RENDÉSZET - TUDOMÁNY - AKTUALITÁSOK

A rendészettudomány a fiatal kutatók szemével

KONFERENCIAKÖTET 2021

RENDÉSZET-TUDOMÁNY-AKTUALITÁSOK - 2021
A rendészettudomány a fiatal kutatók szemével

Online konferenciakötet

Szerkesztette:

Baráth Noémi Emőke

Mezei József

Doktoranduszok Országos Szövetsége Kiadó

Doktoranduszok Országos Szövetsége

Rendészettudományi Osztály

Budapest

ISBN: 978-615-5586-89-7

A kötetben megjelent tanulmányok szakmai lektorai és szekcióvezetői:

Dr. Auer Ádám
Dr. Farkas Johanna
Dr. Hegedűs Judit
Dr. Kemény János
Dr. Regényi Kund
Dr. Ritecz György
Dr. Tóthi Gábor
Prof. Dr. Sallai János
Dr. Czenczer Orsolya

A Doktoranduszok Országos Szövetsége Rendészettudományi Osztály 2020/2021-es év tisztségviselői és a konferencia szervezői:

Baráth Noémi Emőke- elnök
Mezei József -általános alelnök
Kovács Szitkay Eszter - titkár
Fekete Márta- büntetés-végrehajtási területért felelős tudományos referens
Schmidt Laura - kommunikációs referens
Szigetvári Oszkár - rendőrségi területért felelős tudományos referens
Beke József - nemzetbiztonsági területért felelős tudományos referens
dr. Pozsgai Petra – nemzetközi referens
Görömbei Zoltán- osztálytag
Molnár Tamás -osztálytag
Suhajda Attila -osztálytag
Pászti Péter - osztálytag

A kötet a Rendészet-Tudomány-Aktualitások 2021. A rendészettudomány a fiatal kutatók szemével című tudományos konferencián elhangzott előadásokat tartalmazza.

A rendezvény az Emberi Erőforrások Minisztériuma megbízásából az Emberi Erőforrás Támogatáskezelő által meghirdetett Nemzeti Tehetség Program NTP-FKT-M-18-0003 kódszámú pályázati támogatásból valósult meg.

Tartalomjegyzék

Pék Richárd Tamás: A terrorizmus jelzőinek hullámaiban 5

Nagy Melánia: Kiskorúak a frontvonalon 15

Tőzsér Erzsébet: Megoldások az USA rendészeti szerveinek munkaerőválságára és azok hazai adaptálásának lehetőségei 23

Héder Klára: Megfigyeléssel kapcsolatos civil és rendvédelmi attribúciók 32

Bálint Krisztián: Biztonsági kamerákon alapuló hallgatói jelenléti ívkészítő rendszer analitikai funkciói 42

Tegyey Andrea: Gondolatok a rendőri motivációról 50

Borbély Zsuzsanna:Munkahelyi stressz és a koronavírus-járvány első hulláma a rendőrtanulók körében 57

Mozsonyi Norbert: Új technológiákból eredő globális fenyegetések, nemzetbiztonsági, adatvédelmi szempontjai a magánszféra tükrében 67

Suhajda Attila: Integrációs tapasztalatok Ausztriában és Németországban 2015 után 80

Rezsneki Zsombor: Rakétaképesség a Világűrbe 89

Bereczky Nikolett: A győzelem a döntési térben, az győzelem a csatatéren 98

Véger Alexandra: Koronavírus-helyzet kezelés a magyar börtönökben 107

Ivanics Zsófia: A fogvatartotti munkáltatásra vonatkozó szakirodalom főbb irányai 114

Bellavics Mária Zsóka: A pszichiátriai állapot és a börtönökben mutatott szabálysértő viselkedés összefüggései 122

Baráth Noémi Emőke: A kriminálpszichológiai attitűd megjelenése a rendőr hallgatók körében..... 132

Papp Petra: Gondolatok a bűnmegelőzésről 138

Molnár Alíz Zsuzsanna: Emberi kapcsolatok hiánya és illegális gyülekezések a járványhelyzetben..... 147

Fodorné Zagyi Orsolya: Az egészségügyi adatok védelme az e-health technológiák tükrében 159

Bereczky Nikolett: A győzelem a döntési térben, az győzelem a csatatéren[1]

Absztrakt

Az információs szféra a hibrid hadviselés kritikus műveleti területe. Ha a NATO új technológiai stratégiát akar kidolgozni, akkor azt a fejlődő földrajzi, geopolitikai és katonai területek összefüggésében kell megtennie. A NATO *Science & Technology Trends* potenciális diszruptorai közül kiemelek kettőt: az *Adatot* és a mesterséges intelligenciát. Bemutatom, hogy mindkettőt több területen is lehetséges használni a hadviselésben, kiemelve a deepfake példáját. A két diszruptor egymással karöltve elősegítheti az információs fölényt és a „bizonytalanság elleni küzdelmet": ez döntő hadviselési előny lehet, ami gyorsabb és minőségibb döntéseket tesz lehetővé.

