NEMZETBIZTONSÁGI SZEMLE
12. évfolyam (2024) 3. szám 64–81. | DOI: 10.32561/nsz.2024.3.5

Ollári Viktor[1]

A technológiai szingularitás egyes biztonsági kihívásai

Certain Security Issues of the Technological Singularity

A 21. század második évtizedére a mindennapi életünket átszövő infokommunikáció kínálta lehetőségek mellett a vonatkozó kihívások száma is jelentősen megnövekedett, új – gazdasági és a biztonság más szféráit érintő – frontot nyitva az államok közötti versengésekben. A hardvertechnológia fejlődése a 2010-es években új lendületet adott a mesterséges intelligencia (MI) alap- és alkalmazott kutatásoknak, az MI-alkalmazások intenzív terjedésének. 2022 a nagy nyelvi modellek (Large Language Model, LLM) terén hozott figyelemre méltó áttörést. Az MI-potenciál, fuzionálva a nagy tömegű, valós idejű adatokat generáló technológiákkal (például IoT) és az információk továbbítását biztosító, tervezetten „mindenhol jelen lévő" infokommunikáció technológiai IKT-megoldásokkal (5G/6G), kézközelbe hozta a technológiai szingularitást (TS). Jelen tanulmányban a vonatkozó szakirodalom elemzése útján a TS biztonságunkra gyakorolt egyes hatásait vizsgáltam, rámutatva, hogy a TS viszonylatában elégtelen korunk biztonsági/kibervédelmi megközelítése.

Kulcsszavak: *technológiai szingularitás, mesterséges intelligencia, 5G/6G, nemzeti biztonság*

The second decade of the 21st century brought the pre-technological singularity (TS) era when ICT solutions infiltrated all the verticals of our lives offering a plethora of possibilities and posing an unpredictable number of challenges. They have been initiating novel – economy, security etc. – frontlines in interstate competition. The new hardware technologies sped up the research of Artificial Intelligence (AI) and the global penetration of AI-based solutions for a tremendous number of use cases. 2022 brought a breakthrough in R&D and the use of Large Language Models (LLMs). The potential embodied in AI, its fusion with massive real-time data generating technologies (IoT) and ubiquitous ICT eco-system (5G/6G) brought the TS in tangible proximity, making

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

a profound effect on our world's security. Certain aspects of security issues and the effects of TS are examined in this paper by analysing the relevant literature, illustrating the limitations of the present security/cyber defence approach to TS.

***Keywords**: technological singularity, Artificial Intelligence, 5G/6G, national security*

Bevezető

Az emberiség technológiai fejlődése, nagy valószínűséggel, a jelenleg ismert trendek mentén halad majd tovább az elkövetkező évtizedben. Ezért joggal feltételezhető, hogy jelenünk és a közeljövő K+F-eredményeinek – kiemelten az úgynevezett feltörekvő és áttörést hozó és kritikus technológiák – szinergiája megalapozza az „önfejlesztő" ökoszisztémák korszakát, ami már joggal tekinthető a Neumann János által megjövendölt szingularitásnak. Meglátásom szerint a technológiai szingularitás (TS) – leszűkítve a szóba jöhető technológiák körét a ma már elérhetőkre – az alábbi három technológia szimbiózisának eredményeként szökkenhet szárba:

- a mesterséges intelligencia (MI) egyértelműen a TS elemző/tervező/szervező/irányító szegmensét képezi;
- az újgenerációs infokommunikációs megoldások, amelyek alatt az 5G és annak utódgenerációs (6G) ökoszisztémáit értem, amelyek
  - a szabványaikban foglaltan széles körű lefedettség mellett biztosítanak kiemelkedően gyors, nagy tömegű adatátvitelt, exponenciálisan növekvő számú felkapcsolódó eszköz számára;
  - alapját képezik az MI és az adatgyűjtő/feladat-végrehajtó ökoszisztéma közti stabil, nagy sebességű adatáramlásnak;
- a dolgok internete (IoT-) megoldások biztosítják az MI irányító „szerepkörében" kiadott utasításainak végrehajtását, illetve generálják (egyebek mellett) az MI elemző/tervező funkcióit támogató, folyamatosan frissülő, valós idejű adatfolyamok sokaságát.

Az általam TS-triádként említett MI – 5G/6G – IoT egyes kiber- és nemzetbiztonsági jellemzőivel számos szakértő foglalkozott részletesen. A vonatkozó szakirodalom, valamint hazai és nemzetközi szabályozók megvizsgálása, elemzése révén igazolni kívánom, hogy korunk biztonsági / kibervédelmi megközelítése nem elégséges a TS kockázatainak hatékony kezeléséhez. Célom a TS biztonságunkra gyakorolt lehetséges hatásainak felvázolása, még ha ezzel szembe is megyek Vernor Vinge (1993) megállapításával, amely szerint a TS alapvetően változtatja meg jövőnk alakulásának feltételrendszerét, így meglévő ismereteinkre csak mérsékelten alapozhatunk.

Technológiai szingularitás

Neumann János szerint a technológiai fejlődés szükségszerűen elér egy olyan pontot, amelynél a technológiák szinergiája paradigmaváltást indukál, amelyet követően „az emberi

élet, ahogyan azt eddig ismertük, nem folytatódhat."[2] Vizsgálataim során a megalapozó technológiák szinergiáiban rejlő lehetőségekre utalva, a TS transzhumanizmus[3]-mentes, az Ipar 4.0/5.0-val összefüggésben vázolt kritériumokkal[4] összhangban álló meghatározását veszem alapul, amely szerint „az MI egy adott ponton képessé válik önmaga rekurzív fejlesztésére, önmagánál fejlettebb megoldások (gépek/mesterséges entitások) létrehozására".[5]

A TS-megalapozó EDT-triád

A NATO szakértői csoportja 2020-ban publikált írásában az elsődleges stratégiai célok közé sorolta az MI és újgenerációs IKT-megoldásokat is felölelő EDTk[6] (feltörekvő és áttörést hozó technológiák) terén megvalósítandó dominanciát a szövetség számára.[7]

Korunk K+F+I-aktivitásai az emberi kreativitás mellett egyre inkább függenek az MI nyújtotta ráfordított idő- és erőforrás-csökkentő támogatásától, az MI pedig akkor képes szolgálatásainak „javát nyújtani", amennyiben a megfelelő minőségű és mennyiségű (például IoT-forrásból származó) adat, valamint azok begyűjtését és továbbítását biztosító kommunikációs közeg (5G/6G ökoszisztéma) a rendelkezésére áll. Röviden tekintsük át az érintett technológiák főbb jellemzőit.

IoT

Kiterjesztően értelmezve az IoT meghatározását – minden olyan eszköz, amely képes egymással kommunikálva infrastruktúrát alkotni, hozzáférést biztosítva az egyes infrastruktúra-elemek által generált/gyűjtött adatokhoz és/vagy aktuátorként működni – e kategóriához sorolható az összes, kommunikációs ökoszisztémához csatlakozni, valamint adatgyűjtésre, -létrehozásra vagy -megosztásra képes megoldás.[8] Azaz minden úgynevezett okoseszköz, környezeti paraméterek elemzését szolgáló megoldás, az okos-ökoszisztémák (-otthon, -város), a sor még hosszan folytatható, hiszen napjaink legtöbb IT-/IKT-eszköze valamilyen szinten az IoT-hoz sorolható. Egyes felmérések szerint 2023-ban 15,14 milliárd IoT-termék üzemelt, az előrejelzések szerint 2030-ban megközelítőleg 30 milliárd lesz mindennapi használatban, amiből 8 milliárdot alkalmaznak üzleti/ipari rendszerekben.[9] A 6G esetében már számolnak az emberi testen viselt vagy beültetett (például egészségügyi) IoT-eszközökkel is.[10]

---

2 Ulam 1958: 6.
3 Ember-gép fúzió, az emberi tudat tovább létezése virtuális ökoszisztémákban. Kurzweil 2014.
4 Germany: Industrie 4.0 2017.
5 Seewald 2022: 94–95.
6 MI, autonóm rendszerek, kvantum-, űr- és biotechnológiák, hiperszonikus rendszerek, új anyagok és gyártási eljárások, energia és meghajtás, újgenerációs kommunikációs hálózatok. Lásd Reding–Eaton 2020; NATO 2023.
7 Siposné Kecskeméthy 2021: 8.
8 Tóth 2023a: 99.
9 Vailshery 2023.
10 Lásd Rajasekaran 2024.

