



GIBA TAMÁS

A MESTERSÉGES INTELLIGENCIA ÉS A
VÉDELMI ÁGAZAT EGYES TALÁLKOZÁSI
PONTJAI

MILITARY AND INTELLIGENCE CYBERSECURITY RESEARCH PAPER

2025/2.



BEVEZETŐ

A mesterséges intelligencia mára egy olyan megkerülhetetlen jelenséggé vált, amelyre szinte minden iparág a profitmaximalizálás, az automatizáció és a hatékonyságnövelés zászlóshajójaként tekint. Ez a technológia, mint megannyi forradalmi eszköz, képes lehet az emberi jólét, illetve mind a makro-, mind a mikrogazdasági termelés volumenének növelésére, továbbá a védelmi ágazat tekintetében is számos úttörő megoldást kínálhat. A közismert, „aki lemarad, az kimarad” szállóige hatványozottan igaznak bizonyul a mesterséges intelligenciával kapcsolatos kutatások területén, hiszen az iparág rendkívül dinamikusan fejlődik, a lépestartás pedig – főleg a védelmi szektorban – nemzetbiztonsági érdek minden nemzet számára. Ebből is következik azonban, hogy a számottevő pozitív hatások ellenére nem hagyhatóak figyelmen kívül a mesterséges intelligenciával együtt járó kockázatok sem. Erre, illetve a védelmi szektorral való további összefonódásokra irányítja rá a figyelmet a Geneva Centre for Security Sector Governance által kiadott SSRBacgrounder 2025 március 26-i számának szerzői, Alexandru Lazar és Dawn Lui¹. Jelen írás az ő elemzésük gondolatmenetét követve, kiegészítve és kritikai elemzéssel megközelítve kívánja vizsgálni a mesterséges intelligencia és a védelmi szektor találkozásainak kérdéseit.

Amikor a mesterséges intelligenciáról beszélünk, akkor nem egyszerűen csak azokra a mesterséges intelligencia modellekre gondolunk, amelyek a kapott információkból képesek következtetéseket levonni, előrejelzéseket vagy összefoglalókat készíteni, hanem azokra a mesterséges intelligencia által működtetett rendszerekre is, amelyek már képesek fizikai kapcsolatba lépni a környezetükkel, önállóan döntéseket hozni és ezek alapján cselekedni.² Előbbire példaként szolgálhatnak a mesterséges intelligencia alapú chatbotok (ld. ChatGPT), utóbbira a modernkori hadviselésben is használt, mesterséges intelligenciával támogatott úgynevezett autonóm fegyverrendszerek alkalmazása az orosz-ukrán fegyveres konfliktusban,³ valamint az Izraeli Védelmi Erők által Gázában.⁴

¹ Alexandru LAZAR - Dawn LUI: *Artificial intelligence and the defence sector*, DCAF, 2025 (Elérhető: <https://www.dcaf.ch/artificial-intelligence-and-defence-sector>)

² Thomas HELLSTRÖM – Niclas KAISER – Suna BENSCH: *A Taxonomy of Embodiment in the AI Era*, Electronics, 2024/13.

³ Vasco COTOVIO – Clare SEBASTIAN – Allegra GOODWIN: *Ukraine's AI-enabled drones are trying to disrupt Russia's energy industry. So far, it's working*, CNN Business, 2024 (Elérhető: <https://edition.cnn.com/2024/04/01/energy/ukrainian-drones-disrupting-russian-energy-industry-intl-cmd/index.html>)

⁴ Yuval ABRAHAM: *'Lavender': The AI machine directing Israel's bombing spree in Gaza*, +972 Magazine, 2024 (Elérhető: <https://www.972mag.com/lavender-ai-israeli-army-gaza/>)

A fentiekre tekintettel nem véletlen, hogy a védelmi ágazatban⁵ is jelentősen megnövekedett a mesterséges intelligenciával kapcsolatos kutatások volumene, a fejlett haderők egyre több területen kívánják felhasználni a technológia adta lehetőségeket, az Amerikai Egyesült Államok hadereje például már 2023 augusztusában létrehozott egy munkacsoportot, amelynek célja a mesterséges intelligencia felelős és stratégiai módon történő hasznosításának kutatása.⁶ A hivatkozott tanulmányban a szerzőpáros arról számol be, hogy amennyiben a kutatások előremutató eredményekkel zárulnak, ki kívánják terjeszteni annak alkalmazását a hadviselés, a finanszírozás és az egészségügy területére is.⁷

A mesterséges intelligenciával járó kockázatok - így különösen az emberi jogok veszélybe sodródása, az adatvédelemmel járó kihívások, a demokratikus intézmények erodációja - mind olyan problémakörök, amelyeket a nemzetközi közösség is felismert és a mai napig dolgozik a megfelelő reakción.