1.Bevezető

A mai NATO veszélyes, kiszámíthatatlan és változó biztonsági környezettel néz szembe, valamint egzisztenciális kihívásokkal és fenyegetésekkel minden stratégiai irányból – beleértve az állami és nem állami szereplőket is –, mint például: kiberfenyegetések, terrorizmus, hibrid hadviselés és információs műveletek. Ha a NATO meg akarja őrizni azt a szellemi, technológiai, tudományos és innovációs előnyét (Marino, 2017), amellyel az elmúlt 70 évben rendelkezett, akkor teljes mértékben meg kell értenie ezeket a technológiai fejlődéseket, azok lehetséges felhasználását, valamint operatív és stratégiai következményeit. Kreatívan be kell vonnia az egész Szövetséget, hogy alkalmazkodjon a kapcsolódó fenyegetésekhez és lehetőségekhez, kihasználva a rendelkezésre álló pénzügyi és szellemi tőkét.

A NATO *Science & Technology Trends: 2020-2040* elnevezésű kiadványában bemutatásra kerül, hogy a feltörekvő és diszruptív technológiák (emerging and disruptive technologies) hogyan hathatnak a NATO katonai műveleteire, védelmi képességeire és politikai döntéseire (NATO STO, 2020). A dokumentumban nyolc egymással szorosan összefüggő területet határoztak meg, mint fő stratégiai diszruptorok a következő 20 évben. A tanulmányomban ezek közül kettőt emelek ki: az egyik Big Data és Fejlett Elemzések (Big Data and Advanced Analytics), a másik pedig a mesterséges intelligencia. A szakirodalmat megvizsgálva alátámasztom, hogy ez a két terület miért lesz jelentős hatással a jövő hadviselésére. Ezekhez jelentősen támaszkodom a Congressional Research Service által 2020. novemberében készült Mesterséges Intelligencia és Nemzetbiztonság című elemzésére (CRS, 2020), illetve a NATO HQ által 2021-ben kiadott A NATO Döntéshozása a Big Data és a Mesterséges Intelligencia Korában (NATO Decision-Making in the Age of Big Data and Artificial Intelligence) publikációra.

Jelen írásban *feltörekvő*nek azon a technológiákat vagy tudományos felfedezéseket tekintjük, amelyek várhatóan a 2020–2040 közötti időszakban érik el "érettségüket" és jelenleg nem használják széles körben, vagy amelyeknek jelenleg a Szövetség védelmi, biztonsági és vállalati funkcióira gyakorolt hatása nem teljesen egyértelmű. *Diszruptív*nak pedig azokat a technológiákat vagy tudományos felfedezéseket, amelyek várhatóan jelentős, esetleg

[1] Phd hallgató,Nemzeti Közszolgálati Egyetem,Hadtudományi Doktori Iskola
bereczky.nikolett@uni-nke.hu

forradalmi hatást gyakorolnak a NATO védelmi, biztonsági vagy vállalati funkcióira a fentebb említett időszakban. *Konvergens* alatt pedig technológiák kombinációját értjük, amelyeket újszerű módon kombinálnak, hogy diszruptív hatást érjenek el. Nem minden technológia vagy tudományos felfedezés feltörekvő vagy diszruptív. Továbbá nem minden feltörekvő technológia lesz diszruptív és nem minden diszruptív technológia lesz feltörekvő (NATO STO, 2020, 6). A diszruptivitásra jó példa az, ahogyan a régi vezetékes telefonokat felváltották mobiltelefonok, vagy ahogyan a mobiltelefonokat felváltották az okostelefonok.