5G/6G

A szabványalkotók már alapvetően egy, az ipari alkalmazásokat – ide sorolva az IoT-jellegű technológiákat – eredendően támogató kommunikációs technológia megalkotását tűzték ki célul az 5G tervezése során. A kibertér egyre jelentősebb összetevőjeként az újgenerációs mobil IKT-hálózatok „adat-érhálózat" jellegű funkcióval rendelkeznek már ma is, amely szerep a TS-ben kiteljesedik.

Biztonság és architektúra szempontjából kiemelendő, hogy a 3G még alapvetően célhardverekre épülő megoldás volt, a 4G-ben megkezdődött egyes hálózati funkciók informatikai alapokra helyezése, az 5G esetében már alapvetően számoltak a standard (kereskedelmi forgalomban elérhető) IT-hardverek alkalmazásával, mindezt kiegészítve a szoftverizáció és virtualizáció funkcióival. Az 5G és utódgenerációi esetében a nagy pontosságú helymeghatározás, nagy sebességgel és/vagy nagy magasságban mozgó végponti készülékek kiszolgálása is jelentős szerepet kap. Az 5G képességportfoliója három jellemző felhasználási forgatókönyv köré csoportosítható:[11]

- nagyszámú felcsatlakoztatott IKT-megoldás (gép-gép és IoT-kommunikáció) kiszolgálása (Massive Machine Type Communications, mMTC);
- nagy sebességű adatátvitel (Enhanced Mobile Broadband, eMBB);
- megbízható, rövid késleltetési idejű kommunikáció (Ultra Reliable Low Latency Communications, uRLLC).

Az 5G esetében távlati cél, a 6G-nél (ITU IMT-2030)[12] elvárás, hogy a szolgáltatás úgyszólván mindenhol jelen legyen. A szabványokban megfogalmazott hálózati topológia kialakítása már az 5G esetében is ennek jegyében történt, alapozva az üvegszálas jeltovábbítási gerinchálózatokra, tervezve a különböző méretű cellák (makro/mikro/piko/femto) integrálásával, megosztott antennarendszerek alkalmazásával stb.[13] A 6G – az ITU/3GPP/ETSI ajánlások, műszaki leírások szerint – már „születetten inkluzív", azaz tervez a műholdas[14] és nagymagasságú (18–22 km) platformrendszerek (HAPS),[15] szolgáltatófüggetlen (ad hoc) és a wifi-hálózatok integrálásával.[16] A 3GGP szabvány 18-as verziója – bázisállomások telepítési korlátaira, az elérhető frekvenciatartományokra, a rádiójel terjedésének sajátosságaira, a hálózat energiaigényére stb. tekintettel – már az 5G-nél is vizsgálja az MI alkalmazásának lehetőségeit.[17]

Mesterséges intelligencia

Hasonlatosan az emberi intelligenciához, az MI sem rendelkezik globálisan elfogadott definícióval. Az EU MI Rendelete, az OECD definíciójára építve, az MI-t olyan gép alapú

11 Tóth 2023b.
12 A Nemzetközi Telekommunikációs Unió *(International Telecommunication Union, ITU)* IMT-2030 néven hivatkozik a következő generációs mobil telekommunikációs technológiára (6G).
13 Farkas 2023: 24.
14 Tóth 2023b: 55.
15 Jellemzően drónokra tervezett bázisállomások.
16 Liu et al. 2024.
17 Lásd: www.3gpp.org/ftp/Inbox/Marcoms/3GPP_Poster%20v2.pdf

rendszernek írja le, „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".[18]

A NATO Foundation Defense College szerint az MI

> „a gépek azon képessége, hogy adott feladatokhoz kapcsolódóan, bizonyos fokú önállósággal utánozzák az emberi agy problémamegoldó és döntéshozatali folyamatait, nagy mennyiségű információ nagy sebességgel történő feldolgozásával, a (1) szoftverek, (2) algoritmusok és mély neurális hálózatok képességeinek kiaknázásával, valamint egyre növekvő mennyiségű (3) adat (úgynevezett MI Triád) felhasználásával".[19]

Az MI-generációk kapcsán két fő fejlesztési hullámot azonosítanak a kutatók:[20]

1. „gyenge"/„szűk" MI (ANI) – a napjainkban alkalmazott, strukturált adatkészletek segítségével feltanított, funkcióspecifikus (például adatelemző, -feldolgozó, -azonosító, következtető és döntéstámogató algoritmusok stb.) megoldások;
2. „erős"/„általános" MI (AGI) – például a nagy nyelvi modellek (OpenAI ChatGPT) dinamikus terjedésével és fejlődésével „kézközeli" távolságra kerülő, az emberi intelligencia képességeivel felvértezett, már nem címkézett adatkészletekkel „tanított", magas szintű absztraháló potenciállal felvértezett algoritmuskomplexumok.

A fentieket kibontva, az MI

- folyamatosan frissülő adatokkal rendelkezik „működési területéről", valamint a működését befolyásoló egyéb tényezőkről,
  - ezeket biztosítják számára, és/vagy detektálva fizikai és virtuális környezetét begyűjti azokat;
- a rendelkezésére álló adatokat információvá alakítva képes döntéseket hozni, ide sorolva tanulási/önfejlesztő rutinjait is;
- döntései változást generáló folyamatokat indíthatnak el a valós és/vagy a kibertérben.

A harmadik fejlődési lépcső, a mesterséges szuperintelligencia, amely a feltételezések szerint jelentősen meghaladja az emberi intelligenciát.[21] Ennek eléréséhez nyithat ajtót a nagy nyelvi modellek (LLM) alkalmazása, amelyek felhasználási lehetőségei, szemantikai és szentimentelemző kapacitásaik okán, számtalan egyéb terület mellett kiterjedhetnek a honvédelemre, a rendvédelemre, a kibervédelemre, illetve a tudomány és oktatás világára. Az elmúlt évtizedben, a benne rejlő potenciált felismerve, az üzleti szféra magához vonzotta a tudományos világ kiemelkedő kutatóit, és dominánssá vált az MI K+F+I-ben, megalapozva a technológia globális társadalmi penetrációjának robbanásszerű növekedését. Erősödő trend az MI bevonása az alkotó jellegű kutatásokba

18 2021/0106(COD) 5662/24 2024.
19 Berger 2021: 4.
20 Bánkuty-Balogh 2022: 104–106.
21 Kovács–Gurály 2023: 13.

(új antitestek megalkotása, hidrogénfúzió stb.).[22] Mindemellett, számos kutató figyelmeztet az általuk megtestesített veszélyekre.[23]

A kibertér és a TS

A TS vonatkozásában a kibertér megkerülhetetlen fogalom, amely az MI-hez hasonlóan nem rendelkezik egységesen elfogadott definícióval. William Gibson vízióiban[24] egy az emberiség adatvagyonának menedzselését szolgáló szimulációs mátrixként jelenik meg.

