011: 83.
[19] Komáromi 2025.
[20] Szűcs 2017.
[21] NBS 124. *h)* pont.
[22] Komáromi 2025.

Migráció és demográfia

A migráció egy alapvetően komplex kockázati faktor, tekintettel arra, hogy nem maga a jelenség, hanem a rá épülő bűncselekmények, tevékenységek vagy a következmények és a bekövetkező események azok, amelyek az igazi kockázatokat jelentik. A migrációra épülő tevékenységek lehetnek például a szervezett bűnözés, az okmányhamisítás, az embercsempészet. A migrációval összefüggő következmények is sokrétűek lehetnek, mint például az etnokulturális konfliktusok kiéleződése és a demográfiai eltolódás.[23] Tekintettel arra, hogy hazánk egyelőre tranzitország (a migránsok csak áthaladnak az országon, nem céljuk itt letelepedni), egyes bevándorlással érintett biztonsági faktorok csak áttételesen érintik, azonban nem lehet tudni – az elmúlt évek nemzetközi párbeszédeire alapozva –, mikor vezetnek be egy elosztási mechanizmust az Európai Unióban.[24] A szuverenitás fogalmából is következik, hogy az állam kizárólagos főhatalommal bír az általa irányított terület és az ott lakó népesség felett, továbbá maga választja meg kulturális és politikai rendszerét, amely külső befolyástól mentes. Ennek érdekében szükséges az ilyen irányú – nyílt vagy leplezett – törekvések felderítése és elhárítása, amely mind politikai, mind nemzetbiztonsági szinten kiemelt.

Amikor a migráció szóba kerül, sokan elfelejtik, hogy ez egy kétarcú jelenség: amennyiben van bevándorlás, akkor szükségszerűen van kivándorlás is. Magyarország szempontjából is kihívást jelentő probléma a tartósan külföldre távozó, főleg fiatal munkaerő, mivel ez negatívan érinti az adóbevételeket, illetve a nyugdíjrendszert is, hiszen a demográfiai csökkenés mellett a meglévő kivándorlás miatt egyre kevesebb adófizető termeli ki a növekvő nyugdíjállományt, ami hosszú távon akár a nyugdíjrendszer összeomlásához is vezethet. Jelen kategóriába kell még sorolni az úgynevezett „agyelszívás" jelenségét is, amely a magasan képzett munkaerő elvándorlását jelenti (ideértendők az orvosok, a mérnökök stb.).[25] Az NBS is kiemelt kockázati kategóriába sorolja a tartós népességfogyást és a lakosság átlagéletkorának folyamatos emelkedése miatt kritikus demográfiai helyzet kialakulását.[26] A kivándorlás és a népességcsökkenés a gazdaságra is negatív hatással van, hiszen a szakképzett vagy a magasan kvalifikált munkaerő (kiváltképpen a fejlődő iparágak, mint az IT területén) hozzájárul hazánk gazdasági növekedéséhez és stabilitásához. A politikai döntéshozatal megalapozottságához a titkosszolgálatok hozzá tudnak tenni, hiszen olyan szűk körben ismert információkat is képesek megszerezni, amelyek előmozdíthatják a hazai gazdaságot, és ez akár munkahelyet is teremthet.

[23] Póczik Szilveszter szerint ezek a kategóriák: demográfiai; egészségügyi; embercsempész-hálózatok; emberkereskedelem; etnikai bűnözés; etnokulturális különbségek; gazdasági kihívások; globális kényszermigráció; konfliktusok migrációja; korrupció; közbiztonsági kihívások; legalizációs cselekmények; okmánybiztonság, hamis okiratok; ötödik hadoszlop jelenség; politikai feszültségek, kihívások; szervezett bűnözés; szociális kihívások; terrorizmus; tiltott határátlépés; védelmi képesség gyengülése; vízumhoz kötődő visszaélések; xenofóbia, rasszista indítékú bűncselekmények. Póczik 2008: 18–74.

[24] Farkasa 2021.

[25] Csanády et al. 2008.

[26] NBS 124. *g)* pont.