A hetedik katonai forradalmat (Hoffman, 2019) a technológiai környezet gyors változásai ösztönzik. Az ember által létrehozott konfliktusok (a háború a legszélsőségesebb esetben) Clausewitz-i értelemben nagy társadalmi csoportok (pl. államok, pszeudo-államok, közösségek, társadalmak stb.) akaratának az ütközése. Ilyen konfliktus során, akár egyenrangú versenytársakkal, akár aszimmetrikus fenyegetésekkel állunk szemben, a technológia egy olyan lehetőség, amelyet ki kell használni. Azzal, hogy a demokratizált technológia még inkább az emberi lét központi elemévé válik, túlméretezett szerepet kap a konfliktusok alakításában is.

Stratégiai és geopolitikai kontextusban a konfliktusok természete változik, ebbe jelentősen beletartozik az átalakuló technológiai környezet is. A konfliktusnak ez a változó jellege hibrid háborúkban, hiper-háborúkban (Allen – Hussain, 2017), memetikus hadviselésben (Giesea, 2017) vagy következő generációs konfliktusokban nyilvánul meg. Mindegyikben, a diszruptív technológiák a meglévő technológiákkal és katonai képességekkel egyesülve új módokat és eszközöket kínálnak a konfliktusokban való részvételre.

2.Science & Technology Trends: 2020-2040

A Science & Technology Trends (NATO STO, 2020) jelentés alapvető célja az, hogy növelje a Szövetségen belüli megértés szintjét a tudományos és technológiai fejlesztésekben rejlő lehetőségek iránt. Emellett cél az is, hogy széles közönséget érjen el, a NATO-n és partnerein belül és kívül egyaránt. A jelentés szigorúan a következőkön alapul:

- a nyílt szakirodalomban tárgyalt technológiai trendek,
- a technológiai fejlődés globális perspektívája,
- a tudományos és technológiai szakértelem által megalapozott logikai érvelés.

A jelentés segítséget nyújt a döntéshozók számára a következők mérlegelésében:

- Miért lesznek fontosak a feltörekvő és diszruptív technológiák (emerging and disruptive technologies, továbbiakban EDT) a Szövetség jövőbeli tevékenységei szempontjából?
- Hogyan alakulhatnak ki ezek az EDT-k az idő során?
- Milyen fejlesztések és lehetséges következmények várhatók a Szövetség számára rövid, közép- és hosszú távon?

A Science & Technology Trends azokra a technológiákra összpontosít, amelyekről a legvalószínűbb, hogy húszéves időkereten belül diszruptívak lesznek, beleértve azokat is, amelyek túljutottak a kezdeti feltárási szakaszon, de még nem kerültek széles körben kiaknázásra. Ezek a fő stratégiai diszruptorok a következők:

- Big Data és Fejlett Elemzések (Big Data and Advanced Analytics, továbbiakban Adat),
- Mesterséges Intelligencia (továbbiakban MI),
- Autonómia,

- Űr,
- Hiperszonikus fegyverrendszerek(Hypersonics),
- Kvantum,
- Biotechnológia,
- Anyagok.

A diszruptív hatások nagy valószínűséggel az EDT-k kombinációi és a köztük lévő komplex kölcsönhatások révén fognak jelentkezni. Az előrejelzések szerint a következő szinergiák és kölcsönös függőségek lesznek nagy hatással a jövőbeli katonai képességek fejlődésére:

- Adat-MI-Autonómia,
- Adat-MI-Biotechnológia,
- Adat-MI-Anyagok,
- Adat-Kvantum,
- Űr-Kvantum,
- Űr-Hypersonics-Anyagok.

A következőkben két nagy és ahogyan a fenti példákban is láthattuk, egymással szorosan összefüggő terület kerül bemutatásra: az Adat és az MI.

3.Adat: (Big) Data és Fejlett Elemzések

A bizonytalanság a katonai műveletek tipikus tényezője és Clausewitz már a XIX. században úgy vélte, hogy a véletlennek alapvető és elkerülhetetlen szerepe van a háború fejlődésének és kimenetelének meghatározásában (Clausewitz, 1989, 85). Ennek eredményeként a katonai szervezetek mindig is rendkívüli gondossággal jártak el és hatalmas erőfeszítéseket tettek annak érdekében, hogy olyan szervezeteket és eljárásokat hozzanak létre, amelyek a rendelkezésre álló információk alapján a háborús „ködön" keresztül is irányíthassák a műveleteiket. Manapság a Big Data evolúciója és elérhetősége ígéretes lehetőséget nyújt magán- és állami szervezeteknek, köztük a fegyveres erőknek és a NATO-nak abban, hogy csökkentsék a műveleti területeiken a véletlen szerepét. A döntéseknek a korábban lehetségesnél jóval nagyobb mennyiségű információra való alapozása valódi forradalmat eredményezhet a komplex szervezetek döntéshozatali folyamataiban, különösen azért, mert ezek az információk a valóság különböző dimenzióira vonatkoznának, amelyek korábban nem voltak feltárhatók vagy naprakészek (NATO HQ, 2021, 38). (Megjegyzés: a Big Data kifejezésnek számos definíciója van, pl. Wilder-James szerint: A Big Data olyan adat, amely meghaladja a hagyományos adatbázis-kezelő rendszerek kapacitását, túl nagy és túl gyorsan változik, vagy nem illeszkedik az adatbázis-architektúrák megkötéseibe. Annak érdekében, hogy az értékeket kinyerjük, alternatív megoldást kell választani a feldolgozásban (Wilder-James, 2014)).

