Szemelvények a katonai műszaki tudományok eredményeiből III.

Szerkesztette
Földi László

LUDOVIKA
EGYETEMI KIADÓ

Szemelvények a katonai műszaki tudományok eredményeiből III.

Szemelvények a katonai műszaki tudományok eredményeiből III.

Hallgatói kötet

Szerkesztette

Földi László

LUDOVIKA
EGYETEMI KIADÓ

Budapest, 2022

Szerzők

Albert Gábor
Bakos Tamás
Bencsik Gábor
Berta Katalin
Deli Gábor
Domán László
Gajdács László
Győző-Molnár Árpád
Horváth Attila
Horváth Ákos
Igaz-Danszky Tamás
Jagodics Ibolya
Kersák József Zsolt
Kiss Ádám István
Kovács Gergely
Kovács-Horváth Adrienn
Kutassy Emese
Lakatos Bence R.
Leskó György
Lévai Zsolt
Major Gábor
Marlok Tamás
Matusz Márk Péter
Szabadföldi István
Szajkó Gyula
Szilágyi Tibor
Tamás Enikő Anna
Teknős László
Terék Tamás
Tímár Attila
Tóth Bence
Vass Gyula

Lektorok

Berek Tamás
Bíró Tibor
Haig Zsolt
Horváth Attila
Kátai-Urbán Lajos
Németh András
Padányi József

Ludovika Egyetemi Kiadó
Székhely: 1089 Budapest, Orczy út 1.
Kapcsolat: info@ludovika.hu
A kiadásért felel: Deli Gergely rektor
Felelős szerkesztő: Karácsony Fanni
Olvasószerkesztő: György László
Korrektor: Bíró Csilla, Pokorádi Zsófia
Tördelőszerkesztő: Stubnya Tibor

ISBN 978-963-531-703-5 (elektronikus PDF) | ISBN 978-963-531-704-2 (ePub)

© A szerkesztő, 2022
© A szerzők, 2022
© Ludovika Egyetemi Kiadó, 2022

Minden jog védve.

Tartalom

Szabadföldi István

A mesterséges intelligencia alkalmazási lehetőségei az elektronikai hadviselésben

Absztrakt

A mesterséges intelligencia (MI) egyre nagyobb szerepet játszik a katonai műveletek tervezésében és támogatásában, a hírszerzésben és elhárításban, elemzésben, az autonóm fegyverrendszerek és járművek terén. Az MI egyik legfontosabb szerepe a Big Data „5V-s kihívása" által jelentett kockázat csökkentése (volume – mennyiség, variety – változatosság, velocity – sebesség, veracity – valódiság, value – érték). Az összadatforrású felderítés kiterjedt és átfogó hírszerzési műveletekkel szerzi be és dolgozza fel a sikeres művelet végrehajtásához szükséges információkat. Az elektronikai hadviselés, amely elektromágneses energiát használ az elektromágneses spektrum ellenség általi használatának felderítésére, csökkentésére vagy megakadályozására, valamint a saját csapatok általi hatékony felhasználásának biztosítására, fontos eleme az információs műveleteknek, amelyek számos kihívással néznek szembe. Idetartoznak a kiterjesztett spektrumú átviteli módok, mint a közvetlen szekvenciás szórt spektrum (DSSS), a frekvenciaugrásos szórt spektrum (FHSS) és az időugrásos szórt spektrum (THSS) alapú módszerek, amelyek megnehezítik a rádiófrekvenciás kommunikáció felfedését és lehallgatását. A mesterséges intelligencia használata áttörést jelenthet ezen kihívások kezelésében.
Kulcsszavak: *MI, összadatforrású felderítés, elektronikai hadviselés, Big Data, szórt spektrum technikák*

Artificial Intelligence Application Opportunities in the Electronic Warfare

Artificial Intelligence (AI) is playing an increasing role in the planning and support of military operations. It is becoming a key tool in intelligence and analysis of enemy intelligence, in the use of autonomous weapon systems and vehicles. One of the most important roles of AI is to reduce the risk posed by Big Data's "5V challenge" (volume, variety, velocity veracity, value). All-Source Intelligence obtains and processes the information needed to perform a successful operation with extensive and comprehensive intelligence operations. Electronic warfare, which uses electromagnetic energy to detect, reduce, or prevent the use of the electromagnetic spectrum by the enemy and ensure its effective use by its own troops, is an important component of information operations that faces many challenges. These include extended spectrum transmission modes, Direct Sequence Spread Spectrum Technique (DS SST), Frequency Hopping Spread Spectrum Technique (FH SST), and Time Hopping Spread Spectrum (TH SST) methods that make it difficult to intercept radio electronic communications. The use of Artificial Intelligence can be a breakthrough to tackle those challenges.
Keywords: *Artificial Intelligence, All-Source Intelligence, Electronic Warfare, Big Data, Spread Spectrum Technique*

Bevezető

A hadművészet történetében kezdetektől fontos szerepet játszott az információszerzés és annak megfelelő feldolgozása. A digitalizáció – azaz a 4. ipari forradalom – alapvető változásokat hozott az információszerzés és -feldolgozás vonatkozásában. A szenzorok elterjedése, az IoT/IoMT/IoBT, a Big Data, a mesterséges intelligencia (MI), a virtuális és kiterjesztett valóság (VR/AR) eszközei a tervezés, helyzetfelismerés és döntéstámogatás adatforrásainak exponenciális bővülését hozta el hatást gyakorolva a logisztikai és a műveleti tervezésre, beleértve a modellezést és a szimulációt. Az információs műveleteknek úgy a hadászati-stratégiai, mint a hadműveleti-harcászati vonatkozásában fontos, sőt döntő szerepe van, hiszen a saját és az ellenség technikai felkészültségének, képességeinek, helyzetének ismerete elsődleges a sikeres tervezés és a műveletek végrehajtása szempontjából.

A MI egyre növekvő szerepet játszik a katonai műveletek tervezésében, támogatásában, kulcsfontosságú eszközzé válik a hírszerzésben és az ellenség hírszerzésének elemzésében, az autonóm fegyverrendszerek, járművek alkalmazásában.

Az összadatforrású felderítés kiterjedt adatszerző műveletekkel gyűjti be és dolgozza fel a sikeres művelet végrehajtásához szükséges adatokat értelmezhető információvá.

Az elektronikai hadviselés azon katonai tevékenység, amely az elektromágneses energiát felhasználva meghatározza, felderíti, csökkenti vagy megakadályozza az elektromágneses spektrum ellenség részéről történő használatát, és biztosítja annak a saját csapatok általi hatékony alkalmazását.[1]

Az elektronikai hadviselés az információs műveletek fontos eleme, amely számos kihívással rendelkezik.

Ezek között kell említeni a kiterjesztett spektrumú adásmódokat, a fázisugratásos vagy direkt szekvenciális (*direct sequence spread spectrum technique* – DS SST), a frekvenciaugratásos (*frequency hopping* – FH SST), illetve az időugratásos (*time hopping spread spectrum* – TH SST) módok alkalmazását, amelyek nehezítik a rádiófrekvenciás információátvitel lehallgatását.

Ebben jelenthet áttörést a mesterséges intelligencia alkalmazása.

Mi a mesterséges intelligencia (MI)? – Áttekintés és demisztifikáció

Az MI-nek – bár mint fogalom már az 1950-es évek óta használt – ma sincs általánosan elfogadott meghatározása. Az MI nem önálló applikációként értelmezhető, hanem olyan technológia, amely meglévő funkcionális megoldásokat támogat, és alapvetően olyan algoritmusokon alapul, amelyeket célzottan, meghatározott problémák megoldására fejlesztettek ki, amely algoritmusok egyre nagyobb adatkészletek összegyűjtésére, rendszerezésére, feldolgozására, elemzésére, továbbítására és az ezekre való

[1] Haig Zsolt et al.: *Elektronikai hadviselés.* Budapest, NKE, 2014. 33.

