NEMZETBIZTONSÁGI SZEMLE
10. évfolyam (2022) 1. szám 30–51. • DOI: 10.32561/nsz.2022.1.3.

Szabadföldi István[1]

A mesterséges intelligenciával támogatott nyílt információszerzés (OSINT) – evolúció és kihívások

The Artificial Intelligence supported OSINT – Evolution and Challenges

A mesterséges intelligencia (MI) egyre nagyobb szerepet játszik az adatfeldolgozásban, mind a polgári mind a katonai műveletek tervezésében és támogatásában, a hírszerzésben és elhárításban, elemzésben. Az MI egyik legfontosabb szerepe a big data „5V-s kihívása" által jelentette kockázat csökkentése (volume – mennyiség, variety – változatosság, velocity – sebesség, veracity – valódiság, value – érték). Az összadatforrású felderítés (all-source intelligence, ASI) kiterjedt, közvetlen emberi cselekménnyel folytatott, képi, rádióelektronikai, műszeres, radar-, nyílt adatforrású felderítés összessége, átfogó hírszerzési műveletekkel szerzi be és dolgozza fel a sikeres műveletek végrehajtásához szükséges információkat. Ezen eszközök, műveletek vonatkozásában mindig is kiemelkedő szerepet játszott a nyílt forrású információszerzés (open source intelligence, OSINT), amely mára az internet elterjedésével és a világhálón tárolt adattömeg feldolgozásával és elemzésével lényegében a klasszikus emberi erőforrású hírszerzési tevékenység (human intelligence, HUMINT) egy jelentős részét kiváltotta. Az MI alkalmazása az OSINT-ben az infomációszerzésnek mind a sebességét mind a hatékonyságát növeli úgy a szövegbányászat, mint a képfelismerés vagy az összefüggések keresésének és elemzésének vonatkozásában.

Kulcsszavak: *mesterséges intelligencia, összadatforrású felderítés, big data, nyílt adatforrású információszerzés*

Artificial Intelligence (AI) is playing an increasing role in data processing, both in civil and military operations planning and support, intelligence and counter-intelligence, and in analysis. One of the key roles of AI is to reduce risks posed by Big Data's "5V

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola, e-mail: istvan.szabadfoldi@hotmail.com

Challenge" (Volume, Variety, Veracity, Velocity, Value). All-source Intelligence (ASI) is a comprehensive system that acquires and processes the information necessary to conduct successful operations through intelligence operations encompassing man-made, visual, radio-electronic, measuring, radar, open source intelligence. All-source Intelligence obtains and processes the information needed to perform a successful operation through extensive and comprehensive intelligence operations. Open-Source Intelligence (OSINT) always played a prominent role in these tools and operations, and as of today it has essentially replaced big part of the classical human intelligence activity (HUMINT) by acquiring, processing and analysing data stored on the World Wide Web. The use of AI in OSINT increases both the speed and efficiency of obtaining information from text mining to image recognition or the search and analysis of correlations.

Keywords: *Artificial Intelligence, All-source Intelligence, Big Data, Open Source Intelligence*

1. Bevezető

A politikában és a nemzetek közötti kapcsolatok történetében kezdetektől döntő szerepet játszott az információszerzés és annak megfelelő feldolgozása. A digitalizáció, az úgynevezett *emerging and disruptive technologies* (EDT) – feltörekvő és felforgató technológiák – megjelenése az elmúlt egy évtizedben alapvető változásokat hozott az információszerzés és -feldolgozás vonatkozásában. A szenzorok elterjedése, az IoT/IoMT/IoBT *(Internet of Things/Internet of Military Things/Internet of Battlefield Things)* – dolgok internete/katonai eszközök internete/harctéri eszközök internete –, a big data, a mesterséges intelligencia (MI), a virtuális/kiterjesztett valóság (*virtual reality/augmented reality,* VR/AR) eszközei a tervezés, helyzetfelismerés és döntéstámogatás adatforrásainak exponenciális bővülését hozta el.

Az MI növekvő szerepet játszik a katonai műveletek tervezéséhez elengedhetetlen magas szintű hírszerzés támogatásában, ezzel együtt az ellenség hírszerző tevékenységének elemzésében. Az összadatforrású felderítés kiterjedt adatszerző műveletekkel gyűjti be és dolgozza fel a sikeres művelet-végrehajtáshoz szükséges adatokat és alakítja értelmezhető információvá. A nyílt forrású adatszerzés a hírszerzés elfogadottan egyenrangú eszköze a többi hírszerzési ággal együtt, a hírszerzés teljes eszközrendszerét tekintve. Minthogy a publikus információk növekvő mennyiségben hozzáférhetők, az OSINT szerepe is ezzel együtt nő mint információszerzési eszköz. Már a 20. század közepén is az Amerikai Egyesült Államokban a hírszerzési információk 40%-a származott nyílt forrásokból, mára viszont ez az arány elérte a 80–90%-ot.[2]

Mivel a növekvő információs igény és az azt kielégítő intézmények egyre kevésbé igénylik – és valójában sok esetben értelmetlen is – az információ minősítését, és az avulás miatt a korábban minősített információk is viszonylag hamar nyíltan hozzáférhetővé válnak, ez felértékeli az OSINT szerepét. Emellett fontos tényező még

[2] Resperger István (szerk.): *A nemzetbiztonság elmélete a közszolgálatban.* Budapest, Dialóg Campus, 2018.

a költség és a biztonsági kockázat minimalizálása. Az OSINT a többi hírszerzési ág (HUMINT, SIGINT, *signal intelligence,* rádió-elektronikai felderítés, IMINT, *imagery intelligence,* képalkotó felderítés, MASINT, *measurement and signature intelligence,* technikai jelfelderítés) viszonylatában kényelmes és költséghatékony eszköze tud lenni a politikai döntéshozók által a nemzetbiztonsági szolgálatokra rótt információszerzési igénynek. A szakirodalom szerint a titkosszolgálatok a szakmai munkára fordított költségvetésük 95%-át a HUMINT-, a SIGINT-, az IMINT- és a MASINT-tevékenység végzésére fordítják, amelyekkel az összes információ 20%-át szerzik meg, míg az OSINT a költségvetés 5%-át fogyasztva a megszerzett információk 80%-át képes produkálni.[3]

A fentiek okán az OSINT-tevékenységet szinte minden nemzetbiztonsági vagy rendvédelmi szervezet struktúrájában önálló szervezeti egység végzi erre kiképzett munkatársakkal.