Az ENSZ fogalomtára[25] szerint a kibertér „az elektronikus kommunikáció fiktív vagy virtuális környezete, melynek legismertebb megjelenési formája az Internet". A világszervezet Leszerelési Kutatóintézetének 2023-as tanulmánya,[26] illetve a Tallinni kézikönyv[27] Kuehl (2009) definícióját idézi, amely szerint a kibertér „az informatikai ökoszisztéma egy az egész bolygóra kiterjedő (globális) tartománya. […] az infokommunikációs technológiákra épülő, egymástól függő és egymáshoz kapcsolódó hálózatok révén, elektronikai infrastruktúra és az elektromágneses spektrum felhasználásával létrehoz, tárol, módosít, cserél és kiaknáz információkat."[28]

Az Európai Unió[29] az USA Nemzetbiztonsági Ügynöksége keretén belül működő CNSS[30] definícióját vette alapul, amely a kiberteret „az információs környezet az egymástól kölcsönösen függő információs rendszer infrastruktúrák – ideértve az Internetet, a telekommunikációs és számítógép hálózatokat, valamint az integrált adatfeldolgozó és -irányító/ellenőrző megoldásokat – globális tartományaként" írja le.[31]

A NATO AJP-3.20 doktrínája kiterjesztő jelleggel „összekapcsolt, valamint a sziget jellegűen üzemelő kommunikációs, információtechnológiai vagy egyéb elektronikus rendszereket és hálózatokat, valamint az ezekben tárolt/továbbított/feldolgozott adatokat felölelő tartományként" határozza meg a kiberteret. A NATO Kooperatív Kibervédelmi Kiválóságközpontjának szakértői a doktrína háromrétegű – fizikai (hardver), logikai (szoftverek, protokollok, alkalmazások stb.), kiberszemélyiség (felhasználói valós és virtuális entitások)[32] – modellel összhangban „összekapcsolt információs rendszerek és a velük interakcióban álló felhasználók időfüggő halmazaként" írják le a kiberteret.[33]

Az MH Kibervédelmi Szakmai Koncepciójában a kibertér „az elektromágneses spektrum használatával meghatározható, dinamikusan változó tartomány, mely az összekapcsolt hálózatok, eszközök és kiegészítő fizikai infrastruktúrák közötti adatok kezelésére szolgál".[34] A jelenleg hatályos Nemzeti Kiberbiztonsági Stratégia (NKS) szerint a kiber-

22 Maslej et al. 2023.
23 Madiega 2023.
24 Burning Chrome, Neuromancer (1982).
25 Lásd: https://publicadministration.un.org/egovkb/en-us/Resources/Glossary#c
26 UNIDIR 2023.
27 Schmitt 2017: 258.
28 Kuehl 2009: 27.
29 Az EU kiberfenyegetésekkel szembeni cselekvési forgatókönyve.
30 Az USA kormányzati szerveinek IKT biztonságiszabályzat-alkotó bizottsága.
31 Lásd: www.niap-ccevs.org/Ref/CNSSI_4009.pdf
32 Haig 2022: 119.
33 Ottis–Lorents 2010: 267.
34 60/2013. (IX. 30.) HM utasítás 2. fejezet, 8. pont.

tér „globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét jelenti”.[35]

Az idézett definíciók közös halmazát a kibertér fizikai hálózati szegmense alkotja, rávilágítva arra, hogy aki képes ellenőrizni a hálózat csomópontjait – PC, szerver, okostelefon stb. –, a köztük húzódó kommunikációs csatornát, az a maga javára fordíthatja az ezeken tárolt/feldolgozott/továbbított információt.[36] A kibertér külső (fizikai/földrajzi) határait keresve szembesülhetünk néhány kihívással. Az egyre növekvő számú felhasználó igényeit kiszolgálandó, a földi/földközeli IKT-infrastruktúra-elemek száma dinamikusan növekszik, ezzel a kibertér kiterjedését is változtatva. A kibertér legkülső tartománya, kiterjesztően alkalmazva a NATO AJP-3.20-at, a csillagközi tér lehet, köszönhetően a Voyager-1 és Voyager-2 űrszondáknak.

Társadalomföldrajzi megközelítésből, ha nincs jelen tudatos entitás adott időpontban a kibertér vizsgált részén és/vagy nem történik adatgenerálás, -módosulás, -továbbítás vagy -hasznosulás, „akkor és ott” a vizsgált „térrész” tekinthető-e a kibertér elemének? Analógiaként alkalmazva Pirisi–Trócsányi (2019) azon megállapítását, amely szerint a térstruktúrák a természeti környezet és az emberi közösségek interakciós ökoszisztémájának dinamikus egymásra hatásából jönnek létre[37] igazolható, hogy a kibertér – formája és térszerkezete alapján – dinamikus („organikus”) jellemzőkkel írható le,[38] tér és idő szempontjából egyszerre pontszerű és „végtelen”.[39] A Pirisi–Trócsányi által vázolt humáncentrikus térértelmezési modell a földrajzi tér részeként ábrázolja a „cseppfolyós” jellegű kiberteret, amelyet a felhasználói igények/érdekek pillanatról pillanatra alakítanak.[40]

A fent vázoltak alapján a kibertér kettős minőségű szféraként írható le. Az IKT-infrastruktúrák (elektronikai hadviselés)[41] irányából vizsgálva a kibertér határai viszonylag pontosan megjelölhetők – az ember alkotta IKT-ökoszisztéma legkülső perifériája. Társadalomföldrajzi megközelítések (valamint a védelmi, nemzetbiztonsági befolyásolási műveletek)[42] irányából vizsgálódva, az interakciók mennyiségét/minőségét elemezve a kibertér egy organikus, pillanatról pillanatra változó ökoszisztéma, amely egyszerre képezi majd a TS idegi és érhálózatát.

A TS egyes biztonsági kérdései

Mivel a TS hatása várhatóan kiterjed majd az emberi létezés szinte valamennyi síkjára, biztonsági kihívásai/kockázatai igen összetett kérdéskört képeznek, ide sorolva a technológiai fejlődés kényszerét, ami végigkíséri az emberiség történelmét a bronzötvözés-technológiától az MI kiaknázásáig.[43] Amely közösség figyelmen kívül hagyta környezete jelentős innovációs

35 1139/2013. (III. 21.) Korm. határozat.
36 Adams 2024: 19.
37 Pirisi–Trócsányi 2019: 40.
38 Kelemen 2023: 77.
39 Mészáros 2001.
40 Pirisi–Trócsányi 2019: 61–62.
41 Haig et al. 2014.
42 Haig 2018: 180.
43 Schmidt 2023: 41.

áramlatait, annak nyomásgyakorló képessége erodálódott és geopolitikai, geoökonómiai hátrányba került. Kommunikációra épülő világunkban a „fejlődési kényszer" példájaként említhető a „célközönség gondolatainak, véleményének átalakítására, valamint meggyőzésére, esetleg manipulálására" hangsúlyt fektető adaptív információs fölény (AIF) elérését biztosító ismeretek, eljárások és technológiák birtoklása,[44] mivel a TS-triád szimbiózisa az AIF folyamatosan növekvő hatékonyságú, új eljárásainak automatikus kidolgozását biztosíthatja; amely állam „nem kíván" élni e lehetőséggel, bizonyosan hátrányba kerül.