Radikalizáció

Megfigyelhető jelenség a különböző radikális eszmék terjedése, mint a radikális iszlám, szélsőjobboldali nézetek, vagy éppen a szélsőbaloldali antifasiszta, radikális környezet- vagy állatvédelmi attitűd térhódítása. Ezek egymást gerjesztő folyamatok,[27] amit további faktorok erősítenek, mint a migráció jelensége vagy a gazdasági visszaesés. A társadalom radikalizációja nem csupán közbiztonsági kihívások elé állítja az adott államot, hanem szélsőséges esetben az ilyen csoportok akár az alkotmányos rend erőszakos megváltoztatása érdekében is felléphetnek, vagy a kritikus és/vagy állami infrastruktúra működését is megzavarhatják, amelynek felderítése és elhárítása nemzetbiztonsági feladat.[28] Továbbá az ilyen csoportok kapcsán felmerülhet a terrorista cselekmények elkövetése is, amely az NBS 124. *e)* pontja alapján kiemelt kockázatnak minősül.

A radikális csoportok kapcsán fontos megjegyezni, hogy a globalizációval és a digitalizációval azok is nemzetköziesedtek, így kiemelt jelentőségű a nemzetbiztonsági szolgálatok és a rendvédelmi szervek közötti hazai és nemzetközi kooperáció, illetve a radikális csoportok térnyerésének, szerveződésének online térben történő monitorozása, esetlegesen elhárítása különböző eszközökkel. Fontos továbbá kiemelni jelen alfejezetnél, hogy ezen csoportok külföldi állami és nem állami szervezetek általi erősítése még nagyobb kihívást jelent, és a hibrid (nem hagyományos) hadviselés eszköze lehet. Ezen csoportok felhasználása ilyen célból nem csupán társadalmi tényező, hanem a politikai tényezők közé is besorolható lehet.

Technológiai tényezők

A PESTEL-elemzés idesorolja, hogy milyen technológiák állnak rendelkezésre, és hogyan használhatók fel ezek egy vállalkozásban. A technológia fejlődése gyors ütemben zajlik, és fontos vele lépést tartani.[29] A technológiai tényezők egy állam szempontjából nem csupán kockázatot, hanem rendkívüli lehetőségeket is jelentenek, amelyeknek az esetleges alkalmazására külön fejezetben térek ki.

Jelen rész kapcsán hangsúlyozandó az NBS 124. *k)* pontja, amely kiemelt kockázatként nevesíti „a forradalmi technológiai fejlesztések illetéktelen kezekbe kerülésével a nemzet biztonságát veszélyeztető támadásokat vagy terrorcselekmények megjelenését". Az alábbiakban olyan forradalmi technológiákat ismertetek röviden, amelyek ellenérdekelt kézbe jutva komoly károkat tudnak okozni, és hátrányosan érinthetik hazánk szuverenitását.

[27] Murányi 2021.
[28] Nbtv. 5 § *b)* pont.
[29] Komáromi 2025.

Fokozódó digitalizáció

Manapság szinte minden információ átkerül a digitális térbe, az ez irányú fejlesztések egyre inkább észrevehetők a mindennapokban is. A fentiekhez kapcsolódóan kiemelendő az e-kormányzás, illetve e-közigazgatás is, amely az állami feladatok és szolgáltatások digitális térbe történő áthelyezését jelenti, de a számos lehetőség mellett kockázatot is hordoz magában. A fentiekhez kapcsolódóan az NBS is kiemelt kockázatként nevesíti a „jelentős károkat okozó kibertámadásokat a kormányzati informatikai rendszerek, az E-közigazgatás, a közműszolgáltatók, a stratégiai vállalatok, a létfontosságú infrastruktúra egyéb elemei és más, a társadalom működésében fontos szervezetek számítógépes hálózatai ellen".[30] Ez a jövőben is várhatóan fennálló, sőt növekvő problémakör, amely a biztonsággal foglalkozó intézmények technikai és humán felkészültségét is előirányozza.