A nagy mennyiségű és különböző forrású és típusú (szöveg, kép, hang, videó) adatok rendelkezésre állásával azonban új kihívással néznek szembe a szolgálatok. Adott témára, specifikus területre vonatkozó információt ezekből OSINT-eszközzel, de humán elemző-értékelő erőforrással kiszűrni, rendszerezni munkaigényes és ezzel együtt költséges is, mégpedig növekvő mértékben. Ebben tud a mesterséges intelligencia hatékony támogatást nyújtani.

2. Mi a mesterséges intelligencia (MI) – áttekintés és demisztifikáció

Mielőtt az MI tárgyalásába belemennénk, érdemes néhány szót fordítani az *emerging and disruptive technologies* (EDT) társadalmi és biztonsági vonatkozásaira.

A 2019. decemberi londoni találkozójukon a NATO-vezetők megállapodtak egy EDT megvalósítási ütemtervről, azzal a céllal, hogy segítse a NATO munkáját a legfontosabb technológiai területeken, és lehetővé tegye a Szövetség számára e technológiáknak az elrettentés, védelem, valamint a képességfejlesztés területeire gyakorolt hatásaik értékelését. 2021 februárjában a NATO védelmi miniszterei jóváhagyták a *Foster and Protect: NATO's Coherent Implementation Strategy on Emerging and Disruptive Technologies* című dokumentumot,[4] amely iránymutatást ad a NATO-nak az EDT-k elfogadásában és az azokhoz való alkalmazkodásban. Két fő területre fókuszál: egyfelől a kettős felhasználású technológiák (azaz polgári és katonai kontextusban egyaránt hasznosítható technológiák) fejlesztésének elősegítésére, amelyek erősítik a szövetség pozícióját, másfelől létrehozza a szövetségesek fórumát a fenyegetésekkel szembeni védekezést segítő bevált gyakorlatok cseréjére.

[3] Izsa Jenő: *Nemzetbiztonsági alapismeretek*. Jegyzet. Budapest, ZMNE, 2009.
[4] NATO: *Emerging and Disruptive Technologies* (é. n.).

A NATO innovációs tevékenységei jelenleg hét kulcsfontosságú területre összpontosítanak, amelyeket a Koherens Végrehajtási Stratégia (Coherent Implementation Strategy) prioritásként jelölt meg:

- mesterséges intelligencia (MI);
- adatok és számítástechnika;
- autonómia;
- kvantumalapú technológiák;
- biotechnológia és humán fejlesztések;
- hiperszonikus technológiák;
- űrtevékenység.

Az MI kiemelt szerepet kapott az USA és a szövetség részéről a jövőre nézve mint olyan technológia, amelyben a fölény megszerzése/megtartása kulcsfontosságú a demokratikus világ biztonsága és védelmi pozícióinak megőrzése szempontjából. Ennek külön hangsúlyt ad az USA Kongresszusa által felállított kétpárti szakértői bizottság jelentése, amely közel 750 oldalban foglalta össze a jelenlegi helyzetet és a tennivalókat.[5]

Az MI-nek annak ellenére, hogy már az ötvenes évek óta használt fogalom, ma sincs általánosan elfogadott tudományos definíciója. Megállapításom az, hogy az MI nem értelmezhető önálló alkalmazásként, hanem technológia, amely meglévő funkcionális megoldásokat támogat meghatározott problémák megoldására kifejlesztett algoritmusokon alapuló eljárásokkal. Ezen algoritmusok nagy adatkészletek összegyűjtésére, rendszerezésére, feldolgozására, elemzésére, továbbítására és az ezekre való reagálásra alkalmasak, azaz képesek az emberi értelem kognitív képességének megfelelő, illetve azt közelítő műveletekre, mégpedig nagyobb sebességgel.

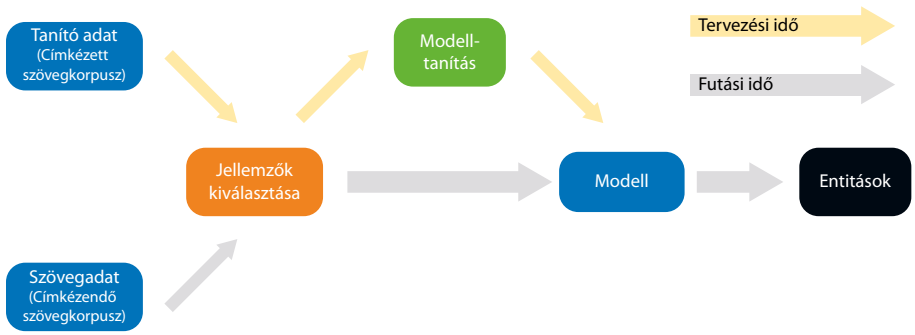
Az MI-nek alapvetően három típusát különböztetjük meg:[6]

- Narrow (AI) MI, azaz szűk vagy gyenge mesterséges intelligencia: olyan számítógépes rendszer, amely az embernél hatékonyabban tud elvégezni pontosan meghatározott feladatot. Itt tartunk ma.
- General (AI) MI, általános mesterséges intelligencia, amelyet olykor „erős MI-nek" is neveznek: az ember kognitív képességeit meghaladva képes bármilyen intellektuális feladatot elvégezni. Az ilyen típusú MI-vel működő robotokat láthatunk filmekben, ahol tudatos gondolkodással saját céljaiknak megfelelően működnek. Ez ma még nagyrészt a fantázia világa.
- Artificial Super Intelligence – ASI, a mesterséges szuperintelligenciával rendelkező számítógép képes az embert minden területen felülmúlni, például akár a tudományos kutatásban, általános bölcsességben és a társadalmi képességekben is. A tudósok jó része meg van győződve, hogy ez elérhetetlen.

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, amelyekből adatmodellt készít, majd előrejelzéseket és válaszokat ad.