Emellett a világunk egyre digitálisabbá és virtuálisabbá válik. A következő 20 évben ez a tendencia várhatóan felgyorsul, és alapvetően alakítja át a Szövetség működését és képességeit. Szenzorhálózatok, autonómia, új kommunikációs technológiák (pl. 5G), digitális ikrek (vagyis egy fizikai entitás virtuális replikája) és számos egyéb új és kibővített analitikai módszer fejlesztése növeli majd a képességünket a körülöttünk lévő emberi, fizikai és információs terek megértésére. Az Adat központi szerepet játszik majd a katonai képességek kiaknázásban mindegyik EDT - különösen a mesterséges intelligencia – tekintetében (NATO STO, 2020, 13-14).

A társadalmi és egyéni interakciók fokozott virtualizálása pedig drámai módon járul hozzá a társadalmi és személyes adatok hozzáférhetőségéhez. Ennek a virtualizációnak az egyik tere a közösségi média. A közösségi média tartalma folyamatosan növekszik, de küzd a valódiság és az érték kérdéseivel. Különösen a DARPA folytatja a közösségi média hatásainak kutatását olyan területeken, mint az információáramlás mintái, érzelmek és vélemények elemzése, minták észlelése, kulturális narratívák, a kialakulóban lévő közösségek modellezése, bizalmi elemzés, hálózati dinamika modellezés vagy automatizált tartalomelőállítás (DARPA, 2019). A társadalom minél több szegletébe jut el a közösségi média, annál jelentősebben és kifinomultabban befolyásolja a kollektív politikai és közösségi hatalom kifejeződését. A technológia már megmutatta a politikai és társadalmi diskurzus természetének megváltoztatásának lehetőségét, ami a lakosság új, gyors és határozott mozgósításához vezetett a politikai és társadalmi célok elérése érdekében. Hasonlóképpen, a közösségi médiában történő adatgyűjtés lehetővé teszi az ember közösségi viselkedésének és a csoportdinamikáknak a megértését (NATO STO, 2020, 44).

4.Mesterséges intelligencia

A mesterséges intelligenciának az alap gondolata Alan Turing nevéhez kötődik, melyről 1950.-ben a „Computing Machinery and Intelligence" cikkében írt. Ezt követően 1956.-ban a „Dartmouth Summer Research Project on Artificial Intelligence" workshopon lefektették a mesterséges intelligencia tudományterület alapjait (Gyires-Tóth, 2020). E szerint egy általánosságban vett mesterséges intelligencia:

- képes környezete ismeretében döntéseket hozni,
- ezek a döntések hasonlóak a természetes intelligenciához,
- ha a környezet (akár jelentősen is) megváltozik, képes a megváltozott környezethez alkalmazkodni.

2010. környékén robbanásszerűen nőtt meg a mesterséges intelligencia iránt az érdeklődés, ami főként három dolognak volt köszönhető:

- az adatmennyiség növekedése,
- a gépi tanulási módszerek fejlődése,
- a megnövekvő számítási kapacitás.

A mesterséges intelligenciának három fajtáját különböztetik meg: az általánost, a keskenyt és a szuper mesterséges intelligenciát.