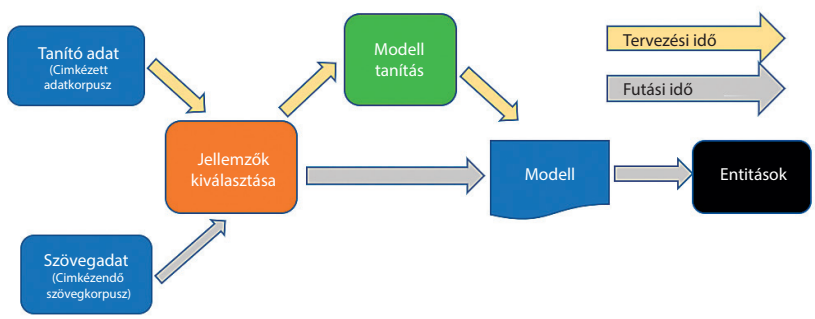
reagálásra alkalmasak, azaz képesek az emberi értelem kognitív képességének megfelelő, illetve azt közelítő műveletekre.

Az MI-nek alapvetően három típusát különböztetjük meg:

– Gyenge mesterséges intelligencia, amelyet szűk mesterséges intelligenciának *(narrow MI)* is neveznek, olyan számítógépes rendszer, amely az embernél hatékonyabban el tud végezni egy szűken meghatározott feladatot. Itt tartunk ma.
– Általános mesterséges intelligencia *(general MI),* amelyet olykor „erős MI-nek" is neveznek, képes meghaladni az emberi eredményeket bármilyen intellektuális feladatban. Például ezzel a típusú MI-vel működő robotokat láthatunk olyan filmekben, ahol tudatos gondolkodásra épülő saját céljaiknak megfelelően tevékenykednek.
– Mesterséges szuperintelligenciával (*artificial super intelligence* – ASI) rendelkező számítógép képes lenne az embert csaknem minden területen túlszárnyalni, többek között a tudományos kreativitásban, az általános bölcsességben és a társadalmi készségekben is.

Az MI egy részhalmazának tekinthető a gépi tanulás (*machine learning* – ML), amely matematikai adatmodellekkel tanít be számítógépeket közvetlen felügyelettel vagy anélkül. A gépi tanulás algoritmusokkal azonosít mintákat az adatokban, amelyekkel adatmodellt készít, majd előrejelzéseket és válaszokat ad.

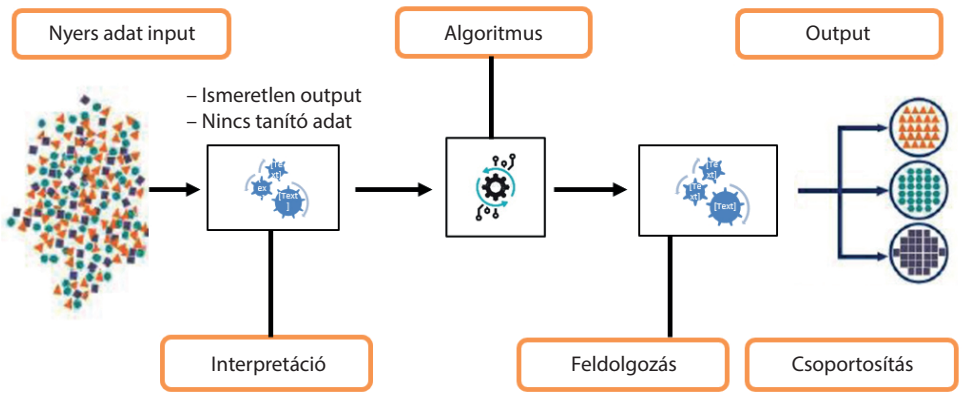
A felügyelt tanulás (*supervised learning* – SL) olyan folyamat, amelynél az osztályozó paramétereket az ismert kategóriákból álló minták felhasználásával a kívánt teljesítmény elérése érdekében kiigazítják. Az SL egy funkcionális gépi tanulási feladatot képez a címkézett tanító adatokból. A tanuló adatok tanító példákat tartalmaznak. Az SL-ben minden példa egy bemeneti objektumból (általában egy vektorból) és egy várható kimeneti értékből (felügyelt jelből) áll.



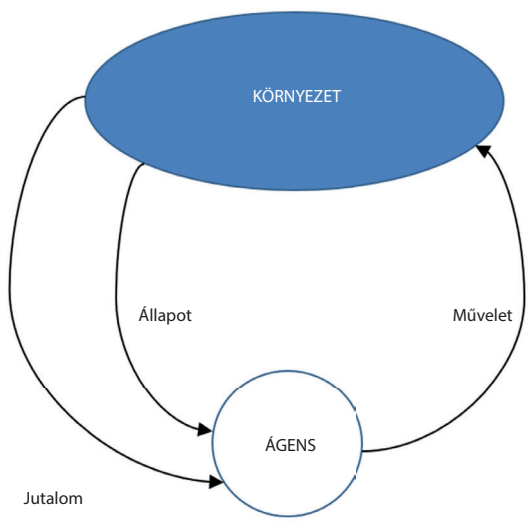
1. ábra: A felügyelt tanulás (SL) diagramja

Forrás: Wei Wang et al.: Investigation on Works and Military Applications of Artificial Intelligence. *IEEE Access.* 8. (2020). 131614–131625.

Felügyelet nélküli tanulás – *unsupervised learning* (UL) – során a tanulási adatok nincsenek címkézve, és a tanulási cél a megfigyelt értékek osztályozása vagy megkülönböztetése. Lényegében ez egy statisztikai módszer, amely képes felismerni a jelöletlen adatok potenciális struktúráit. A felügyelet nélküli tanulás diagramját a 2. ábra mutatja. Az UL-t gyakran használják az adatbányászatban, hogy feltárjanak, felfedezzenek valamit nagy mennyiségű, strukturálatlan adatban. Ilyen például a képfelismerés.



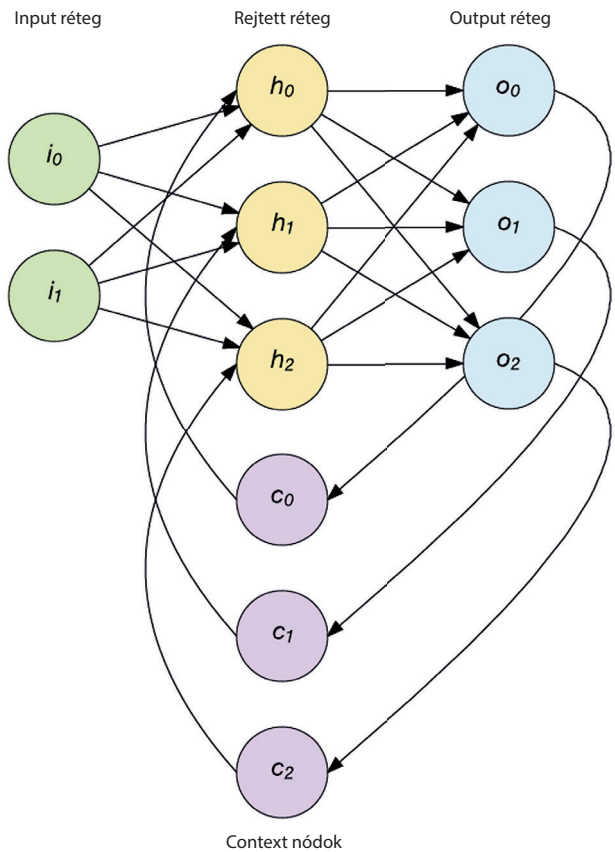
2. ábra: A felügyelet nélküli tanulás (UL) diagramja
Forrás: Wei Wang et al. (2020): i. m.



3. ábra: A megerősítő gépi tanulás diagramja
Forrás: Wei Wang et al. (2020): i. m.

Az ML fejlett szintje a megerősítő gépi tanulás – *reinforcement learning* (RL) – amikor a rendszert pozitív visszacsatolásokkal erősítik meg a felismerésekben. Az RL-t a kontrollelméletből (control theory), a statisztikából, a pszichológiából és kapcsolódó tárgyakból fejlesztették ki, és Pavlov feltételesreflex-kísérletére vezethető vissza.

A mélytanulás – *deep learning* (DL) – esetében a gépet nagy mennyiségű adattal tanítják be összetett feladatokra az emberi agy analógiájára létrehozott neurális hálózatok segítségével, amelyben a neuronok (node-ok) egy-egy részfunkció végrehajtását végzik, illetve összegzik azokat. Itt fontos megemlíteni az úgynevezett *black box* jelenséget, amelynél az egyes neuronszintekben (hidden layer) végbemenő folyamatot az ember már nem képes követni, illetve átlátni, így azok jelentős megbízhatósági kockázatot hordoznak magukban.[2]



4. ábra: Egy neurális háló strukturális diagramja
Forrás: Wei Wang et al. (2020): i. m.