SZABÁLYOZÁSI KÖRNYEZET

A Nemzetközi Vöröskereszt szervezete 2018-ban készített egy átfogó tanulmányt, amelyben a szerző az autonóm fegyverrendszerek alkalmazhatóságát vetette össze a nemzetközi humanitárius joggal.⁸ Az abban megfogalmazottak alkalmasak lehetnek arra, hogy analógiaként alkalmazzuk őket a mesterséges intelligencián alapuló fegyverrendszerekre is, tekintve, hogy ugyanazokat az alapelveket szükséges érvényre juttatni, nevezetesen a megkülönböztetés, arányosság és elővigyázatosság elvét. Ezt az analógiát erősíti az is, hogy mind a NATO szakosított szervei, mind pedig egyes tagállamai széles körben végeznek kutatásokat és képzéseket azért, hogy a nemzetközi közjog intézményeinek kibertéri tevékenységekre való alkalmazhatóságát alátámasszák és megerősítsék.⁹ A mesterséges intelligencia alkalmazása pedig magától értetődő módon jelentős hatást fog gyakorolni a

⁵ A védelmi ágazatra ebben a tanulmányban, mint gyűjtőfogalomra utal a Szerző, amely ágazat magába foglalja rendvédelmi, honvédelmi, nemzetbiztonsági szférát és azok kormányzati irányítását is.

⁶ 2nd Lt. Andrew P. BARLOW - CDT Allison BENDER: *Innovating Defense: Generative AI's Role in Military Evolution*, U.S. Army, 2025 (Elérhető: https://www.army.mil/article/286707/innovating_defense_generative_ais_role_in_military_evolution)

⁷ David ONIANI - Jordan HILSMAN - Yifan PENG - Ronald K. POROPATICH - Jeremy C. PAMPLIN - Gary L. LEGAULT - Yanshan WANG: *Adopting and Expanding Ethical Principles for Generative Artificial Intelligence from Military to Healthcare*, npj Digital Medicine 6/11, 2023

⁸ Neil DAVISON: *A legal perspective: Autonomous weapon systems under international humanitarian law*, ICRC, 2018 (Elérhető:

https://www.icrc.org/sites/default/files/document/file_list/autonomous_weapon_systems_under_international_humanitarian_law.pdf)

⁹ Tallinn Manual valamennyi kiadása; <https://rm.coe.int/64th-cahdi-pr-aurel-sari-presentation/1680aaaf48>; <https://www.cambridge.org/core/books/cyber-operations-and-international-law/74D210E76E46531542AD27CECF07ABDE>

jövőben a különféle kibertéri tevékenységekre és műveletekre is, ami ezt a fajta párhuzamba állítást is megalapozza. A Vöröskereszt tanulmánya hangsúlyozta a fenti elvek azonossága mellett, hogy hivatkozva az Egyes Hagyományos Fegyverekről szóló nemzetközi egyezményre, a részes államok között egyetértés van abban, hogy a fegyverrendszerek és az erő alkalmazása során az érdemi, vagy hatékony emberi beavatkozást fenn kell tartani, ezt az álláspontot képviseli maga a Vöröskereszt is.¹⁰

Egyes szerzők globális biztonsági kockázatként tekintenek arra, hogy a nemzetközi közösség még nem dolgozott ki olyan jogi kötőerővel bíró dokumentumot, amely a mesterséges intelligencia katonai műveletekben, vagy a védelmi ipari szektorban történő alkalmazásának szabályozását rendezné.¹¹ A hivatkozott szerző nézetei szerint ezt a joghézagot az Európai Uniónak szükséges kitöltenie.

