

Ollári Viktor¹

A technológiai szingularitás és a tömegpusztító fegyverek egyes hasonlóságai és különbségei

Certain Similarities and Differences Between the Technological Singularity and Weapons of Mass Destruction

Absztrakt

Alig két éve még kevesen feltételezték a mesterséges intelligencia (MI) napjainkra megvalósuló, robbanásszerű fejlődését. Jelen tanulmány a technológiai szingularitást megalapozó technológiákat, ezen belül hangsúlyosan az MI mint a tömegpusztító fegyverekkel összevethető hatást megvalósító technológiákat elemzi. Kvantitatív adatgyűjtés révén kiválasztott releváns szakirodalmak elemzésével vizsgáltam, hogy milyen mértékben vethető össze az MI diszruptivitása a tömegpusztító fegyverekével; képes lehet-e az MI közvetlenül is pusztító hatást kifejteni, illetve azt, hogy lehetséges-e a szabályozása az első hidegháború idején megismert jogi instrumentumokkal.

Kulcsszavak: mesterséges intelligencia, MI, technológiai szingularitás, tömegpusztító fegyverek, WMD

Abstract

A few experts would have predicted such explosive growth of artificial intelligence (AI) now barely two years ago. This paper analyses the technologies that underpin the technology singularity, focusing on AI as a technology with effects comparable to weapons of mass destruction. Through quantitative data collection, selected relevant literature is analysed to examine the extent to which the disruptiveness of AI can be

¹ Doktori hallgató, Nemzeti Közszerológati Egyetem Hadtudományi és Honvédtisztképző Kar Katonai Műszaki Doktori Iskola, e-mail: ollari.viktor@protonmail.com

compared to WMD, whether AI can have a direct destructive impact and whether it can be regulated by the legal instruments known during the Cold War I.

Keywords: Artificial Intelligence, AI, Technological Singularity, Weapons of Mass Destruction, WMD

Bevezető

Míg 2022 elején kevesen feltételezték, hogy megvalósulhat a mesterséges intelligencia (MI) ilyen arányú, mindennapi, széles körű alkalmazása, addig 2023 januárjában a ChatGPT regisztrált felhasználóinak száma elérte a 100 milliót. 2023 végére közel 2 milliárdan látogattak el az alkalmazás weboldalára, 2024 decemberében már heti 300 millió aktív felhasználót szolgált ki.² Szintén a tudományos fantasztkum világába sorolták számosan, hogy a nagy nyelvi modellek (LLM³) számos területen elérik, vagy akár meg is haladják a humán kompetenciákat a 2020-as évek közepéig.

Az MI stratégiai jellegét erősíti a tény, hogy a technológia vezető hatalmai (USA, Kína) legfelsőbb politikai szinten kezdeményeztek egyeztetéseket a vonatkozó kontrollmechanizmusok kialakítása érdekében.⁴

Az MI fejlődésének sarokköveiként értékelhető a fejlesztéséhez, működéséhez és folyamatos adaptálódásához szükséges minőségi adatok mennyisége,⁵ illetve ezen információtömeg „gyors” elérését/áramlását biztosító, nagy megbízhatóságú IKT-infrastruktúra⁶ rendelkezésre állása. Halála előtt kevéssel Neumann János hipotetikus jelleggel megfogalmazta, hogy a tudomány és technológia egyre gyorsuló fejlődése a jövőben olyan paradigmaváltást (szingularitást) hoz létre, amelyet követően „az emberi élet, ahogyan azt eddig ismertük, nem folytatódhat”.⁷

Jelen tanulmányban a napjainkat befolyásoló technológiai hármás (MI–5G/6G–IoT) lehetséges paradigmaváltást okozó szimbiotikus hatását⁸ értem a technológiai szingularitás (TS) fogalma alatt; szem előtt tartva a TS definícióját, amely szerint az MI egy adott ponton képessé válik önmaga rekurzív fejlesztésére, önmagánál fejlettebb megoldások létrehozására.⁹

A hazai és külföldi szakirodalom, ennek hiányában a téma neves és elismert szerzői publikációinak tanulmányozásával, elemzésével és értékelésével megvizsgálom, milyen mértékben feleltethető meg az MI és a tömegpusztító fegyverek hatása; igazolható-e, hogy az MI képes lehet közvetlen diszruptív hatást kiváltani; illetve, hogy lehetséges-e az MI „fegyverkezési versenyt” az első hidegháborúban alkalmazott fegyverkorlátozási jogi instrumentumokkal szabályozni.

² WIGGERS et al. 2025.

³ Large language model.

⁴ DEPP 2024.

⁵ Pl. az IoT-technológia, big data stb. forrásokból származó adattömeg.

⁶ 5G, kiemelten 6G, a jövő technológiáját illetően a kvantumkommunikáció.

⁷ ULAM 1958: 6.

⁸ MCCAIN 2023.

⁹ SEEWALD 2022: 94–95.

Technológiai alapozás

A TS megvalósulásának szűk keresztmetszeteit technológiai oldalról vizsgálva, az egyre növekvő mennyiségű, dinamikus frissülő, strukturált adatok¹⁰ rendelkezésre állása és adatok közel valós idejű továbbítását biztosító, nagy megbízhatóságú IKT-hálózatok (elsődlegesen 5G/6G) megfelelő penetrációjú globális alkalmazása szükséges minimumként azonosítható.

Az új generációs mobilkommunikációs hálózatok már egyértelműen az informatikai hálózatok körébe sorolhatók, kiegészítve mindezt a szoftverizáció és virtualizáció funkcióival és a szabványokban megfogalmazott „mindenhol jelen lévőség” igényével, különösen a 6G tekintetében.¹¹ Az 5G képességportfóliója három jellemző köré csoportosítható:¹²

- nagyszámú felcsatlakoztatott eszköz kiszolgálása (mMTC¹³),
- nagy sebességű adatátvitel (eMBB¹⁴),
- megbízható és egyben rövid késleltetési idejű kommunikáció (uRLLC¹⁵).

A 6G-vízió¹⁶ olyan technológiai ökoszisztémát vázol, amely biztosítani képes, hogy a Föld népességének túlnyomó része fenntartható, magas biztonsági szintű kibertérhez kapcsolódhasson.¹⁷ A 6G szinte korlátlan mennyiségű, közel teljes körű, számos dimenzióból megközelített/feldolgozott, releváns információ közel azonnali elérését biztosíthatja a felhasználó entitások számára.

Elfogadva azon definíciót, amely szerint IoT-megoldásnak tekinthető minden olyan eszköz, amelyek egymással összekapcsolódva infrastruktúrát alkotnak, biztosítva a hozzáférést az egyes infrastruktúra-elemek (azok csoportja/egésze) által generált/gyűjtött adatokhoz (és/vagy aktuátorként viselkedni); gyakorlatilag az IoT-kategóriába sorolható minden, hálózathoz csatlakozni és adatgenerálásra/-gyűjtésre képes megoldás.¹⁸

A mesterséges intelligencia vonatkozásában az EU MI Rendelet¹⁹ vonatkozó definícióját veszem alapul, amely szerint az MI „olyan gép-alapú rendszer, amelyet úgy terveztek, hogy különböző szintű autonómiával működjön, és amely explicit vagy implicit célok érdekében képes olyan kimeneteket létrehozni (például előrejelzések, ajánlások, döntések), amelyek befolyásolják a fizikai vagy virtuális környezetet”.

Ami az MI generációit illeti, különböző megfogalmazások alatt két fő fejlesztési hullámot különítenek el a szakértők:²⁰

¹⁰ Egyebek mellett nagy tömegű IoT-ökoszisztémára támaszkodva.

¹¹ TÓTH 2023: 79.

¹² TÓTH 2023: 57.

¹³ *Massive machine type communication* – pl. IoT-eszközök, gép-gép kommunikáció kiszolgálása.

¹⁴ *Enhanced mobile broadband* – nagy tömegű adatátvitelt igénylő forgatókönyvek, pl. virtuális és kiterjesztett valóság (VR, AR) kiszolgálása.

¹⁵ *Ultra reliable low latency communications* – pl. távsebészet, önzetető és pilóta nélküli járművek kiszolgálása.

¹⁶ ITU-R M.2160-0 (11/2023).

¹⁷ SINGH et al. 2025.

¹⁸ OLLÁRI 2024a; 2024b.

¹⁹ Az Európai Parlament és a Tanács (EU) 2024/1689 Rendelete.

²⁰ BÁNKÚTY-BALOGH 2022: 104–106; BODA 2024b.

1. „Gyenge,” vagy „szűk” MI (ANI²¹) – a korunkban létező, jól strukturált (címkézett) adatkészletekkel tanított, adott környezetben működő, feladat-specifikus (például képtartalom-elemzési) megoldások. Ezen modellek emberi képességeket imitálnak, de az ezeket igénylő feladatokat nagyságrendekkel gyorsabban és sokszor hatékonyabban képesek végrehajtani.
2. „Erős”, vagy „általános” MI (AGI²²) – az általános célú MI-modellek²³ megjelenésével a közeljövő időtávjába átkerülő, az emberi intelligenciával egyenértékű, nem címkézett adatkészletekkel „tanított”, absztrakciós és adaptációs képességgel rendelkező, emberi döntésekre képes MI.