Big data és mesterséges intelligencia

Big data alatt – ahogy a neve is sugallja – nagy mennyiségű adathalmazt, illetve *big data* elemzés alatt a nagy mennyiségű adat tárolását, feldolgozását, tisztítását és elemzését értjük.[31] Számos iparág alkalmazza, mivel olyan végtermék tud létrejönni egy jól elemzett adathalmazból, amely a nagyvállalatok, sőt az államok számára is igencsak értékes. A módszertanhoz kapcsolódó egyik legismertebb eset a Cambridge Analytica botrány, amikor a 2016-os amerikai elnökválasztás kapcsán felmerült, hogy a cég illetéktelenül hozzáfért 87 millió Facebook-felhasználó adataihoz, amelyeknek az elemzése és egy célzott stratégia által került hatalomra Donald Trump.

A mesterséges intelligencia (a továbbiakban: MI) alatt egy olyan speciális szoftvert értünk, amely az emberi értelemhez hasonlóan képes tanulni, fejlődni, feladatokat megoldani.[32] Az MI szorosan kapcsolódik a *big data* elemzéshez, mivel egyrészt egy jól működő MI-hez szükséges a nagy mennyiségű adat betáplálása, másrészt egy ilyen szoftver felgyorsítja az adatok feldolgozását, rendszerezését és elemzését.[33] Az MI-re az egyik legismertebb aktuális példa a ChatGPT, egy olyan *chatbot,* amely képes bonyolult feladatok megoldására, kérdések megválaszolására, és alkalmas lehet a hagyományos keresőmotorok forradalmasítására (például Google, Bing, Yandex stb.).[34]

A fentiekben nevesített technológiák azt is lehetővé tehetik, hogy külső felek befolyásolják akár a választásokat, vagy egyszerűen a közvéleményt olyan irányba tereljék, amely a radikális eszmék térnyerését segítené elő. Habár a módszertanok alkalmasak arra, hogy a bűnmegelőzési, bűnfelderítési, illetve nemzetbiztonsági tevékenységet segítsék, nem szabad elfelejtkezni az ellenérdekelt alkalmazás lehetőségéről sem.

[30] NBS 124. *d)* pont.
[31] Microsoft [é. n. b].
[32] Microsoft [é. n. a].
[33] Microsoft [é. n. b].
[34] Rádi 2023.

Kvantumszámítógépek

A kvantumszámítógépek kifejlesztése kapcsán hatalmas verseny folyik a világ fejlett államai között, figyelemmel arra, hogy ez a forradalmi technológia lehetővé teszi, hogy az eddig alkalmazott védelmi technológiák hatástalanok legyenek.[35] A kvantumszámítógépek fejlesztése és megszerzése minden állam érdeke, illetve az is, hogy olyan új védelmi technológiákat hozzanak létre, amelyek alkalmasak a kvantumszámítógépek által használt algoritmusok, kártékony kódok kivédésére. Így a fejlesztéssel kapcsolatos információk rendkívül szenzitívek, azok védelme, illetve megszerzése mindenképpen nemzetbiztonsági érdek, az ország szuverenitásának védelme szempontjából kiemelt jelentőségű.

Természeti tényezők

A PESTEL-elemzésben a környezeti tényezők magukban foglalják azt, hogy milyen környezeti problémák vannak. Példaképpen említhető az éghajlatváltozás vagy a természeti erőforrások hiánya.[36] A tanulmány szempontjából is kiemelt témakörnek tekinthetők a természeti tényezők, mivel sokszor olyan jellegű kockázatokat rejtenek magukban, amelyeket nehezen lehet előre látni, elhárításuk pedig össztársadalmi, sőt többnemzeti feladat is lehet.