Elméleti megközelítés

A biztonsági jelentését vizsgálva, a *Közszolgálati online lexikon* szerint a biztonság „egyrészt a veszély és fenyegetések hiányát, másrészt a veszély és a fenyegetések elhárításának képességét jelenti". A „tér" meghatározó jellegét szem előtt tartva, a biztonság egy érzet, amelynek milyenségét meghatározza, hogy az egyén mely társadalom, kultúra vagy szubkultúra részese, mivel a „biztonság" teljesen mást jelent egy budapesti, fokvárosi vagy jeruzsálemi lakos számára.

A koppenhágai iskola öt szektoron (katonai, politikai, társadalmi, gazdasági, környezeti) keresztül értelmezi a biztonságot. A katonai szektor jeleníti meg az állam azon feladatait, amelyek a területének és lakosságának védelmét célozzák, és alapvetően befolyásolják úgy az egyén, mint egyéb entitások (például gazdálkodó szervezetek) szubjektív biztonságérzetét. A politikai szektor a társadalmi rend (kormányzati rendszerek és az „ezeket legitimáló ideológiák") biztonságáról, szuverenitásának megőrzéséről szól. A gazdasági szektor biztosítja a forrásokat az állam és a társadalom egészséges működéséhez; diszfunkcionálissá válása – akár katonai beavatkozás vagy belső társadalmi feszültségek nélkül is – előidézheti a „bukott állam" állapotot. A környezeti szektor alapvetően az ember természeti környezetét érő, abból származó kockázatokat (klímaváltozás, környezetszennyezések stb.) foglalja magában. A társadalmi szektor a közösség identitását (kultúra, nyelv, vallás, struktúrák, összetétel stb.) érintő kihívásokat öleli fel.[45]

Buzan a politikai szektor kapcsán kifejti, egy állam stabilitását célzó politikai fenyegetések alapvetően a szuverenitásának intaktságát igyekeznek aláásni, így valamennyi szektor fenyegetései és az azok elhárítására tett lépések címkézhetők politikainak is.[46] A katonai szektort érintően fegyveres erők expedíciós alkalmazása (például Szahel-övezet) gazdasági és társadalmi célzattal is történhet; a környezeti szektor adott küszöbértéket meghaladó eseményei (például tartós szárazság vagy árvizek) kihatással lehetnek valamennyi szektorra; és ez elmondható a gazdasági szektor vonatkozásában is. A „koppenhágai" öt szektor vonatkozásában közös „platformként" tekinthetünk a kibertérre, amely az elmúlt 30+ évben exponenciálisan növekvő hatást gyakorol azokra, és ezek a szektorok is hatnak a kibertérre, így az egyes szektorok közti (amúgy is illékony) határvonalak egyre „illuzórikusabbá" válnak.

A társadalmi szektorhoz tartozóan kiemelt problémaként jelentkezik a kibertéri agresszió, amely ma már nemcsak az anonimitás kiaknázást jelenti, de az egymást

44 Haig 2022: 116.
45 Remek 2014: 69–76.
46 Buzan et al. 1998: 141–142.

„ismerő" entitások offline viszonyaiba is átszivárog.[47] A kiberagressziót vizsgáló 8-faktoros (Cyber-MAD[48]) modell az általános emberi agressziót kiváltó okok mellett kitér a virtuális személyiség zavaraira is.[49] A Cyber-MAD mint elnevezés összecseng az 1960–1970-es években kikristályosodott nukleáris doktrínákkal,[50] hiszen az állatvilágból magunkkal hozott alapvető csoportdinamikai sajátosság a túlzott erőszak közösségbomlasztó hatása, amely a közösség és az egyed túlélési képeségeit egyaránt lecsökkenti.[51]

Speciális megközelítés

Jelenünk egyre gyakrabban használt biztonságpolitikai kifejezése a II. hidegháború. Egyesek ennek kezdetét a 2014-es ukrán–orosz konfliktustól datálják, míg mások amellett érvelnek, hogy a Kína–USA (leginkább gazdasági) kapcsolatok feszültebbé válásától (2018) számítandó. Azonban, mint arra többen rámutatnak, a Kína–USA gazdasági konfliktus nem felel meg a hidegháború definíciójának; mivel bár elkezdődött a világ blokkosodása (Kína–Oroszország), a „Globális Délért" folyó küzdelem, de valós ideológiai különbségek nem alakultak ki, és a „blokkok" túl sok szálon kötődtek egymáshoz.[52]

Buzan megállapítja, az „I. hidegháború" meghatározó eleme a két blokk vezető hatalmainál felhalmozott tömegpusztító fegyverek (*weapon of mass destruction,* WMD) mennyisége, ami arra szorította őket, hogy következetesen kerüljék a közvetlen konfliktust, mivel a földi élet végét jelenthette volna egy nukleáris eszkaláció (erős védelmi dilemma), így az elrettentés és az elkerülés került a katonai stratégiák fókuszába. Buzan további kritériumként határozza meg a felek közti ideológiai különbséget, és azt, hogy ezen ideológiákért akár harcolni is hajlandók voltak. Mivel jelenünk konfliktusainak egyenletéből hiányzik a zéróösszegű ideológiai polarizáció, ezek „küzdelemre érdemes vitává" minősülnek, aminek tárgya lehet a gazdasági, kulturális és politikai hatalom.

Vizsgálható kérdés, hogy a TS – és annak megalapozó technológiái, kiemelten az MI – képes-e a tömegpusztító fegyverekkel analóg „erős védelmi dilemmát" generálni. A tömegpusztító fegyverek hatását illetően az emberiség tényleges és publikus tapasztalatokkal rendelkezik, ami az MI-ről nem mondható még el. Bár a világsajtó „gyilkos" MI/robotként említette a líbiai polgárháborúban (2020) bevetett Kargu-2 UAV-t, a citált ENSZ-jelentés csak a drón jelenlétét és műszaki paramétereit rögzítette, ami szerint az a kezelővel fenntartott adatkapcsolat híján is képes támadást végrehajtani.[53]

Reális a TS/MI besorolása a WMD-kategóriába? A *Hadtudományi lexikon* szócikke szerint WMD-nek tekintendő minden olyan megoldás, amely „a többi fegyverhez képest, azonos körülmények esetén, hatásaik sajátos jellegénél és méreteinél fogva, viszonylag rövid idő alatt rendkívül nagymértékű pusztítást okoznak az élőerőben, a haditechnikai

47 Kopecký–René 2017.
48 Cyber Motivations for Aggression and Deviance – az agresszió és deviencia kibermotivációi.
49 DeMarisco et al. 2021.
50 R. S. McNamara „garantált pusztítás" doktrínájának (1965) jegyeit mutató „stratégiai elégségesség" doktrína (1971) kritikájában jelent meg először a *„Kölcsönösen garantált pusztítás (MAD)"* kifejezés. – Brennan 1971.
51 Csányi 2004: 303.
52 Buzan 2024.
53 Bode 2024.

eszközökben, az épületekben, valamint más létesítményekben".[54] Egy orvosi/egészségügyi megközelítés szerint olyan „kémiai, biológiai és radiológiai eszközök, melyek kis mennyiségben is képesek halált okozni; a túlélők egészségét pedig hosszútávon és súlyosan befolyásolják".[55] Az ENSZ szakértői bizottságának definíciója szerint WMD az „atombomba, a radioaktív anyagból készült fegyverek, halálos kémiai és biológiai fegyverek; továbbá valamennyi, jövőben kifejlesztésre kerülő fegyver, melynek pusztítóhatása összevethető az atombombáéval, vagy a felsorolt fegyverek egyikével".[56]

