RENDŐRSÉGI TANULMÁNYOK

A RENDŐRSÉG TUDOMÁNYOS TANÁCSÁNAK FOLYÓIRATA

VIII. évfolyam 2025/2.

FELELŐS KIADÓ:
Dr. Németh József PhD rendőr ezredes, Rendőrség Tudományos Tanácsa elnök

KIADÓ
Rendőrség Tudományos Tanácsa
Cím: 1139 Budapest, Teve u. 4-6.
1903 Bp. Pf.: 314/15.
Telefon: +36 1 443-5533, BM: 33-355
Fax: +36 1 443-5784, BM: 33-884
E-mail: rtt@orfk.police.hu
Webcím: www.bm-tt.hu/rtt
HU ISSN 2630-8002 (online)

KÖZLÉSI FELTÉTELEK

A szerkesztőség olyan kéziratokat vár közlésre, amelyek a bűnmegelőzés, a bűnüldözés, a közbiztonság, a közrend, a határrendészet, a vezetés-irányítás és a mindenoldalú biztosítás kérdéseit elemzik, értékelik. A kéziratokon kérjük feltüntetni a szerző nevét, szolgálati helyét, beosztását, telefonszámát. Kérjük, hogy a cikkek szövegét e-mailben küldjék meg. A szerkesztőség a beérkezett kéziratot szakmai szempontból lektoráltatja, és fenntartja a jogot a kéziratok stilizálására, korrigálására, tipografizálására. A megjelenő írások nem a Rendőrség Tudományos Tanácsa, hanem a szerzők saját, tudományos szabadságán alapuló álláspontját képviselik. El nem fogadott kéziratot nem áll módunkban visszaküldeni. A szerkesztőség másodközlést nem vállal.

TARTALOM

2025/2.

SZERZŐK

2025/2.

DR. BEZERÉDI IMRE
PhD rendőr alezredes,
egyetemi docens,
parancsnokhelyettes,
Nemzeti Közszolgálati Egyetem
Rendészettudományi Kar
Rendvédelmi Tagozat

DR. HORVÁTH ORSOLYA MELINDA
óraadó,
Pécsi Tudományegyetem Állam- és Jogtudományi
Kar Büntető és Polgári Eljárásjogi Tanszék

DR. KARDOS SÁNDOR ISTVÁN
PhD rendőr alezredes,
címzetes egyetemi docens,
osztályvezető,
Országos Rendőr-főkapitányság
Személyügyi Főigazgatóság
Humánigazgatási Szolgálat
Fegyelmi Osztály

DR. PETRÉTEI DÁVID
osztályvezető,
Nemzeti Szakértői és
Kutató Központ
Daktiloszkópiai Szakértői Osztály

PROF. DR. EM. SALLAI JÁNOS
nyugállományú rendőr ezredes,
Nemzeti Közszolgálati Egyetem
Rendészettudományi Doktori
Iskola

DOI-azonosító: https://doi.org/10.53304/RT.2025.2.01

HORVÁTH ORSOLYA MELINDA

MI-re van szükség a jövőben?

Absztrakt
A rendészeti és bűnüldözési szervek hatékony működése kulcsfontosságú a közbiztonság és a jogállamiság fenntartásában, különösen a folyamatosan fejlődő technológiai környezetben. Kutatásunk a mesterséges intelligencia (MI) oktatásban betöltött szerepére fókuszál, kiemelten vizsgálva annak alkalmazási és fejlesztési lehetőségeit a rendészeti és bűnüldözési képzésben. A szakirodalmi áttekintés során azonosítottuk az MI-rendszerek előnyeit és kihívásait, figyelembe véve mind az oktatói, mind a hallgatói nézőpontokat. Az MI támogatja az inkluzív oktatást, a személyre szabott visszajelzéseket, valamint a nemzetközi együttműködést a rendészeti képzésben. Az oktatók számára hatékony eszközként szolgál a tanulási élmény fejlesztésére és a képzési stratégiák optimalizálására. Ugyanakkor az adatvédelmi és etikai aggályok, valamint a digitális függőség és a szociális kapcsolatok csökkenése jelentős kihívásokat jelentenek. A bűnüldözési célú oktatásban az MI alkalmazása még korlátozott, így szükséges további empirikus kutatások elvégzése annak érdekében, hogy a rendészeti képzés stratégiájába integrálható, célzott MI-megoldások szülessenek.

Kulcsszavak: mesterséges intelligencia, oktatás, bűnüldözés

Abstract
The effective operation of law enforcement and investigative agencies is crucial for maintaining public safety and the rule of law, especially in an ever-evolving technological environment. Our research focuses on the role of artificial intelligence (AI) in education, specifically examining its application and development potential in law enforcement and criminal justice training. Through a literature review, we identified the advantages and

challenges of AI systems from both the instructor's and the learner's perspectives. AI supports inclusive education, personalized feedback, and international cooperation in law enforcement training. For instructors, it serves as a powerful tool to enhance the learning experience and optimize training strategies. However, concerns regarding data protection, ethical considerations, digital dependency, and the potential decline in social interactions present significant challenges. The application of AI in law enforcement education remains limited, emphasizing the need for further empirical research to develop targeted AI solutions that can be effectively integrated into law enforcement training strategies.

Keywords: artificial intelligence, education, law enforcement

Bevezetés

A közbiztonság fenntartásában és a jogállamiság megőrzésében kiemelt szerep jut a hatékony rendőrség és bűnüldöző szervezetek számára. Az új technológiák és módszerek megjelenésével a bűnözés és maguk a bűnözők is változnak, ők maguk is a legújabb technológiákat alkalmazzák. A sikeres rendfenntartás eszköze így nem lehet más, mint szintén a legmodernebb technológiák, eszközök alkalmazása, beleértve a mesterséges intelligencia rendszereket, big data elemzések, digitális megfigyelési rendszerek alkalmazását is.

Ezen technológiák alkalmazásával a bűnügyi felderítés gyorsabb és pontosabb megvalósítása történhet meg. Az emberi hibák minimalizálhatók vagy kizárhatók, a reakcióidő csökkenthető. A bűnügyi adatok elemzésével a bűnmegelőzési szerepek is előtérbe kerülnek, proaktív intézkedések valósíthatók meg.

A technológiai fejlődés adta lehetőségek kihasználása egyben ezen eszközök megismerését, áttételes célokra történő felhasználását is jelenti. Egy technikailag támogatott és felszerelt rendőrségnek jól képzettnek is kell lennie, hogy hatékonyan legyen képes az állampolgárok biztonságát és szabadságát védeni a bűnözés visszaszorításával.

Az oktatási versenyképesség kulcsfontosságú szerepet játszik a gazdasági fejlődésben, a jövő generációjának sikerében. A fejlett oktatási technológiák alkalmazásával mind a tanulók, mind az oktatók előnyökhöz jutnak. A digitális tananyagok, különböző interaktív platformok, a mesterséges intelligencia alapú rendszerek képesek a diákok egyéni igényeihez, tanulási sebességéhez igazodni, személyre szabott tanulási élményt nyújtani. A legújabb technológiák segítik az olyan készségek fejlesztését, mint a kritikus gondolkodás, problémamegoldás, digitális írástudás, ezáltal is támogatva a későbbi munkaerőpiaci sikeres elhelyezkedést, érvényesülést. Akárcsak a bűnüldözési területen, úgy az oktatási rendszerek helytállása is része a globális versenynek. Egy hatékonyabb, rugalmasabb módszerekkel rendelkező oktatás biztosítja, hogy a végzettek versenyképes tudással lépjenek be a munka világába, ezáltal az adott országok is növeljék gazdasági versenyképességüket.

A kutatás célja és módszere

A bevezető alapján is megállapítható, hogy a modern technológiák alkalmazása versenyelőnyhöz juttathatja annak használóját. Ennek megfelelően a tanulmányban bemutatjuk a mesterséges intelligencia alkalmazásával azon oktatási lehetőségeket, melyek szűken értelmezve a bűnügyi oktatás hatékonyságát növelhetik, tágan értelmezve a rendészeti-jogi képzés fejlődését segíthetik elő, végső soron hozzájárulhatnak a közbiztonság, jogállamiság fenntartásához.

Kutatásunkban a desk research módszert hívtuk segítségül az alábbi kérdések megválaszolásához:

- Milyen jellemzőit ismerhetjük meg az MI alkalmazásának az oktatásban az előnyök és hátrányok vizsgálata mentén?
- A szakképzés és felsőoktatás (elérhető információk alapján rendészeti oktatás) területén milyen sajátosságok jellemzik az MI oktatásban betöltött szerepét?

- Mi jellemzi a bűnüldözés és az MI kapcsolatát? Milyen területeken alkalmazható felsorolás szintjén, példálózó jelleggel az MI a bűnüldözésben?
- Mi jellemzi a jogi oktatás és az MI kapcsolatát?
- Vannak-e elérhető információk, kutatási eredmények a bűnüldözési célú oktatás MI-használatáról?
- Milyen valós példák, jó gyakorlatok azonosíthatók?
- Milyen fejlesztési javaslatok, további kutatási lábak fogalmazhatók meg a fenti kérdések megválaszolását követően?

A kutatás során törekedtünk arra, hogy a rendelkezésre álló tudományos szakcikkek a legfrissebb kutatási eredményeket mutassák be. A kutatás limitációi között említhetjük, hogy a kutatás nem kíván részletesen foglalkozni az MI-stratégiák vizsgálatával sem nemzetközi, sem országos szinten, így azok említése kizárólag a téma szempontjából az értelmezéshez szükséges információkat tartalmazza majd. A kutatás továbbá nem vizsgálja az egyes bűnüldözési célú mesterségesintelligencia-rendszerek alkalmazhatósági kérdéseit (kritikus rendszerek), pusztán felsoroló jelleggel veszi górcső alá a felhasználási területeket. Szintén nem célja a kutatásnak a kutatási témában a kérdésekhez kapcsolódóan az eddig megjelent tudományos szakcikkek teljeskörű elemzése és feldolgozása (metaanalízis vagy review készítése). A tanulmány egy olyan összegző írást kíván közölni, mely a szakirodalmi áttekintést követően képes kijelölni a lehetséges javaslatokat, fejlesztési irányokat az oktatás területén, beleértve további kutatási lábak megvalósítási javaslatát.

Mesterséges intelligencia – fogalmi keretek, felhasználási területek

A gazdasági előrejelzések szerint 2030-ra közel tizenhatezer milliárd dolláros hozzájárulást okoz a mesterséges intelligencia használata a globális gazdaságban, melynek legnagyobb haszonélvezője Kína és az Egyesült Államok lesz. Az elemzés arra is rávilágít, hogy a technológiai előny megszerzésével új szereplők jelenhetnek meg a globális piacon, melyek ma

még nem léteznek, vagy jelentős versenyhátránnyal rendelkeznek, és ezt sikerül majd átlépniük.[1]

A mesterséges intelligencia (továbbiakban MI, vagy angolul artificial intelligence, AI) „olyan gyorsan fejlődő technológiacsalád", mely gazdasági és társadalmi előnyök generálását eredményezheti olyan területeken, mint például az egészségügy, pénzügyek, közszféra és belügy. Az EU AI Act[2] – mely 2024. augusztus elsején lépett hatályba – fogalmi meghatározása szerint MI-rendszerekről beszélhetünk, olyan szoftverről, melyet meghatározott technikák – mint például gépi tanulási, logikai, tudás alapú és statisztikai megközelítések – mentén fejlesztettek annak érdekében, hogy kimeneteiben tartalmakat, előrejelzéseket, ajánlásokat, döntéseket legyen képes generálni az emberi célkitűzéseknek megfelelően, ezáltal is kölcsönhatásba lépve környezetével, és befolyásolva azt. A gépi tanulási megközelítések alatt értjük a felügyelt, felügyelet nélküli és a megerősítő tanulást, többek között a mélytanulást (deep learning). A logikai és tudás alapú megközelítések a teljesség igénye nélkül említve magukba foglalják a tudásbázisokat, a következtetőmotorokat, a szimbolikus érvelést. A Bayes-féle becslés, az egyes keresési és optimalizálási módszerek végezetül a statisztikai megközelítések alá tartoznak. Az egyes megközelítések az AI Act 1. számú mellékletében olvashatók.

Az MI segítségével javíthatók az előrejelzések, optimalizálni lehet műveleteket, valamint olyan személyre szabott szolgáltatásokat lehet nyújtani, melyek képesek versenyelőnyt biztosítani alkalmazóik számára.

A generatív MI-rendszerek megjelenésével ma már könnyen és ingyenesen hozzáférhetőek sokak számára, így meglévő adatok alapján új szövegek, médiatartalmak, képek hozhatók létre a felhasználók által. Ilyen generatív MI-rendszerek például a ChatGPT, a DALL-E, a Bing AI stb. A generatív MI-rendszerek széleskörű hozzáférésével azonban a csalások és

[1] Sizing the prize What's the real value of AI for your business and how can you capitalise? Forrás: https://www.pwc.com/gx/en/issues/analytics/assets/pwc-ai-analysis-sizing-the-prize-report.pdf Letöltés ideje: 2024. 09. 15.

[2] Lásd részletesebben: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:32024R1689 Letöltés ideje: 2024. 09. 17.

kiberfenyegetések, támadások száma is jelentősen növekszik, a személyes adatok védelme sérülhet.

Az MI széleskörű alkalmazhatósága ugyanakkor hozzájárul az innováció elősegítéséhez, a hatékonyság növeléséhez. Az alábbi területeken hívhatjuk segítségül az MI-rendszereket – a teljesség igénye nélkül:

- Egészségügyi alkalmazás: orvosi diagnosztikai terület (például bőrrák azonosítása képfelismerő rendszerek segítségével vagy algoritmusok alkalmazásával).[3]
- Pénzügyi területen az MI segítségével azonosíthatók a csalások, kockázatelemzés végezhető, valamint személyre szabott tanácsadás is nyújtható bizonyos korlátok között. (Ugyanakkor szükséges kiemelni az érzelmi támogatás hiányát, mint az ügyfélkapcsolati élmény nyújtásának romlását.)[4]
- Autonóm járművek esetén valós idejű környezeti érzékelést tesznek lehetővé az alkalmazott szenzorok.[5]
- Az oktatás során személyre szabott tanulási anyagok készíthetők, egyéni visszajelzések adhatók a tanulók számára.[6]

[3] Tajerian A., Kazemian M., Tajerian M., Akhavan Malayeri A.: Design and validation of a new machine-learning-based diagnostic tool for the differentiation of dermatoscopic skin cancer images. 2023, PLoS ONE 18(4): e0284437.

[4] Boustani, N. M.: Artificial intelligence impact on banks clients and employees in an Asian developing country. Journal of Asia Business Studies 2022/2. szám. 267-278. o.

[5] Hozhabr Pour, H.; Li, F.; Wegmeth, L.; Trense, C.; Doniec, R.; Grzegorzek, M.; Wismüller, R. A. Machine Learning Framework for Automated Accident Detection Based on Multimodal Sensors in Cars. Sensors 2022/22. szám. 3634. o.

[6] Luckin, Rose., Holmes, Wayne., Griffiths, Mark., Forcier B.,Laurie.: Intelligence Unleashed. An argument for AI in Education. UCL Knowledge Lab, University College London, Pearson, 2016. 17-23. o.
Forrás: https://static.googleusercontent.com/media/edu.google.com/hu//pdfs/Intelligence-Unleashed-Publication.pdf
Letöltés ideje: 2024. 09. 30.

- A termelés optimalizálását segíti az MI alkalmazása a mezőgazdaságban, például a képfelismerés segítségével a növények egészségi állapotát vagyunk képesek azonosítani.[7]
- A gyártás területén segíti az automatizációt, a robotizált összeszerelést.[8]

Az MI alkalmazásának vizsgálata az oktatásban már több évtizedre tekint vissza a tudományos kutatásokban. A formális oktatás és az egész életen át tartó tanulás támogatása érdekében cél, hogy az MI elősegítse az olyan adaptív tanulási környezetek fejlesztését, melyek rugalmasak, inkluzívak, személyre szabottak és hatékonyak.[9]

Az MI szerepe az oktatásban

Az MI szerepe az oktatásban, akárcsak a kutatástámogatásban, megkérdőjelezhetetlen. A tanulási tapasztalatok és oktatási eredmények javításával kiemelt szerep jut a mesterséges intelligenciának. Alkalmazási előnyei mind társadalmi, gazdasági és egyéni hasznosság szintjén megjelennek. Integrációja azonban számos kérdést is felvet, melyek akár hátrányként, akár kihívásként is azonosíthatóak. Jelen rész az MI előnyeit és hátrányait mutatja be mind az oktatók, mind a hallgatók, tanulók oldaláról megközelítve.

[7] Kamilaris, A. and Prenafeta-Boldú, F. X.: Deep Learning in Agriculture: A Survey. Computers and Electronics in Agriculture. 2018, 147. szám. 70-90. o.
[8] Lee, J., Bagheri, B., & Kao, H. A.: A cyber-physical systems architecture for industry 4.0-based manufacturing systems. Manufacturing Letters 2018/3 szám. 18-23. o.
[9] Luckin, Rose., Holmes, Wayne., Griffiths, Mark., Forcier B., Laurie: Intelligence Unleashed. An argument for AI in Education. UCL Knowledge Lab, University College London, Pearson, 2016. 17-23. o. Forrás: https://static.googleusercontent.com/media/edu.google.com/hu//pdfs/Intelligence-Unleashed-Publication.pdf Letöltés ideje: 2024. 09. 30.

Az MI előnyei az oktatásban

A tanulói oldal előnyeire reflektálnak a legfrissebb kvalitatív elemzést alkalmazó (iparági jelentéseket, empirikus bizonyítékokat is magukba foglaló esettanulmányok áttekintése) kutatási eredmények,[10] miszerint az MI alkalmazása képes a tanulók tanulás iránti elkötelezettségét és ezáltal tanulási eredményeit javítani a személyre szabott és adaptív tanulási élmény biztosításával.

Szintén a tanulási eredmények javítását teszi lehetővé olyan tanulási környezet kialakítása, melyben az MI eszközök segítségével vetélkedőket hoznak létre, értékelik a hallgatói munkát a természettudományos oktatásban, ezáltal is bemutatva az MI szerepét az oktatási gyakorlatok és értékelési stratégiák kialakításában.[11]

A személyre szabott tanulás lehetősége mellett az MI elősegíti az oktatás inkluzivitásának megvalósítását is, azaz olyan személyre szabott támogatási formákat kínál, melyek nemcsak egyének, hanem speciális igényekkel rendelkező csoportok számára is megteremthetik az inkluzív oktatási környezetet. A tanulói tudás hiányosságának feltárásával a tanulási eredmények szintén javíthatók.[12]

Az oktatói oldalon a mesterséges intelligencia alkalmazásának előnyei mellett nevesíthetjük az adminisztratív támogatást, mely olyan oktatói feladatok automatizálását jelenti, mint az osztályozás és hallgatói értékelés. Ilyen és ehhez hasonló feladatok terheinek csökkentésével az oktatók a tényleges oktatási tevékenységük további fejlesztését tudják ellátni (például tantervfejlesztést), valamint támogatni tudják a hallgatói interakciókat

[10] Pandya, Dr Vishal and Monani, Dimpal and Aahuja, Divya and Chotai, Urjita, Traditional vs. Modern Education: A Comparative Analysis. IJRAR June 2024, Volume 11, Issue 2, p.172-174.
[11] Almasri, Firas. Exploring the Impact of Artificial Intelligence in Teaching and Learning of Science: A Systematic Review of Empirical Research. 2024, Res Sci Educ 54, p. 977–979. o.
[12] Farahani MS, Ghasmi G. Artificial Intelligence in education: Acomprehensive study. Forum for Education Studies. 2024; 2(2): 1379.

is.[13] Az adminisztratív feladatok támogatását jelenti még az olyan rutinfeladatok automatizációja is, mint például a hallgatók beiratkozásának, egyes kurzusainak az ütemezése a mesterséges intelligencia segítségével.[14]

Az MI-használattal olyan elemzések készíthetők, melyek képesek az egyes hallgatók tanulási mintázatait azonosítani, feltárni az egyéni hiányosságokat[15], és szükség esetén a beavatkozási pontokat is jelölik a prediktív hallgatói teljesítmények ismertetésével.[16] Utóbbira példaként hozhatjuk fel, hogy hazai kutatások (például BME-n) is zajlanak az MI-rendszerek támogatta köznevelésben és felsőoktatásban történő lemorzsolódás mintázatainak felismerésére. Elsősorban az oktatói oldalon emelhetjük ki az adatvezérelt betekintés előnyeit, ugyanakkor az egyéni tanulás, az LLL (life-long learning) térnyerésével hallgatói oldalon is lehetőségként jelenik meg az AI alkalmazása.

A nyelvi és kulturális akadályok leküzdése,[17] áthidalása, így a nemzetközi hallgatók oktatása és a globális oktatási környezet kialakítása is célként fogalmazható meg egyes oktatási stratégiákban. Emellett előnyként

[13] Ye., M., Zhunussov: The role of artificial intelligence in modern education: advantages, challenges and pathways to success. Manaš Ķozybaev atyndaġy Soltùstìk Ķazaķstan universitetìnìņ habaršysy. 2024. 180-188. doi: 10.54596/2958-0048-2024-2-180-188.

[14] Abiola Ajuwon, Enitan Shukurat Animashaun, Njideka Rita Chiekezie: Advancing human resources management practices in educational institutions: Enhancing teacher retention and student outcomes using AI. International Journal of Management & Entrepreneurship Research. 2024, 6 (8): 2488-2506. o., valamint Josephine Domingo-Alejo: AI Integrated Administration tool design with ML Technology for Smart Education System. Conference: 2024 4th International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE). 2024, May. 1423. o.

[15] Farahani MS, Ghasmi G. Artificial Intelligence in education: Acomprehensive study. Forum for Education Studies. 2024; 2(2): 1379. o. https://doi.org/10.59400/fes.v2i2.1379

[16] Ye., M., Zhunussov.: The role of artificial intelligence in modern education: advantages, challenges and pathways to success. Manaš Ķozybaev atyndaġy Soltùstìk Ķazaķstan universitetìnìņ habaršysy. 2024. 180-181. o. doi: 10.54596/2958-0048-2024-2-180-188.

[17] Elizabeth, Ango, Fomuso, Ekellem.: Enhancing Multicultural and Multilingual Education through Problem-Based Teaching with Conversational AI: A ChatGPT Perspective. 2024. doi: 10.36227/techrxiv.170593903.35081891/v1

azonosítható a chatbotok és virtuális mentorok, tutorok alkalmazása, melyek 0-24 órán keresztül elérhetők, így támogatva azonnali segítséggel a diákokat,[18] ezzel is elősegítve a tanulási hatékonyság növelését.

Az MI kihívásai az oktatásban

A hátrány megnevezés, amennyiben klasszikus SWOT-analízisben gondolkozunk megtévesztő lehet. Ennek oka, hogy ami hátrányként (threatenként, azaz veszélyként) értelmezhető az analízisben, az a technológiai fejlődés és kutatási megújulás természetéből kiindulva is esetünkben inkább értelmezhető lehetőségként (opportunity). Ennek megfelelően az alfejezetben azon kihívásokat (hátrányként azonosítható szempontokat) emeljük ki, melyek további kutatások mentén fejlesztési lehetőségként értelmezhetők. Mind az adatvédelmi, mind az etikai aggályok problémáival találkozhattunk már a hírekben, szakirodalomban. Az MI-rendszerek torzításának kezelése, valamint a megfelelő adatvédelem biztosítása komoly kihívásokat jelent az alkalmazók számára.[19]

A fejlett és modern oktatási rendszerek alkalmazásával, beleértve az MI oktatásba történő integrálását is, az oktatási infrastruktúrákhoz és digitális erőforrásokhoz történő hozzáférés jobban elmélyítheti az oktatási egyenlőtlenségeket. A digitális megosztás ezen problémakörével az MI-technológiák méltányos megvalósítása akadályokba ütközhet.[20]

Szintén kihívásként értelmezhető az oktatói felkészültség kérdésköre az MI használat során. Olyan képzéseket és támogatást (intézményi) szükséges biztosítani, mellyel az oktatók képesek hatékonyan integrálni a modern MI-technológiákat oktatási gyakorlatukba. Az oktatók MI-rendszerekre történő oktatása alkalmával is további lehetséges kihívásokra szükséges

[18] Lasha, Labadze., Lela, Machaidze: Role of AI chatbots in education: systematic literature review. 2023. p. 20. doi: 10.1186/s41239-023-00426-1
[19] Pandya, Dr Vishal and Monani, Dimpal and Aahuja, Divya and Chotai, Urjita, Traditional vs. Modern Education: A Comparative Analysis (June 24, 2024). IJRAR June 2024/2. szám. 172-173. o. doi: http://dx.doi.org/10.2139/ssrn.4876084
[20] Zhunussov (2024): i.m.

felhívni a figyelmet. Ilyen lehet például az innovációval szembeni ellenállás, mely az MI-vel kapcsolatos szkepticizmusban[21] ragadható meg. (Ilyen klasszikus érvek lehetnek: a kreativitás csökkentése, a kritikus gondolkodás megölése a szkepticisták körében.)

Másik oldalon tehát megjelenik az oktatók, tanárok MI-technológiák alkalmazására történő felkészítése, mely fundamentuma a hatékony alkalmazásnak. Egy szaúd-arábiai középiskolai tanárokat vizsgáló kutatás feltárta, hogy a tágabb oktatási környezet, beleértve a személyre szabott szakmai fejlődést, az infrastrukturális beruházások és átfogó szabályozás mellett elengedhetetlen az MI hatékony elsajátításában.[22]

További kihívásként azonosítható – bár nem az oktatói oldalon jelenik meg – a pénzügyi források rendelkezésre állásának hiánya. Ez egyrészről megjelölhető a beruházási igényekben,[23] valamint a meglévő hardverekhez és adatkészletekhez való korlátozott hozzáférésben is.[24] Kihívásként azonosítható továbbá, akárcsak más digitális eszközhasználatnál is, a technológiai függőség kialakulása a felhasználóknál. Az emberi interakció csökkenésével az optimális egyensúly megtalálása is szükségessé válik.[25]

[21] Natalia, Bobro: Advantages and disadvantages of implementing artificial intelligence in the educational process. Molodij včenij. 2024. 74. o. doi: 10.32839/2304-5809/2024-4-128-38.
[22] Ashwag, Almethen: Challenges in implementing artificial intelligence applications in secondary-level education: A teacher-centric perspective. Mağallaẗ Kulliyyaẗ Al-Tarbiyyaẗ (Print). 2024. doi: 10.21608/mfes.2024.270936.1776
[23] Bobro (2024): i.m.
[24] F., L., O., Wadsworth., Justin, R., Blaney., Matthew, Springsteen., Bob, Coburn., Nischal, Khanal., Tessa, Rodgers., Chase, Livingston., Suresh, Muknahallipatna: Frameworks and Challenges for Implementing Machine Learning Curriculum in Secondary Education. International journal of technology in education and science, 8(1). 2024. 164-181. o. doi: 10.46328/ijtes.531
[25] Labadze & Machaidze (2023): i.m.

Előnyök	Kihívások
Személyre szabott és adaptív tanulási élmény, javítja a tanulási eredményeket (Pandya, 2024)	Adatvédelmi és etikai aggályok (Pandya, 2024)
Inkluzív oktatás megvalósítása, speciális igényű csoportok támogatása (Farahani & Ghasmi, 2024)	Oktatási egyenlőtlenségek elmélyítése a digitális megosztás révén (Zhunussov, 2024)
Adminisztratív feladatok automatizálása, több idő az oktatási tevékenységek fejlesztésére (Malik, 2024)	Oktatói felkészültség hiánya az MI-rendszerek hatékony alkalmazására (Zhunussov, 2024)
Tanulási mintázatok azonosítása és prediktív elemzések a hallgatói teljesítmény javítására (Farahani & Ghasmi, 2024)	Innovációval szembeni ellenállás, szkepticizmus (Bobro, 2024)
Rutinfeladatok automatizálása (beiratkozás, kurzusok ütemezése) (Ajuwon et al., 2024)	Pénzügyi források hiánya az infrastruktúra fejlesztésére (Bobro, 2024)
Oktatók hallgatókkal való interakciójának támogatása (Malik, 2024)	Hardverekhez és adatkészletekhez való korlátozott hozzáférés (Wadsworth et al., 2024)
Nyelvi és kulturális akadályok leküzdése (Ekellem, 2024)	Technológiai függőség (Labadze & Machaidze, 2023)
Virtuális tutorok, chatbotok (Labadze & Machaidze, 2023)	Emberi interakció csökkenésének veszélye (Labadze & Machaidze, 2023)

1. számú táblázat
Az MI oktatási rendszerek előnyei és azzal kapcsolatos kihívások

Míg a mesterséges intelligencia átalakító potenciált kínál az oktatásban, kulcsfontosságú, hogy kezeljük ezeket a kihívásokat, és biztosítsuk előnyeinek méltányos elosztását. A kiegyensúlyozott megközelítés, mely magában foglalja az oktatók, a döntéshozók és a technológusok közötti együttműködést, elengedhetetlen az AI erősségeinek kiaknázásához, miközben csökkenti annak kockázatait.[26]

Összefoglalva elmondható, hogy az MI oktatásban történő alkalmazása eredményesebb tanulási környezetet, vonzó és hatékony színteret hozhat létre. Alkalmazásával lehetőséget teremt az automatizált osztályozásra, adaptív értékelésre, a kiterjesztett és virtuális valóság alkalmazására (AR- és VR-eszközök alkalmazása), az egyéni tanulási utak támogatására a teljesítmény előre jelzése mellett, akárcsak a nyelvtanulás segítésére.

Hogyan támogatja az MI a bűnügyi nyomozás oktatását?

A korábbi fejezetben olvashattuk, hogy az MI szerepe és előnyei vitathatatlanok az oktatásban. A köznevelés, szakképzés, felsőoktatás, felnőttképzés területén olyan eszközt kínál, mely egyrészt a tanulói értelmezést, feldolgozást támogatja, másrészt az oktatók fejlődését is elősegíti. Ennek megfelelően a bűnüldözéshez, bűnmegelőzéshez kapcsolódó tanulmányok során az MI-rendszerek alkalmazása szintén elősegíti az oktatási szereplők fejlődését, miközben gyakorlati haszna is elvitathatatlan.

Kettős funkciója (edukáció és bűnüldözés) szerint így képes egyszerre a bűnfelderítés hatékonyságát növelni, miközben sikeresen készíti fel a bűnüldöző személyzetet a modern rendőrség által megkívánt feladatok ellátására is. A fejezetben azokat a területeket vesszük alapul felsorolásszerűen, melyek mindkét funkcióhoz kapcsoltan értelmezhetők.

[26] Pandya (2024): i.m.

Adatelemzésekhez kapcsolódó támogatás

A bűnüldözési minták és trendek feltárásához, elemzéséhez elengedhetetlen a nagy mennyiségű adatok pontos és szakszerű feldolgozása, hiszen azok a megalapozott döntéshozatal és stratégiai tervezés fundamentumai.[27] Az adatokban rejlő – emberi szem számára láthatatlan – mintázatok, összefüggések, kapcsolatok a nyomozások tervezését, végső soron a közrend fenntartását is segítik.[28]

Az AI-eszközöket alkalmazzák az arcfelismerésben, a bűnözés előrejelzésében és az egyének nyomon követésében, amelyek nélkülözhetetlenek a modern rendőrségi és bűnmegelőzési stratégiákhoz.[29]

A nyomozási technikák fejlesztése

A mesterséges neurális hálózatok segítségével a szituációs adaptív tanulás, a nem nyilvánvaló kapcsolatok azonosításának képessége és a törvényszerűségek feltárása alkalmazásával olyan kulcsfontosságú művelettípusokat azonosítottak, melyek a kriminalisztika területén alkalmazhatók: a bűncselekmények és elkövetők azonosítása, előrejelzés és osztályozás.

A hálózat abban is támogatást nyújt, hogy a meglévő és feldolgozott adatok között olyan kapcsolat jöjjön létre, mely segíti a vizsgálatok értelmezését, a bűnügyi tanulmányok közötti kapcsolódási pontok feltárását és összekötését a hatékony ismeretelsajátítás érdekében.[30]

Jogi oktatás elősegítése

A jogi oktatást, a joganyag elsajátítását szintén segíti az MI. A jogi érvelés alapjainak megismerésével, a gyakorlati problémák megoldására történő

[27] Kuppala et al., Benefits of Artificial Intelligence in the Legal System and Law Enforcement. 2022. 2022 International Mobile and Embedded Technology Conference (MECON). doi: 10.1109/MECON53876.2022.9752352

[28] Diana, Stepanenko., Dmitry, Bakhteev., Yuliana, Evstratova: The Use of Artificial Intelligence Systems in Law Enforcement. 2020/14(2):206-214. doi: 10.17150/2500-4255.2020.14(2).206.

[29] Bag (2024): i.m.

[30] Stepanenko et al. (2024): i.m.

felkészítéssel a bűnüldözési kihívásokat támogatja. Az MI képes a rendelkezésre álló nagy mennyiségű információ big data összefüggésében feldolgozni azokat és az oktatási rendszerbe integrálni a gyakorlatot, mindezt kiváló eredménnyel. Egy kísérlet igazolta, hogy az MI-rendszert alkalmazó osztály átlaga magasabb volt, mint a hagyományos oktatási módszereket alkalmazó jogot hallgató osztályé. A jobb osztályzatok elérése mellett a kísérleti csoport résztvevői tanulmányi teljesítményének gyorsabb javulását is tapasztalták, ezzel is bizonyítva az MI hatékonyságát a jogi oktatásban.[31]

Akárcsak más területen, az MI-rendszerek bűnüldözési tárgyú tanulmányokban történő alkalmazásakor is felmerülnek azok az etikai aggályok, melyek elsősorban az adatvédelmi kérdésekhez kapcsolódnak, de ugyanúgy értelmezhetők az elfogultság kételye mentén, vagy a döntéshozatali folyamatok elszámoltathatóságának hiányával. Bag et al. (2024) tanulmányában külön felhívja a figyelmet az etikai normák egyensúlyának fontosságára és a tisztességes és igazságos bűnüldözési gyakorlat biztosítására.[32]

Konklúzió és javaslatok

A mesterséges intelligencia oktatásban való alkalmazása átfogó és mélyreható változást hoz a rendészeti és bűnüldözési képzésben, különösen az adaptív, személyre szabott tanulási folyamatok, a prediktív elemzések és az interaktív oktatási formák megjelenésével. A fentiek alapján elmondható, hogy a mesterséges intelligencia integrációja egyrészt az oktatók munkáját támogatja (adminisztráció, értékelés, tanulási mintázatok felismerése), másrészt a hallgatók elköteleződését és teljesítményét is képes javítani. Egyelőre azonban még csak a gyakorlati alkalmazások kezdeti fázisáról beszélhetünk, különösen a bűnüldözési és jogi oktatás területén. Az MI-rendszerek bevezetésével kiemelt figyelmet kell fordítani az adatvé-

[31] Li, Juan, Ma. (2022). Artificial Intelligence in Legal Education under the Background of Big Data Computation. 51-53. doi: 10.1109/ICCBE56101.2022.9888165
[32] Bag (2024): i.m.

delmi és etikai kérdésekre, a rendszerhasználatból eredeztethető infrastruktúrafejlesztésekre, nem utolsósorban az oktatók digitális kompetenciáinak megerősítésére.

Mindezeket figyelembe véve az alábbi javaslatok fogalmazhatók meg:

- Oktatási intézkedések szintje
  - Olyan képzési stratégiák kidolgozása, melyek figyelembe veszik az egyes szakterületi sajátosságokat (pl. jogi érvelés, bizonyítás kérdései, reaktív válaszlehetőségek, intézkedéstaktikai hangsúly stb.) és ennek megfelelően építenek be modulokat az MI működéséről, jogi kereteiről és alkalmazási lehetőségeiről az oktatásba.
  - Az oktatók, adminisztratív személyzet felkészítése és továbbképzése szintén egyik alapfeltétele az MI sikeres oktatási integrációjának. Az oktatói és adminisztratív személyzet kompetenciáinak fejlesztése érdekében rövid ciklusú, pedagógiai alkalmazási (beleértve az egyes didaktikai módszereknél alkalmazott lehetőségeket) és adminisztratív terhek csökkentését bemutató képzések, intézményi mentorprogram létrehozása szükséges, melynél a digitálisan kompetens kollégák segíthetik a technológiában kevésbé jártas oktatókat, személyzetet. Emellett fontos lehet olyan demokörnyezet biztosítása is, ahol szabadon kipróbálhatók a tanult alkalmazások, mielőtt azokat „éles" környezetben alkalmaznák. A demokörnyezet után pilotprogram indítása is megfontolandó, hogy az eredmények összehasonlíthatók (pre-post) és skálázhatók legyenek.
  - Az adatvédelmi kérdések kiemelten fontosak mind a tanulók, mind az oktatók körében, különösen a rendészeti oktatás még érzékenyebb jellegéből adódóan. Ennek megfelelően intézményi szinten szükséges olyan szabályzatok kialakítása, melyek biztosítják az adatok anonimitását, meghatározott esetekben az MI döntési mechanizmusainak átlátását (itt saját MI-rendszerek be-

tanításában is szükséges gondolkodni, lásd részletesebben a következő pontot), az alkalmazók beleegyezését az ilyen jellegű eszközök használatába (oktatási szabályzatok módosításán keresztül például).

– Fejlesztési és technológiai javaslatok
  - Az előző részben már elhangzott a pilotprogram alkalmazásának lehetősége, mely kiemelten fontos például a szimulációs feladatoknál[33] (esetmegoldó gyakorlatok, virtuális nyomozás stb.). A program keretein belül VR-alapú helyszínelési gyakorlatok, de akár egyéni igényekre szabott tanulási pályák, tananyagajánlások is alkalmazhatók. A programok segítségével tesztelhető és fejleszthető a működés, valamint a módszer elfogadottsága is fokozatosan integrálható az oktatási környezetbe.
  - Ahogy a leíró részben már utaltunk rá, az MI segítségével az egyes hallgatók tanulási mintázatai is azonosíthatók, így például beavatkozási pontokat lehet meghatározni a gyengébben teljesítő tanulóknál, hallgatóknál. A tanulási stílust is figyelembe véve külön tananyagajánlás alkalmazható, tanári támogatás is felajánlható. Utóbbi esetben kiemelendő, hogy hosszú távú cél lehet az oktatók szükségorientált támogatási rendszerének kidolgozása, mely célzottan segít, és nem kötelező jellegű tanórákhoz, kreditekhez rendelt konzultációt foglal magában. A személyre

[33] Egy hazai kutatás is megerősítette, hogy a szimuláció, szerepjáték olyan, rendvédelmi és honvédelmi tiszthelyettesi képzésben alkalmazott didaktikai módszer, melynek hatékonyságát magasra értékelték (90% felett) az ilyen képzést folytató tanintézetekben megkérdezettek. Emellett egy másik kérdőíves felmérés, mely a közrendvédelmi ág hivatásos állományú tagjait kérdezte, szintén megerősítette a módszer hatékonyságát, emellett az okos eszközök rendőr tiszthelyettesi képzésbe történő bevonásának szükségességét is. Lásd részletesebben Krauzer, Ernő: A rendőr tiszthelyettes képzés oktatás-módszertani fejlesztése. In: Szabó, Csaba & Molnár, Dániel (szerk.): Studia Doctorandorum Alumnae II. Budapest, Magyarország: Doktoranduszok Országos Szövetsége (DOSZ). 2023. 169-465. o.

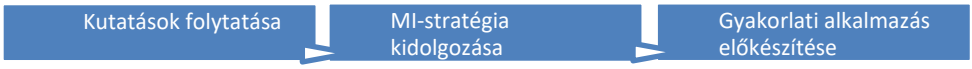
szabott tanulási utak kidolgozása a hosszú távú motiváció fenntartásához járulhat hozzá a tanulóknál.

- Az előző pontból is következik, hogy azokban az esetekben ott, ahol az oktatói feladatok alóli mentesítés lehetséges, alkalmazzunk MI-eszközöket. A 0-24 órában elérhető chatbotok ilyenek lehetnek például a kurzusinformációk, vizsgainformációk megválaszolására, egyes követelmények pontosítására. Ezek létrehozása egyszerű, nem igényel jelentős erőforrásokat, mégis segíti a tanulókat, hallgatókat az alapszintű információk közötti tájékozódásban.

– Jövőbeni kutatási irányok
  - A fent említett javaslatok megvalósítása magában foglalja az empirikus vizsgálatok megkezdését is. Azaz, szükséges, hogy olyan kvantitatív kutatások történjenek, melyek összevetik a különböző oktatási módszereket, különösen rendészeti kontextusban. Ennek megfelelően javasolt pre-post teszt alapú kutatások végzése, ezzel párhuzamosan a hallgatói-oktatói-adminisztratív személyzet attitűd- és elégedettségmérése is. Kvalitatív kutatási módszerrel pedig szükséges a mélyebb szintű dimenziókat is feltárni (lemorzsolódási kérdések, pályaelhagyás, motivációs kérdések).
  - Nemzetközi kitekintés keretein belül érdemes összehasonlítani és egyben feltárni az MI alapú rendszerek alkalmazási lehetőségeit a rendészeti képzésben, az ezekhez kapcsolódó szabályozási környezetet, és azt, hogy milyen kvantitatív eredmények állnak rendelkezésre a hatékonyság terén.
  - A hosszú távú hatékony integráció feltétele az alkalmazó környezet általi elfogadottság, így szükséges folyamatosan elégedettségi méréseket végezni, ami megakadályozza az esetlegesen fellépő félelmek tovagyűrűzését, az elvárások túlzó mértékű megjelenését. Az eredmények tükrében sikeres vezetői kommunikáció alkalmazható.

Összefoglalva elmondhatjuk, hogy az MI oktatásban történő alkalmazásával olyan paradigmaváltás figyelhető meg, mely a személyre szabottság és az adaptív tanulás irányába való közelítést foglalja magában. A gyakorlati alkalmazás, tapasztalatok gyűjtése azonban aktívan zajlik, ennek lehetünk szemtanúi. Ahhoz, hogy mind a gazdasági (globális versenybe kapcsolódás), társadalmi (rend, közbiztonság) és egyéni igényeket (életen át tartó tanulás, munkaerőpiaci sikeres elhelyezkedés) kielégítsük, figyelemmel az MI-rendszerek lehetséges kihívásaira, fontos, hogy mielőbb további kutatásokat folytassunk a fent javasoltak mentén.

Láthatjuk, hogy az EU AI Act tavaly lépett csak hatályba, ugyanakkor következő lépésként a nemzeti szabályozás, a keretrendszerek kialakítása fogja meghatározni a jogalkotók, döntéshozók és előkészítők feladatát. Az egyes színtereken – mint az oktatás – szintén változások várhatók a fejlődés elősegítése érdekében, a helyes szabályozás kialakításáért, melyet a generatív AI terjedése is sürget.