Humán eredetű katasztrófák

Eklatáns magyarországi példaként[37] lehet felhozni jelen kategóriában a vörösiszap-katasztrófát,[38] de bármely, az emberre visszavezethető, nem környezeti eredetű probléma is idesorolandó, amely szándékosan vagy mulasztás által következik be. Jelen esetben az egyik legrosszabb forgatókönyvként lehet megnevezni az atomkatasztrófákat, amilyen a csernobili eset is volt. De a közelmúltbeli történéseket is lehet említeni, amikor felmerült annak a lehetősége, hogy ha az orosz–ukrán háború miatt az ukrán oldalon található zaporizzsjai erőművet támadás éri, az nukleáris katasztrófát okoz.[39] A fentiekre utaló információk gyűjtése kiemelt jelentőségű, hiszen előzetes információk nélkül nem készíthető fel a lakosság egy ilyen esemény bekövetkezésére (például jódtabletták szétosztásával).[40]

[35] NKI 2018.
[36] Komáromi 2025.
[37] NBS 124. *n)* pont.
[38] Sztojcsev 2020.
[39] Magyarországon egyelőre nem kell aggódni a zaporizzsjai atomerőmű miatt, de a helyzet nem megnyugtató 2022.
[40] Kornel 2024.

Klímaváltozás, elsivatagosodás, ivóvíz- és élelmiszerhiány

Jelen kategória önmagában is rendkívül súlyos tud lenni, hiszen a klímaváltozás alapvetően akár a bolygó élhetetlenné válásához is vezethet, a kialakult elsivatagosodás az élelmiszer és az ivóvíz hiányához, azok árának megemelkedéséhez, és ebben a kevésbé tehetős európai réteg is érintett lehet, nem beszélve a harmadik világbeliekről, akik végső elkeseredésükben útnak indulnak a fejlettebb államok felé, ami így visszamutat a migrációs kockázatokra. Már a 2020-as NBS is kiemelt kockázatként nevesítette a fentieket, de az idő előrehaladtával ez még inkább fokozódó kihívássá fog válni.[41] A nemzetbiztonság szerepe jelen kategóriában főként az új technológiák kapcsán merülhet fel, hiszen a fenti kihívásokat kezelő technológiák megszerzése, illetve a fejlesztés illetéktelen kézben történő megakadályozása már nemzetbiztonsági feladat lehet.

Energiahordozók és ritkaföldfémek hiánya

Az energiaimportban bekövetkezett fennakadásból fakadó ellátási válsághelyzet egyrészt létrejöhet[42] mesterségesen (az adott állam nem exportál valamilyen okból), vagy hosszú távon, természetes úton, hiszen a manapság használt energiahordozók a legtöbb esetben nem megújuló energiaforrások, így számuk véges. Ezért, illetve az egyes államoknál található energiaforrások nem egyenlő megoszlása miatt fontos az energiadiverzifikáció, ezek leggazdaságosabb módjainak megtalálása hírszerzési feladat is lehet. Továbbá a hazai energiaszektor kritikus infrastruktúrájának védelme mindenképpen titkosszolgálati feladat, ugyanis ellenérdekelt támadás bekövetkezhet akár a kibertérben, akár a valóságban mind állami és nem állami szereplők, mind esetlegesen radikális csoportok által.

Vírusok és betegségek

A Covid–19 okozta pandémiás helyzet óta tudjuk, hogy egy járvány milyen szintű kihívást tud okozni nemcsak egy állam, hanem az egész világ számára is. Az egészségügyi ellátórendszer túlterhelésén kívül a gazdasági kihívások is jelentősek voltak, számos iparágat rendkívül súlyosan érintettek a lezárások (például turizmus és vendéglátás stb.). A fentiekre tekintettel nem csoda, hogy a jogalkotó a kiemelt kockázatok közé sorolta „a lakosság tömeges és súlyos megbetegedésének kockázatát hordozó járványos betegség magyarországi megjelenését és gyors terjedését".[43] A titkosszolgálatok ezen a téren a kormányzat munkáját támogató információk megszerzését tudják végrehajtani (például oltások és egyéb egészségügyi felszerelések beszerzéséhez kapcsolódóan), de az elhárítás szempontjából releváns az álhírterjesztések megakadályozása is.