Habár közvetlen hatás tekintetében – amit ma még leginkább túl- vagy alábecsülni tudunk, mivel a „Gartner-féle szenzáció görbe" első harmadánál tart –[57] az MI nem szükségszerűen felel meg a fenti definícióknak, számos kockázat azonosítható. A generatív MI-modellek alkalmazhatósági palettája és az ezekre épülő megoldások – kiemelve a katonai, államigazgatási, gazdasági szakértői, döntéstámogató és automatizált döntéshozó rendszereket, tudományos (például biológiai/orvosi/gyógyszer) kutatásokat támogató rendszereket – alkalmazásának feltétele egyfajta bizalom megléte a technológia alkalmazói, üzemeltetői és a végfelhasználók részéről.[58] Az MI integrálásának lehetőségét a civil és katonai döntéshozatali mechanizmusba számos kormány aktívan vizsgálja, amely folyamat új lendületet kapott a generatív modellek megjelenésével. E törekvéseket Rivera és társai[59] kutatásainak tükrében érdemes értékelni: a kísérlet során öt LLM (GPT-4, GPT-3.5, Claude 2, Llama-2-Chat, GPT-4-Base) döntési tendenciáit vizsgálták egy stratégiai döntéstámogató szimuláció keretében, és kivétel nélkül mindegyik az eszkalációs ciklus felé tolta az események irányát, két modell az atomfegyverek bevetését is sürgette.

Az MI-technológiát kiaknázandó, a humán szellemi tevékenység egyre nagyobb hányadát allokáljuk a kibertérbe, kitéve azt a kiberteret jellemző kockázatoknak. Továbbá az MI ártó célú alkalmazása és/vagy sérülékenységeik kiaknázása (például biológiai, orvosi kutatások vagy a katonai döntéstámogatás területén) a tömegpusztító fegyverekéhez mérhető hatások kiváltására is alkalmas lehet, még ha „erős védelmi dilemmát" (önmagában) jelentős valószínűséggel nem képez; azonban (például) katonai rendszerekkel összekötve olyan lehetséges fenyegetést testesíthet meg, amelyet a szemben álló feleknek kezelniük kell.

Henry Kissinger és Graham Allison (2023) három fő különbséget vázol fel az MI és a WMDk között:

- Az MI-fejlesztések jelentős részét privát entitások folytatják, akik a nemzeti biztonsági megfontolásokat a profit mögé sorolják.
- Az MI K+F+I költségigénye nagyságrendekkel kisebb (fejlesztésük gyorsabb), mint a nukleáris fegyvereké; valamint, az ellenfél tényleges MI-képességeinek azonosítása (szemben például az atomfegyverekkel) jelentősen nehezebb.
- Az MI-technológia nagyságrendekkel gyorsabban fejleszthető, mint a fegyverrendszerek – így nincs idő hosszas (nemzetközi) egyeztetésekre.[60]

54 Krajnc 2019: 1099.
55 Gosden–Gardener 2005: 397.
56 Carus 2012: 5.
57 Perry 2023.
58 Gozalo-Brizuela – Garrido-Merchán 2023.
59 Rivera et al. 2024.
60 Kissinger–Allison 2023.

Kissinger és Allison kiemelik, hogy az MI K+F+I vezető entitásainak többsége az USA-ban tevékenykedik, így eredményeik viszonylag transzparensek. A kevésbé nyílt K+F disszeminációs gyakorlatot folytató Kína – mint az Egyesült Államok deklarált ellenfele – esetében korlátozottabbak a lehetőségeink az ország tényleges MI-képességeinek megismerésére. A szerzők továbbá megállapítják, hogy az MI-megoldások alkalmazása közel mérhetetlen sebességgel terjed, és a nemzetközi közösség nem szükségszerűen a súlyának megfelelően kezeli ezt a technológiát.

Kissinger, Schmidt és Huttenlocher (2023) rámutat, hogy bár a csúcskategóriás MI-fejlesztéseket néhány technológiai szuperhatalom kisszámú csoportja kontrollálja, az idő haladtával a technológia is „avul", ezzel olcsóbbá válik, lehetővé téve szélesebb körű proliferációját.[61] Kissinger és társai véleménye szerint a helyzet kezelésének kulcsa az I. hidegháború szereplőit jellemző morál (felelősségtudat, az alkalmazás következményeinek azonosítása) kialakításában rejlik, semmint jogszabályok alkotásában.

Egyetértve a szerzőkkel, az MI kihívásainak jogszabályi kezelése – tekintettel a technológia fejlesztésének és terjedésének (jogalkotói szempontból) szinte követhetetlen sebességére – legjobb esetben is csak versenyt futhat az MI fejlődésével. Bár a „morál" kialakítása sem rövid távú feladat, de hatása proaktívabb és adaptívabb lehet a jogi szabályozásnál. Kissinger és Allison (2023) továbbá azt javasolja, hogy még az előtt kerüljön sor egy „MI-ellenőrzési" megállapodásra, mielőtt a technológia szerves részévé válik az államok biztonsági struktúrájának. Mivel számos vezető vállalkozás (Palantir, Thales Group, IBM, Raytheon, BAE Sytems stb.) már aktívan fejleszt és értékesít MI-alapú döntéstámogató (stb.) megoldásokat az államigazgatási és a katonai szféra számára,[62] a kissingeri javaslatok végrehajtásával már valószínűleg elkéstünk.[63]

A TS idegrendszere

Korunk nemzetközi rendet és (a gazdasági / kulturális) befolyást érintő „krónikus konfliktusai" hátterében zajló küzdelmek egyik kiemelt jelentőségű színpada a TS idegrendszerének tekinthető kibertér.

A hidegháborút követően, az internetéra elejétől számos hadtudományi és geopolitikai tanulmány már alkalmazta a kibertér (mint ötödik geopolitikai tartomány) fogalmát.[64] A NATO varsói csúcstalálkozóján (2016) kiadott nyilatkozat már műveleti területként hivatkozik a kibertérre, amelyet „a NATO-nak védelmeznie kell a légtérhez és a tengeri területekhez hasonlatosan".[65] Az EU 2016-os Külügyi és Biztonsági Stratégiája szintén nagy jelentőséget tulajdonított a kibertér védelmének, amelyet megerősített az úgynevezett „Biztonsági Unióra vonatkozó uniós stratégia".[66] Magyarország MI Stratégiája a nemzeti szuverenitás védelmének vonatkozásában az MI és a kiberbiztonság területén is lehetséges

61 Kissinger et al. 2023.
62 Law 2023.
63 Fehér 2023: 360; Rivera et al. 2024.
64 Kuehl 2009: 24–25.
65 NATO 2016.
66 Európai Unió 2016.

kihívásokról értekezik.[67] Az Nbtv.[68] 74. § *a)* bekezdése alapján a nemzetbiztonsági érdek elsődlegesen Magyarország szuverenitásának biztosítását takarja, de a bekezdés felsorolásából kiemelném az „ország függetlensége és területi épsége elleni támadó szándékú törekvések felderítése", valamint „az ország politikai, gazdasági, honvédelmi érdekeit sértő vagy veszélyeztető leplezett törekvések felfedése és elhárítása" részeket, amelyek a kibertér vonatkozásában is indukálnak védelmi kötelezettségeket; hiszen – a koppenhágai iskola biztonsági koncepciója alapján[69] – információs társadalmunk életében a biztonságérzet elválaszthatatlan részét képezik a NIS2 irányelv[70] I. számú mellékletében felsorolt szolgáltatások (pénzügy, egészségügy, közigazgatás stb.) akadálytalan elérhetőségének tudata, amelyek már alapvetően támaszkodnak a kibertérre. Az NBS III. fejezet 8. pontja a nemzeti szuverenitás terén alapvető értékként jeleníti meg a kibertér biztonságát,[71] azonban a védelemért felelős entitásoknak – a kibertér vázolt sajátosságai okán – elmosódó szervezeti és országhatárok világában kell jogszerűen helytállniuk. A felhőszolgáltatások korában jelentős kérdés, hogy például az Amazon szolgáltatásait igénybe vevő entitás adatai valójában milyen fizikai lokációkon találhatók, és adott esetben kinek van felettük joghatósága. A hálózati lét másik velejárója, hogy adott kibertámadás „elkövetője" lehet a kibertér nagyszámú csomópontja úgy, hogy ezzel elsöprő többségük nincs tudatában, míg a támadás mögött álló entitás (többé/kevésbé) rejtve marad.[72]