1. számú ábra
Oktatási célú MI-rendszerek kialakításának fázisai a rendészeti és bűnüldözési célú oktatásban

Irodalomjegyzék

Abiola Ajuwon, Enitan Shukurat Animashaun, Njideka Rita Chiekezie: Advancing human resources management practices in educational institutions: Enhancing teacher retention and student outcomes using AI. International Journal of Management & Entrepreneurship Research. 2024, 6 (8): 2488-2506. o.

Josephine Domingo-Alejo: AI Integrated Administration tool design with ML Technology for Smart Education System. Conference: 2024 4th International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE). 2024, May. 1423-1428. o.

Ashwag, Almethen. (2024). Challenges in implementing artificial intelligence applications in secondary-level education: A teacher-centric perspective. Mağallaẗ Kulliyyaẗ Al-Tarbiyyaẗ (Print),
DOI-azonosító: 10.21608/mfes.2024.270936.1776

Almasri, F. Exploring the Impact of Artificial Intelligence in Teaching and Learning of Science: A Systematic Review of Empirical Research. Res Sci Educ 54, 977–997 (2024).
DOI-azonosító: https://doi.org/10.1007/s11165-024-10176-3

Boustani, N.M. (2022), "Artificial intelligence impact on banks clients and employees in an Asian developing country", Journal of Asia Business Studies, Vol. 16 No. 2, 267-278. o.
DOI-azonosító: https://doi.org/10.1108/JABS-09-2020-0376

Diana, Stepanenko., Dmitry, Bakhteev., Yuliana, Evstratova. (2020). The Use of Artificial Intelligence Systems in Law Enforcement. 14(2): 206-214. o.
DOI-azonosító: 10.17150/2500-4255.2020.14(2).206-214

Elizabeth, Ango, Fomuso, Ekellem. (2024). Enhancing Multicultural and Multilingual Education through Problem-Based Teaching with Conversational AI: A ChatGPT Perspective.
DOI-azonosító: 10.36227/techrxiv.170593903.35081891/v1

EU AI Act.

Forrás: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:32024R1689

Farahani MS, Ghasmi G. Artificial Intelligence in education: Acomprehensive study. Forum for Education Studies. 2024; 2(2): 1379. o.
Forrás: https://doi.org/10.59400/fes.v2i2.1379

F., L., O., Wadsworth., Justin, R., Blaney., Matthew, Springsteen., Bob, Coburn., Nischal, Khanal., Tessa, Rodgers., Chase, Livingston., Suresh, Muknahallipatna. (2024). Frameworks and Challenges for Implementing Machine Learning Curriculum in Secondary Education. International journal of technology in education and science, 8(1):164-181. o.
DOI-azonosító: 10.46328/ijtes.531

Hozhabr Pour, H.; Li, F.; Wegmeth, L.; Trense, C.; Doniec, R.; Grzegorzek, M.; Wismüller, R. A Machine Learning Framework for Automated Accident Detection Based on Multimodal Sensors in Cars. Sensors 2022, 22, 3634. o.
DOI-azonosító: https://doi.org/10.3390/s22103634

Josephine, Domingo-Alejo. (2024). AI Integrated Administration tool design with ML Technology for Smart Education System. 42:1423-1428. doi: 10.1109/icacite60783.2024.10616455

Kamilaris, A. and Prenafeta-Boldú, F.X. (2018) Deep Learning in Agriculture: A Survey. Computers and Electronics in Agriculture, 147, 70-90. o.
DOI-azonosító: https://doi.org/10.1016/j.compag.2018.02.016

Kartik, S., Pandya. (2024): The role of artificial intelligence in education 5.0: opportunities and challenges. 5:e011-e011.
DOI-azonosító: 10.37497/sdgs.v5igoals.11

Krauzer, Ernő. (2023). A rendőr tiszthelyettes képzés oktatás-módszertani fejlesztése. In: Szabó, Csaba & Molnár, Dániel (szerk.), Studia Doctorandorum Alumnae II (169–465. o.). Budapest, Magyarország: Doktoranduszok Országos Szövetsége (DOSZ).

Kuppala et al., (2022): Benefits of Artificial Intelligence in the Legal System and Law Enforcement, 2022 May. 2022 International Mobile and Embedded Technology Conference (MECON).
DOI-azonosító: 10.1109/MECON53876.2022.9752352

Lasha, Labadze., Lela, Machaidze. (2023). Role of AI chatbots in education: systematic literature review. 20 o.
DOI-azonosító: 10.1186/s41239-023-00426-1

Lee, J., Bagheri, B., & Kao, H. A. (2018). A cyber-physical systems architecture for industry 4.0-based manufacturing systems. Manufacturing Letters, 3, 18-23. o.

Li, Juan, Ma. (2022). Artificial Intelligence in Legal Education under the Background of Big Data Computation. 51-53.
DOI-azonosító: 10.1109/ICCBE56101.2022.9888165

Luckin, Rose., Holmes, Wayne., Griffiths, Mark., Forcier B.,Laurie. Intelligence Unleashed. An argument for AI in Education. UCL Knowledge Lab, University College London, Pearson, 2016.
Forrás: https://static.googleusercontent.com/media/edu.google.com/hu//pdfs/Intelligence-Unleashed-Publication.pdf
Letöltés ideje: 2024.09.30.)

Mácsár Gábor: Felsőfokú rendészeti képzésben részt vevő hallgatók pályán maradásának és lemorzsolódásának kérdései. Doktori értékezés. https://disszertacio.uni-eszterhazy.hu/137/1/Disszert%C3%A1ci%C3%B3.pdf

Milad, Shahvaroughi, Farahani., Ghazal, Ghasmi. (2024). Artificial Intelligence in education: A comprehensive study. 2(3):1379-1379. doi: 10.59400/fes.v2i3.1379

Natalia, Bobro. (2024). Advantages and disadvantages of implementing artificial intelligence in the educational process. Molodij včenij, 72-76. doi: 10.32839/2304-5809/2024-4-128-38

Olanike, Abiola, Ajuwon., Enitan, Shukurat, Animashaun., Njideka, Rita, Chiekezie. (2024). Integrating AI and technology in educational administration: Improving efficiency and educational quality. Open access research journal of science and technology.

DOI-azonosító: 10.53022/oarjst.2024.11.2.0102

Pandya, Dr Vishal and Monani, Dimpal and Aahuja, Divya and Chotai, Urjita, Traditional vs. Modern Education: A Comparative Analysis (June 24, 2024). IJRAR June 2024, Volume 11, Issue 2, 172-183. o.
DOI-azonosító: http://dx.doi.org/10.2139/ssrn.4876084

Pervin, Kumar, Malik. (2024). The Role of Artificial Intelligence in Education: Opportunities and Challenges. Indian Scientific Journal Of Research In Engineering And Management,
DOI-azonosító: 10.55041/ijsrem35475

PWC (sz.n.) Sizing the prize What's the real value of AI for your business and how can you capitalise?
Forrás: https://www.pwc.com/gx/en/issues/analytics/assets/pwc-ai-analysis-sizing-the-prize-report.pdf

Rosemary Luckin, Wayne Holmes: Intelligence Unleashed: An argument for AI in Education. UCL Knowledge Lab, University College London. Pearson, 2016.

Tajerian A, Kazemian M, Tajerian M, Akhavan Malayeri A (2023) Design and validation of a new machine-learning-based diagnostic tool for the differentiation of dermatoscopic skin cancer images. PLoS ONE 18(4): e0284437.
DOI-azonosító: https://doi.org/10.1371/journal.pone.0284437

Ye., M., Zhunussov. (2024). The role of artificial intelligence in modern education: advantages, challenges and pathways to success. Manaš Ķozybaev atyndaġy Soltùstìk Ķazaķstan universitetìniņ habaršysy, 180-188. o.
DOI-azonosító: 10.54596/2958-0048-2024-2-180-188.

DOI-azonosító: https://doi.org/10.53304/RT.2025.2.02

BEZERÉDI IMRE

A felhasználói viselkedéselemzés szerepe a kibertámadások megelőzésében: rendészeti kihívások és lehetőségek a digitális korban

Absztrakt

A tanulmány a kiberbiztonság növekvő fontosságát vizsgálja a felhasználói viselkedéselemzés (User Behavior Analytics, UBA) kontextusában, fókuszálva a rendészeti kihívásokra. A digitális technológiák fejlődése új kockázatokat teremt, ahol a humán tényező kulcsfontosságúvá válik a védelmi rendszerekben. A kutatás feltárja a felhasználói viselkedés és kiberbiztonság összefüggéseit, elemzi a kibertámadások evolúcióját és a mesterséges intelligencia alkalmazási lehetőségeit. Megállapítja, hogy az emberi tényező a kiberbiztonság leggyengébb láncszeme, ugyanakkor a gépi tanulás és a mesterséges intelligencia jelentősen növelheti a fenyegetésdetektálás hatékonyságát. Kiemeli a rendszeres képzések, tudatosságnövelő programok és interdiszciplináris együttműködés fontosságát. Végkövetkeztetése, hogy a felhasználói viselkedéselemzés integrálása paradigmaváltást indíthat el a kiberbűnözés elleni védekezésben.

Kulcsszavak: kiberbiztonság, felhasználói viselkedéselemzés, rendészeti kihívások, mesterséges intelligencia

Abstract

The study examines the growing importance of cybersecurity through user behavior analysis (UBA), focusing on law enforcement challenges. The rapid development of digital technologies creates new risks where the human factor becomes crucial in defense systems. The research explores the relationships between user behavior and cybersecurity, analyzing cyber attack evolution and artificial intelligence application possibilities. It concludes

that the human element remains the weakest link in cybersecurity, while machine learning and Artifical Intelligence can significantly enhance threat detection efficiency. The study emphasizes the importance of regular training, awareness programs, and interdisciplinary cooperation. Its key conclusion suggests that integrating user behavior analysis can initiate a paradigm shift in combating cybercrime, offering a holistic approach to digital security challenges.

Keywords: cybersecurity, user behavior analysis, law enforcement challenges, artificial intelligence

Bevezetés

A rendészeti szférában régóta bevett gyakorlat az anekdotikus bölcsesség alkalmazása a bűncselekmények és más jogsértések szemléltetésére. Az egyik ilyen klasszikus körzeti megbízottaktól származó megállapítás szerint *„addig nincs baj, amíg nem lopnak mozdonyt, malomkövet vagy parazsat."* Míg ez a mondás a nem mindennapi, viszont egyszerű megítélésű és látható bűncselekményekre vonatkozott, a mai világban a fenyegetések egyre inkább láthatatlanok és szofisztikáltak. A technológiai fejlődés és a digitális világ térnyerésével a modern kor mozdonyai, malomkövei és a parázs már nem fizikai tárgyak, hanem adatok, informatikai rendszerek és digitális infrastruktúrák formájában jelennek meg.

A kibertámadások megelőzésének egyre nagyobb szerepe van mind az állami, mind a magánszektor védelmében, ahol a rendészeti eszközök és megközelítések új kihívásokkal néznek szembe. A bűncselekmények elkövetői egyre kifinomultabb technikákat alkalmaznak, gyakran kihasználva a felhasználói szokásokat és rendszeres viselkedési mintákat, nem pedig az anomáliákat. A támadók jellemzően a napi rutinra építenek, például olyan forrásokról küldenek adathalász e-maileket, amelyekről a felhasználók rendszeresen kapnak üzeneteket, így növelve a sikeres megtévesztés esé-

lyét. Ebben az új környezetben a felhasználói viselkedéselemzés (User Behavior Analytics, UBA) kiemelt fontosságúvá vált a rendészeti és kiberbiztonsági szférában egyaránt. A viselkedési minták alapos feltérképezése és a megszokottól való eltérések azonosítása kulcsfontosságúvá vált a digitális fenyegetések korai felismerésében és kezelésében.

A tanulmány célja, hogy áttekintést nyújtson a felhasználói viselkedéselemzés rendészeti alkalmazásáról a kibertámadások megelőzésében, különös tekintettel a belső fenyegetések felismerésére és a szociális manipuláció (social engineering) elleni védekezésre. Az információbiztonsági monitoring és az anomáliák detektálása kritikus eszköz lehet a rendőrség és más bűnüldöző szervek számára, amelyeknek egyre inkább szükségük van az új technológiák és eljárások bevezetésére a hatékony kiberbiztonsági feladataik ellátása érdekében. A bűnüldöző szervek számára különös nehézséget jelent, hogy lépést tartsanak a folyamatosan változó kibertérben megjelenő új fenyegetésekkel, ezért a kiberbiztonság területén alkalmazott innovatív megoldások és módszerek fontos szerepet képviselnek a hatékony védekezés szempontjából. Ahogy a támadások egyre inkább az emberi tényezőre, vagyis a felhasználói hibákra építenek, úgy válik egyre fontosabbá a felhasználói viselkedés elemzése a védekezési stratégiákban. A humán tényező és a kiberbűnözés közötti összefüggések mélyebb megértése nemcsak a megelőzés szempontjából fontos, hanem a bűnüldözés hatékonyságát is növelheti a digitális bűncselekmények elleni küzdelemben. A kutatás kitér a felhasználói viselkedési minták elemzésére, a technológiai és oktatási stratégiák szerepére, valamint a mesterséges intelligencia (MI) és a gépi tanulás (ML) lehetőségeire a kiberbiztonsági rendszerekben.

A kutatás célja

A kiberbiztonság egyre növekvő fontossága és a digitális infrastruktúrák folyamatos térnyerése révén a felhasználói viselkedés elemzése központi kérdés a kibertámadások megelőzésében. A digitális technológiák gyors fejlődése és azok széleskörű alkalmazása következtében a felhasználói sze-

rep kulcsfontosságúvá vált a kiberbiztonság fenntartásában. Ahogy a támadások egyre inkább célzottá válnak, a humán tényező, különösen a felhasználói viselkedés és az emberi döntéshozatal, döntő szerepet játszik a szervezetek és egyének kitettségében a kibertámadásokkal szemben.[1]

A gyakorlati tapasztalatok azt mutatják, hogy egyetlen figyelmen kívül hagyott biztonsági figyelmeztetés vagy egy gyanús e-mail megnyitása is elegendő lehet ahhoz, hogy egy szervezet teljes informatikai infrastruktúrája kompromittálódjon.[2] A kiberbiztonság területén az egyik legígéretesebb kutatási irányvonal a felhasználói viselkedéselemzés alkalmazása. Az UBA-rendszerek folyamatosan monitorozzák és elemzik a felhasználói tevékenységeket, képesek azonosítani a normál viselkedési mintákat, majd detektálni az azoktól való eltéréseket. Ez a megközelítés különösen hatékony a belső fenyegetések azonosításában, ahol a jogosult felhasználók tevékenysége jelenthet biztonsági kockázatot.[3]

A felhasználói tudatosság fejlesztése kulcsfontosságú eleme a hatékony kibervédelemnek.[4] A rendszeres és megfelelően strukturált képzések szignifikánsan növelik a szervezetek biztonsági szintjét. A digitalizáció térnyerésével és a globális hálózatok bővülésével a kibertámadások egyre szofisztikáltabbá válnak, ami növekvő fenyegetést jelent mind az állami, mind a magánszektor számára. Ez összhangban van a nemzetközi kutatási eredményekkel is, amelyek hangsúlyozzák a humán tényező jelentőségét a kiberbiztonságban.[5]

---

[1] Aldawood, Hussain – Skinner, Geoffrey: Reviewing cyber security social engineering training and awareness programs – Pitfalls and ongoing issues. Future internet, 2019, 11 (3), 73. sz.

[2] Verizon: 2023 Data Breach Investigations Report.
Forrás: https://www.verizon.com/business/resources/reports/dbir/ Letöltés ideje: 2024. 09. 28.

[3] Leitold Ferenc: A felhasználói viselkedés, mint információbiztonsági kockázat becslése. Konferencia-menedzselő rendszer, networkshop. 2019. Forrás: https://doi.org/10.31915/NWS.2019.24

[4] IBM: Cost of a Data Breach Report 2024. Forrás: https://www.ibm.com/reports/data-breach Letöltés ideje: 2024. 09. 12.

[5] Safa, Nader Sohrabi – Von Solms, Rossouw – Furnell, Steven: Information security policy compliance model in organizations. computers & security. 2016/56. szám. 70-82. o.

A viselkedéselemzésre és a tudatos felhasználói magatartásra oktatás, valamint a megfelelő szervezeti szabályrendszerek megalkotása kulcsfontosságúak lesznek a jövőbeni kiberbiztonsági rendszerekben, különösen egy olyan világban, ahol a felhasználói szokások és minták megfigyelése egyre gyakrabban válik támadások kiindulópontjává. Az olyan biztonsági kockázatok, mint a ChatGPT és más MI alapú eszközök vállalati használata sokszor tiltva vannak, mivel ezeken keresztül bizalmas adatok szivároghatnak ki, amikor a felhasználói tartalmak a szolgáltatás részévé válnak. A felhasználói viselkedés és a kiberbiztonsági kockázatok közötti összefüggések mélyebb megértése elengedhetetlen a hatékony védelmi mechanizmusok kialakításához. A felhasználói figyelmetlenség, a tudatosság hiánya és a rutinszerű viselkedésminták jelentős szerepet játszanak a kibertámadások sikerességében, különösen a szociális manipulációval és belső fenyegetésekkel szemben.[6] Az emberi tényező kiemelt fontosságú a modern kibertámadásokban, ahol a támadók gyakran pszichológiai manipulációt alkalmaznak céljaik elérése érdekében.[7]

Az UBA és az MI alkalmazása hozzájárulhat a kibertámadások proaktív felismeréséhez és megelőzéséhez. Ezek a technológiák lehetővé teszik a normál felhasználói viselkedéstől való eltérések automatikus detektálását, ami kulcsfontosságú a potenciális fenyegetések korai szakaszban történő azonosításában.[8] A felhasználói tudatosság fejlesztésére irányuló programok hatékonyságának növelése érdekében fontos a képzési módszerek fo-

[6] Bányász Péter – Bóta Bettina – Csaba Zágon: A social engineering jelentette veszélyek napjainkban. In: Biztonság, szolgáltatás, fejlesztés, avagy új irányok a bevételi hatóságok működésében. Magyar Rendészettudományi Társaság Vám- és Pénzügyőri Tagozat. Budapest, 2019. 12-37. o.

[7] Hadnagy, Christopher: Social engineering: The science of human hacking. John Wiley & Sons. 2018.

[8] Kumaraguru, Ponnurangam – Sheng, Steve – Acquisti, Alessandro – Cranor, Lorrie Faith – Hong, Jason: Teaching Johnny not to fall for phish. ACM Transactions on Internet Technology (TOIT), 2010, 10.2: 1-31. o.

lyamatos fejlesztése és személyre szabása. Az interaktív és gyakorlatorientált megközelítések különösen hatékonynak bizonyultak a kiberbiztonsági ismeretek átadásában és a helyes viselkedésminták kialakításában.[9]

A kutatásom célja mindezek alapján:

1. Feltárni a felhasználói viselkedés és a kiberbiztonság közötti komplex összefüggéseket, különös tekintettel arra, hogy az emberi tényező miként válik kulcsfontosságúvá a kibertámadások megelőzésében és a szervezetek biztonságának fenntartásában.
2. Tanulmányozni a kibertámadások evolúcióját és növekvő szofisztikáltságát a digitalizáció és a globális hálózatok bővülésének kontextusában, rávilágítva arra, hogy ez milyen kihívásokat jelent mind az állami, mind a magánszektor számára a jövő kiberbiztonsági rendszereinek fejlesztésében.
3. Elemezni a User Behavior Analytics (UBA) rendszerek és az MI alkalmazásának lehetőségeit a kibervédelemben, vizsgálva, hogy ezek a technológiák hogyan járulhatnak hozzá a normál felhasználói viselkedéstől való eltérések automatikus detektálásához és a potenciális fenyegetések korai felismeréséhez.
4. Megvizsgálni a felhasználói tudatosság fejlesztésére irányuló programok hatékonyságát, valamint feltárni azokat a komplex stratégiákat, amelyek a felhasználók viselkedésének tudatos formálását célozzák, figyelembe véve, hogy a technológiai megoldások önmagukban nem elegendőek a kiberbiztonság fenntartásához.

Ezen kutatási célok átfogó keretet adnak a tanulmány témáinak és kérdéseinek, lehetővé téve a kiberbiztonság és a felhasználói viselkedés elemzésének mélyebb megértését. A kutatás célja, hogy hozzájáruljon a kiberbiztonsági stratégiák fejlesztéséhez és a potenciális fenyegetések elleni védekezés erősítéséhez, figyelembe véve az emberi tényezőt és a technológiai

[9] Bada, Maria – Sasse, Angela M. – Nurse, Jason RC: Cyber security awareness campaigns: Why do they fail to change behaviour? arXiv preprint arXiv:1901.02672, 2019.

innovációt egyaránt. A kutatás nemcsak a kiberbiztonsági fenyegetésekre adott válaszok kidolgozásában, hanem a biztonsági kultúra és tudatosság fejlesztésében is fontos szerepet játszik. A javasolt intézkedések és stratégiák integrálása segíthet a kiberbűnözés elleni küzdelem hatékonyságának növelésében, hozzájárulva egy biztonságosabb digitális ökoszisztéma kialakításához.

Irodalmi áttekintés

A felhasználói viselkedés elemzésének elméleti alapjai

A felhasználói viselkedés elemzése (UBA) egy viszonylag új és innovatív megközelítés a kiberbiztonság területén, amely az emberi tényezőre helyezi a hangsúlyt a technológiai biztonsági intézkedések mellett. Ez a módszer jelentős paradigmaváltást jelent a hagyományos kiberbiztonsági szemlélethez képest, amely korábban elsősorban technikai jellegű kihívásként kezelte a problémát, és főként az infrastruktúra, valamint az információk védelmére koncentrált a rosszindulatú programok, hálózati támadások és egyéb technikai fenyegetések ellen.[10]

Az elmúlt évtizedekben azonban egyre nyilvánvalóbbá vált, hogy a technikai védelem önmagában nem elégséges a komplex kiberbiztonsági kihívások kezelésére. A felhasználók hibái, figyelmetlensége, vagy akár szándékos károkozása olyan jelentős kockázati tényezőket jelentenek, amelyeket a hagyományos technológiai megoldások nem képesek megfelelően kezelni.[11] Ez a felismerés vezetett a felhasználói viselkedés, mint potenciális biztonsági fenyegetésforrás intenzívebb vizsgálatához a kiberbiztonsági kutatásokban. A felhasználói viselkedés elemzésének elméleti alapja azon a feltételezésen nyugszik, hogy a felhasználók tevékenységei –

[10] Muha Lajos – Krasznay Csaba: Az elektronikus információs rendszerek biztonságának menedzselése. Nemzeti Közszolgálati Egyetem. Budapest, 2018.
[11] Verizon: 2023 Data Breach Investigations Report. Forrás: https://www.verizon.com/business/resources/reports/dbir/ Letöltés ideje: 2024. 09. 28.

legyenek azok normálisak vagy a megszokottól eltérőek – értékes információkat szolgáltatnak a potenciális fenyegetésekről és biztonsági problémákról.[12] Ez az elmélet szorosan kapcsolódik a viselkedési mintázatok felismerésének és elemzésének koncepciójához, amely a pszichológia és a kognitív tudományok területéről származik.[13] Az UBA-rendszerek elsődleges célja, hogy folyamatosan monitorozzák és elemezzék a felhasználói tevékenységeket, azonosítva azokat a viselkedési mintákat, amelyek eltérnek a megszokottól, és potenciálisan egy kibertámadás vagy biztonsági incidens előjelei lehetnek. Ez a megközelítés lehetővé teszi a proaktív védekezést, szemben a hagyományos, reaktív biztonsági intézkedésekkel.

Az UBA-rendszerek működésének elméleti alapja a normál viselkedési minták meghatározása és az ezektől való eltérések detektálása. Ez a folyamat magában foglalja a nagy mennyiségű felhasználói adat gyűjtését, elemzését és értelmezését, amihez fejlett adatelemzési és ML-algoritmusokat alkalmaznak.[14] Az anomália-detekció során ezek a rendszerek képesek azonosítani olyan subtle, azaz árnyalatnyi eltéréseket is, amelyek emberi elemzők számára észrevétlenek maradnának.[15] A felhasználói viselkedés elemzésének egyik kulcsfontosságú elméleti aspektusa a kontextuális információk figyelembevétele. A rendszerek nem csak izolált eseményeket vizsgálnak, hanem figyelembe veszik a felhasználó szerepkörét, munkakörét, szokásos tevékenységi mintáit és az adott szervezeti környezetet is. Ez az

[12] Bányász Péter – Bóta Bettina – Csaba Zágon: A social engineering jelentette veszélyek napjainkban. In: Biztonság, szolgáltatás, fejlesztés, avagy új irányok a bevételi hatóságok működésében. Magyar Rendészettudományi Társaság Vám- és Pénzügyőri Tagozat. Budapest, 2019. 12-37. o.

[13] Kovács László – Krasznay Csaba: Digitális Mohács 2.0: kibertámadások és kibervédelem a szakértők szerint. Nemzet és Biztonság–Biztonságpolitikai Szemle 10.1. 2017. 3-16. o.

[14] Szádeczky Tamás: Big Data a közigazgatásban. In: Sasvári, Péter (szerk.): Informatikai rendszerek a közszolgálatban. Ludovika Egyetemi Kiadó. Budapest, 2020. 113-126. o.

[15] Bederna Zsolt – Váczi Dániel – Pollner Péter – Szádeczky Tamás: Támadás hálózatba szervezve. In: Auer, Ádám; Joó, Tamás (szerk.): Hálózatok a közszolgálatban. Dialóg Campus Kiadó. Budapest, 2019. 223-247. o.

átfogó megközelítés lehetővé teszi a fals pozitív riasztások számának csökkentését és a valódi fenyegetések pontosabb azonosítását. Az UBA-rendszerek elméleti alapjainak fontos része a folyamatos tanulás és adaptáció koncepciója.[16]

Mivel a felhasználói viselkedés és a kiberbiztonsági fenyegetések állandóan változnak, ezek a rendszerek folyamatosan frissítik és finomítják modelljeiket az új adatok és tapasztalatok alapján.[17] Ez a dinamikus megközelítés biztosítja, hogy az UBA-rendszerek hatékonyan alkalmazkodjanak az evolválódó fenyegetési környezethez. A felhasználói viselkedés elemzésének elméleti alapjai egy komplex, multidiszciplináris megközelítést tükröznek, amely integrálja a kiberbiztonsági ismereteket, a viselkedéstudományokat és a fejlett adatelemzési módszereket. Ez az innovatív megközelítés lehetővé teszi a szervezetek számára, hogy hatékonyabban azonosítsák és kezeljék a felhasználói viselkedésből eredő biztonsági kockázatokat, kiegészítve és megerősítve a hagyományos technológiai védelmi megoldásokat.[18]

A felhasználói viselkedés szerepe a kiberbiztonságban

A felhasználói viselkedés elemzése (UBA) egy viszonylag új megközelítés a kiberbiztonságban, amely az egyes felhasználók általános viselkedési mintáinak elemzésén alapul. Az UBA-rendszerek a felhasználók normális tevékenységét monitorozzák, majd ezeket az adatokat felhasználják az anomáliák és potenciális támadások azonosítására. Ez a technika különösen

[16] Leitold Ferenc: Practical approach for measuring the level of user behaviour. In: 2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA). IEEE, 2019. 1-2. o.

[17] Legárd Ildikó: Célpont vagy! -a közszolgálat felkészítése a kiberfenyegetésekre." Hadmérnök 15.1. 2020. 91-105. o.

[18] Homoliak, Ivan – Toffalini, Flavio – Guarnizo, Juan – Elovici, Yuval – Ochoa, Martina: Insight into insiders and it: A survey of insider threat taxonomies, analysis, modeling, and countermeasures. ACM Computing Surveys (CSUR), 52(2), 2019. 1-40. o.

hatékony a belső fenyegetések felismerésében, amikor a támadások a jogosult felhasználók fiókjain keresztül történnek.[19]

Az UBA-rendszerek különösen hatékonynak bizonyulnak a belső fenyegetések azonosításában, különösen akkor, amikor a támadások legitim felhasználói fiókokon keresztül történnek.[20] Az ML integrálása jelentős előrelépést hozott ezen a téren, mivel AI alapú rendszerek 85%-os pontossággal képesek előre jelezni a potenciális biztonsági incidenseket, meghaladva a hagyományos módszerek hatékonyságát.[21] Ez a megközelítés összhangban van a nemzetközi trendekkel, melyek az ML alkalmazásának növekvő jelentőségét hangsúlyozzák a kiberbiztonság területén.[22] A felhasználói tudatosság növelése kritikus tényező a hatékony kiberbiztonság megvalósításában, mivel a rendszeres képzések és szimulált támadási gyakorlatok akár 60%-kal is csökkenthetik a sikeres social engineering támadások arányát. Egy longitudinális vizsgálat szerint a szervezeti biztonsági kultúra kialakítása és fenntartása jelentős mértékben hozzájárul a kibertámadások megelőzéséhez.[23] A gyakorlati megoldások közé tartoznak a szimulált adathalász támadások is, amelyek lehetőséget biztosítanak a felhasználók számára, hogy kockázatmentes környezetben tanulják meg felismerni a potenciális fenyegetéseket. Ezek a képzések nemcsak az elméleti tudás átadását, hanem a valós életben alkalmazható készségek fejlesztését is célozzák,

[19] Hadarics Kálmán: Incidens-menedzsment gyakorlat. Nemzeti Közszolgálati Egyetem. Budapest, 2019.
[20] Arohan, Yash – Yadav, Ashwin – Pandey, Aakash – Churi, Shardul – Saxena, Manvi – Vaghani, Akshit: An introduction to context-aware security and User Entity Behavior Analytics. International Journal of Advance Research, Ideas and Innovations in Technology, 2020, 6.5: 27-33. o.
[21] Liu, Fucheng – Wen, Yu – Zhang, Dongxue – Jiang, Xihe – Xing, Xinyu – Meng, Dan: Log2vec: A heterogeneous graph embedding based approach for detecting cyber threats within enterprise. In: Proceedings of the 2019 ACM SIGSAC conference on computer and communications security. 2019. 1777-1794. o.
[22] Buczak, Anna L. – Guven, Erhan: A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications surveys & tutorials, 2015, 18.2: 1153-1176. o.
[23] Abawajy, Jemal: User preference of cyber security awareness delivery methods. Behaviour & information technology, 2014, 33.3: 237-248. o.

összhangban az adathalászat elleni képzések hosszú távú hatékonyságát vizsgáló nemzetközi kutatásokkal.[24] A felhasználói viselkedéselemzés lehetőséget nyújt a kockázatok előrejelzésére, miközben a felhasználók oktatása és tudatosságának növelése csökkentheti a támadások sikerességét. A jövőbeni kutatásoknak a felhasználói viselkedés finomabb elemzésére és az algoritmusok továbbfejlesztésére kell összpontosítaniuk, hogy a védekezési rendszerek még proaktívabbá váljanak. Egyes kutatások rámutatnak, hogy a felhasználók tevékenységeinek szisztematikus elemzése kulcsfontosságú információkat szolgáltat a potenciális fenyegetésekről, lehetővé téve a proaktív védekezést és a biztonsági incidensek korai felismerését.[25]

A felhasználói viselkedéselemző rendszerek elsődleges célja a normálistól eltérő viselkedési minták azonosítása, amelyek potenciálisan kibertámadások vagy biztonsági incidensek előjelei lehetnek. A szociális manipulációs technikák, mint például az adathalászat, azon az alapvető pszichológiai megfigyelésen alapulnak, hogy a felhasználók bizonyos körülmények között könnyen befolyásolhatók, és hajlamosak figyelmen kívül hagyni a biztonsági protokollokat, különösen, ha egy jól felépített megtévesztéssel találkoznak. Ez a jelenség összhangban van a social engineering támadások pszichológiai mechanizmusait részletesen vizsgáló kutatásokkal. A szervezeti kultúra és a személyes attitűdök kulcsfontosságú szerepet játszanak a biztonsági magatartás kialakításában. Magyarországon végzett kutatások szerint a szervezetek jelentős része nincs megfelelően felkészülve a modern kiberfenyegetések felismerésére és kezelésére, ami kritikus sebezhetőséget jelent a célzott támadásokkal szemben. A hazai vállalatok gyakran alábecsülik a kiberbiztonság jelentőségét, és nem fordítanak elegendő erőforrást a védelmi rendszerek fejlesztésére és a munkavállalók oktatására. A prob-

[24] Kumaraguru, Ponnurangam – Sheng, Steve – Acquisti, Alessandro – Cranor, Lorrie Faith – Hong, Jason: Teaching Johnny not to fall for phish. ACM Transactions on Internet Technology (TOIT), 2010, 10.2. 1-31. o.

[25] Krasznay Csaba: A kiberbiztonság stratégiai vetületeinek oktatási kérdései a közszolgálatban. Nemzet és Biztonság – Biztonságpolitikai Szemle 2017/3. szám. 38–53. o.

léma megoldása érdekében a rendszeres és gyakorlatorientált kiberbiztonsági képzések fontosságát hangsúlyozzák a szakértők.[26] Fontos megemlíteni, hogy Magyarországon több kijelölt szervezet is létezik, amelyek segítséget nyújthatnak a vállalatoknak ezen a területen, például az Alkotmányvédelmi Hivatal (AH), a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NKI) és más szakosított állami szervek. A probléma méretéhez képest azonban kevés szó esik arról, hogy a cégeknek lenne honnan segítséget kérni Magyarországon is.

Az interaktív, szimuláción alapuló képzések jelentősen hatékonyabbak a hagyományos, elméleti oktatásnál. A szerzők szerint ezek a gyakorlatok nem csak az elméleti tudást, hanem a valós helyzetekben alkalmazható készségeket is fejlesztik, ami kulcsfontosságú a gyorsan változó fenyegetési környezetben. A felhasználói viselkedéselemzés területén a jövőbeni kutatásoknak a viselkedési minták finomabb elemzésére és az algoritmusok továbbfejlesztésére kell összpontosítaniuk.[27] Érdemes lenne nagyobb hangsúlyt fektetni a biometrikus sajátosságok vizsgálatára is, mint például a kurzormozgás felismerése és annak egy adott felhasználóhoz rendelése, ami további azonosítási réteget biztosíthat a rendszerekben. Az ML-modellek és a big data analitika integrálása a viselkedéselemző rendszerekbe jelentősen növelheti a fenyegetések előrejelzésének pontosságát és a védelmi rendszerek proaktivitását.

A felhasználói viselkedés elemzése jelentős mértékben támaszkodik a viselkedési anomáliák felismerésére, amelyek egy adott felhasználó normál viselkedési mintáitól való eltérések lehetnek, például egy szokatlan bejelentkezési helyszín vagy egy nem megszokott időben történő tevékenység.[28] Ezek az anomáliák jelezhetik, hogy egy külső támadó hozzáférést

[26] Kiss Adrienn – Kollár Csaba: Az információbiztonság időszerű kérdései a magyarországi kkv-k körében. Scientia et Securitas, 4(2), 2024. 98-107. o.
[27] Beuran, Razvan – Chinen, Ken-Ichi – Tan, Yasuo – Shinoda, Yoichi: Towards effective cybersecurity education and training. 2016.
[28] Nagy Zoltán: A kiberbűncselekmények fogalma és csoportosítása. In: Kiss, T. (szerk.): Kibervédelem a bűnügyi tudományokban. Dialóg Campus, Budapest, 2020. 33-44. o.

szerzett egy felhasználói fiókhoz, vagy egy belső fenyegetés kezd kibontakozni.

A kognitív torzítások és az emberi hibák elmélete

Az egyik jelentős elméleti megközelítés, amely alapvetően befolyásolja a felhasználói viselkedést a kiberbiztonság területén, a kognitív torzítások elmélete. Ezek a mentális rövidítések vagy heurisztikák az emberek döntéshozatalát egyszerűsítik, de gyakran hibás következtetésekhez vezethetnek, különösen a gyors és precíz döntések szituációiban. A kiberbiztonság területén, ahol egy-egy döntés kritikus jelentőségű lehet, ezek a torzítások különösen veszélyesek. Az egyik legkritikusabb ilyen kognitív torzítás a „sérthetetlenség illúziója", amelynek hatására a felhasználók jelentősen alábecsülik a kibertámadások kockázatát. Ez a jelenség különösen aggasztó, mert sok felhasználó túlbecsüli a saját képességeit a fenyegetések felismerésében és kezelésében, ami csökkenti az éberséget és a biztonsági előírások betartásának hajlandóságát.[29]

A kognitív torzítások mellett a szociális tanulás elmélete is kulcsfontosságú szerepet játszik a kiberbiztonsági magatartás formálásában. Ez az elmélet azt hangsúlyozza, hogy az emberek hajlamosak mások viselkedését utánozni, különösen akkor, ha az adott személy tekintéllyel bír. Ennek következménye az, hogy egy szervezet biztonságtudata jelentősen romolhat, ha a vezetők vagy kollégák nem megfelelő viselkedést mutatnak. Azokban a szervezetekben, ahol a vezetők jó példát mutatnak a biztonsági protokollok betartásában – például aktívan részt vesznek a kiberbiztonsági képzéseken, láthatóan betartják a biztonsági előírásokat és kommunikálják ezek fontosságát –, a munkavállalók is nagyobb valószínűséggel követik ezeket az előírásokat. A vezetői példa tehát döntő hatással van a kiberbiztonsági

[29] Bicskei Tamás: A mesterséges intelligencia közigazgatásban való felhasználásával okozott kár. KözigazgatásTudomány 2023/1. szám. 99-114. o.

kultúra kialakítására és fenntartására.[30] A szociális tanulás hatása a munkahelyi kiberbiztonságra nem csupán a vezetői struktúrákon keresztül érvényesül, hanem a horizontális, kollégák közötti interakciók is meghatározó szerepet játszanak. Az ilyen típusú tanulás különösen fontos a kiberbiztonsági gyakorlatok esetében, mivel a kollégák viselkedése és hozzáállása gyakran közvetlenül befolyásolja az egyéni biztonságtudatosságot. A peer-to-peer tanulási módszerek alkalmazása révén hatékonyan erősíthető a munkahelyi biztonsági kultúra. Ez a módszer lehetőséget biztosít arra, hogy a kollégák közvetlen tapasztalatokat osszanak meg egymással, ezáltal növelve az egyéni elköteleződést és tudatosságot a kiberbiztonsági elvek betartásában.[31]

A kognitív torzítások és a szociális tanulás elméletei nem csupán elméleti jelentőséggel bírnak, hanem gyakorlati következményekkel is járnak. A hatékony kiberbiztonsági stratégiák kialakításánál ezek a pszichológiai tényezők kulcsszerepet játszanak. A szituációs gyakorlatok és az interaktív képzési módszerek alkalmazása segíthet a kognitív torzítások csökkentésében, valamint a helyes viselkedésminták megerősítésében, ami elengedhetetlen a biztonságos szervezeti kultúra kialakításához.[32] A nemzetközi kutatások is alátámasztják ezeket az eredményeket, hiszen a felhasználók biztonsági protokollokhoz való alkalmazkodása szoros összefüggésben áll a kognitív folyamatokkal és a szociális környezettel. Ez a globális tapasztalat rávilágít arra, hogy a pszichológiai tényezők figyelembevétele univerzális jelentőségű a kiberbiztonsági stratégiák tervezésénél, nem csupán a hazai, hanem a nemzetközi kontextusban is.[33]

[30] Bandura, Albert – Hall, Prentice: Albert Bandura and social learning theory. Learning Theories for Early Years 78. 2018.
[31] Happa, Jassim – Glencross, Mashhuda – Steed, Anthony: Cyber security threats and challenges in collaborative mixed-reality. Frontiers in ICT 6. 2019: 5. o.
[32] Morsella, Ezequiel – Bargh, John A. – Gollwitzer, Peter M.: Social cognition and social neuroscience. Oxford handbook of human action, 2008.
[33] Bulgurcu, Burcu – Cavusoglu, Hasan – Benbasat, Izak: Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS quarterly, 2010. 523-548. o.

A felhasználói viselkedéselemző (UBA) rendszerek elméleti háttere

Az UBArendszerek elméleti hátterében az ML és az adatelemzés komplex módszertana áll, amely lehetővé teszi a felhasználói viselkedés mélyreható és valós idejű elemzését. Ezek a rendszerek különösen hatékonyak a belső fenyegetések azonosításában, ahol a hagyományos védelmi megoldások gyakran kudarcot vallanak. A belső fenyegetések egyre növekvő kockázatot jelentenek a modern szervezetekben, így az UBA-rendszerek alkalmazása kritikus szerepet játszik a kiberbiztonságban.[34] Az UBA-rendszerek gépitanulás-algoritmusokra és adat alapú elemzésekre építenek, amelyek lehetővé teszik a felhasználói viselkedés folyamatos megfigyelését és a szokatlan tevékenységek valós idejű azonosítását. Az Európai Unióban az UBA-rendszerek alkalmazása során különös figyelmet kell fordítani a személyes adatok védelmére és a vonatkozó jogszabályok betartására. Az Európai Unió Általános Adatvédelmi Rendelete (GDPR) alapelvei, mint a jogszerűség, méltányosság és átláthatóság, célhoz kötöttség, adatminimalizálás, pontosság és tárolási korlátozás, meghatározzák, hogy a személyes adatokat csak meghatározott, jogszerű és egyértelműen kifejezett célokra lehet gyűjteni, és azoknak relevánsnak és a szükségesre korlátozottnak kell lenniük. Ezen túlmenően, az Európai Unió mesterséges intelligenciáról szóló jogszabálya (AI Act) kockázat alapú megközelítést alkalmaz az MI-rendszerek szabályozásában. Ez a megközelítés arányos és hatékony, kötelező erejű szabályokat vezet be az MI-rendszerekre vonatkozóan, figyelembe véve azok kockázati szintjét.[35] Ezek a rendszerek képesek gyorsan reagálni a fenyegetésekre, mivel figyelik az adatokat és elemzik a mintákat, így az eltérések esetén azonnal figyelmeztetést küldenek, amely kritikus lehet a dinamikusan változó kiberbiztonsági környezetben. Az UBA-rend-

[34] Homoliak, Ivan – Toffalini, Flavio – Guarnizo, Juan – Elovici, Yuval – Ochoa, Martina: nsight into insiders and it: A survey of insider threat taxonomies, analysis, modeling, and countermeasures. ACM Computing Surveys (CSUR), 52(2), 2019. 1-40. o.

[35] Országgyűlés Hivatala: Infojegyzet 2024/23. szám. Forrás: https://www.parlament.hu/documents/d/guest/infojegyzet_2024_23_eu_mi_rendelet Letöltés ideje: 2025. 03. 01.

szerek elméleti hátteréhez szorosan kapcsolódik az MI és a big data elemzés, amelyek lehetővé teszik az adathalmazok hatékony feldolgozását és a viselkedési minták pontosabb felismerését.