41 NBS 124. *q)* pont.
42 NBS 124. *i)* pont.
43 NBS 124. *o)* pont.

Környezeti eredetű katasztrófák

Az ipari katasztrófákhoz hasonló kategória, azonban ez nem humán, hanem környezeti eredetű. Magyarország természeti adottságaira tekintettel a hurrikán, a tengeri árvíz – amely általánosságban külföldön kiemelt kategória szokott lenni – nem kiemelt jelentőségű. Azonban már a különböző belvizek és a folyókhoz kapcsolódó árvizek, heves viharok kockázatot jelenthetnek,[44] ugyanakkor ezek kezelése alapvetően nem nemzetbiztonsági feladat, viszont az előrejelzést végző hivatalos szervek munkája befolyástól mentes működésének szavatolása már az lehet.

Jogi tényezők

Vállalati szempontból a jogi tényezők érintik a törvényeket és az előírásokat, amelyek befolyásolhatják egy adott cég működését. Ez magában foglalja például az adótörvényeket vagy a munkajogot.[45] Az NBS a jogi tényezők kapcsán is fogalmaz meg kijelentéseket biztonsági aspektusból, ezek kifejezetten a fentiekben már nevesített tényezők kapcsán felmerülő jogi szabályozatlanságokra utalnak, ilyen az NBS 159. pontja is, amely deklarálja a kibertérben jelentkező új típusú kockázatok kapcsán, hogy a technológiai és társadalmi háttér erősítésén túlmenően a kibertér jogi szabályozásának fejlesztése is célkitűzés.

Szintén a technológia (MI) kapcsán emeli ki az NBS 161. pontja, hogy koncentrálni kell a megfelelő jogi és felelősségi környezet kialakítására. Továbbá új típusú kockázatként jelent meg a nem hagyományos fizetőeszközök (kriptovaluták) nem kellő szabályozottsága is.[46]

Kiemelendő, hogy a nemzetközi jogi térben kockázatok megnevezésére is sor került, amelyek befolyásolhatják hazánk biztonsági környezetét, ilyen többek között a nemzetközi jog csökkenő kikényszeríthetősége,[47] vagy hogy a nagyhatalmi törekvések a nemzetközi jogot figyelmen kívül hagyják.[48]

Az ellenérdekelt (állami és nem állami) fél fentiekre ható tevékenysége

Habár jelen alfejezet inkább a politikai tényezők közé illene, a hagyományos PESTEL-elemzésen túlmutató helyet szántam neki, tekintettel, hogy az ilyen jellegű kockázati faktor a fentiekben már felsorolt tényezőkre alapul. Nemzetbiztonsági szempontból a legnagyobb relevanciával az bír, ha az egyes – előzőleg felsorolt és kifejtett – kockázatok nem véletlenszerűen, illetve önmaguktól következnek be, hanem külső befolyás által generálják őket, esetlegesen egy fennálló kihívást erősít meg egy másik fél. Ez lehet akár állami szereplő (Magyarországgal ellentétes érdekeltségű állam, állami

[44] NBS 124. *p)* pont.
[45] Komáromi 2025.
[46] NBS 76. pont.
[47] NBS 44. pont.
[48] NBS 52. pont.

hátterű hackercsoport stb.) vagy nem állami szereplő is (nem kormányzati szervezet, terrorista csoport, nem állami hátterű bűnözői, hackercsoport stb.). Akármilyen típusú kockázat erősítése, kialakítása egy másik fél által már nemzetbiztonsági kockázat, ami az ország szuverenitásának, külső befolyástól mentes működésének biztosítását indukálja. Az ilyen irányú esetleges tevékenység felderítése és elhárítása rendkívüli jelentőségű, az NBS úgy fogalmaz, hogy kiemelt kockázat az „összehangolt és széles körű diplomáciai, információs és titkosszolgálati műveletek, pénzügyi-gazdasági nyomásgyakorlással, pénzügyi spekulációs támadásokkal vagy katonai fenyegetéssel párosulva (hibrid) Magyarország destabilizálása, kormányzati cselekvőképességének, politikai stabilitásának és társadalmi egységének gyengítése, továbbá nemzetközi érdekérvényesítő képességének korlátozása céljából".[49]