A lehetséges fenyegetéseket megtestesítő entitások épp úgy besorolhatók az állami (háttérrel rendelkező) szereplők, bűnözői csoportok, ideológiai alapon tevékenykedő hacktivisták, illetve belsős elkövetők mátrixába, mint ahogyan a kiberteret érintő főbb fenyegetettségek összevethetők az IKT-infrastruktúrák feltérképezett kitettségeivel.[73] Figyelembe véve a kibertér hálózati jellegét, az EU NIS Együttműködési Csoport koordinálásával elvégzett, az uniós kommunikációs infrastruktúrák és hálózatok kiberbiztonságát és ellenálló képességét vizsgáló felmérésben megfogalmazott tíz fő fenyegetettség[74] és nyolc fő sérülékenység[75] a kibertér fenyegetési térképében is jelentős szerepet játszik.

Az MI tervezett, egyre növekvő arányú alkalmazására tekintettel, a fent soroltakat szükséges kiegészíteni az MI irányából felmerülő fenyegetettségekkel és sérülékenységekkel.[76] A gépitanulás-algoritmusok (ML) egyaránt alkalmazhatók kiberbűncselekmények elkövetésére, illetve ezen algoritmusok támadásával a kimeneti eredmények módosíthatók. A módosítás lehet alig észrevehetően kifinomult (befolyásoló), de eredményezheti az algoritmus – így az általa menedzselt szolgáltatás(ok) – összeomlását is. Az ML-algoritmusok

67 ITM 2020.
68 1995. évi CXXV. törvény.
69 Remek 2014: 71.
70 (EU) 2022/2555 irányelv.
71 1163/2020. (IV. 21.) Korm. határozat.
72 Marton 2019: 23.
73 Lásd: https://ec.europa.eu/newsroom/dae/redirection/document/102529
74 *Támadások:* adattörlő/zsarolóvírus, ellátási lánc elleni, kiszervezett szolgáltatások nyújtói ellen/rajtuk keresztül végrehajtott, hálózatokba történő beépülésre épülő, DDoS, fizikai rongálás/szabotázs, beszállítóra gyakorolt állami befolyásra építő, kapcsolódási. *Egyéb fenyegetések:* tápellátás megszűnése, belsős fenyegetések.
75 *Alacsony biztonsági szintű:* hálózati elem, végponti eszköz (pl. IoT), üzemeltetés; *sérülékeny:* adatirányítási protokollok, fizikai infrastruktúra (pl. tenger alatti adatkábelek); *függőségek:* beszállítók/szolgáltatók, tápellátás, szakértelem.
76 Alanazi 2023.

elleni támadások célja vagy a helyes döntés/előrejelzés elterelése a támadó által kívánt irányba – például az adott hálózati eszköz (szerver) túlterhelt, de az MI, hibás döntést hozva, további forgalmat irányít felé –, vagy az algoritmus vizsgálatának tárgyát érintő osztályozási folyamatot térítik el – például önvezető járművek adatfolyamait közösségi média jelfolyamként osztályozza és késleltetetten továbbítja.[77] Egy adott IKT-hálózat menedzseléséért felelős MI-algoritmusok befolyásolása révén az elkövetők saját vagy megbízójuk előnyére terelhetik el, használhatják ki az adott kibertérszegmens adatait; lehetőségük nyílhat az általa kiszolgált alkalmazások kompromittálására, szinergiájuk ártó jellegű kiaknázására, akár terror jellegű cselekmények elkövetésére.

Az LLM-ek alkalmazása kapcsán jelenleg azonosított biztonsági kihívások között szerepel a felhasználók által betáplált (feltett kérdés, „kiadott" feladat), egyben modellek tanításához is felhasznált adatok (kritikus információk) kérdésköre. Továbbá a ChatGPT-3.5 megjelenését követően igen hamar megjelentek bűnelkövetéseket támogató „ikrei" (például WormGPT, FraudGPT). Az ismertté vált LLM „hacking" [78] technikák (prompt[79] injektálás, Jailbreak) rávilágítanak a technológia lehetséges biztonsági kihívásainak széleskörűségére; kiemelt példaként említve azon (eredményes) kísérletet, amely során a kutatók egy olyan promptot alkottak, amely a GPT-4-et hatékony, a weboldalak sérülékenységeit automatikusan felderítő és kiaknázó eszközzé alakította.[80]

Mindezekre tekintettel a kibertér kritikus infrastruktúra jellegének magas szintű, proaktív védelme minden, a 21. században prosperálni és érdekeit eredményesen érvényesíteni kívánó állam alapvető feladata.[81] Ugyanakkor nehéz kérdés, hogy hol húzhatjuk meg a „nemzeti kibertér" védendő határait. Habár az NKS I./3. pontja definiálja Magyarország kiberterét, ennek gyakorlati alkalmazhatósága kérdéseket vet fel. Az „a globális kibertér elektronikus információs rendszereinek azon része, amelyek Magyarországon találhatóak" jól körülhatárolható; azonban a nem fizikai szférákra[82] utaló „a globális kibertér elektronikus rendszerein keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok közül azok, amelyek Magyarországon történnek vagy Magyarországra irányulnak, illetve amelyekben Magyarország érintett" azonosítása már kihívásokat generál. A felhőtechnológiák terjedésével általánossá válik, hogy csak adattöredékek lesznek számos, hazai területen kívül található szerveren és/vagy egyéb peremoldali megoldáson,[83] amelyeket a felhőszolgáltatás alakít a felhasználó számára egységes információvá.

Összegzés

Írásomban röviden bemutattam a (transzhumanizmustól mentes) technológiai szingularitás megalapozó technológiáit (TS-triád), a kibertérrel kapcsolatos összefüggéseit

77 Jeong 2020.
78 Egy adott modell viselkedését befolyásoló eljárások.
79 Az LLM számára általános (emberi) nyelven megírt „parancs".
80 Mozes et al. 2023; Fang et al. 2024.
81 Kelemen 2023: 85.
82 Logikai, kiberszemélyiség – lásd NATO AJP-3.20.
83 A felhasználóhoz legközelebb eső hálózati adatfeldolgozó, -tároló egység.

és mindezekre alapozva a TS egyes, biztonsággal kapcsolatos összefüggéseit. Bemutattam a kibertér egyes sajátosságait, változékony, országhatárokat elmosó jellegét.

Rámutattam, hogy a TS-triád „primus inter pares"[84] összetevőjének tekinthető az MI. A technológia stratégiai jelentőségét támasztják alá a Kissinger és munkatársai[85] által megfogalmazott kockázatok és a technológia nemzetközi felügyeletét célzó javaslatok. Habár az elektronikus hírközlési hálózatok kiberbiztonságát érintő fenyegetettségek és sérülékenységek a kibertér szempontjából relevánsak, de a TS relációjában az MI hatását (közel korlátlan információra és masszív adatkommunikációra épülő exponenciális fejlődés) is figyelembe szükséges venni. Ennek megfelelően a TS kiberkockázatai nem kezelhetők kizárólag a hagyományos, reaktív kibervédelmi megoldásokkal; szükséges új, proaktív vagy offenzív védelmi eljárások kidolgozása, alkalmazása.