Az AGI megvalósulását számos szakértő 15 éven belül nem tartja reálisnak. Részben a számítási kapacitások telítődésére, az ehhez szükséges energia korlátosságára és a tanításhoz rendelkezésre álló adatok elégtelenségére hivatkozva. Mások mellett érvelnek, hogy az MI bevonása az MI-kutatásokba hozhat olyan nem várt eredményeket, új megközelítéseket hardver és „szoftver” (algoritmus) szinten, amelyek robbanásszerű fejlődést generálva, akár már öt-tíz éven belül az AGI-korszakba „taszíthatják” az emberiséget.²⁴

A jövőbeni harmadik stáció az emberi intelligenciát meghaladó mesterséges szuperintelligencia (*technológiai szingularitás*).²⁵

Jelenünket érintően a nagy nyelvi modellek (LLM) alkalmazása – fejlesztési (gyermek-) „betegségei” ellenére – érzékelhetően kezdi befolyásolni világunkat.²⁶ A 2024-es évben jelentős előrelépést könyvelhetett el az iparág. A technológia fejlődését jól szemlélteti, hogy 2024-ben az úgynevezett MMLU²⁷ benchmarkteszten a szakértői szinttől (89,8%) legfeljebb négy százalékpontos eltérési határon belül teljesített a nagyobb LLM-ek közel 50%-a. A GPQA²⁸ teszten még jobban teljesítettek az emberek, de már két modell (Claude 3.5 Sonnet, Gemini 2.0 Flash) az emberi szakértői szintet (65,4%) elérve, annak közelében teljesít, míg az OpenAI o1 jelentősen meghaladva azt 75,7%-ot ért el. Szükséges rávilágítani, hogy a nem szakértői szint a GPQA esetén 33,9%, amelyet az újabb jelentősebb LLM-ek majd mindegyike túlszárnyal.²⁹ A 2024. december végén elérhetővé tett, magas érvelési képességekkel jellemzett OpenAI o3 az első LLM, amely felülmúlta (76%) az emberi válaszadókat az ARC-AGI³⁰ teszten, illetve a legjobb 200 humán kódíró közé került. Ami a modell matematikai képességeit illeti, 2,2%-os eredményt ért el a kimagasló nehézségű

²¹ Artificial narrow intelligence.

²² Artificial general intelligence.

²³ Pl. OpenAI ChatGPT.

²⁴ ASCHENBRENNER 2024; RODRÍGUEZ 2024.

²⁵ KOVÁCS–GURÁLY 2023: 13.

²⁶ MADIEGA 2023.

²⁷ *Measuring massive multitask language understanding* (nagy tömegű, többfeladatos nyelvi megértés mérése), ismereteket felmérő teszt matematika, történelem, IT-tudományok, (USA) jog és történelem stb. témakörökben. HENDRYCKS et al. 2021.

²⁸ *Graduate-level Google-proof Q&A* (főiskolai szintű, Google-biztos kérdés-felelet), biológia/fizika/kémia tematikájú, kiemelten nehéz kérdéseket tartalmazó tesztkészlet. REIN et al. 2023.

²⁹ Lásd: <https://www.vellum.ai/llm-leaderboard>

³⁰ *Abstract and reasoning corpus – artificial general intelligence* (elvonatkoztatási és érvelési korpusz – általános mesterséges intelligencia).

FrontierMath teszten, amelyet minden eddigi modell csak 2%-ra tudott teljesíteni; illetve a középiskolás „matekzszenik” színvonalát elérő, illetve meghaladó szinten (96,7%) teljesítette az AIME³¹ feladatsort.³²

Az MI-megoldások olyan védelmi/nemzetbiztonsági célokra is felhasználhatók, mint fordítási és kommunikációtámogató feladatok, az állomány egészségügyi és bevetetőségi állapotának felmérése, előrejelzése, fenyegetésdetektálás és valós idejű helyzetértékelés, célmeghatározás, kiképzés és gyakorlat szimuláció, műveleti/taktikai/logisztikai/karbantartási tevékenységek akár prediktív jellegű támogatása, kibervédelem, multimédiás (hang, kép stb.) tartalomelemzés,³³ autonóm járművek vezérlése.³⁴ Az LLM-ek, kiaknázandó elemző-értékelő, generatív (például jelentéskészítő) és döntéstámogató képességeiket, rendkívül rövid időn belül intenzív alkalmazhatósági vizsgálatok tárgyává váltak a védelmi és a nemzetbiztonsági szférában. Továbbá korán megkezdődtek a stratégiai tervezést és a nemzetközi döntéshozatali támogató alkalmazhatóságukat vizsgáló kutatások. Mindemellett, az USA légierje (mások mellett) képzési, „háborús játékokhoz” is felhasználta a technológiában rejlő lehetőségeket.³⁵ Az USA hírszerzési közösségét összefogó Nemzeti Hírszerzési Igazgató Hivatala (ODNI³⁶) a Carnegie Mellon Egyetem bevonásával vizsgálta az LLM-ek alkalmazásának kivitelezhetőségét,³⁷ aminek eredményeként olyan megoldások születtek, mint a META Llama alapjain nyugvó „Defense Llama”.³⁸

Nyilvánossá vált tanulmányok rámutatnak arra, hogy a kínai szakértőket is élenként foglalkoztatja az LLM-ek alkalmazhatósága. A META Llama-13B és a Stanford Egyetem erre alapozott Vicuna-13B modelljének továbbfejlesztéséből létrehozott ChatBIT, az érintett publikáció megállapítása szerint, magas hatékonysággal ismeri fel az árnyalt/összetett katonai információ kontextusokat. Elemzési képességei (például fegyverrendszerek hatékonyságának értékelése) rendkívül magas szintűek; a kutatók alkalmasnak látják rendszerbe állításra információkinyerő, helyzetelemzési és művelettámogató célokra.³⁹

MI-hidegháború (?)

Keegan érvelése szerint a háború, megkülönböztetve annak rituális és abszolút (clauswitzi) verzióját, a kultúra folytatása más eszközökkel.⁴⁰ A hidegháború szempontjából a keegan-i rituális háború jellemzői⁴¹ figyelemre méltóak. Otterbein megközelítésében

³¹ American invitational mathematics examination (amerikai meghívásos matematika vizsga).

³² GLAZER et al. 2024; URISTA 2024.

³³ Arc (és egyéb biometrikus jellemzők), járművek, fegyverzet, egyéb eszközök, érzelmek stb. detektálása/azonosítása.

³⁴ OLLÁRI-SURÁNYI 2024.

³⁵ CABALLERO-JENKINS 2024.

³⁶ Office of the Director of National Intelligence.

³⁷ GALLAGHER et al. 2023.

³⁸ Lásd: <https://scale.com/blog/defense-llama>

³⁹ CHEUNG 2024.

⁴⁰ KEEGAN 2002; BODA 2024b: 106.

⁴¹ Megegyezésem alapon zajlik, célja nem a pusztítás, hanem a bátorság felmutatása, kiállás a becsületért, mindkét fél győztesnek érezheti magát (döntetlenre hozzák ki).

a rituális háború az ellenfél erejének felmérését, tesztelését szolgálja.⁴² A hidegháború alatt a szemben álló felek között voltak kisebb közvetlen súrlódások, proxyháborúk,⁴³ folyamatosan zajlott a szemben álló felek erejének tesztelése, de széles skálájú eszkaláció nem történt. A szembenállás milyenségét számos, közösen lefektetett szabály keretezte, köztük számos olyan, amelyek alapvető célja volt a forró háborúvá válás megelőzése.

Barry Buzan definíciója szerint, a hidegháború a „nemzetközi rend és hatalom kapcsán kialakuló tartós és jelentős politikai konfrontáció, amelyet az erős védelmi dilemma miatt egyik fél sem akar forró háborúval megoldani”.⁴⁴ Az Új/második hidegháború kezdetét illetően számos időpontot fogalmaztak meg kutatók. 2014-től (a Krím orosz megszállása), 2018-on át (Kína–USA) technológiai és kereskedelmi háború kiéleződése, 2022-ig (orosz–ukrán konfliktus) több dátum is felmerül. Mások arra mutatnak rá, hogy karakteresen elkülönülő, az egyes tömbök „lakossága” által tömegesen követhető ideológiai különbségek nem alakultak ki 2022-ig a szemben álló felek, blokkok⁴⁵ között, és a blokkok még ma is több szálon kötődnek egymáshoz. Az „első hidegháború” idején a szemben álló feleknél előállított tömegpusztító fegyverek mennyisége ösztönözte a forró, közvetlen konfliktusok kerülését, mivel a nukleáris eszkaláció az egész Földet érintette volna, s ez egy úgynevezett „erős védelmi dilemmát” generált. További „hidegháborús” kritérium az ideológia, amelyért az érintettek harcolni is hajlandóak.⁴⁶ Ez a feltétel napjaink konfliktus-keretrendszeréből hiányzik, így leginkább „küzdelemre érdemes vitákról”⁴⁷ beszélhetünk.⁴⁸