[2] Wei Wang et al. (2020): i. m.

Az MI-vel kapcsolatos publikációk és nyilvános események egyre növekvő száma ellenére, vagy inkább ezek miatt, továbbra is széles körben mítoszok és tévhitek terjednek arról, hogy mi is az MI valójában, és mire képesek az MI-rendszerek. Ezek a félrevezetések megnehezítik, nem segítik az MI lehetőségeinek megértését és kockázatait általában, de különösen a védelmi-biztonsági területen.

Az MI-technológia lehetőségeit és korlátait világosan meg kell érteni és figyelembe kell venni, különösen a döntéshozók számára, hogy elkerüljék a nehezen vagy nem elérhető célokat kitűző projektek elindítását.[3]

Feltörekvő és formabontó technológiák (*emerging and disruptive technologies* – EDT) társadalmi és biztonsági vonatkozásai

A technológia demokratizálódása (azaz csökkentett költségek és jobb hozzáférés) biztonsági kockázatokat hoz magával, ami a szabályozások szintjének újragondolását vetíti előre annak érdekében, hogy megvédjék a társadalmat azoktól a csúcstechnológiát alkalmazó rosszindulatú szereplőktől, akik képesek könnyen hozzáférhető módon rendkívül veszélyes berendezéseket és megoldásokat előállítani. Mára különösen a vegyi, biológiai, radiológiai és nukleáris technológiákat (CBRN) hagyományosan szigorúan szabályozták a proliferáció megelőzése érdekében, de ezek a szabályozások nem elegendőek, ha „bárki felállíthat egy biotechnológiai laboratóriumot a kertben vagy az alagsorban”.[4]

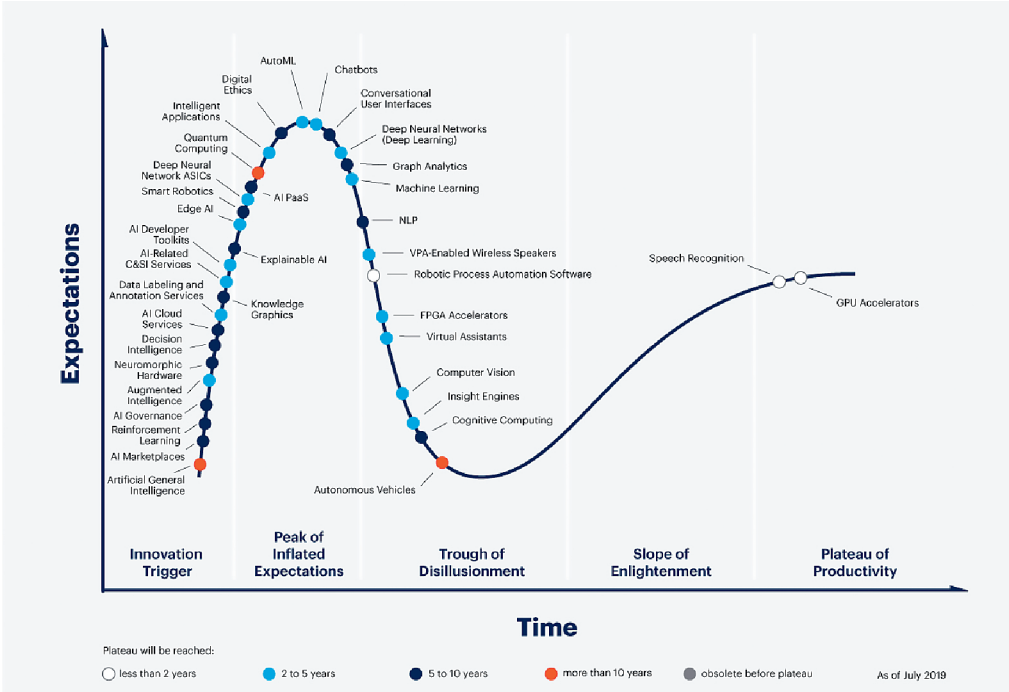
Az MI fejlődésének menete

Az MI az 1950-es évek közepén három fejlődési cikluson ment keresztül. Az első időszakban a megoldások a szabályokon alapuló megközelítésekre (döntési fák, logikai és fuzzy logika) fókuszáltak, például szakértői rendszerek. A második szakasz a statisztikai módszerek (azaz a felügyelt, felügyelet nélküli és megerősítő tanulás) fejlesztésére és alkalmazására összpontosított. Az ilyen gépi tanulási módszerek nagyon sikeresek voltak, és jó alapot nyújtottak az e-mailes spamszűréstől az internetes keresőmotorok kifejlesztéséig. A fejlődés harmadik szakasza az emberhez hasonló tanulási rendszerek (neurális hálózatok, mélytanulás) használatára összpontosít.[5]

[3] Lora Saalman (szerk.): *The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk.* Stockholm, Sipri, 2019. 11

[4] NATO Science & Technology Organization: *Science & Technology Trends 2020–2040. Exploring the S&T Edge.* 2020. 35.

[5] NATO Science & Technology Organization (2020): i. m. 51.; GAO: *Artificial Intelligence. Emerging Opportunities, Challenges, and Implications.* 2018. március.



5. ábra: Az MI Gartner-féle hype-ciklusa
Forrás: Top Trends on the Gartner Hype Cycle for Artificial Intelligence, 2019. *Gartner,* 2019. szeptember 12.

A Gartner-féle hype-ciklus jól mutatja az MI várható technikai fejlődését és alkalmazását.

Az MI katonai alkalmazása

Az MI fogalmának megjelenésével gyakorlatilag egyidős annak katonai célra történő alkalmazása a katonai műveletek tervezésében, támogatásában, a hírszerzésben és az ellenség hírszerzésének elemzésében. Az MI egy másik alkalmazási területe az autonóm fegyverrendszerek, járművek szegmense. Az MI alkalmazásától várható az ember-gép interfészek *(machine-learning, man-machine teaming)* vonatkozásában a katonai alkalmazások során elérhető nagyobb pontosság és hatékonyság.

A MI egyik legfontosabb szerepe a Big Data alapvető „3V kihívásából" (*volume* – mennyiség, *variety* – változatosság és *velocity* – sebesség) adódó kockázat csökkentése, de a másik „2V" (*veracity* – megbízhatóság, *value* – érték) kihívásnak történő megfelelésben is jelentős szerepe van.

Az MI katonai alkalmazási területeit az alábbi felsorolásban foglalta össze a NATO Science and Technology Committee (STC) számára 2019-ben készített jelentés:[6]

- harctéri sebesültellátás;
- C4ISR (parancs, vezérlés, kommunikáció, számítógép, hírszerzés, felügyelet és felderítés);
- kiberbiztonság és -védelem;
- elektronikai hadviselés;
- emberierőforrás-menedzsment;
- információs és döntéstámogatás;
- hírszerzés;
- logisztika;
- békefenntartó műveletek;
- autonóm robotrendszerek;
- közösségi média;
- kiképzés.

A fentieken túl, más megközelítésben, két rendkívül fontos területet emel ki az EU a védelempolitikai programjával összhangban kiírt EDIDP-MI-2020 pályázati felhívásban: a helyzetfelismerés és döntéshozatal támogatása, valamint a tervezés (például logisztikai tervezés, műveleti tervezés), beleértve a modellezést és a szimulációt.[7]

Az MI katonai alkalmazásával kapcsolatos várakozások

Ami az MI jövőbeli katonai alkalmazásával kapcsolatos elvárásokat illeti, a NATO az elkövetkező húsz évben, négy jellemzőt ad meg a számos kulcsfontosságú fejlett katonai technológia meghatározásához.[8]

Az MI-megoldások elsősorban *intelligensek* lesznek, vagyis integrált MI-t, tudásközpontú elemzési képességeket és szimbiotikus MI-emberi intelligenciát használnak fel arra, hogy új, formabontó alkalmazásokat nyújtsanak a technológiai spektrumban.

Másodszor, az MI-megoldások *összekapcsolódnak (interconnected).* Kihasználják a virtuális és fizikai tartományok hálózatát, beleértve az érzékelők, szervezetek, egyének és autonóm ügynökök hálózatát, amelyek új titkosítási módszerekkel és elosztott főkönyvi technológiákkal (*blockchain* – blokklánc) kapcsolódnak egymáshoz.