Lehetséges szuverenitásvédelmi lépések a kockázatok mérséklésének érdekében

A fentiekben felsorolt kockázatok alapvetően össztársadalmi, illetve kormányzati lépéseket indukálnak, hiszen olyan szinten összefüggő és szerteágazó problémakörökről beszélünk, amelyek hatékony kezelése nem kivitelezhető csupán a nemzetbiztonsági szolgálatok vagy a rendvédelmi szervek által. Ahogy az NBS 126. pontja is fogalmaz: „A biztonság szavatolása érdekében elsődleges cél a nemzeti intézkedések hatékonyságának és rugalmasságának, valamint a nemzeti együttműködés szilárdságának erősítése. Az azonosított kihívások megelőzése, kezelése és elhárítása elsődlegesen nemzeti felelősség, amely a Kormány feladata, együttműködésben a társadalommal." Ugyanakkor szükséges lehet, hogy az egyes kockázatok elhárítása, megelőzése érdekében a hazai nemzeti biztonság szavatolásában részt vevő szervek (rendvédelmi szervek, honvédség, minisztérium stb.) különböző intézkedéseket, fejlesztéseket hajtsanak végre.

Magyarország szuverenitásának – beleértve a digitális szuverenitást is – védelme kapcsán kiemelendő, hogy jelen tevékenység nem kell hogy elsősorban reaktív legyen, hanem minél inkább a proaktív szemléletmód irányába kell elmozdulni. Ennek érdekében a hazai rendvédelmi szerveknek szükségszerűen emelniük kell munkájuk színvonalát, képességeiket fejleszteni kell, különös tekintettel az új típusú technológiákra. A 21. század információs kihívása nem az, mint korábban, hogy a rendelkezésre álló adatok szűkösek, hanem éppen ellenkezőleg, hatalmas mennyiségű adat keletkezik nap mint nap, azonban azok megszerzésén túlmenően rendkívüli kihívást jelent azok feldolgozása, szintetizálása, illetve hasznosítása.

A mesterséges intelligencia nem csupán kihívás lehet, hanem egyben lehetőség is, egyfajta kétélű pengeként jelentkezik. Az NBS 161. pontja is azt mondja, hogy „a mesterséges intelligencia szerepe a jelen és a jövő fejlesztései szempontjából rendkívüli jelentőségű, ezért ki kell terjeszteni alkalmazását. Koncentrálni kell azokat az infrastrukturális és humán erőforrásokat, amelyek megfelelő jogi és felelősségi környezet kialakításával lehetővé teszik a mesterséges intelligencia-alapú rendszerek

[49] NBS 124. *c)* pont.

fejlesztését és biztonságos üzemeltetését." Amennyiben Magyarország számára hozzáférhetővé válik egy olyan MI, amelynek használata biztonságos, és a nagy mennyiségű adathalmazokat segít rendszerezni és elemezni, akkor a fellelhető információkat hatékonyabban lehetne feldolgozni, későbbi hasznosításuk pedig hazánk szuverenitásának védelméhez is hozzájárulhat. A kérdéskör nehézségét okozza, hogy az ilyen MI-k fejlesztése idő-, energia- és forrásigényes, és általában csak a magasan kvalifikált munkaerővel és erős gazdasággal rendelkező országok tehetik meg. Azonban ha Magyarország egy ilyen szoftver megvételét tervezi, akkor számolnia kell azzal, hogy a felhasznált adatok esetlegesen kitettek lesznek a fejlesztő ország részére, akár egy tudatosan beépített kiskapu által, amely a feldolgozott adatokat továbbítja. Ilyen módon a digitális szuverenitás nemhogy nem valósul meg, hanem tovább sérül.