A mesterséges intelligencia tekintetében az első átfogó, a tagállamok számára kötelező érvényű szabályanyagot az Európai Unió fektette le, 2024-ben, rendelet formájában.¹² Kifejezett célja, hogy az Európai Unión belül a mesterséges intelligencia rendszerek biztonságosak, etikusak és megbízhatóak legyenek, mindezeket úgy kívánja véghez vinni, hogy a technológiát fejlesztők és szolgáltatók számára ír elő kötelezettségeket. Fontos megemlíteni, hogy a szabályozás pusztán a kereskedelmi célú mesterséges intelligenciára tartogat normatív utasításokat, kizárva ebből a katonai és nemzetbiztonsági felhasználást, vagyis az előző gondolatban jelzett aggályokra még nem jelent megoldást, de egy azt megelőző lépésként már felfogható, hiszen a mai biztonsági környezetben a védelmi-biztonsági szféra civil szférával való kutatói, fejlesztői együttműködése már magától értetődő, ahogy ezt több meghatározó nyugati hírszerző szolgálat vezetője is hangsúlyozta már az elmúlt években.¹³

Megfigyelhető egyfajta megnövekedett érdeklődés az Európai Unió tagállamaiban is, a mesterséges intelligencia védelmi célú felhasználását illetően. Franciaország Védelmi Minisztériuma 2019-ben megalkotta a mesterséges intelligencia integrálásának stratégiáját, amely a katonai képességek fejlesztésére és hatékonyabb ellenőrzésére hivatott,¹⁴ majd 2024-

¹⁰ Uo. 11. o.

¹¹ Raluca CSERNOTAI: *Governing Military AI Amid a Geopolitical Minefield*, Carnegie Europe, 2024 (Elérhető: <https://carnegieendowment.org/research/2024/07/governing-military-ai-amid-a-geopolitical-minefield?lang=en¢er=europe>)

¹² Az Európai Parlament és a Tanács (EU) 2024/1689 rendelete (2024. június 13.) a mesterséges intelligenciára vonatkozó harmonizált szabályok megállapításáról, valamint a 300/2008/EK, a 167/2013/EU, a 168/2013/EU, az (EU) 2018/858, az (EU) 2018/1139 és az (EU) 2019/2144 rendelet, továbbá a 2014/90/EU, az (EU) 2016/797 és az (EU) 2020/1828 irányelv módosításáról (a továbbiakban: Rendelet)

¹³ PETRUSKA Ferenc – VIKMAN László: *Egy formabontó hírszerzési nyilatkozat a jogi sérülékenységek szempontjából*. Military and Intelligence Cybersecurity Research Paper 2021/4. (Elérhető: https://hhk.uni-nke.hu/document/hhk-uni-nke-hu/4_2021_MIC_RP.pdf)

¹⁴ Héloïse FAYET: *French thinking on AI integration and interaction with nuclear command and control, force structure, and decision-making*, European Leadership Network, 2023 (Elérhető:

ben a francia vezetés létrehozta a Mesterséges Intelligencia Védelmi Miniszteri Ügynökséget,¹⁵ 300 millió eurós költségvetéssel.¹⁶ Németország kormánya is a mesterséges intelligencia kutatása és fejlesztése mellett tört lándzsát, ennél fogva létrehozták a Helmut Schmidt Egyetem berkein belül a Védelmi Mesterséges Intelligencia Megfigyelőközpontot, amely döntő szerepet játszik a német Bundeswehren belüli mesterséges intelligencia kutatásokban.¹⁷

Ígéretes és előremutató kezdeményezésként értékelhető, hogy az Amerikai Egyesült Államok 2023-ban elindította a Mesterséges Intelligencia és az Autonómia Felelősségteljes Katonai Alkalmazásáról szóló politikai deklarációs iratot. A nyilatkozat ambiciózus célja, hogy nemzetközi konszenzust teremtsen a felelős magatartásról, és iránymutatást adjon az államoknak a katonai mesterséges intelligencia fejlesztéséhez, telepítéséhez és használatához. A részes államok első plenáris ülését 2024. márciusában hívták össze, ahol az Amerikai Egyesült Államok kormánya rendszeres párbeszédet ígért a részes államok számára.¹⁸

HOGYAN HASZNOSÍTHATÓ A MESTERSÉGES INTELLIGENCIA A VÉDELMI SZÉKTORBAN

Geneva Centre for Security Sector Governance már idézett tanulmánya¹⁹ szerint három pozitív hatással járhat a mesterséges intelligencia használata a védelmi iparban:

- az automatizáció nyújtotta előnyök,
- a hatékonyabb helyzetértékelés, valamint
- az irányításban és ellenőrzésben lévő potenciálok.