Keskeny MI-nek (Artificial Narrow Intelligence) azon eljárásokat nevezzük, melyek egy speciális témakörben (pl. képfelismerés, beszédszintézis) nagy hatékonysággal – sokszor az embernél is jobban – használhatóak, azonban más tématerületen nagyon korlátozottan vagy egyáltalán nem működnek. Az összes jelenlegi rendszer ebbe a kategóriába tartozik. A szakértők általában egyetértenek abban, hogy hosszú évtizedekbe telik majd, mire a terület eléri a fentebb említett általános mesterséges intelligencia (Artificial General Intelligence) szintjét (DIB, 2019). (A mesterséges szuperintelligencia (Artificial Super Intelligence) pedig az olyan rendszereket jelöli, melyek képesek emberi tudáson túlmutató következtetéseket, döntéseket hozni.) A mesterséges intelligenciának meghatározó ága a gépi tanulás. Gépi tanuló rendszereknek az olyan – főként statisztika alapú – algoritmusokat nevezzük, melyek szabályok explicit megadása nélkül, a folyamatból rögzített minták alapján képesek egy adott folyamatot szabályzó sajátosságok meghatározására (Gyires-Tóth, 2020).

Az általános mesterséges intelligencia (Artificial General Intelligence) fejlesztése jelentős (és potenciálisan lehetetlen) technikai kihívást jelent, annak ellenére, hogy több mint 60 éve végeznek ebben a témában kutatásokat. Nem valószínű, hogy az MI rendszerek a következő 20 évben el fogják érni ezt a kognitív képességi szintet.

5.Az Adat és a Mesterséges Intelligencia

Az Adattal közösen az MI forradalmi hatást gyakorolhat a NATO műveleteire és képességeire. A mesterséges intelligencia segítségével a sok adat felhasználható tudássá és végső soron a NATO döntési előnyévé válik.

Csakúgy, mint a kereskedelmi és az állami szektor esetében, a technológiai fejlődés lehetővé tette a katonaság és a biztonsági szféra szakemberei számára, hogy nagy mennyiségű adatot gyűjtsenek, és számos ország (kormány és fegyveres erők) alakít ki irányítási modelleket annak érdekében, hogy ki lehessen használni a Big Data előnyeit a valós idejű hírszerzés, a döntéshozatal, a szituációs tudatosság terén és az ellenfelekkel szembeni általános versenyelőny szempontjából (NATO HQ, 2021, 23).

Az Adat és az MI közötti szinergia különösen fontos a harckészültség minden aspektusát illetően, integrálásuk harci modellekbe és szimulációkba, döntéstámogató rendszerekbe, kibervédelmi rendszerekbe és autonóm járművekbe lehetővé teszik az ember és gép közötti gyors és hatékonyabb döntéshozatalt. De alkalmaznak már mesterséges intelligenciát a logisztika, a hírszerzés, a megfigyelés, a felderítés, a kibertéri műveletek, az információs műveletek, a kép-, hang-, videómanipuláció (deepfake), de a halálos autonóm fegyverrendszerek területén is.

A szakértők egyetértenek abban, hogy az MI alkalmazása a fegyveres erőkben „minden területen jelen van ... és a hadviselés minden szintjén" (Svenmarck et al., 2018). Sokan azonban az Adat-stratégia kidolgozásának korai szakaszában vannak. Így más szektorok tanulságai útmutatást adhatnak a bevált gyakorlatokról, amikor az adat irányítási modelljeikről a Big Data irányítási keretrendszerekre térnek át.

Felmerül a kérdés, hogy a mesterséges intelligencia alapú információs hadviselés mennyire befolyásolhatja a NATO döntéshozatalát. A mesterséges intelligencia által támogatott információs hadviselés olyan algoritmusok használatát vonja maga után, amelyek képesek a nagy adatok feldolgozására és azokból való tanulásra annak érdekében, hogy adott célpontok ellen támadásokat hajtsanak végre, s ezáltal elérjék a kívánt hatást az információs térben. Az MI-alapú információs műveletek az információs környezet minden egymással összefüggő dimenzióját is megcélozzák – így a fizikait, információsat, a kognitívat és az érzelmit.

Az MI-alapú információs hadviselés négy alapvető területen különbözik a „szokásos" információs hadviseléstől (NATO HQ, 2021, 60):

1. Sebesség: Az MI felgyorsíthatja a műveletek ütemét például azáltal, hogy gyorsabban azonosítja a célpontokat az algoritmusok megnövekedett mintafelismerési képessége által.

2. Hatály: Az MI kiterjesztheti az információs hadműveletek körét azáltal, hogy olyan eszközöket használ, amelyek fél-autonóm vagy autonóm módon hajtanak végre támadásokat több platformon.

3. Skálázhatóság: Az MI megnövelheti annak esélyét, hogy egy adott üzenet vagy narratíva rendkívül gyorsan elterjedjen az információs térben.