A fentiekre való tekintettel vagy olyan partnertől szükséges licenszt vásárolni, amelynek üzletfél-megbízhatósága nem megkérdőjelezhető, vagy szükségszerűen saját terméket kell fejleszteni. Álláspontom alapján, habár a második eset rendkívül idő-, költség- és energiaigényes, mindenképpen érdemes ezt a forgatókönyvet követni, hiszen egy ilyen jellegű szoftver rendvédelmi, illetve nemzetbiztonsági célú felhasználása roppant körültekintést igényel, ugyanis beláthatatlan következménye lehet, ha egy ilyen MI a magyar rendészeti intézményrendszer minden információs adatbázisához hozzáférne, és azt vagy annak elemzett formáját továbbítaná valamilyen illetéktelen félnek. De nem lehet eltekinteni hosszú távon, sőt már-már közép- és rövid távon sem egy ilyen szoftver beszerzésétől, mivel a rendkívüli mennyiségű adatállomány elemzése humán szinten nem kellőképpen hatékony. A hatékonyság csökkenése pedig azt eredményezheti, hogy egy releváns esemény bekövetkezése előtt nem lesz arra utaló ismeret, sőt, rosszabb esetben az utólagos felderítési tevékenységet is megnehezítheti. Fontos megjegyezni azonban, hogy további jogi, szakmai, illetőleg erkölcsi kérdést jelent a különböző adatbázisok összekapcsolása és esetlegesen azok kombinált elemzése, akár a mesterséges intelligencia segítségével.

Összegzés

Összességében megállapítható, hogy hazánkat és Európát számos kihívás és kockázat érinti a biztonság széles mezsgyéjén, amelynek kezelése, elhárítása rendkívül összetett, több szerv és akár nemzetek fokozott koordinációját teszi szükségessé. A biztonsági kihívások összefüggő láncolata miatt egy-egy elemet nem lehet szimplán önmagában értelmezni, hiszen azok egymást gerjeszthetik, indukálhatják. Álláspontom alapján az egyik legnagyobb lehetőség – a benne rejlő kihívások ellenére – a technológiai innovációk célirányos fejlesztése, illetve beszerzése, amellyel akár számos más kockázati faktor kezelhető, csökkenthető. A mesterséges intelligencia, a *big data* és a kvantumszámítógépek kapcsán a legnagyobb probléma lehet, amennyiben az adott állam nem áll a megfelelő fejlettségi szinten, így egy esetlegesen ellenérdekelt állam vagy piaci, illetve más szereplő a képességei által előnyösebb helyzetben lehet. Fontos kiemelni, hogy a digitális szuverenitás elérése nemcsak állami érdek, hanem egyéni is. A fentiek alapján a legfontosabb minimum a technológiai fejlődés szoros követése.

Felhasznált irodalom

A digitális szuverenitás jelentősége. *ICT Global,* 2023. szeptember 11. Online: https://ictglobal.hu/rovid-hirek/a-digitalis-szuverenitas-jelentosege/

Csanády Márton Tamás et al. (2008): A magyar képzett migráció a rendszerváltás óta. *Magyar Tudomány,* 169(5), 603–616.

Dobák Imre (2011): *Az uniós külső határok által kettéosztott Kárpátok Eurorégió biztonságföldrajzi elemzése.* PhD-értekezés. Pécs: PTE Földtudományok Doktori Iskola.

Farkasa (2021): Újra napirendre kerülhet az unióban a menekültkvóta. *Index,* 2021. január 6. Online: https://index.hu/kulfold/2021/01/06/menekultkvota_napirend_europai_unio/

Haig Zsolt (2018): *Információs műveletek a kibertérben*. Budapest: Dialóg Campus Kiadó.

Komáromi Zsombor (2025): PESTEL elemzés, PEST analízis példákkal. *Kanga Design,* 2025. január 10. Online: https://kangadesign.hu/pestel-elemzes.html

Kornel (2024): Katasztrófa esetén jódtabletta? *Kekjod,* 2024. december 13. Online: https://kekjod.hu/katasztrofa-eseten-jodtabletta/

Magyarországon egyelőre nem kell aggódni a zaporizzsjai atomerőmű miatt, de a helyzet nem megnyugtató. *VG,* 2022. augusztus 8. Online: www.vg.hu/energia-vgplus/2022/08/magyarorszagon-egyelore-nem-kell-aggodni-a-zaporizzsjai-atomeromu-miatt-de-a-helyzet-nem-megnyugtato/

Microsoft [é. n. a]: *Mit jelent a mesterséges intelligencia?* Online: https://azure.microsoft.com/hu-hu/resources/cloud-computing-dictionary/what-is-artificial-intelligence#%C3%B6nvezet%C5%91-aut%C3%B3k

Microsoft [é. n. b]: *Mit jelent a big data elemzés?* Online: https://azure.microsoft.com/hu-hu/resources/cloud-computing-dictionary/what-is-big-data-analytics

Mező Ferenc (2007): Az emberi szükségletekre irányuló lélektani műveletek (PSYOPS). *Hadtudomány,* 17(1), 121–125.