A nemzetközi szakirodalom megerősíti, hogy az UBA-rendszerek hatékonysága nemzetközileg is elismert, különösen a többfázisú felhasználói viselkedés elemzésében. Ezek a rendszerek univerzálisan alkalmazhatók, és fontos szerepet játszanak a globális kiberbiztonsági stratégiákban, hangsúlyozva a felhasználói viselkedés mélyreható elemzésének jelentőségét.[36]

A kibertámadások típusai és trendjei

A kibertámadások evolúciója és komplexitásának növekedése korunk egyik legjelentősebb biztonsági kihívását jelenti. A digitalizáció térnyerésével párhuzamosan a támadási vektorok és módszerek is jelentősen átalakultak, ami folyamatos alkalmazkodást követel mind a védelmi szakemberektől, mind a felhasználóktól.[37] A Nemzeti Kibervédelmi Intézet 2023-as jelentése szerint Magyarországon az elmúlt években különösen megnövekedett a zsarolóvírus támadások száma, amelyek főként az Európai Unió országaira összpontosítottak.[38] Ez összhangban van a globális trendekkel, amit az Europol Internet Organised Crime Threat Assessment (IOCTA) jelentése is megerősít,[39] kiemelve a Ransomware as a Service (RaaS modell) támadások növekvő fenyegetését Európa-szerte.

---

[36] Beláz Annamária – Berzsenyi Dániel: Kiberbiztonsági Stratégia 2.0: A kiberbiztonság stratégiai irányításának kérdései. NKE Stratégiai Védelmi Kutatóközpont Elemzések, 2017/3. szám. 1-15. o.

[37] Sasvári Péter (szerk.): Informatikai rendszerek a közszolgálatban II. Ludovika Egyetemi Kiadó. Budapest, 2020.

[38] Nemzeti Kibervédelmi Intézet (2024). Éves kiberbiztonsági jelentés. Forrás: https://nki.gov.hu/wp-content/uploads/2024/07/Eves-kiberbiztonsagi-jelentes.pdf Letöltés ideje: 2024. 09. 23.

[39] Europol (2024). Internet Organised Crime Threat Assessment (IOCTA). Forrás: https://www.europol.europa.eu/cms/sites/default/files/documents/Internet%20Organised%20Crime%20Threat%20Assessment%20IOCTA%202024.pdf Letöltés ideje: 2024. 09. 23.

A kritikus infrastruktúrák elleni támadások száma is emelkedő tendenciát mutat, ami nemzetbiztonsági szempontból is kiemelt figyelmet érdemel. Ez a trend nem csak Magyarországra jellemző. Az Egyesült Államokban a Cybersecurity and Infrastructure Security Agency (CISA) 2022-es jelentése szerint a kritikus infrastruktúrák elleni támadások 55%-kal nőttek az előző évhez képest.[40]

A kibertámadások típusai

Az ENISA (European Union Agency for Cybersecurity) 2023-as Threat Landscape jelentése átfogó elemzést nyújt a globális kiberbiztonsági fenyegetettségek fejlődéséről, valamint a különböző támadási vektorokról. A jelentés nyolc fő fenyegetettségi csoportot különít el, amelyek különösen jelentőségteljesek az előfordulásuk és hatásuk tekintetében. Az internetes fenyegetések, más néven cyberthreats, olyan támadások, amelyek az interneten keresztül történnek, céljuk pedig a hálózati rendszerek, alkalmazások és adatbázisok kompromittálása. Ezek a támadások magukban foglalhatják a webes szolgáltatások elleni támadásokat (pl. webes sebezhetőségek kihasználása), valamint a botnetekkel végrehajtott támadásokat, amelyek széleskörű kárt okozhatnak a felhasználók és szervezetek számára. Az ellátási láncok elleni támadások különösen veszélyesek, mivel nemcsak a célzott szervezeteket érinthetik, hanem azok beszállítóit, partnereit és ügyfeleit is. Az ilyen támadások során a támadók egy gyenge pontot keresnek az ellátási lánc valamelyik szereplőjében, és azon keresztül érik el a célrendszereket. A SolarWinds és a Kaseya esetei például világosan bemutatták, hogy ezek a támadások milyen széleskörű és hosszú távú hatással lehetnek. A social engineering támadások során a támadók pszichológiai manipulációval próbálják megszerezni az áldozatoktól azokat az információkat, amelyek hozzáférést biztosítanak kritikus rendszerekhez. Az ilyen támadások egyik legelterjedtebb formája az adathalászat (phishing), amely

[40] America's Cyber Defense Agency: 2021 Trends Show Increased Globalized Threat of Ransomware. 2022. Forrás: https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-040a Letöltés ideje: 2024. 09. 23.

során a támadók megtévesztő e-mailekkel vagy üzenetekkel csalják ki a felhasználóktól az érzékeny adatokat, például jelszavakat vagy pénzügyi információkat. A malware-ek, vagyis a rosszindulatú szoftverek, olyan programok vagy kódok, amelyek célja a számítógépes rendszerek megfertőzése és kompromittálása. A malware-ek típusai közé tartoznak a vírusok, férgek, trójaiak, spyware-ek és a rootkit-ek. A malware-támadások sokszor automatizáltak és rendkívül elterjedtek, mivel a támadók könnyen hozzáférhetnek olyan eszközökhöz, amelyekkel tömeges támadásokat indíthatnak. A DoS (Denial of Service), illetve elosztott változata, a DDoS (Distributed Denial of Service) támadások célja, hogy egy hálózati szolgáltatást vagy szervert túlterheljenek, ezzel akadályozva a normál működést. Ezen támadások következtében az áldozatok nem férnek hozzá a kívánt szolgáltatásokhoz, ami különösen nagy problémát jelenthet az üzleti szférában, mivel bevételkiesést és presztízsveszteséget is eredményezhet. Az információ manipulációja egyre nagyobb fenyegetést jelent, különösen a közösségi média és az online hírek korában. Az ilyen támadások során a támadók dezinformációval vagy félrevezető információval próbálnak politikai, gazdasági vagy társadalmi befolyást szerezni. Az adatvédelmi fenyegetések olyan támadásokra utalnak, amelyek célja az egyének személyes adatainak ellopása, megsértése vagy illegális felhasználása. Az adatszivárgások és adatlopások az egyik leggyakoribb következményei ezeknek a támadásoknak, amelyek súlyos pénzügyi és reputációs károkat okozhatnak mind a magánszemélyek, mind a szervezetek számára.

Az GDPR az európai gazdasági térségben működő szervezetekre vonatkozik, és szigorú követelményeket támaszt az adatvédelem területén, beleértve a személyes adatok kezelését, az incidensek bejelentését és a büntetések kiszabását. A GDPR mellett más régiókban is léteznek hasonló szabályozások, mint például a kaliforniai fogyasztói adatvédelmi törvény (CCPA), Brazíliában a Lei Geral de Proteção de Dados (LGPD), vagy Kanadában a Personal Information Protection and Electronic Documents Act (PIPEDA). Ezek a szabályozások gyakran eltérő követelményeket támasztanak az adatvédelem terén, ami jelentős megfelelési kihívásokat jelent a

nemzetközi szervezetek számára. Az EU és az USA szabályozási különbségeiből eredő problémák jelentős kihívásokat jelentenek a globális működésű vállalatok számára. Az USA-ban nincs átfogó szövetségi adatvédelmi törvény, ehelyett ágazati szabályozások (pl. HIPAA az egészségügyben, GLBA a pénzügyi szektorban) és állami szintű jogszabályok (pl. CCPA Kaliforniában, CDPA Virginiában) mozaikja létezik. Ez a fragmentált megközelítés ellentétben áll az EU GDPR egységes keretrendszerével, ami megfelelési nehézségeket okoz a határokon átnyúló adatkezelést végző szervezeteknek. A két rendszer közötti legjelentősebb különbségek közé tartozik az adatkezeléshez szükséges jogalap, az adattovábbítási mechanizmusok és az egyéni jogok érvényesíthetőségének mértéke.[41] Konkrét példa a szabályozási különbségekből eredő problémákra a Schrems-ügyek sorozata, amelyek eredményeként az Európai Unió Bírósága érvénytelenítette mind a Safe Harbor, mind a Privacy Shield adattovábbítási keretrendszereket, jelentősen megnehezítve az EU és az USA közötti adattovábbítást. Ezek a döntések rávilágítottak az amerikai megfigyelési gyakorlatok és az európai adatvédelmi elvek összeegyeztethetetlenségére.[42]

Az ENISA Threat Landscape 2023 jelentése rávilágít arra, hogy a kiberbiztonsági fenyegetések folyamatosan fejlődnek, és egyre szofisztikáltabbak lesznek. Az említett nyolc fenyegetettségi csoport azért került kiemelésre, mert ezek széles körben előforduló és potenciálisan súlyos következményekkel járó támadási formák, amelyek számos szektort érintenek. A kiberbiztonság javítása érdekében a szervezeteknek erőforrásaikat ezen te-

[41] Bradford, Anu: The Brussels effect: How the European Union rules the world. Oxford University Press. 2020.

[42] Court of Justice of the European Union: Judgment in Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems. 2020. Forrás: https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp2000-91en.pdf Letöltés ideje: 2025. 03. 15.

rületek védelmére kell összpontosítaniuk, folyamatosan figyelemmel kísérve az új fenyegetéseket és a legfrissebb védelmi megoldásokat alkalmazva.[43]

Kibertámadási trendek

Az ENISA Threat Landscape 2023 jelentése alapján a zsarolóvírusok továbbra is a legjelentősebb kiberfenyegetettséget jelentik, ami annak köszönhető, hogy ezek a támadások egyre célzottabbá és összetettebbé váltak. A zsarolóvírusok nemcsak az adatokat titkosítják, hanem egy új stratégiát, az úgynevezett *„dupla zsarolást"* alkalmazzák, ahol a támadók nem csupán a titkosított adatok visszavásárlásáért követelnek váltságdíjat, hanem az ellopott adatok nyilvánosságra hozatalával is fenyegetnek. Ez a módszer tovább növeli az áldozatokra nehezedő nyomást. Ráadásul a kiberbűnözők által kínált RaaS modellek révén a kevésbé technikai hátterű szereplők is könnyen hozzáférhetnek ezekhez az eszközökhöz, növelve a támadások gyakoriságát és hatókörét. Egyre gyakrabban találkozhatunk olyan kiberkémkedési műveletekkel is, amelyek során a támadók legális eszközöket használnak fel a műveleteik elfedésére, megnehezítve ezzel a felderítést. Az ilyen legális szoftverek, mint például a PowerShell vagy más rendszergazdai eszközök beépülhetnek az áldozatok infrastruktúrájába, anélkül, hogy gyanút keltenének. Ez különösen veszélyessé válik, mert hosszabb időn keresztül észrevétlenek maradhatnak, és lehetővé teszik a támadók számára, hogy érzékeny adatokat szerezzenek vagy további támadásokat készítsenek elő.

A geopolitikai feszültségek és konfliktusok továbbra is meghatározó szerepet játszanak a kiberműveletekben. Egyre inkább elterjedt, hogy állami támogatással működő szereplők célzott támadásokat hajtanak végre, amelyek célpontjai elsősorban kormányzati szervek, kritikus infrastruktúrák és ipari vállalatok. Ezek a támadások nem pusztán károkozásra irányulnak,

[43] European Union Agency for Cybersecurity (2023). Ensia Threat Landscape 2023. Forrás: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023 Letöltés ideje: 2024. 09. 23.

hanem hosszú távú stratégiai előnyök megszerzésére, például politikai befolyás növelésére vagy ipari kémkedésre. Érdekes fejlemény, hogy miközben a hagyományos mobil kártevők száma csökken, az adware-ek és kémprogramok száma továbbra is magas. Ezek a programok a felhasználók tevékenységeit követik nyomon, és gyakran rejtve futnak a háttérben anélkül, hogy a felhasználó tudomást szerezne róluk. Az adware-ek hirdetésekkel bombázzák a felhasználókat, míg a kémprogramok érzékeny adatokat gyűjtenek, például helymeghatározási információkat vagy böngészési előzményeket. A social engineering támadások szintén új szintre léptek, mivel a támadók egyre inkább a fizikai világban próbálják megtéveszteni az áldozatokat. Míg a social engineering hagyományosan elsősorban adathalászat révén történt, manapság már személyesen is megtéveszthetik az embereket, például deepfake technológiák segítségével. Az elmúlt időszakban drámaian megnövekedett a biometrikus csalások száma, ami komoly kihívást jelent a kiberbiztonság területén. A deepfake kísérletek volumene 2022 és 2023 között 3000%-kal emelkedett. Míg 2022-ben ritkán fordult elő, hogy csalók deepfake technológiát használtak a biometrikus ellenőrzések kijátszására a regisztrációs folyamat során, 2023-ban ez gyökeresen megváltozott. Az MI fejlődésének és a deepfake szoftverek növekvő elérhetőségének köszönhetően ezek mennyisége és kifinomultsága várhatóan tovább növekszik 2024-ben. Az elmúlt hat hónapban a deepfake-ek tették ki a biometrikus csalások mintegy 30-40%-át.

Jelenleg viszonylag kevés csaló felelős a nagyléptékű deepfake gyártásért, és ugyanez a csoport támadja a különböző ügyfeleket azonos módszerekkel. Mivel azonban a csalók hajlamosak eladni vagy megosztani taktikáikat más csalókkal, ez a helyzet hamarosan megváltozhat.[44] Ezzel a módszerrel a támadók egy valós személy hangját vagy kinézetét hamisítják meg, hogy bizalmas információkat szerezzenek. Az AI-technológiák, különösen az AI-chatbotok, új lehetőségeket nyitnak a kiberbűnözők számára is. Az AI

[44] Entrust: Fraud Report. Entrust Corporation. Minnesota, 2024. Forrás: https://www.entrust.com/sites/default/files/documentation/reports/entrust-fraud-report.pdf Letöltés ideje: 2025. 03. 15.

alapú chatbotok segítségével automatizálhatóvá válnak a támadások, például az adathalász kampányok. Ezen túlmenően az AI-t dezinformáció terjesztésére is felhasználják, valamint deepfake videókat és hangfelvételeket készíthetnek, amelyek segítségével hiteles személyekként léphetnek fel a támadók. A deepfake videókkal történő támadások jelentős problémát okoznak a vállalati kommunikációban és különösen a távoli munkavégzés során használt videókonferencia platformokon. Ezek a csalások különösen veszélyesek, mivel a technológia fejlődésével egyre nehezebb megkülönböztetni a valódi és a mesterségesen létrehozott videókat. A védekezés érdekében sok szervezet többfaktoros azonosítási protokollokat, offline ellenőrzési mechanizmusokat és előre meghatározott biztonsági jeleket vezetett be a videókonferenciákon történő interakciók során.[45] A DDoS-támadások szintén új dimenzióba léptek, mivel egyre nagyobb volumenű és összetettebb támadásokkal találkozhatunk, amelyek már nemcsak a hagyományos célpontokat, hanem a mobilhálózatokat és az IoT-eszközöket is célba veszik. A DDoS-as-a-Service modellek elterjedése pedig tovább növeli a támadások gyakoriságát, mivel ezek a szolgáltatások könnyen elérhetők és megrendelhetők bárki számára. Az információ manipulációjának területén az MI által generált tartalmak egyre inkább aggodalomra adnak okot. Bár a deepfake technológia már korábban is ismert volt, most az egyszerűbb, olcsóbb módszerek is elérhetők, amelyekkel könnyedén létrehozhatók hamisított képek és videók, a valóság manipulálása érdekében. Ezek a „cheap fakes" néven ismert tartalmak gyorsan terjednek a közösségi médiában, és jelentős hatással vannak a közvéleményre. A támadások során különösen a magas jogosultságokkal rendelkező alkalmazottakat, például a fejlesztőket és rendszergazdákat célozzák meg, akik hozzáféréssel rendelkeznek a vállalat kulcsfontosságú rendszereihez. Ezek a támadások gyakran hosszú távú károkat okoznak, és az egész iparágra hatással lehetnek. A 2023-as fenyegetettségi trendek rámutatnak arra, hogy a kiberbiztonsági fenyegetések mind komplexitásukban, mind méretükben növekednek. Az

[45] Verdoliva, Luisa. Media forensics and deepfakes: an overview. IEEE journal of selected topics in signal processing. 2020/5. szám. 910-932. o.

új technológiák, például az AI, új lehetőségeket nyitnak a támadók számára, miközben a klasszikus támadási módszerek, mint a zsarolóvírusok és a social engineering, továbbra is komoly veszélyt jelentenek. A fenyegetésekkel szembeni védekezés érdekében a szervezeteknek szorosan kell követniük ezeket a trendeket, és naprakész védelmi stratégiákat kell alkalmazniuk.[46]

Új kibertámadási irányok

Az ENISA legfrissebb jelentése rávilágít, hogy a kiberbűnözésben új trendek alakultak ki, amelyek közül kiemelkedik a ritkábban használt programozási nyelvek, például a Rust és a Go elterjedése. Ezeket a nyelveket a támadók azért részesítik előnyben, mert nehezítik a kártékony kódok elemzését, ami megnehezíti a biztonsági szakértők dolgát. Különösen a Go nyelv sajátossága, hogy a lefordított bináris állományok nagyobb méretűek, mint a hagyományosan használt nyelveké, mivel statikusan linkelik a szükséges könyvtárakat. Ez a méretbeli különbség – például a „Hello World" program binárisa Go nyelven több MB, míg C vagy C++ nyelven mindössze néhány KB – azt eredményezi, hogy sok malware scanner figyelmen kívül hagyja ezeket a nagy fájlokat, mivel kisebb méretű kártékony kódokra optimalizálták őket. A felhőinfrastruktúrák szerepe szintén kiemelkedővé vált a kiberbűnözésben, különösen a felhő hibás konfigurációit kihasználó támadások révén. A bűnözők egyre inkább célozzák az áldozatok felhő alapú rendszereit, és ezek az infrastruktúrák maguk is sok esetben a social engineering kampányok részévé válnak. Például adathalász kampányok során fájlmegosztó szolgáltatásokat használnak a kártékony fájlok terjesztésére. Az FBI már figyelmeztetést adott ki arra vonatkozóan, hogy kiberbűnözők keresőmotor-hirdetési szolgáltatásokat használnak fel, hogy legitim márkáknak álcázzák magukat, és így irányítsák a felhasználókat adathalász vagy zsarolóvírussal fertőzött oldalakra. A módszer lényege, hogy a bűnözők olyan hirdetéseket helyeznek el, amelyek megtévesztően hasonlítanak az eredeti cégek weboldalaira, így a felhasználók

[46] European Union Agency for Cybersecurity (2023): i.m.

könnyen félrevezethetők, és rosszindulatú tartalmakkal fertőződhetnek meg. Ezen túlmenően, a cryptojacking, azaz az áldozatok számítási erőforrásainak titkosított bányászatra való felhasználása továbbra is népszerű technika a kiberbűnözők körében. Bár az újabb fenyegetések, mint például a deepfake és az AI alapú social engineering technikák növekvő trendet mutatnak, a bűnözők többsége még mindig a jól bevált, régebbi módszereket részesíti előnyben. Ezek kevesebb technikai tudást és erőfeszítést igényelnek, miközben jelentős anyagi hasznot hoznak. A kémprogramok használata továbbra is virágzik, ami súlyos aggodalmakat kelt a magánélet védelmével kapcsolatban.[47]

Az elemzés rámutat arra is, hogy a Crime-as-a-Service (CaaS) piacok gyorsan növekednek, és egyre elérhetőbbé válnak a különféle kibertámadási szolgáltatások. Ez azt jelenti, hogy gyakorlatilag bárki, aki megfelelő pénzösszeggel rendelkezik, megvásárolhatja a kibertámadások terveit vagy akár teljesen automatizált eszközöket. Ez a jelenség drámaian növeli a támadások gyakoriságát és elérhetőségét, különösen a laikus támadók számára, akik korábban nem rendelkeztek technikai háttérrel. A geopolitikai helyzet, különösen az orosz-ukrán háború, szintén fokozta a hacktivista tevékenységeket, és az oroszbarát csoportok, mint például a NoName057, aktívan toboroznak embereket túlterheléses támadások indítására.[48] Ezek a csoportok különösen az egyszerűen kezelhető, letölthető programokkal célozzák meg a laikusokat, lehetővé téve számukra, hogy könnyedén részt vegyenek kibertámadásokban. Az új technológiák, mint az MI és a felh alapú rendszerek kihasználása, valamint a Crime-as-a-Service modellek elterjedése komoly fenyegetést jelentenek a globális kiberbiztonságra.[49]

Elhíresült kibertámadások

A kiberbűnözés növekvő fenyegetettsége számos példán keresztül világosan mutatja a globális gazdasági és társadalmi rendszerek sebezhetőségét,

[47] European Union Agency for Cybersecurity (2023): i.m.
[48] Forrás: https://www.radware.com/cyberpedia/ddos-attacks/noname057(16)/ Letöltés ideje: 2024. 09. 21.
[49] European Union Agency for Cybersecurity (2023): i.m.

valamint az új technológiák kihasználásának képességét a támadók részéről. Az elmúlt években tapasztalt nagy volumenű, kifinomult támadások – mint a Colonial Pipeline, a SolarWinds vagy a Kaseya ellen irányuló zsarolóvírus-támadások – rávilágítottak arra, hogy a kritikus infrastruktúrák és vállalatok egyre nagyobb kockázatnak vannak kitéve.

2021 májusában a Colonial Pipeline, az Egyesült Államok legnagyobb üzemanyag-vezetékrendszere súlyos RaaS-modell támadás áldozatává vált. A támadást a DarkSide nevű bűnszervezet hajtotta végre, amely a RaaS-modellt alkalmazta, így különféle eszközöket és infrastruktúrát biztosított más bűnözők számára is. A támadás során a hackerek bejuttatták a kártékony szoftvert a vállalat számítógépes rendszerébe, amely titkosította az adatokat, ezzel megakadályozva a működést. A Colonial Pipeline kénytelen volt leállítani a teljes működését, ami az USA keleti partvidékén üzemanyaghiányt és pánikszerű felvásárlást okozott. A támadók 4,4 millió dollár váltságdíjat kaptak Bitcoinban, amelynek kifizetését a vállalat a gyors helyreállítás érdekében fontolóra vette. Ez az eset nemcsak rávilágított a kritikus infrastruktúrák sebezhetőségére, hanem az amerikai kormány is szigorúbb szabályozásokat vezetett be a kiberbiztonság terén, hogy megakadályozza hasonló esetek bekövetkezését. A Colonial Pipeline elleni támadás példáján keresztül jól látható, hogy a kiberbűnözők célpontjai egyre inkább a kritikus infrastruktúrák, amelyek leállítása komoly társadalmi és gazdasági következményekkel járhat. Ez az eset világossá tette, hogy a kritikus infrastruktúrák sebezhetősége nem csupán technológiai kérdés, hanem nemzetbiztonsági és gazdasági fenyegetés is. A támadások ilyen típusú kockázatokat mutatnak, így a vállalatok és kormányok számára fontos, hogy megerősítsék a kiberbiztonsági védelmet, beleértve a proaktív monitoringot, a gyors reagálást és a szabályozási környezet fejlesztését. Az amerikai kormány erre válaszul szigorúbb szabályozásokat vezetett be a

kritikus infrastruktúrák védelmére, amely követendő példa lehet más országok számára is, mivel a nemzetközi együttműködés kulcsfontosságú ezen fenyegetések kezelése során.[50]

A SolarWinds elleni támadás 2020 végén zajlott, és az egyik legkifinomultabb állam által támogatott kibertámadásnak számít. A támadók a SolarWinds Orion szoftverének frissítéseibe csempésztek be kártékony kódot, amely lehetővé tette számukra, hogy több ezer szervezet rendszerébe, köztük az Egyesült Államok kormányzati ügynökségeibe is bejussanak. Az incidenst az orosz külső hírszerzéshez kötötték, ami tovább növelte a nemzetközi feszültségeket. A támadók így az érzékeny adatokat, például a belső kommunikációt és a titkos információkat is megszerezhették. Az eset rávilágított a supply chain támadások veszélyére, ahol a támadók nem közvetlenül a célpontokat támadják meg, hanem egy harmadik fél, például szoftverszállító rendszereit manipulálják. A támadás következményeként számos ország és szervezet felülvizsgálta kiberbiztonsági stratégiáját és beszállítói láncának biztonságát, hogy megakadályozza a jövőbeli hasonló incidenseket. Az állam által támogatott támadások, például a SolarWinds-incidens rávilágítanak arra, hogy a geopolitikai célok elérésében a kibertámadások egyre nagyobb szerepet játszanak. Az ilyen támadások nemcsak gazdasági kárt okoznak, hanem megingathatják a nemzetközi biztonságot és bizalmat is. A SolarWinds-támadás azt mutatja, hogy a beszállítói láncok sebezhetősége központi kérdéssé vált. Az ilyen típusú támadások felderítése különösen nehéz, mivel a támadók a beszállítók infrastruktúrájába mélyen beágyazott kártékony kódokkal dolgoznak, amelyeket nehéz észlelni. Az ellátási lánc biztonságának javítása érdekében ajánlott a beszállítói auditok bevezetése, valamint a fejlett monitoring és biztonsági eszközök alkalmazása, amelyek képesek az anomáliák korai felismerésére. A szervezeteknek különös figyelmet kell fordítaniuk a beszállítók és alvállalkozók kiberbiztonsági gyakorlatainak értékelésére, valamint a szigorú biztonsági

[50] Turton, William - Riley, Michael - Jacobs, Jennifer: Colonial pipeline paid hackers nearly $5 million in ransom. Bloomberg (May 13, 2021) Forrás: https://www.bloomberg.com/news/articles/2021-05-13/colonial-pipeline-paid-hackers-nearly-5-million-in-ransom Letöltés ideje: 2024. 09. 23.

szabványoknak való megfelelésre.[51] Az incidens kivizsgálása során feltárták, hogy az emberi tényező jelentős szerepet játszott a támadás sikerében. A kongresszusi meghallgatások és a SolarWinds korábbi alkalmazottainak beszámolói alapján kiderült, hogy a vállalat egyik gyakran használt jelszava a *„solarwinds123*" volt, amelyet nyilvánosan elérhetővé tettek egy GitHub repozitóriumban.[52]

2021 júliusában a REvil zsarolóvírus csoport egy nagy volumenű támadást indított a Kaseya VSA szoftver ellen, amelyet IT-szolgáltatók használnak a különböző ügyfeleik rendszerének kezelésére. A támadás során a REvil hackerei egy sebezhetőséget kihasználva több mint 1500 vállalatot érintettek világszerte. A zsarolóvírus titkosította az érintett rendszereket, és 70 millió dollár váltságdíjat követeltek az univerzális dekódolóért. Ez volt az eddigi legnagyobb ismert váltságdíj-követelés, amely nemcsak a Kaseya ügyfeleit, hanem az IT-ágazatot is komolyan érintette. Az esemény rámutatott a RaaS-modell veszélyességére, ahol a zsarolóvírus fejlesztői és üzemeltetői különböző csoportok, ezáltal megnehezítve a felderítést és a védekezést. A Kaseya támadása figyelmeztetés volt a vállalatok számára, hogy a kiberbiztonsági intézkedések és a rendszeres biztonsági frissítések menynyire elengedhetetlenek a hasonló támadások megelőzésére. A zsarolóvírusok fejlődése is jelentős aggodalomra ad okot, különösen a RaaS-modell megjelenésével. A REvil zsarolóvírus támadás a Kaseya szoftver ellen bemutatta, hogy a támadók már nem egyénileg, hanem jól szervezett szolgáltatásként nyújtanak támadási infrastruktúrát és eszközöket, ami megnöveli a támadások számát és hatékonyságát. A támadók egy 0-day sérülékenységet használtak ki a Kaseya rendszerében. Ez azt jelenti, hogy a belépési

[51] Sanger, David E.: Russian hackers broke into federal agencies, US officials suspect. The New York Times, 2020, 13. Forrás: https://www.nytimes.com/2020/12/13/us/politics/russian-hackers-us-govern-ment-treasury-commerce.html Letöltés ideje: 2024. 09. 23.
[52] Keumars Afifi-Sabet: SolarWinds blames intern for weak 'solarwinds123' password. Forrás: https://www.itpro.com/security/cyber-attacks/358738/intern-blamed-for-weak-password-that-may-have-sparked-solarwinds Letöltés ideje: 2025. 03. 16.

pont a Kaseya szoftver biztonsági rése volt, amelyet a támadók kihasználtak a zsarolóvírusos támadás végrehajtásához.[53] A RaaS-modell megnehezíti a támadók azonosítását és a védekezést, mivel a támadásokat végrehajtó csoportok nem azonosak a kártékony szoftverek fejlesztőivel. A jövőben szükséges a nemzetközi jogi keretek és a bűnüldözési eszközök továbbfejlesztése, hogy hatékonyan lehessen felvenni a harcot az ilyen modellekkel. A bűnüldöző szervek együttműködése kulcsfontosságú a RaaS platformok felszámolásában és a támadók felelősségre vonásában.[54]

Az MI és a deepfake technológia megjelenése új típusú támadásokhoz vezetett a kiberbűnözés terén. 2019-ben egy brit energiavállalat vezérigazgatója egy telefonos hívás során, amelyet a német anyavállalatának vezetőjétől kapott, 220 000 eurót utalt át egy magyar beszállítónak, mert azt hitte, hogy valóban a német vezetővel beszél. Valójában azonban a hívás során egy MI által generált hangot hallott, amely tökéletesen utánozta a német vezető hangját és akcentusát. Ez az eset rávilágított arra, hogy az MI alapú social engineering támadások mennyire veszélyesek lehetnek, és hogy a hagyományos kiberbiztonsági intézkedések, mint például a jelszavak és a kétfaktoros hitelesítés nem elegendőek a védelemhez. A deepfake technológia potenciális kiberbiztonsági kockázatai miatt szükségessé vált a megbízható azonosítási és ellenőrzési rendszerek fejlesztése, amelyek képesek a manipulált médiatartalmak kiszűrésére. Az MI és a deepfake technológia megjelenése új típusú social engineering támadásokat tett lehetővé, amelyek sokkal kifinomultabbak és nehezebben észlelhetők. Az MI segítségével a támadók képesek utánozni vezetők vagy más kulcsfontosságú személyek hangját, viselkedését vagy akár teljes megjelenését akár valós idejű videós formában is, így könnyebben tudnak bizalmas információkat

[53] ICS Cyber Security Blog: A Kaseya-incidens és annak tágabb összefüggései. Forrás: https://icscybersec.blog.hu/2021/07/10/kaseya-incidens-osszefuggesei Letöltés ideje: 2025. 03. 12.

[54] Cimpanu, Catalin: REvil asks for $70 million to decrypt systems impacted in Kaseya ransomware attack. The Record by Recorded Future. Forrás: https://therecord.media/revil-gang-asks-70-million-to-decrypt-systems-locked-in-kaseya-attack Letöltés ideje: 2024. 09. 19.

kicsalni vagy pénzügyi tranzakciókat végrehajtatni. Az új típusú támadások kivédése érdekében fontos, hogy a vállalatok olyan MI alapú védelmi rendszereket fejlesszenek ki, amelyek képesek felismerni a deepfake manipulációkat és más, MI alapú fenyegetéseket.[55]

Az ML és a MI segítségével fejlettebb védelmi rendszerek hozhatók létre, amelyek képesek észlelni és megelőzni az új típusú támadásokat. A mélytanulási architektúrák, mint a Meso-4 és a MesoInception-4, hatékonyan alkalmazhatók a deepfake videók felismerésére. A Meso-4 hálózat négy egymást követő konvolúciós és pooling rétegből áll, míg a MesoInception-4 az első két konvolúciós réteget egy inception modul variánsával helyettesíti a hatékonyság növelése érdekében. Mindkét módszer a videók mesoscopic szintű elemzésével képes észlelni a hamisításokat, a képi zajra és a magas szintű szemantikai jellemzőkre összpontosítva.[56] A kiberbiztonsági stratégiák fejlesztésében fontos szerepet játszik a technológiai és fizikai védelmi módszerek együttes alkalmazása. Az MI segítségével fejlettebb észlelési és megelőzési technológiák fejleszthetők ki, de a fizikai megoldások, mint például az élőségvizsgálat, szintén elengedhetetlenek a biztonságos azonosításban.

A Mirai botnet 2016-ban végrehajtott támadása az IoT-eszközök sebezhetőségének drámai példája volt. A Mirai botnet, amely főként IoT-eszközökből állt, a világ egyik legnagyobb DDoS (Distributed Denial of Service) támadását hajtotta végre, amely több nagy weboldalt, például a Twittert, a Netflixet és az Amazont is elérhetetlenné tett. A támadás csúcspontján a botnet másodpercenként 1,2 terabyte adatforgalmat generált, amely összeomlasztotta a célzott szolgáltatásokat. Az esemény figyelmeztetést adott a vállalatoknak arra vonatkozóan, hogy az IoT-eszközök védelme és biztonságos konfigurálása elengedhetetlen, mivel a nem megfelelően védett esz-

[55] Stupp, Catherine. Fraudsters used AI to mimic CEO's voice in unusual cybercrime case. The Wall Street Journal, 2019, 30.08.
[56] Afchar, Darius – Nozick, Vincent- Yamagishi, Junichi – Echizen, Isao: Mesonet: a compact facial video forgery detection network. In: 2018 IEEE international workshop on information forensics and security (WIFS). IEEE. 2018. 1-7. o.

közök könnyen botnetek részévé válhatnak. A Mirai botnet példája világosan megmutatta, hogy a biztonsági rések kihasználása a kiberbűnözők számára új lehetőségeket teremt, így a megfelelő biztonsági intézkedések bevezetése kulcsfontosságú. Az IoT-eszközök elterjedése és a Mirai botnet példája rávilágít arra, hogy az összekapcsolt rendszerek és eszközök szélesebb támadási felületet biztosítanak a kiberbűnözők számára. Az IoT-eszközök sebezhetőségei lehetővé teszik, hogy a támadók nagy mennyiségű forgalmat generáljanak, ami elérhetetlenné tehet kritikus online szolgáltatásokat. A jövőbeni védelem érdekében az IoT-eszközök biztonságának fejlesztése kiemelten fontos, beleértve az alapértelmezett jelszavak megszüntetését, a rendszeres biztonsági frissítéseket és az eszközök biztonsági protokolljainak javítását.[57]

A jövőben a vállalatoknak és a kormányoknak folyamatosan figyelemmel kell kísérniük a kibertámadásokat, és rugalmas, adaptív védelmi stratégiákat kell kidolgozniuk a fenyegetések hatékony kezelésére. Az új technológiák, mint az MI és az IoT, különösen fontos szerepet játszanak a kibertámadások terjedésében, és a védelmi intézkedéseknek alkalmazkodniuk kell e változásokhoz.

Felhasználói viselkedéselemzés a kibertámadások megelőzésében
Viselkedési mintázatok és anomáliák felismerése

A felhasználói viselkedés meghatározó szerepet játszik a kiberbiztonsági incidensek kialakulásában és megelőzésében. A kutatások egyértelműen rámutatnak, hogy az incidensek jelentős hányada emberi tényezőkre vezethető vissza, melyek gyakran a hiányos ismeretekből vagy figyelmetlenségből erednek. A jelszóhasználat terén tapasztalható hiányosságok különösen aggasztóak. Mancic és Kiss kutatásában megállapította, hogy Szlovákiában többen használnak 12 karakteres vagy annál hosszabb jelszavakat, mint

[57] Antonakakis, Manos - April, Tim - Bailey, Michael et al.: Understanding the mirai botnet. Proceedings of the 26th USENIX Security Symposium. USENIX Association. 2017. 1093-1110. o.

Magyarországon. A felmérés eredményei azt mutatják, hogy Magyarországon többen alkalmaznak kis- és nagybetűket, számokat, valamint különleges karaktereket a jelszavaikban, mint Szlovákiában. A személyes információk használata a jelszavakban Magyarországon ritkábban fordul elő, mint Szlovákiában. A Mann-Whitney U-teszt eredményei azt mutatják, hogy Szlovákiában a jelszóhasználat esetén, amikor értelmes szót használnak, a p-érték magasabb, mint Magyarországon. Ennek alapján megállapítható, hogy a Szlovákiában élők nagyobb kockázatnak vannak kitéve a támadásokkal szemben, mint a magyar lakosok. A Kaspersky jelentése szerint a biztonságos jelszó létrehozásánál fontos figyelni arra, hogy a jelszó legalább 10-12 karakter hosszú legyen, minél hosszabb, annál jobb. El kell kerülni az olyan könnyen kitalálható jelszavakat, mint az *„12345”*, mivel ezeket másodpercek alatt feltörhetik *„brute force”* támadással. A jelszónak kis- és nagybetűket, számokat, valamint különleges karaktereket kell tartalmaznia, mivel ez megnehezíti a feltörését. A Keeper 2023-as jelentése szerint egy erős jelszó 16 karakterből áll, tartalmaz nagybetűket, számokat és különleges karaktereket, emellett nem tartalmaz személyes információkat, és ugyanazt a jelszót nem szabad több helyen használni. Az Amerikai Kibervédelmi Ügynökség (CISA) arra figyelmeztet, hogy az egyszerű jelszavak nem biztonságosak, ezért soha ne válasszunk könnyen kitalálható jelszót, például a születési dátumunkat, mivel az ilyen jelszavakat könnyen feltörhetik. Az IoT-eszközök védelmének egyik módja, hogy ilyen nehezen kitalálható jelszavakat használunk. Ezenkívül nagyon fontos, hogy mindig változtassuk meg az IoT-eszközeink alapértelmezett jelszavait.[58]

A szándékos visszaélések szintén jelentős részét képezik a kiberbiztonsági incidenseknek. A magyar közszférában és kritikus infrastruktúrában előforduló belső visszaélések közül az adatszivárogtatás és a jogosultságokkal való visszaélés a leggyakoribb problémák közé tartozik. A munkavállalók többsége nem gondolja, hogy baj származhat abból, ha a közösségi oldalakon munkahelyi fotókat tesznek közzé, mert észre sem veszik, hogy

[58] Mandić, Dorottya – Kiss, Gábor: Password usage in hungary and slovakia among users of smart devices. Biztonságtudományi Szemle, 2024, 6.2. 57-67. o.

például látszódik a háttérben egy tábla fontos jelszavakkal. Abból is gond lehet, ha valaki nem publikus adatokat tartalmazó fájlt tölt fel egy szerverre, amit aztán a Google megtalál és kereshetővé tesz. A magyar szervezeteknél a jogosultságkezelés gyakran nem elég szigorú, ami teret enged a visszaéléseknek.[59]

A viselkedésbeli anomáliák detektálása a kiberbiztonság és a biztonsági rendszerek kulcsfontosságú területe, amely lehetővé teszi a gyanús tevékenységek korai észlelését és a potenciális fenyegetések azonosítását. A viselkedésbeli anomáliák olyan eltérések, amelyek a normális vagy megszokott viselkedési mintáktól való eltéréseket jelentenek, és gyakran jelezhetik a rendszerekhez vagy adatokhoz való jogosulatlan hozzáférést.[60] Az anomália alapú detektálási technikák modellezik a normális hálózati és rendszerviselkedést, és az anomáliákat a normális viselkedéstől való eltérésként azonosítják. Ezek a módszerek különösen vonzóak, mert képesek detektálni a nulladik napi támadásokat, amelyekre még nem léteznek ismert szignatúrák. A normális tevékenység profiljainak testreszabása minden rendszer, alkalmazás vagy hálózat esetében megnehezíti a támadók dolgát annak kiderítésében, hogy mely tevékenységeket hajthatják végre észrevétlenül. Ezen eltérések észlelése számos technológiai és matematikai módszert igényel, amelyek közé tartoznak a statisztikai elemzések, az ML, valamint az MI algoritmusai. Az ML-technikák, például a felügyelt és felügyelet nélküli tanulási algoritmusok, különösen hatékonyak a komplex viselkedési minták felismerésében és az anomáliák azonosításában. A mély tanulás térnyerésével új lehetőségek nyíltak meg az anomália detektálása terén. A neurális hálózatok képesek rendkívül összetett és rejtett minták felismerésére, különösen nagy mennyiségű adat esetén, ami jelentősen javíthatja a detektálás pontosságát és hatékonyságát. Az anomália alapú technikák egyik fő kihívása a potenciálisan magas hamis riasztási arány (FAR),

[59] Lázár Fruzsina (2023). A kibertér veszélyei: zsarolóvírus és adatszivárogtatás. Forrás: https://behaviour.hu/a-kiberter-veszelyei-zsarolovirus-es-adatszivarogtatas/ Letöltés ideje: 2024. 09. 28.