Az MI-hidegháború kérdését vizsgálva felmerül a kérdés: azonosítható-e tömegpusztító fegyverként (WMD⁴⁹) a TS és annak központi magja az MI? Lehetséges „erős védelmi dilemma” létrehozása MI-alapokon? A *Hadtudományi Lexikon* szócikke szerint WMD-ként definiálható az, ami „a többi fegyverhez képest, azonos körülmények esetén, hatásai sajátos jellegénél és méreteinél fogva, viszonylag rövid idő alatt rendkívül nagymértékű pusztítást okoznak az élőerőben, a haditechnikai eszközökben, az épületekben, valamint más létesítményekben”.⁵⁰ Habár készültek forгатatókönyvek a nukleáris fegyverek korlátozott alkalmazására, a szakértők megalapozottan feltételezik, hogy ezen szcenáriók megvalósíthatósági valószínűsége alacsony, és valószínűbb a széles körű eszkaláció. Ez az első csapásváltás során százezer halálát eredményezi, ezzel lenullázva a clausewitz-i politikai érdek jelentőségét, hiszen ezt követően bármely politikai (és társadalmi, nem extrém ideológiai) cél irrelevánssá válik.⁵¹

Mindezeket figyelembe véve megállapítható, hogy önmagában az MI nem felel meg a WMD-definíciónak. Azonban a TS keretein belül, ahol IoT-ként azonosítunk minden

⁴² OTTERBEIN 2004; BODA 2024b: 106.

⁴³ Andrew Mumford (2013): „Olyan konfliktus, amibe harmadik fél indirekten avatkozik be azzal a céllal, hogy befolyásolja annak a stratégiai kimenetelét az általa támogatott fél számára.” BODA 2024a.

⁴⁴ BUZAN 2024.

⁴⁵ Euroatlanti térség – BRICS(+) formáció.

⁴⁶ Zéróösszegű ideológiai polarizáció.

⁴⁷ Gazdasági vagy politikai hatalom, kulturális befolyás érdekében.

⁴⁸ BUZAN 2024.

⁴⁹ Weapon of Mass Destruction.

⁵⁰ KRAJNC 2019: 1099.

⁵¹ BODA 2024b.

olyan eszközt, amely lehetővé teszi az MI számára, hogy WMD-t hozzon létre és/vagy vezéreljen, valójában közelítünk az erős védelmi dilemmához.

Kissinger és Allison három alapvető eltérést azonosít az MI és a WMD-k között. Először is, az MI-fejlesztések jelentős részét privát entitások folytatják, számukra másodlagosak a nemzeti biztonsági tényezők (első a profit). Másodszor, az MI-fejlesztés – összevetve a nukleáris WMD-ekkel – olcsóbb és egyszerűbb; továbbá a nukleáris fegyverek fejlesztése relatíve jól nyomon követhető, szemben az ellenfél MI képességeinek azonosításával. Harmadszor, az MI-technológia fejlesztése jelentősen gyorsabb, mint a fegyverrendszereké. Az MI-verseny szempontjából problematikus, hogy míg a nyugati társadalmak fejlesztési eredményeinek többsége azonnal ismertté válik, csak közvetett információkkal rendelkezünk Kína való MI-képességeiről.⁵² Az élvonalbeli MI-fejlesztések néhány technológiai szuperhatalom⁵³ kisszámú entitásának kezében van, a rohamos gyorsaságú fejlesztések eredményeként a korábbi generációk olcsóbbá válnak, és proliferációjuk felgyorsul. Az MI fegyverkorlátozás jellegű szabályozását a gyors fejlődés és a nem nyomon követhető képességmentő nagyban nehezíti. Kissinger és társai „az MI alkalmazásával kapcsolatos általános felelősségtudat és következmények tudatos felmérésének képességében” jelölik meg a probléma megoldását, mivel a jogszabályok és megállapodások szinte kizárólag reaktív jellegűek lehetnek, ami az MI fejlődését tekintve nem elégséges. Mindettől függetlenül, a szerzők javaslatot tettek arra, hogy az USA és Kína között még az előtt önkorlátozó megállapodás szülessen, hogy az MI az államok biztonsági komplexumának elemévé váljon.⁵⁴

A médiában egyre gyakoribbak az MI önálló támadási képességeire utaló tartalmak, és a közvélemény tudatában megjelent az MI-szorongás.⁵⁵ Illetve, a szorongásnak táptalajt adhatnak mindazon publikus hírek és információk, amelyek nyilvánvalóvá teszik az átlagpolgár számára, hogy az államigazgatás és az ipari szféra⁵⁶ aktívan készül az újgenerációs védelem-/biztonságpolitika és hadviselés korára úgy, hogy az USA–Kína MI-fegyverkezési verseny egyértelműen zajlik, és a kissingeri „fegyverzetkorlátozó megállapodások” még váratnak magukra. Ellenben a Biden-adminisztráció egy MI-technológia továbbadását szigorúan korlátozó rendeletet adott ki 2025 januárjában.⁵⁷ Még ha egy „MI-fegyverzetkorlátozási” megállapodás nem is vezetne tényleges eredményre, folyamatos kommunikációt biztosíthatna a felek között, (némi) jobb rálátást egymás képességeire, ezeken keresztül egy (törékeny) stabilitás lenne elérhető úgy, hogy a felek, némi kompromisszum árán, profitálhatnának belőle. A Ballisztikus Rakétaelhárító Szerződés (ABM⁵⁸), vagy Közepes Hatótávolságú Nukleáris Erők korlátozásáról szóló Szerződés (INF⁵⁹) azt a célt szolgálta, hogy a szemben álló felek (hozzávetőlegesen) tisztában lehessenek egymás képességeivel,

⁵² KISSINGER–ALLISON 2023.

⁵³ Elsődlegesen az USA és Kína birtokában.

⁵⁴ KISSINGER–SCHMIDT–HUTTENLOCHER 2023.

⁵⁵ Hasonlatosan az 1980-as évekig tartó, nukleáris háború bekövetkeztét vizionáló „nukleáris-szorongáshoz”. Pl.: KIM et al. 2023.

⁵⁶ Pl. NITZBERG 2025.

⁵⁷ Forrás: <https://www.bis.gov/press-release/biden-harris-administration-announces-regulatory-framework-responsible-diffusion>

⁵⁸ Anti Ballistic Missile Treaty.

⁵⁹ Intermediate-Range Nuclear Forces Treaty.

illetve lehetőség szerint ne legyenek olyan eszköz birtokában, amely túlzott paranoiát okozva világégest generálhatna.⁶⁰

Negyedik generációs kitekintés

Míg az ókor és a középkor idején a kockázatvállalásra épülő természetes bátorságot (hősiesség) helyezték piedesztálra,⁶¹ addig az újkor idején – technikailag a második világháború végéig egyértelműen, de az 1980-as évek végéig – a harcos/hős katona ideája tovább élt,⁶² de a hangsúly inkább tevődött át a kockázatok – kiképzési és technikai alapú – menedzselésére (hazaszeretetre épülő bátorság). A második világégest követően az európai civil társadalmak hamarabb, az amerikai társadalom néhány évtized késéssel kezdett érzékenyebben reagálni a katonai érdekérvényesítések áldozati listáira. Így egyre erőteljesebbé váltak azon érdekek, amelyek a saját áldozatok minimalizálását helyezték előtérbe. Ezt felismerve a kisebb/feltörekvő társadalmi csoportok, közösségek változtattak stratégiájukon, sikerre vezetve az egykori gyarmatok függetlenségi küzdelmeit, meghátrálásra kényszerítve az USA-t Vietnámban, a Szovjetuniót Afganisztánban. A William S. Lind és szerzőtársai által 1989-ben megfogalmazott 4. Generációs Hadviselés (4GH) egy, a változó világsszellemre reagáló, a hadviselés egy decentralizált, a politikai/társadalmi/gazdasági/katonai hálózatokat kiaknázó és ezek spektrumain operáló (totális jellegű), nemzeti jellegében homályosuló,⁶³ improvizatív és magasan fejlett (digitális) technológiákat kiaknázó, az információs és pszichológiai műveleteket előtérbe helyező, az előző generációs hadviselés elemeit felhasználó és jellegében a gerillaharc jegyeit is felmutató (aszimmetrikus),⁶⁴ térben és időben korlátozott kiterjedésű, alacsony intenzitású koncepció.⁶⁵ A 4GH-ban egyre nagyobb szerepet kapnak a nem állami szereplők, úgy a „biztonsági vállalkozások”,⁶⁶ mint egyes ügyekhez és/vagy társadalmi csoportokhoz köthető (művelet-végrehajtó, -támogató) entitások.⁶⁷ Az 1990-es évektől fellendülő IT-iparág, különösen a 2010-es évektől, egyre hatékonyabb autonóm és távvezérelhető fegyverrendszereket⁶⁸ volt képes biztosítani a hadseregek számára, amelyek lehetővé tették az élőerő megóvásának maximalizálását, illetve erőteljesen támogatták a 4GH-koncepció megvalósítását a fizikai, információs és kognitív dimenziókban.