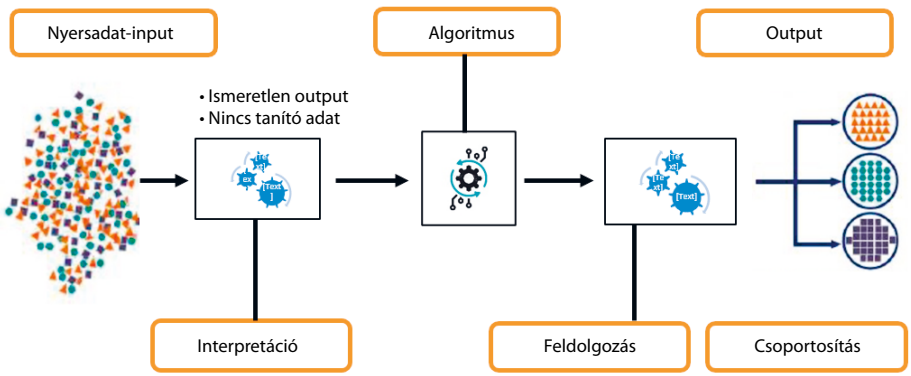
[5] National Security Commission on Artificial Intelligence: *Final Report* (2021).
[6] Lásd: https://azure.microsoft.com/en-us/overview/what-is-artificial-intelligence

A felügyelt tanulás (*supervised learning,* SL) során az osztályozó paramétereket az ismert kategóriákból álló minták felhasználásával a kívánt teljesítmény eléréséhez igazítják. Az SL funkcionális gépi tanulási feladatot képez a címkézett tanító adatokból, amelyek tanító példákat tartalmaznak. Az SL-ben minden példa egy bemeneti objektumból (általában egy vektorból) és egy várható kimeneti értékből (felügyelt jelből) áll. Ezt mutatja be az alábbi, 1. ábra.



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. alapján a szerző szerkesztése

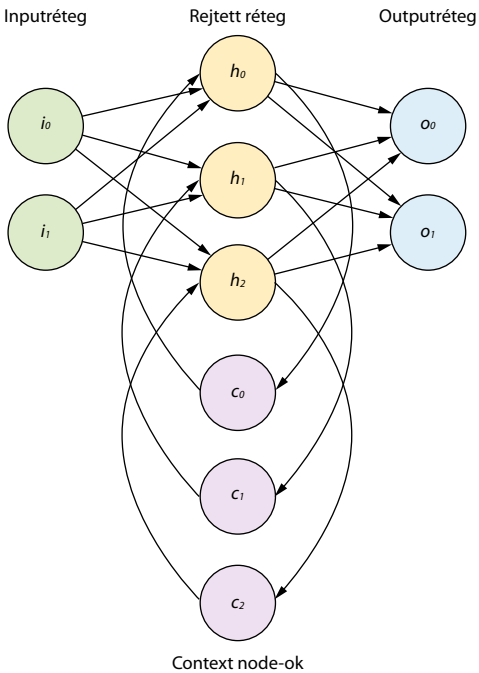
Felügyelet nélküli tanulás (*unsupervised learning,* UL) során a tanító adatok nincsenek címkézve, a tanulási cél a megfigyelt értékek osztályozása vagy megkülönböztetése. Lényegében statisztikai módszer, amely képes felismerni a jelöletlen adatok potenciális struktúráit. A felügyelet nélküli tanulás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



2. ábra: A felügyelet nélküli tanulás (UL) diagramja
Forrás: Wang et al. (2020): i. m. alapján a szerző szerkesztése

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 mély tanulás (*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.[7]



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

Az MI-technológia lehetőségeit és korlátait világosan meg kell érteni és figyelembe kell venni – különösen a döntéshozóknak –, hogy elkerüljék a nehezen vagy nem elérhető célokat kitűző projektek elindítását.[8]

[7] Wang et al. (2020): i. m.
[8] Lora Saalman (szerk.): *The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk,* Volume II, East Asian Perspectives. SIPRI, 2019.

3. A mesterséges intelligencia katonai alkalmazása

A mesterséges intelligencia (MI) fogalmának megjelenésével lényegében egy idős annak katonai célra való alkalmazása a katonai műveletek tervezésében, támogatásában, a hírszerzésben és az ellenség hírszerzésének elemzésében, valamint az autonóm fegyverrendszerek, járművek terén, az ember-gép interfészek *(machine-learning, man-machine teaming)* vonatkozásában elérhető nagyobb pontosság és hatékonyság érdekében.

Az MI egyik legfontosabb szerepe a big data alapvető „5V kihívásából" adódó kockázat csökkentése.

Az MI katonai alkalmazási területeit az alábbi felsorolásban foglalta össze a NATO Science and Technology Committee (STC) számára 2019-ben készített jelentés:[9]

- harctéri sebesültellátás;
- C4ISR, *command control communication computers intelligence surveillance reconnaissance* (parancs, vezérlés, kommunikáció, számítógép, hírszerzés, megfigyelés és felderítés);
- kiberbiztonság és -védelem;
- elektronikai hadviselés;
- emberierőforrás-menedzsment;
- információs és döntéstámogatás;
- hírszerzés;
- logisztika;
- békefenntartó műveletek;
- robot autonóm rendszerek;
- közösségi média;
- kiképzés.

Fenti területeken 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.[10]

4. A hírszerzés eszközrendszere

Röviden összefoglalva, a hírszerzési doktrínák alapvetően hat hírszerzési, információgyűjtési típust különböztetnek meg:[11]

- rádióelektronikai felderítés (*signal intelligence,* SIGINT);
- képalkotó felderítés (*imagery intelligence,* IMINT);

[9] Matej Tonin: *Artificial Intelligence: Implications for NATO Armed Forces.* Report. NATO Parliamentary Assembly, 2019. október 13. 5.

[10] European Commission: *European Defence Industrial Development Programme (EDIDP)* (2020. július 23.).

[11] Izsa (2009): i. m.

- technikaijel-felderítés (*measurement and signature intelligence,* MASINT);
- humán hírszerzés (*human-source intelligence,* HUMINT);
- nyílt adatforrású hírszerzés (*open-source intelligence,* OSINT);
- térinformatikai hírszerzés (*geospatial intelligence,* GEOINT).

A SIGINT-en belül további megkülönböztetés tehető aszerint, hogy milyen jelet fogunk el információszerzési célból. Ezek alapján a távközlési rendszereken sugárzott üzenetek lehallgatása és az elektronikai és egyéb eszközök által kibocsátott jelek elfogása révén megkülönböztethetjük még:

- a távközlési felderítést (*communication intelligence,* COMINT),
- az elektronikai felderítést (*electronic intelligence,* ELINT) és
- a gépi kibocsátású jelek felderítését (*foreign instrumentation signals intelligence,* FISINT).

Természetesen a taxonómia tovább folytatható a besorolások, elnevezések, az eszközök és a cél vonatkozásában. Az összadatforrású hírszerzésnek az OSINT csak az egyik és nem kizárólagos forrása. Mindenképpen szükséges az OSINT által produkált adatok más nyílt tevékenységből vagy minősített forrásokból származó adatokkal való összevetése.