4. Kifinomultság: Az MI által egyre meggyőzőbb szintetikus médiatartalmakat (pl. deepfake) lehet létrehozni – vagyis egyre nehezebb megkülönböztetni a valós személyeket a mesterségesen létrehozottaktól.

A deepfake olyan új, mély tanuláson – ami a gépi tanulás talán leghangsúlyosabb típusa napjainkban - alapuló technológia, amellyel lehetséges úgy manipulálni kép-, hang- és videófelvételeket, hogy az azokon szereplő személyek azt mondják vagy tegyék, amiket sohasem mondtak vagy tettek. A deepfake használatának társadalmi szinten súlyos következményei lehetnek. Segítségével lehetséges például manipulálni a választásokat (mondjuk a választás előtti este megjelenik egy lejárató videó az egyik jelöltről. Ebben az esetben hiába derül ki akár rögtön a választások után, hogy a videó egy hamisítvány volt, a választás eredménye addigra már megszületett), csökkenteni az intézményekbe vetett bizalmat, súlyosbítani a társadalmi megosztottságot, aláásni diplomáciai kapcsolatokat vagy akár veszélyeztetni a nemzetbiztonságot (ez elérhető például egy olyan deepfake videó elterjesztésével, amelyen amerikai katonák Afganisztánban helyi civileket ölnek meg és közben felgyújtanak egy Koránt annak érdekében, hogy erőszakot provokáljanak az amerikai katonákkal szemben, majd nem sokkal később megjelenhet egy másik deepfake videó, amin az látható, hogy egy ismert londoni imám bosszúra szólítja fel az embereket) (Chesney – Citron, 2019). Ezek mellett azonban van egy más jellegű, de kulcsfontosságú kockázata is: a biztonságpercepció manipulálása – ezt a deepfake minden korábbi eszköznél hatékonyabban teheti lehetővé (Bereczky, 2020).

Katonai területen az Adat növeli a támadó műveletek hatékonyságát és kiterjesztését a nem hagyományos területekre, lehetővé téve az egyének és társadalmi csoportok kifinomult célzását a nemzeti hatalom eszközein keresztül (diplomáciai, információs, katonai és gazdasági). De az Adat fokozott NATO-szintű használata sebezhetőségeket hoz létre a parancsnoki döntéshozatalban, amelyeket kihasználhatóak. A célzott kiber- vagy információs támadások fókuszpontja egyre rejtettebb lesz és kifejezetten a döntéshozatal és a bizalom aláásására lesz létrehozva. A döntéshozatalban az Adatra való túlzott támaszkodás növeli a kiber- és információs támadások kockázatát és az általuk okozható kár nagyságát (NATO STO, 2020, 47).

Míg adott esetben a végeláthatatlan mennyiségű adatot felhasználva információs fölénybe is lehet kerülni, addig azonban több kihívással is szembe kell nézni, mint például a kiszámíthatatlanság, megmagyarázhatatlanság és a kihasználhatóság.

Az MI algoritmusok gyakran kiszámíthatatlan és nem konvencionális eredményeket hoznak. 2016.-ban a DeepMind nevű vállalat létrehozta az AlphaGo-nak elnevezett programját, ami 4:1 arányú győzelmet aratott a világbajnok Go játékos, Lee Sedol felett. A meccs után Sedol megjegyezte, hogy az AlphaGo meglepő és innovatív lépéseket tett. Az MI azon képessége, hogy katonai körülmények között hasonlóan rendhagyó eredményeket produkáljon, előnyt jelenthet a harcban, különösen, ha ezek az eredmények meglepik az ellenséget. Azonban elemzők arra figyelmeztetnek, hogy, ha a katonák a lehetséges veszélyek átfogó megismerése

előtt a technológia bevezetésére sietnek, akkor „technikai adósság" keletkezhet, amely kifejezés olyan MI-rendszerek kihatására utal, amelyek egyenként minimális kockázattal bírnak, de együttesen növelik a kollektív kockázatot (MITRE, 2017).