[60] Chandola, Varun – Banerjee, Arindam – Kumar, Vipin: Anomaly detection: A survey. ACM computing surveys (CSUR), 2009, 41.3. 1-58. o.

mivel a korábban nem látott, de legitim rendszerviselkedések is anomáliaként kategorizálhatók. Ennek kezelésére gyakran alkalmaznak hibrid technikákat, amelyek ötvözik a visszaélés és az anomália detektálását, így növelve az ismert behatolások észlelési arányát és csökkentve az ismeretlen támadások hamis pozitív arányát. A viselkedésbeli anomáliák detektálásának további fejlesztése és finomítása folyamatos kutatási terület, amely kritikus fontosságú a jövő kibervédelmi rendszereinek hatékonyságához és robusztusságához.[61]

Gépi tanulás és mesterséges intelligencia alkalmazása

Gépi tanulás és mesterséges intelligencia a viselkedéselemzésben

A legitim nagy nyelvi modellek (Large Language Models, LLMs) bűnözői visszaélései mellett egyre több rosszindulatú LLM-et kínálnak mind a felszíni, mind a sötét weben, kiszolgálva a kibertámadásokban, adathalászatban és gyermekek szexuális kizsákmányolásában (CSE) részt vevő elkövetőket. Jelentések érkeztek MI-vel támogatott, MI-vel módosított és MI által generált gyermekek szexuális bántalmazását ábrázoló anyagokról (CSAM), és várhatóan ezek száma a közeljövőben növekedni fog. Az MI-eszközök és a deepfake technológiák finomítják a csalók social engineering képességeit is.[62]

A felügyelt tanulás során a rendszert előre meghatározott „címkézett" adatokkal látják el, lehetővé téve számára a normális és a rendellenes viselkedés közötti különbségtételt. Különösen hatékony, ha már ismert támadási mintázatokat kell azonosítani, mint például a szokatlan erőforrás-használat vagy a bejelentkezési minták drámai eltérései. A felügyelt tanulási algoritmusok, mint például a támogató vektorok módszere (SVM) vagy a random forest, képesek nagy pontossággal osztályozni a felhasználói tevékenységeket normális és gyanús kategóriákba, különösen a már ismert támadási típusok, például adathalászat vagy jogosultságokkal való visszaélés

[61] Buczak, Anna L. – Guven, Erhan: i.m.
[62] Europol: Internet Organised Crime Threat Assessment (IOCTA): i.m.

esetében. A felügyelet nélküli tanulás módszer során a rendszer „címkézetlen" adatokkal dolgozik, ahol önállóan kell felismernie a normál és az anomáliás viselkedés közötti különbségeket. A klaszterezési algoritmusok, mint például a K-means vagy a hierarchikus klaszterezés, kulcsszerepet játszanak a felügyelet nélküli tanulásban, lehetővé téve a hasonló viselkedési minták csoportosítását és a jelentősen eltérő klaszterek azonosítását. Ez különösen hasznos a zero-day támadások vagy a belső fenyegetések felderítésében, ahol a hagyományos, szabály alapú rendszerek gyakran kudarcot vallanak. A harmadik módszer a mélytanulás. Az ilyen jellegű rendszerek, neurális hálózatok, különösen a rekurrens neurális hálózatok (RNN) és a hosszú- és rövidtávú memória (LSTM) hálózatok, kiemelkedően jól teljesítenek a szekvenciális adatok, mint például a felhasználói tevékenységek idősorainak elemzésében. Ezek a modellek képesek hosszútávú függőségeket és komplex mintázatokat felismerni a viselkedési adatokban, lehetővé téve a kifinomult támadások korai szakaszban történő azonosítását.[63]

Bár az ML-algoritmusok jelentős előrelépést jelentenek a kiberbiztonsági viselkedéselemzésben, számos kihívással is szembesülnek. Az egyik legjelentősebb probléma a hamis pozitív riasztások magas aránya, amely túlterhelheti a biztonsági csapatokat. A másik kihívás az algoritmusok „fekete doboz" jellege, amely megnehezíti a döntéshozatali folyamat értelmezését és magyarázatát.[64]

A jövőben várhatóan növekvő hangsúlyt kap az értelmezhető mesterséges intelligencia (XAI) alkalmazása a kiberbiztonsági viselkedéselemzésben. Ez lehetővé teszi az ML-modellek döntéseinek jobb megértését és magyarázatát, amely kulcsfontosságú a bizalom növelésében és a szabályozási követelményeknek való megfelelésben. Ezen kívül a federated learning technikák alkalmazása is ígéretes területnek tűnik, amely lehetővé teszi a modellek tanítását anélkül, hogy az érzékeny adatokat központilag kellene

[63] Buczak, Anna L. – Guven, Erhan: i.m.
[64] Sommer, Robin – Paxson, Vern: Outside the closed world: On using machine learning for network intrusion detection. In: 2010 IEEE symposium on security and privacy. IEEE, 2010. p. 305-316. o.

tárolni, növelve ezzel a biztonságot és az adatvédelmet. A felügyelt és felügyelet nélküli tanulási módszerek, valamint a mélytanulási technikák kombinálása lehetővé teszi a komplex, többrétegű védelmi rendszerek kialakítását, amelyek képesek hatékonyan reagálni a folyamatosan változó fenyegetési környezetre. Az értelmezhető AI és a federated learning várhatóan tovább növelik majd ezeknek a rendszereknek a hatékonyságát és megbízhatóságát.[65]

Gépi tanulási algoritmusok a kibertámadások megelőzésében

A kibertámadások megelőzésében alkalmazott ML-algoritmusok széles skálája lehetővé teszi a különböző típusú fenyegetések hatékony azonosítását és kezelését. Ezek az algoritmusok kulcsfontosságú szerepet játszanak a modern kiberbiztonsági rendszerekben, biztosítva a gyors és pontos fenyegetésészlelést és -elhárítást.[66]

A logisztikus regresszió különösen hatékony eszköz a bináris döntések meghozatalában, például annak meghatározásában, hogy egy adott felhasználói tevékenység normálisnak vagy potenciális fenyegetésnek tekinthető-e. Ez az algoritmus képes nagy pontossággal elkülöníteni a legitim felhasználói viselkedést a gyanús aktivitástól, ami kulcsfontosságú a proaktív védekezésben. A logisztikus regresszió előnye, hogy viszonylag egyszerű implementálni és értelmezni, ugyanakkor rendkívül hatékony lehet bizonyos típusú kiberfenyegetések azonosításában. Az algoritmus kimenete egy valószínűségi érték, amely megmutatja, hogy egy adott aktivitás milyen valószínűséggel tartozik a „normális" vagy a „fenyegető" kategóriába, lehetővé téve a biztonsági rendszerek számára a gyors és automatizált döntéshozatalt.[67]

A k-legközelebbi szomszéd (k-NN) algoritmus egy olyan megközelítést alkalmaz, amely a felhasználói viselkedési mintákat a korábban megfigyelt,

[65] Li, Tian – Sahu, Anit Kumar – Talwalkar, Ameet – Smith, Virginia: Federated learning: Challenges, methods, and future directions. IEEE signal processing magazine, 2020, 37.3. 50-60. o.
[66] Buczak, Anna L. – Guven, Erhan: i.m.
[67] Sommer, Robin – Paxson, Vern: i.m.

normálisnak tekintett mintákhoz hasonlítja. Ez a módszer különösen alkalmas a finom eltérések észlelésére, amelyek gyakran jelzik egy kibertámadás korai szakaszát, lehetővé téve a gyors beavatkozást még a jelentős károk bekövetkezése előtt. A k-NN algoritmus előnye, hogy nem feltételez előzetes tudást a fenyegetések pontos természetéről, hanem a hasonlóságok és eltérések alapján képes azonosítani a potenciális veszélyeket. Ez különösen hasznos az olyan új típusú támadások felismerésében, amelyekre még nincs specifikus védelmi mechanizmus.[68]

Az anomália alapú tanulási modellek kiemelkedően hatékonyak az új, korábban ismeretlen fenyegetések azonosításában. Ezek a modellek képesek olyan viselkedési mintázatokat azonosítani, amelyek jelentősen eltérnek a normál felhasználói tevékenységtől, például hirtelen jelszóváltoztatások vagy szokatlan hálózati aktivitások esetén, ami lehetővé teszi a biztonsági szakemberek számára, hogy gyorsan reagáljanak a potenciális veszélyekre. Az anomália-detekció különösen értékes a zero-day támadások felismerésében, amelyek olyan új fenyegetések, amelyekre még nem létezik ismert védekezési módszer. Az algoritmusok folyamatosan tanulnak a normális viselkedési mintákból, és minden jelentős eltérést potenciális fenyegetésként kezelnek, biztosítva a rendszerek rugalmasságát az evolválódó kiberfenyegetésekkel szemben.[69]

A neurális hálózatok és a mélytanulás alkalmazása forradalmasította a nagy adathalmazok elemzését és a rendkívül komplex minták felismerését a kiberbiztonság területén. Ezek az algoritmusok képesek hatalmas mennyiségű adatot feldolgozni és olyan összefüggéseket feltárni, amelyek az emberi elemzők vagy egyszerűbb algoritmusok számára láthatatlanok ma-

[68] Liu, Fucheng – Wen, Yu – Zhang, Dongxue – Jiang, Xihe – Xing, Xinyu – Meng, Dan: Log2vec: A heterogeneous graph embedding based approach for detecting cyber threats within enterprise. In: Proceedings of the 2019 ACM SIGSAC conference on computer and communications security. 2019. 1777-1794. o.

[69] Ahmed, Mohiuddin – Mahmood, Abdun Naser – HU, Jiankun: A survey of network anomaly detection techniques. Journal of Network and Computer Applications. 2016/60. szám. 19-31. o.

radnának. A mélytanulási modellek különös előnye, hogy képesek folyamatosan alkalmazkodni a változó fenyegetési környezethez, ami kulcsfontosságú a modern, gyorsan fejlődő kibertámadások elleni védekezésben.[70]

A jövőben várhatóan tovább nő az ML szerepe a kiberbiztonságban, különös tekintettel az olyan fejlett technikákra, mint a federated learning, amely lehetővé teszi a modellek tanítását anélkül, hogy az érzékeny adatokat központilag kellene tárolni, növelve ezzel a biztonságot és az adatvédelmet.[71]

A magyar rendészeti szervek ML- és MI-képességeivel kapcsolatban fontos megjegyezni, hogy bár vannak előrelépések, a hazai ökoszisztéma még fejlesztésre szorul. Magyarországon több egyetem és kutatóintézet is foglalkozik kiberbiztonsághoz kapcsolódó ML-kutatásokkal, köztük a Budapesti Műszaki és Gazdaságtudományi Egyetem (BME), az Óbudai Egyetem és a Nemzeti Közszolgálati Egyetem (NKE) releváns tanszékei. A magyar rendészeti képességek tekintetében azonban jelentős kihívást jelent a szakképzett munkaerő hiánya és a technológiai infrastruktúra korlátozott volta. A Nemzeti Kibervédelmi Intézet (NKI) és a Nemzetbiztonsági Szakszolgálat rendelkezik bizonyos elemzési és monitoring képességekkel, de a komplex ML-rendszerek fejlesztése és implementálása terén még vannak hiányosságok. Mindezek alapján kijelenthető, hogy bár léteznek hazai szakemberek és kutatók a területen, a rendészeti szervek saját fejlesztési képességei korlátozottak. A jelenlegi helyzetben a leghatékonyabb megoldás egy hibrid megközelítés lenne: a hazai kutatóműhelyekkel való együttműködés erősítése mellett kereskedelmi megoldások adaptálása és a nemzetközi kooperáció fokozása. Az Európai Unió által támogatott programok, mint például a Horizon Europe, lehetőséget biztosítanak a hazai képességek fejlesztésére és a nemzetközi tudástranszferre. A Horizon Europe prog-

[70] T. Nagy László: Mesterséges intelligencia, multimédia, tanulástámogatás. In: Új technológiákkal, új tartalmakkal a jövő digitális transzformációja felé. Hungaranet Egyesület. Budapest, 2023. 69-76. o.
[71] Buczak, Anna L. – Guven, Erhan: i.m.

ram fontos elemei közé tartozik a kutatási és innovációs pályázatok támogatása, amelyek hozzájárulhatnak a magyar rendészeti szervek technológiai fejlesztéséhez és a szakképzett munkaerő bővítéséhez. Emellett a program lehetőséget kínál arra is, hogy Magyarország részt vegyen nemzetközi projektekben, és tapasztalatokat cseréljen más országokkal az MI és ML alkalmazásában. Ezáltal a magyar rendészeti szervek képesek lehetnek hatékonyabban alkalmazni az MI-technológiákat és javítani a biztonsági kockázatok kezelését.[72]

Az MI és az ML alkalmazása social engineering támadások ellen

A social engineering típusú támadások elleni védekezésben az MI és az ML alkalmazása kiemelkedően hatékonynak bizonyult. Ezek a technológiák képesek olyan finom mintázatokat felismerni, amelyek jellemzőek a social engineering technikákra, például az adathalász e-mailek esetében. Az MI alapú rendszerek automatikusan elemzik a beérkező e-mailek tartalmát, és azonosítják a gyanús elemeket, mint az ismeretlen vagy álcázott linkek, illetve a korábban azonosított támadási mintákhoz hasonló szövegrészek.[73] További problémát jelent, hogy a vezető MI-rendszereket fejlesztő magáncégek (mint az OpenAI, Google vagy a Microsoft) kereskedelmi termékeinél gyakran nem teljesen átlátható, hogy pontosan milyen adatokat gyűjtenek és elemeznek. A modellek betanításához használt adatbázisok összetétele és az adatgyűjtési gyakorlatok részletei gyakran üzleti titoknak minősülnek, ami jelentős kockázatot jelent a vállalati és nemzetbiztonsági alkalmazások esetében. Az Apple 2023 végén bevezetett Private Cloud Compute technológiája, amely az iOS 17.4 frissítéssel vált elérhetővé, jó példa az MI alapú megfigyelési képességek térnyerésére a mindennapi eszközökben. A rendszer kezdetben csak az Egyesült Államokban működik, és képes a felhasználók kommunikációját, médiáit és egyéb tartalmait elemezni

[72] Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal: Az EU Horizont Európa kutatási és innovációs keretprogramja. Forrás: https://nkfih.gov.hu/hivatalrol/nemzetkozi-kapcsolatok/horizont-europa Letöltés ideje: 2025. 03. 27.

[73] Bertino, Elisa – Islam, Nayeem: Botnets and internet of things security. Computer. 2017. 50.2. 76-79. o.

potenciális biztonsági fenyegetések azonosítása érdekében. Bár az Apple hangsúlyozza, hogy a rendszer a készüléken belül működik, és nem küld adatokat külső szervereknek, a technológia mélységi hozzáférése a felhasználói adatokhoz precedenst teremthet a kibervédelem nevében történő magánszféra-korlátozásra.[74]

A fejlett MI-rendszerek nemcsak az e-maileket, hanem a felhasználók teljes hálózati tevékenységét is képesek folyamatosan monitorozni és elemezni. Ezen monitorozás lehetővé teszi olyan gyanús viselkedési minták azonosítását, amelyek social engineering támadásokra utalhatnak, például amikor egy felhasználó szokatlan időpontban vagy módon próbál hozzáférni érzékeny információkhoz. Az ilyen jellegű elemzések lehetővé teszik a szervezetek számára, hogy jobban megértsék a potenciális támadási felületeiket és a felhasználói viselkedés változásait. A skálázhatóság, az értelmezhetőség, az ellenséges támadások és az adatvédelmi kérdések továbbra is jelentős kihívást jelentenek, amelyeket további részletes kutatással kell kezelni.[75] Az MI-rendszerek egyik legjelentősebb előnye a valós idejű válaszintézkedések végrehajtásának képessége. Ez magában foglalhatja a gyanús fiókok azonnali lezárását, a rendszergazdák automatikus értesítését, vagy akár a hálózati hozzáférés korlátozását a feltételezett támadás forrásából.[76] Az ilyen gyors és automatizált reakciók jelentősen csökkentik a social engineering támadások sikerességének esélyét, és minimalizálják az esetleges károk mértékét. Ezen túlmenően a folyamatos monitorozás lehetővé teszi a támadási minták valós időben történő elemzését, amely hozzájárul a jövőbeni fenyegetések megelőzéséhez.

[74] Newman, Lily Hay: Apple Intelligence Promises Better AI Privacy. Here's How It Actually Works. Forrás: https://www.wired.com/story/apple-private-cloud-compute-ai/?utm_source=chatgpt.com Letöltés ideje: 2025. 03. 13.
[75] Sur, Soumik – El-dosuk, Mohamed – Kamel, Sherif: Machine learning techniques for cyber security. Journal of Theoretical and Applied Information Technology, 2024, 102.7.
[76] Tsinganos, Nikolaos - Sakellariou, Georgios -Fouliras, Panagiotis - Mavridis, Ioannis: Towards an automated recognition system for chat-based social engineering attacks in enterprise environments. In: Proceedings of the 13th International Conference on Availability, Reliability and Security. 2018. 1-10. o

A proaktív védekezés lehetősége az MI-rendszerek egyik legfontosabb előnye: képesek előre jelezni és felismerni a potenciális fenyegetéseket a felhasználói viselkedés alapján, még mielőtt a tényleges támadás bekövetkezne. Az automatizálás kulcsfontosságú előnye az MI alapú rendszereknek. Az ML segítségével megvalósított automatikus fenyegetésészlelés nemcsak gyorsabb reakcióidőt tesz lehetővé, hanem jelentősen csökkenti az emberi beavatkozás szükségességét, és ezzel együtt az emberi hibák lehetőségét is.[77] Az MI-rendszerek skálázhatósága különösen előnyös nagy szervezetek esetében, mivel képesek hatalmas mennyiségű adatot feldolgozni és elemezni, így lehetővé téve több ezer, vagy akár több millió felhasználó hálózati tevékenységének egyidejű monitorozását.

Fontos megjegyezni, hogy az MI alapú rendszerek hatékonysága nagyban függ a rendelkezésre álló adatok minőségétől. Az ML-modellek pontossága és megbízhatósága szorosan összefügg az input adatok pontosságával és reprezentativitásával. Hibás vagy hiányos adatok esetén az algoritmusok pontatlan eredményeket produkálhatnak, ami téves riasztásokhoz vagy valós fenyegetések észlelésének elmulasztásához vezethet.[78] Az MI-rendszerek folyamatos karbantartást és frissítést igényelnek a pontos és megbízható működés fenntartása érdekében. Ez folyamatos erőforrás-befektetést követel mind anyagi, mind szakértői szempontból, amit a szervezeteknek figyelembe kell venniük az MI alapú kiberbiztonsági megoldások implementálásakor.

Bár az ML és az MI alkalmazása jelentős előrelépést jelent a kiberbiztonság területén, ezek a technológiák nem jelentenek univerzális megoldást minden kiberbiztonsági kihívásra. A hatékony védelem érdekében szükség van az MI alapú rendszerek és a hagyományos biztonsági megoldások integrált alkalmazására, valamint a folyamatos kutatásra és fejlesztésre, hogy lépést tarthassunk az egyre kifinomultabb kiberfenyegetésekkel.

---

[77] Chandola, Varun – Banerjee, Arindam – Kumar, Vipin: Anomaly detection: A survey. ACM computing surveys (CSUR), 2009, 41.3. 1-58. o.

[78] Sommer, Robin – Paxson, Vern: Outside the closed world: On using machine learning for network intrusion detection. In: 2010 IEEE symposium on security and privacy. IEEE. 2010. 305-316. o.

Kibervédelem és felhasználói oktatás

A kiberbiztonság területén a humán tényező továbbra is jelentős szerepet játszik, mivel a munkavállalók információbiztonsági ismeretei és gyakorlati alkalmazásuk közvetlenül befolyásolják a kibertámadások elleni védekezés hatékonyságát. Bár a technológiai fejlődés jelentős előrelépést hozott, a humán tényező gyakran a leggyengébb láncszemnek tekinthető, mivel az emberi hibák vagy figyelmetlenség könnyen kihasználhatóak a kiberbűnözésben. A munkavállalók információbiztonsági ismereteinek szintje, valamint ezen ismeretek gyakorlati alkalmazására való képessége közvetlenül befolyásolja a kibertámadások elleni védekezés hatékonyságát. Ez az összefüggés nem csupán statisztikai korrelációt mutat, hanem okokozati kapcsolatot is feltételez: a magasabb szintű felhasználói tudatosság közvetlenül hozzájárul a kiberbiztonsági incidensek számának csökkenéséhez és a potenciális fenyegetések korai felismeréséhez[79].

A felhasználói tudatosság növelése

A kiberbiztonsági tudatosságnövelő programok eredményessége és hatékonysága szoros összefüggést mutat azok strukturális felépítésével és implementációs stratégiáival. A legeredményesebb programok kardinális elemei között szerepel a folyamatos és progresszív képzési struktúra. Ennek elengedhetetlen része a rendszeresen ütemezett, moduláris felépítésű tudásfrissítő programok integrálása. A kibervédelemben a felhasználói oktatás nélkülözhetetlen szerepet tölt be a szervezetek biztonsági pozíciójának megerősítésében. A munkavállalók információbiztonsági tudatossága és szakmai felkészültsége közvetlen és erős korrelációt mutat a kibertámadások elleni védekezés eredményességével, ami alátámasztja a képzések kiemelt jelentőségét a modern vállalati környezetben. A tudatosságnövelő

[79] Bada, Maria – Sasse, Angela M. – Nurse, Jason RC: Cyber security awareness campaigns: Why do they fail to change behaviour? arXiv preprint arXiv:1901.02672, 2019.

programok nem csupán az egyéni kompetenciákat fejlesztik, hanem hozzájárulnak egy átfogó biztonsági kultúra kialakításához is, amely a szervezet minden szintjén megnyilvánul.[80]

A tudatosságnövelési programok elsődleges célkitűzései között szerepel az alapvető kiberbiztonsági kompetenciák szisztematikus fejlesztése és a szabálykövető magatartás erősítése. A hazai felhasználók különösen sérülékenyek az adathalász támadásokkal szemben, ami hangsúlyozza a munkavállalók pszichológiai felkészítésének fontosságát.

Interaktív gyakorlatok a kiberbiztonság oktatásában

A modern kibervédelmi képzési programok átfogó célkitűzése, hogy a felhasználók mélyreható és gyakorlatban alkalmazható ismereteket szerezzenek a kibertámadások különböző típusairól, a folyamatosan változó és egyre kifinomultabb potenciális biztonsági kockázatokról, valamint az ezek ellen alkalmazható eredményes védekezési stratégiákról és taktikákról. Az oktatási módszerek terén jelentős paradigmaváltás figyelhető meg: a hagyományos, passzív ismeretátadást felváltják az interaktív, gyakorlatorientált megközelítések.[81]

Ebben az alfejezetben bemutatok több olyan interaktív gyakorlatot, amelyek jelentősen növelik a résztvevők kiberbiztonsági tudatosságát:

1. Virtuális valóság (VR) alapú szimulációk: A VR alapú szimuláció, ahol a résztvevők fizikailag mozoghattak a virtuális térben, jelentősen növelte a kritikus infrastruktúra védelmével kapcsolatos tudatosságot. A szimulációban a résztvevők valós időben reagálhattak különböző incidensekre, beleértve a fizikai behatolási kísérleteket, tűzeseteket és kombinált kibertámadásokat. A VR-szimuláció különösen hatékonynak bizonyult a különböző típusú veszélyforrások

[80] Bulgurcu, Burcu – Cavusoglu, Hasan – Benbasat, Izak: i.m.
[81] Kumaraguru, Ponnurangam – Sheng, Steve – Acquisti, Alessandro – Cranor, Lorrie Faith – Hong, Jason: Teaching Johnny not to fall for phish. ACM Transactions on Internet Technology (TOIT). 2010, 10.2. 1-31. o.

közötti összefüggések megértésében és a stresszhelyzetben történő döntéshozatal gyakorlásában.[82]

2. Technikai kiberbiztonsági gyakorlatok: Ezek a gyakorlatok valós vagy virtuális informatikai rendszereken zajlanak, és céljuk a támadásokra való felkészülés és az informatikai rendszerek védelme. Ide tartoznak a zászlófoglaló (CTF) gyakorlatok is, amelyekben a résztvevők IT-biztonsági feladványokat oldanak meg.[83]
3. Tabletop gyakorlatok (TTX): Ezeknek a nem technikai jellegű gyakorlatokbaj a célja a kommunikációs és incidenskezelési készségek fejlesztése. A résztvevők egy szimulált környezetben gyakorolják a döntéshozatalt és a csapatmunkát, miközben megismerkednek a kiberbiztonsági fenyegetésekkel és a védekezési stratégiákkal.[84]
4. E-learning tananyagok: Interaktív online tananyagok, amelyek segítik a felhasználókat a biztonságtudatos jó gyakorlatok elsajátításában. Témáik között szerepel az általános IT-biztonság, a biztonságos jelszóhasználat és az adathalászat.[85]
5. Interaktív hibrid gyakorlatok: Švábenský és munkatársai (2018) kifejlesztettek egy hibrid kibervédelmi gyakorlatot, amely ötvözi a fizikai és digitális komponenseket. A résztvevők valós irodai környezetben dolgoztak, miközben a képzők különböző típusú támadásokat szimuláltak, beleértve a social engineering kísérleteket, a fizikai biztonsági incidenseket és a digitális támadásokat. A gyakorlat kü-

[82] Nemzeti Kibervédelmi Intézet: Felhasználói kézikönyv. A 41/2015. BM rendelet által meghatározott védelmi intézkedésekhez. Forrás: https://nki.gov.hu/it-biztonsag/kiadvanyok/segedletek/kezikonyv-a-41-2015-bm-rendelet-alkalmazasahoz/ Letöltés ideje: 2025. 03. 12.

[83] Szabó András: Technikai kiberbiztonsági gyakorlatok–Nemzetközi kitekintés. Hadmérnök 2018/1. szám. 286-301. o.

[84] Szabó András: Ajánlás TTX gyakorlatok szervezéséhez. Hadmérnök 2018/"KÖFOP" szám. 235-251. o.

[85] Nemzeti Kibervédelmi Intézet: IT biztonsági E-learning tanagyagok biztonságtudatos jó gyakorlatok elsajátításához. Forrás: https://nki.gov.hu/it-biztonsag/tanacsok/it-biztonsagi-e-learning-tananyag-a-jo-gyakorlatok-elsajatitasahoz/ Letöltés ideje: 2025. 03. 19.

lönlegessége, hogy a résztvevők nem tudták előre, hogy mely elemek részei a szimulációnak, ami jelentősen növelte a valósághűséget és a képzés hatékonyságát.[86]

„Real life" tesztek a gyakorlatban

Aldawood és Skinner kutatásukban részletesen elemezték a „real life" tesztek hatékonyságát a kiberbiztonsági tudatosság növelésében. A szerzők meghatározása szerint a „real life" tesztek olyan nem bejelentett, valós munkakörnyezetben végrehajtott gyakorlatok, amelyek célja a biztonsági protokollok betartásának ellenőrzése és a felhasználói viselkedés értékelése. Ilyenek többek között:

a) Tűzriadó utáni biztonsági ellenőrzések: A tűzriadók után végzett szisztematikus ellenőrzések során jelentős arányban találtak zárolás nélkül hagyott számítógépeket, ami jelentős biztonsági kockázatot jelent. A szerzők által kidolgozott módszertan szerint a tűzriadók kiváló lehetőséget biztosítanak a nem bejelentett biztonsági ellenőrzésekre, mivel a felhasználók valós vészhelyzeti protokollokat követnek.
b) Céges USB-eszközök „elvesztése": A kutatás során a szervezet különböző pontjain szándékosan „elvesztett" USB-eszközök nagy részét csatlakoztatták a felhasználók a vállalati hálózathoz anélkül, hogy előzetesen ellenőrizték volna azok biztonságosságát. Ez a módszer különösen hatékonynak bizonyult a biztonságtudatosság hiányosságainak feltárásában.[87]

[86] Švábenský, V., Vykopal, J., Cermak, M., & Laštovička, M.: Enhancing cybersecurity skills by creating serious games. In: Proceedings of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education. 2018. 194-199. o.
[87] Aldawood, Hussain – Skinner, Geoffrey: Reviewing cyber security social engineering training and awareness programs -Pitfalls and ongoing issues. Future internet, 2019, 11 (3), 73. sz.

c) Álcázott adathalász kampányok: Heartfield és Loukas (2018) kutatása során a belső IT-osztály nevében küldött, céges arculattal rendelkező adathalász e-mailek a címzettek jelentős részét sikeresen megtévesztették, és a felhasználók megadták hitelesítő adataikat. A szerzők megállapítják, hogy az ilyen belső tesztek, ha megfelelő visszajelzéssel és oktatással párosulnak, jelentősen növelik a felhasználók éberségét a valódi támadásokkal szemben.[88]
d) Álcázott social engineering kísérletek: Több kísérlet során bebizonyosodott, hogy az álcázott telefonos social engineering kísérletek során, ahol az elkövető IT-támogatónak adta ki magát, a felhasználók jelentős része hajlandó volt megosztani jelszavát vagy más érzékeny információt. Ezek az eredmények rávilágítanak a rendszeres képzések fontosságára a social engineering támadások elleni védekezésben[89].

A felhasználói tudatosság mérése és hatékonyságvizsgálata

A programok sikeressége szempontjából az is rendkívül lényeges, hogy az oktatás tartalma kapcsolódjon a munkavállalók napi tevékenységeihez, így a munkakörükre vonatkozó konkrét példák és szituációk alkalmazása elengedhetetlen. Ezen kívül az interaktív elemek (pl. szimulációk, játékok) bevonása az oktatási folyamatba jelentősen növeli a felhasználók elköteleződését és a tanultak gyakorlati alkalmazásának esélyeit. Alshaikh átfogó kutatása empirikusan alátámasztja a felhasználói tudatosság jelentőségét a szervezeti kiberbiztonsági védelem szempontjából. A tanulmány számos szervezet bevonásával mutatta ki, hogy a strukturált kiberbiztonsági tudatosságnövelő programok jelentősen csökkentik a sikeres kibertámadások számát. A kutatás kiemeli, hogy a kiberbiztonsági incidensek nagy része

[88] Heartfield, Ryan; Loukas, George: Detecting semantic social engineering attacks with the weakest link: Implementation and empirical evaluation of a human-as-a-security-sensor framework. Computers & Security 2018/76. szám. 101-127. o.
[89] Mouton, Francois – Leenen, Louise – Venter, Hein S.: Social engineering attack examples, templates and scenarios. Computers & Security 2016/59. szám. 186-209. o.

emberi hibákra vezethető vissza, így a felhasználók képzése kritikus fontosságú a szervezeti biztonság fenntartásában.[90] Bada és Nurse (2019) kifejlesztettek egy komplex mérési keretrendszert, amely lehetővé teszi a felhasználói tudatosság objektív értékelését. A keretrendszer négy fő dimenzióban értékeli a felhasználói tudatosságot: ismereti szint, attitűd, viselkedés és készségek. A kutatók szerint a tudatosságnövelő programok hatékonyságának valós mérése csak több dimenzió együttes vizsgálatával lehetséges, mivel az elméleti ismeretek nem feltétlenül tükröződnek a gyakorlati viselkedésben. A rendszeres, tudományosan megalapozott oktatási programok a tanulmányok szerint hatékonyabbak a kiberbiztonsági incidensek kezelésében, és a folyamatos képzések, különösen a negyedévente ismétlődők, hatékonyabbak az éves képzéseknél. A kutatási eredmények megerősítik, hogy a felhasználói tudatosság fejlesztése alapvető eleme a modern kiberbiztonsági stratégiáknak.[91]

A jogosultságkezelés és felhasználói tudatosság kapcsolata

A jogosultságkezelési folyamatok hiányosságai jelentős kockázatot jelentenek a szervezetek számára. A leggyakoribb probléma az adminisztratív hozzáférések túlzottan széles körű biztosítása, ami megnyitja az utat mind a szándékos visszaélések, mind a véletlenszerű károkozás előtt. Különösen kritikus ez a közszférában és az infrastruktúra területén, ahol az adatszivárgások és a jogosultságokkal való visszaélések kiemelt kockázati tényezőt jelentenek. A minimális jogosultság elvének következetes betartása – vagyis hogy minden felhasználó csak a munkájához feltétlenül szükséges hozzáféréseket kapja – kulcsfontosságú az adatszivárgások megelőzésében. Krasznay kutatása szerint a közszféra szervezeteinek jelentős részénél hiányoznak a megfelelő jogosultságkezelési protokollok, amit súlyosbít,

[90] Alshaikh, Moneer: Developing cybersecurity culture to influence employee behavior: A practice perspective. Computers & Security, 2020, 98: 102003.
[91] Bada, Maria – Sasse, Angela M. – Nurse, Jason RC: i.m.

hogy a közigazgatásban dolgozók kiberbiztonsági képzettsége nem megfelelő szintű, ami közvetlenül hozzájárul a jogosultságkezelési problémákhoz és az adatszivárgások kockázatának növekedéséhez.

A helyzet javításához elengedhetetlen egy biztonságos jogosultságkezelési rendszer kiépítése és az adatvédelmi protokollok szigorú betartása. A tanulmány következtetése szerint a közszféra szervezeteinek sürgősen fejleszteniük kell kiberbiztonsági gyakorlataikat, különös tekintettel a jogosultságkezelésre és az adatvédelemre. A megoldás része lehet a személyes jelenléttel zajló képzési események szervezése. A gyakorlati workshopok és szemináriumok kiemelkedően hatékonynak bizonyulnak a komplex biztonsági koncepciók átadásában és a gyakorlati készségek fejlesztésében. A tapasztalatok azt mutatják, hogy az aktívan részt vevő alkalmazottak eredményesebben azonosítják a potenciális biztonsági fenyegetéseket a valós munkakörnyezetben. Ez a gyakorlatorientált megközelítés nemzetközileg is igazolt módszer a kiberbiztonsági tudatosság hosszútávú és fenntartható fejlesztésére.

Kiberbiztonsági kultúra kialakítása a szervezeteken belül

A modern szervezetek működésében a kiberbiztonság és a felhasználói oktatás alapvető szerepet tölt be a komplex biztonsági architektúra megteremtésében és fenntartásában. A kiberfenyegetések folyamatos evolúciója miatt a munkavállalók megfelelő felkészültsége és tudatossága nélkülözhetetlen az eredményes védekezési stratégiák szempontjából. A szervezeti kiberbiztonsági kultúra kialakítása nem korlátozódik csupán technikai jellegű intézkedések bevezetésére, hanem magában foglalja a munkavállalók attitűdjeinek és viselkedésmintáinak mélyreható és szisztematikus átalakítását is.[92]

A kiberbiztonsági kultúra sikeres megteremtésében meghatározó szerepet játszik a vezetői elköteleződés. A felsővezetés által demonstrált példamutató magatartás és a kiberbiztonság stratégiai szintű kezelése kettős ha-

[92] Bulgurcu, Burcu – Cavusoglu, Hasan – Benbasat, Izak: i.m.

tást gyakorol: egyrészt közvetlenül befolyásolja a munkavállalók hozzáállását a biztonsági előírásokhoz, másrészt formálja hosszútávú elköteleződésüket a szervezeti kultúra iránt. A kutatások szerint a vezetői példamutatás és a rendszeres kommunikáció a kiberbiztonság fontosságáról 37%-kal növeli a munkavállalók motivációját a biztonsági protokollok betartására. Hu és társai tanulmánya rámutat, hogy a következetes vezetői támogatás és figyelem 2-3 év alatt képes jelentősen átalakítani a szervezet kiberbiztonsági kultúráját, ami a biztonsági incidensek számának átlagosan 40%-os csökkenéséhez vezet.[93] Az alkalmazottak tudatosságának növelése kulcsfontosságú szerepet játszik a kiberbiztonsági kultúra kialakításában. A rendszeresen megvalósított, tudományosan megalapozott képzési programok és tudatosságnövelő kampányok elengedhetetlenek a munkavállalók kiberbiztonsági kompetenciáinak folyamatos fejlesztéséhez. Az interaktív oktatási módszerek, mint például a workshopok és a szituációs gyakorlatok, különösen hatékonyak, mivel a valós incidensek elemzésén alapuló tréningek segítenek a gyakorlati tudás megszilárdításában. A célzott kampányok hatékonyságát tovább növeli a többcsatornás kommunikációs stratégia alkalmazása, amely lehetővé teszi az üzenetek széleskörű elérését és rendszeres visszamérésekkel történő ellenőrzését, ezáltal biztosítva az adaptív fejlesztési programok megvalósítását.[94]

A nyílt kommunikáció alapvető fontosságú a szervezeti kiberbiztonsági kultúra megerősítése érdekében. A kiberbiztonsági információk transzparens és rendszeres megosztása, valamint a kétirányú kommunikációs csatornák kialakítása nem csupán a bizalom építésében játszik kulcsszerepet, hanem hozzájárul a biztonsági protokollok hatékony betartásához is. A rendszeres biztonsági tájékoztatók megtartása, a dokumentált eljárásrendek

[93] Hu, Qing – Dinev, Tamara – Hart, Paul – Cooke, Donna: Managing employee compliance with information security policies: The critical role of top management and organizational culture. Decision Sciences 2012/4. szám. 615-660. o.
[94] Hadnagy, Christopher: Social engineering: The science of human hacking. John Wiley & Sons. 2018.

kidolgozása és az incidensjelentési protokollok standardizálása biztosítják a szervezeti átláthatóságot és felelősségvállalást.[95]

Siponen, Mahmood és Pahnila (2014) tanulmánya rávilágít arra, hogy a kiberbiztonsági felelősségvállalás kiterjesztése a szervezetek egészére, minden munkavállalóra jelentős hatással van a szervezeti védelem hatékonyságára. Kutatásukban azt találták, hogy azokban a szervezetekben, ahol a munkavállalók aktívan részt vesznek a kiberbiztonsági intézkedésekben, 37%-kal kevesebb sikeres kibertámadás történt. A tanulmány hangsúlyozza, hogy a felelősségvállalás növeli a munkavállalók tudatosságát saját szerepükkel kapcsolatban, ami 42%-kal nagyobb eséllyel vezet a biztonsági protokollok betartásához és az incidensek jelentéséhez. A kutatók kiemelik, hogy az aktív munkavállalói részvétel gyorsabb észleléshez és kezeléshez vezet, ami átlagosan 45%-kal javítja az incidensek kezelésének hatékonyságát. Továbbá, a dolgozók bevonása a kiberbiztonsági stratégiák kialakításába növeli az elkötelezettséget, ami 31%-kal magasabb szabálykövetési arányt eredményez. Siponen és társai kutatása egyértelműen alátámasztja, hogy a munkavállalók kiberbiztonsági felelősségének növelése elengedhetetlen a szervezetek ellenálló képességének fokozásában. Az aktív részvétel és a felelősségvállalás pozitív hatással van a szervezeti kiberbiztonsági kultúrára, és jelentősen csökkenti a kibertámadások sikeres végrehajtásának esélyét.[96]

A pozitív kiberbiztonsági viselkedések ösztönzésére javasolt jutalmazási rendszerek bevezetése fontos eszköz lehet. A munkavállalók elismerése motiválhatja őket arra, hogy aktívan vegyenek részt a szervezet védelmi intézkedéseiben. A jutalmazási rendszerek alkalmazása jelentősen növelheti a dolgozók elkötelezettségét és a biztonsági protokollok betartását. A kiberbiztonsági kultúra folyamatos értékelése és fejlesztése elengedhetetlen. A rendszeres felmérések, auditok és visszajelzések lehetőséget

[95] Bulgurcu, Burcu – Cavusoglu, Hasan – Benbasat, Izak: i.m.
[96] Siponen, Mikko – Mahmood, M. Adam – Pahnila, Seppo: Employees' adherence to information security policies: An exploratory field study. Information & management 2014/2. szám. 217-224. o.

biztosítanak a szervezetek számára, hogy azonosítsák a gyenge pontokat és a fejlesztési lehetőségeket. A folyamatos értékelések révén a szervezetek rugalmasan tudnak alkalmazkodni a változó kiberfenyegetésekhez, és szükség esetén frissíthetik a biztonsági intézkedéseiket.[97]

A kiberbiztonsági gyakorlatok mindennapi munkafolyamatokba való integrációja elengedhetetlen. A biztonsági protokollok betartását, a jelszókezelést és az adatbiztonsági intézkedések folyamatos alkalmazását természetes módon kell beépíteni a szervezetek napi működésébe. Ez elősegíti, hogy a munkavállalók biztonságtudatosan végezzék feladataikat A rendszeres tréningek, e-learning kurzusok és szimulált támadási gyakorlatok mind hozzájárulnak ahhoz, hogy a munkavállalók felkészültek legyenek a kiberbiztonsági kihívások kezelésére.[98]

A felhasználói tudatosság növelése a rendőrségen belül

A rendőrség kiemelkedő szerepet játszik a társadalom biztonságának fenntartásában, a kibervédelem és a kiberbiztonság egyre nagyobb jelentőséggel bír. A rendőrség, mint közszolgáltató intézmény, érzékeny adatokat kezel, és gyakran szembesül kiberfenyegetésekkel, beleértve az adatlopást, a zsarolóvírusokat, valamint az állami vagy szervezett bűnözői csoportok által végrehajtott támadásokat. A hatékony kiberbiztonsági működés és a felhasználói tudatosság növelése kulcsfontosságú a szervezet ellenálló képességének növelésére és a közbizalom megőrzésére. A rendőrségi szervezetek egyre inkább függenek az információs technológiáktól, ami növeli sebezhetőségüket a kibertámadásokkal szemben. A hagyományos bűnözéssel való küzdelem mellett a rendőrségnek a kiberbűnözés új formáival is meg

[97] Bada, Maria – Sasse, Angela M. – Nurse, Jason RC: i.m.

[98] Bauer, Stefan – Benroider, Edward WN.: From information security awareness to reasoned compliant action: analyzing information security policy compliance in a large banking organization. ACM SIGMIS Database: the DATABASE for Advances in Information Systems, 2017, 48.3: 44-68. o.

kell birkóznia, ami folyamatos képzést és technológiai fejlesztéseket igényel.[99]

Az informatikai rendszerek biztonságos használata szempontjából kritikus tényező, hogy a rendészeti dolgozók megfelelő ismeretekkel rendelkezzenek a kiberbiztonsági kockázatokról. A rendőrség által használt informatikai rendszerek sebezhetőségei megkérdőjelezik a hagyományos bűnüldözési eszközök hatékonyságát a kiberbűnözés elleni harcban. A rendőrségnek új készségeket és technológiákat kell elsajátítania, beleértve a digitális forenzikus eszközöket és a hálózati biztonsági megoldásokat.[100] A felhasználói tudatosság növelése elengedhetetlen ahhoz, hogy a rendőrségi alkalmazottak hatékonyan felismerjék a kibertámadások jeleit és minimalizálják a támadások kockázatát az adatbiztonsági protokollok betartásával.

A kiberbiztonsági tudatosságnövelő kampányok gyakran kudarcot vallanak, mert nem veszik figyelembe a viselkedésváltozás pszichológiai aspektusait. A képzési programoknak nem csupán az ismeretek átadására, hanem az attitűdök és szokások megváltoztatására is fókuszálniuk kell, beleértve a rendszeres gyakorlati szimulációkat és a személyre szabott visszajelzéseket is.[101]

A rendőrségi dolgozók szakterület-specifikus képzése elengedhetetlen a kiberbiztonsági képzések hatékonyságának növeléséhez, különösen a bűnügyi nyomozás terén, ahol informatikai rendszereket és adatokat használnak fel a bűncselekmények felderítéséhez. A célzott képzési programok növelik a dolgozók tudatosságát és javítják a kiberbiztonsági incidensek kezelésének sikerességét. A rendőrségi képzéseknek specifikus modulokat kell tartalmazniuk a kiberbűnözés különböző formáira, a digitális bizonyí-

[99] Bossler, Adam M. – Holt, Thomas J.: Patrol officers' perceived role in responding to cybercrime. Policing: an international journal of police strategies & management, 2012, 35.1: 165-181. o.
[100] Leppänen, Anna – Kirauvo, Timo – Kajantie, Sari: Policing the cyber-physical space. The police journal, 2016, 89.4: 290-310. o.
[101] Bada, Maria – Sasse, Angela M. – Nurse, Jason RC: i.m.

tékok kezelésére és a kibertérben történő nyomozási technikákra összpontosítva.[102] A kiberbiztonsági képzésekben a digitális bizonyítékok kezelésére és a kibertérben történő nyomozási technikákra való összpontosítás elengedhetetlen a hatékony kiberbűnözés elleni fellépéshez. A digitális bizonyítékok beszerzése és kezelése során fontos az eredetiség és hitelesség megőrzése, amely különleges szakértelmet és technológiát igényel, mivel a hagyományos bizonyítékok beszerzésétől és lefoglalásától eltérő módon végezhető el.[103] A kibertérben történő nyomozás során a technológiai fejlődés és a kiberbűnözés változó módszerei miatt folyamatosan frissíteni kell a nyomozási technikákat, és szükség van a nemzetközi együttműködésre is.[104] Az információbiztonsági menedzsmentnek holisztikus megközelítést kell alkalmaznia, beleértve a technológiai megoldásokat, a szervezeti folyamatokat, az emberi tényezőket és a jogi megfelelőséget. A rendszeres kockázatértékelés, a folyamatos monitoring és az incidenskezelési tervek fontos szerepet játszanak.[105] A kibervédelmi stratégiák és a biztonságtudatossági programok beépítése a szervezeti kultúrába és a felsővezetés aktív támogatása nélkül a kiberbiztonsági programok nem működnek hatékonyan. A kiberbiztonság túlmutat a hagyományos információbiztonságon; ki kell terjednie minden olyan eszközre és infrastruktúrára, amely a kibertérhez kapcsolódik. A rendőrség esetében ez magában foglalja a rendőrségi járművek kommunikációs rendszereit, a testkamerákat és más IoT-

[102] Holt, Thomas J. – Bossler, Adam M: Predictors of patrol officer interest in cybercrime training and investigation in selected United States police departments. Cyberpsychology, Behavior, and Social Networking, 2012, 15.9. 464-472. o.
[103] Gyaraki Réka: A számítógépes bűnözés nyomozásának problémái. PhD értekezés. PTE-ÁJK Doktori Iskola. Pécs, 2018. Forrás: https://ajk.pte.hu/files/file/doktori-iskola/gyaraki-reka/gyaraki-reka-muhelyvita-ertekezes.pdf Letöltés ideje: 2025. 03. 14.
[104] Grund Borbála: A kibertér bűncselekményeiről és a kiberbűnözés hazai gyakorlatáról. Forrás: https://jog.tk.hu/mtalwp/a-kiberter-buncselekmenyeirol-es-a-kiberbunozes-hazai-gyakorlatarol?download=pdf Letöltés ideje: 2025. 03. 14.
[105] Soomro, Zahoor Ahmed – Shah, Mahmood Hussain – Ahmed, Javed: Information security management needs more holistic approach: A literature review. International journal of information management, 2016, 36.2. 215-225. o.

eszközöket. A vezetői elkötelezettség kulcsszerepet játszik a kiberbiztonsági kultúra kialakításában.[106]

A rendészeti szervek számára elengedhetetlen a folyamatos fejlődés és alkalmazkodás a kiberbiztonsági irányelvek, az adatvédelmi szabályok és a felhasználói tudatosság terén a gyorsan változó technológiai környezetben. A kiberbiztonság nem csupán technikai kérdés, hanem kulturális és oktatási kihívás is, amely megköveteli a rendőrségi dolgozók aktív részvételét a kiberbiztonsági kultúra kialakításában és fenntartásában. A hatékony kiberbiztonsági stratégia kialakítása érdekében a rendőrségnek komplex, többrétű megközelítést kell alkalmaznia. A folyamatos képzés és a gyakorlati szimulációk szerepe kiemelkedő, hiszen ezek segítik a rendőrségi dolgozókat a kibertámadások hatékony észlelésében és kezelésében. Életszerű forgatókönyvek alkalmazása a képzési programokban, mint például az adathalászat és social engineering támadások szimulációja, lehetőséget biztosít a gyakorlati tapasztalatok megszerzésére.