Szembeötlő kettősség figyelhető meg az úgynevezett „nyugati” (elsődlegesen az euroatlanti) társadalmak esetén. Habár a szórakoztatóipar által előállított termékek⁶⁹

⁶⁰ MAURER 2018.

⁶¹ Lásd pl. görög, germán hős eposzok.

⁶² Lásd pl. a vietnámi háború kultuszát az amerikai társadalomban.

⁶³ Egyes társadalmi elemek/csoportok, nemzeti, nemzetközi, nemzetek feletti szereplők egyidejű, akár dinamikusán változó összetételű részvételével zajló folyamatok. Egyéni szinten is elmosódik a határ a civil és a katonai szereplők között.

⁶⁴ Nem katonai eszközök, módszerek (társadalmi destabilizálás, információs támadás, kémkedés, célzott támadás személyek vagy objektumok ellen) előtérbe helyezése. BODA 2023.

⁶⁵ BODA 2024a.

⁶⁶ Privát katonai szolgáltatók (*private military contractor*, PMC).

⁶⁷ Szürke- és feketezonás pénzügyi szolgáltatók, terror- és szervezett bűnözéshez sorolt szervezetek, hackercsoportok stb.

⁶⁸ Pl. drónok.

⁶⁹ Kiemelten filmek és „videójátékok”.

egyre erőszakosabbak, a társadalom érzékenysége a szenvedésre általánosságban növekszik. Egyes kutatók, szembe menve a korábban megállapítottaktól, amellet érvelnek, hogy nincs bizonyíthatóan empatikus készségeket csökkentő hatása az erőszakos tartalmak fogyasztásának.⁷⁰ Más megvilágításból vizsgálva a kérdést, kutatók egy része azon álláspontot képviseli, hogy a drónok és egyéb „autonóm fegyverrendszerek”⁷¹ alkalmazói oldalról, a videójátékok világába helyezték át a hadviselést. Egy konzolkezelő számára a kiiktatandó célszemély nem valóságos ember, hanem egy „kiberentitás”, így a megsemmisítése jelentős lelkiismereti problémát nem okoz. Mások felhívják a figyelmet arra, hogy ezen alkalmazások kezelői – a technológia sajátosságai okán⁷² – számos esetben szembesülnek azzal, hogy nem lehetnek biztosak abban, jogos fegyverhasználat történt-e. Továbbá, kifejezetten a drónkezelők esetében ismétlődő feladat lehet egy adott célterület rendszeres megfigyelése, amely során az ott tartózkodókat vizsgálják, kvázi kötődés alakul ki, majd ezt követően támadási parancsot kapnak, amelynek végrehajtása jelentős stresszhatást fejt ki rájuk stb.⁷³ Az MI bevonása, a távvezérelhető és autonóm fegyverrendszerek alkalmazása ezen stresszt csökkentheti. Részben a beérkező információk elemzése révén csökkentik a kezelőkön lévő felelősségstresszt, mivel – ha nem is „hivatalosan” – átvesszi a felelősséget például egy adott képanyag elemzése révén. Ugyan nem (feltétlenül) az MI hajtja végre a likvidálást, de a kezelő hivatkozhat arra, hogy az MI erősítette meg a célt. Amennyiben a teljes vezérlést átvesszi, az emberi elem (és sérülékenységei) kiiktatható, de jelentős mértékben dehumanizálja a szemben álló felet, a szimpla statisztikai hatékonyság vizsgálatának szintjére szorítva műveleti feladatok tervezését és végrehajtását.⁷⁴

Egyes kutatók az MI hadviselésre gyakorolt pozitív (lehetséges) hatásai közé sorolják, hogy a saját élőerő kímélése mellett egy MI-vezérelt (autonóm) fegyverrendszer, amennyiben a hatályos nemzetközi hadijog és egyéb szabályozók és megállapodások figyelembevételével tanították (programozták), minden körülmény között, kifáradástól mentesen biztosítja a végrehajtott művelet jogszabályi megfelelőségét.⁷⁵ A megállapítás elméleti szinten helytálló, de az emberi elem kiemelésével egy hatékony mesterséges entitást kapunk, amely nem rendelkezik olyan tulajdonságokkal, mint nagylelkűség, kímélet. A feladatát magas hatékonysággal végrehajtja. Mindemellett számos olyan kérdés merül fel, amely az emberi kulturális diverzitásra vezethető vissza. Kiragadott példaként, az MI miként ismeri fel nagy hatékonysággal a tényleges megadást és a megtévesztést; miként mérlegel a járulékos (civil) veszteségek tekintetében; a művelet végrehajtását vagy az emberi élet kímélését helyezi előbbre?

A kiberműveletek a 4GH szerves részét képezik. Napjainkra, levonva a 2007-es Észtországot ért és az azt követő jelentősebb kibertámadások⁷⁶ tanulságait, az egyes

⁷⁰ APA 2020, ROY-COLL 2024.

⁷¹ Az a gép, amely közvetlen emberi segítség nélkül képes a környezetét érzékelni, ez alapján döntést hozni és cselekedni. BODA 2022.

⁷² Az adatátviteli csatorna szűk sávzsélessége, a távolságból fakadó átviteli kihívások, interferenciák stb. okán sok esetben nehezen elemezhető képanyag.

⁷³ HIJAZI et al. 2017; CAMPBELL 2021.

⁷⁴ BODA 2024a: 114.

⁷⁵ BODA 2024a:118.

⁷⁶ KOVÁCS 2023: 88–96.

államok, valamint a szövetségeket tekintve a NATO⁷⁷ egyre nagyobb hangsúlyt fektet a kibervédelmi és „kiberelrettentési” (válaszcsepási) képességek létrehozására. Nem lezárt annak vizsgálata, hogy pontosan mi tekinthető „jelentősebb”⁷⁸ támadásnak, és miként biztosítható, hogy az ellencsapás ténylegesen az agresszor katonai szempontból legitim eszközeit érje.

Az MI-alkalmazás szempontjából kiemelt ötödik generációs hadviselés (5GH) elsődlegesen az érzékelés és információ internalizálásának milyenségét igyekszik befolyásolni úgy, hogy a támadás alanya ne legyen tudatában, hogy támadás alatt áll, és hogy éppen elveszíti a háborút. Az 5GH mellett érvelő szerzők szerint az újgenerációs hadviselés alapvető célja az ellenfél társadalmi csoportjainak morális, kulturális befolyásolása úgy, hogy az országukról, társadalmukról, közösségükről, a világról, a politikai folyamatokról alkotott képük a támadó elvárásai szerint torzuljon.⁷⁹ Azaz elsődlegesen tekinthető az információs/pszichológiai műveletek alkalmazása, az „adaptív információs fölény” megszerzése érdekében, ahol a hangsúly a célközönség gondolatainak, véleményének átalakítására, valamint meggyőzésére, esetleg manipulálására helyeződik.⁸⁰

MI-eszkáláció

Egyetlen kifejezéssel összefoglalva a (stratégiai) „bizonytalanság” a legalkalmasabb kifejezés a mesterséges intelligencia hatásának leírására. Egyes szerzők szerint éppen az MI jelenthet megoldást az úgynevezett „bizonytalanság kódének”⁸¹ eloszlására, az irracionális döntések kiszűrésével az élőerő megóvásának hatékonysága is növelhető.⁸²

Érdemes azonban figyelembe venni, hogy ez abban az esetben következhet be, ha az MI hatásköre⁸³ korlátozott és/vagy csak az egyik fél rendelkezik stratégiai, műveleti, taktikai döntéseinek meghozatalát támogató MI-megoldással. Ellenkező esetben megvalósulhat az „MI-eszkáláció”. A döntéstámogató MI-rendszerbe érkező „azonnalos”, nagy tömegű, multimodális adatokat vizsgálva a rendszer azonosíthatja, hogy a szemben álló fél is MI-megoldást alkalmaz, és elkezd ennek megfelelő, irracionálisnak tűnő, hatékony döntéseket hozni, javaslatokat tenni. Más területről hozott példával illusztrálva, egy MI-támogatású chipfejlesztési projekt során a DL modell olyan megoldásokat javasolt, amelyek szignifikánsan túlmutattak az eredetileg becsült végtermék hatékonyságán, funkcióportfólióján, az emberi fejlesztők

⁷⁷ A 2016-os varsói csúcs műveleti területként azonosította a kiberteret, a 2019-es londoni külügyminiszeri találkozó deklarálta és a főtitkári éves jelentés megfogalmazta, hogy egy jelentősebb támadás aktiválhatja a szövetség V. cikkelyét, ezt a 2021-es brüsszeli csúcstalálkozó megerősítette. Lásd KASSAI 2022.

⁷⁸ Hagyományos fegyverekkel összemérhető károkozás. BODA 2024a:117.

⁷⁹ QURESHI 2019.

⁸⁰ HAIG 2022: 116.

⁸¹ Az emberi megismerés korlátaiból fakadó taktikai helyzetértékelési bizonytalanság.

⁸² BODA 2024a: 120–121.