A kiszámíthatatlanságot tovább bonyolítja, hogy a legnagyobb teljesítményű MI algoritmusok jelenleg nem képesek megmagyarázni azt, hogy hogyan működnek. Például a Google létrehozott egy macskaazonosító rendszert, amely lenyűgöző eredményeket ért el a macskák azonosításában a YouTube-on. Azonban a rendszer egyik fejlesztője sem tudta meghatározni, hogy a rendszer a macskák mely jellegzetességeit használja a rendszer azonosítási folyamatában (Markoff, 2012). Az úgynevezett „megmagyarázhatóság" hiánya minden ilyen MI algoritmusban általános. Több kutatóintézet is megkísérelte már az ilyen típusú algoritmusok visszafelé történő elemzését, hogy jobban megismerjék belső folyamataikat. Az egyik ilyen tanulmányban a kutatók elemezték azt a programot, amelynek célja a függönyök képekben való azonosítása volt, és felfedezték, hogy az MI algoritmus először ágyat, és nem pedig ablakot keresett, és ennél a pontnál abbahagyta a képen a keresést. A kutatók később rájöttek, hogy ez azért van, mert a tanuló adathalmazban a függönyöket tartalmazó képek többsége hálószoba volt (Bornstein, 2016). A projekt megmutatta annak a lehetőségét, hogy a tanuló adathalmazok véletlenül olyan hibákat vezethetnek be a rendszerbe, amelyeket a felhasználók nem ismerhetnek fel azonnal vagy nem értenek meg. A megmagyarázhatóság további problémákat vethet fel katonai környezetben, mivel az MI érvelésének átláthatatlansága miatt az üzemeltetők túlságosan vagy akár egyáltalán nem bízhatnak a rendszerben. Egyes elemzők különösen aggódnak amiatt, hogy az emberek idegenkedhetnek a teljes mértékben MI-elemzésen alapuló döntés meghozatalától, ha nem értik, hogy a gép hogyan hozta létre a megoldást.

Az MI rendszerek elterjedése megnöveli a „feltörhető dolgok" számát, beleértve a kinetikus energiát szállító rendszereket (pl. mozgó járművek), amelyek viszont lehetővé tehetik, hogy ezek a tevékenységek halálos hatásokat indukáljanak. Ezenkívül az MI-rendszerek különösen kiszolgáltatottak a lopásoknak, mivel szinte teljes egészében szoftveralapúak. Ez azt is jelenti, hogy az ellopott kód akár azonnal felhasználható és tetszés szerint reprodukálható (DIB, 2019). Számos mesterséges intelligencia alkalmazást polgári használatra fejlesztettek – amik azonban akár fegyverrendszerekben történő felhasználásra is adaptálhatók – és, amiket széles körben megosztottak internetes oldalakon, ami miatt hozzáférhetővé váltak a katonai nagyhatalmak és a nem állami szereplők számára is (Nordrum, 2016).

6.Összefoglaló

Az Adat és a mesterséges intelligencia használata számtalan kiaknázatlan lehetőséget nyújt a hadviselésben, azonban ahhoz, hogy ezt a lehető legjobban ki lehessen használni, több dolognak is teljesülnie kell, és valószínűleg egy paradigmaváltás is szükségessé kell, hogy váljon. Egyrészt a kormányoknak és a biztonsági szervezeteknek világosan meg kell érteniük az Adat értékét a különböző területeken, hogy kiváló minőségű, használható, valós idejű információkat nyújtsanak stratégiai, taktikai és operatív szinten. Másrészt szükséges a szervezeti adatközpontú kultúra és az adatközpontú paradigma megalkotása - ideértve annak biztosítását, hogy az összes releváns személy rendelkezzen a szükséges készségekkel, tudással és felkészültséggel (NATO HQ, 2021, 24).

Az Adat és az MI kiemelt fontosságú lehet, ha például azt tekintjük, hogy mit írt Bogdanov és Chekinov – két ismert orosz hadtudós – még 2015-ben az új-generációs hadviselésről:

„…a stratégiai célok elérése a jövő háborúiban lehetetlen lesz az ellenség feletti információs dominancia kialakítása nélkül" (NATO HQ, 2021,58).

De egy másik információs korszak hadviseléséről szóló tanulmány is hasonlót állít: "[W]inning in the decision space is winning in the battlespace." vagyis a győzelem a döntési térben, az győzelem a csatatéren (Mancillas, 2017). És ahol az információ fegyver, ott mindenki háborúban van. Így nézünk elébe az elkövetkezendő 20 évnek.

Hivatkozások

Allen, Greg – Chan, Taniel (2017): Artificial Intelligence and National Security, Belfer Center for Science and International Affairs. 23.
https://www.belfercenter.org/sites/default/files/files/publication/AI%20NatSec%20-%20final.pdf

Allen, John – Hussain, Amir (2017): On Hyper-War.
https://fortunascorner.com/2017/07/10/on-hyper-war-by-gen-ret-john-allenusmc-amir-hussain/.