Az izraeli Rayzone Group TA9-es adatelemző rendszere[9] kiváló példája az MI, a Big Data és az IoT adatfúziós integrációjának, amely természetesen a katonai és polgári

[6] Matej Tonin: *Artificial Intelligence: Implications for NATO's Armed Forces.* 2019. október 13. 5.
[7] European Commission: *European Defence Industrial Development Programme (EDIDP).* 2020. 25.
[8] NATO Science & Technology Organization (2020): i. m.
[9] Lásd: www.rayzone.com/

hírszerzői/elhárítói technológiai fejlesztésekben gyökerezik, de amely már az üzleti hírszerzés *(business intelligence)* vállalati környezetében is hatékonyan alkalmazható.

Harmadszor, *elosztottak* lesznek. Vagyis decentralizáltak és mindenütt jelen lévők, széles érzékelési tartománnyal rendelkező szenzorokkal, adattárolókkal és számítási kapacitással támogatják a katonai műveletek céljai elérését.

Negyedszer pedig *digitálisak* lesznek. Ez azt jelenti, hogy digitálisan integrálják a humán, a fizikai és az információs területeket az új diszruptív hatások támogatása érdekében.[10]

Kulcsterületek az MI katonai alkalmazása előrehaladásának vizsgálatához

> „A Pentagon vizsgálja, hogyan lehetne kihasználni az MI-t a harctéri autonómia, hírszerzési elemzés, nyilvántartás nyomon követése, prediktív-előrejelző karbantartás és a katonai orvoslás terén elérendő előnyök érdekében. Az MI a Védelmi Minisztérium (DoD) kulcsfontosságú növekvő volumenű beruházási területe, közel egymilliárd dollárral a 2020-as költségvetésben. A DoD közös mesterséges intelligencia központja (JMIC) költségvetése megduplázódott, meghaladja a 208 millió dollárt, s jelentős növekedés várható a 2021-es évben és azon túl is. A katonaság jelenleg arra törekszik, hogy integrálja a fegyverrendszerei fejlesztéseibe az MI-t, a humán műveleteket kibővítse MI által vezérelt robot manőverekkel a harctéren és fokozza a katonai tűzerő pontosságát."[11]

A gépi tanulás matematikai algoritmusokat és képleteket használ a minták kivonására az adatok tömegéből. Azonban ha egy ellenséges szereplő elegendő mennyiségben látja az MI-rendszerünk által kapott bemeneti és kimeneti adatokat, abból kikövetkeztetheti, hogy milyen algoritmusok működnek, hasonlóan a *reverse engineering*hez. A folyamat az egymással szemben álló matematikusok közötti csatává válik hasonlóan a II. világháború és a hidegháború kódfeltörő versenyeihez.[12]

A C4ISR (parancs, irányítás, kommunikáció, számítógépek, hírszerzés, felügyelet és felderítés) esetében MI-vel támogatott autonóm rendszereket használnak, amelyek az „unalmas, piszkos, veszélyes" (3D: *dull, dirty and dangerous*) vagy költséges feladatokat képesek végrehajtani.[13] A háborús szcenáriók MI általi döntéstámogatása és az MI által ajánlott cselekvési tervek (COA) a Google Home-hoz, az Apple Sirihez vagy az Amazon Alexához hasonló virtuális asszisztensekkel érhetők el.

Az autonóm rendszerek, illetve járművek (UxV-k) sokkal magasabb hatékonysággal és biztonsággal működhetnek MI-s támogatással.

[10] NATO Science & Technology Organization (2020): i. m. 6.

[11] DoD Growth in Artificial Intelligence: The Frontline of a New Age in Defense. *Breaking Defense,* 2019. szeptember 18.

[12] *Artificial Intelligence. The Frontline of a New Age in Defense.* (É. n.) 18.

[13] *Unmanned Systems Roadmap 2007–2032.* 2007.

Az MI várhatóan analitikai megoldások kidolgozásával segít a NATO-n belül a hosszú távú kapacitástervezésben *(capability planning),* ideértve a döntéshozatalt, azaz komplex tényezők értékelésének támogatását a döntéshozók számára.

A CBRN-veszélyek gyors észlelésére, azonosítására és nyomon követésére (DIM) vonatkozó NATO-követelmények kielégítése érdekében az MI alkalmazása javítja a detektálás, az érzékelők integrálásának és az adatfúziónak az autonómiáját. Orvosi alkalmazás esetén az MI potenciálisan segítséget nyújthat az esetalapú klinikai ismeretek, a diagnosztika és a kezelés legjobb gyakorlatainak kidolgozásában, a halálozás csökkentésére és az alapvető funkciók fenntartására/helyreállítására veszélyeztetettség esetén, a teljes küldetés vonatkozásában. Az MI automatizált döntési és diagnosztikai támogató eszközöket is nyújthat az új traumatikus esetekkel foglalkozó orvosok segítésére.

Felismerve az MI fejlesztése és alkalmazása technológiai vezető szerepének a fontosságát, a NATO 2020-ban elindította a Military Uses of Artificial Intelligence, Automation, and Robotics (MUAAR) projektet a Multinational Capability Development Campaign (MCDC) keretében.[14]

Az MI és a Big Data fejlett adatelemzés (Advanced Analytics – BDAA) várható hatása a katonai alkalmazásokban

A mesterséges intelligencia szorosan kapcsolódik a Big Data technológiához. A hatékony MI-alkalmazáshoz szükséges adatbevitel kulcsfontosságú sikertényező, amely sokféle forrással rendelkezik. Ezért a Big Data technológiai fejlődése döntő hatással van az MI-megoldásokra. Az Advanced Data Analytics fejlett analitikai módszereket jelent nagy mennyiségű információ megértéséhez és megjelenítéséhez. A BDAA-nak négy alapvető eleme az adatgyűjtés, az érzékelők, a kommunikáció, az elemzés és a döntéshozatal.[15]

Az MI kritikus kihívásai

A fent említett lehetőségek és képességek elérése és maradéktalan kiaknázása érdekében a mesterséges intelligenciának további fejlődésre van szüksége több területen.

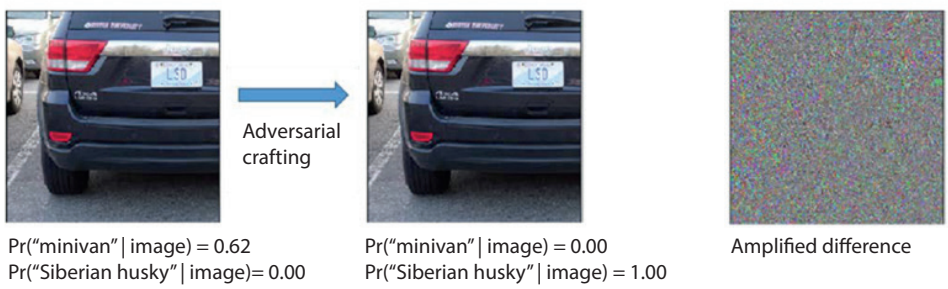
Ezek egyike a *black box,* azaz a fekete doboz problémájának megoldása. Az MI black box problémája a mesterséges neurális hálózatok alkalmazásában jelentkezik. A neurális hálózatok rejtett csomópont- (node) rétegekből állnak. Ezen csomópontok mindegyike feldolgozza az adott inputot, és az outputot továbbítja a következő csomópontrétegnek. A mélytanulás nagy méretű mesterséges neurális hálózatot használ, sok rejtett réteggel, amely önmagát „tanítja" a minták felismerésével. A probléma abban rejlik, hogy nem láthatjuk, amit a csomópontok „megtanultak", sem a rétegek közötti kimenetet, sem

[14] NATO: *Military Uses of Artificial Intelligence, Automation, and Robotics (MUAAR).* 2020.
[15] NATO Science & Technology Organization (2020): i. m. 42.

a következtetést. Tehát nem tudhatjuk, hogyan elemzik a csomópontok az adatokat. Ez az MI fekete doboza.