⁸³ Az MI által elérhető adatok köre, mennyisége; döntési kompetenciái, ezek (jogosultsági) horizontális és vertikális kiterjedése stb.

logikáján.⁸⁴ Az MI-eszkáláció egy hatványozottan gyorsuló folyamat, mivel a szemben álló modellek, kvázi GAN⁸⁵-ként, technikailag és szükségszerűen egymást tanítják.

Szükséges szem előtt tartani, hogy amennyiben a szemben álló felek egyaránt AGI-val rendelkeznek, az eszkáláció közel elkerülhetetlen, mivel az alkalmazott modell döntési gyorsaságát az emberi elme nem képes felülmúlni. Az AGI alkalmazását, korlátozását vállaló fél magas valószínűséggel egyben a vesztes fél lesz. Ezért a felek, egy igen rövid időintervallumot követően kénytelenek lesznek az AGI számára korlátlan cselekvési szabadságot biztosítani.⁸⁶

Az eszkálációt más irányból megközelítve, az LLM-alapú védelmi, nemzetbiztonsági, külügyi döntéshozatalt támogató megoldások esetében szükséges szem előtt tartani, hogy egy LLM az emberi tudás és történelem esszenciája. Ezért logikus végeredményként, ezen modellek sajátosságait vizsgálva a kutatók azon eredményre jutottak, hogy hajlamosak a nemzetközi események kinetikus (szélsőséges) eszkálálására.⁸⁷

Igazságos MI-alkalmazás

Figyelemmel a 4GH jellemzőire, a tényleges katonai erő alkalmazásától eltekintve, problematikus magas biztonsággal elkülöníteni az általános diplomáciai tevékenységet, a geoökonómiai eszköztár mindennapi alkalmazását ezek 4GH-célú érvényesítésétől, a nemzetbiztonsági szolgálatok hibrid hadviselést támogató tevékenységétől.

A nemzetbiztonsági érdek hazai megközelítését az Nbtv.⁸⁸ 74. § a) bekezdése tisztázza, amely a jogalkotó szerint Magyarország függetlenségének (szuverenitásának) biztosítása, alkotmányos rendjének védelme. Ez összevethető az „igazságos hírszerzés” elmélete szerinti célportfólióval.⁸⁹ Tekintettel arra, hogy a nemzetbiztonsági entitások sok esetben nem tények, hanem a feltételezések alapján vizsgálódnak, az MI alkalmazása ennek támogatására egyrészt lehetőséget biztosít feltételezések gyors alátámasztására, illetve az MI olyan feltételezésekre is „javaslatot tehet”, amelyeket az illetékes szolgálatok elemző-értékelő feladatot ellátó munkatársai nem vettek figyelembe. Az „MI-eszkáláció” lehetősége ezen esetben is fennáll, mivel az alkalmazott MI- (például LLM-) modellek mintafelismerő képessége felderítheti, amennyiben egy ellenérdekelt fél/ország MI-támogatású nemzetbiztonsági tevékenységet folytat és ennek megfelelő „javaslatokat” tesz, amit szignifikáns valószínűséggel – viszonylag rövid idő alatt – az ellenérdekelt fél MI-je is azonosít, és ennek tükrében módosítja kimeneti eredményeit (ajánlásait). Hasonlóan ítéltethető meg az MI alkalmazása az „igazságos információs műveletek” esetében is. Az autonóm – *on-the-loop*⁹⁰ vagy *out-of-the-loop*⁹¹

⁸⁴ KARAHAN et al. 2024.

⁸⁵ *Generative adversarial network* – generatív versengő hálózat.

⁸⁶ BODA 2024b.

⁸⁷ A vizsgált modellek (GPT-4, GPT-3.5, Claude 2, Llama-2-Chat, GPT-4-Base) mindegyike „eszkálált”, a GPT-3.5, Llama-2-Chat, GPT-4-Base javasolta az atomfegyverek bevetését. RIVERA et al. 2024.

⁸⁸ 1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról.

⁸⁹ Az állam területének, politikai életének (beleértve gazdasági és stratégiai érdekeit), kultúrájának védelme. BODA 2022: 97.

⁹⁰ Az emberi felügyelet, beavatkozási lehetőség a cselekvési „hurokban” marad.

⁹¹ A cél meghatározását és az eszköz aktiválását követően nincs lehetőség emberi beavatkozásra, az ember kikerül a cselekvési „hurokból”.

– fegyverrendszerek tekintetében a már említett jogkövetés vs. hatékonyság és kiszámíthatóság paradoxon vet fel számos kérdést. Különösen az *out-of-the-loop* megoldások esetében kényes a felelősség kérdése, mivel az aktiválást követően az eszköz várható viselkedése nem szükségszerűen ismert az alkalmazást elrendelő számára, illetve téves gyártói információk alapján hozza meg a bevetést elrendelő döntését. Magától értetődően az autonóm fegyverrendszer felelőssége sem értelmezhető.⁹²

A fentiek alapján, az MI igazságos, felelős alkalmazásának sarokköve a lehetséges következmények ismerete, ezek megbecslésének képessége. Ez már egy új típusú, az MI alkalmazásának sajátos velejáróit kezelni képes politikai/gazdasági/katonai/rendvédelmi vezetői mentalitást igényel.

Tudomány és gazdaság

A Thomas Friedman (2005) által felvázolt, az internet révén megalapozott „Globalizáció 3.0” előnyeit kiaknázó Kína a 2010-es évekre potenciális kihívóvá vált az USA és a „Nyugat” számára.⁹³ Ezt kezelendő, részben nemzetbiztonsági érdekekre hivatkozva, 2019-ben (Trump-adminisztráció) az USA aktívan blokkolni kezdte a kínai vállalatok és egyéb entitások hozzáférését fejlett chiptechnológiákhoz, illetve az azok előállítását biztosító megoldásokhoz (például EUV-⁹⁴ litográfia). 2022-ben ezt a Biden-adminisztráció kiegészítette a chiptervezés terén etalonnak számító EDA szoftver elérhetőségének korlátozásával. Ezzel, a hivatalosan elfogadott álláspont szerint, Kína 1–3 generációval elmaradt a versenytársak mögött, és nem képes 7 nanométeresnél (nm) fejlettebb chiptechnológia megvalósítására, míg a TSMC már 4 és 3 nm-es chipeket szállít az MI-technológia alapjának számító NVIDIA H100 és B100, B200 GPU-kba.⁹⁵ A korlátozások azonban ösztönözték a kínai belső innovációs folyamatokat. A távol-keleti ország az EU K+F-költségével közel azonos (200+ Mrd EUR) összeget fordított új technológiák fejlesztésére 2022-ben.⁹⁶ A chiptervezés és -gyártás terén bevezetett USA-korlátozások alternatív lehetőségek – például fotonikus chiptechnológia és a chipre integrált úgynevezett optikai neurális hálózatok (ONN⁹⁷) – vizsgálatára sarkallták a kínai kutatókat.⁹⁸

A TS-triád elemei tekintetében Kína és az USA előnye nehezen behozható a követők számára. Az MI-t támogató „fejlett integrált áramkörök tervezése és gyártása” területén Kína jelentősen lekörözte vetélytársait, a top 10%-ba tartozó, magas idézettségű tudományos publikációk arányát tekintve (lásd 1. ábra).

⁹² BODA 2022.

⁹³ OLLÁRI 2024b: 246.

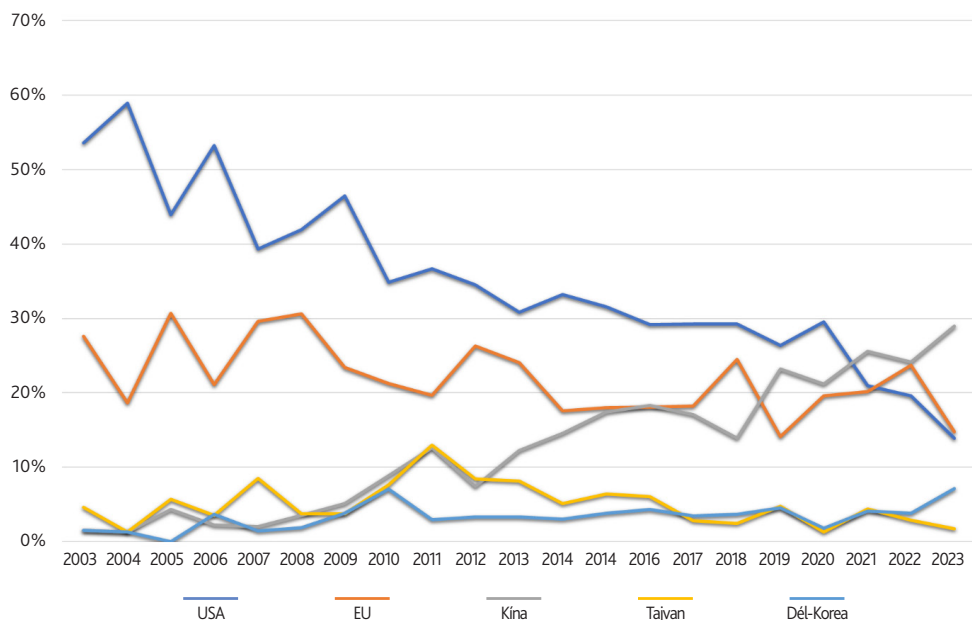
⁹⁴ Extrém ultraibolya.