Jelen cikknek nem tárgya a többi hírszerzési módozat tartalmi kifejtése, hanem a nyílt adatforrású hírszerzés (*open-source intelligence,* OSINT) tárgyalása.

5. Az OSINT és fejlődése[12]

A nyílt információszerzés nem új keletű jelenség, lényegében az emberiség történelmével egyidős. Az első OSINT-források között említhetők az utazói útleírások, a szóbeli úti és élménybeszámolók, a történelmi krónikák és a konkrét csatákról szóló háborús visszaemlékezések. A rendelkezésre álló nyílt forrásanyagok mennyisége a nyomtatás megjelenésével, majd a távközlés fejlődésével nagyságrendekkel megnőtt, az internet megjelenése ezt a növekedést tovább sokszorozta. A szolgálatok számára mára a legnagyobb kihívás az, hogy miként dolgozza fel, szűrje ki a lényeget a hatalmas mennyiségű nyílt információból.

Az OSINT fejlődése a 21. századra komoly evolúciós folyamaton ment át.[13] A kifejezés fogalmának és történetének megértéséhez a II. világháború idejére kell visszamennünk, amikor a BBC a külföldi rádióadások monitoringját végezte. Az OSINT jelentősége a hidegháború alatt tovább nőtt. Az 1989 utáni biztonság fogalmának kibővülése az OSINT számára új területeket nyitott, majd az internet eljövetele és a szeptember 11-i terrortámadások hatása az OSINT-et a terrorista tevékenységek elemzése/megelőzése fő eszközévé tette.

[12] Resperger (2018): i. m.

[13] Miron Lakomy: *Military Application of Open-Source Intelligence on the Internet. In 4th Annual International Research Conference GlobState 2021 Security Environment in the (Post) Pandemic World and Its Implications for the Conduct of Military Operations* (30 November – 02 December 2021), 85-915. Bydgoszcz, Polska, 2021.

Az OSINT fogalmi rendszerében megkülönböztetünk OSINT-tevékenységet, OSINT-adatot, OSINT-információt és hitelesített OSINT-információt.[14]

Az OSINT-tevékenység önálló, nyílt adatszerző tevékenység, amely során személyek vagy szervezetek által nyilvánosan vagy korlátozottan közzétett, legális eszközökkel megszerezhető nem minősített adatoknak a hírszerzési igények kielégítésére történő felkutatását, gyűjtését és feldolgozását (rendszerezés, értékelés) jelenti.

Az OSINT-adat az „elsődleges forrástól származó, más által még nem közölt, nem feldolgozott, nyomtatott, kisugárzott, szóban közölt vagy más formájú adat (pl. fotó, audio- vagy videófelvétel, műholdkép, személyes levél, nyilatkozat stb.”.[15]

Az OSINT-információ már adott szempontok alapján kiválogatott és jóváhagyott, nyílt forrásokból összeállított információ, mint például az újságok, a könyvek, a rádió- és a televízió-műsorok, napi jelentések stb.

A hitelesített OSINT-információt már elemzők más – akár minősített – forrásokból származó információkkal, tényekkel való összevetés alapján megbízhatónak nyilvánították, illetve adott esetben már korábban ellenőrzött, megbízható forrásból származik.

A nyílt forrású adatszerzés által szerzett információknak meg kell felelni a hírszerzési információkkal szemben támasztott követelményeknek, azaz „újszerűnek, időszerűnek, feldolgozottnak, hitelesnek, valamint rendelkezésre állónak” kell lennie.[16] Az internetről elérhető források esetében az OSINT-adatfeldolgozás eljárásrendjébe tartozik a forrás, valamint a közzétett információ ellenőrzése, amely során a fő szempontok a „pontosság, a megbízhatóság, a hitelesség/szakmai elismertség, az időszerűség, az objektivitás és a fontosság”.[17]

OSINT-források a NATO-kézikönyv[18] alapján:

- hagyományos médiaforrások (nyomtatott és elektronikus);
- kereskedelmi online prémiumforrások;
- a kereskedelmi online információ egyéb formái;
- „szürke” irodalom;
- nyílt humán szakértők és megfigyelők;
- kereskedelmi célú képanyagok;
- kereskedelmi kamarák;
- nem kormányzati szervezetek;
- vallási szervezetek.

A nyílt adatszerzés célja egyfelől az, hogy a hírszerzési tevékenység a felhasználók információigényeit minél nagyobb mértékben kielégítse, másfelől maguk a felhasználók határozhatják meg, hogy a hírszerzés nyílt információkból állítsa össze a tájékoztatót, mivel adott körülmények között csak az ilyen módon beszerzett információk használhatók fel.

Minthogy a nyílt adatforrású hírszerzés legális, nemcsak a hírszerző szolgálatok foglalkoznak vele, hanem az üzleti világban különböző szolgáltatók is. Lényegében

14 Resperger (2018): i. m.
15 Resperger (2018): i. m.
16 Resperger (2018): i. m.
17 Resperger (2018): i. m.
18 NATO: *NATO Open Source Intelligence Handbook* (2001).

OSINT-tevékenységet folytatnak például a vállalatvezetők felé sajtófigyelő szolgáltatást nyújtó médiacégek/személyek is. Bizonyos nagyvállalatok OSINT-képességei akár elérhetik a hírszerző szolgálatok által képviselt szintet is, ehhez a polgári használatú technológia rendelkezésre áll, így ez ma már szinte kizárólag megfelelő finanszírozási háttér kérdése.[19]

Az internet a nyílt forrású adatok legnagyobb és egyben legkönnyebben elérhető tárháza, azonban a feldolgozást egyfelől az adatredundancia, másfelől az információk hitelességének bizonytalansága nehezíti, mivel az interneten megtalálható információk jelentős része téves, hiányos vagy megtévesztő. A hiteles információk kinyerése alapos adatfeldolgozást igényel, amelyet külön hírszerzési csoport végez, amelynek tevékenysége az internetes közösségi hálózatokban a tagok által megosztott információk megszerzésére irányul. Ez a közösségi hálózatokból származó információszerzés.

Az OSINT forrásai az interneten jelentős fejlődésen mentek át az idők folyamán. A web 1.0 az önálló weboldalak, üzenőfalak világa, majd a web 2.0 a közösségi média (Twitter, Facebook, Instagram), a blogok, a fájlmegosztó és streamelési szolgáltatások (Youtube, SoundCloud, Spotify), webes térkép platformok (Google térkép), a felhő adattárolók sokaságát hozta el. A dark web világa a TOR, a ZERONET, a FREENET és az Invisible Internet Project (I2P) megjelenésével a cenzúra nélküli internetezést, a peer-to-peer kommunikációt teszi lehetővé. Az I2P szabad szoftver segítségével névtelen (anonim vagy pszeudonim) virtuális magánhálózat építhető ki. Ezek komoly OSINT-kihívások, és a hírszerzés legfőbb csataterei.