A mesterséges intelligencia alkalmazása a rutinszerű, főként adminisztratív jellegű feladatoknál értékes emberi erőforrások felszabadítását tudja eredményezni, amely felszabadult erőforrásokat így komplexebb stratégiai feladatok végrehajtására lehet átcsoportosítani. További előny, hogy javíthatja a költségvetés allokálásának hatékonyságát, és képes észlelni a pénzügyi anomáliákat is.

https://www.europeanleadershipnetwork.org/wp-content/uploads/2023/11/French-bibliography_AI_Nuclear_Final.pdf

¹⁵ Ministerial Agency for Artificial Intelligence in Defence (MAAID)

¹⁶ James BROOKS: *France announces R&D agency for military artificial intelligence*, ResearchProfessional News, 2024 (Elérhető: <https://www.researchprofessionalnews.com/rr-news-europe-france-2024-3-france-announces-r-d-agency-for-military-ai/>)

¹⁷ Defense AI Observatory – DAIO (Elérhető: <https://defenseai.eu/english>)

¹⁸ Az Amerikai Egyesült Államok Külügyminisztériuma: *Politikai nyilatkozat a mesterséges intelligencia és az autonómia felelős katonai alkalmazásáról* (Elérhető: <https://www.state.gov/bureau-of-arms-control-deterrence-and-stability/political-declaration-on-responsible-military-use-of-artificial-intelligence-and-autonomy>)

¹⁹ Alexandru LAZAR - Dawn LUI i.m. (2025)

Annak köszönhetően, hogy a technológia képes hatalmas, az emberi elme által már nem feldolgozható mennyiségű információk befogadására, elemzésére és mindezek alapján következtetések levonására, a valós idejű helyzetértékelés kulcsfontosságú a dinamikusan fejlődő védelmi iparban. Az emberi erőforráson alapuló adatelemzés egyik óhatatlan mellékhatása a hibázás lehetősége, amelyet teljes mértékben annulál a gépi intelligencia. A védelmi képességek tekintetében akár egy apró figyelmetlenség is végzetes következményekkel járhat.

Hasonló a helyzet az irányítás és a felügyelet kérdése kapcsán, ahol szintén fundamentális jelentőségű a valós idejű információk eljuttatása a kompetens döntéshozók számára. A védelmi erők egészére vonatkozó, nagy mennyiségű, olykor szeparált információs csatornák együttes elemzése lehetővé teheti a honvédelmi erők részére a felkészültség fokozását.

Megvizsgálva a szerzők által felsorolt három vitathatatlan előnyt, könnyen belátható, hogy a védelmi ágazaton belül főleg a nemzetbiztonsági szférában kardinális kérdés a naprakész információk megszerzése, rendszerezése és azok helyes értékelése, tekintve, hogy a fő feladatuk a nemzet biztonságának, szuverenitásának szavatolása. Magától értetődően, számos helyről jogosultak információ- vagy adatigénylésre, betekinhetnek közhiteles adatbázisokba és egyéb titkosszolgálati eszközök és módszerek állnak a rendelkezésükre, hogy minél több ismeret birtokában legyenek. Magyarországon például a nemzetbiztonsági szolgálatok a feladatuk teljesítése érdekében jogosultak bármely adatkezelési rendszerből adatot kérni a cél megjelölésével, így különösen állami szervtől, többségi tulajdonú gazdasági társaságtól, hitelintézetektől.²⁰

A nemzetbiztonsági szférához, valamint a titkosszolgálatok feladatvégrehajtásához kapcsolható a mesterséges intelligencia nyílt forrású információszerző képessége. Az OSINT (open source intelligence) a hírszerzésnek azon ágazata, amely a nyilvánosan elérhető források megszerzésére és feldolgozására irányul, ezek a források lehetnek akár tudományos publikációk, konferenciák előadásanyagai vagy napilapok. Kiemelt ágazatról beszélhetünk, hiszen egyes szerzők – optimista – becslései szerint a titkosszolgálatok adatállományának 80 és 90 százaléka közé teszik a nyílt forrásból származókat.²¹ Tekintve, hogy a napjainkban a mesterséges intelligencia ügynökök szinte mindegyike hozzáfér az internetes forrásokhoz, a nemzetbiztonsági ágazatban történő hasznosításuk kézenfekvő. A speciálisan erre a célra létrehozott modellek képesek lehetnek másodpercek alatt olyan prediktív elemzések és adatgyűjtések végrehajtására, amelyek manuális, emberi erőforrással napokat vesznek