⁹⁵ *Graphic processing unit* – grafikus feldolgozóegység.

⁹⁶ OLLÁRI 2024b: 248.

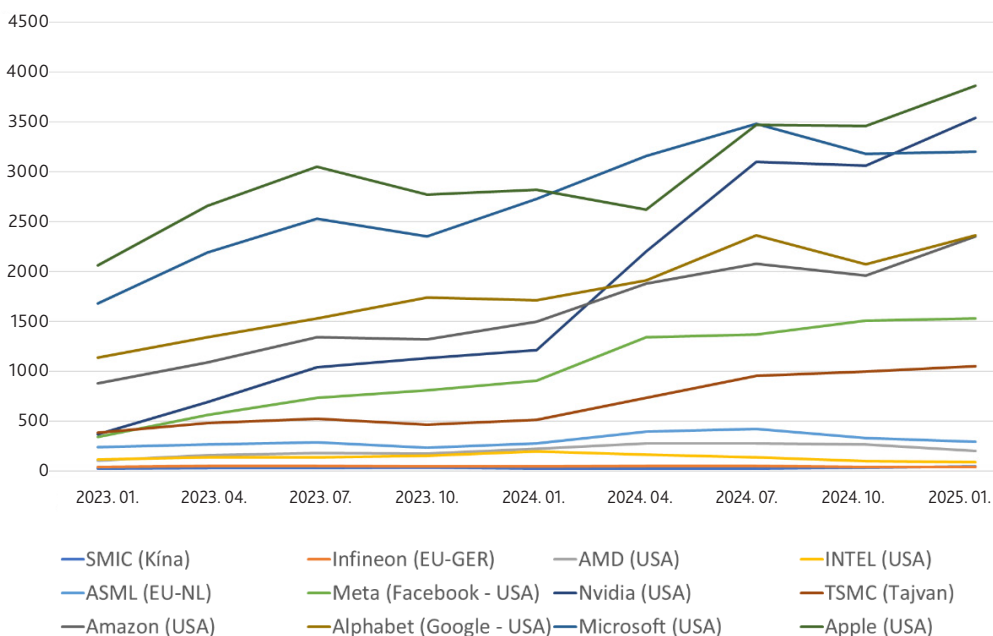
⁹⁷ Optical Neural Network – az AGI egyik lehetséges alapozó technológiájaként jellemzik.

⁹⁸ XUE et al. 2024.



1. ábra: A fejelett integrált áramkörök tervezésével és gyártásával kapcsolatos, top 10%-ba tartozó tudományos művek publikációs rátája

Forrás: GAIDA – WONG-LEUNG – ROBIN 2023



2. ábra: A jelentősebb technológiai cégek piaci tőkeértéke 2023. 01. és 2025. 01. között

Forrás: a szerző szerkesztése <https://companiesmarketcap.com/> alapján

Egyértelműen kijelenthető, hogy a nagy nyelvi modellek elérhetőségének széles körű elterjedése jótékony hatással volt a legnagyobb technológiai vállalkozásokra. Piaci tőkeértékük az „LLM-éra” eddigi szakaszában átlagosan megháromszorozódott. A 2. ábra értékeit vizsgálva érdemes kiemelni, hogy az európai félvezetőgyártás nem tudott lépést tartani az LLM-hez köthető gazdasági és technológiai folyamatokkal.

Összegezve megállapítható, hogy míg az alkalmazás-fejlesztés releváns gazdasági túlsúly a „Nyugat”, elsősorban az USA oldalán látszik megjelenni, a humán és nyersanyag-erőforrások tekintetében Kína (és BRICS+ partnerei) van előnyös helyzetben. A tudományos teljesítményt tekintve relatíve még kiegyensúlyozott a verseny.

MI-kihívások

A koppenhágai iskola felosztását tekintve a katonai szektor az állam védelmi kötelezettségeit; a politikai szektor a „társadalmi rend”⁹⁹ védelmét, szuverenitását megőrző feladatait; a gazdasági szektor az állam működéséhez források védelmének biztosítását; a környezeti szektor a természeti környezetet érő, abból származó kockázatokkal kapcsolatos feladatokat; a társadalmi szektor a közösség identitásának védendő elemeit¹⁰⁰ foglalja össze.¹⁰¹

Az állam stabilitását aláásó politikai törekvések egyben szuverenitását is támadják (akár az 5GH keretén belül). Ezért bármely biztonsági szektor tekintetében az azonosított fenyegetések és védelmi lépések érintik a politikai szektort. Ezen átfedések valamennyi szektor vonatkozásában megfigyelhetők.¹⁰² Az MI-alapú védelmi, nemzetbiztonsági megoldások komplex adatszerzési, tartalomgenerálási, kiber- és kinetikus műveletindítási potenciálja az érintett biztonsági szektorok összességének kompromittálására alkalmas lehet olyan hatékonysággal,¹⁰³ amely hagyományos IT-ökoszisztémát és szignifikáns humán közreműködést feltételezve nem lenne megvalósítható.

A világsajtó, a líbiai polgárháború egy epizódja (Békevihar¹⁰⁴) során a török gyártmányú Kargu-2 UAV-ok („lézengő” lövedékek) bevetését már „gyilkos” MI/robot alkalmazásként állította be. Azonban a cikkek alapjául szolgáló ENS-jelentés mindössze a Kargu-2 felhasználásának tényét tartalmazta, és azt a műszaki adatot, hogy ez a drón a kezelővel fenntartott adatkapcsolat nélkül is képes támadást végrehajtani.¹⁰⁵ Mivel a jelentés nem tért ki arra, hogy a bevetések során tényleges emberi felügyelet nélkül cselekedett volna a drónok bármelyike, nem alkalmazható az MI műveleti célú, autonóm jellegű bevetésének bizonyítására. Hasonló helyzet alakult ki az orosz–ukrán konfliktus kapcsán. A média rendszeresen jelentet meg cikkeket, amelyek az MI katonai alkalmazását, az ezzel kapcsolatos, túlnyomórészt ukrán fejlesztők és az országot támogató entitások K+F-erőfeszítéseit jelenítik meg.¹⁰⁶ Kétségtelen, hogy

⁹⁹ Kormányzati ökoszisztéma és az azt legitimáló ideológiák.

¹⁰⁰ Kultúra, nyelv, vallás, struktúrák, összetétel stb.

¹⁰¹ REMEK 2014.

¹⁰² BUZAN – WÆVER – DE WILDE 1998: 141–142.

¹⁰³ A technológia adatfeldolgozó, elemző/értékelő, önfejlesztő, finomhangoló képességeit figyelembe véve.

¹⁰⁴ A Nemzeti Egyetértés Kormányja által, Haftar tábornok csapatai ellen indított 2020. évi hadművelet.

¹⁰⁵ BODE 2024.

¹⁰⁶ BONDAR 2024.

az MI jelentős támogatást nyújthat a drónok számára az elektronikai hadviseléssel szembeni ellenálló képességük növelésére,¹⁰⁷ drónrajok vezérléséhez, jól detektálható célpontok¹⁰⁸ azonosításához. Támogathatják a multimodális¹⁰⁹ (lehetséges) célpont-azonosítást. Elméleti szinten a rejtett objektumok, illetve adott személyek azonosítása sem lehetetlen, azonban a bizonytalansági tényező olyan szinten van, hogy az autonóm csapásvégrehajtás számos, a nemzetközi hadijoggal szembe menő következménnyel járhat. Kiragadott példaként, az ideális feltételek mellett végzett arcazonosítás közel 100%-os hatékonyságú lehet, azonban az ettől eltérő esetekben még a leghatékonyabb algoritmusok esetében is szignifikánsan növekszik az azonosítási hibaarány.¹¹⁰ Rejtett objektumok esetén reális veszély, hogy az ellenfél az elektronikai hadviselés eszköztárát felhasználva hamis célokat telepít, avagy a drónt küldő fél objektumát „festi meg”¹¹¹ úgy, hogy azt „baráti tűz” érje. A humán célpontokat illetően, a biometrikus jellemzők és a ruházat azonosítása kellően bizonytalan ahhoz, hogy kizárólag ezek alapján jogszerű támadást lehessen kezdeményezni – emberi jóváhagyás nélkül.

Összegzés

A vázoltak alapján megállapítható, hogy az MI önmagában nem tekinthető WMD-nek. Azonban a TS keretrendszerében, valós idejű és releváns adatok szinte korlátlan mennyiségéhez és a végrehajtó (például kiterjesztetten értelmezett IoT) technológiákhoz hozzáférve a tömegpusztító fegyverekkel összevethető hatást érhetnek el, így erős védelmi dilemmát generálhatnak, részben a vázolt MI-eszkáláció jelenségén keresztül.