Az *explainable AI,* azaz magyarázható MI jelent megoldást a black box problémára, amely olyan eredményeket hoz létre, amelyeket az ember megérthet és megmagyarázhat. Amíg az ilyen funkcionalitás elérhetővé nem válik, a fekete doboz problémája okot ad arra, hogy továbbra is óvatos maradjon az MI-vel szemben.[16]

A másik komoly kihívás az ellenséges célú inputhamisítás. A *deep neural network* (DNN) mély neurális hálózat esetén be lehet állítani a bemeneti jelet úgy, hogy az osztályozási rendszer meghibásodjon. Ha a bemeneti jel dimenziója nagy, ami jellemző például képek esetében, gyakran elég, ha a bemenet egyes elemeit (pixelek) észrevehetetlenül kis mértékben megváltoztatják, és a rendszert máris becsapják ezzel. Az alábbi ábra a manipuláció előtti és utáni képet, valamint a manipuláció előtti és utáni osztályok valószínűségét mutatja. Látható hogy a kép ugyanaz, de a rendszer szibériai huskynak ismerte fel a minivant.[17]



6. ábra: A minivanből hogy lesz szibériai husky?
Forrás: Peter Svenmarck – Linus Luotsinen – Mattias Nilsson – Johan Schubert: Possibilities and Challenges for Artificial Intelligence in Military Applications, *Conference: NATO Big Data and Artificial Intelligence for Military Decision Making Specialists' Meeting at: Bordeaux, France*, 2018.

Az eredeti (balra) és a manipulált (középen) kép „abszolút különbsége" (20-as faktorú erősítéssel) jobbra látható. A manipulált képet (középen) Kurakin alapvető iteratív módszerével (BIM) állítják elő.

[16] Carlos Zednik: Solving the Black Box Problem: A Normative Framework for Explainable Artificial Intelligence. *Philosophy & Technology,* 34. (2021). 265–288.
[17] Peter Svenmarck et al.: *Possibilities and Challenges for Artificial Intelligence in Military Applications.* 2018. 7.

Elektronikai hadviselés (EHV) – electronic warfare (EW)

Hasonlóképpen az MI definíciójához, az EW definíciója is fejlődött az elmúlt évtizedekben.

A NATO az elektronikai hadviselést az elektromágneses energiát (EM) kiaknázó katonai műveletként határozza meg a helyzetfelismerés és a támadó és védekező hatások létrehozása érdekében.

Az amerikai haderők közös doktrínájában az EW kifejezés olyan katonai tevékenységet jelent, amely magában foglalja az EM-energia és az irányított energia (DE) felhasználását az elektromágneses spektrum (EMS) ellenőrzésére vagy az ellenség megtámadására. Eszerint az EW három részből áll: *electronic attack* (EA), *electronic protection* (EP) és *electronic warfare support* (ES).[18]

Az EW-tevékenységek besorolását illetően még a nyugati szövetségen belül is különböző definíciók léteznek. A NATO-szabvány szerint három EW-művelet létezik: elektronikai támadás (*electronic attack* – EA), elektronikai védelem (*electronic defence* – ED) és elektronikai megfigyelés (*electronic surveillance* – ES). (AJP-3.6 [B] és AJP-3.6 [C].)

Az amerikai fegyveres erők új közös doktrínája szerint azonban az EW elektronikai támadásból (EA), elektronikai védelemből (e*lectronic protection* – EP) és elektronikai támogatásból (*electronic support* – ES) áll.[19]

Ami a taktikai szintű EW-műveleteket illeti, további definíciók léteznek, úgymint *electronic counter measures* (ECM), *electronic counter-counter measures* (eccm) és *electronic support measures* (ESM).

2020-ban az USA DoD felcserélte az „elektronikai hadviselés" kifejezést az „elektromágneses hadviselés" kifejezéssel.[20]

A jelenlegi magyar (MH ÖHD EHV) doktrína a következőképpen határozza meg az elektronikai hadviselést:

> „Az elektronikai hadviselés olyan hatásalapú katonai tevékenységek/műveletek összessége, amelyek elektromágneses környezetben, az elektromágneses energia tudatos használatával biztosítják az elektromágneses műveletek részeként végrehajtott támadó és védelmi jellegű hatások/célok elérését. Az EM (elektromágneses) spektrumot hasznosító katonai tevékenység, amely magában foglalja az elektromágneses keresést, a sugárzások, beleértve az irányított energiát, észlelését és azonosítását, és az elektromágneses energia felhasználása az ellenség megakadályozására vagy korlátozására az EM spektrum hatékony kihasználása és a saját csapatok általi használhatóság érdekében."

Az elektronikai támogatás (*electronic support* – ES) az elektronikai hadviselés azon eleme, amely az ellenség helyzetére vonatkozó tájékozottság és a fenyegetés késedelem

[18] *Electronic Warfare.* Joint Publication 3-13.1. 2012. február 8.

[19] *Joint Electromagnetic Spectrum Operations.* Joint Publication 3-85. 2020. május 22. 21.

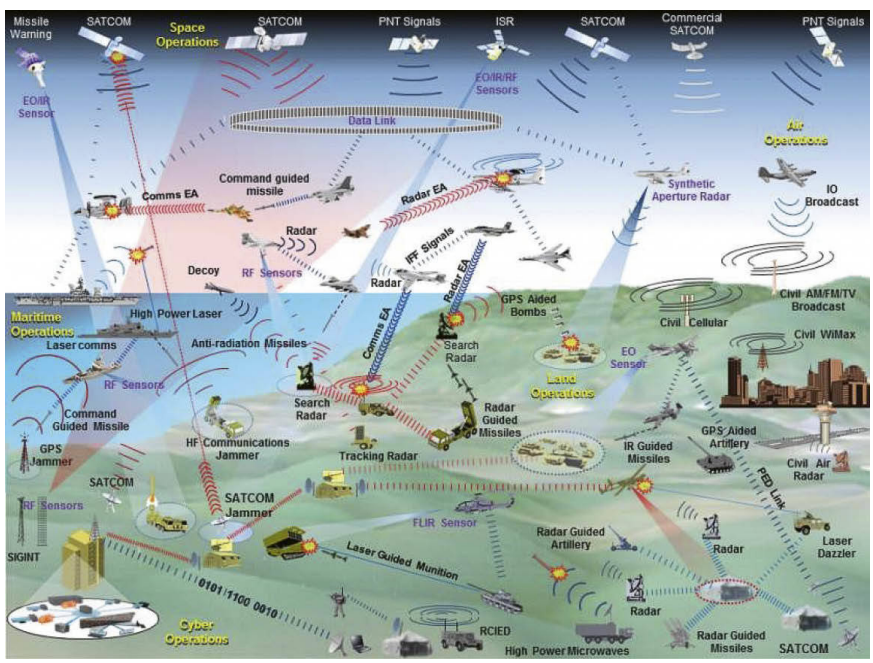
[20] GAO: *Electromagnetic Spectrum Operations. DOD Needs to Address Governance and Oversight Issues to Help Ensure Superiority.* 2020. december. 1.

nélküli felismerése céljából magába foglalja az elektromágneses kisugárzások kutatását, felfedését és azonosítását, valamint a kisugárzók helyének meghatározását.

Az elektronikai támadás (*electronic attack* – EA) az elektronikai hadviselés azon elemei, amelyek magukba foglalják az elektromágneses és egyéb irányított energiák alkalmazását abból a célból, hogy megakadályozzák vagy korlátozzák az elektromágneses spektrum ellenség által való hatékony használatát.

Az elektronikai védelem (*electronic defence* – ED) az elektronikai hadviselés azon aktív és passzív elemei, amelyek biztosítják az elektromágneses spektrum saját részről történő hatékony használatát az ellenség elektronikai megfigyelése, illetve támadása, valamint a saját csapatok által okozott nem szándékos rádiózavarok előfordulása esetén is.[21]

A 7. ábra a mai harctér rendkívül összetett környezetét ábrázolja az EW-műveletek és harceszközök különböző szintjeivel. Az EW fejlődése – főként a műveletek következményei, valamint az új technológiák által megkövetelt és kínált változások miatt – az EMS elszigetelt műveleteiből az elektromágneses környezetben (EME) történő egyesített elektromágneses műveletek (EMO) irányába történő elmozdulást eredményezte.