6. Az OSINT műveleti alkalmazásai

Az OSINT-rendszerek alkalmazása mind a bűnüldözésben, mind a hírszerzésben mára már igen elterjedtté vált.

A fejlett titkosszolgálati rendszereket szállító cégek OSINT-megoldásai jellemzően öt fő funkciót fednek le:

- célprofilozás;
- közvélemény befolyásolása, figyelése;
- fake news;
- dark web monitoring – terrorelhárítás, szervezett bűnözés és kiberbűnözés elleni fellépés;
- avatarképesség.

A célprofilozás speciális profilozást végez fejlett adatgyűjtési és elemzési képességek alapján. Feltárja és statisztikákat gyűjt a célszemély közösségimédia-kapcsolatairól, földrajzi helymeghatározással azonosítja és elemzi azon helyszíneket, ahonnan a célszemély közösségi médiumokat és/vagy a mobiltelefonját – feljogosítva a nyílt információközlést a GPS-koordinátákról – használta, adatgyűjtést végez a célszemély közösségi oldalának tartalmai, valamint a rendszer meglévő adatai alapján, feltárja a célszemély viselkedési mintáit.

[19] Effect Group: www.effectgroup.io

A közvélemény befolyásolásának figyelése és az úgynevezett *sentiment analysis* téma-, illetve hangulatalapú tömeges adatgyűjtést, -elemzést és szükség esetén riasztást végez, ha egy előre megadott téma jelenik meg a weben. A rendszer folyamatosan figyeli és gyűjti az információt a web minden rétegében, beleértve a weboldalakat, közösségi hálót, videómegosztó webhelyeket, blogokat, fórumokat, miközben az eredeti megosztóra és fórumra összpontosít. A felhasználó által létrehozott robotok kifinomult adatgyűjtési feladatokat futtatnak, és gyakorlatilag bármilyen típusú webforrást megcéloznak, bármely nyelven. A felhasználó által definiált változókból és műveletekből nyert adatszerzéssel együtt ad választ a „ki, mit, mikor, hol és hogyan" kérdéseket illetően bármely előre megadott témára vonatkozóan.

A Fakenews funkció automatizált megoldást kínál a közösségimédia-felhasználók hitelességének elemzésére, majd a hamis hírek és azokat posztoló felhasználók elkülönítésére. Miután a hamis kampány hatókörét és céljait elemezték és megértették, a kármentő stratégiát ki lehet dolgozni és elkezdeni.

A dark web kutatásának egyik legfontosabb része – amellett hogy a nem indexelt óriási adattartalomban célspecifikus kutatást végez – az illegális web „búvóhelyek" észlelésére és nyomon követésére kifejlesztett *„hidden service locator"*-ok használata. Ezek a funkciók valós idejű, prioritásalapú riasztásokat biztosítanak teljesen automatizált, intelligens felügyeleti algoritmusok használatával. Figyelemmel kísérik az ellenséges/bűnözői tevékenységet a célkiválasztástól a tervezésen át a tényleges cselekményig. Új kommunikációs csomópontokat tárnak fel a változó dark weben a rosszindulatú tevékenységek nyomon követése érdekében.

Aktív OSINT-tevékenység az avatarok használata, amelyek lényegében virtuális HUMINT-ügynököknek tekinthetők. Az avatar lehet például egy hamis személyazonossággal létrehozott profil, amely a célszemély valamely érdeklődési területét (politka, szex, gasztronómia stb.) kihasználva lép kapcsolatba vele, kerül az ismeretségi körébe, férkőzik a bizalmába. Az avatarok lehetővé teszik az elemzők számára, hogy biztonságosan kommunikáljanak, figyeljék és manipulálják a célpontokat. Az avatarok a rendszerben gyorsan definiálhatók, módosíthatók, vagy új attribútumok adhatók meg az egyes avatarokhoz.

Fentieken túl fontos tisztázni a deep web – dark web környezetet. A deep web minden olyan internetes tartalomra vonatkozik, amelyet különböző okok miatt nem indexelnek olyan keresőmotorok, mint a Google. Ez a definíció tehát magában foglalja a dinamikus weboldalakat, a blokkolt webhelyeket (például azokat, amelyek a hozzáféréshez CAPTCHA-válaszadást kérnek), a privát webhelyeket (például azokat, amelyekhez bejelentkezési hitelesítés szükséges), a nem HTML/kontextuális/szkriptes tartalmakat és korlátozott hozzáférésű hálózatokat. A teljes deep web becslések szerint az internetes tartalmak mintegy 80%-át jelenti.

A korlátozott hozzáférésű hálózatok lefedik mindazokat az erőforrásokat és szolgáltatásokat, amelyek normál esetben nem elérhetők a szabványos hálózati konfigurációval, így lehetőséget kínálnak a rosszindulatú szereplők fellépésére. Idetartoznak azok a webhelyek, amelyek domainnevei olyan domain name system (DNS) rootokon vannak regisztrálva, amelyeket nem az Internet Corporation for Assigned Names and Numbers (ICANN) kezel, és ezért olyan nem szabványos felső szintű domainekkel

(*top-level domains,* TLD) rendelkező URL-eket tartalmaznak, amelyekhez egy adott DNS-kiszolgálóra van szükség.

További példa a domainnevüket a szabványos DNS-től teljesen eltérő rendszeren regisztráló webhelyek, mint például a .BIT tartományon regisztrált „Bitcoin Domain". Ezek a rendszerek az ICANN által előírt domainnév-szabályozást kikerülik, az alternatív DNS-ek decentralizált jellege szintén nagyon megnehezíti ezeknek a tartományoknak a beazonosítását.

4. ábra: Az internet felosztása: surface web – deep web – dark web
Forrás: a szerző szerkesztése

A korlátozott hozzáférésű hálózatok között találhatók a darknet-hálózatok, olyan infrastruktúrákon tárolt webhelyek, amelyek speciális szoftverek – például a TOR – használatát teszik szükségessé az elérésükhöz. A dark web és a deep web között különbség van, bár egyesek szinonimaként használják őket, de a dark web csak egy része a deep webnek. A dark web hálózatokon titkosított peer-to-peer kapcsolat jön létre a partnerek között. A dark web rendszerek példái közé tartozik a TOR, a Freenet vagy az Invisible Internet Project (I2P). A dark web a törvénytelen cselekményekkel kapcsolatos információk adattárháza. Idetartoznak a malware-szoftverekkel kapcsolatos információktól a pedofil oldalakon át a bérgyilkosságot végrehajtó hirdetésekig szinte minden, ami törvénytelen. Természetesen mind a deep webből, mind a dark webből kinyerhetők OSINT-módszerekkel, a megfelelő eszközökkel információk.