Az MI-eszkáláció kialakulásának két lehetőségét azonosítottam:

- Adott konfliktusokban szemben álló felek által alkalmazott MI-modellek egymásra hatásán keresztül, azaz a beérkező adatok révén, egymás tevékenységét detektálva és elemelve exponenciálisan gyorsuló fejlődési ciklusba lépnek (kvázi GAN jelenség).
- Az LLM-ek technológiai sajátosságaikból fakadóan (nagy tömegű tanító adatbázis) hajlamosak lehetnek a vizsgált konfliktus szélsőséges (nukleáris) eskálálására javaslatot tenni.

Mindezekon felül, az LLM-ek tanító adatkészlete számos olyan információt tartalmazhat, amely lehetővé teszi nagy hatékonyságú kiberfegyverek¹¹² mellett kémiai, biológiai tömegpusztító fegyverek, de akár nukleáris fegyverek kifejlesztését, a vonatkozó

¹⁰⁷ PL. GPS-zavarásokkal szembeni immunitást biztosíthat a drónraj szintű alternatív, MI-támogatású navigációs megoldások alkalmazása.

¹⁰⁸ Nagyobb méretű szárazföldi, tengeri, légi járművek, egyéb műtárgyak.

¹⁰⁹ Komplex, a látható fény és az infravörös tartományban készült videótartalmak, radar- és hőképek, rádióforgalmazás, hangkörnyezet stb. elemzésén alapuló azonosítási eljárások.

¹¹⁰ HAZAI 2024.

¹¹¹ „A” fél, amennyiben ismeretekre tesz szert a „B” fél által alkalmazott objektum MI-algoritmusairól, kihasználhatja azok sérülékenységeit, hogy saját érdekében befolyásolja (pl. offenzív támadás – *evasion attack*) a modell működését. Lásd VAN et al. 2022.

¹¹² PL. dezinformációk nagy sebességű generálása, állandó finomítása. PUSCAS 2024.

kutatások támogatását, gyorsítását, ami számos biztonsági problémát vet fel globális szinten.¹¹³

Habár Kissinger és szerzőtársai jelezték, hogy az MI esetében nehezen megvalósítható a hatékony „MI-fegyverzet korlátozó” szerződések tető alá hozása, szorgalmazták azt, mivel ezek dinamikus és folyamatos kommunikációt feltételeznek az érintett felek között, hozzájárulva világunk stabilitásához. Az MI-fegyverzet-korlátozással kapcsolatos kérdéskörrel összefüggésben arra világítottam rá, hogy már Kissinger szerint sem lehetséges magas biztonsággal azonosítani az ellenfelek tényleges MI-képességeit (szemben például a nukleáris képességekkel), továbbá az MI-technológia tapasztalt¹¹⁴ és egyes kutatók által feltételezetten exponenciálisan gyorsuló fejlődése közel lehetetlenné teszi, hogy az első hidegháborúban megismert jogi instrumentumokkal az MI-fegyvereket szabályozni lehessen.

Mint arra rámutattam, a technológiával kapcsolatosan jelenleg az USA tűnik gazdasági és technológiai területen előnyben lévőnek. Szükséges hozzátenni, hogy a tudományos kutatások területét elemezve Kína az USA-val összevethető eredményeket mutat fel. A Biden-kormányzat egyik utolsó lépéseként kibocsátott, az MI-technológia továbbadását korlátozó jogszabály jelzi, hogy a területen kialakult technológiai, kereskedelmi (nemzetbiztonsági háttérű) konfliktus nem a nyugvópont irányába mozdul el az elkövetkezendő időszakban.

Felhasznált irodalom

- APA (American Psychological Association) (2020): *APA Reaffirms Position on Violent Video Games and Violent Behavior* (Press Release). 2020. március 3. Online: <https://www.apa.org/news/press/releases/2020/03/violent-video-games-behavior>
- ASCHENBRENNER, Leopold (2024): *Situational Awareness: The Decade Ahead*. 2024. június. Online: <https://situational-awareness.ai/>
- BÁNKÚTY-BALOGH Lilla (2022): A mesterséges intelligencia elterjedésének geoökonómiai hatásai és Magyarország. *Külgazdaság*, 66(7–8), 102–130. Online: <https://doi.org/10.47630/KULG.2022.66.7-8.102>
- BODA Mihály (2022): A hibrid háború etikája: az igazságos hibrid háború elmélete. In: M. SZABÓ Miklós (szerk.): *A hadtudomány aktuális kérdései I.* Budapest: Ludovika, 95–109.
- BODA Mihály (2023): Hibrid háború: konfliktusforma a harmonikus béke és a direkt háború között – A hibrid háború katonafilozófiai értelmezése. In: GÖZCE István – PADÁNYI József (szerk.): *Lehelyezett kő: Tanulmányok M. Szabó Miklós emlékére*. Budapest: Ludovika, 21–28.
- BODA Mihály (2024a): A kockázatkerülő háború és a bátorság a 20–21. század fordulóján. *Honvédségi Szemle*, 152(3), 113–125. Online: <https://doi.org/10.35926/HSZ.2024.3.9>

¹¹³ Li et al. 2024.

¹¹⁴ Évente megjelenő új, jelentősen fejlettebb generációk. Lásd ChatGPT. A 2022-es 3.5 modell egy éven belül követte a 4-es, majd ismét egy éven belül a számos benchmarkon az embert leköröző o3.

- BODA Mihály (2024b): A háború mint kaméleon. A fegyvertechnika fejlődésének hatása a háború és a politika viszonyára a kezdetektől a mesterséges intelligenciáig. *Hadtudomány*, 34(3), 99–113. Online: <https://doi.org/10.17047/HADTUD.2024.34.3.99>
- BODE, Ingvild (2024): Emergent Normativity: Communities of Practice, Technology, and Lethal Autonomous Weapon Systems. *Global Studies Quarterly*, 4(1). Online: <https://doi.org/10.1093/isagsq/ksad073>
- BONDAR, Kateryna (2024): Understanding the Military AI Ecosystem of Ukraine. *Center for Strategic and International Studies (report)*, 2024. november 12. Online: <https://www.csis.org/analysis/understanding-military-ai-ecosystem-ukraine>
- BUZAN, Barry (2024): A New Cold War? The Case for a General Concept. *International Politics*, 61, 239–257. Online <https://doi.org/10.1057/s41311-024-00559-8>
- BUZAN, Barry – WÆVER, Ole – DE WILDE, Jaap (1998): *Security: A New Framework for Analysis*. Boulder, Colorado: Lynne Rienner.
- CABALLERO, William N. – JENKINS, Phillip R. (2024): On Large Language Models in National Security Applications. *arXiv:2407.03453v1 [cs.CR]*. Online: <https://doi.org/10.48550/arXiv.2407.03453>
- CAMPBELL, Jamal M. (2021): *Psychological Effects on UAV Operators and Proposed Mitigation Strategies to Combat PTSD (Thesis)*. Monterey (Califronia, USA): Naval Postgraduate School. Online: <https://apps.dtic.mil/sti/trecms/pdf/AD1150884.pdf>
- CHEUNG, Sunny (2024): PRC Adapts Meta's Llama for Military and Security AI Applications. *China Brief*, 24(21). Online: <https://jamestown.org/program/prcs-adaptation-of-open-source-llm-for-military-and-security-purposes/>
- DEPP, Michael (2024): A Blueprint for a Functional China-US Working Group on AI. *The Diplomat*, 2024. április 27. Online: <https://thediplomat.com/2024/04/a-blueprint-for-a-functional-china-us-working-group-on-ai/>
- FRIEDMAN, Thomas L. (2005): It's a Flat World, After All. *The New York Times Magazine*, 2005. április 3. Online: <https://www.nytimes.com/2005/04/03/magazine/its-a-flat-world-after-all.html>
- GAIDA, J. – WONG-LEUNG, J. – ROBIN, S. (2023): *Critical Technology Tracker. Who Is Leading the Critical Technology Race. A Project by the Australian Strategic Policy Institute*. Online: <https://techtracker.aspi.org.au>
- GALLAGHER, Shannon et al. (2023): *A Retrospective in Engineering Large Language Models for National Security*. Carnegie Mellon University Software Engineering Institute. Online: <https://insights.sei.cmu.edu/library/a-retrospective-in-engineering-large-language-models-for-national-security/>
- GLAZER, Elliot et al. (2024): FrontierMath: A Benchmark for Evaluating Advanced Mathematical Reasoning in AI. *arXiv:2411.04872v5 [cs.AI]*. Online: <https://doi.org/10.48550/arXiv.2411.04872>
- HAIG Zsolt (2022): Kibertéri kognitív befolyásolás az információs műveletekben. *Hadtudományi Szemle*, 15(2), 115–130. Online: <https://doi.org/10.32563/hsz.2022.2.7>
- HAZAI Lászlóné (2024): A klasszikus biometriától, biostatistikától az automatikus biometrikus személyazonosság-ellenőrzésig. *Nemzetbiztonsági Szemle*, 12(1), 64–84. Online: <https://doi.org/10.32561/nsz.2024.1.5>