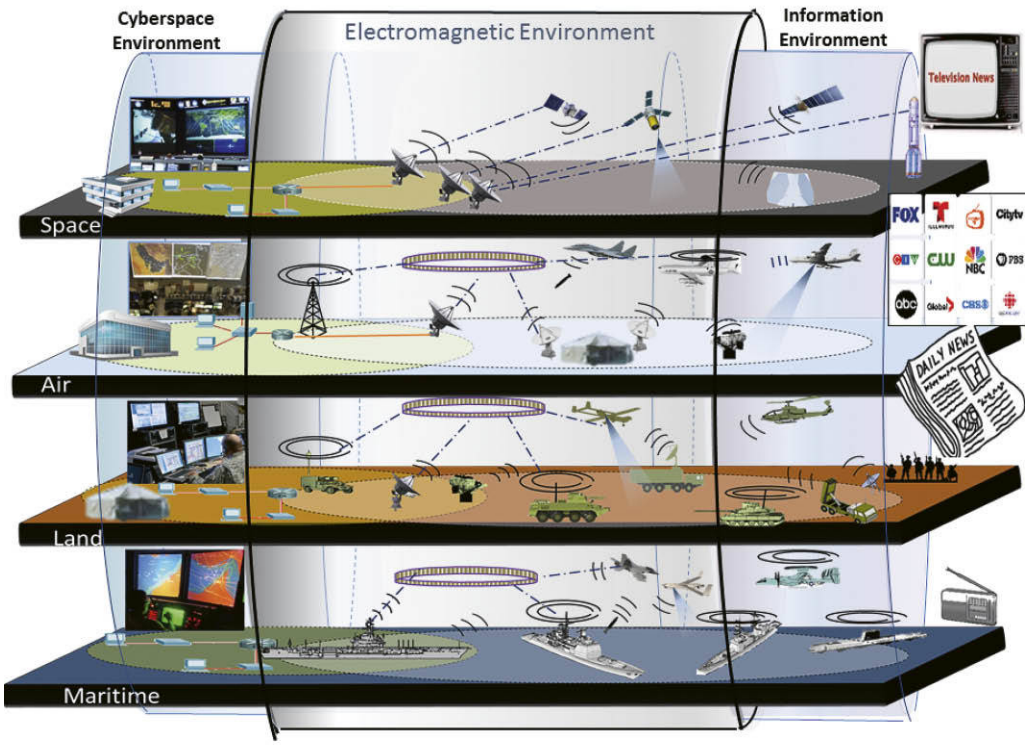


7. ábra: Az elektronikai hadviselés a mai katonai környezetben

Forrás: Malte von Spreckelsen: Electronic Warfare – The Forgotten Discipline. Why is the Refocus on this Traditional Warfare Area Key for Modern Conflict? *Joint Air Power Competence Centre,* 2018. december 13.

[21] Haig et al. (2014): i. m.

„A NATO-n belül az EMO magában foglalja az EM energia célzatos kisugárzását és vételét az EME-ben olyan katonai műveletekhez, mint a kommunikáció, navigáció, támadás, harctéri helyzetfelismerés és célmeghatározás. Az EMO nemcsak az egyes területeken teszi lehetővé a műveleteket, hanem biztosítja azt az összekötő szálat is, amely összekapcsolja és integrálja a katonai erőket az egyes területek között, valamint a kibertérben és az információs környezetben."[22]



8. ábra: Az EMO az EME-ben
Forrás: Spreckelsen (2018): i. m.

A megfelelő hírszerzés és felderítés – és különösen a technikai eszközökkel történő felderítés – felismeri az ellenség elektronikai harcrendjét (EOB), amely elengedhetetlen az elektronikai hadviselésben. A megszerzett és értelmezett adatok tájékoztatást adnak a kommunikációs és nem kommunikációs eszközök paramétereiről, az adók típusáról és céljáról, azok modulációjáról, a csatornák alkalmazási lehetőségeiről, az impulzus időtartamáról, az impulzus ismétlődéséről, a frekvenciáról, a sávszélességről, a kapcsolódó fegyverrendszerekről és egyéb sugárzási adatokról. Ezek az adatok segítenek az ellenség EOB-jének modellezésében.[23]

[22] Haig et al. (2014): i. m.
[23] Haig et al. (2014): i. m. 42.

A mesterséges intelligencia alkalmazása az elektronikai hadviselésben

Az MI-alapú EW-rendszerek alkalmazásának elsődleges okai a hatékony döntéstámogatási képesség elérése, a nagy mennyiségű adat kezelése, a helyzetfelismerés javítása, a változó forgatókönyv vizualizálása és megfelelő válaszok generálása.[24]

Az EW MI-alkalmazások két kategóriába sorolhatók: hadműveleti/harcászati MI-alapú EW-rendszerek és stratégiai szintűek. Stratégiai szinten az MI alkalmazása befolyásolhatja, hogy a katonai vezetés hogyan szervezi meg a hadrendjét, haderőcsoportosítását, háborús stratégiáit, a konfliktusok mértékére és fokozódására vonatkozó döntéseket, a hírszerzési adatok megosztását és értelmezését, a háború kiterjesztését és jellegét, a különleges eszközök bevetésének következményeit stb.

Az MI stratégiai szintű alkalmazása a hírszerzésben, a megfigyelésben és a felderítésben (ISR) nagyon fontos szerepet játszik, mindenekelőtt a katonai jelentőségű információk feldolgozásában. A megbízható és pontos ISR döntő fontosságú a több területet érintő helyzetfelismerés szempontjából.

Az MI komoly szerepet játszhat a modern hadviselésben alkalmazott nagy mennyiségű EW érzékelő adatainak kezelésében, a dinamikusan változó harctéri körülmények valós idejű elemzésében. Az MI elősegítheti a gyors és optimális támadást is, minimálisra csökkentve a saját erők kockázatát. Az MI által támogatott fejlett célzó és navigációs technikák javíthatják a hatékonyságot a taktikai és stratégiai védelmi rendszerek széles skáláján azáltal, hogy lehetővé teszik a jobb célzást, nyomon követést és célkiválasztást.

Az MI jelentős szerepet játszhat a számítógépes hálózatok feltérképezésében és feltörésében, amelyeken keresztül támadó és védekező célú információkhoz juthat.

Az MI taktikai szintű alkalmazásával nagyon jelentős javulást érhetünk el a tervezésben, a bizonytalanságok megszüntetésében és a harckészségben, ami a harcászati célok elérésében jelentős sikert hozhat. Az EW-technikák részeként használható különféle MI-algoritmusok közé tartoznak a neuro-számítástechnika és a mélytanulási technikák, amelyek információt szereznek a környezetből, tárolják és később felhasználják azokat.

Az MI szerepe az információgyűjtésben, -értelmezésben és -elemzésben is kiemelkedő. A katonai környezetben az információt főként a SIGINT, a HUMINT, valamint a MASINT eszközeivel gyűjtik be. Ezek az információk megfelelő értelmezést és elemzést igényelnek, hogy hasznosíthatók legyenek a döntéshozatalban. A hírszerzési közösség által tapasztalt információtúlterhelés kérdését a gépi tanulás segítségével lehet hatékonyan kezelni, ami minden forráselemzőnek segítséget nyújthat a változó biztonsági környezet megértésében.

Az MI-technikák a SIGINT-rendszerekben is használhatók az ellenségtől elfogott RF-jelek észlelésére és a fenyegetések előrejelzésére. Segíthet a kommunikációs vagy radarrendszerek által küldött RF-jelek dekódolásában. A konvolúciós neuronhálózat (CNN) felhasználható az EW-rendszerek DOA *(direction of arrival),* azaz a sugárzási

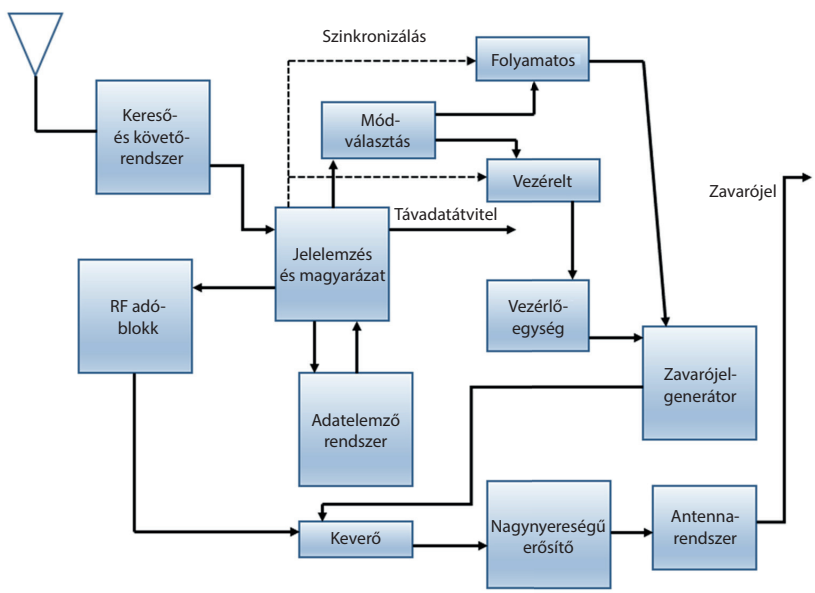
[24] Purabi Sharma – Kandarpa Kumar Sarma – Nikos E. Mastorakis: Artificial Intelligence Aided Electronic Warfare Systems. Recent Trends and Evolving Applications. *IEEE Access,* 8. (2020). 224761–224780.