7. OSINT támogatása mesterséges intelligenciával

Az OSINT-forrásból nyert információk hatékony értékelésének, osztályozásának, felhasználásának előfeltétele azok megértése. A kognitív pszichológia által a múlt század elején felismert összefüggések és megértési modellek két alapvető intelligenciatípust különböztetnek meg.[20]

Az intelligencia összetevői két nagy csoportba sorolhatók, megkülönböztetik a „folyékony" és a „kristályos" intelligenciát. A folyékony (vagy fluid intelligencia) azt a képességet jeleníti meg, amellyel megértjük és hasznosítjuk az új információkat, vagyis az újszerű helyzetekben mutatott teljesítményt mutatja. A rögzült vagy kristályos intelligencia pedig azt jeleníti meg, hogy a tanult ismereteket, élettapasztalatokat mennyire vagyunk képesek hatékonyan alkalmazni. Vannak tudományos értelmezések, amelyek arra következtetnek, hogy létezik egy általános intelligencia (g-faktor) is, amely az úgynevezett „részképességekből" felépülő hierarchia csúcsán helyezkedik el.[21]

A természetes intelligencia felosztásának alapján az MI vonatkozásában a „kristályos" intelligencia leképezésére alkalmasak a felügyelt tanulásos ML- és RL-rendszerek, a „fluid" intelligencia vonatkozásában pedig a DNN (*deep neural network,* mély neurális hálók), illetve a felügyelet nélküli tanulásos ML-rendszerek.

Ami az OSINT internetes információkeresésre való alkalmazását illeti, a fő területek az információbiztonság, a digitális marketing és a mesterséges intelligencia voltak a 2000-es évektől. Az első OSINT-publikációk a hírszerzéssel, a harctevékenységgel és a terrorizmus felderítésével, a kommunikációval és a haditechnikával foglalkoztak. Az OSINT MI-vel való alkalmazását a gépi tanulási algoritmusok és a természetes nyelvi feldolgozás (NLP, *natural language processing*) használata az interneten található nagy mennyiségű információ kezelésére céllal említi a szakirodalom. Az OSINT és az MI közötti együttműködés platformokon, modelleken, keretrendszereken vagy rendszereken keresztül valósul meg.[22]

Míg a gépi tanulási algoritmusok az OSINT teljesítményének és sebességének növelését segítik elő, a természetes nyelvi feldolgozás az OSINT által feltárt eredmények elemzését támogatja. Az információbiztonság területén az OSINT MI-vel történő támogatása a kiberfenyegetések felderítése, a bűnüldözés, a digitális bizonyítékok gyűjtése, a penetrációs tesztek, az adatszivárgás és a vezeték nélküli hálózatok biztonsága vonatkozásában eredményes. Az egyik fő cél az OSINT automatizálásában a teljesítménynövekedés elérése.

Egy konkrét OSINT-alkalmazás a GI *(geospatial intelligence).*[23] Ez a rendszer olyan OSINT-szolgáltatást kínál, amely az automatizált adatgyűjtést, a big data adatelemzést és a human-in-the-loop elemzést kombinálja. A mesterséges intelligenciát, a gépi

---

20 Michael Glassman – Min Ju Kang: Intelligence in the Internet Age: The Emergence and Evolution of Open Source Intelligence (OSINT). *Computers in Human Behavior,* 28. (2012), 2. 673–682.

21 Kendra Cherry: What Is General Intelligence (G Factor)? *Verywell Mind,* 2021. április 25.

22 João Rafael Gonçalves Evangelista et al.: Systematic Literature Review to Investigate the Application of Open Source Intelligence (OSINT) with Artificial Intelligence. *Journal of Applied Security Research,* 16. (2021), 3. 345–369.

23 Lásd: https://storymaps.arcgis.com/stories/94b664c916aa4030baa704de8e9c3745

tanulást és a mély tanulást alkalmazzák valós globális problémák megoldására a távérzékelt adatok *(remotely sensed data)* és különösen a műholdképek feldolgozásánál. Gépi tanulási, mély tanulási és mesterségesintelligencia-algoritmusokat használva a több forrásból származó nagy adatmennyiség feldolgozásánál összefüggések felismerésére törekednek ezekben az adatokban. Emellett az eredményeket szűrik relevanciájuk szerint, feltárják a trendeket, minőségbiztosítást is végeznek, és végső soron végrehajtható felderítést biztosítanak ezáltal.

8. Példák az OSINT nemzetbiztonsági és katonai alkalmazásaira

Az *open source intelligence* rendkívül értékes adatforrás a hírszerzési elemzők számára a potenciális terrorizmusra vonatkozó figyelmeztetések és jelzések azonosítása és elemzése során. Az internetes webes adatok adatbányászata nagy mennyiségű információt biztosít a potenciális terrorizmusra vonatkozó figyelmeztetések és indikátorok azonosításához és elemzéséhez.

8.1. Terrorelhárítás

Az adatbányászat és az adaptív rezonanciaelmélet (*adaptive resonance theory,* ART) az egyik eszköz ehhez az elemzéshez.[24] A jellemzők kimutatása klaszteres adatkészleteken keresztül konkrét kulcsszavak keresésével indul. Ennek eredményessége érdekében a feldolgozás sebességének jelentős növelése szükséges.

A neurális hálózatok alkalmazása révén az adatok párhuzamos feldolgozása jelentősen javítja a feldolgozás sebességét a hagyományos szekvenciális módszerekhez képest. Az ART egy neurális hálózat, amelyet az e-kereskedelemben használnak annak érdekében, hogy a fogyasztóknak más, számukra valószínűsíthetően szintén érdeklődésre számot tartó termékre hívják fel a figyelmet a vásárlási lehetőségek vonatkozásában. Például, ha tetszik az „A" termék, akkor a „B" termék is tetszhet alapon.