A rendőrségi kiberbiztonsági képzésekben három fő szintet lenne célszerű központilag bevezetni: alapszintű, középszintű és emelt szintű képzést. Az alapszintű képzés minden rendőrségi dolgozó számára kötelező legyen, és olyan alapvető kiberbiztonsági ismereteket tartalmazzon, mint a jelszókezelés, kétfaktoros hitelesítés, adatok titkosítása, adathalász támadások felismerése és elkerülése, biztonságos internethasználat rendőrségi eszközökön, incidensjelentési protokollok és eljárások, valamint mobil eszközök biztonságos használata. A középszintű képzés a kiberbűnözéssel gyakrabban találkozó kollégák számára készüljön, és digitális bizonyítékok alapszintű kezelését és biztosítását, kiberbűncselekmények felismerését és kategorizálását, online nyomozási technikák alapjait, adatvédelmi előírások gyakorlati alkalmazását, valamint áldozatsegítést digitális bűncselekmények esetén tartalmazzon. Az emelt szintű képzés a kibernyomozóknak és specialistáknak szóljon, és fejlett digitális forenzikus technikákat,

[106] Von Solms, Rossouw – Johan Van Niekerk: From information security to cyber security. In: computers & security 38. 2013. 97-102. o.

malware-analízis alapjait, hálózati forgalom elemzését, titkosított kommunikáció és darkweb nyomozási technikákat, valamint nemzetközi együttműködést a határokon átnyúló kiberbűncselekmények esetén foglaljon magába. A képzések hatékonyságának mérése és folyamatos fejlesztése kulcsfontosságú legyen a rendőrségi kiberbiztonsági tudatosság fenntartásához, amelyhez rendszeres tudásfelmérések, szimulált támadások és teljesítményértékelések szükségesek. A képzési programok tartalmát folyamatosan frissíteni kell a legújabb kiberfenyegetések és támadási módszerek alapján, szoros együttműködésben a nemzeti kiberbiztonsági központokkal és nemzetközi rendvédelmi szervezetekkel.

A szervezeti kultúra fejlesztése szintén elengedhetetlen, mivel a kiberbiztonsági értékek integrálása a mindennapi működésbe növeli a közös felelősséget a biztonság megőrzésében. A vezetői elköteleződés kulcsszerepet játszik a kiberbiztonsági kezdeményezések támogatásában, ezért fontos, hogy a felsővezetés aktívan részt vegyen a képzésekben és a stratégiai döntésekben.

A felhasználói tudatosság növelése érdekében rendszeres információs kampányokat kell indítani, amelyek a kiberbiztonsági tudatosságot célozzák meg, valamint személyre szabott visszajelzések révén segítik a munkatársak fejlődését. A technológiai fejlesztések bevezetése, például fejlett kiberbiztonsági eszközök alkalmazása és a személyes adatok védelmét szolgáló intézkedések szintén alapvetőek a kibertámadások megelőzése érdekében.

A rendőrségnek továbbá érdemes együttműködnie más szervezetekkel, beleértve a kormányzati és magánszektorbeli partnereket, hogy megossza a legjobb gyakorlatokat és tapasztalatokat. A nemzetközi képzéseken való részvétel lehetőséget ad a legújabb trendek és technológiák megismerésére, hozzájárulva a kiberbiztonsági tudás bővítéséhez. Összességében a rendőrségnek integrált, folyamatosan fejlődő kiberbiztonsági megközelítést kell alkalmaznia a 21. század kihívásainak hatékony kezelésére és a közbizalom megőrzésére.

Az Európai Unió által 2022-ben elfogadott NIS2 (Network and Information Systems Directive) irányelv implementációja a rendvédelmi szervek számára is új megfelelőségi követelményeket támaszt, különös tekintettel az incidensjelentési kötelezettségekre és a kockázatértékelési eljárásokra. Az irányelv alapján a nagy kockázatú szervezeteket – amilyenek tipikusan a közigazgatási intézmények is – pénzbírságokkal sújthatják a megfelelés hiánya esetén. Ennek következtében nem csupán a vezetőség, hanem a teljes szervezet közös érdeke a megfelelés biztosítása és a folyamatos minősítések megszerzése. Ebben a kontextusban érdemes megvizsgálni azt a kérdést, hogy a minősítést kiadó felügyeleti szervek miért nem tényleges penetrációs tesztek vagy szimulált kibertámadások alapján értékelik a szervezetek felkészültségét. A valós helyzeteket modellező gyakorlati próbák sokkal pontosabb képet adhatnának a kiberbiztonsági kultúra tényleges érettségéről és hatékonyságáról, mint a pusztán dokumentációs és adminisztratív megfelelés ellenőrzése. Ez a megközelítés lehetővé tenné a valódi sebezhetőségek azonosítását és a kiberbiztonsági kultúra gyakorlati dimenzióinak fejlesztését, ami különösen fontos a közigazgatási szervezetek esetében, ahol gyakran érzékeny adatok és kritikus infrastruktúrák védelme a tét. A NIS2 irányelv implementációja során a rendvédelmi szervek különleges státuszának figyelembevétele kulcsfontosságú, hogy a műveleti titkosságot ne veszélyeztesse, miközben hatékonyan alkalmazkodnak az új megfelelőségi követelményekhez, beleértve az incidensjelentési kötelezettségeket és a kockázatértékelési eljárásokat. A rendészeti szervek együttműködése a kiberbűnözés elleni fellépés során fontos, de jelenleg hiányoznak azok a szabályozók, akciótervek és módszertani utasítások, amelyek a feladatokat, felelősöket és határidőket rögzítenék. Az operatív szinten a nemzeti kiberkoordinátor és a munkacsoportok szintjén valósul meg a működés, de a bűnüldözési folyamatok összehangolása gyakran ad-hoc megoldásokhoz kötődik. A kiberbiztonsági stratégia megalkotása politikai

szinten valósult meg, de az operatív és taktikai szinteken további normák és szakmai szabályok kidolgozása szükséges.[107]

A GovCERT és a Nemzeti Elektronikus Információbiztonsági Hatóság (NEIH) fontos szerepet játszik a kibervédelemben, az incidenskezelésben és a jogszabályi előírások ellenőrzésében. Ezek a szervezetek hathatós segítséget nyújthatnak a rendvédelmi szerveknek a kiberfenyegetések kezelésében, és lehetővé teszik az információk megosztását a határon átnyúló kibertámadások esetén. A rendészeti informatikai szakképzés fejlesztése is elengedhetetlen, hogy a szervezetek rendelkezzenek olyan szakemberekkel, akik képesek kezelni a kiberbiztonsági kihívásokat.[108] A NIS2 irányelv által előírt követelmények, mint például a kockázatelemzés, az eseménykezelés és a tudatosságnövelés, alapvetőek a szervezetek rezilienciájának erősítéséhez a kiberbiztonsági fenyegetésekkel szemben. Magyarországon a NIS2 követelményeinek való megfelelést első ízben a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről szóló 2023. évi XXIII. törvény (a továbbiakban: Kibertan törvény) szabályozta, amely a kiberbiztonsági tanúsítás és felügyelet hatósági feladatait is meghatározta. A Kibertan törvény részletesen szabályozta a kiberbiztonsági tanúsítási rendszereket, a tanúsító hatóságok feladatait, a megfelelőségértékelést és a piacfelügyeleti intézkedéseket. A Kibertan törvényt a Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény (a továbbiakban: Kiberbiztonsági törvény) 2025. január 1-jei hatályba lépésével hatályon kívül helyezte a Kibertan törvényt. A Kiberbiztonsági törvény célja, hogy biztosítsa az elektronikus információs rendszerek és digitális eszközök biztonságát, hozzájárulva a gazdasági tevékenységek zavartalan folytatásához, a pénzügyi veszteségek elkerüléséhez és a felhasználók bizalmának megőrzéséhez. Az érintett szervezeteknek gondoskodniuk kell az elektronikus információs rendszereik biztonságáról, beleértve a kockázatok feltárását és kezelését, valamint a biztonságot sértő események megelőzését és hatásainak csökkentését. A

[107] Nemzeti Kibervédelmi Intézet: Segédlet a Kiberbiztonsági törvény hatályának értelmezéséhez. Forrás: https://nki.gov.hu/hatosag/tartalom/hataskor/ Letöltés ideje: 2025. 03. 25.
[108] Vásárhelyi, Örs. Magyarország kiberbiztonságának jövője az európai uniós NIS2 irányelv tükrében. Nemzetbiztonsági Szemle 2024/3. szám. 18-35. o.

törvény nem csupán az állami szervek, hanem a kritikus infrastruktúrát üzemeltető szervezetek számára is kötelezővé teszi a kiberbiztonsági intézkedések bevezetését, figyelembe véve a nemzetbiztonsági szempontokat is. A rendőrség, mint a társadalom biztonságának fenntartásában kulcsszerepet játszó szervezet, érzékeny adatokat kezel, és gyakran szembesül kiberfenyegetésekkel. A rendőrségi dolgozók szakterület-specifikus képzése elengedhetetlen a kiberbiztonsági képzések hatékonyságának növeléséhez, különösen a bűnügyi nyomozás terén, ahol informatikai rendszereket és adatokat használnak fel a bűncselekmények felderítéséhez.

Összegzés

A tanulmány egy átfogó elemzést nyújt a kiberbiztonsági kihívásokról, különös hangsúlyt fektetve a felhasználói viselkedés és a kognitív torzítások szerepére a kiberbiztonsági incidensek előfordulásában. Az elemzés célja nem csupán a technológiai megoldások bemutatása, hanem a kiberbűnözés elleni védekezés új, innovatív megközelítéseinek feltérképezése is, amelyek potenciálisan átalakíthatják a kiberbiztonsági stratégiai tervezést és operatív megvalósítást. Alapvető megállapításai közé tartozik a felhasználói magatartás és a kognitív torzítások közötti komplex összefüggések feltárása. Ez a mélyreható elemzés rávilágít arra a paradoxonra, hogy míg a technológiai infrastruktúra folyamatosan fejlődik, az emberi tényező továbbra is a kiberbiztonsági védelem leggyengébb láncszeme. Az emberi kogníció sajátosságainak és a döntéshozatali folyamatok pszichológiai aspektusainak integrálása a kiberbiztonsági stratégiákba lehetővé teszi a széles körű megközelítést, amely túlmutat a hagyományos, pusztán technológiai fókuszú védekezési mechanizmusokon. Az MI és az ML-algoritmusok alkalmazása a viselkedési anomáliák detektálásában kiemelkedő jelentőséggel bír a tanulmányban. A kutatás hangsúlyozza, hogy ezek a fejlett technológiák nemcsak a detekciós képességek exponenciális növekedését eredményezik, hanem lehetővé teszik a potenciális fenyegetések prediktív azonosítását is. Az értekezésben bemutatott esettanulmányok és elméleti

modellek demonstrálják, hogy az ML által támogatott viselkedéselemzés képes olyan szubtilis mintázatok felismerésére, amelyek az emberi elemzők számára gyakran rejtve maradnak. Ezáltal jelentősen kiterjesztik a kiberbiztonsági védelmi rendszerek hatékonyságát és reakcióképességét. A kutatás során különös figyelmet szenteltem a social engineering alapú támadások prevenciójának, amely a modern kiberbűnözés egyik legkomplexebb kihívását jelenti. E támadási formák elsődlegesen az emberi tényező manipulálására építenek, így a felhasználói interakciók szisztematikus elemzése és a viselkedési mintázatok folyamatos monitorozása kulcsfontosságúvá válik. A tanulmány javasolja az integrált megközelítést, amely ötvözi a technológiai megoldásokat a célzott oktatási programokkal és a szervezeti kultúra formálásával, így egy paradigmaváltást jelenthet a social engineering elleni védekezés területén. A gyakorlati implementációs javaslatok, mint például a rendszeres képzések, közösségi tudatosságnövelő programok és online információs platformok kialakítása, konkrét cselekvési terveket kínálnak, amelyek szignifikánsan hozzájárulhatnak a kiberbiztonsági kultúra fejlesztéséhez, mind a rendészeti szerveken belül, mind a társadalom szélesebb rétegeiben. E javaslatok különösen fontosak a rendészeti szervek kontextusában, ahol a kiberbiztonsági incidensek potenciális következményei nemcsak az adott szervezetre, hanem a nemzeti biztonságra is közvetlen hatást gyakorolhatnak. A tanulmányban felvázolt kiberbiztonsági hetek és helyi közösségi rendezvények koncepciója innovatív megközelítést kínál a társadalmi szintű tudatosságnövelésre, ezek a kezdeményezések potenciálisan katalizátorként szolgálhatnak egy kollektív kiberbiztonsági kultúra kialakításában. A tanulmány által javasolt online platformok célja olyan dinamikus tudásbázis létrehozása, amely lehetővé teszi a felhasználók számára a naprakész információkhoz és gyakorlati útmutatókhoz való folyamatos hozzáférést, így erősítve a preventív szemléletet a kiberbiztonság területén. Az általam feltárt összefüggések és javasolt megoldások implementációja ugyanakkor számos kihívást is felvet, különösen a rendészeti szervek speciális működési környezetében. Az adatvédelmi és etikai megfontolások, a technológiai infrastruktúra fejlesztésének

költségvonzatai, valamint a szervezeti kultúra átalakításának komplexitása olyan tényezők, amelyek további kutatást és körültekintő mérlegelést igényelnek a gyakorlati megvalósítás során. A jövőbeli kutatási irányok között indokolt lehet a tanulmányban bemutatott elméleti modellek és gyakorlati javaslatok empirikus validálása, valamint azok hosszútávú hatásainak longitudinális vizsgálata a rendészeti szervek kiberbiztonsági gyakorlatára vonatkozóan. Az ilyen jellegű kutatások nemcsak a javasolt megoldások hatékonyságának kvantifikálását tennék lehetővé, de hozzájárulnának a folyamatos optimalizációhoz és a változó fenyegetettségi környezethez való adaptációhoz is. Továbbá, a nemzetközi komparatív analízis lehetőséget nyújt a különböző jogrendszerek és rendészeti kultúrák kontextusában alkalmazott viselkedéselemzési módszerek hatékonyságának összevetésére. Az ilyen jellegű összehasonlító tanulmányok nemcsak a legjobb gyakorlatok azonosítását segítenék elő, hanem hozzájárulnának egy globális, harmonizált megközelítés kialakításához a kiberbiztonsági kihívások kezelésében. Kiemelt figyelmet kell fordítani az interdiszciplináris együttműködésre a javasolt megoldások implementációja során. A kiberbiztonsági szakemberek, rendészeti tisztviselők, pszichológusok, jogászok és adatvédelmi szakértők együttműködése elengedhetetlen ahhoz, hogy a megoldások ne csupán technológiailag, hanem etikailag is megalapozottak és jogilag konformak legyenek. A jövőkép, amely a felhasználói viselkedéselemzés integrálására épít a rendészeti szervek kiberbiztonsági stratégiájában, potenciálisan paradigmaváltást indíthat el a kiberbűnözés elleni küzdelem területén. Ez a megközelítés nemcsak reaktív védelmet biztosít, hanem proaktív, prediktív képességekkel ruházza fel a rendészeti szerveket, lehetővé téve számukra, hogy egy lépéssel a potenciális fenyegetések előtt járjanak. A tanulmány hangsúlyozza a kiterjesztett megközelítés fontosságát, amely integrálja a technológiai innovációt, a pszichológiai megfontolásokat és a szervezeti kultúra formálását, elengedhetetlen a jövő komplex kiberbiztonsági fenyegetéseivel szembeni hatékony védekezés kialakításához. A felvetett kérdések és javasolt megoldások implementációja nemcsak a kiberbiztonsági védelem hatékonyságának növelését ígéri, de potenciálisan egy

biztonságosabb, ellenállóbb digitális ökoszisztéma kialakításához is hozzájárulhat, amely képes adaptálódni a folyamatosan evolválódó fenyegetettségi környezethez. Tanulmányom elején azon régi rendőrmondásra utaltam, miszerint *„addig nincs baj, amíg nem lopnak mozdonyt, malomkövet vagy parazsat."* Az első kettő már beteljesült. Egyre több nagyszabású adatlopási eset és infrastruktúrát célzó támadás történik. A „parázs" azonban még megmaradt – szimbolizálva azt a reményt, hogy a rendészeti szervek folyamatosan fejlődnek, és a kiberbiztonsági stratégiák kidolgozása során egyre hatékonyabb eszközöket használnak a polgárok adatainak védelmére. A parázs égve tartása azt is jelenti, hogy a rendvédelem nem csupán a megelőzésben, de az elkövetők felderítésében és elfogásában is élen jár, biztosítva ezzel a társadalom számára egy biztonságosabb digitális jövőt.

Irodalomjegyzék

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. Behaviour & information technology, 33(3), 237-248. o.

Afchar, Darius – Nozick, Vincent- Yamagishi, Junichi – Echizen, Isao: Mesonet: a compact facial video forgery detection network. In: 2018 IEEE international workshop on information forensics and security (WIFS). IEEE, 2018. 1-7. o.

Ahmed, M., Mahmood, A. N., & Hu, J. (2016). A survey of network anomaly detection techniques. Journal of Network and Computer Applications, 60, 19-31. o.

Aldawood, H., & Skinner, G. (2019). Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues. Future internet, 11(3), 73. o.

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. Computers & Security, 98, 102003.

Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., ... & Zhou, Y. (2017). Understanding the mirai botnet. In 26th USENIX security symposium (USENIX Security 17) (1093-1110. o.).

Arohan, Y., Yadav, A., Pandey, A., Churi, S., Saxena, M., & Vaghani, A. (2020). An introduction to context-aware security and User Entity Behavior Analytics. International Journal of Advance Research, Ideas and Innovations in Technology, 6(5), 27-33. o.

Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? arXiv preprint arXiv:1901.02672.

Bandura, A., & Hall, P. (2018). Albert bandura and social learning theory. Learning Theories for Early Years, 78. o.

Bányász, P., Bóta, B., & Csaba, Z. (2019). A social engineering jelentette veszélyek napjainkban. In: Biztonság, szolgáltatás, fejlesztés, avagy új irányok a bevételi hatóságok működésében. Magyar Rendészettudományi Társaság Vám- és Pénzügyőri Tagozat, Budapest. 12-37. o. ISBN 9786158056793

Bauer, S., & Bernroider, E. W. (2017). From information security awareness to reasoned compliant action: analyzing information security policy compliance in a large banking organization. ACM SIGMIS Database: the DATABASE for Advances in Information Systems, 48(3), 44-68. o.

Bederna Zs., Váczi D., Pollner P., & Szádeczky T. (2019). Támadás hálózatba szervezve. In: Auer, Ádám; Joó, Tamás (szerk.) Hálózatok a közszolgálatban. Budapest, Magyarország: Dialóg Campus Kiadó (2019) 247, 223-247. o.

Beláz, A., & Berzsenyi, D. (2017). Kiberbiztonsági Stratégia 2.0: A kiberbiztonság stratégiai irányításának kérdései. NKE Stratégiai Védelmi Kutatóközpont Elemzések, 3, 1-15. o.

Bertino, E., & Islam, N. (2017). Botnets and internet of things security. Computer, 50(2), 76-79. o.

Beuran, R., Chinen, K. I., Tan, Y., & Shinoda, Y. (2016). Towards effective cybersecurity education and training.

Bicskei, T. (2023). A mesterséges intelligencia közigazgatásban való felhasználásával okozott kár. KözigazgatásTudomány, 3(1), 99-114. o.

Bossler, A. M., & Holt, T. J. (2012). Patrol officers' perceived role in responding to cybercrime. Policing: an international journal of police strategies & management, 35(1), 165-181. o.

Bradford, Anu: The Brussels effect: How the European Union rules the world. Oxford University Press, 2020.

Buczak, A. L., & Guven, E. (2015). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications surveys & tutorials, 18(2), 1153-1176. o.

Bulgurcu, B., Cavusoglu, H. & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS quarterly, 523-548. o.

Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. ACM computing surveys (CSUR), 41(3), 1-58. o.

Hadarics, K. (2019). Incidens-menedzsment gyakorlat. Nemzeti Közszolgálati Egyetem. Budapest.

Hadnagy, Christopher: Social engineering: The science of human hacking. John Wiley & Sons. 2018.

Happa, J., Glencross, M., & Steed, A. (2019). Cyber security threats and challenges in collaborative mixed-reality. Frontiers in ICT, 6, 5. o.

Heartfield, R., & Loukas, G. (2018). Detecting semantic social engineering attacks with the weakest link: Implementation and empirical evaluation of a human-as-a-security-sensor framework. Computers & Security, 76, 101-127. o.

Holt, T. J., & Bossler, A. M. (2012). Predictors of patrol officer interest in cybercrime training and investigation in selected United States police departments. Cyberpsychology, Behavior, and Social Networking, 15(9), 464-472. o.

Homoliak, I., Toffalini, F., Guarnizo, J., Elovici, Y., & Ochoa, M. (2019). Insight into insiders and it: A survey of insider threat taxonomies, analysis, modeling, and countermeasures. ACM Computing Surveys (CSUR), 52(2), 1-40. o.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. Decision Sciences, 43(4), 615-660. o.

Kiss, A., & Kollár, C. (2024). Az információbiztonság időszerű kérdései a magyarországi kkv-k körében. Scientia et Securitas, 4(2), 98-107. o.

Kovács, L. & Krasznay, Cs. (2017). Digitális Mohács 2.0: kibertámadások és kibervédelem a szakértők szerint. Nemzet és Biztonság–Biztonságpolitikai Szemle, 10(1), 3-16. o.

Krasznay, Cs. (2017). A kiberbiztonság stratégiai vetületeinek oktatási kérdései a közszolgálatban. Nemzet és Biztonság–Biztonságpolitikai Szemle, 10(3), 38-53. o.

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., & Hong, J. (2010). Teaching Johnny not to fall for phish. ACM Transactions on Internet Technology (TOIT), 10(2), 1-31. o.

Legárd, I. (2020). Célpont vagy! –a közszolgálat felkészítése a kiberfenyegetésekre. Hadmérnök, 15(1), 91-105. o.

Leitold, F (2019). A felhasználói viselkedés, mint információbiztonsági kockázat becslése. Konferencia-menedzselő rendszer, networkshop
DOI-azonosító: https://doi.org/10.31915/NWS.2019.24

Leitold, F. (2019b). Practical approach for measuring the level of user behaviour. In 2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA) (1-2. o.). IEEE.

Leppänen, A., Kiravuo, T., & Kajantie, S. (2016). Policing the cyber-physical space. The police journal, 89(4), 290-310. o.

Li, T., Sahu, A. K., Talwalkar, A., & Smith, V. (2020). Federated learning: Challenges, methods, and future directions. IEEE signal processing magazine, 37(3), 50-60. o.

Liu, F., Wen, Y., Zhang, D., Jiang, X., Xing, X., & Meng, D. (2019). Log2vec: A heterogeneous graph embedding based approach for detecting cyber threats within enterprise. In Proceedings of the 2019 ACM SIGSAC conference on computer and communications security (1777-1794. o.).

Mandić, D., & Kiss, G. (2024). Password usage in hungary and slovakia among users of smart devices. Biztonságtudományi Szemle, 6(2.), 57-67. o.

Molnár L. (2020) Mesterséges intelligencia a közigazgatásban. In: Sasvári, Péter (szerk.) Informatikai rendszerek a közszolgálatban I. Budapest, Magyarország: Ludovika Egyetemi Kiadó (2020) 215 189-215. o.

Morsella, E., Bargh, J. A., & Gollwitzer, P. M. (2008). Social cognition and social neuroscience.

Mouton, F., Leenen, L., & Venter, H. S. (2016). Social engineering attack examples, templates and scenarios. Computers & Security, 59, 186-209. o.

Muha, L., & Krasznay, Cs. (2018). Az elektronikus információs rendszerek biztonságának menedzselése. Nemzeti Közszolgálati Egyetem.

Munk, S. (2018). A kibertér fogalmának egyes, az egységes értelmezést biztosító kérdései. Hadtudomány: A Magyar Hadtudományi Társaság Folyóirata, 28(1), 113-131. o.

Nagy, Z. (2020). A kiberbűncselekmények fogalma és csoportosítása. Kiss, T.(szerk.) Kibervédelem a bűnügyi tudományokban. Budapest: Dialóg Campus, 33-44. o.

Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. computers & security, 56, 70-82. o.

Sasvári, P. (2020). Informatikai rendszerek a közszolgálatban II. (P. Sasvári, Ed.). Budapest: Ludovika Egyetemi Kiadó.
DOI-azonosító: http://doi.org/10.36250/00733.00

Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. Information & Management, 51(2), 217-224. o.

DOI-azonosító: https://doi.org/10.1016/j.im.2013.08.006

Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. In 2010 IEEE symposium on security and privacy (305-316. o.). IEEE.

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. International journal of information management, 36(2), 215-225. o.

Stupp, C. (2019). Fraudsters used AI to mimic CEO's voice in unusual cybercrime case. The Wall Street Journal, 30(08).

Sur, S., El-Dosuk, M., & Kamel, S. (2024). MACHINE LEARNING TECHNIQUES FOR CYBER SECURITY. Journal of Theoretical and Applied Information Technology, 102(7).

András, S. (2018). Technikai kiberbiztonsági gyakorlatok–Nemzetközi kitekintés. Hadmérnök, 13(1), 286-301. o.

András, S. (2018). Ajánlás TTX gyakorlatok szervezéséhez. Hadmérnök, 2018, 13. "KÖFOP" szám. 235-251. o.

Švábenský, V., Vykopal, J., Cermak, M., & Laštovička, M. (2018, July). Enhancing cybersecurity skills by creating serious games. In Proceedings of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education (pp. 194-199).Szádeczky, T. (2020). Big Data a közigazgatásban In: Sasvári, Péter (szerk.) Informatikai rendszerek a közszolgálatban I. Budapest, Magyarország: Ludovika Egyetemi Kiadó (2020) 215, 113-126. o.

T. Nagy, L. (2023). Mesterséges intelligencia, multimédia, tanulástámogatás.

Tsinganos, N., Sakellariou, G., Fouliras, P., & Mavridis, I. (2018). Towards an automated recognition system for chat-based social engineering attacks in enterprise environments. In Proceedings of the 13th International Conference on Availability, Reliability and Security (1-10. o.).

Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2015). Managing the introduction of information security awareness programmes in organisations. European Journal of Information Systems, 24(1), 38-58. o.

Vásárhelyi, Örs. Magyarország kiberbiztonságának jövője az európai uniós NIS2 irányelv tükrében. Nemzetbiztonsági Szemle, 2024, 12.3: 18-35. o.

Von Solms, R., Van Niekerk, J. (2013). From information security to cyber security. computers & security, 38, 97-102. o.

Workman, M. (2008). Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. Journal of the American society for information science and technology, 59(4), 662-674. o.

Internetes források

America's Cyber Defense Agency (2022). 2021 Trends Show Increased Globalized Threat of Ransomware.
Forrás: https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-040a
Letöltés ideje: 2024.09.23.

Cimpanu, C. (2021). "REvil asks for $70 million to decrypt systems impacted in Kaseya ransomware attack." The Record by Recorded Future.
Forrás: https://therecord.media/revil-gang-asks-70-million-to-decrypt-systems-locked-in-kaseya-attack
Letöltés ideje: 2024.09.19.

Court of Justice of the European Union: Judgment in Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems, 2020.
Forrás: https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf
Letöltés ideje: 2025.03.15.

Entrust: Fraud Report. Entrust Corporation, Minnesota, 2024.
Forrás: https://www.entrust.com/sites/default/files/documentation/reports/entrust-fraud-report.pdf
Letöltés ideje: 2025.03.15.

European Union Agency for Cybersecurity (2023). Ensia Threat Landscape 2023.
Forrás: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023
Letöltés ideje: 2024.09.23.

Europol (2024). Internet Organised Crime Threat Assessment (IOCTA).
Forrás: https://www.europol.europa.eu/cms/sites/default/files/documents/Internet%20Organised%20Crime%20Threat%20Assessment%20IOCTA%202024.pdf
Letöltés ideje: 2024.09.23.

https://www.radware.com/cyberpedia/ddos-attacks/noname057(16)/
Letöltés ideje: 2024.09.21.

Grund Borbála: A kibertér bűncselekményeiről és a kiberbűnözés hazai gyakorlatáról.
Forrás: https://jog.tk.hu/mtalwp/a-kiberter-buncselekmenyeirol-es-a-kiberbunozes-hazai-gyakorlatarol?download=pdf
Letöltés ideje: 2025.03.14.

Gyaraki Réka: A számítógépes bűnözés nyomozásának problémái. PhD értekezés. PTE-ÁJK Doktori Iskola. pécs, 2018.
Forrás: https://ajk.pte.hu/files/file/doktori-iskola/gyaraki-reka/gyaraki-reka-muhelyvita-ertekezes.pdf
Letöltés ideje: 2025.03.14.

IBM (2024). Cost of a Data Breach Report 2024.
Forrás: https://www.ibm.com/reports/data-breach
Letöltés ideje: 2024.09.12.

ICS Cyber Security Blog: A Kaseya-incidens és annak tágabb összefüggései.
Forrás: https://icscybersec.blog.hu/2021/07/10/kaseya-incidens-osszefuggesei
Letöltés ideje: 2025.03.12.

Keumars Afifi-Sabet: SolarWinds blames intern for weak ‘solarwinds123’ password.

Forrás: https://www.itpro.com/security/cyber-attacks/358738/intern-blamed-for-weak-password-that-may-have-sparked-solarwinds
Letöltés ideje: 2025.03.16.

Lázár Fruzsina (2023): A kibertér veszélyei: zsarolóvírus és adatszivárogtatás.
Forrás: https://behaviour.hu/a-kiberter-veszelyei-zsarolovirus-es-adatszivarogtatas/
Letöltés ideje: 2024.09.28.

Nemzeti Kibervédelmi Intézet (2021): IT biztonsági E-learning tanagyagok biztonságtudatos jó gyakorlatok elsajátításához.
Forrás. https://nki.gov.hu/it-biztonsag/tanacsok/it-biztonsagi-e-learning-tananyag-a-jo-gyakorlatok-elsajatitasahoz/
Letöltés ideje: 2025.03.19.

Nemzeti Kibervédelmi Intézet (2024): Éves kiberbiztonsági jelentés.
Forrás: https://nki.gov.hu/wp-content/uploads/2024/07/Eves-kiberbiztonsagi-jelentes.pdf
Letöltés ideje: 2024.09.23.

Nemzeti Kibervédelmi Intézet (2025): Segédlet a Kiberbiztonsági törvény hatályának értelmezéséhez.
Forrás: https://nki.gov.hu/hatosag/tartalom/hataskor/
Letöltés ideje: 2025.03.25.

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal (2022): Az EU Horizont Európa kutatási és innovációs keretprogramja.
Forrás: https://nkfih.gov.hu/hivatalrol/nemzetkozi-kapcsolatok/horizont-europa
Letöltés ideje: 2025.03.27.

Newman, Lily Hay: Apple Intelligence Promises Better AI Privacy. Here's How It Actually Works.
Forrás: https://www.wired.com/story/apple-private-cloud-compute-ai/?utm_source=chatgpt.com
Letöltés ideje: 2025.03.13.

Országgyűlés Hivatala: Infojegyzet 2024/23. szám.

Forrás: https://www.parlament.hu/documents/d/guest/infojegyzet_2024_23_eu_mi_rendelet
Letöltés ideje: 2025.03.01.

Sanger, David E.: Russian hackers broke into federal agencies, US officials suspect. The New York Times, 2020, 13. o.
Forrás: https://www.nytimes.com/2020/12/13/us/politics/russian-hackers-us-government-treasury-commerce.html
Letöltés ideje: 2024.09.23.

Turton, William - Riley, Michael - Jacobs, Jennifer: Colonial pipeline paid hackers nearly $5 million in ransom. Bloomberg (May 13, 2021)
Forrás: https://www.bloomberg.com/news/articles/2021-05-13/colonial-pipeline-paid-hackers-nearly-5-million-in-ransom
Letöltés ideje: 2024.09.23.

Verizon. (2023). 2023 Data Breach Investigations Report.
Forrás: https://www.verizon.com/business/resources/reports/dbir/
Letöltés ideje: 2024.09.28.

Felhasznált jogszabályok:

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

2024. évi LXIX. törvény Magyarország kiberbiztonságáról

DOI-azonosító: https://doi.org/10.53304/RT.2025.2.03

PETRÉTEI DÁVID

Generatív mesterséges intelligencia a kriminalisztikai szemléken

Absztrakt
Ebben a tanulmányban a generatív mesterséges intelligencia egyik változatát, az úgynevezett nagy nyelvi modellt (LLM) javasolom felhasználni helyszíni szemle jegyzőkönyvek és boncjegyzőkönyvek szövegének megalkotására. A szakember által félmondatokban megfogalmazott leíró részeket a generatív mesterséges intelligencia alakítja jól megfogalmazott folyószöveggé. Ehhez olyan nyílt forrású LLM-re van szükség, amit a rendőrség vagy a belügy saját szerverén tud futtatni, biztonságos adatkapcsolatokkal a végpontok között.

Kulcsszavak: mesterséges intelligencia, nagy nyelvi modell, LLM, helyszíni szemle, jegyzőkönyv, igazságügy, kriminalisztika

Abstract
In this paper, using a variant of generative artificial intelligence is proposed, the so-called large language model (LLM), to generate the text of crime scene investigation reports and forensic autopsy reports. The generative artificial intelligence transforms the descriptive parts formulated in half-sentences by the expert into well-formulated flowing text. This requires an open-source LLM that the Police or the Ministry of Internal Affairs can run on their own server, with secure data connections between the endpoints.

Keywords: artificial intelligence, large language model, crime scene investigation, autopsy, forensic, report

Bevezető helyett

2024. október 8-án hirdették ki a fizikai Nobel-díj nyerteseit. Az indoklás szerint John Hopfield (Princeton) és Geoffrey Hinton (Torontói Egyetem) *„a mesterséges neurális hálókkal történő gépi tanulást lehetővé tevő alapvető felfedezésekért és invenciókért”* érdemelte ki az elismerést.[1]

Ennél beszédesebb bevezetőt kitalálni sem lehetett volna. A mesterséges intelligencia, angol betűszóval AI, ma már a hétköznapjaink része. Gondolhatunk az online ügyfélszolgálatok robot asszisztenseire, vagy akár az önvezető járművekre. A mélytanuló algoritmusokat használó neurális hálók mintafelismerő, képelemző, összefüggéseket megtaláló, predikciós stb. képességeit felfedezte, illetve még jelenleg is fedezi fel a forenzikus és a rendészettudomány. Szó szerint több ezer külföldi tanulmány foglalkozik a kérdéssel, és már a hazai szakirodalom is szaporodik.[2] A kulcsfogalmakat, mint a mélytanulás vagy a neurális háló, itt nem fejtem ki, azok megtalálhatók a mesterséges intelligencia fejlődésének kockázatait is alaposan bemutató, közelmúltban megjelent tanulmányban.[3]

---

[1] Forrás: https://telex.hu/techtud/2024/10/08/fizikai-nobel-dij-2024

[2] Fazekas István: A mesterségesintelligencia-kutatás eredményei a kriminalisztika néhány vonatkozásában. Belügyi Szemle 2018/7-8. szám. 55–65. o. DOI: https://doi.org/10.38146/BSZ.2018.7-8.4; Czebe András: A mesterséges intelligencia alkalmazásának elméleti keretei a büntetőeljárásban. Kúriai Döntések 2021/7. szám. 1111–1119. o.; Herke Csongor (2021): A mesterséges intelligencia kriminalisztikai aspektusai. Belügyi Szemle 2021/10. szám. 1709–1724. o. DOI: https://doi.org/10.38146/BSZ.2021.10.2; Lontai Márton – Pamzsav Horolma – Petrétei Dávid (2024a): Mesterséges intelligencia a törvényszéki tudományokban Revolúció vagy invázió? I. rész. Belügyi Szemle 2024/4. szám. 577-592. o. DOI: https://doi.org/10.38146/bsz-ajia.2024.v72.i4.pp577-592; Lontai Márton – Pamzsav Horolma – Petrétei Dávid: Mesterséges intelligencia a törvényszéki tudományokban Revolúció vagy invázió? II. rész. Belügyi Szemle 2024/8. szám. 1355-1369. o. DOI: https://doi.org/10.38146/bsz-ajia.2024.v72.i8.pp1355-1369

[3] Tóth Levente: Az intelligens fenyegetés: Hogyan veszélyeztetheti a mesterséges intelligencia a biztonságunkat? Belügyi Szemle 2024/7. szám. 1187-1205. o. DOI: https://doi.org/10.38146/bsz-ajia.2024.v72.i7.pp1187-1205

Ebben a tanulmányban a mesterséges intelligencia egyetlen fajtájára, az úgynevezett generatív mesterséges intelligenciára, azon belül is a nagy nyelvi modellekre (LLM) koncentrálok.

Közelítés kriminalisztikai oldalról

A szemle a legősibb bizonyítási eljárások egyike, hiszen minden, amit nem a felek mondtak el a hatóság előtt (vallomások), hanem a hatóság-bíróság maga észlelt, szemlének tekinthető. A legősibb perjogi rendelkezések szerint is a sérülést okozó fegyvert, a sebeket, az elszakadt ruházatot meg kell mutatni az eljáró hatóságnak-bíróságnak, hogy azt figyelembe tudják venni. A szemlének ma is csak egyik fajtája a helyszíni szemle; kriminalisztikai szempontból szemle lesz az is, amit a szakértő a szakértői vizsgálat leletező részében tesz. A továbbiakban szemle alatt érteni fogom ezeket a vizsgálódásokat is.

A szemle három legfontosabb eredményterméke a megfelelő dokumentáció, a további vizsgálatra alkalmasan rögzített bűnjelek, illetve a szintézis, a helyszínen talált állapot és elváltozások átfogó értékelése a verziók felállításának érdekében.[4]

Ezek közül a cikk lényegi részét tekintve a megfelelő dokumentációra koncentrálok.

Napjainkban a hagyományos írott anyag, azaz jegyzőkönyv (vagy esetenként hivatalos feljegyzés) mellett gyakorlatilag mindig készül bőséges fotódokumentáció, általában fényképmellékletbe rendezve, ritkábban a jegyzőkönyvbe szövegközi ábraként beszúrva. A rendőrség nagyjából húsz éve kizárólag digitális fényképezőgéppel dolgozik, és az utóbbi években már nem követelmény a digitális képek papírra nyomtatása sem, tehát a képek mennyiségének nincs anyagi vagy logisztikai korlátja.

[4] Petrétei Dávid: A bűnügyi helyszín a szabványosítási tendenciák és az új Be. tükrében. Rendőrségi Tanulmányok 2018/3. szám. 4-48. o.; Petrétei Dávid: Elkövetői profilalkotás és a bűnügyi helyszín elemzése. Rendőrségi Tanulmányok 2020/1. szám. 3-49. o.

Kiemelt bűncselekményeknél ugyancsak rendszeres a videofelvételek (az eljárási jogszabályok szóhasználatában: kép- és hangfelvétel) készítése. Ezzel kapcsolatban megjegyzendő, hogy egy szemlén általában nem kötelező a folyamatos kép- és hangfelvétel készítése, lehetséges akár több rövid, néhány perces felvétellel megörökíteni a releváns eseményeket (pl. holttest vetkőztetése, szaktanácsadó nyilatkozata). A folyamatos kép- és hangfelvétel készítésének elsősorban eljárásjogi hatásai és funkciói vannak (nem szükséges a jegyzőkönyvet az eljárási cselekménnyel egyidőben elkészíteni, nem szükséges a jegyzőkönyv tartalmát felolvasni stb.). Szemléken a sarokba felállványozott videókamera folyamatos működése-működtetése nem jogi előírás, és általában túl sok értelme sincs.

Napjainkban a helyszínek háromdimenziós képi rögzítése gyakorlatilag nem csak lehetséges, hanem egyre inkább elterjed, immár hazánkban is. Ehhez lézerszkennerek, strukturált fényű szkennerek, vagy a fotogrammetria módszeréhez egyszerű fényképezőgépek szükségesek. Talán nem szükséges külön hangsúlyozni a térhatású digitális képek jelentőségét: bejárhatók, körbe forgathatók a helyszínek, az egyes bűnjeltárgyak.[5] Egyes három dimenzióban rögzített bűnjeltárgyak akár ki is nyomtathatók, a bíró vagy a vádlott kezébe adható a bűnjeltárgy morfológiailag pontos műanyag másolata.[6] A jövőben a helyszín akár bejárható lesz a virtuális valóságban is, bár eleinte valószínűleg a tárgyalások méltóságának rovására menne, ha virtuálisan a helyszínen, fizikailag az arcot takaró sisakban a tárgyalóteremben vívna szópárbajt az ügyész és a védő.