irány becslésének javítására. Mély megerősített tanuláson (DRL) alapuló módszerek alkalmazhatók az ECCM- *(electronic counter-counter measures)* rendszerben a saját kommunikációnak az EW-környezethez hozzáigazításához, ahol az ellenfél adaptív zavarást alkalmaz.[25]

A mélytanuláson alapuló módszer alkalmas arra, hogy kiválassza az antennákat egy adott kognitív radar megoldásban. A DNN (*deep neural network*) konvolúciós rétegekből épül fel többszintű osztályozó keretrendszerként. A tanító adatokat úgy generálják, hogy minden osztály jelezzen egy antennaalrendszert. Ezek eredményeként a cél DOA-becslése a legkisebb hibával határozható meg.

MI-alapú módszerrel képes együttesen meghatározni a zavaró jelenlétét annak támadási jellemzőivel együtt. A zavaró jelenlétét két különböző neuronhálózat, a DCNN és a mély RNN segítségével határozhatjuk meg. A zavaró jelenlétét és típusát a forgatókönyvek sokfélesége határozza meg, amelyeket szoftver definiált rádiókkal (SDR) állítanak elő.

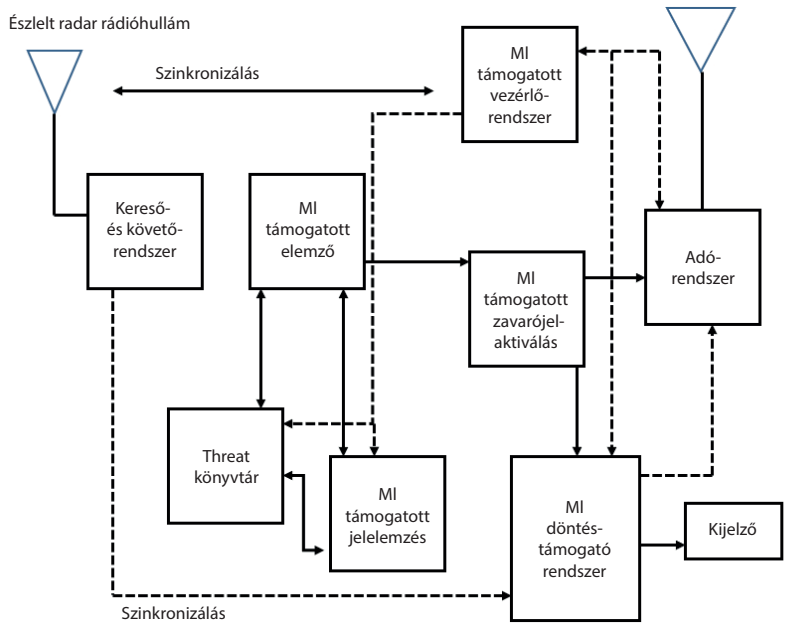
Az alábbi ábrán egy MI-támogatás nélküli „klasszikus" EW-rendszer logikai blokkdiagramja látható. A továbbiakban az MI alkalmazásának további lehetőségeit vizsgálva egy MI-támogatott EW-rendszer blokkdiagramján szemléltetem az MI-támogatott EW-rendszer logikai működését.



9. ábra: Egy tipikus EW-rendszer blokkdiagramja
Forrás: Sharma–Sarma–Mastorakis (2020): i. m.

[25] Sharma–Sarma–Mastorakis (2020): i. m.

Az MI alkalmazása az EW-ben csökkentheti a kognitív terhelést, és javíthatja az EW hatékonyságát a több doménben végzett műveleteknél, a bejövő adatok gyors és pontos, a prioritásnak megfelelő rendezésével, így a kevésbé fontos jelek eltávolíthatók. Az MI által támogatott EW-rendszer logikai blokkdiagramja látható a 10. ábrán.



10. ábra: MI-alapú EW-rendszer blokkdiagramja
Forrás: Sharma–Sarma–Mastorakis (2020): i. m.

Gépi tanuláson alapuló zajszerű jeladás (featureless signalling)

A direktszekvenciás szórt spektrumot (DSSS) a zavarás hatásának csökkentésére az ellenséges vevő termikus zajszintje alatt használják a jel észlelésének elkerülése érdekében. A DSSS elosztási szekvenciák diszkrét jellege és egyedi eloszlása viszonylag megkönnyíti a kapott átvitt jelek detektálását. Ennek a problémának a kiküszöbölése érdekében egy gépi tanuláson alapuló rendszer lehet alkalmas, amely jellegtelen, nem ismétlődő zajszerű jeleket generál. A séma számos előnnyel jár a szokásos DSSS-rendszerrel szemben, beleértve a jelek alacsony észlelési/lehallgatási valószínűségét és további feldolgozási lehetőségét is.

Egy Ismail Shakeel által jegyzett – *Machine Learning Based Featureless Signalling* című – tanulmányban az ML-alapú szórt spektrum (MLSS) technika a standard DSSS-PN- (pszeudozaj) rendszerek gyenge, kis valószínűségű észlelési és lehallgatási (LPD/LPI – *low probabilities of detection and interception*) képessége miatt szinkronizálható,

jellegtelen jeleket állít elő az erre szolgáló gépi tanulási (ML) módszer segítségével. Ennek a módszernek a hibateljesítményét és a generált jelek jellemzőit megvizsgálták és összehasonlították a szokásos DSSS-jelekkel.

A kapott eredmények azt mutatták, hogy a javasolt séma nem korrelált szórt jeleket generál, jó JR- *(jamming-resilient)*/LPD/LPI-tulajdonságokkal. A jelek Gauss-jellegét elemzik, autokorrelációs függvényeket alkalmaznak a jelben esetleg előforduló ismétlődő minták azonosítására. Ezek a tesztek nem mutattak azonosítható tulajdonságokat. A szerző megjegyzi, hogy az adószűrő, a HPA- és az RF-moduláció néhány észlelhető tulajdonságot adhat a jelhez, azonban fejlettebb módszerekre, például ciklostacionárius-alapú technikákra lenne szükség az ilyen jellemzők esetleges létezésének azonosításához a jelben.[26]

Az *autoencoder* technika a teljes kommunikációs rendszert végpontok közötti optimalizálási problémának tekinti, és megpróbálja rekonstruálni a továbbított üzenetet a vevő kimenetén, míg a hagyományos megközelítés egyedileg optimalizálja a jelfeldolgozó modulokat (kódoló, modulátor, csatornaazonosító, demodulátor stb.) egy ismert csatornamodellhez illeszkedő kommunikációs elmélet használatával. Az autoencoder olyan módszert kínál, amely felhasználható hullámformák kifejlesztésére az ismeretlen csatornamodellekkel rendelkező komplex környezetekben, valamint amellyel fejlett kommunikációs rendszereket lehet kifejleszteni a dinamikusan változó környezethez való alkalmazkodáshoz és optimalizáláshoz valós idejű tanulás segítségével. Az autoencoder architektúra egy teljesen összekapcsolt, *feed-forward* neurális hálózat, amely több rejtett réteget használ a mélytanuláshoz.