Az *artificial neural network* (ANN) azaz mesterséges neurális háló az agyhoz hasonlóan egymáshoz kapcsolódó mesterséges neuronokból áll, amelyek rétegei adaptálódnak más, módosítható paraméterekkel rendelkező node-ok kimenetéhez. Az agy nagyon összetett, nem lineáris, párhuzamos feldolgozásra képes, és sokkal gyorsabban hajtja végre a mintafelismerést, -észlelést és vezérlést, mint a legtöbb számítógép. Az ANN számítási teljesítménye az architektúrájának párhuzamos, elosztott struktúrájából következik.

Az 1. táblázat egy 11 kifejezés használatával kinyert jellemzőkből álló modell, amely szemlélteti, hogyan használható az ART OSINT-elemzésre, valamint a potenciális terrorcselekmény előkészületeinek azonosítására és elemzésére. Az adatok figyelmeztetések és indikátorok a terrorizmus elleni háborúban.

[24] Jami Carroll: OSINT Analysis using Adaptive Resonance Theory for Counterterrorism Warnings. In *Artificial Intelligence and Applications. AIA '2005, Innsbruck,* 2005. 756–760.

1. táblázat: ART-alapú terrorcselekmény-előrejelző megoldás alap bináris logikai táblázata

Adatforrás	Osama bin Laden	Piszkos bomba	Boston	Khalid Sheikh Mohammed	Légi katasztrófa	Los Angeles	Zein al Abidin Mohammed Hussein	Épületrobbantás	Chicago	Abu Bakar Baasyir	Atomerőmű-robbantás
0	0	0	0	0	0	1	0	0	1	0	0
1	0	1	0	0	0	0	0	1	0	0	1
2	0	0	0	1	0	0	1	0	0	1	0
3	0	0	0	0	1	0	0	1	0	0	1
4	1	0	0	1	0	0	0	0	0	1	0
5	0	0	0	0	1	0	0	0	0	0	1
6	1	0	0	1	0	0	0	0	0	0	0
7	0	0	1	0	0	0	0	0	1	0	0
8	0	0	0	0	1	0	0	1	0	0	0
9	0	0	1	0	0	1	0	0	1	0	0

Forrás: Carroll (2005): i. m.

Az Adatforrás oszlop az e-mailt jelzi. A kulcsszavakra bináris „1” vagy „0” értékek utalnak egy elemzett e-mailben. (Ez természetesen lehet emberi hírforrás [HUMINT], névjegy, dokumentum, multimédiás fájl stb.) Ebben az egyszerűsített példában tíz e-mailre írják be az ART-kódot „1”-gyel, ha „igaz” értékre utal az adott entitásra vonatkozóan, vagy „0”, ha „hamis”. Az ART-algoritmus futtatása eredményeként a vizsgált e-maileket *(feature vector)* összevetik a vonatkoztatási attribútumokkal *(prototype vector),* aminek eredményeként következtetni lehet potenciális terrorveszélyre, szélsőség irányába való orientálódásra az adott személy vonatkozásában.[25]

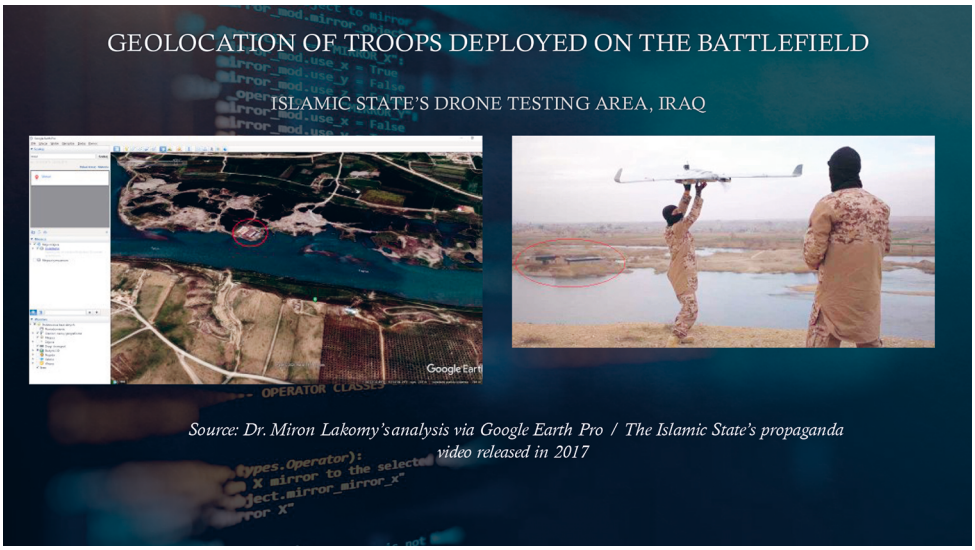
8.2. GlobState 2021 konferencia

Az OSINT katonai alkalmazásának ismert eseteibe adott betekintést a 4th Annual International Research Conference GlobState 2021 – Security Environment in the (Post) Pandemic World and Its Implications for the Conduct of Military Operations (30 November – 02 December 2021)[26] konferencián Prof. Miron Lakomy (University of Silesia) a *Military Application of Open Source Intelligence on the Internet* című

[25] Carroll (2005): i. m.
[26] Lásd: https://cdissz.wp.mil.pl/pl/pages/agenda_globstateiv

előadása során. Ezek mindegyikében bizonyítottan vagy erősen gyanítható módon mesterséges intelligencia is segítette az OSINT-adatok feldolgozását:

- Az Iszlám Állam moszuli kiképzőtáborának észlelése (2014) – GEOINT/IMINT;
- Az IS Drone bombájának elemzése (2017) – IMINT/TECHINT;
- az IS olajvagyonának földrajzi elhelyezkedése Irakban (2017) – GEOINT;
- a kínai információs műveletek felfedése a közösségi médiában #MILESGUO BOT NETWORK (2021) – közösségimédia-elemzés;
- a lengyel–fehérorosz határon szolgáló csapatok azonosítása (2021) – IMINT/TECHINT/közösségimédia-elemzés.



5. ábra: Az Iszlám Állam moszuli kiképzőtáborának észlelése (2014) – GEOINT/IMINT
Forrás: Prof. Miron Lakomy (University of Silesia)

8.3. Katonai infrastruktúrák OSINT-megfigyelése

Kiterjedt OSINT-megfigyelés zajlott a Nagorno-Karabakh (2020) konfliktus során (6., 7. ábra), amelynek anyagai bejárták az internetet, valamint az orosz katonai erők szíriai tevékenysége vonatkozásában (8. ábra). Szintén OSINT-eszközzel derítették fel a kalinyingrádi körzet radareszközeit (9. ábra):

- az Orosz Föderáció 15. különleges gépesített lövészdandár bevetése a környezetben–(2020) – IMINT;
- fehér foszforos gyújtólőszerek használata;
- a konfliktus mindkét oldalán az áldozatok számbavétele;
- csapatok/fegyverrendszerek harctéri helymeghatározása.