²⁰ A nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény 40. § (1) bekezdés

²¹ Riccardo GHIONI - Mariarosaria TADDEO - Luciano FLORIDI: *Open source intelligence and AI: a systematic review of the GELSI literature*. AI & society, 1–16. <https://doi.org/10.1007/s00146-023-01628-x>

igénybe. Természetesen a generált elemzések és tartalmak utóellenőrzése kiemelt fontosságú, főleg annak fényében, hogy a döntéselőkészítés gerincét a pontos analízisek adják.

Ezekon kívül a titkosszolgálatok és rendvédelmi szervek remekül ki tudják aknázni a mesterséges intelligencia mintázatfelismerő képességét. Az előre betanított protokollokat és viselkedési mintákat követve kulcsfontosságú szerepet tölthet be a prediktív rendészeti²² módszerekben, sőt, a kémelhárítási profilú nemzetbiztonsági szolgálatok munkáját és hatékony képes kiegészíteni. Teszi ezeket a bonyolult kapcsolati hálók közötti összefüggések megtalálásával, a cellainformációk elemzésével, vagy például több – akár tízórányi – videófelvetelek elemzésével, amely komplett munkanapokat takaríthat meg a személyi állománynak.

A mesterséges intelligencia képes komplett fegyverrendszerek irányítására is, vagy pilóta nélküli repülőrendszerek koordinálására, megkönnyítve ezzel a felderítést, a harcérintkezést és a logisztikai támogató műveleteket.

Kiválóan felhasználható a mesterséges intelligencia a kibertér biztonságosabbá tartásához, mivel segítséget nyújthat a hálózati infrastruktúrát fenyegető támadások felderítésében, előrejelzésében vagy elhárításában. Az Indiai Védelmi Kutatási és Fejlesztési Szervezet²³ kifejlesztette a NETRA²⁴ névre hallgató mesterséges intelligencia alapú védelmi rendszert, amely az világháló forgalmát figyeli a biztonsági fenyegetések észlelése érdekében. Ez a rendszer harcászati szinten is hasznosítható lehet, amely képes lehet figyelmeztetést adni az ellenséges csapatmozgásokról, következtetéseket levonni a közelgő támadásokról, vagy viselkedésminták azonosítására.²⁵

Számos, a védelmi iparban aktívan tevékenykedő gazdasági társaság mesterséges intelligencia által támogatott katonai kiképzési szimulációs szoftvereket fejlesztett, amely amellet, hogy költségvetési erőforrást takarít meg, képes realisztikus környezetet teremteni a harcoló katonák számára. A technológia alkalmas arra is, hogy imitálja azt a harctéren is előforduló megannyi változót, amely azonnali beavatkozást igényelnek.²⁶

Ha a fenti állításokat és előnyöket összevetjük azokkal a hírekkel, amelyek szerint globálisan több nemzetbiztonsági és titkosszolgálatot is érintenek emberi erőforrásbéli

²² KISFONAI Bernadett: A bűnügyek jövőbeli megelőzése, avagy a prediktív rendészet új arca, *Rendőrségi Tanulmányok*, 2023/3., DOI azonosító: <https://doi.org/10.53304/RT.2023.3.02>

²³ India's Defence Research and Development Organisation - DRDO

²⁴ Network Traffic Analysis

²⁵ Ajay VERMA: *The Algorithmic Battlefield: How AI is Redefining Military Might*, Medium, 2025 (Elérhető: <https://medium.com/@ajayverma23/the-algorithmic-battlefield-how-ai-is-redefining-military-might-5d3fb3e9c590>)

²⁶ A téma kapcsán lásd: <https://sdi.ai/blog/military-training-simulation-software-ai/>

problémák,²⁷ továbbá, ha figyelembe vesszük, hogy a modern világunk legfontosabb kihívásaiként tarthatjuk számon különböző dezinformációs törekvéseket,²⁸ a manipulált hang- és videófelvételeket, illetve egyéb álhíreket, belátható, hogy a mesterséges intelligencia tudatos és ésszerű alkalmazása ezeket a problémákat képes enyhíteni.