Az MLSS-jel generálását egy *software-defined radio* (SDR) adó végzi. Az LDPC-kódolt MLSS-jelet a betanított hálózat állítja elő. A DSSS-alapú rendszerekben a szórási szekvenciákat mind az adó, mind a vevő ismeri, és a kulcs a szinkronizálás, amely az adó szórási szekvenciáit igazítja a vevőhöz használt szekvenciákhoz, mindkettő által ismert titkos kulcs használatával.[27]

Következtetések

Az MI határozottan új perspektívákat nyit meg a védelmi technológiák terén. Nagy elvárások vannak az MI-technikák alkalmazásával kapcsolatban számos katonai területen, azonban továbbra is vannak megoldatlan kérdések, és további kutatások szükségesek annak érdekében, hogy megfeleljenek ezeknek az elvárásoknak.

Ez azonban nem azt jelenti, hogy szkeptikusnak kell lennünk az MI széles körű alkalmazhatóságát illetően, sokkal inkább meg kell értenünk, hogy több intellektuális erőfeszítést és pénzt kell fordítani a K+F-re.

[26] Ismail Shakeel: *Machine Learning Based Featureless Signalling.* arXiv:1807.07260 [eess]. 2018. július 19. 7.
[27] Shakeel (2018): i. m. 7.

Az MI elért ahhoz a ponthoz, ahol több katonai területen is alkalmazhatóvá vált. Az MI katonai alkalmazásainak meg kell felelni az átláthatósági követelményeknek, biztosítani kell a modell stabil teljesítményét, összhangban a katonai követelményekkel, minimalizálni kell a sebezhetőségeket, amelyek drasztikusan csökkenthetik a rendszer teljesítményét, és az ML számára elegendő tanulási adatot kell rendelkezésre bocsátani.

Az elektronikai hadviselés kritikus a katonai műveletek számára mind békében, mind háborúban. A digitális technika fejlődése és az MI-alapú EW-rendszerek lehetővé teszik a modern katonai erők számára, hogy rendkívül rugalmas és adaptív elektronikai harcrendet fejlesszenek ki, amely elősegíti az elektromágneses környezethez való gyors alkalmazkodást.

Mivel az MI-vel autonóm műveletek indíthatók, a helyzetfelismerés hatékonysága nő, a döntéshozatal megbízhatóbbá válik. Az MI által támogatott EW-rendszer hatékonyan azonosíthatja az ellenséges radarokat, csökkentve a fenyegetés súlyosságát, majd ettől függően megfelelő MI-alapú ellenstratégia alakítható ki az ellenséges EW-fenyegetés kiküszöbölésére. A radarjel elemzése során összegyűjtött információk felhasználhatók egy fenyegetési könyvtár elkészítésére az elektronikai harcrend (EOB) kialakítása érdekében, a jobb helyzetfelismerés és rugalmas ellenintézkedések érdekében a folyamatosan fejlődő EW-forgatókönyv szerint. Az MI-alapú technológiák alkalmazása megbízható eszközöket nyújthat a harcászati és stratégiai tervezőknek a hadviselési erőfeszítések végrehajtásához.

Felhasznált irodalom

Artificial Intelligence. The Frontline of a New Age in Defense. (É. n.) Online: https://cdn2.hubspot.net/hubfs/2097098/MCM120_BreakingDefense_AI_ebookR1%20(1).pdf

DoD Growth in Artificial Intelligence: The Frontline of a New Age in Defense. *Breaking Defense,* 2019. szeptember 18. Online: https://breakingdefense.com/2019/09/dod-growth-in-artificial-intelligence-the-frontline-of-a-new-age-in-defense/

Electronic Warfare. Joint Publication 3-13.1. 2012. február 8. Online: https://fas.org/irp/doddir/dod/jp3-13-1.pdf

European Commission: *European Defence Industrial Development Programme (EDIDP).* 2020. Online: https://ec.europa.eu/research/participants/data/ref/other_eu_prog/edidp/wp-call/edidp_call-texts-2020_en.pdf

GAO: *Artificial Intelligence. Emerging Opportunities, Challenges, and Implications.* 2018. március. Online: www.gao.gov/assets/gao-18-142sp.pdf

GAO: *Electromagnetic Spectrum Operations. DOD Needs to Address Governance and Oversight Issues to Help Ensure Superiority.* 2020. december. Online: www.gao.gov/assets/gao-21-64.pdf

Haig Zsolt – Kovács László – Ványa László – Vass Sándor: *Elektronikai hadviselés.* Budapest, NKE, 2014.

Joint Electromagnetic Spectrum Operations. Joint Publication 3-85. 2020. május 22. Online: www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_85.pdf

NATO: *Military Uses of Artificial Intelligence, Automation, and Robotics (MUAAR).* 2020. Online: www.act.nato.int/application/files/5515/8257/4725/2020_mcdc-muaar.pdf

NATO: *Military Uses of Artificial Intelligence, Automation, and Robotics (MUAAR).* 2020. Online: www.act.nato.int/application/files/5515/8257/4725/2020_mcdc-muaar.pdf

NATO Science & Technology Organization: *Science & Technology Trends 2020–2040. Exploring the S&T Edge.* 2020. Online: www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf

Saalman, Lora (szerk.): *The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk.* Stockholm, Sipri, 2019. Online: www.sipri.org/sites/default/files/2019-10/the_impact_of_artificial_intelligence_on_strategic_stability_and_nuclear_risk_volume_ii.pdf

Shakeel, Ismail: *Machine Learning Based Featureless Signalling.* arXiv:1807.07260 [eess]. 2018. július 19. Online: http://arxiv.org/abs/1807.07260

Sharma, Purabi – Kandarpa Kumar Sarma – Nikos E. Mastorakis: Artificial Intelligence Aided Electronic Warfare Systems. Recent Trends and Evolving Applications. *IEEE Access,* 8. (2020). 224761–224780. Online: https://doi.org/10.1109/ACCESS.2020.3044453

Spreckelsen, Malte von: Electronic Warfare – The Forgotten Discipline. Why is the Refocus on this Traditional Warfare Area Key for Modern Conflict? *Joint Air Power Competence Centre,* 2018. december 13. Online: www.japcc.org/electronic-warfare-the-forgotten-discipline/

Svenmarck, Peter – Linus Luotsinen – Mattias Nilsson – Johan Schubert: *Possibilities and Challenges for Artificial Intelligence in Military Applications.* 2018.

Tonin, Matej: *Artificial Intelligence: Implications for NATO's Armed Forces.* 2019. október 13. Online: www.nato-pa.int/download-file?filename=/sites/default/files/2019-10/REPORT%20149%20STCTTS%2019%20E%20rev.%201%20fin-%20ARTIFICIAL%20INTELLIGENCE.pdf

Top Trends on the Gartner Hype Cycle for Artificial Intelligence, 2019. *Gartner,* 2019. szeptember 12. Online: www.gartner.com/smarterwithgartner/top-trends-on-the-gartner-hype-cycle-for-artificial-intelligence-2019/

Unmanned Systems Roadmap 2007–2032. 2007. Online: www.globalsecurity.org/intell/library/reports/2007/dod-unmanned-systems-roadmap_2007-2032.pdf

Wang, Wei – Hui Liu – Wangqun Lin – Ying Chen – Jun-An Yang: Investigation on Works and Military Applications of Artificial Intelligence. *IEEE Access.* 8. (2020). 131614–131625. Online: https://doi.org/10.1109/ACCESS.2020.3009840

Zednik, Carlos: Solving the Black Box Problem: A Normative Framework for Explainable Artificial Intelligence. *Philosophy & Technology,* 34. (2021). 265–288. Online: https://doi.org/10.1007/s13347-019-00382-7

A Katonai Műszaki Doktori Iskolában folyó képzés és fokozatszerzés igen széles kutatási palettát jelent. A haditechnikai fejlesztések mellett – azokkal párhuzamosan – kiterjedt kutatások folynak a katasztrófavédelem és a vízügyi kérdések területén is. Úgy is mondhatjuk, hogy a doktori iskola három lábon áll.

Ez a sokszínűség nagy lehetőségeket rejt. Az eltérő tudományágakban kutató doktoranduszok közvetlenül látnak rá más tudományterületek módszereire, eszközeire, kutatási témáira, amelyekből új inspirációkat nyerhetnek. Általános jelenség ez a tudományos kutatásban, így ezeket a lehetőségeket mi sem hagyhatjuk ki.

A doktori iskolában folyó kutatásokkal szemben elvárás, hogy az új tudományos eredmények hasznot hozzanak. Ez a követelmény a doktori iskola mindhárom területére vonatkozik. Ez a kötet egyik eleme ennek a felelősségteljes munkának.