[5] Metzger Máté – Ujvári Zsolt – Gárdonyi Gergely: A fotogrammetria kriminalisztikai célú alkalmazása: helyszínek, holttestek, tárgyak rekonstrukciója három dimenzióban. Belügyi Szemle 2020/11. szám. 57-70. o. DOI: https://doi.org/10.38146/BSZ.2020.11.4; Ujvári Zsolt – Metzger Máté: A fotogrammetria kriminalisztikai alkalmazása – tudományosan megalapozott módszerek fényképezőgép segítségével történő 3D képrögzítéshez. Rendőrségi Tanulmányok 2024. évi különszáma. 79-220. o. DOI: https://doi.org/10.53304/RT.2024.ksz.02

[6] Fülöp Péter – Ujvári Zsolt – Petrétei Dávid – Kiss István – Dudás-Boda Eszter – Metzger Máté – Fullár Alexandra: Az igazságügyi szakértői szemléltetés modern eszközei és lehetőségei. Ügyészek Lapja 2023/5-6. szám. 91-102. o.

Egyes telefonokban gyári tartozék a lidar, azaz lézerszkenner, és a kevert valóság megjelenítésére képes alkalmazások. Ilyenek például az Apple iPhone 12 és afeletti modelljei. Ezek alapvetően nem bűnügyi-igazságügyi célra készültek, hanem például bútorvásárláskor az üzletben beszkennelt fotelt a telefonunkon be tudjuk helyezni a nappalink beszkennelt képébe, és meg tudjuk nézni, elfér-e majd, illetve hogyan mutat. Ezek a lézerszkennerek még a legdrágább telefonokban is mindössze néhány méter hatótávolságúak, nem ellenfelei az állványos szkennereknek vagy a szakember által készített több száz fényképből összeállított fotogrammetrikus képnek, de nem is ez a céljuk. A jövőben akár a járőrök is felszerelhetőek lesznek ilyen eszközökkel, hogy a helyszínre érve, azt átvizsgálva, az elkövető elfogása vagy a sértett ellátása-kimentése közben háromdimenziós képre rögzítsék a talált állapotot.

Még manapság is jó szolgálatot tesz egy igényes, a lényeget kiemelő helyszínvázlat. Ezek döntő többsége sem a klasszikus zöld milliméter-papírra készül már, hanem különböző számítógépes alkalmazásokkal, többnyire felülnézeti képként, de akár háromdimenziós ábraként is.[7]

A jegyzőkönyv

A dokumentáció módszerei tehát folyamatosan fejlődnek, egyre bőségesebb eszközökkel kényeztetik el a bűnüldözőket és a jogalkalmazókat. Ennek ellenére a legősibb eszköz, az írásos-szöveges „jelentés” („report”) megmaradt. Sokszor temették pedig! Először talán a fényképezés, azután a videófelvételek elterjedésekor. Jó tíz évvel ezelőtt vásárolta a hazai rendőrség az első lézerszkennert, attól is azt várták akkor sokan, hogy tömeges elterjedése, illetve rendszeres használata majd „kiváltja” a szemleírást. Ez nem történt meg, és nem is várható, legalábbis reméljük.

Fent írtam, hogy a szemle három funkciója közt szerepel a talált állapot és az elváltozások átfogó értékelése, a megállapítások szintézise, illetve a

[7] Fenyvesi Csaba: Kriminalisztika. Ludovika Egyetemi Kiadó. Budapest, 2022. 295. o. ISBN: 9789635315598

verziók felállítása. Ez akkor képzelhető el, ha a közvetlen tapasztalást és megfigyelést végző képzett szakember a megállapításait nyelvi eszközökkel formába önti, hogy azt az eljárás később szereplői is megismerhessék. Akár azért (is), hogy ők más következtetéseket vonjanak le ugyanabból. Önmagukban a legélesebb fényképek sorozata sem pótolhatja a helyszínt közvetlenül megismerő szakember megállapításait. Persze még eggyel hátrébb léphetünk: a fényképeken is csak az fog szerepelni, amit a szakember fontosnak tart megörökíteni.

Az írásos dokumentáció megkerülhetetlen, és a jövőben is az marad. Az összes többi helyszínrögzítési módszer csak kiegészíti a jegyzőkönyvet, mellékletként.

Az írásos jegyzőkönyv elkészítése nélkülözhetetlen, de ez nem jelenti azt, hogy elkészítése könnyű vagy gyors. A helyzet az, hogy a szemle során a leginkább kimerítő, leginkább időrabló, energiaigényes feladat a jegyzőkönyv elkészítése. Ma már okoseszközön, tableten történik a legtöbb helyszíni szemle elkészítése a magyar rendőrségnél. De mit tapasztalunk, ha elfogulatlanul tekintünk az eszközre? A tableten a nyomozó nagyjából pont ugyanazt csinálja, mint amit egy laptopon is meg lehetne. Csak kényelmetlenebb. A laptopon pedig nagyjából ugyanazt csinálja, mint amit egy írógépen is lehet. Ha alaposan végiggondoljuk, az okoseszköz egyetlen „okos” funkcióját sem használjuk ki (GPS, térkép, diktálás, videokonferencia, okmányok szkennelése, szemlén jelen lévő személy általi hitelesítés videofelvételen stb.) – a nyomozó a hatvanas évek óta ugyanúgy gépeli be a mondatokat, csak most már igazi billentyűzete sincs hozzá. Ennek a kifejtése ugyancsak messzire vezetne, így ebben a tanulmányban egy „áramvonalasabb” megoldást igyekszem bemutatni.

Leszögezhetjük, hogy a jegyzőkönyv gépelése rendkívül időrabló, és ha ezt a bizottságvezető csinálja, a bizottság vezetésére sem ideje, sem energiája nem marad. A kriminalisztikai gondolkodásról nem is beszélve. A gépnek diktálás, angol kifejezéssel speech-to-text, vagy ahogy az Orwell-féle 1984-ben hívják a hasonló eszközöket: beszélír éppen csak eggyel jobb megoldás. Ugyanis megfontoltan kell az előre megfogalmazott szép, kerek,

szakszerű mondatokat rádiktálni a gépre, ami ezt utána írott szöveggé alakítja, általában tagolás és írásjelek nélkül.

A generatív mesterséges intelligencia

A generatív AI legfontosabb tulajdonsága, hogy képes tartalmat létrehozni, generálni, innen a neve. E cikk első változata 2024-ben a Rendőrség Tudományos Tanácsához benyújtott pályamű volt, ennek jeligéje volt az „*Elektrubadúr*”. Ez Stanisław Lem lengyel sci-fi szerző egyik mesterművében, a Kiberiádában, annak is Első pótutazás című fejezetében szereplő generatív mesterséges intelligencia, bár nem hívják így.[8] Lényegében olyan gép, ami bármilyen megadott témában, bármilyen megadott szempontok alapján képes bármilyen verset írni. Ahhoz, hogy valódi költészetre legyen képes, alkotója nagyon alapos munkát végzett:

„*A programot, amely egy közönséges költő fejében lakozik, a civilizáció teremtette, amelyben az illető a világra jött; ezt a civilizációt az előző hozta létre, az előzőt egy még korábbi, és így tovább, egészen a világmindenség kezdetéig, amikor a jövendő poéta információi még kuszán kószáltak az ősködben. Ennélfogva a gép programozásához előbb meg kellett ismételni – ha nem is az egész világmindenséget elejétől fogva, de legalábbis jókora részét (…) Mindenekelőtt épített egy gépet, amely a káoszt modellezte, és villamos lélek lebegett benne a villamos vizek felett, aztán betáplálta a fény paramétereit, aztán az ősködökét, és így lassacskán elérte az első jégkorszakot (…)*”[9]

A generatív mesterséges intelligencia nem ezt az utat járta be, Lem elképzelt gépével ellentétben nem modellezte sem az őskáoszt, sem a minket

[8] Szabó Lajos: A mesterséges intelligencia Stanisław Lem életművében. Biztonságtudományi Szemle 2024/3. 13-25. o.

[9] Lem, Stanisław: Teljes science-fiction univerzuma II. Szukits Könyvkiadó. Szeged. 2006. 459-460. o. ISBN: 978-963-497-189-4

megelőző civilizációkat.[10] Az úgynevezett nagy nyelvi modellek (LLM), azaz a csevegőprogramok, szövegalkotásra épülő programok gigantikus mennyiségű szöveget tettek magukévá, és ennek hatására, ennek felhasználásával képesek maguk is szövegalkotásra. Ilyen a ma már közismert, elterjedt, gyakorlatilag ingyenesen is használható ChatGPT például, de egyre több vállalat épít ki mesterséges intelligenciára épülő ügyfélszolgálatot is.

Léteznek zene, kép vagy mozgókép generálására is alkalmas mesterséges intelligenciák, amelyek tehát ugyanígy generatívak, de nem nagy nyelvi modellek. Ezekkel kattintásvadász képeket lehet készíteni a közösségi médiára, mintha valódi szobrok vagy valódi termékek lennének („ez a kisfiú a tengerparti homokból építette meg az Eiffel-tornyot, oszd meg te is, ha tetszik!" – és látunk egy képet, amin biztosan nem homokból épült bonyolult szerkezet van, boldogan mosolygó, ám riasztóan „mű" kisfiúval…) A videomegosztó oldalak tele vannak olyan alkotásokkal, ahol az AI megrajzolta az országokat képregény-főgonoszként, vagy a nemzeti himnuszokat középkori lovagként, és a lehetőségeknek csak a fantázia szabhat határt. (Illetve ennek az egésznek a kérdéses értéke vagy haszna, de a jelek szerint ez nem sok embert érdekel.) A veszélytől, hogy a mesterséges intelligencia majd a fejünkre nő, valószínűleg az fog megmenteni bennünket, hogy céltalan bohóckodásra használjuk leginkább, mérhetetlen mennyiségű értéktelen és érdektelen adattal tömve.

A helyszíneken a képi dokumentálást nem bízhatjuk generatív mesterséges intelligenciára, hiszen ő a mi kérésünknek megfelelő képeket fog alkotni, nem a látottakat fogja megörökíteni. Kifejezetten óvatosnak kell lenni minden „képoptimalizáló" vagy képjavító szoftverrel, nehogy olyat tegyen rá a képre, vagy tüntessen el onnan, ami a gép szerint a mi kívánságainkat vagy igényeinket kielégíti, de a valóságnak nem felel meg.

Szövegalkotásra azonban felhasználható a generatív AI, a nagy nyelvi modelleket fel is szokták használni erre. A szemlékről készült jegyző-

[10] Szabó Lajos: i.m.

könyv, illetve a boncjegyzőkönyv erősen formalizált, felismerhető szempontok szerint jól strukturált szöveg. Ráadásul sajátos nyelvezetet használ, hogy minden olvasó többé-kevésbé ugyanazt értse az olvasottak alatt, például a metszett sérülés más, mint a vágott, illetve a hétköznapi életben ritkán találkozunk a szövethíd vagy a hámzászlócska főnévvel, a sérvesedik vagy a belehel igékkel. A cigarettacsikk nem csak úgy „ott van" a lépcsőn: a cigarettavég a negyedik lépcsőfok járófelületén a lépcső alulról szembőlnézeti jobb oldalától harminckét, a járófelület szélétől pedig három centiméterre helyezkedik el.

A generatív AI – nagy nyelvi modell a helyszínen

Fentebb írtam, hogy a jegyzőkönyv begépelése időrabló és erőforrás-pazarló tevékenység. A „beszélír" (*speech-to-text*) megoldás is csak félmegoldás, hiszen szakmailag megalapozott, nyelvtanilag helyes, szép kerek mondatokban érdemes csak fogalmazni, ráadásul a kész szöveg valószínűleg tagolatlan lesz; hiszen, ha azt mondjuk „pont" vagy „új bekezdés", a legtöbb beszélír azt is leírja.

A nagy nyelvi modell azonban képes arra, hogy a tőmondatokban, szavakban adott jellemzést szép kerek igényes mondatokká formázza. Tudja kezelni az olyan emberi megnyilvánulásokat, mint például *„a padlót padlószőnyeg borítja, zöld alapon fehér pöttyökkel… sötétzöld alapon… a pöttyök inkább sárgák, egymástól négy… nem, négy és fél centiméterre vannak a fél centis pöttyök… legyen a szőnyeg malachitzöld".* Ha a mesterséges intelligencia tudja, hogy mi lesz az elvárt eredménytermék: strukturált, szakkifejezéseket használó jegyzőkönyv, akkor az ilyen töredékes információkat, alakszerűtlen közléseket is kerek mondatokká, bekezdésekké fogja alkotni. A szemlét végzőnek természetesen komoly felelőssége van a generált szöveg alapos visszaellenőrzésében, hogy abban csak olyan állítások szerepeljenek, amelyek a helyszín jellemzőinek valóban megfelelnek.

Ezt az elnagyolt hipotézisemet játékos tesztelésnek vetettem alá. Egyszerű hétköznapi táblagépemre letöltöttem az amerikai Open AI cég ChatGPT 4 alkalmazását, ami bárki számára ingyenesen hozzáférhető nagy nyelvi modell, talán a legismertebb a színtéren. Első alkalommal megkértem, hogy írjon helyszíni szemle jegyzőkönyvet egy gépkocsifeltörésről. Tartalmilag ijesztően jó eredmény született, amiben a legijesztőbb az volt, hogy szó szerint ennyi volt részemről az utasítás (az úgynevezett „prompt"), és mégis kerek egész jegyzőkönyv született. Ami azt jelenti, hogy a helyszínt, a dátumot, a gépkocsit, az elkövetés módszerét, a rögzített bűnjeleket és az eltulajdonított tárgyakat mind konfabulálta, azaz kitalálta az én szórakoztatásomra. Ezért másodszor megadtam neki bizonyos alapadatokat: a gépkocsi típusát, színét, elhelyezkedését, illetve azt is, hogy melyik ablak van betörve. Ezeket mind belefoglalta a második jegyzőkönyvbe. Harmadszorra igyekeztem korrigálni a filmes-tévés szókincsét a rendőri-igazságügyi bikkfanyelvnek megfelelően. Azaz kértem, hogy az üveget üvegtörmeléknek nevezze, a bizonyítékot bűnjelnek. Kértem, hogy csak azt tekintse bűnjelnek, amit elcsomagolunk és elviszünk, ezeket számozza is be, a többi elváltozást ne számozza be, ellenben nevezze egyéb releváns elváltozásnak. A harmadik jegyzőkönyv már megállta volna a helyét a legtöbb hazai rendőrkapitányságon. Újra hangsúlyozom a kész szöveg alapos visszaellenőrzésének szükségességét.

Ez természetesen nem tudományos igényű tesztelés volt, hanem inkább játékos próbálkozás. Másrészt a gépkocsifeltörés talán a legegyszerűbb szemlék egyike. Mindezekkel együtt az eredmény meglepően biztató. Két kisebb (néhány mondatos) korrekciót követően gyakorlatilag hibátlan szemlejegyzőkönyv állt elő. Kifejezett kérdésemre a ChatGPT azt válaszolta, hogy megtanulta a bizonyíték helyett a bűnjel szót, és onnantól ezt fogja használni a szemlejegyzőkönyvek kontextusában.

Vajon mire lenne képes ez a színvonalú (még egyszer: ingyenes, bárki számára hozzáférhető) technológia, ha beletáplálnánk a 2019–2023 közt született valamennyi rendőrségi szemlejegyzőkönyvet, illetve valamennyi

boncjegyzőkönyvet a négy egyetemi orvosszakértői intézetből és a Nemzeti Szakértői és Kutató Központból…? Ezt természetesen nem tehetjük meg.

Aggályok, avagy hol lakik a szellem a gépből?

A külföldi magánvállalat által üzemeltetett LLM természetesen nem tölthető fel valódi helyszíni szemlékkel: igazából fogalmunk sincs, hogy hova kerül a feltöltött anyag, ahhoz ki és hogyan férhet hozzá legálisan vagy esetleges üzemzavar során. A generatív mesterséges intelligencia nem „fér el" egy táblagépen vagy egy telefonon. Ami a saját eszközünkön van, az csak egy végpont; az érdemi munka hatalmas teljesítményű szervereken zajlik, valahol Amerikában, esetleg a Távol-Keleten.

Nem mellesleg ugyanez az oka annak, hogy nyílt forrású „speech-to-text" szolgáltatásokat sem vesz igénybe a rendőrség a jelentések, jegyzőkönyvek megírásához: nem tudni, hogy a hangüzeneteket, miközben megjárják az utat a szerverekig és vissza, lemásolhatja-e valaki, vagy belehallgathat, alávetheti-e elemzésnek, keresésnek. Bűnügyi adatok, különleges személyi adatok esetében az ilyen bizonytalanság megengedhetetlen.

Mi a megoldás? Avagy innovációs javaslatom

Jelenleg néhány nagyvállalat uralja a generatív mesterséges intelligenciák piacát, termékeiket ingyen vagy több-kevesebb összegért lehet használni. Gőzerővel fejlesztik azonban a nyílt forrású generatív mesterséges intelligenciákat is. Ezek egyelőre nem érik utol a nagyvállalatok termékeit, de a közeljövőben várhatóan elérik azt a szintet, amit az ingyenes platformok, például a ChatGPT 4 képvisel. Az pedig bőven elegendő.

Amint egy nyílt forrású LLM eléri azt a szintet, amit a jelenlegi nagyvállalati LLM-ek képviselnek, a rendőrség vagy a belügy azonnal szert tehet egyre. Rátelepítheti egy csakis erre vásárolt és rendszerbe állított nagy

teljesítményű szerverre, amit azonnal biztonságosan elszigetelhet és levédhet a külső beavatkozásoktól. Ezt követően a rendőrség integrált ügyviteli rendszerében digitalizált több tízezer szemlejegyzőkönyvet vagy hivatalos feljegyzést könnyedén bele lehet táplálni, hogy tanuljon. Ugyanígy lehetne eljárni az orvosi egyetemek és a Nemzeti Szakértői és Kutató Központ boncjegyzőkönyveivel, kiegészítve az egyetemi repozitóriumokban szabadon hozzáférhető jogi és kriminalisztikai szakkönyvekkel, szakcikkekkel, illetve a Nemzeti Jogszabálytár joganyagával, a bírósági határozatok tárával.

A következő lépés az lenne, hogy néhány önkéntes, lehetőleg gyakorló vagy volt helyszínelők, esetleg nyomozó vagy ügyész, nekiálljon „tanítani" a rendszert. Azaz generáltatnának vele jegyzőkönyveket, jelentéseket, változatos elképzelt forgatókönyvek alapján, kifejezetten abból a célból, hogy az esetleges hibákat javítsák, a szóhasználatot korrigálják, a konfabulálást kiszúrják, stb. Párhuzamosan ugyanezt a feladatot végezné halottszemlék és boncjegyzőkönyvek vonatkozásában orvosszakértők, rezidensek kis önkéntes csapata is. Gyakorlatilag a szerver bekapcsolását követően a szövegkorpusz betáplálása szó szerint pillanatok alatt megtörténhet, utána a „tanítás" legfeljebb egy hetet venne igénybe.

Ezt követően már csak biztonságos adatkapcsolat kérdése, hogy a helyszínelőknél egyébként is rendszeresített táblagépeken az LLM alapú szemlejegyzőkönyv fusson. A „beszélír" funkciót ugyanezen a biztonságos adatkapcsolaton keresztül bonyolítaná a rendszer, az eszköz mikrofonját az egyéb szolgáltatások számára akár le is lehetne tiltani. Így a helyszínen a jegyzőkönyv írójának akár mindkét keze szabad lehetne: az általa mondottakat, megállapításait, leírásait, mérési eredményeit a mesterséges intelligencia alakítaná jól strukturált, szaknyelvet igényesen használó, kerek egész mondatokból álló jegyzőkönyvvé.

Innen már csak egy lépés az, ami egyelőre science fiction, hogy a jegyzőkönyv kérdez, ha valami nem világos számára, vagy ha feloldhatatlan ellentmondást észlel a közlésben. Illetve a jegyzőkönyv javasol, ha az em-

ber kérdez tőle *(„ez egy rattan bútor… milyen porokkal szoktak nyomkutatást végezni az ilyeneken?”*) – a science fiction az, ha a jegyzőkönyv olykor kérdés nélkül is javasol. Valószínűleg azonban ez is csak egy-két lépés lesz a rendszer beüzemelésétől.

Lezárás

Mindaz, amit felvázoltam, a legközelebbi jövő realitása. Akár 2025 első hónapjaiban felbukkanhat olyan open source LLM, ami összevethető a jelenlegi nagy nyelvi modellek képességeivel, és felhasználható lenne jegyzőkönyvek szövegének megalkotására. Az olyan nagy teljesítményű szerver, amin a rendszert futtatni lehet, egy középkategóriás személygépkocsi áránál nem kerül többe. A végpontok a már rendelkezésre álló tabletek lehetnének. A biztonságos adatkapcsolat kiépítése a szerver és a tabletek között ugyancsak nem megoldhatatlan feladat, ezek folyamatos fenntartása, az adatbiztonság folyamatos figyelemmel kísérése ugyanolyan feladat lenne, mint például a RZsNEO integrált ügyviteli platform esetében.

Kiemelném, hogy ilyen fejlesztés legjobb tudomásom szerint sehol sem zajlik a világban, egyelőre egytelen rendőrség vagy szakértői intézet sem használ nagy nyelvi modellt jegyzőkönyvek vagy jelentések szövegének megírására, és a mesterséges intelligenciával kapcsolatos, exponenciálisan növekvő számú publikációk közt sem találtam ilyesmit.

A mesterséges intelligencia ilyen jellegű hasznosítása teljesen aggálymentes, nem hoz meg és nem támogat emberi döntéseket, nem mérlegeli emberek veszélyességét vagy gyanússágát. Csak segíti a munkát, mint egy művelt írnok. A generált jegyzőkönyv tartalmáért tehát továbbra is az azt hitelesítő szakember felelne.

Végül pedig fontoljuk meg: a világ akkor is változik, ha mi nem.

FORRÁSOK

Czebe András: A mesterséges intelligencia alkalmazásának elméleti keretei a büntetőeljárásban. Kúriai Döntések 2021/7. szám. 1111–1119. o.

Fazekas István: A mesterségesintelligencia-kutatás eredményei a kriminalisztika néhány vonatkozásában. Belügyi Szemle 2018/7-8. szám. 55–65. o. DOI: https://doi.org/10.38146/BSZ.2018.7-8.4;

Fenyvesi Csaba: Kriminalisztika. Ludovika Egyetemi Kiadó. Budapest, 2022. 295. o. ISBN: 9789635315598

Fülöp Péter – Ujvári Zsolt – Petrétei Dávid – Kiss István – Dudás-Boda Eszter – Metzger Máté – Fullár Alexandra: Az igazságügyi szakértői szemléltetés modern eszközei és lehetőségei. Ügyészek Lapja 2023/5-6. szám. 91-102. o.

Herke Csongor (2021): A mesterséges intelligencia kriminalisztikai aspektusai. Belügyi Szemle 2021/10. szám. 1709–1724. o. DOI: https://doi.org/10.38146/BSZ.2021.10.2

Lem, Stanisław: Teljes science-fiction univerzuma II. Szukits Könyvkiadó. Szeged. 2006. ISBN: 978-963-497-189-4

Lontai Márton – Pamzsav Horolma – Petrétei Dávid (2024a): Mesterséges intelligencia a törvényszéki tudományokban Revolúció vagy invázió? I. rész. Belügyi Szemle 2024/4. szám. 577-592. o. DOI: https://doi.org/10.38146/bsz-ajia.2024.v72.i4.pp577-592;

Lontai Márton – Pamzsav Horolma – Petrétei Dávid: Mesterséges intelligencia a törvényszéki tudományokban Revolúció vagy invázió? II. rész. Belügyi Szemle 2024/8. szám. 1355-1369. o. DOI: https://doi.org/10.38146/bsz-ajia.2024.v72.i8.pp1355-1369

Metzger Máté – Ujvári Zsolt – Gárdonyi Gergely: A fotogrammetria kriminalisztikai célú alkalmazása: helyszínek, holttestek, tárgyak rekonstrukciója három dimenzióban. Belügyi Szemle 2020/11. szám. 57-70. o. DOI: https://doi.org/10.38146/BSZ.2020.11.4

Petrétei Dávid: A bűnügyi helyszín a szabványosítási tendenciák és az új Be. tükrében. Rendőrségi Tanulmányok 2018/3. szám. 4–48. o.;

Petrétei Dávid: Elkövetői profilalkotás és a bűnügyi helyszín elemzése. Rendőrségi Tanulmányok 2020/1. szám. 3-49. o.

Szabó Lajos: A mesterséges intelligencia Stanisław Lem életművében. Biztonságtudományi Szemle 2024/3. 13-25. o.

Tóth Levente: Az intelligens fenyegetés: Hogyan veszélyeztetheti a mesterséges intelligencia a biztonságunkat? Belügyi Szemle 2024/7. szám. 1187-1205. o. DOI: https://doi.org/10.38146/bsz-ajia.2024.v72.i7.pp1187-1205

Ujvári Zsolt – Metzger Máté: A fotogrammetria kriminalisztikai alkalmazása – tudományosan megalapozott módszerek fényképezőgép segítségével történő 3D képrögzítéshez. Rendőrségi Tanulmányok 2024. évi különszáma. 79-220. o. DOI: https://doi.org/10.53304/RT.2024.ksz.02

DOI-azonosító: https://doi.org/10.53304/RT.2025.2.04

SALLAI JÁNOS

Európa határok nélkül?
Európa határfogalom-ellenőrzés nélkül

40 éve, 1985. június 14-én írták alá a Schengeni Megállapodást

Absztrakt
Már az európai gondolat megszületésénél rögzítették a személyek szabad áramlásának megvalósítása iránti igényt. Ennek elvi és gyakorlati kivitelezésére kicsit megkésve, 1985-től születtek meg a schengeni megállapodások. 1985-ban írták alá az alapító államok politikai vezetői a Schengeni Megállapodást,[1] amely 33 szakaszban rögzítette a hosszútávú elképzelést: a tagállamok közös határai mentén a határforgalom-ellenőrzés felszámolását. A schengeni megállapodás gyakorlati végrehajtására vonatkozó egyezményre 5, míg annak hatálybalépésére 10 évet kellett várni. Így 30 éve, 1995-től a schengeni térségben megvalósult a személyek szabad áramlása. Később az Amszterdami Szerződés hatálybalépését (1999) követően a schengeni aquis fokozatosan az Európai Unió I. pillérének részévé vált, azaz közösségiesedett, először a határellenőrzés, majd a határon átnyúló rendőri együttműködés.

Kulcsszavak: Schengen, határok, határforgalom-ellenőrzés, Schengeni Egyezmény, Schengeni Végrehajtási Egyezmény

Abstract
The demand for the realization of the free movement of persons was already recorded at the birth of the European idea. The theoretical and practical implementation of this demand was somewhat delayed, with the

[1] Sallai János: A Schengeni Egyezmény. In: Ezer kérdés – ezer válasz az Európai Unióról. Szerk. Ízikné Hedri Gabriella. Nemzeti Tankönyvkiadó. Budapest, 2003. 224. o.

Schengen agreements emerging from 1985. In 1985, the political leaders of the founding states signed the Schengen Agreement, which outlined a long-term vision in 33 articles for the elimination of border control along the common borders of member states. It took 5 years to agree on the practical implementation of the Schengen Agreement and 10 years for it to come into effect. Thus, since 1995, the free movement of persons has been realized in the Schengen area for 30 years. Later, following the entry into force of the Amsterdam Treaty (1999), the Schengen acquis gradually became part of the First Pillar of the European Union, meaning it was integrated into the community, first concerning border control and then cross-border police cooperation.

Keywords: Schengen, borders, border traffic control, Schengen Agreement, Schengen Implementation Agreement

Az európai uniós (Schengen) tagállamok állampolgárai (és akik a térségben legálisan tartózkodnak) számára mára természetessé vált, hogy a közös belső határokat bármikor, bárhol ellenőrzés nélkül átléphetik. Nem ront a helyzeten, hogy ideiglenesen ezt a szabadságot korlátozhatták a tagállamok. Például kiemelt rendezvény (Labdarúgó EB, VB) vagy veszély (COVID-19, tömeges illegális migráció) esetén, illetve közbiztonsági okok miatt szelektív-differenciált határforgalom-ellenőrzést vezethettek be.

De honnan is indult el a folyamat? Mióta beszélhetünk Schengeni Egyezményről? A feltett kérdésekre válaszként adhatunk egy konkrét dátumot, 1985. június 14-ét, és visszautalhatunk korábbi időkre, a Benelux Unió létrehozására (1948), vagy az Északi Útlevél Unió[2] kezdetére, melynek tagjai már 1952-ben elhatározták, hogy a közös határaik mentén felszámolják a határforgalom-ellenőrzést, ezzel lehetővé teszik a skandináv államokban a személyek szabad áramlását[3].

[2] Az Északi Útlevél Unió országai (Dánia, Finnország, Izland, Norvégia, Svédország) 2001-ben csatlakoztak a Schengeni Egyezményhez.

[3] Fejes Zsuzsanna – Sallai János – Soós Edit – Tóth Judit – Vájlok László: Schengenre hangolva. In: Európai Műhelytanulmányok. Budapest, 2004. 3. o.

Az áruk, a tőke, a szolgáltatások és a személyek szabad áramlása már a Római Szerződés óta célként fogalmazódott meg a Montánunió, majd Közös Piac tagállamai részéről, ugyanakkor a megvalósulás terén a személyek szabad áramlásának folyamata elmaradt.

Ha a Schengeni Egyezmény közvetlen előzményeit keressük, akkor az egyrészt Észak-Európába vezet, ahol 1954. március 22-én az Északi Tanács tagállamaiban (Dánia, Izland, Svédország, Norvégia, Finnország) létrejött az Egységes Északi Munkaerőpiac. Másrészt az Európai Gazdasági közösség államaihoz, ahol 1984 júniusában az Európai Tanács a Fontainebleau-i Nyilatkozatban[4] megfogalmazta az utas- és áruforgalom határellenőrzésének és vámellenőrzésének a belső határokon való eltörlését. Ugyanekkor az Európai Tanács egy ad hoc bizottságot hozott létre *„A Polgárok Európája"* névvel (Adonino Bizottság), amely egy útlevélunió lehetőségét vizsgálta meg. Ennek a célja az volt, hogy az EK-útlevek birtokosai szabadabban mozoghassanak, egészen a belső határon történő személyellenőrzés fokozatos felszámolásáig. A fentiekkel párhuzamosan 1984 júliusában Helmut Kohl német kancellár és Francois Miterrand francia államfő, az események sürgetésére, Saarbrückenben aláírták az első bilaterális megállapodást, amelyben a Franciaország és az NSZK közötti határszakaszon a személyforgalom megkönnyítéséről döntöttek, amelynek teljes gyakorlati megvalósulása majd csak a Schengeni Végrehajtási Egyezmény gyakorlati hatálybalépésével következett be.[5]

Így jutottak 1985. június 14-ig, amikor a Mosel folyó partján, a luxemburgi Schengen városában írta alá a fenti nézeteket átfogó egyezményt Franciaország, Németország és a Benelux államok.[6] Mindennek 2025-ben

[4] Sallai János: A bel- és igazságügyi együttműködés általános jogi tudnivalói. Hanns Seidel Alapítvány. Budapest, 2004. 15. o.
[5] Az EU a szabadság, biztonság és jog térsége. (222 kérdés és 222 válasz a bel- és igazságügyi együttműködésről). BM Oktatási Főigazgatóság, Budapest, 2004. 275. o.
[6] Sallai János – Szőke István – Varga János – Vass Ferenc – Vájlok László – Virányi Gergely: Határellenőrzés az Európai Unióban. Hanns Seidel Alapítvány. Budapest, 2000. 268. o.

már 40 éve, és a hajdani 5 alapító tag névsora kibővült az EU-tagok[7] névsorával, miután az Amszterdami Szerződés[8] a Schengeni Egyezményt fokozatosan az első pillérbe integrálta[9], azaz közösségiesítette[10]. Így megvalósult a személyek szabad áramlása, még akkor is, ha esetenként közbiztonsági okok és a COVID-19 miatt ezt időlegesen felfüggesztették, vagy egyes tagállamok (pl. 2024-ben Németország) egyoldalúan az országba befelé irányuló határforgalom esetén határforgalom-ellenőrzést[11] vezettek be.

Schengen[12] tehát mérföldkő az Európai Unió,[13] az európai integráció történetében. A luxemburgi kisvárost[14] a nemzetközi politika rajzolta fel a térképre, ahol a Mosel folyó partján kikötött az a hajó, amelyen a szerződés aláírói megállapodtak a hosszútávú együttműködésről, és a ratifikálást már a parton ejtették meg. Ezek az országok a következők voltak: Franciaország, Németország, Belgium, Luxemburg és Hollandia. A pontos dátum 1985. június 14. A szerződés aláírói célul tűzték ki, hogy „*megszüntessék a közös határokon az ellenőrzést a személyforgalomban és hogy ezen szakaszokon megkönnyítsék az áruforgalmat,*[15] *tekintettel arra, hogy az Egységes Európai Okmánnyal kiegészített, az Európai Közösségeket Alapító*

[7] Sallai János: A bel- és igazságügyi együttműködés általános jogi tudnivalói. Hanns Seidel Alapítvány. Budapest, 2004. 103. o.
[8] 1997. október 2-án írták alá és 2 év múlva, 1999. május elsején lépett hatályba.
[9] Egységes belbiztonsági és jogi térség Európában. Szerk. Harmati Gergely – Masika Edit. Miniszterelnöki Hivatal Integrációs Stratégiai Munkacsoport. Budapest, 1999. 509. o.
[10] Ritecz György: A Schengeni Egyezmény előírásai és Magyarország. In: Cég és Jog 2002/7-8. szám. ARGUTUS Kiadó Kft. Budapest. 52-58. o.
[11] A szerző személyes tapasztalata.
[12] Ritecz György – Sallai János: A Schengeni Egyezmény és a magyar határőrizet. In: európa tükör 2001/5. szám. 65-100. o.
[13] Az európai uniós tagság nem jelentett és nem jelent teljes jogú Schengen-tagságot. Lásd korábbi Nagy-Britannia, vagy a 2004-ben és azt követően EU-s tagállamok esetét. Horvátország később lett EU-tag, mint Románia és Bulgária, ugyanakkor hamarabb vált teljes jogú Schengen-taggá.
[14] A szerző először 1998-ban járt Schengenben, ahol akkor csak három rozsdás vasoszlop és 12 csillag emlékeztette a látogatót a történelmi helyszínre. Akkor a hagyományos papír alapú térképeken alig-alig lehetett felfedezni a települést.
[15] Ekkor áruforgalom-ellenőrzés már nem volt a határon, ugyanakkor a személyi ellenőrzés miatt a kamionoknak meg kellett állni a határátkelőhelyeken.

Szerződés úgy rendelkezik, hogy a belső piac belső határok nélküli térség."[16] Az aláírt Schengeni Megállapodás (SchM) 33 cikkből állt, és már a 2.§ rögzítette, hogy a „*személyforgalomban a rendőri és a vámszervek 1985. június 25-től kezdődően, főszabályként, egyszerű szemrevételezéssel ellenőrzik a közös határon csökkentett sebességgel áthaladó turista-járműveket, megállítás nélkül. Szúrópróba-szerűen azonban mélyrehatóbb ellenőrzést is végezhetnek. Az ilyen ellenőrzéseket, ha lehetséges, olyan módon kialakított, speciális helyeken kell elvégezni, hogy a határátkelésnél a többi gépjármű forgalma ne akadjon meg.*"[17] Már a megállapodásban is szerepeltek gyakorlati végrehajtásra vonatkozó előírások, például egy 8 cm-es zöld korong[18] kihelyezése az autó szélvédőjére az ellenőrzés megkönnyítése céljából.

1985-ben a Szovjetunióban főszereplővé vált Gorbacsov és a reformjai, azonban a hidegháború végét ekkor még nem lehetett megjósolni. A tagállamok eltérő nézeteinek összehangolása és más okok[19] miatt a SchM gyakorlati hatálybalépése[20] folyamatosan elhúzódott. Elsősorban a gyakorlati egyezmény hiánya késleltette leginkább a schengeni gondolat kivitelezését. A megállapodást aláíró felek elkötelezettek voltak, mégpedig, hogy hosszú távon a belső határok mentén felszámolják a határellenőrzést, melynek érdekében „*a külső határaikra telepítsék át az ellenőrzést. Ennek érdekében erőfeszítéseket tesznek azokra a tilalmakra és szigorításokra vonatkozó tör-*

[16] Az EU a szabadság, biztonság és jog térsége. (222 kérdés és 222 válasz a bel- és igazságügyi együttműködésről) Szerk. Sallai János. BM Oktatási Főigazgatóság, 2004. Budapest. 114. o.
[17] SchM 2. cikk
[18] Uo. 3. cikk
[19] Például a határforgalom-ellenőrzés lebontása, vámellenőrzés megszüntetése az ott szolgálatot teljesítő hivatalnokokat ellenérdekeltté tette a gyors bevezetés terén. A határon átnyúló rendőri együttműködéshez hiányzott az infrastruktúra, ami szintén késleltető szerepet játszott.
[20] Fórizs Sándor (2016): A rendészeti változások iránya, tendenciái, mozgatórugói. In: A határrendészettől a rendészettudományig. Szerk. Gaál Gyula, Hautzinger Zoltán. Pécs. 31-41. o.

vényeik és rendeleteik előzetes összehangolására, ha ez szükséges, amelyeken az ellenőrzések alapulnak, és törekednek arra, hogy további intézkedéseket hozzanak a (köz)biztonság védelme érdekében, és hogy megakadályozzák az olyan államok állampolgárainak jogellenes bevándorlását, amelyek nem tagjai az Európai Közösségeknek."[21] Ennek érdekében az alábbiakban állapodtak meg:

„a) megállapodások kidolgozása a rendőri együttműködésről a bűnözés megelőzése és a bűncselekmények felderítése területén;

b) az esetleges nehézségek megvizsgálása a nemzetközi jogsegély- és kiadatási szerződések alkalmazásában, a Felek között e területen megvalósuló együttműködés javítására legalkalmasabb megoldások kialakítása végett;

c) azoknak a megoldásoknak a megtalálása, amelyek lehetővé teszik a bűnözés elleni közös fellépést, többek között a rendőrök számára az átüldözéshez való esetleges jogosítvány megadásának vizsgálatával, figyelembe véve a meglévő kommunikációs eszközöket és a nemzetközi jogsegélyt."[22]

Már ebben az időben is nagy gondot jelentett a kábítószerrel, fegyverrel, lőszerrel való visszaélés, amellyel szemben az aláíró felek vállalták a kötelezettséget, hogy jogharmonizáció segítségével kölcsönösen együttműködve fellépnek.[23]

A Schengeni Megállapodás 1985-től megteremtette az elvi feltételt, hogy hosszú távon az aláíró államok között létrejöjjön a határellenőrzés nélküli térség, amely később, ha a belépő állomok teljesítik a feltételeket, újabb tagokkal bővülhet.

[21] SchM 17. cikk

[22] Egyezmény a Benelux Gazdasági Unió államai, a Németországi Szövetségi Köztársaság és a Francia Köztársaság kormányai között a közös határaikon történő ellenőrzések fokozatos megszüntetéséről szóló, 1985. június 14-i Schengeni Megállapodás végrehajtásáról. 18. cikk

[23] Ritecz György: Gondolatok az Európai Egységes Határőrség kialakításáról. In: EU-Tanulmányok IV. Nemzeti Fejlesztési Hivatal. Budapest, 2004. 695-763. o.

A gyakorlati alkalmazás felé vezető út következő állomása 1990 volt, amikorra a tagállamok szakemberei kidolgozták a Schengeni Végrehajtási Egyezményt[24] (SchVE), amely egyrészt értelmezte a téma kapcsán a legfontosabb fogalmakat,[25] másrészt részletes útmutatót adott a schengeni gondolatok gyakorlati megvalósulásához. A végrehajtási egyezmény kidolgozását nagyban hátráltatták a leomló Berlini Fal és a német egyesítés kezdeti jogi problémái.[26] A SchVE a korábbi SchM 33 cikkelyéhez képest egy részletesebb, bővebb szerződés, amely 142 cikkben foglalta össze a szerződés gyakorlati végrehatására irányuló szabályokat. Az SchVE felépítése, főbb területei a következők:

- Alapfogalmak, meghatározások
- A ellenőrzések megszüntetése a belső határokon és a személyek mozgása:
    - A belső határok átlépése
    - A külső határok átlépése
    - Vízumok
    - A külföldiek közlekedési feltételei
    - Tartózkodási engedélyek és beléptetési tilalom
    - Kiegyenlítő intézkedések
    - A menedék iránti kérelem elbírálásának feladatai
- Rendőrség és biztonság
    - Rendőri együttműködés
    - Bűnügyi jogsegély
    - A „ne bis in idem” elvének alkalmazása
    - Kiadatás
    - Büntető ítéletek végrehajtásának átadása
    - Kábítószerek
    - Lőfegyverek és lőszerek

[24] Uo.
[25] Például mi a belső határ, külső határ, harmadik állam.
[26] Norbert Schuman: Schengeni együttműködés a kezdetektől a jelenig. Baden-Württemberg Belügyminisztériuma. Stuttgart, 2000. 4. o.

- A Schengeni Információs Rendszer
  - A Schengeni Információs Rendszer működtetése és használata
  - A személyes jellegű adatok védelme és az adatok biztonsága a Schengeni Információs Rendszerben
  - A Schengeni Információs Rendszer költségeinek felosztása
- Áruszállítás és áruforgalom
- A személyes adatok védelme
- A Végrehajtó Bizottság
- Záró rendelkezések[27]

Az 1990-ben aláírt egyezmény azonban még nem jelentett gyors megvalósulást. Az eredeti egyezménytől 5 év telt el a SchVE aláírásáig, és még újabb 5 évnek kellett eltelnie a gyakorlati hatályba lépéséig. Ennek fő oka az eltérő informatikai eszközpark, illetve a tagállamokban a jogharmonizáció szükségessége volt. Ugyanakkor az életbe lépést sürgették a repülőtér- és kikötőtulajdonosok, akik ekkorra már jelentős kiadást könyvelhettek el, az átalakítás kapcsán, amely lehetővé tette a belső és külső határ szerinti határforgalom-ellenőrzést.

A Schengeni megállapodás/egyezmény kapcsán 1985, 1990, 1995 meghatározó dátumok. Így 2025-ben immár 40 éve annak, hogy a Mosel folyó partján kikötött az a hajó, amelynek utasai Schengenben aláírták a megállapodást, 35 éve, hogy megszületett a végrehajtási egyezmény, és 30 esztendeje, hogy gyakorlatilag is hatályba lépett a SchVE. A schengeni megállapodások folyamatos végrehajtását a Amszterdami Szerződés és a tamperei, bécsi, hágai, stockholmi programok biztosították.