Bereczky, Nikolett (2020): Deepfake: az illúzió, mint valóság. A haza szolgálatában. 21-27.
https://dosz.hu/__doc/dokumentumfile/2020/a-haza-szolgalataban-online-kotet.pdf?fbclid=IwAR0pd7QbbQfpjzRrZ7LZlErm8WyrGg78_bvElb5ik89LGEIZzFHthMrCCnU

Chesney, Robert – Citron, Danielle Keats (2019). Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. *California Law Review* 107. 1753-1820.

CRS. Congressional Research Service (2020.11.20): Artificial Intelligence and National Security.
https://fas.org/sgp/crs/natsec/R45178.pdf

DARPA. Defense Advanced Research Projects Agency (2019): Budget Estimates FY 2020, RDT&E Program. Tech. Rep.
https://www.darpa.mil/attachments/DARPA_FY20_Presidents_Budget_Request.pdf

DIB. Defense Innovation Board (2019): AI Principles: Recommendations on the Ethical Use of Artificial Intelligence by the Department of Defense – Supporting Document. 25.
https://media.defense.gov/2019/Oct/31/2002204459/-1/-1/0/DIB_AI_PRINCIPLES_SUPPORTING_DOCUMENT.PDF

Giesea, Jeff. (2017): It's Time to Embrace Memetic Warfare. Open Publications, NATO StratCom, Riga, Latvia.
https://www.act.nato.int/images/stories/media/doclibrary/open201705-memetic1.pdf

Gyires-Tóth, Bálint (2020): A mélytanulás múltja, jelene és jövője. Híradástechnika LXXV., Budapest.
https://www.hte.hu/documents/10180/4681952/HT_2020_ksz1_MJIK2019_All.pdf

Hoffman, Frank G. (2019): Healthy Skepticism about the Future of Disruptive Technology and Modern War - Foreign Policy Research Institute. https://www.fpri.org/article/2019/01/healthy-skepticism-about-the-future-of-disruptive-technology-and-modern-war/

Mancillas, James W. (2017): "Integrating AI into Military Operations: A Boyd Cycle Framework," in Closer than You Think: The Implications of the Third Offset Strategy for the US Army. Carlisle, PA: US Army War College Press. 74.

Marino, Thomas (2017): Maintaining NATO's Technological Edge: Strategic Adaptation And Defence Research & Development. General Report, NATO Parliamentary Assembly, Brussels. https://www.nato-pa.int/download-file?filename=sites/default/files/2017-11/2017%20-%20174%20STC%2017%20E%20bis%20-%20MAINTAINING%20NATO%27S%20TECHNOLOGICAL%20EDGE.pdf

Markoff, John (2012): "How Many Computers to Identify a Cat? 16,000.". The New York Times. http://www.nytimes.com/2012/06/26/technology/in-a-big-network-of-computers-evidence-of-machine-learning.html

MITRE. The MITRE Corporation (2017): "Perspectives on Research in Artificial Intelligence and Artificial General Intelligence Relevant to DOD". Office of the Assistant Secretary of Defense for Research and Engineering. 32.

NATO HQ (2021): NATO Decision-Making in the Age of Big Data and Artificial Intelligence. https://www.iai.it/sites/default/files/978195445000.pdf

NATO STO. NATO Science & Technology Organization (2020): Science & Technology Trends: 2020-2040. Brussels. https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf

Nordrum, Amy (2016): "Darpa Invites Techies to Turn Off-the-Shelf Products into Weapons in New 'Improv' Challenge," IEEE Spectrum. https://spectrum.ieee.org/tech-talk/aerospace/military/darpa-invites-techies-to-turn-offtheshelf-products-into-weapons-in-new-improv-challenge

Svenmarck, Peter – Luotsinen, Linus – Nilsson, Mattias – Schubert, Johan (2018): Possibilities and Challenges for Artificial Intelligence in Military Applications. NATO Big Data and Artificial Intelligence for Military Decision Making Specialist's Meeting, NATO Science & Technology Organization.

Von Clausewitz, Carl (1989): On war. Princeton University Press. Princeton, New Jersey.

Wilder-James, Edd (2014): Defining Big Data. Forbes. https://www.forbes.com/sites/edddumbill/2014/05/07/defining-big-data/?sh=12c644bc5667