KOCKÁZATOKRÓL ÉS MELLÉKHATÁSOKRÓL

Az újonnan megjelenő, forradalmi jelentőségű technológia alkalmazásának természetesen árnyoldalai is vannak, amelyekre már több jogvédő szervezet is felhívta a figyelmet, jóllehet ezek a szervezetek főleg az emberi jogi és adatvédelmi kockázatokkal számolnak.²⁹ A Harvard Egyetem egyik kibertér kutatásra szakosodott kutatóközpontjának 2018-ban készült tanulmánya hat iparág (büntető bíraskodás, pénzügyi szektor, egészségügy, tartalom moderálás, emberi erőforrások és oktatás) részletes vizsgálatával mutatta be, hogy a mesterséges intelligencia alkalmazása milyen emberi jogi aggályokat vethet fel. A kutatási eredményeik – számos pozitív hatástól eltekintve – a magánélethez való univerzális jog, továbbá az adatvédelem területén találtak leginkább veszélyforrásokat, de a mesterséges intelligencia jelentősen befolyásolta az egyenlőséghez, a szabad véleménynyilvánításhoz és a munkához való jogot.³⁰

A legnagyobb kockázat mindezek ellenére a kiberbiztonsági kihívásokban keresendő. Az egyre jobban érzékelhető pszichológiai befolyásolási törekvéseknek kedvezett a mesterséges intelligencia térhódítása, a kiberbűnözők fegyverarzenálja kibővült egy szofisztikált, megfigyeléseken alapuló rendszerrel, amely képes ún. deepfake tartalmak létrehozására és hatékonyabb adathalászatra.

Maga a félrevezetés, az álhírek terjesztése, a manipulált kép- és hangfelvételek nyilvánosságra hozása nem csak a kiberbűnözők eszköze, azt előszeretettel használják állami szereplők is, példaként említhetők az orosz befolyásolási technikák.³¹ A mesterséges

²⁷ A téma kapcsán lásd: https://www.telegraph.co.uk/world-news/2024/07/22/german-intelligence-service-bnd-short-staffed-russia-threat/?utm_source=chatgpt.com, https://www.abc.net.au/news/2024-12-01/inside-the-uk-push-to-recruit-more-spies/104510104?utm_source=chatgpt.com.

²⁸ Andreu CASERO-RIPOLLÉS - Laura ALONSO-MUÑOZ - Diana MORET-SOLER: *Spreading False Content in Political Campaigns: Disinformation in the 2024 European Parliament Elections*, Media and Communication, 2025/13

²⁹ A téma kapcsán lásd: <https://ennhri.org/ai-resource/key-human-rights-challenges/>

³⁰ Filippo A. RASO - Hannah HILLIGOSS - Vivek KRISHNAMURTHY - Christopher BAVITZ - Levin KIM: *Artificial Intelligence & Human Rights: Opportunities & Risks*, The Berkman Klein Center for Internet & Society Research Publication Series, Research Publication No. 2018-6, 2018

³¹ Josip MANDIĆ - Darijo KLARIĆ: *Case study of the russian disinformation campaign during the war in Ukraine – propaganda narratives, goals, and impact*, National Security and the Future, 2023/24

intelligencia ebben az esetben képes olyan koholt felvételek létrehozására, amely aláshatja a demokratikus intézmények hatékonyságát, továbbá bizonyos közéleti szereplők jóhírét.

Előfordulhat az az eset is, amikor maga a mesterséges intelligencia rendszere kerül kibertámadás alá. Mivel a szóban forgó rendszer is kódsorokból és digitális folyamatleírásokból áll, fokozottan ki van téve olyan manipulációs szándékoknak, amelyekben a támadók felül akarják írni a meghatározott viselkedési protokollokat, arra sarkallva ezzel az eszközöket, hogy ne az elvártak szerint viselkedjenek. Egy ilyen mértékű támadásnál a károk beláthatatlanok lehetnek, kezdve az egyszerű adatszívargásoktól a félretájékoztatáson át egészen a katonai műveletek manipulálásáig. Természetesen az adatszívargás sem elhanyagolható, annál is inkább, mivel akár a katonai, akár a nemzetbiztonsági adattár komponenseinek nagyrésze olyan szenzitív információnak számít, amely potenciális célpontja lehet ellenséges hírszerző szolgálatok számára.