Magyarország a vasfüggöny felszedése után kinyilvánította euro-atlanti csatlakozás iránti igényét.[28] A hazánk teljes jogú tagságához vezető úton

[27] Egyezmény a Benelux Gazdasági Unió államai, a Németországi Szövetségi Köztársaság és a Francia Köztársaság kormányai között a közös határaikon történő ellenőrzések fokozatos megszüntetéséről szóló, 1985. június 14-i Schengeni Megállapodás végrehajtásáról.
[28] Ritecz György: A magyar Határőrségről Magyarország NATO csatlakozása kapcsán. In: Társadalom és Honvédelem 1999/ 2. szám. 119-129. o.

minden területen már az 1990-es évek közepétől elindult a felkészülés. Ehhez az EU és a NATO is jelentős segítséget nyújtott. Ennek a folyamatnak a részeként a magyar határőrség számára PHARE (COP) és bilaterális támogatású technikai fejlesztési, jogalkotási, képzési és twinning programok keretén belül adtak támogatást. Schengen kapcsán először 1998-ban valósult meg szakmai tanulmányi út a Német Szövetségi Határőrséghez, amelyet követően a határőrség Budapesti Vezetőképző Intézet (BVTI) falai között sor került az első schengeni képzési projektekre. Ezeket követte az Europol–Schengen projekt, amelyet a Rendőrtiszti Főiskola nyert el, és ezáltal a hazai határőr, rendőr kollégák megismerhették a holland, német, francia, osztrák schengeni modelleket és az Europolt. Hazánk 2004. május 1-jei Európai Unióba való belépését követően 2007. december 21-től[29] teljes jogú Schengen-taggá vált, ezáltal állampolgárai élvezhetik a *„szabadság – biztonság – jog”* térségben a szabad mozgás előnyeit, amely kiegészült a szabad munkavállalással.

Mára természetessé vált, ami régen elképzelhetetlen volt, hogy úgy haladunk át Európában az államhatárokon, hogy már nem is érzékeljük a korábbi határátkelőhelyeket, és nem érezzük a gyomrunkban az útlevél- és vámellenőrzés pszichológiai hatását. Ugyanakkor az elmúlt évek kihívásai, a COVID-19 világjárvány,[30] a tömeges illegális migráció[31] a schengeni tagállamokban eltérő reakciókat váltottak ki, és a globális, kontinentális problémákra a schengeni tagállamok közül többen lokális megoldásként (ellentétesen a schengeni gondolatokkal és szabályokkal) a belső határokon visszaállították a határforgalom-ellenőrzést.

[29] A szárazföldön, míg a légi határok vonatkozásában 2008. 03. 28-tól.
[30] Ritecz György (2022): Az államhatárok régi/új szerepben a COVID19 járványban es azt követően. In: Michalkó, G. – Németh, J. – Birkner, Z. (szerk): Turizmusbiztonság, járvány, geopolitika. Bay Zoltán Alkalmazott Kutatási Közhasznú Nonprofit Kft. Budapest, 2022. 23-36. o.
[31] Ritecz György: Az Európába irányuló tömeges irreguláris migráció felfutásának és megszűnésének okai. In: Hadtudomány 2018/3-4. szám. MHTT. Budapest. 66-78. o.

A globalizáció következtében kialakult helyzet Európát arra ösztönzi, hogy a versenyképességrt lehetőleg megőrizze, illetve javítsa. Ennek érdekében a személyek és munkaerő szabad áramlását fenn kell tartani, illetve meg kell erősíteni, aminek egyik biztosítéka a schengeni térség értékeinek megőrzése. Ugyanakkor az elmúlt időszakban bekövetkezett migrációs folyamatok hatása miatt a schengeni értékek védelme új kihívások elé állítja a tagállamokat, főleg a külső határok felügyelete, őrizete terén. Véleményem szerint a külső határokkal rendelkező schengeni tagállamok iránt nagyobb szolidaritást kell tanúsítaniuk a csak belső szárazföldi határokkal rendelkező tagállamoknak. Mind az EU politikai vezetésének, mind az általa működtetett Frontexnek nagyobb szerepet kell vállalnia a schengeni térség biztonsága érdekében a külső határok védelmében.

Felhasznált irodalom

„*A Schengeni Egyezmény elmélete, gyakorlata és hatása a magyar határőrizeti rendszer kiépítésére*" c. MTA. OKTK. nyilvántartási száma: A.1882/VII/01 kutatási projekt. 2001-2002.

Az EU a szabadság, biztonság és jog térsége. (222 kérdés és 222 válasz a bel- és igazságügyi együttműködésről). BM Oktatási Főigazgatóság. Budapest, 2004.

Megállapodás a Benelux Gazdasági Unió államai, a Németországi Szövetségi Köztársaság és a Francia Köztársaság kormányai között a közös határaikon történő ellenőrzések fokozatos megszüntetéséről szóló, 1985. június 14-i Schengeni Megállapodás végrehajtásáról.

Egységes belbiztonsági és jogi térség Európában. Miniszterelnöki Hivatal Integrációs Stratégiai Munkacsoport. Budapest, 1999.

Fejes Zsuzsanna – Sallai János – Soós Edit – Tóth Judit – Vájlok László: Schengenre hangolva. In: Európai Műhelytanulmányok. Budapest, 2004.

Fórizs Sándor: A rendészeti változások iránya, tendenciái, mozgatórugói. In: Gaál Gyula, Hautzinger Zoltán (szerk): A határrendészettől a rendészettudományig. Pécs.

Kobolka István – Ritecz György – Sallai János: Szabadság, biztonság, jog térségének kiterjesztése a Kárpát-medencében. Szakmai Tudományos Közlemények 2004/2. szám. Budapest.

Kobolka István – Sallai János: A schengeni határnyitás elsődleges tapasztalatai. Szakmai Szemle 2008/2. szám. Budapest.

Norbert Schuman: Schengeni együttműködés a kezdetektől a jelenig. Baden-Württemberg Belügyminisztériuma. Stuttgart, 2000.

Ritecz György: A magyar Határőrségről Magyarország NATO csatlakozása kapcsán. In: Társadalom és Honvédelem 1999/ 2. szám.

Ritecz György: A Schengeni Egyezmény előírásai és Magyarország. In: Cég és Jog 2002/7-8. szám. ARGUTUS Kiadó Kft. Budapest.

Ritecz György: Gondolatok az Európai Egységes Határőrség kialakításáról. In: EU-Tanulmányok IV. Nemzeti Fejlesztési hivatal. Budapest, 2004. 695-763. o.

Ritecz György: Az Európába irányuló tömeges irreguláris migráció felfutásának és megszűnésének okai. In: Hadtudomány 2018/3-4. szám. MHTT. Budapest.

Ritecz György: Az államhatárok régi/új szerepben a COVID19 járványban es azt követően. In: Michalkó, G. – Németh, J. – Birkner, Z. (szerk): Turizmusbiztonság, járvány, geopolitika. Bay Zoltán Alkalmazott Kutatási Közhasznú Nonprofit Kft. Budapest, 2022.

Ritecz György-Sallai János: A Schengeni Egyezmény és a magyar határőrizet. In: európa tükör 2001/5. szám.

Sallai János - Szőke István - Varga János - Vass Ferenc - Vájlok László - Virányi Gergely: Határellenőrzés az Európai Unióban. Hanns Seidel Alapítvány. Budapest, 2000. 268. o.

Sallai János: A Schengeni Végrehajtási Egyezmény felépítése tartalma, gyakorlati tapasztalatai és jövője az Amszterdami Szerződés tükrében. Határőrség Képzési és Módszertani Főosztály. Budapest, 2000. 164. o.

Sallai János: A Schengeni Egyezmény. In: Ezer kérdés – ezer válasz az Európai Unióról. 2003.

Sallai János: A bel- és igazságügyi együttműködés általános jogi tudnivalói. Hanns Seidel Alapítvány. Budapest, 2004.

Sallai: János: A Schengeni Végrehajtási Egyezmény felépítése, tartalma és végrehajtásának tapasztalatai. In: Rendvédelmi füzetek. Rendőrtiszti Főiskola. Budapest, 1999.

Schengeni Egyezmény a Benelux Gazdasági Unió Államainak kormányai, a Német Szövetségi Köztársaság kormánya és a Francia Köztársaság kormánya között a közös határokon történő ellenőrzés fokozatos megszüntetéséről. Schengen.

Schengeni Közös Kézikönyv. Európai Unió Tanácsa. Brüsszel, 2005.

Tóth Árpádné Masika Edit –Tóth Judit –Sallai János – Ritecz György – Szikinger István – Szamosvölgyi Csaba –Finszter Géza – Eördögh Árpád –Rajczy Lajos: Magyarország csatlakozása az EU megreformált igazságügyi együttműködéséhez, a megváltozott külső feltételek között – Belügyi együttműködés. In: Európai Tükör – Műhelytanulmányok. Integrációs Stratégiai Munkacsoport Kiadványa, 1997.

Tóth Judit: Átjárható határok az Európai Unióban. (Személyek szabad mozgása). Európai Füzetek. 2003.

Volker Westphal: A Schengeni Szerződés a határrendészeti gyakorlatban. Swisttal, 1998.

Volker Westphal: Aktuelles aus der Gesetzgebung, Literatur und Rechtspreheung. Lübeck, 2004.

DOI-azonosító: https://doi.org/10.53304/RT.2025.2.05

KARDOS SÁNDOR ISTVÁN

A parancs … az parancs

Absztrakt
A szerző a katonai bűncselekmények közé tartozó parancs iránti engedetlenséget vizsgálja meg. Szakirodalmi előzmények, valamint jogerősen lezárt büntető- és fegyelmi eljárások alapján mutatja be a magatartás elkövetési és megvalósulási körülményeit, a bűncselekmény legfőbb jellemzőit. Írásával segítséget kíván nyújtani a rendőri vezetőknek a parancs iránti engedetlenség észlelésekor szükséges, elvárt és kötelező parancsnoki intézkedésekhez.

Kulcsszavak: rendőrség, katonai bűncselekmény, parancs iránti engedetlenség, vezetői intézkedések

Abstract
The author examines misconduct against command, which is categorized as military crime. The author presents the circumstances of such behaviour through previously published literature as well as on the basis of legally closed disciplinary proceedings. With this publication, the author aims to provide guidance to police leaders what measures are needed, expected, and compulsory when they recognize misconduct against command.

Keywords: police, military crime, misconduct against command, measures by leaders

Bevezetés

A katonai jellegű szervezetek eredményes működésének egyik alapfeltétele, hogy az állomány tagjai a számukra meghatározott feladatot, a kiadott jogszerű és törvényes utasítást, a parancsot az előírásoknak megfelelően teljesítsék. Nem okozhat meglepetést tehát az a körülmény, miszerint a katonai jellegű szerveknél a paranccsal szembeni engedetlenség szankcionálásának büntetőjogi lehetősége (is) biztosított. Tanulmányomban e kérdéskört vizsgálom meg.

A rendőrség alá-fölérendeltségi viszonyok révén, hierarchikusan és egyben a weberi hivatali, bürökratikus viszonyok között[1] végzi napi, általános és speciális feladatai. A szervezeti viszonyokban a bürokráciával párhuzamosan a katonai beosztásokon és katonai rendfokozatokon alapuló hierarchia is jelen van, a magasabb szinten elhelyezkedő vezető/parancsnok a katonai viszonyok között értelmezhető utasítások, parancsok révén irányítja beosztottjait.

A rendőri szervezet katonai elvek szerinti „működése" megítélésem szerint nem tekinthető teljeskörűnek, mivel nem minden szolgálati ág, illetve szakszolgálat esetében jelenik meg, illetve érvényesül következetesen és egyértelműen a katonai hierarchia. Egyes területeken a munkavégzés során a hivatalai jellegű feladatvégrehajtás dominál, és kisebb mértékben érzékelhető a katonai hierarchia a mindennapokban. A rendőrségen belül a katonai „működés" a szolgálatoknál eltérő mértékben és arányban mutatható ki. E körülmény leginkább a rendészeti területen dominál, más szervezeti elemeknél, például a gazdasági vagy humánigazgatási szakterületen sokkal kevésbé érvényesül. A bűnügyi szolgálati ágnál e vonatkozásban egyfajta kettősség tapasztalható, egyidőben van jelen a szolgálati tevékenység ellátásakor a katonai, illetve a hivatali működés.

E körülményekre és jellemzőkre figyelemmel – álláspontom szerint – a rendőrség nem nevezhető a fogalom klasszikus értelmezése szerinti katonai

[1] Jenei György: Max Weber bürokráciaelmélete és a neoweberiánus szintézis. Pro Publico Bono – Magyar Közigazgatás 2016/3. szám. Budapest. 42-44. o.

szervezetnek, hanem inkább katonai jellegűnek értelmezem. E fogalomértelmezés kizárólag a publikáció keretein belül releváns, mivel a napi szolgálatellátás jellegétől, formájától függetlenül a hivatásos állományú rendőr a büntetőjog alapján katonának minősül, és katonai bűncselekményt tettesként katonaként követhet el.[2] Vagyis a katonai jelleg, mint megközelítés mellett is egyértelműen kijelenthető, hogy a rendőrség esetében a törvényes rend és fegyelem megléte kiemelten fontos feltétele a szervezet hadrafoghatóságának és készenlétének,[3] mivel a bürokratikus jellemzőkön túlmenően a rendőrégen – ellentétben a civil szféra bürokratikus szervezeteivel – az alá-fölérendeltségi viszonyok a meghatározóak.[4]

Általánosan elfogadott vélekedés, hogy a katonai jellegű szervezetek esetében az értékek, az erkölcsi megbízhatóság mást jelent, mint hasonló civil vonatkozásaik.[5] A normák és értékek a meghatározott szervezeti kultúrában érvényesülnek. A szervezet és az egyén egymással kölcsönös függőségi viszonyokban álló csoportok hálózata, ezáltal a szervezetek visszahatnak az egyén viselkedésére.[6] E felvázolt körülmények és a jelzett egyedi jellemzőkkel rendelkező és speciális szabályozók alapján működő rendőrségen – mint katonai jellegű közösségben és munkahelyen – törvénysze-

[2] A Büntető Törvénykönyvről szóló 2012. évi C. törvény (a továbbiakban: Btk.) 127. § (1), (2) és (3) bekezdései

[3] Honfi Attila: A katonai fegyelem és a bekövetkezett bűncselekmények összefüggései a Magyar Honvédségnél az 1990-es években. Zrínyi Miklós Nemzetvédelmi Egyetem Kossuth Lajos Hadtudományi Kar Szociológia Pedagógia és Pszichológia Tanszék. Egyetemi Tankönyv. Budapest, 2006. 89. o.

[4] Kovács Gábor: A rendészeti szervek szervezeti kultúrájának összetevői és sajátosságai, a téma feldolgozása a Rendőrtiszti Főiskola vezetéselméleti oktatásában. Pécsi Határőr Tudományos Közlemények 10. kötet. Pécs, 2006. 223-234. o.

[5] Harai Dénes: A modern haderőtechnika és értékfelfogása. Társadalom és Honvédelem. 2015/1. szám. Budapest. 71-78. o.

[6] Vámosi Zoltán: Szociológiai aspektusok. Főiskola jegyzet. Gábor Dénes Főiskola. Budapest, 2001.

rűen jellemző a külvilágtól történő elhatárolódás, a zártság, melynek alapvetően védelmi jellege van, és a jogsértések elleni fellépés eredményességét és hatékonyságát is szolgálja.[7]

Vizsgálatomat több évtizedes fegyelmi szakterületi tapasztalataimra alapozom, miszerint a parancsmegtagadás, mint magatartás elkövetési/megvalósulási körülményeinek pontos értékelése és a történések szakszerű (akár büntetőjogi) minősítése kapcsán sem a beosztotti állomány, sem a parancsnokok, sőt gyakran a fegyelmi jogkört gyakorló elöljárók sem rendelkeznek mindenre kiterjedő ismerettel. Az elöljárók ezen ismerethiánya – szakmai álláspontom szerint – negatív hatást gyakorolhat a kiadott paranccsal szembeni ellenszegülés, vagyis a parancs iránti engedetlenség felfedésekor elvárt, szükséges és kötelező vezetői intézkedések eredményességére, hatékonyságára. E körülmény pedig megítélésem szerint alapvető módon befolyásolja a katonai rend és fegyelem védelmét, fenntartásának hatékonyságát, illetve az elkövetőnek és másoknak az esetleges későbbi parancsmegtagadástól történő visszatartását.

Mindezekre figyelemmel tanulmányomban – szakirodalmi előzmények, valamint jogerősen, elmarasztalással zárult katonai büntetőeljárások és fegyelmi tárgyú intézkedések[8] adatai alapján – a rendőrség[9] hivatásos állományú tagjai által megvalósuló/megvalósított parancs iránti engedetlenség bűncselekmény körülményeit, a magatartások főbb jellemzőit mutatom be

[7] Elek László: Korrupciós kockázatok a közszektorban, különös tekintettel a rendészeti (rendőri) igazgatás területére. Belügyi Szemle 2014/10. szám. Budapest. 59-98. o.

[8] Megítélésem szerint kizárólag a jogerősen és egyben elmarasztalással zárult eljárások alkalmasak objektív elemzésre/értékelésre, mivel ezen ügyekben kétséget kizáróan és tényszerű eljárási adatok alapján nyert bizonyítást az elkövetett cselekmény, valamint az elkövető(k) esetbeli felelőssége.

[9] A tanulmányban a rendőrség kifejezést a rendvédelmi feladatokat ellátó szervek hivatásos állományának szolgálati jogviszonyáról szóló 2015. évi XLII. törvény (a továbbiakban: Hszt.) 1. § (1) bekezdés a) pontjában meghatározott, az általános rendőrségi feladatok ellátására létrehozott szerv vonatkozásában használom.

és vizsgálom meg.[10] Arra kívánok rámutatni, hogy egy utasítás vagy parancs megtagadása, az azzal szembeni engedetlenség önmagában nem eredményez minden esetben büntetőeljárást a hivatásos állományú rendőrrel szemben, mivel az elkövetési körülmények jelentősen befolyásolják e cselekmény minősítését. Ezáltal a paranccsal szembeni engedetlenség, mint magatartás bizonyos elkövetési feltételek hiányában nem minősül bűncselekménynek, meghatározott feltételek esetén fegyelemsértést alapoz(hat) meg.

Azt is be kívánom mutatni, hogy amennyiben egy utasítással/paranccsal szemben megjelenő engedetlenség bűncselekmény megalapozott gyanúját kelti, akkor sem feltétlenül és nem kizárólagosan minősíthető az eset parancs iránti engedetlenségnek.

A parancs értelmezése a rendőrségen, mint katonai jellegű szervezetben

Napjainkban alapvető igényként fogalmazódik meg, hogy az állami szervek munkatársai feladataikat kötelességtudóan, szakszerűen, felelősséggel végezzék. A hivatásos állománytagok munkavégzése – és a szolgálati időn kívüli tevékenysége is, vagyis a mindennapjai – az adott területre vonatkozó jogszabályi rendelkezések pártatlan, előítéletektől és befolyástól mentes végrehajtására vonatkozó elvárással egészül ki.[11] Nem képezheti vita tárgyát, hogy a katonai jellegű, hierarchikusan felépülő, alá- és fölérendeltségek viszonyrendszerében „működő” rendőrség – mint rendvédelmi szerv[12] – eredményes működése, feladatainak maradéktalan ellátása,

[10] Vizsgálatom a katonai bűncselekmények speciális eljárási szabályainak, valamint a büntetőeljárások rendszerének teljes körű értékelésére és részletes bemutatására nem terjed ki.

[11] Kovács István: A parancs szerepe a rendészeti vezetésben. Katonai Jogi és Hadijogi Szemle 2024/2. szám. 50. o.

[12] A központi államigazgatási szervekről, valamint a Kormány tagjai és az államtitkárok jogállásáról szóló 2010. évi XLIII. törvény 1. § (5) bekezdése alapján rendvédelmi szervek: a rendőrség, a büntetés-végrehajtási szervezet, a hivatásos katasztrófavédelmi szerv,

valamint a szervezettel szemben támasztott szakmai követelmények megvalósítása, a szakmai elvárások teljesítése elképzelhetetlen a feladatvégrehajtásra vonatkozó parancsok maradéktalan betartása és betartatása nélkül. E gondolatiság nem korunk terméke, mivel a katonai jellegű szervezetnél az alárendeltek engedelmességi kötelezettsége már a mai tudásunk szerint ismert legkorábbi hadtudományi műben is megjelent[13], valamint már a „legrégebbi korokban" is általában súlyos büntetéssel fenyegették a parancs iránti engedetlen katonai magatartást.[14] A közelebbi múltból merítve sem értékelhető – megítélésem szerint – egyértelműen túlzónak napjainkban az az immáron százéves kinyilatkoztatás, miszerint: *„A katonai szervezetnek, ennek a rendkívül bonyolult organizmusnak az életképességét a függelem biztosítja. A függelem pedig a feltétlen engedelmességre való kötelességet foglalja magában."*[15]

A parancs iránti engedetlenség vizsgálatát megelőzően szükséges a rendőri szervezet vezetési, parancsadási rendszerének értékelése. A rendvédelmi szervek vonatkozásában – a vezetéstudomány alaptéziseként – a vezetési stílusok tág és szűk értelmezése ismert. A tágabb értelmezés a teljes szervezet irányítását, a szűkebb értelmezés pedig egy szervezeti elem vezetését jelenti. A két értelmezés alapján az irányító és vezető személye is elkülöníthető, az irányító a szervezeten és az általános hierarchián kívül, a vezető személye pedig az általa irányított szervezet vagy szervezeti elem csúcsán, de a rendszeren belül helyezkedik el. E minőségében a vezető a munkavégzésre vonatkozó parancs kiadására jogosult, amely az általa val-

a Nemzetbiztonsági Szolgálat, a Polgári Nemzetbiztonsági Szolgálat és a Katonai Nemzetbiztonsági Szolgálat.

[13] Szun-Ce: A hadviselés törvényei. Balassi Intézet. Budapest. 1995. – *„Ha szokásává tesszük a katonáknak, hogy amire tanítjuk, mindig teljesítse, akkor az mindig engedelmeskedni fog. De ha eltűrjük, hogy ne teljesítse azt, amire tanítjuk, akkor a nép nem fog engedelmeskedni (parancsainknak). Ha parancsainkat megszokott engedelmességgel teljesítik, akkor a sokasággal könnyű lesz szót értenünk."*

[14] A római jogban parancsmegtagadás esetén háborúban halállal volt büntethető. Lásd: Vincze Miklós: A katonai büntetőjog kétezer éves tükre. Ügyészek Lapja 2006/6. szám.

[15] Miskolci Jogászélet 1925/12. szám. 6-7. o.

lott elvek, szakmai tapasztalatok, kialakult eljárások/eljárási rendek, valamint a konkrét – általában munkahelyi – körülmények által meghatározott, és ezek összessége határozza meg az adott vezető konkrét vezetési stílusát.[16]

A kiadott parancs megtagadását, teljesítésének elmulasztását vizsgálatom keretében kizárólag a vezető személyének vonatkozásában és kizárólag a hivatásos állomány esetében értékelem. A rendőri szervezet működőképességének igénye bármely állománycsoportba[17] tartozók esetében feltételezi a vezetői utasítás végrehajtásának szükségességét, a parancs teljesítésének kötelezettsége viszont fokozottan jelentkezik a hivatásos állománynál, mivel a rendvédelem „*feladatait csak szilárd erkölcsi-fegyelmi közegben képes megoldani, … ez az elvárás funkciójukból következően különösen a hivatásosokra vonatkozik…*”[18]. A parancsteljesítési kötelezettség jelentőségét az a körülmény is igazolja, hogy e kötelem (már) a hivatásos állományba történő kinevezéskor, az eskü szövegében is megjelenik, miszerint *„… elöljáróim parancsainak engedelmeskedem…”*.

A vezetés kapcsán két alapelv – az egyszemélyi és a centrális vezetés – különíthető el. Egyszemélyi vezetés esetén a vezető a szervezet jogszerű működéséért, tevékenységéért osztatlan és teljes felelősséggel tartozik, ezen túlmenően a szervezet képviselete, fejlesztése is a feladatai közé tartozik.[19] Centrális vezetés esetében a szervezet elsőszámú vezetőjétől kapott parancsokat, utasításokat a szervezetben vezető tisztséget (beosztást) betöltő személyek is kötelesek végrehajtani, és azt az irányításuk alá tartozó

[16] Kovács Gábor et. al.: A szervezetvezetés elmélete. Dialóg Campus. Budapest, 2017.
[17] A Rendőrségről szóló 1994. évi XXXIV. törvény (a továbbiakban: Rtv.) 4/A. § (3) bekezdése alapján az általános rendőrségi feladatok ellátására létrehozott szerv személyi állománya hivatásos állományú rendőrökből, igazságügyi alkalmazottakból, rendvédelmi igazgatási alkalmazottakból, a munka törvénykönyvéről szóló törvény hatálya alá tartozó munkavállalókból, tisztjelöltekből, valamint szerződéses határvadászokból állhat.
[18] Törő Lajos: A katonai etika, a tiszti hivatás és értékrend néhány kérdése. Hadtudományi Szemle 2016/1. szám. 287. o.
[19] Alice Miller: More already on the central comittee’s leading small groups. China Leadership Monitor 2014/44. szám. 1-8. o.

állománnyal végrehajtatni.[20] A feladatok/információk áramlása és a kapcsolattartás a rendőrségnél parancsirányítási rendszer útján történik, amelyhez a vezetők sajátos jogkört birtokolnak. A rendszert alapvetően a vezetői utasítási/parancsadási és a beosztottak végrehajtási kötelezettsége jellemzi.[21]

Fontos kiemelni, hogy a rendvédelmi szerveknél – így a rendőrségnél is – a kiadott parancs nem „egyirányú". A parancsot kapó beosztott – a parancsot kiadó személy és a parancs tekintélyének fenntartása mellett – bizonyos, a büntetőjog kereteivel is védett módon, visszacsatolásként a parancsot jogszerűen megkérdőjelezheti, illetve azt meg is tagadhatja, amely körülmény büntethetőséget kizáró okként jelenik meg. Ugyanezen büntetőjogi keretrendszer a vezető által kiadott parancsot is védett „eszköznek" tekinti.[22] Vagyis a parancsra végrehajtott jogellenes cselekményért a katona kizárólag akkor büntethető, ha tudatában volt annak, hogy a végrehajtással bűncselekményt követ el.

A katonai vétség – így a parancs iránti engedetlenség vétsége – esetén a jogbiztonság és az elkövető személyének védelme körébe sorolható a büntetőjog által biztosított büntethetőséget megszüntető azon ok, miszerint a katona elkövető a szolgálati viszonyának megszűnését követően csak korlátozott időtartamig felelős a katonai jellegű jogsértésekért.[23]

A Rendőrségi törvény is rendelkezik arról, hogy a bűncselekmény elkövetésére vonatkozó/utasító parancs végrehajtását a (parancsot kapó) rendőr

[20] John Levin et. al.: Introduction to Choice Theory. United Kingdom. Oxford University Press. 2004.

[21] Kovács Gábor: A rendészeti szervek vezetés- és szervezéselmélete. Budapest: Nemzeti Közszolgálati Egyetem. 2014.

[22] Btk. 130. § (1) és (2) bekezdése. Büntethetőséget kizáró ok. Btk. 130. §: *„Nem büntethető a katona a parancsra végrehajtott cselekményért, kivéve, ha tudta, hogy a parancs végrehajtásával bűncselekményt követ el. A parancsra elkövetett bűncselekményért a parancsot adó is tettesként felel, ha a katona tudta, hogy a parancs végrehajtásával bűncselekményt követ el, egyébként a parancsot adó közvetett tettesként felel."*

[23] A büntethetőséget megszüntető ok. Btk. 131. §: *„ …Nem büntethető katonai vétség miatt az elkövető, ha szolgálati viszonyának megszűnése óta egy év eltelt."*

mely esetekben kell, hogy megtagadja,[24] a szabályozás viszont abban a vonatkozásban egyértelmű, hogy egyéb esetekben nincs jogszerű lehetőség a normaszegő parancs megtagadására.[25] Ugyanezen elvárások/alapelvek megjelennek a szolgálati törvényben is.[26]

A parancs jogellenessége akkor értékelhető nyilvánvalónak, ha a jogellenesség nyomban és mindenki számára közérthetően következik,[27] illetve nyilvánvalóan a parancsot kapó számára is egyértelműen felismerhető, hogy annak végrehajtásával bűncselekményt követne el.[28] Ezzel párhuzamosan a rendőri szervezet belső részletszabályozása keretében – mind a parancsnokok, mind a beosztottak vonatkozásában – megjelennek a konkrét végrehajtásra vonatkozó kötelmek is.[29] A bemutatott normák általi sza-

[24] Rtv. 12. § (1) bekezdése: *„A rendőr a feladata teljesítése során köteles végrehajtani a szolgálati elöljáró utasításait. Meg kell tagadnia az utasítás végrehajtását, ha azzal bűncselekményt követne el."*

[25] Rtv. 12. § (2) bekezdése: *„A rendőr a szolgálati elöljáró jogszabálysértő utasításának teljesítését – bűncselekmény elkövetésének kivételével – nem tagadhatja meg, de az utasítás jogszabálysértő jellegére, ha az számára felismerhető, haladéktalanul köteles az elöljáró figyelmét felhívni. Ha az elöljáró az utasítást fenntartja, azt az utasított kérelmére köteles írásba foglalva kiadni. Az írásba foglalás megtagadása vagy elmaradása az utasítást adó közvetlen felettesénél bejelenthető, e jog gyakorlásának azonban az utasítás teljesítésére nincs halasztó hatálya."*

[26] Hszt. 103. § (1) és (2) bekezdése *„A hivatásos állomány tagja szolgálatteljesítése során köteles végrehajtani a szolgálati elöljáró parancsát, a felettes rendelkezését, kivéve, ha azzal bűncselekményt követne el. Bűncselekmény kivételével a hivatásos állomány tagja a jogszabálysértő parancs, rendelkezés végrehajtását nem tagadhatja meg. Ha azonban annak jogellenessége felismerhető számára, arra haladéktalanul köteles a szolgálati elöljáró figyelmét felhívni. Ha a szolgálati elöljáró a parancsát, a felettes a rendelkezését ennek ellenére fenntartja, azt kérelemre írásba kell foglalnia. A jogszabálysértő parancs, rendelkezés végrehajtásáért kizárólag az azt kiadó felel."*

[27] Fővárosi Bíróság Katonai Tanácsa KB. VIII. 437/1883.

[28] Hajdú-Bihar Megyei Bíróság Katonai Tanácsa KB. II. 42/2019.

[29] A rendőség szolgálati szabályzatáról szóló 30/2011. (IX. 22.) BM rendelet (a továbbiakban: Szolgálati Szabályzat) 90. § (5) és (6) bekezdése. *„Az utasítást az alárendelt ellentmondás nélkül, kellő időben és a legjobb tudása szerint hajtja végre. Ha a parancs teljesítését másik szolgálati elöljáró parancsa akadályozná, az alárendelt az előzőleg ka-*

bályozás alapján kijelenthető, hogy a rendszer mind a parancsot kiadó elöljáró, mint a végrehajtásra kijelölt beosztott részére megfelelő jogszabályi kereteket és védelmet – fegyelmi- és büntetőjogi védelmet – biztosítanak a normaellenes parancs teljesíthetősége kapcsán azáltal, hogy mindkét fél számára nem kizárólag lehetőségek, hanem kötelezettségek is megfogalmazódnak.[30]

A normaháttér alapján a rendőrségen a parancs kiadásának rendszere nem *„parancsuralomnak”*, hanem szigorúan centralizált és szabályozott rendvédelmi modellnek értékelhető, amely a befolyásolás jogát a szervek közötti irányítási jogkörként értékeli,[31] hiszen a rendőrség nem működhet a jogszabályok szigorú betartása és végrehajtása nélkül.[32]

Mindezek mellett a parancs és a parancs iránti feltétel nélküli engedelmesség a rendőrség fegyelmének, katonai szolgálati rendjének legfontosabb tartópillérének és biztosítékának, legelemibb részének tekinthető, ahol a feltétel nélküliség nem korlátlanságot, hanem az alá-fölérendeltségen alapuló normatív, a büntetőjog által is védett közjogi szervezetszabályozást jelent.[33] Megítélésem szerint e normatív védelem körébe sorolhatóságot igazolja az a körülmény is, miszerint a parancs iránti engedetlenség az egyetlen olyan katonai bűncselekmény, amelynek már a vétségi alapesete

pott utasítást köteles jelenteni. Ha a szolgálati elöljáró ennek ellenére utasítást ad parancsa végrehajtására, azt teljesíteni kell. Az utóbbi utasítás teljesítését követően az első utasítás végrehajtását meg kell kezdeni, valamint folytatni kell. Az első utasítás teljesítésének elmulasztásáért, késedelmes teljesítéséért az új utasítást adó szolgálati elöljáró felelős. Az, aki az újabb parancsot adta, értesíti erről az előző utasítást adó szolgálati elöljárót. Az utasítás végrehajtását mindkét szolgálati elöljárónak jelenteni kell. A fontosabb utasításokat a szolgálati elöljáró írásban adja ki, és gondoskodik az érintett beosztottak előtt történő kihirdetésükről.”

[30] Korda György: A katonai és honvédelmi kötelezettségek elleni bűncselekmények. Zrínyi Katonai Kiadó. Budapest, 1988. 143. o.

[31] Madarász Tibor: Közigazgatás és jog. Közigazgatási és Jogi Kiadó. Budapest, 1987.

[32] Kovács István: Klasszikus vezetési funkciók a parancsuralmi rendszerben (állományvédelmi) ellenőrzés, és korrupciómegelőzés a helyi és a területi rendvédelmi szervek körében. Nemzeti Közszolgálati Egyetem. Budapest, 2019.

[33] Hautzinger Zoltán: A katonai büntetőjog rendszertana. Pécs: AndAnn, 2010.

is – a bűncselekmény tényállásának (1) bekezdésében is megjelenítve – büntethető elzárással.[34]

A (katonai) parancs fogalmának értelmezésekor fontos megállapítások tehetőek a Rendészettudományi Szaklexikon és Hadtudományi Lexikon-megfogalmazásinak összevetésekor.

Rendészettudományi Szaklexikon	**Hadtudományi Lexikon**
„(1) Az elöljáró szolgálati akaratának legfőbb kifejezési módja, vezetési eszköze, rendelkezése az alárendelt kötelezettségeinek teljesítésére. *(2) Az alárendeltek kötelező magatartási szabálya, az elöljárói akarat megvalósítási eszköze. A ~csal szemben az alárendelt engedelmességgel tartozik.* *(3) Egyedi utasítás meghatározott tevékenység, faladat végrehajtására.”*[35]	*„A parancsnok kezében vezetési eszköz, amelyet a katona köteles maradéktalanul végrehajtani. A ~ot lehet szóban, írásban (rajzban), jelekkel és jelzésekkel adni. Az elöljárónak parancsadásakor támaszkodnia szükséges a rendelkezésre álló adatokra, figyelembe kell venni a végrehajtás feltételeit, az alárendelt személyi tulajdonságait, felkészültségét. Az elöljáró a ~ot úgy adja, hogy az a végrehajtó alárendelt számára világos, egyértelmű és az adott körülményekhez képest a legrövidebb legyen, a végrehajtó katona pedig érezze a ~ szükségességét, hogy annak tudatában meggyőződésből cselekedhessen. Magasabb szintű parancsnokok hatáskörüknek megfelelően*

[34] Btk. 444. § (1) bekezdése. A törvény 46. §-a szerint az elzárás tartamát napokban kell meghatározni, annak legrövidebb tartama öt, leghosszabb tartama kilencven nap, azt büntetés-végrehajtási intézetben kell végrehajtani.

[35] Rendészettudományi Szaklexikon. Budapest: Dialóg Campus. 2019. 438. o.

	írásos formában is adhatnak ki rendelkezéseket. Az írásbeli rendelkezésben meg kell határozni annak hatályát, a kihirdetés módját és a végrehajtás jelentésének határidejét."[36]

1. számú táblázat
A Rendészettudományi Szaklexikon és a Hadtudományi Lexikon fogalommeghatározása a „parancs" kifejezésre

A fogalommeghatározások különbözőségei és eltérő hangsúlyi elemei ellenére mindkét változatban megtalálható az a négy jellemző, amelyek a parancs értelmezését adják.

A parancs elsődlegesen vezetői akaratot kell, hogy kifejezzen, amely a parancsadó akaratán kívül azt is feltételezi, hogy a címzett ebből az akaratból következtessen/következtethessen arra, hogy neki tennie kell valamit.[37]

A katonai parancs csak részben jeleníti meg a parancsadó egyéni akaratát, mivel abban a szervezeti akarat is jelen van. E kettő nem különíthető el egymástól, és a parancs címzettje sem értelmezheti azt úgy, mint a parancsadó személyes elvárását/akaratát. E körülményből következik a második jellemző, hogy a parancsot teljesíteni kell, annak kötelező jellege független attól, hogy a címzett mit gondol a parancsról. A parancsok esetében a *„racionális-morális"* értelemben vett *„rossz"* parancsot is kötelező teljesíteni bizonyos feltételek mellett.[38]

A parancs harmadik – a két lexikon meghatározásában is fellelhető – jellemzője, hogy az kizárólag a hierarchikus, alá-fölérendeltségi viszonyrendszerek között értelmezhető. Negyedik ismérve pedig az, hogy a kiadott parancs teljesítése erkölcsileg indokolt. A két utóbbi jellemvonás szervesen

[36] Hadtudományi Lexikon – új kötet. Dialóg Campus. Budapest. 2019. 875. o.
[37] Hart, Herbert L. A.: Commands and Authoritative Legal Reasons. In: Essays on Bentham. OUP. Oxford, 1982. 252. o.
[38] Boda Mihály: Az akarattól a tettig: a parancsteljesítés erkölcsi szerkezete. Hadtudomány 2016/26. szám. 26. o.

épül egymásra, mivel a katonai jellegű hierarchiának nem kizárólag a magasabb rendfokozaton vagy beosztáson alapuló fizikai jellegűnek minősülő keretei vannak, hanem a vezető/parancsnok olyan erkölcsi keretekkel is rendelkezik vagy kell, hogy rendelkezzen, amelyek indokolják, megalapozzák a feljebbvaló parancsa teljesítésének erkölcsi alapjait. Ez azt jelenti, hogy a beosztott, illetve alárendelt katonának minden esetben van erkölcsi indoka arra, hogy feljebbvalója parancsát teljesítse.[39]

A rendvédelmi szervek – köztük a rendőrség – állománya a posztmodern kor katonáinak tekinthető.[40] E vonatkozásban az egyik fő eltérés a korábbi, modern kori hadseregekhez képest, hogy a posztmodern kor katonája önkéntes katona, ezáltal a közösségi (a katonai) tagság kritériumai között a szervezethez kapcsolódó személyes értékek és érdekek felértékelődnek, és gyakran legalább olyan fontosak, mint a közösségi értékek és ezen érdekeken alapuló indokok,[41] mivel elsődlegesen a tagok számára a maguk által választott értékek (önérdekek) indokolják a katonai szervezetbe történt belépést.[42]

Meg kell említeni, hogy a katonai jellegű szervezetnél a parancs mögötti fenyegetésre is figyelemmel kell lenni annak kiadásakor és végrehajtásakor egyaránt.[43] E fenyegetés két szinten jelentkezhet. Az egyik a büntetőeljárástól való félelem a parancs iránti engedetlenség kapcsán, amely mind jogszerű, mind a jogellenes parancs esetében „kimutatható". E körülményt értékeli/értékelheti a bíróság, amikor enyhítő körülményként veszi figye-

[39] Wolff, Robert Paul: The Conflict between Authority and Autonomy. In: Joseph Raz (szerk.): Authority, Basil Blackwell. 1990. 20. o.
[40] Moskos, Charles C.: A posztmodern haderő felé: az Egyesült Államok, mint paradigma. In: Tálas Péter (szerk.): Civil-katonai kapcsolatok: a tudományok határán. Zrínyi Kiadó. Budapest, 2006. 62-63. o.
[41] Gabriel, Richard A.: The Warriors Way – A Treatise in Military Ethics. Canadian Defense Academy Press. Kingstone, 2007. 84. o.
[42] Moskos: i.m. 113-117. o.
[43] Hautzinger Zoltán: A katonai büntetőjog rendszere, a katonai büntetőeljárás fejlesztési lehetőségei. Doktori PhD értekezés. Pécsi Tudományegyetem Állam- és Jogtudományi Kar Doktori Iskola. 2010. 113. o.

lembe a parancsra történt elkövetést. A másik szinten megmutatkozó, a parancs végrehajtása általi fenyegetés olyan jellegű és/vagy mértékű, amely képtelenné teszi az alárendeltet annak teljesítésére, ezért a végrehajtást megtagadja. Ez esetben a kényszer vagy fenyegetés a felelősséget kizáró, korlátozó körülményként jelenhet meg.[44]

A katonai büntetőeljárás rendszere

A korábban taglaltak alapján a parancs a katonai jellegű szervezetek – így a rendőrség – működésének elengedhetetlen feltétele, amelyre tekintettel annak jogszerűtlen megtagadása esetén büntetőjogi eszközökkel is biztosított a védelme. A téma vizsgálata során megítélésem szerint a katonai büntetőeljárások rendszerének – legalább érintőleges – bemutatása elengedhetetlen.

A paranccsal szembeni ellenszegülés, vagyis a parancs iránti engedetlenség katonai bűncselekmény[45], amely a hivatásos állományba tartozó elkövetővel szemben speciális elmarasztalási és szankcionálási szabályokat, valamint egyedi, a szolgálati jogviszonyból eredő sajátosságokra épülő igazságszolgáltatási eljárási rendet követel meg[46]. Ezen szabályozás elsődleges célja a katonai rend és fegyelem fenntartása, a szabályrendszer – vagyis a katonai büntetőeljárás rendszere – a „civil" életben/világban ismeretlen, értelmezhetetlen, és annak megléte indokolatlannak (is) tűnhet/tűnik.

A katonai büntetőeljárások rendszere – figyelemmel a katonai rend és fegyelem, vagyis a szervezet rendeltetésszerű működése fenntartásának igényére, továbbá a különös alany meglétére és személyiségi jogaira[47] –

[44] Sántha Ferenc: Az elöljáró parancsa, mint büntethetőségi akadály a magyar büntetőjogban. Miskolci Egyetemi Jogi Közlemények 2014/22. szám. 319. o.
[45] Btk. 444. §
[46] Fejes Erik: Emlékkötet dr. Kovács Tamás (1940-2020) altábornagy legfőbb ügyész tiszteletére. Magyar Katonai Jogi és Hadijogi Társaság. Budapest. 2023. 127. o.
[47] Fővárosi Ítélőtábla Katonai Tanácsa 6.Kbf.38/20l7/10.

elkülönül a köztörvényes bűncselekményekétől. A katonai büntetőeljárások egyediségét alapvetően az a körülmény alapozza meg, miszerint katonai bűncselekményt tettesként kizárólag katona követhet el, e vonatkozásban a rendőrség esetében kizárólag a hivatásos állomány tagja minősül katonának.[48] Az elkövetés szempontjából lényeges, hogy a büntethetőség nem kizárólagosan a ténylegesen állományban lévőkre vonatkozik, mivel katonai bűncselekmény miatt a hivatásos szolgálati jogviszony megszűnését követő egy éven belül (még) büntethető az elkövető.[49] A rendőrség egyéb állománycsoportjaiba tartozók büntetőjogi értelmezésben nem tekinthetőek katonának, ezáltal – önállóan – katonai bűncselekményt nem követhetnek el.