Jelenünk egészen más, mint azt akár két évvel ezelőtt is előre jelezték. Figyelembe véve a jelen írásban vázolt TS-triád főbb fejlődési/fejlesztési irányait, joggal feltételezhető, hogy technológiai fejlődésünk sarokköve egyre inkább a nagy tömegű, aktuális adatokat biztosító megoldások (IoT), a szervező és fejlesztő entitásként megjelenő MI, valamint a nagy mennyiségű adatátvitelt biztosító, végponti eszközök akár millióit stabilan kiszolgálni képes, biztonságos kommunikációs platformok (5G/6G) szimbiózisa lesz, amire a transzhumanizmus-mentes technológiai szingularitás kifejezést alkalmaztam.

A kettős minőségű – statikus és dinamikus jellemzőkkel leírható – 5. geopolitikai szféra (kibertér) fontossága egyre meghatározóbbá válik, figyelembe véve a TS-triád – kiemelten 5G/6G – 2030-ig tervezett szabványosítási és K+F-terveit, -ajánlásait. A korunk nemzetközi rendet és (gazdasági vagy kulturális) befolyást érintő krónikus konfliktusai hátterében zajló küzdelmek kiemelt jelentőségű színpada a kibertér marad, ami jól mutatja annak exponenciálisan növekvő jelentőségét. A felette gyakorolt ellenőrzés igénye szükségszerűen megjelenik az egyes országok és szövetségi rendszerek katonai, geopolitikai és geoökonómiai stratégiáiban. Szükséges azonban megállapítani, hogy a kibertér hatékony felügyelete – kettős minőségéből fakadóan – többdimenziós megközelítést igényel. Azon országok (és szövetségek), amelyek figyelmen kívül hagyják a TS-megalapozó és kritikus technológiák, valamint a kapcsolódó ökoszisztémák és erőforrások (beleértve a HR) fejlesztését, az elkövetkezendő évtizedekben hátrányos helyzetbe kerülnek a nemzetközi érdekérvényesítés küzdelmeiben. Az összegző jelleggel ismertetett technológiák egyenként is számos – jelentős részt ismert – biztonsági kihívást jelenítenek meg, azonban TS-ként azonosított szimbiózisukban a biztonsággal kapcsolatos kérdések újraértelmezése válik szükségessé, megvilágítandó a TS biztonsági vakfoltjait – amelyek kiemelt forrása lesz az MI.

Feltételezve, hogy világunk nem esik át egy jelentős, technológiai visszaesést indukáló eseményen, azon államok, amelyek képesek azonosítani a vonatkozó technológiai és gazdasági trendeket és innovációs tevékenységük révén csatlakozni ezekhez, vagy akár vezető (-közeli) pozíciót megszerezni, lehetőségük nyílik rá, hogy részlegesen felülírva a geopolitika és geoökonómia (a Globalizáció 3.0-ig szigorúan érvényben lévő)[86] szabályait, jelentősen javítsák érdekérvényesítő képességeiket. Habár, mint azt Vernor Vinge

[84] Első az egyenlők között.
[85] Kissinger et al. 2023.
[86] Friedman 2005.

1993-ban megállapította, a TS „hatályon kívül" helyezi világunk leíró (beleértve a jövőt tervező/előrejelző) modelljeit.

Felhasznált irodalom

Adams, Alphonso (2024): *Cyberspace in War* [pdf]. Maxwell Air Force Base (USA, Alabama): Air University Press. Online: www.airuniversity.af.edu/Portals/10/AUPress/Papers/DP_36_Adams_Cyberspace_in_War.pdf

Alanazi, Mohammad (2024): 5G Security Threat Landscape, AI and Blockchain. *Wireless Personal Communications*. 2024. február 11., 1467–1482. Online: https://doi.org/10.1007/s11277-023-10821-6

Bánkuty-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

Berger, Federico (2021): The Alliance in the Loop: NATO and Artificial Intelligence. NATO Foundation. Online: www.natofoundation.org/wp-content/uploads/2021/12/NDCF-Paper-Berger-NATO-and-Artificial-Intelligence-151121.pdf

Bode, Ingvild (2024): Emergent Normativity: Communities of Practice, Technology, and Lethal Autonomous Weapon Systems. *Global Studies Quarterly,* (4), 1–11. Online: https://doi.org/10.1093/isagsq/ksad073

Brennan, Donald G. (1971): Strategic Alternatives: I. *The New York Times,* 1971. május 24. 31. Online: www.nytimes.com/1971/05/24/archives/strategic-alternatives-i.html

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 – Wilde, Jaap De (1998): *Security: A New Framework for Analysis*. Boulder, Colorado: Lynne Rienner. Online: https://doi.org/10.1515/9781685853808

Carus, W. Seth (2012): *Defining Weapons of Mass Destruction*. Washington, D.C.: National Defense University Press. Online: https://doi.org/10.21236/ADA577317

Csányi Vilmos (2004): Az emberi természet biológiai gyökerei. In *Mindentudás Egyeteme 3.* Budapest: Kossuth, 295–316. Online: https://real-eod.mtak.hu/1076/1/16%20Cs%C3%A1nyi%20Vilmos.pdf

Demarisco, Dominic et al. (2021): Aggression in the Digital Era: Assessing the Validity of the Cyber Motivations for Aggression and Deviance Scale. *Assessment,* 29(4), 764–781. Online: https://doi.org/10.1177/1073191121990088

Európai Unió (2016): *Közös kül- és biztonságpolitika – globális stratégia*. Online: https://eur-lex.europa.eu/HU/legal-content/summary/common-foreign-and-security-policy-global-strategy.html

Fang, Richard et al. (2024): *LLM Agents can Autonomously Hack Websites*. arXiv:2402.06664. Online: https://doi.org/10.48550/arXiv.2402.06664

Farkas Tibor (2023): A kommunikációs és információs rendszerek értelmezése napjainkban: Követelmények és kihívások. In Tóth András (szerk.): *Új típusú kihívások az infokommunikációban*. Budapest: Ludovika, 11–30.

Fehér András Tibor (2023): A mesterségesintelligencia-alapú hidegháború etikai háttere. In Kovács Zoltán (szerk.): *A mesterséges intelligencia és egyéb felforgató*

technológiák hatásainak átfogó vizsgálata. Budapest: Katonai Nemzetbiztonsági Szolgálat, 355–392. Online: www.knbsz.gov.hu/hu/letoltes/kiadvanyok/01_MI.pdf

Friedman, Thomas L. (2005): It's a Flat World, After All. *The New York Times*, 2005. április 3. Online: www.nytimes.com/2005/04/03/magazine/its-a-flat-world-after-all.html

Germany: Industrie 4.0. (2017). Online: https://ati.ec.europa.eu/sites/default/files/2020-06/DTM_Industrie%204.0_DE.pdf

Gosden, Christine – Gardener, Derek (2005): Weapons of Mass Destruction – Threats and Responses. *British Medical Journal,* 331(7513), 397–400. Online: https://doi.org/10.1136/bmj.331.7513.397

Gozalo-Brizuela, Roberto – Garrido-Merchán, Eduardo C. (2023): *A Survey of Generative AI Applications.* arXiv, 2306.02781 (cs.LG). Online: https://doi.org/10.48550/arXiv.2306.02781

Haig Zsolt et al. (2014): *Elektronikai hadviselés.* Budapest: Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar.

Haig Zsolt (2018): *Információs műveletek a kibertérben.* Budapest: Dialógus Campus.