Jelenleg ingoványos talajként tekintünk az elszámoltathatóság kérdésre, amely mindenképpen egyértelmű szabályozást kíván meg. Abban az esetben, ha a mesterséges intelligencia használata közben hiba merül fel, vagy visszaélést követnek el, nem egyértelmű, hogy ki tehető emiatt felelőssé. A kódsorokat gépelő szoftverfejlesztők? Esetleg az a személy, aki az adatokat szolgáltatata, amelyből a rendszer a rossz következtetést vont le? Aki nem ellenőrizte vissza a rendszer által generált eredményt?

Problémát jelenthet az is, ha nem a megfelelő célokra, vagy túlzott mértékben veszik igénybe a rendszer adta lehetőségeket, előfordulhatnak olyan döntéshozatali helyzetek, ahol az emberi ítélőképesség, emberi intuíció kihagyhatatlan komponens. Ezeket a képességeket alááshatja, ha minden esetben a mesterséges intelligencia által szolgáltatott javaslatokra támaszkodunk.

ÖSSZEGZÉS

A DCAF idézett háttéranyagának gondolatmenetét követve jelen tanulmányban áttekintésre került, hogy a védelmi ágazatban milyen potenciális előnyökkel és veszélyekkel, kockázatokkal járhat a mesterséges intelligencia alkalmazása. Ez a téma a hazai kutató közösségben is egyre fokozódó érdeklődést tükröz³² és további vizsgálata, illetve az egyes sajtós szakterületekhez igazodóan specializált megközelítése nélkülözhetetlen lesz a jövőben.

³² KNBSZ mindkét MI kötete, Kovács László: *Hadviselés a 21. században: kiberműveletek*. Ludovika Egyetemi Kiadó, 2023, Budapest (Elérhető: https://tudasportal.uni-nke.hu/xmlui/bitstream/handle/20.500.12944/21611/1057_Hadviseles_a_21_szazadban_Kibermuveletek.pdf?sequence=1&isAllowed=y;), Petruska Ferenc: Nemzetközi szabályozás szükségessége az autonóm fegyverekre. *Hadtudomány*, Évf. 34. szám 4. (2024) <https://orcid.org/0000-0003-2625-7317>, MEZEI Kitti (szerk.):

A mesterséges intelligencia jelenlegi állapota szerint rendkívül nagy hatékonysággal képes elvégezni azokat a rutinszerű, adminisztratív feladatokat, amelyek nem igényelnek nagy mértékű szellemi energiabefektetést. Kiválóan felhasználható továbbá olyan adatbázisok kivonatolására, összegzésére, illetve feldolgozására, amely az emberi agyi kapacitás korlátjaiból fakadóan már nem értelmezhetőek. Fontos azonban tisztában lenni azokkal a kibervédelmi, adatvédelmi és emberi jogi kockázatokkal, amelyek óhatatlanul beárnyékolják a technológiát.

Emberi visszaellenőrzés és felügyelet nélkül, minden elképzelhető munkafolyamatban támaszkodni a mesterséges intelligenciára ugyanakkora hiba, mint egyáltalán nem használni. Tudatos, felelősségteljes és megfelelő szabályozási környezettel körülbástyázott alkalmazása lehetővé teszi mind a védelmi iparág valamennyi szegmense és szereplője számára a professzionálisabb, hatékonyabb munkavégzést, nem is beszélve az eredményesebb erőforrásallokálásról, mind emberi, mind költségvetési források tekintetében.

Azt lehet látni, hogy a mesterséges intelligencia, mint egy újabb felforgató technológia, minden bizonnyal a jövőben alapjaiban fogja megváltoztatni azt a hadviselési módot, amelyet ma ismerünk. Ennek tükrében elkerülhetetlenné válik a modern haderő szisztémájának újragondolása, egyre nagyobb hangsúlyt kell fektetni az olyan nem konvencionális hadviselési irányokra, mint például a kiberhadviselés, a dezinformációs kampányok, vagy az automatizált fegyverrendszerek.