- HENDRYCKS, Dan et al. (2021): Measuring Massive Multitask Language Understanding. *arXiv arXiv:2009.03300v3*. Online: <https://doi.org/10.48550/arXiv.2009.03300>
- HIJAZI, Alaa et al. (2017): Psychological Dimensions of Drone Warfare. *Current Psychology*, 38, 1285–1296. Online: <https://doi.org/10.1007/s12144-017-9684-7>
- KARAHAN, Emir Ali et al. (2024): Deep-Learning Enabled Generalized Inverse Design of Multi-Port Radio-Frequency and Sub-Terahertz Passives and Integrated Circuits. *Nature Communications*, 419, 456–459. Online: <https://doi.org/10.1038/s41467-024-54178-1>
- KASSAI Károly (2022): A kibertér műveleti képesség szerepének, jelentőségének és fókuszának evolúciója a NATO stratégiai dokumentumai alapján. *Military and Intelligence CyberSecurity Research Paper*, (9), 1–38. Online: <http://hdl.handle.net/20.500.12944/100742>
- KIM, Jeff et al. (2023): AI Anxiety: A Comprehensive Analysis of Psychological Factors and Interventions. *SSRN*, 2023. szeptember 15. Online: <https://doi.org/10.2139/ssrn.4573394>
- KISSINGER, Henry A. – ALLISON, Graham (2023): The Path to AI Arms Control. *Foreign Affairs*, 2023. október 13. Online: <https://www.henryakissinger.com/articles/the-path-to-ai-arms-control/>
- KISSINGER, Henry A. – SCHMIDT, Eric – HUTTENLOCHER, Daniel (2023): ChatGPT Heralds an Intellectual Revolution. *The Wall Street Journal*, 2023. február 24. Online: <https://www.henryakissinger.com/articles/chatgpt-heralds-an-intellectual-revolution/>
- KOVÁCS László (2023): *Hadviselés a 21. században: kiberműveletek*. Budapest: Ludovika.
- KOVÁCS Zoltán – GURÁLY Roland (2023): A mesterséges intelligencia és egyéb felforgató technológiák. In KOVÁCS Zoltán (szerk.): *A mesterséges intelligencia és egyéb felforgató technológiák hatásainak átfogó vizsgálata*. Budapest: KNBSZ, 7–26. Online: https://www.knbsz.gov.hu/hu/letoltes/kiadvanyok/01_MI.pdf
- KRAJNC Zoltán főszerk. (2019): *Hadtudományi Lexikon*. Budapest: Dialóg Campus.
- LI, Nathaniel et al. (2024): The WMDP Benchmark: Measuring and Reducing Malicious Use With Unlearning. *arXiv:2403.03218v7 [cs.LG]*, 2024. május 15. Online: <https://doi.org/10.48550/arXiv.2403.03218>
- LIU, Yang et al. (2024): Advancements in Brain-Machine Interfaces for Application in the Metaverse. *Frontiers in Systems Neuroscience*, (18). Online: <https://doi.org/10.3389/fnins.2024.1383319>
- MADIEGA, Tambiama (2023): *General-Purpose Artificial Intelligence*. European Parliamentary Research Service, 2023. március. Online: [https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/745708/EPRS_ATA\(2023\)745708_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/745708/EPRS_ATA(2023)745708_EN.pdf)
- MAURER, John D. (2018): The Purposes of Arms Control. *Texas National Security Review*, 2(1), 8–27. Online: <http://dx.doi.org/10.26153/tsw/870>
- MCCAIN, Abby (2023): How Fast Is Technology Advancing? Growing, Evolving, and Accelerating at Exponential Rates. *ZIPPIA*, 2023. január 11. Online: <https://www.zippia.com/advice/how-fast-is-technology-advancing/>
- NITZBERG, Alex (2024): Autonomous Systems and Weapons Company Anduril Announces Plan to Build Massive Manufacturing Facility in Ohio. *FOXBusiness*, 2025. január 16. Online: <https://www.foxbusiness.com/fox-news-military/>

autonomous-systems-weapons-company-anduril-announces-plan-build-massive-manufacturing-facility-ohio

- OLLÁRI Viktor (2024a): A technológiai szingularitás egyes biztonsági kihívásai. *Nemzetbiztonsági Szemle*, 12(3), 64–81. Online: <https://doi.org/10.32561/nsz.2024.3.5>
- OLLÁRI Viktor (2024b): Certain Geopolitical Insights into the Technological Singularity. In *Proceedings of the International Conference on National and International Security*. 2024. október 17–18., 239–256. Online: <https://doi.org/10.52651/nmb.c.2024.9788080406738.239-256>
- OLLÁRI Viktor – SURÁNYI Zsolt (2024): A mesterséges intelligencia alkalmazásának egyes kérdőjelei. *Honvédtörvény*, 76(3–4), 75–92. Online: <https://doi.org/10.29068/HO.2024.3-4.73-90>
- PUSCAS, Ioana (2024): Large Language Models and International Security. *UNIDIR*, 2024. november 11. Online: https://unidir.org/wp-content/uploads/2024/11/large_language_models_web-1.pdf
- REIN, David et al. (2023): GPQA: A Graduate-Level Google-Proof Q&A Benchmark. *arXiv arXiv:2311.12022v1*. Online: <https://doi.org/10.48550/arXiv.2311.12022>
- ROY, Nicolas – COLL, Michel-Pierre (2024): Empathy: Exploring the Impact of Violence in Video Games. *eLife*, 13. Online: <https://doi.org/10.7554/eLife.94949>
- QURESHI, Waseem A. (2019): Fourth- and Fifth-Generation Warfare: Technology and Perceptions. *San Diego International Law Journal*, 21(1). Online: <https://digital.sandiego.edu/ilj/vol21/iss1/7>
- REMEK Éva (2014): Mekkora a „biztonságunk árnyéka” globalizált világunkban? In BORDÁS Sándor – GLAVANOVICS Éva (szerk.): *Nemzeti és etnikai konfliktusok a Kárpát-medencében*. Székesfehérvár: Kodolányi János Főiskola, 67–78. Online: <https://www.kodolanyi.hu/jol-let/images/tartalom/File/publikaciok/Nemzeti-es-etnikai-konfliktusok.pdf>
- RIVERA, Juan-Pablo et al. (2024): Escalation Risks from Language Models in Military and Diplomatic Decision-Making. In *FAccT '24: Proceedings of the 2024 ACM Conference on Fairness, Accountability, and Transparency*, 836–898. Online: <https://doi.org/10.1145/3630106.3658942>
- RODRÍGUEZ, Elio Quiroga (2024): Critical Analysis of a Militaristic Approach in the Context of Agi: A Postcolonial Perspective. *AI & Society*, 40, 2335–2337. Online: <https://doi.org/10.1007/s00146-024-02069-w>
- SEEWALD, A. K. (2022): A Criticism of the Technological Singularity. In DINGLI, A. et al. (szerk.): *Disruptive Technologies in Media, Arts and Design*. Springer, 91–119. Online: https://doi.org/10.1007/978-3-030-93780-5_8
- SINGH, P. R. et al. (2023): 6G Networks for Artificial Intelligence-Enabled Smart Cities Applications: A Scoping Review. *Telematics and Informatics Reports*, 9, 100044. Online: <https://doi.org/10.1016/j.teler.2023.100044>
- SCHMIDT, Eric (2023): Innovation Power: Why Technology Will Define the Future of Geopolitics. *Foreign Affairs*, 102(2), 38–52. Online: <https://heinonline.org/HOL/P?h=hein.journals/fora102&i=256>

- SINGH, Rohit et al. (2024): Towards 6G Evolution: Three Enhancements, Three Innovations, and Three Major Challenges. *IEEE Network*, 2025. május 29. Online: <https://doi.org/10.1109/MNET.2025.3574717>
- TÓTH András (2023): Az 5G-technológia jellemzői és a kialakításában rejlő kihívások. In TÓTH András (szerk.): *Új típusú kihívások az infokommunikációban*. Budapest: Ludovika, 51–98.
- ULAM, Stanislaw (1958): *John von Neumann*. Rhode Island (USA): American Mathematical Society.
- URISTA, Timothy (2024): The Rapid Rise of 'o3': A New Turning Point in the AGI Debate. *AI Advances*, 2024. december 21. Online: <https://ai.gopubby.com/the-rapid-rise-of-o3-a-new-turning-point-in-the-agi-debate-45c04177ac4f>
- VAN, Min-Hao (2022): Defending Evasion Attacks via Adversarially Adaptive Training. *2022 IEEE International Conference on Big Data (Big Data)*, 1515–1524. Online: <https://doi.org/10.1109/BigData55660.2022.10020474>
- WIGGERS, Kyle et al. (2025): ChatGPT: Everything You Need to Know About the Ai-Powered Chatbot. *Tech Crunch*, 2025. január 3. Online: <https://techcrunch.com/2025/01/03/chatgpt-everything-to-know-about-the-ai-chatbot/>
- XUE, Zhiwei et al. (2024): Fully Forward Mode Training for Optical Neural Networks. *Nature*, 632, 280–286. Online: <https://doi.org/10.1038/s41586-024-07687-4>