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

ITM (2020): *Magyarország Mesterséges Intelligencia Stratégiája* 2020–2030. Online: https://digitalisjoletprogram.hu/files/2f/32/2f32f239878a4559b6541e46277d6e88.pdf

Jeong, Doowon (2020): Artificial Intelligence Security Threat, Crime, and Forensics: Taxonomy and Open Issues. *IEEE Access,* 8, 184560–184574. Online: https://doi.org/10.1109/ACCESS.2020.3029280

Kelemen Roland (2023): A kibertér jellemzőinek biztonság központú vizsgálata. *Jog–Állam–Politika,* 15(1), 75–90. Online: https://doi.org/10.58528/JAP.2023.15-1.75

Kissinger, Henry A. – Allison, Graham (2023): The Path to AI Arms Control. *Foreign Affairs,* 2023. október 13. Online: 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: www.henryakissinger.com/articles/chatgpt-heralds-an-intellectual-revolution/

Kopecký, Kamil – René, Szotkowski (2017): Specifics of Cyberbullying of Teachers in Czech Schools – A National Research. *Informatics in Education,* 16(1), 103–119. Online: https://doi.org/10.15388/infedu.2017.06

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: Katonai Nemzetbiztonsági Szolgálat, 355–392. Online: www.knbsz.gov.hu/hu/letoltes/kiadvanyok/01_MI.pdf

Krajnc Zoltán főszerk. (2019): *Hadtudományi lexikon.* Budapest: Dialóg Campus.

Kuehl, Daniel T. (2009): From Cyberspace to Cyberpower: Defining the Problem. In Kramer Franklin D. – Starr, Stuart H. – Wentz, Larry K. (szerk): *Cyberpower and National Security.* Nebraska, USA: University of Nebraska Press, 24–42. Online: https://doi.org/10.2307/j.ctt1djmhj1.7

Kurzweil, Ray (2014): The Singularity is Near. In Sandler, R. L. (szerk.): *Ethics and Emerging Technologies.* London: Palgrave Macmillan, 393–406. Online: https://doi.org/10.1057/9781137349088_26

Law, Marcus (2023): Top 10 Military Technology Companies Putting AI into Action. *Technology Magazine,* 2023. március 7. Online: https://technologymagazine.com/top10/top-10-military-technology-companies-putting-AI-into-action

Liu, Hongshan et al. (2024): *Near-Space Communications: the Last Piece of 6G Space-Air-Ground-Sea Integrated Network Puzzle*. arXiv:2401.00283 [cs.IT]. Online: https://doi.org/10.34133/space.0176

Madiega, Tambiama (2023): *General-purpose Artificial Intelligence*. Európai Parlament, 2023. március. Online: www.europarl.europa.eu/RegData/etudes/ATAG/2023/745708/EPRS_ATA(2023)745708_EN.pdf

Marton Péter (2019): *Biztonsági komplexumok*. Budapest: Budapest Corvinus Egyetem.

Maslej, Nestor főszerk. et al. (2023): *Artificial Intelligence Index Report 2023*. Stanford (USA): AI Index Steering Committee, Institute for Human-Centered AI. Online: https://aiindex.stanford.edu/report/

Mészáros Rezső (2001): A kibertér társadalomföldrajzi megközelítése. *Magyar Tudomány,* 46(7), 769–779. Online: https://epa.oszk.hu/00700/00775/00032/769-779.html

Mozes, Maximilian et al. (2023): *Use of LLMs for Illicit Purposes: Threats, Prevention Measures, and Vulnerabilities*. arXiv:2308.12833v1 [cs.CL]. Online: https://doi.org/10.48550/arXiv.2308.12833

NATO (2016): *Warsaw Summit Communiqué*. 2016. július 9. Online: www.nato.int/cps/en/natohq/official_texts_133169.htm

NATO (2023): *Emerging and Disruptive Technologies*. Online: www.nato.int/cps/en/natohq/topics_184303.htm

NIS COOPERATION GROUP (2024): *Cybersecurity and Resiliency of Europe's Communications Infrastructures and Networks*. 2024. 02. 21. Online: https://ec.europa.eu/newsroom/dae/redirection/document/102529

Obrusánszky, Borbála (2008): *Dzsingisz kán: a bölcsesség kulcsa*. Hága: Mikes International.

Ottis, Rain – Lorents, Peeter (2010): Cyberspace: Definition and Implications. In *Proceedings of the 5th International Conference on Information Warfare and Security*. Dayton, OH, US, 8–9 April. Academic Publishing Limited, 267–270. Online: https://ccdcoe.org/library/publications/cyberspace-definition-and-implications/

Perry, Lori (2023): What's New in Artificial Intelligence from the 2023 Gartner Hype Cycle. *Gartner,* 2023. augusztus 17. Online: www.gartner.com/en/articles/what-s-new-in-artificial-intelligence-from-the-2023-gartner-hype-cycle

Pirisi Gábor – Trócsányi András (2019): *Fejezetek a társadalomföldrajz világából*. Pécs: Publikon.

Rajasekaran, Arun Sekar et al. (2024): A Survey on Exploring the Challenges and Applications of Wireless Body Area Networks (WBANs). *Cyber Security and Applications,* 2024(2). Online: https://doi.org/10.1016/j.csa.2024.100047

Reding, D. F. – Eaton, J. (2020): *Science & Technology Trends 2020–2040*. Brüsszel: NATO Science & Technology Organization. Online: www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf

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: 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*. arXiv:2401.03408. Online: https://doi.org/10.1145/3630106.3658942
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
Schmitt, N. Michael (2017): *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.
Seewald, Alexander K. (2022): A Criticism of the Technological Singularity. In Dingli, Alexiei 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
Siposné Kecskeméthy Klára (2021): A NATO 2030 jelentés – stratégiai prioritások új megközelítésben. *Honvédségi Szemle,* 149(4), 3–16. Online: https://doi.org/10.35926/HSZ.2021.4.1
Tóth András (2023a): Az Internet of Things rendszerek biztonsági kihívásai. In Tóth András (szerk.): *Új típusú kihívások az infokommunikációban*. Budapest: Ludovika, 99–136.
Tóth András (2023b): Az 5G-technológia jellemzői és a kialakításában rejlő kihívások. In Tóth András (szerk.): *Új típusú kihívások az infokommunikációban*. Budapest: Ludovika, 51–98.
Ulam, S. (1958): *John von Neumann*. Rhode Island (USA): American Mathematical Society.
UNIDIR (2023): *The United Nations, Cyberspace and International Peace and Security Responding to Complexity*. 2023. május. Online: https://unidir.org/wp-content/uploads/2023/05/the-united-nations-cyberspace-and-international-peace-and-security-en-691.pdf
Vailshery, Lionel Sujay (2023): Number of IoT Connected Devices Worldwide 2019–2023, with Forecasts to 2030. *Statista*, 2023. 07. 27. Online: www.statista.com/statistics/1183457/iot-connected-devices-worldwide/
Vinge, Vernor (1993): *The Coming Technological Singularity: How to Survive in the Post-Human Era*. NASA. Lewis Research Center, Vision 21: Interdisciplinary Science and Engineering in the Era of Cyberspace. Online: https://ntrs.nasa.gov/citations/19940022856

Jogi források

1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiája. Online: https://2010-2014.kormany.hu/download/b/b6/21000/Magyarorszag_Nemzeti_Kiberbiztonsagi_Strategiaja.pdf
1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról. Online: https://net.jogtar.hu/jogszabaly?docid=A20H1163.KOR&txtreferer=00000001.txt
2021/0106(COD) 5662/24 2024. Online: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CONSIL:PE_24_2024_REV_1