Fegyelmi szakterületi tapasztalataim alapján gyakran téves az értelmezése a *„katona”* fogalmának. A magas szolgálati beosztást betöltő, viszont nem hivatásos állományba tartozó rendőri vezető normaszegéseit téves a katonai büntetőeljárás hatálya alá tartozó cselekményként értelmezni. A *„nem katonák”* által megvalósított/elkövetett, a szolgálati rend és fegyelem sérelmét okozó magatartások elsődlegesen fegyelmi intézkedést vonnak maguk után, illetve köztörvényes bűncselekmény gyanúját alapozhatják meg, függetlenül az elkövető katonai rendszerben betöltött beosztásától és a szolgálati hierarchiában elfoglalt helyétől.[50]

A katonai büntetőeljárások szabályrendszerének az általános büntetőeljárási szabályoktól történő elkülönülése nem teljes körű, mivel a katonai büntetőjog az egyedi vonásai és szabályrendszere ellenére alapvetően az általános büntetőjog része. Az elkülönült szabályrendszert az a körülmény indokolja, miszerint a katonai szervezetek különleges szakmai és feladatvégrehajtási körülmények között elkövetett, a máshol nem megvalósuló normaszegő magatartások kapcsán is érvényesíteni lehessen a büntetőjogi elveket.

[48] Btk. 127. § (1)–(3) bekezdése
[49] Btk. 131. §
[50] Kardos Sándor István: Kizárólag a katonai vétségek elbírálása utalható fegyelmi jogkörbe? Katonai Jogi és Hadijogi Szemle 2024/2. szám. 71. o.

A sajátos katonai-szolgálati viszonyok ugyanis önálló bűncselekményi tényállás megalkotását követelték meg, továbbá szükségessé tették bizonyos rendelkezések felvételét, illetve azt is, hogy e rendelkezések kikre vonatkoznak. Ezen túlmenően a sajátos jogintézmény meglétét a speciális katonai büntetések/elmarasztalások céljai kapcsán megfogalmazódó érdekek is indokolják.[51] A katonai büntetőeljárás rendszere kizárólag olyan mértékben tér el, különül el az általános büntetőjogtól, *„amennyiben azt a különleges katonai viszonyok és érdekek valóban megkövetelik”*.[52]

A bűncselekmény megvalósulásának meghatározó kérdése az is, hogy egy adott szolgálati feladatot végrehajtó személy munkája/tevékenysége beletartozik-e a védett (szolgálati) formák fogalomkörébe. A katonai magatartások esetében gyakran nehézséget jelent, illetve nem mindig egyszerű meghatározni a védett szolgálatokat.[53]

A katonai bűncselekmény megvalósulása szempontjából azt is értékelni, kell, hogy a magatartás a katonai (rendőri) rend rendelkezéseit milyen mértékben sértette. Ugyancsak a bírói/bírósági gyakorlat alakította ki azon elkövetési módokat és formákat, amelyek a katonai szolgálat ellátására vonatkozó rendelkezések súlyos megszegését alapozzák meg, vagyis amelyek a szolgálatra vagy a fegyelemre jelentős hátrány veszélyével járnak. E körbe leginkább olyan magatartások tartoznak, amelyek – az egyes katonai bűncselekményeknél, például a szolgálatban kötelességszegés esetén – a törvényben konkrétan megfogalmazott/leírt, és abban a viszonyrendszerben súlyosnak értékelt elkövetési magatartásokkal azonos sérelmet idéznek elő a feladatellátásra, vagy amelyek konkrétan meghiúsítják a szolgálat ellátását. A katonai bűncselekmény által megvalósuló súlyos kötelességszegés tárgyi súlya legalább olyan fokú, illetve mértékű kell, hogy legyen, mint például a szolgálatban történt elalvás, italfogyasztás, kábítószer-használat, illetve a

[51] Korda: i.m. 8. o.

[52] Schulteisz Emil: A katonai büntetőtörvény (1930. évi II. törvénycikk) magyarázata. Általános rész. In: Fejes Erik (szerk.): Schultheisz Emil katonai büntetőjogi értekezései. Magyar Katonai Jogi és Hadijogi Társaság. Budapest, 2018. 39. o.

[53] Madai Sándor: A kötelességszegés szolgálatban bűncselekmény alapkérdése. Katonai Jogi és Hadijogi Szemle 2023/1. szám. 29-45. o.

rendeltetési/felállítási hely engedély nélküli elhagyása. További fontos körülmény, hogy ezen magatartások kizárólag szándékosan követhetők el.

Katonai büntetőeljárásban – ha a nyomozást nem az ügyész végzi – az eljárni jogosult rendőri vezető – az állományából kijelölt nyomozótiszt megbízásával – parancsnoki nyomozást folytat. Az eljárás különös szabályait norma tartalmazza.[54] A normaháttér lehetőséget biztosít arra is, hogy a katonai vétségek – bizonyos feltételek fennállása esetén – ne büntetőeljárás keretében, hanem fegyelmi jogkörbe utalással kerüljenek elbírálásra. E feltételek a joggyakorlat szerint: egyszeri ténybeli megítélés, a cselekmény csekély tárgyi súlya, ténybeli beismerés, vezetői vagy ügyészi szándék és döntés a fegyelmi jogkörbe utalásra.[55]

A magatartások fegyelmi jogkörbe utalását az alapozza meg, hogy amennyiben a megvalósított katonai vétség miatti büntetés célja fegyelmi fenyítéssel is elérhető, akkor az eljárást a cselekmény elbírálása érdekében az ügyész a parancsnok hatáskörébe utalhatja.

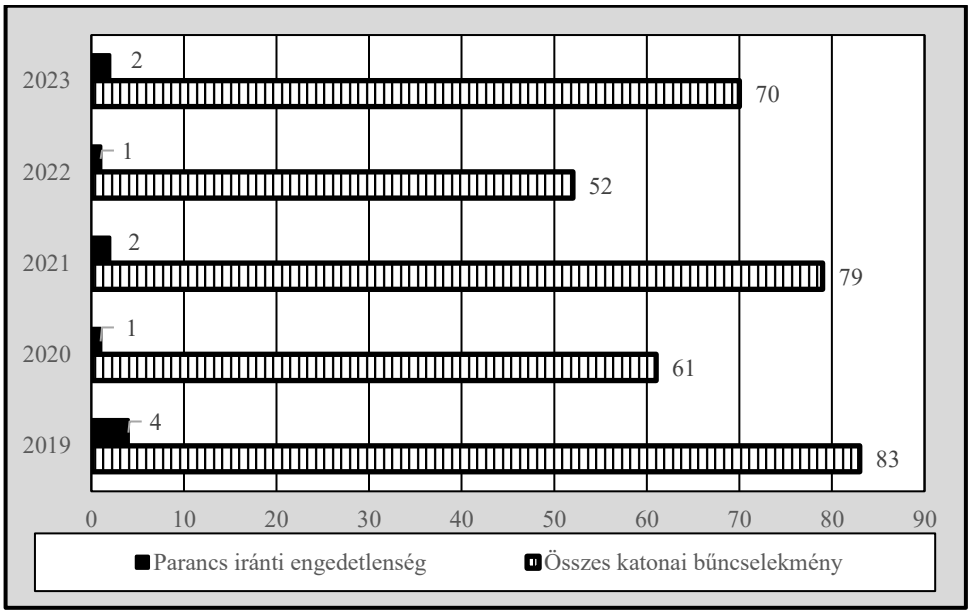
A parancsnok a számára biztosított fegyelmi jogkör alapján folytatja le az eljárást,[56] vagyis az elkövetett cselekmény nem büntetőeljárásban, hanem fegyelmi eljárás keretében – a munkáltatói intézkedések rendszerében – kerül elbírálásra. A fegyelmi jogkörbe visszautalt katonai eljárásokban ezáltal nem büntető ítélet születik, hanem fegyelmi fenyítés kiszabására nyílik lehetőség, amely révén markánsabban érvényesíthető a fegyelmi jogkör gyakorlójának szankcionálási lehetősége, s e körülmény jelentős visszatartó erőt generál(hat) az állomány körében.

A katonai bűncselekmények között a parancs iránti engedetlenség bűncselekmény (vétségi és bűntetti alakzat) évenkénti elkövetési száma csekélynek értékelhető (5 év alatt összesen 10 fő részesült elmarasztalásban), amely adatokat az 1. számú ábra tartalmazza. A 10 fő elkövetőből 1 fő

[54] A belügyminiszter irányítása alatt álló rendvédelmi feladatokat ellátó szervek parancsnoki nyomozásának különös szabályairól szóló 11/2018. (V. 30.) BM rendelet
[55] A büntetőeljárásról szóló 2017. évi XC. törvény 710. § (1) bekezdés
[56] A belügyminiszter irányítása alatt álló fegyveres szervek hivatásos állományú tagjai Fegyelmi Szabályzatáról szóló 11/2006. (III. 14.) BM rendelet 37. §

megrovásban részesült, 3 fő próbára bocsátást, 3 fő pénzfőbüntetést mellékbüntetés nélkül, 3 fő pénzfőbüntetést rendfokozatot érintő mellékbüntetéssel kapott. A vizsgálat tárgyát képező bűncselekmények fegyelmi jogkörben elbírált számáról statisztika nem áll rendelkezésre. A parancs iránti engedetlenség vétség elkövetése miatt indult és fegyelmi jogkörbe utalt eljárások az ügyészség általi feljelentés elutasítását vagy az eljárás megszüntetését követően kerülnek a fegyelmi jogkör gyakorlója által elbírálásra.[57] A visszautalt eljárás a katonai vétség tárgyában, de kizárólag (már csak) a fegyelemsértés elkövetése miatt folyik[58], amelyre tekintettel a fegyelmi statisztikában[59] fegyelemsértésként jelennek meg az eset adatai, annak büntetőjogi előzménye nem képezi a statisztika részét.

[57] Be. 710 § (1) és (2) bekezdései
[58] Hszt. 181. § (3) és (4) bekezdései
[59] A fegyelemkezelő adatállománnyal kapcsolatos feladatokról szóló 11/2013. (III. 29.) ORFK utasítás



1. számú ábra
Az összes katonai bűncselekmény, valamint a parancs iránti engedetlenség miatt alkalmazott jogerős elmarasztalások száma 2019-ben és 2023-ban (a rendőrség hivatásos állománya körében)[60]

A parancs iránti engedetlenség bűncselekmény számszaki megjelenésén – megítélésem szerint – lényegesen túlmutat a magatartás jelentős tárgyi súlya, valamint annak negatív hatása a szolgálati rendre, illetve a rendőri szervezet fegyelmének fenntartására. Akár egy esetben megvalósuló szándékos parancsmegtagadás az éves statisztikai számok nagyságától függetlenül is teljes mértékben alkalmas arra – fegyelmi-szakmai álláspontom, valamint a gyakorlati tapasztalatok alapján –, hogy aláássa, rombolja a konkrét bűncselekménnyel érintett vezető parancsnoki és általános emberi tekintélyét az állomány előtt, és ezáltal rombolja az általános fegyelmi helyzetet.

[60] A publikáció elkészítésekor a 2024. évi fegyelmi statisztika már rendelkezésre állt, az viszont még nem volt kutatható. Forrás: ORFK Fegyelmi Osztály statisztikai adatai.

A parancs iránti engedetlenség elkövetési/megvalósulási körülményeinek vizsgálata és a konkrét jogesetek értékelése

A hatályos Büntető Törvénykönyv 444. §-a rendelkezik a parancs iránti engedetlenségről.[61] A bűncselekmény jogi tárgya a parancs, illetve a parancsadás joga. A katonai jellegű szervezet szolgálati rendjének és fegyelmének meghatározó összetevője, alapja a parancs teljesítéséhez fűződő érdek.

A parancs fogalmát nem találjuk meg a Btk. értelmező rendelkezései között, azonban a Btk. indokolása szerint: *„a parancs meghatározott tevékenység vagy feladat végrehajtására vonatkozó egyedi utasítás."*[62] A megfogalmazás önmagában nem ad teljeskörű értelmezést a parancs mibenlétéhez, a fogalom meghatározásához és konkrét értelmezéséhez szükséges a szervezeti/ágazati törvények, utasítások értelmezése, amelyekkel a komplex fogalmat meg tudjuk határozni. Ez alapvetően azt jelenti, hogy akkor nevezhető/értékelhető/minősíthető egy elöljárói utasítás parancsnak, amennyiben az a katonai szervezet működését szabályozó normaháttér alapján határoz meg kötelezettséget a parancsot kapó katona részére.

A törvény nem minden szolgálati kötelem megszegését rendeli a katonai büntetőjog keretei közé, hanem kizárólag azokat, amelyek megvalósítása

---

[61] Parancs iránti engedetlenség – Btk. 444. § (1) bekezdés: *„Aki a parancsot nem teljesíti, vétség miatt elzárással büntetendő. (2) bekezdés: Ha a parancs iránti engedetlenséget csoportosan követik el, a büntetés két évig terjedő szabadságvesztés. (3) bekezdés: A büntetés bűntett miatt három évig terjedő szabadságvesztés, ha a parancs iránti engedetlenség a) más alárendeltek jelenlétében vagy egyébként nyilvánosan, akár a parancs teljesítésének kifejezett megtagadásával, akár egyéb sértő módon történik, b) a szolgálatra vagy a fegyelemre jelentős hátrány veszélyével jár. (4) bekezdés: A büntetés egy évtől öt évig terjedő szabadságvesztés, ha a (3) bekezdésben meghatározott bűncselekményt háború idején követik el. (5) bekezdés: Aki háborúban a harci parancsot, külföldi hadműveleti területen végzett humanitárius tevékenység vagy békefenntartás során a fegyverhasználatra vonatkozó parancsot nem teljesíti, öt évtől tizenöt évig terjedő szabadságvesztéssel büntetendő."*

[62] Indokolás a Büntető Törvénykönyvről szóló 2012. évi C. törvény módosításáról szóló 2024. évi LXVIII. törvényhez

során a végrehajtásra utasított katona önálló, egyedileg meghatározott feladatot lát el, és a kötelmek megszegése komoly (negatív) kihatással lehet a katonai jellegű szervezet rendjére és fegyelmére, feladatai megvalósításának eredményességére. Mivel a szolgálati előírás e szervezeteknél más és más lehet, ezért az elkövető általi bűnelkövetés tartalmát a rá (elkövetőre) és az általa teljesített konkrét szolgálatra vonatkozóan kiadott normák, szabályok, szabályozók, utasítások határozzák meg, vagyis kizárólag az azokban leírtak megszegése révén valósul meg a bűncselekmény.[63]

– Nem valósította meg a parancs iránti engedetlenség bűncselekményét az a hivatásos állományú, tiszti rendfokozati állománycsoportba tartozó rendőr, aki az általa folytatott nyomozásokban az ügyészi átiratokban jelzett, valamint a vezetői utasításokban/elvárásokban megfogalmazott hiányosságok pótlását osztályvezetői utasításra nem kezdte meg. Az elöljáró által szóban meghatározott ügyfeldolgozásra kötelezés ugyanis nem egy konkrét nyomozásra és nem meghatározott eljárási cselekményekre terjedt ki, továbbá végrehajtási határidő sem került elrendelésre, hanem általános, a belső szabályozókban is rögzített munkavégzésre szólt az utasítás. Mivel a parancs fogalmába nem tartoznak bele a normákban, szabályzatokban foglalt általános (belső) előírások, az azokban foglalt kötelmek megszegése abban az esetben is csupán fegyelemsértés, ha az elöljáró külön is felhívja a beosztott figyelmét a szabályok betartására. Ezáltal az elkövető esetbeli szándékos mulasztása, vagyis a feladat végrehajtásának megtagadása – kizárólag – fegyelemsértés megalapozott gyanújának megállapítására volt alkalmas. A fegyelmi eljárás elmarasztalással zárult.[64]

[63] Korda: i.m. 63. o.
[64] Budapesti Rendőr-főkapitányság 01140-103/1-4/2023. Fe.

Nem értelmezhetőek a parancs fogalmaként a szabályokban, normákban, jogszabályokban foglalt általános előírások. Ez alapján a szabályozók megszegése kizárólag fegyelmi vétség megállapítására alkalmas, abban az esetben is, ha az elöljáró azok betartására külön is felhívta a beosztott figyelmét.

– Nem valósította meg a parancs iránti engedetlenség bűncselekményét az a hivatásos állományú, főtiszti rendfokozati állománycsoportba tartozó rendőr, aki a rendőrségi objektumba történő belépést rögzítő mágneskártyát minden esetben használta, viszont – többszöri parancsnoki felszólítás ellenére – egy másik, a konkrét szolgálati helyre történt belépést regisztráló mágneskártya használatát megtagadta. A kártyahasználat elmulasztását azzal indokolta, hogy a két beléptetést túlszabályzásnak értékelte, és mivel a második beléptető rendszer technikailag fejletlen, ezáltal nem alkalmas reális érkezési/távozási adatok rögzítésére. Az elkövető a számára belső normában meghatározott kötelmet esetbeli magatartásával szándékosan, nyíltan és véglegesen megtagadta. Mivel az érintett nem a szolgálatteljesítést érdemben érintő parancsot tagadott meg, hanem a munkaidő-nyilvántartáshoz szükséges „járulékos jellegű" kötelezettségét nem hajtotta végre, illetve a belépés, mint tevékenység nem kapcsolódott az érintett rendőri szolgálati feladatokhoz, ezért a feladatot megtagadó szándékosan, a napi kötelmek súlyos mértékű megszegésével megvalósított magatartása kizárólag fegyelemsértés megalapozott gyanújának megállapítására volt alkalmas. Mindezekre tekintettel annak ellenére sem valósult meg a parancs iránti engedetlenség bűncselekmény, hogy az elkövető több alkalommal, következetesen, a jövőre nézve is megtagadta a belépésre/beléptetésre vonatkozó utasítás/parancs végrehajtását. A fegyelmi eljárás elmarasztalással zárult.[65]

[65] Kúria Mfv.II.10.218/2019/3.

Amennyiben a parancs végrehajtását megtagadó személy a részére kiadott feladatot a kijelentésben megnyilvánuló megtagadást követően mégis időben teljesíti, cselekménye csupán szolgálati tekintély megsértésének minősül, mivel a normaháttér elsődlegesen a szolgálati elöljáró akaratának megvalósulásához fűződő érdeket védelmezi, és ezen esetekben legnagyobb mértékben a parancs kiadójának tekintélye sérül.

– Nem parancs iránti engedetlenségnek, hanem a szolgálati tekintély megsértésének vétségét[66] valósította meg az a hivatásos állományú, tiszthelyettesi rendfokozati állománycsoportba tartozó honvéd, aki szolgálati elöljárójának a munkavégzésre vonatkozó utasítását először megtagadta, azonban később, de még a megszabott határidőn belül végrehajtotta azt, a meghatározott feladatot elvégezte.[67]

A parancs a szolgálat irányításának alapvető eszköze a katonai viszonyok között a szolgálat érdekében, illetve az elöljáró parancsot adni jogosult és egyben köteles is, az alárendelt pedig a parancs teljesítésére kötelezett. A parancs alatt minden esetben a szolgálati parancs értendő, tartalmilag a parancs a szolgálattal kapcsolatos tevékenységre, vagy az azzal kapcsolatos, illetve az attól való tartózkodásra irányul, azt mindig meghatározott személyhez vagy személyekhez kell intézni. Vagyis „a *parancs nem más, mint a jogszabályban arra felhatalmazott, parancsadási joggal rendelkező személytől származó, speciális katonai vezetési, illetve irányítási eszköz, amely kifejezi a parancsot adó akaratát, megfelel a jogszabályoknak és egyéb rendelkezéseknek, konkrét, egyértelmű és reális, valamilyen cselekvésre, cselekvéstől való tartózkodásra, vagy megfelelő magatartás*

[66] Btk. 447. § Szolgálati tekintély megsértése: Aki az elöljáró, a szolgálatát teljesítő feljebbvaló, őr vagy más szolgálati közeg tekintélyét más előtt vagy feltűnően durván megsérti, vétség miatt egy évig terjedő szabadságvesztéssel büntetendő. A büntetés bűntett miatt három évig terjedő szabadságvesztés, ha a bűncselekményt több katona előtt vagy egyébként nyilvánosan követik el.
[67] Legfelsőbb Bíróság Katf. I.301/1988

tanúsítására szólítja fel a katonának minősülő személyt vagy katonáknak minősülő személyek egy csoportját."[68]

– Parancs iránti engedetlenség vétségét valósította meg az a hivatásos állományú, tiszthelyettesi rendfokozati állománycsoportba tartozó rendőr, aki a szolgálatát azért nem volt hajlandó ellátni, mert kijelentette, hogy egy vallási felekezet tagja, amely elutasítja az erőszakot, ezzel együtt a fegyver viselését és használatát is. A katonai büntetőeljárás lezárása: a büntetőeljárás megszüntetése a felelősség megállapítása mellett, ügyészi megrovás alkalmazása.[69]

A parancsot nem csak szóban, hanem írásban vagy jelzéssel is adhatják. A parancsnak minden esetben érthetőnek, világosnak és egyértelműnek kell lennie, hogy az érintett az utasítást értelmezni, felfogni, ezáltal teljesíteni tudja. Ebből következik, hogy nem lehet parancsot adni annak a katonának, aki (aktuális) állapota miatt nem képes felfogni vagy végrehajtani azt. A bírói gyakorlat szerint ilyen állapot lehet a bódult vagy ittas állapot, amely kapcsán a befolyásoltság mértékét orvosszakértő bevonásával kell tisztázni az eljárások keretében.

A leírtakra figyelemmel elengedhetetlen, hogy a parancsot adó elöljárónak minden esetben meg kell győződnie arról, hogy a beosztott/alárendelt a kiadott parancsot megértette-e. A beosztott/alárendelt az alaki szabályok szerint a parancs elhangzását követően az *„Értettem!"* kifejezést használja, amellyel a számára adott parancs megértését jelzi. Amennyiben a parancsot adó elöljárónak kételye merülne fel e vonatkozásban, kérheti az alárendeltet, hogy a parancs lényegét ismételje meg. E vonatkozásban a Szolgálati Szabályzat is egyértelműen rendelkezik.[70]

---

[68] Görbe Boldizsár: A parancsra cselekvés büntetőjogi szabályozása. Szegedi Tudományegyetem Állam- és Jogtudományi Kar. Jogi Fórum, Szeged, 2019. 7. o.
[69] Szegedi Regionális Nyomozó Ügyészség 6. Nyom. 315/2021.
[70] Szolgálati Szabályzat 90 § (3) bekezdés: *„a rendőr az utasítás tudomásulvételét „Értettem!" szóval jelenti. Indokolt esetben a szolgálati elöljáró köteles meggyőződni arról,*

– A számukra kiadott utasítás egyértelmű megértése mellett, azt figyelmen kívül hagyva valósították meg a parancs iránti engedetlenség vétségét azok a hivatásos állományú, zászlósi, illetve tiszthelyettesi rendfokozati állománycsoportba tartozó rendőrök, akik egy előállított polgári személy dohányzóhelyre történő kísérése során a vonatkozó szabályzókat figyelmen kívül hagyva elmulasztották bilincs és vezetőszíj használatát. Mulasztásuk következtében az előállított személy a helyszínről elfutott, őt később elfogták. A katonai büntetőeljárás lezárása: pénzbüntetés mellékbüntetés nélkül.[71]

A jogszabályi háttér a szolgálati parancsot büntetőjogi védelemben részesíti. A parancsot kizárólag az arra jogosult szolgálati elöljáró/feljebbvaló adhatja ki, aki a meghatározott jogkörben más katonák felett rendelkezni jogosult, és így a függelemsértés passzív alanyaivá válhat. Elkövetőként aktív alanyok azok a katonák, akik az elöljáró parancsainak engedelmeskedni kötelesek. Hangsúlyozni kell e vonatkozásban, hogy a feljebbvaló a szolgálat szempontjából a neki alá nem rendelt katonák vonatkozásában nem elöljáró, így általában nincs az érintettek felett rendelkezési joga, az alárendeltek tiszteletadási kötelezettséggel tartoznak irányába, ezáltal az e vonatkozásban hozott intézkedéseik minősülnek elöljárói parancsnak, valamint a szakterületére vonatkozó utasítások. Ebből következik, hogy a parancs megtagadása esetén a bűnösség megállapítása szempontjából nem lehet különbséget tenni, hogy elöljáró vagy feljebbvaló volt a parancs kiadója. A büntetés kiszabásánál lehet jelentősége annak, hogy milyen hatással volt az ellenszegülés a katonai szervezet rendjére és fegyelmére.

hogy az alárendelt pontosan megértette az utasítást. A távbeszélőn adott utasítás jogosultságáról kétség esetén visszahívással kell meggyőződni."

[71] Fővárosi Törvényszék Katonai Tanácsa 43.Kb.113/2018/9.

A parancs iránti engedetlenség alapvetően kétféle elkövetési magatartással valósulhat meg: mulasztással, illetve megtagadással. Mulasztás esetén a katona (egyszerűen) nem hajtja végre a kapott utasítást, illetve olyan magatartást tanúsít, amelyet az elöljáró tilalmaz, vagy valamilyen módon eltér a kapott parancstól, illetve olyan módon teljesíti késedelmesen, amely következtében a parancsban elérni kívánt cél már nem valósul, nem valósítható meg.

– Mulasztással valósította meg a parancs iránti engedetlenség vétségét az a hivatásos állományú, tiszthelyettesi rendfokozati állománycsoportba tartozó rendőr, akit elöljárója konkrét időpontra berendelt szolgálati feladat kapcsán, viszont az érintett az utasítás ellenére azért nem jelent meg, mivel a szolgálatvezénylést figyelmetlenül tekintette meg. Hanyagsága révén nem észlelte a számára meghatározott megjelenési kötelezettséget, valamint annak időpontját a rendszerben, ezért az utasítás ellenére a meghatározott helyen és időben nem jelent meg, és e körülmények alapján előzetesen nem is jelezte, hogy az utasításnak nem tud eleget tenni. A katonai büntetőeljárás lezárása: próbára bocsátás.[72]

A másik elkövetési magatartás, a parancs kifejezett megtagadása akkor állapítható meg, amikor annak nem teljesítéséhez olyan magatartás járul hozzá, amellyel az alárendelt az engedetlenségnek külön nyomatékot (is) ad, illetve a nem teljesítésre vonatkozó/irányuló szándékát harmadik személy által is felismerhetően juttatja kifejezésre. E magatartás nem kizárólag szóban, hanem egyéb olyan ráutaló magatartásokkal is történhet, amelyekkel az elkövető világosan kifejezi a vezetői/elöljárói akarattal ellentétes szándékát.

[72] Győri Törvényszék Katonai Tanácsa Kb.I.1/2019/9.

- Szándékosan valósította meg a parancs iránti engedetlenség vétségét az a hivatásos állományú, tiszthelyettesi rendfokozati állománycsoportba tartozó rendőr, akit az alosztályvezető arra utasított, hogy egy ügyben készítsen átiratot a bíróság részére, amelyet – többszöri elöljárói felszólítás ellenére is – azért tagadott meg, mivel megítélése szerint az ügyben kizárólag jelentés készítése volt a feladata, más tevékenység nem. Nevezett az átirat készítésére vonatkozó elöljárói utasítást megtagadta, a meghatározottakat nem hajtotta végre. A katonai büntetőeljárás lezárása: pénzbüntetés mellékbüntetés nélkül.[73]
- Szándékosan valósította meg a parancs iránti engedetlenség vétségét az a hivatásos állományú, zászlósi rendfokozati állománycsoportba tartozó rendőr, aki a szolgálatirányító parancsnok többszöri felszólítására sem készített jelentést a rendőri intézkedésről. Az elkövető arra hivatkozással tagadta meg a parancsot, hogy az intézkedést nem egyedül foganatosította, ezért javasolta, hogy a járőrtársa írja meg a jelentést. Nevezett ismételt elöljárói utasítás ellenére sem készítette el a jelentést. A katonai büntetőeljárás lezárása: próbára bocsátás.[74]
- Szándékosan valósította meg a parancs iránti engedetlenség vétségét az a hivatásos állományú, tiszti rendfokozati állománycsoportba tartozó rendőr, aki az osztályvezető-helyettes utasítása ellenére nem végzett munkát konkrét, a vezető által megnevezett polgári személy kérelme kapcsán. Az elkövető arra hivatkozva tagadta meg a feladatot, hogy a polgári személy ügyfélfogadási időn kívül érkezett, és a rendőr-szakmai feladat elvégzése kizárólag ügyfélfogadási időben történik. A vezetői utasítást egyáltalán nem hajtotta végre, azt végérvényesen megtagadta. A katonai büntetőeljárás lezárása: pénzbüntetés rendfokozatban visszavetés mellékbüntetéssel.[75]

[73] Debreceni Törvényszék Katonai Tanácsa Kbk.II.12/2018/2.
[74] Győri Törvényszék Katonai Tanácsa Kbk.I.4/2023/2.
[75] Fővárosi Ítélőtábla 6.Kbf.24/2020/8.

– Szándékosan valósította meg a parancs iránti engedetlenség vétségét az a hivatásos állományú, tiszthelyettesi rendfokozati állománycsoportba tartozó rendőr, akit az alosztályvezető utasította arra, hogy egy polgári személy elfogásáról készítsen jelentést, de azt megtagadta arra hivatkozással, hogy nem ő, hanem a járőrtársa bilincselte meg az érintett személyt. A katonai büntetőeljárás lezárása: pénzbüntetés mellékbüntetés nélkül.[76]

Minősített esetekként szerepelnek a büntetőjogban, amikor a parancs iránti engedetlenséget csoportosan (legalább három személy vesz részt az elkövetésben), illetve más alárendeltek jelenlétében, vagy nyilvánosan, illetve a parancs teljesítésének kifejezett megtagadásával, akár egyéb sértő módon történik az ellenszegülés. Szintén minősített eset, amikor a parancsmegtagadás a katonai szolgálatra vagy a szervezet fegyelmére jelentős hátránnyal jár, vagy az elkövetés háborús körülmények között történik.

– Több alárendelt jelenlétében valósította meg a parancs iránti engedetlenség bűntettét az a hivatásos állományú, zászlósi rendfokozati állománycsoportba tartozó rendőr, akinek a szolgálatirányító parancsnok meghatározta, hogy intézkedésével kapcsolatban készítsen kiegészítő feljegyzést, de azt több beosztott előtt megtagadta. Az elkövető több alkalommal, többszöri felszólításra is azt jelentette ki, hogy nem fog még külön iratot készíteni, és úgy nyilatkozott a többi beosztott jelenlétében az utasítást kiadó elöljárónak, hogy őt nem érdekli az egész szervezet, határozottan megtagadta a végrehajtást. A magatartás a szolgálatra jelentős hátránnyal járt. A katonai büntetőeljárás lezárása: pénzbüntetés rendfokozati várakozási idő meghosszabbítása mellékbüntetéssel.[77]

[76] Kaposvári Törvényszék Katonai Tanácsa Kbpk.I.4/2021/4.
[77] Debreceni Törvényszék Katonai Tanácsa Kb.III.2/2019/5.

Csoportos elkövetésnél a jelenlévők vonatkozásában lényeges körülmény, hogy a parancs kiadója a szolgálati vagy a szakmai elöljáró legyen. Ebben az esetben a bűncselekmény azért minősül súlyosabban, mert a parancs kiadójának tekintélyét más alárendeltjei előtt is sérti. Az „egyéb sértő módon" történő elkövetés (általában) akkor valósul meg, amikor a parancs címzettje az azt kiadó távollétében, de annak alárendeltjei előtt tanúsít olyan engedetlenséget, amely feltűnően és durván sérti a parancsot kiadó elöljáró tekintélyét.

A parancsmegtagadás szolgálatra vagy fegyelemre gyakorolt jelentős hátránya, illetve annak veszélye általában akkor jelenik meg, amikor a kiadott parancs a katonai szervezet alapvető feladataira vagy alapvető tevékenységének végzésére irányult, és a vele szembeni ellenszegülés megteremti a (katonai) szolgálatra jelentős hátrány bekövetkezésének a lehetőségét. Szintén megállapítható a súlyosabb minősítés, amennyiben az engedetlenség előidézi annak a veszélyét, hogy az elöljáró parancsban kinyilvánított akaratával szembeni megnyilatkozást mások is példaként követhetik.

– A szolgálatra jelentős hátrányt gyakorolva valósította meg a parancs iránti engedetlenség bűntettét az a hivatásos állományú, zászlósi rendfokozati állománycsoportba tartozó rendőr, aki munkavégzésre történt berendelés és többszöri elöljárói felszólítás ellenére nem készített feljelentést egy korábbi intézkedése kapcsán. Az utasítást két egymást követő napon sem teljesítette, egyéb szolgálati feladataira hivatkozva. A katonai büntetőeljárás lezárása: pénzbüntetés rendfokozatban visszavetés mellékbüntetéssel.[78]

Összegzés

Vizsgálatom révén bemutattam, hogy a hivatásos állományú rendőrök esetében nem minden parancsmegtagadás minősül bűncselekménynek, illetve, amennyiben az értékelt magatartás bűncselekmény megalapozott gyanúját

[78] Fővárosi Ítélőtábla Katonai Tanácsa 6.Kbf.15/2023.

kelti, nem minden esetben a parancs iránti engedetlenség a pontos és szakszerű büntetőjogi minősítés. Ennek legfőbb oka, hogy a vezetői/elöljárói parancs végrehajtásának elmulasztása számtalan körülmény által befolyásolt magatartás: alapvetően a konkrétan ellátott szolgálati feladat jellege, a parancs kiadásának módja, a végrehajtás elmulasztásának körülményei, a cselekmény szolgálatra gyakorolt hatása, az elkövető akarata/szándéka szerint minősíthető pontosan és egyértelműen a cselekmény.

Mindezek alapján elengedhetetlen, hogy az utasítás, parancs kiadására jogosult rendőri vezetők és parancsnokok – köztük különösen a fegyelmi jogkört gyakorlók – legyenek azon általános és konkrét ismeretek birtokában, amelyek befolyásolják a parancsaikkal szembe szegülő magatartások minősítését, valamint meghatározzák a magatartások szankcionálása kapcsán kötelező, szükséges, elvárt és lehetséges intézkedéseket.

A parancs iránti engedetlenség bűncselekmény esetszáma az összes katonai bűncselekményhez viszonyítva alacsony, viszont az nem kérdőjelezhető meg, hogy a szolgálati rendre és fegyelemre, ezáltal a rendőri szervezet eredményes működésére gyakorolt negatív hatásuk jelentősen túlmutat az elkövetések számán.

A katona (a rendőr) a számára jogszerűen kiadott parancsot nem bírálhatja, nem minősítheti, az általa feleslegesnek vagy értelmetlennek vélt – de jogszerű – parancs végrehajtását sem tagadhatja meg. Fontos megjegyezni viszont, hogy az elöljáró „bűnös” parancsát az alárendelt – jogszabályi keretek között – megtagadhatja. E szabályozási rendszer mind az elöljárót, mind az alárendeltet védi a parancs kapcsán.[79]

A katonai szervezet eredményes működésének egyik feltétele, hogy az alárendeltek jogellenes parancsmegtagadása – a jogszabályi keretek között – megfelelő módon és mértékben kerüljön szankcionálásra, amelynek célja a szolgálati rend és fegyelem fenntartása, valamint másoknak a hasonló esetektől történő visszatartása. E körülményekre tekintettel a parancs iránti engedetlenség bűncselekménnyel szembeni fegyelmi tárgyú parancsnoki

[79] Görbe i. m. 17. o.

intézkedések szakszerűsége minden esetben kiemelt figyelmet kell, hogy kapjon a rendőri szervezetnél.

Irodalomjegyzék

Alice Miller: More already on the central comittee's leading small groups, China Leadership Monitor 2014/44. szám

Boda Mihály: Az akarattól a tettig: a parancsteljesítés erkölcsi szerkezete. Hadtudomány 2016/26. szám

Fejes Erik: Emlékkötet dr. Kovács Tamás (1940-2020) altábornagy legfőbb ügyész tiszteletére. Magyar Katonai Jogi és Hadijogi Társaság. Budapest, 2023.

Gabriel, Richard A.: The Warriors Way – A Treatise in Military Ethics. Kingstone: Canadian Defense Academy Press. 2007

Görbe Boldizsár: A parancsra cselekvés büntetőjogi szabályozása. Szegedi Tudományegyetem Állam- és Jogtudományi Kar. Jogi Fórum. Szeged, 2019.

Hadtudományi Lexikon – új kötet. Dialóg Campus. Budapest, 2019.

Harai Dénes: A modern haderőtechnika és értékfelfogása. Társadalom és Honvédelem 2015/1. szám. Budapest.

Hart, Herbert L.A.: Commands and Authoritative Legal Reasons. In: Essays on Bentham. Oxford: OUP. 1982.

Hautzinger Zoltán: A katonai büntetőjog rendszertana. AndAnn. Pécs, 2010.

Hautzinger Zoltán: A katonai büntetőjog rendszere, a katonai büntetőeljárás fejlesztési lehetőségei. Doktori PhD értekezés. Pécsi Tudományegyetem Állam- és Jogtudományi Kar Doktori Iskola. 2010.

Honfi Attila: A katonai fegyelem és a bekövetkezett bűncselekmények összefüggései a Magyar Honvédségnél az 1990-es években. Zrínyi Miklós Nemzetvédelmi Egyetem Kossuth Lajos Hadtudományi Kar Szociológia Pedagógia és Pszichológia Tanszék. Egyetemi Tankönyv. Budapest, 2006.

Jenei György: Max Weber bürokráciaelmélete és a neoweberiánus szintézis. Pro Publico Bono – Magyar Közigazgatás 2016/3. szám. Budapest.

John Levin et. al.: Introduction to Choice Theory. United Kingdom. Oxford University Press. 2004

Kardos Sándor István: Kizárólag a katonai vétségek elbírálása utalható fegyelmi jogkörbe? Katonai Jogi és Hadijogi Szemle 2024/2. szám.

Korda György: A katonai és honvédelmi kötelezettségek elleni bűncselekmények. Zrínyi Katonai Kiadó. Budapest, 1988.

Kovács Gábor: A rendészeti szervek szervezeti kultúrájának összetevői és sajátosságai, a téma feldolgozás a Rendőrtiszti Főiskola vezetéselméleti oktatásában. Pécsi Határőr Tudományos Közlemények 10 kötet. Pécs, 2006.

Kovács Gábor: A rendészeti szervek vezetés- és szervezéselmélete. Nemzeti Közszolgálati Egyetem. Budapest, 2014.

Kovács Gábor et. al.: A szervezetvezetés elmélete. Dialóg Campus. Budapest, 2017.

Kovács István: Klasszikus vezetési funkciók a parancsuralmi rendszerben (állományvédelmi) ellenőrzés, és korrupciómegelőzés a helyi és a területi rendvédelmi szervek körében. Nemzeti Közszolgálati Egyetem. Budapest, 2019.

Kovács István: A parancs szerepe a rendészeti vezetésben. Katonai Jogi és Hadijogi Szemle 2024/2. szám.

Madai Sándor: A kötelességszegés szolgálatban bűncselekmény alapkérdése. Katonai Jogi és Hadijogi Szemle 2023/1. szám.

Madarász Tibor: Közigazgatás és jog. Közigazgatási és Jogi Kiadó. Budapest, 1987.

Miskolci Jogászélet 1925/12. szám

Moskos, Charles C.: A posztmodern haderő felé: az Egyesült Államok, mint paradigma. In: Tálas Péter (szerk.): Civil-katonai kapcsolatok: a tudományok határán. Zrínyi kiadó. Budapest, 2006.

Rendészettudományi Szaklexikon. Dialóg Campus. Budapest, 2019.

Sántha Ferenc: Az elöljáró parancsa, mint büntethetőségi akadály a magyar büntetőjogban. Miskolci Egyetemi Jogi Közlemények 2014/22. szám.

Schulteisz Emil: A katonai büntetőtörvény (1930. évi II. törvénycikk) magyarázata. Általános rész. In: Fejes Erik (szerk.): Schultheisz Emil katonai büntetőjogi értekezései. Magyar Katonai Jogi és Hadijogi Társaság. Budapest, 2018.

Szun-Ce: A hadviselés törvényei. Balassi Intézet. Budapest, 1995.

Törő Lajos: A katonai etika, a tiszti hivatás és értékrend néhány kérdése. Hadtudományi Szemle 2016/1. szám.

Vámosi Zoltán: Szociológiai aspektusok. Főiskola jegyzet. Gábor Dénes Főiskola. Budapest, 2001.

Wolff, Robert Paul: The Conflict between Authority and Autonomy. In Joseph Raz (szerk.): Authority, Basil Blackwell. 1990.

Hivatkozott normák

1875. évi Szolgálati Szabályzat a Magyar Királyi Honvédség részére

A Rendőrségről szóló 1994. évi XXXIV. törvény.

A központi államigazgatási szervekről, valamint a Kormány tagjai és az államtitkárok jogállásáról szóló 2010. évi XLIII. törvény.

A rendvédelmi feladatokat ellátó szervek hivatásos állományának szolgálati jogviszonyáról szóló 2015. évi XLII. törvény.

A büntetőeljárásról szóló 2017. évi XC. törvény.

Indokolás a Büntető Törvénykönyvről szóló 2012. évi C. törvény módosításáról szóló 2024. évi LXVIII. törvényhez.

A Büntető Törvénykönyvről szóló 2021. évi C. törvény.

A belügyminiszter irányítása alatt álló fegyveres szervek hivatásos állományú tagjai Fegyelmi Szabályzatáról szóló 11/2006. (III. 14.) BM rendelet.

A belügyminiszter irányítása alatt álló rendvédelmi feladatokat ellátó szervek parancsnoki nyomozásának különös szabályairól szóló 11/2018. (V. 30.) BM rendelet.

A fegyelemkezelő adatállománnyal kapcsolatos feladatokról szóló 11/2013. (III. 29.) ORFK utasítás.

Hivatkozott ítéletek és határozatok

Fővárosi Bíróság Katonai Tanácsa KB. VIII. 437/1883.
Legfelsőbb Bíróság Katf. I.301/1988
Fővárosi Ítélőtábla Katonai Tanácsa 6.Kbf.38/20l7/10.
Fővárosi Törvényszék Katonai Tanácsa 43.Kb.113/2018/9.
Debreceni Törvényszék Katonai Tanácsa Kbk.II.12/2018/2.
Hajdú-Bihar Megyei Bíróság Katonai Tanácsa KB. II. 42/2019.
Debreceni Törvényszék Katonai Tanácsa Kb.III.2/2019/5.
Győri Törvényszék Katonai Tanácsa Kb.I.1/2019/9.
Kúria Mfv.II.10.218/2019/3.
Fővárosi Ítélőtábla 6.Kbf.24/2020/8.
Szegedi Regionális Nyomozó Ügyészség 6.Nyom.315/2021.
Kaposvári Törvényszék Katonai Tanácsa Kbpk.I.4/2021/4.
Fővárosi Ítélőtábla Katonai Tanácsa 6.Kbf.15/2023.
Győri Törvényszék Katonai Tanácsa Kbk.I.4/2023/2.
Budapesti Rendőr-főkapitányság 01140-103/1-4/2023. Fe.