Murányi József Ignác (2021): A terror árnyékában. *Magyar Rendészet,* 21(3), 171–180. Online: https://doi.org/10.32577/mr.2021.3.12

NKI (2018): *A kvantumszámításban rejlő veszélyek.* Online: https://nki.gov.hu/it-biztonsag/hirek/a-kvantumszamitasban-rejlo-veszelyek/

Pató Viktória Lilla (2021): Európai Digitális Identitás, a biztonságosabb és ellenőrizhető személyi adattér. *NKE Európa Stratégia Kutatóintézet,* 2021. október 4. Online: https://eustrat.uni-nke.hu/hirek/2021/10/04/europai-digitalis-identitas-a-biztonsagosabb-es-ellenorizheto-szemelyi-adatter

Póczik Szilveszter (2008): A nemzetközi migráció tendenciái a 20. és a 21. században elméleti és történelmi nézőpontból. In Póczik Szilveszter – Dunavölgyi Szilveszter (szerk.): *Nemzetközi migráció – nemzetközi kockázatok.* Budapest: HVG-ORAC Lap- és Könyvkiadó Kft., 18–74.

Rabi Sándor (2009): *A vállalati környezet vizsgálata és a PEST elemzés kis-, középvállalati alkalmazása.* Online: www.veniens.hu/vallalatepito/2009/09/19/a-vallalati-kornyezet-vizsgalata-es-a-pestelemzes/

Rádi Balázs (2023): Egymásnak feszül a ChatGPT és a Google Bard. *Index,* 2023. február 7. Online: www.index.hu/gazdasag/2023/02/07/chatgpt-google-microsoft-mesterseges-intelligencia-keresomotor-bard/

Szűcs Gáborné (2017): Munkaerőhiány és munkanélküliség együttes jelenléte a munkaerőpiacon. Miben segíthet az oktatás a helyzet megoldásában? In Keserű Barna Arnold (szerk.): *Doktori Műhelytanulmányok 2017.* Győr: Széchenyi István Egyetem Állam- és Jogtudományi Doktori Iskola, 359–370. Online: https://dfk-online.sze.hu/images/egyedi/doktori/doktori%20m%C5%B1helytanulm%C3%A1nyok%202017/sz%C5%B1cs%20g.pdf

Tálas Péter [é. n.]: Szuverenitás. In *Közszolgálati Online Lexikon.* Online: https://lexikon.uni-nke.hu/szocikk/szuverenitas/

Tóth András (2021): Az Európai Unió (szabályozási) útja a szuverenitás felé az adatalapú gazdaságban. *Európai Tükör,* 24(2), 27–56. Online: https://doi.org/10.32559/et.2021.2.2

Sztojcsev Iván (2020): Tíz évvel a vörösiszap-katasztrófa után: a Mal Zrt. már nincs sehol, de jogerős ítéletre várni kell. *HVG,* 2020. október 3. Online: www.hvg.hu/gazdasag/20201003_vorosiszap_ajka_kolontar_devecser_evfordulo/

Von Brockdorff, Philip (2022): *Digitális szuverenitás: az EU digitalizációjának és növekedésének alapvető pillére (saját kezdeményezésű vélemény).* Európai Gazdasági és Szociális Bizottság. Online: https://op.europa.eu/hu/publication-detail/-/publication/119809e3-6502-11ed-9f85-01aa75ed71a1/language-hu

Jogi források

1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról
2023. évi LXXXVII. törvény a nemzeti szuverenitás védelméről
1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról

Tartalom