Kockázatok és lehetőségek a mesterséges intelligencia jogi szabályozásában. Wolters Kluwer, Budapest, (2025)
ISBN: 9789635944255

FELHASZNÁLT IRODALOM

- Alexandru LAZAR – Dawn LUI: Artificial Intelligence and the Defence Sector. Geneva Centre for Security Sector Governance (DCAF), Geneva, 2025.
- Thomas HELLSTRÖM – Niclas KAISER – Suna BENSCH: A Taxonomy of Embodiment in the AI Era. Electronics, 2024/13.
- Andrew P. BARLOW – Allison BENDER: Innovating Defense: Generative AI's Role in Military Evolution. U.S. Army, 2025.
- David ONIANI et al.: Adopting and Expanding Ethical Principles for Generative Artificial Intelligence from Military to Healthcare. npj Digital Medicine, 2023/6(11).
- Neil DAVISON: Autonomous Weapon Systems under International Humanitarian Law. International Committee of the Red Cross (ICRC), Geneva, 2018.
- Tallinn Manual on the International Law Applicable to Cyber Operations. Cambridge University Press, valamennyi kiadás.
- Raluca CSERNOTAI: Governing Military AI Amid a Geopolitical Minefield. Carnegie Europe, Brussels, 2024.
- Az Európai Parlament és a Tanács (EU) 2024/1689 rendelete (AI Act).
- PETRUSKA Ferenc – VIKMAN László: Egy formabontó hírszerzési nyilatkozat a jogi sérülékenységek szempontjából. MIC Research Paper, 2021/4.
- Héloïse FAYET: French Thinking on AI Integration and Interaction with Nuclear Command and Control. European Leadership Network, 2023.
- Az Amerikai Egyesült Államok Külügyminisztériuma: Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy.
- 1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról.
- Riccardo GHIONI – Mariarosaria TADDEO – Luciano FLORIDI: Open Source Intelligence and AI: A Systematic Review. AI & Society, 2023.
- KISFONAI Bernadett: A prediktív rendészet új arca. Rendőrségi Tanulmányok, 2023/3.

- Andreu CASERO-RIPOLLÉS et al.: Disinformation in the 2024 European Parliament Elections. Media and Communication, 2025/13.
- Filippo A. RASO et al.: Artificial Intelligence & Human Rights: Opportunities & Risks. Berkman Klein Center, 2018.
- Josip MANDIĆ – Darijo KLARIĆ: Russian Disinformation Campaign during the War in Ukraine. National Security and the Future, 2023/24.
- KOVÁCS László: Hadviselés a 21. században: Kiberműveletek. Ludovika Egyetemi Kiadó, Budapest, 2023.
- PETRUSKA Ferenc: Nemzetközi szabályozás szükségessége az autonóm fegyverekre. Hadtudomány, 2024/4.
- MEZEI Kitti (szerk.): Kockázatok és lehetőségek a mesterséges intelligencia jogi szabályozásában. Wolters Kluwer, Budapest, 2025.

Military and Intelligence CyberSecurity Research Paper 2025/2.

Szerző(k) / Author(s):

Giba Tamás

Kézirat lezárásának ideje / Manuscript closing time:

2025.10.14.

Szerkesztők / Editors:

Dr. Farkas Ádám PhD

Dr. Magyar Sándor PhD

Kiadó / Publisher:

Nemzeti Közsolgálati Egyetem Hadtudományi és Honvédtisztképző Kar
Nemzetbiztonsági Intézet Katonai Nemzetbiztonsági Tanszék
University of Public Service (Hungary), Faculty of Military Sciences and Officer
Training, National Security Institute Department of Military National Security

Kiadó képviselője / Representative of the publisher:

Dr. Magyar Sándor PhD

Elérhetőségek /Contacts:

<https://nbi.uni-nke.hu/oktatasi-egysegek/katonai-nemzetbiztonsagi-tanszek/katonai-nemzetbiztonsagi-kiberter-muveleti-szakcsoport/researchpaper>

farkas.adam@uni-nke.hu | magyar.sandor@uni-nke.hu

1011 Budapest, Hungária krt. 9-11. /9-11. Hungária Blvd., Budapest, H1011

ISSN:

2786-3778

A borító <https://www.stockvault.net/photo/270507/cyber-security-web-security-network-security> címen elérhető ingyenes háttérkép felhasználásával 2021. február 25-én készült.

The cover was created on 25. February 2021, using a free wallpaper available at <https://www.stockvault.net/photo/270507/cyber-security-web-security-network-security>.

A sorozat egyes számaiban foglalt vélemények, állásfoglalások a szerzők saját véleményét tükrözik. Azok nem tekinthetők sem a kiadó, sem a szerzőt foglalkoztató intézmények hivatalos álláspontjának.

The opinions and resolutions included in each issue of the series reflect the authors' own opinions. They should not be construed as an official point of view of either the publisher or the institutions employing the author.