6. ábra: *Fegyverrendszerek harctéri helymeghatározása*
Forrás: Twitter@startupmonitOr

Az alábbi, OSINT-forrásból származó ábrák nyilvánvalóan mesterséges intelligenciával támogatott képfelismerő elemző folyamat eredményeként kerültek nyilvánosságra.

7. ábra: A folyamatosan zajló katonai műveletek megfigyelése, harctéren bevetett csapatok elhelyezkedése
Forrás: Twitter@NKobserver

8. ábra: A harctéren bevetett csapatok földrajzi helyzete, katonai építmények észlelése és elemzése (GEOINT)
Forrás: Twitter@ArrowontheHill

9. ábra: Katonai infrastruktúra észlelése radarinterferencia-beméró weboldalon (SIGINT/GEOINT)
Forrás: https://orbtwz.users.earthengine.app (Kaliningrad Oblast)

Az interneten elérhető nyílt eszközök alkalmasak katonai csapatösszevonások monitorozására is. Ezek közül a teljesség igény nélkül néhány:

- flightradar24.com;
- marinetraffic.com;
- live webcams;
- social media chatter (Twitter);
- analysis of smartphone apps (fitness tracking apps).

Ugyanígy bárki számára rendelkezésre álló GEOINT-eszközökkel OSINT-tevékenység végezhető:

- Google Earth;
- Google Earth Pro;
- Google Street View;
- Openstreetmap;
- satellites.pro;
- Bing Bird Eye.

9. Az MI alkalmazásának kockázati kihívásai

A fent említett lehetőségek és képességek mellett szólni kell a kockázatokról. Ezek egyike a black box, azaz a fekete doboz problémája, amely a mesterséges neurális hálózatok alkalmazásában jelentkezik. A neurális hálózatok rejtett csomópont- (node-) rétegekből állnak, amelyek mindegyike feldolgozza az adott inputot, és az outputot továbbítja a következő csomópontrétegnek. A mély tanulás nagyméretű mesterséges neurális hálózatot használ, sok rejtett réteggel, ami önmagát „tanítja" a minták felismerésével. A probléma abban rejlik, hogy nem láthatjuk, amit a csomópontok „megtanultak", sem a rétegek közötti kimenetet, sem 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, mint olyan MI-eszköz, amely olyan eredményeket hoz létre, amelyeket az ember megérthet és megmagyarázhat.[27]

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, ezzel a rendszert becsapják. Az alábbi, 10. ábra a manipuláció előtti és utáni képet, valamint a manipuláció előtti és utáni osztályozás valószínűségét mutatja. Látható, hogy a kép ugyanaz, de a rendszer az autót szibériai husky-nak ismerte fel.[28]

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

Ezek a problémák komoly kockázatot jelentenek az OSINT vonatkozásában, hiszen egy jól megtervezett Adversarial Artificial Intelligence művelet egy teljes felderítési stratégiát fel tud borítani, vagy biztosnak hitt információkat összezavarva hamis következtetések levonását eredményezheti.

[27] Carlos Zednik: Solving the Black Box Problem: A Normative Framework for Explainable Artificial Intelligence. *Philosophy & Technology,* 34. (2021), 2. 265–288.

[28] *Peter Svenmarck et al.: Possibilities and Challenges for Artificial Intelligence in Military Applications.* 2018, 7.

10. ábra: Minivan-ből hogy lesz szibériai husky
Forrás: www.researchgate.net/publication/326774966_Possibilities_and_Challenges_for_Artificial_Intelligence_in_Military_Applications

A mesterséges intelligencia szorosan kapcsolódik a big data technológiához, amely az OSINT-források halmaza. A hatékony MI-alkalmazáshoz szükséges adatbevitel kulcsfontosságú sikertényező, amely sokféle forrással rendelkezik. A big data technológiai fejlődése döntő hatással van az MI-megoldásokra. Ezért fontos annak feltárása és tisztázása, hogy mit jelent a big data, és milyen szerepet játszanak a big data eszközök a nemzetbiztonsági döntéshozatalban. Noha a biztonsági tanulmányokban nincsenek kifejezett definíciók a big data fogalmára, a nemzetbiztonsággal összefüggésben elfogadott, hogy: „olyan nagy mennyiséggel, sebességgel és változatossággal jellemezhető információs eszközök, melyek értékké alakítása speciális technológiát és elemzési módszereket igényel". A big data értéke nemzetbiztonsági kontextusban az alapvető hírszerzési követelmények: a gyűjtés, feldolgozás és hasznosítás, elemzés, terjesztés; valamint az elhárítás és a biztonság prizmáján keresztül értékelhető. Az *advanced data analytics* fejlett analitikai módszereket jelent nagy mennyiségű információ megértéséhez és megjelenítéséhez. A BDAA *(big data advanced analytics)* -nak négy alapvető eleme az adatgyűjtés, az érzékelők, a kommunikáció, az elemzés és a döntéshozatal. [29]

Mindenekelőtt a biztonság területén kulcsfontosságú a big data szerepének és korlátainak közös megértése, amely megkönnyíti annak hatékony használatát a biztonsági szakemberek és a döntéshozók számára. Ennek hiányában a döntéshozók nem fogadják el a big data automatizált elemzésének eredményeit, ha nem értik az adatelemzés mögött meghúzódó folyamatot, amely a megállapításokat produkálta, és nem tudják meggyőzően elmagyarázni a nyilvánosság számára az ebből eredő döntéseiket. Másfelől a döntéshozók indokolatlanul is bízhatnak a Big Data-eszközökben, tévesen *„silver bullet"*-ként értelmezve a technológiai megoldásokat.[30]

[29] NATO: *Science & Technology Trends 2020–2040. Exploring the S&T Edge* (2020).
[30] Damien Van Puyvelde – Stephen Coulthart – M. Shahriar Hossain: Beyond the Buzzword: Big Data and National Security Decision-Making. *International Affairs,* 93. (2017), 6. 1397–1416.

10. Következtetés

Az MI-vel támogatott OSINT elért ahhoz a ponthoz, ahol több katonai területen is alkalmazhatóvá vált. Az MI és a big data fejlett adatelemzésének várhatóan növekvő hatása lesz a katonai és nemzetbiztonsági alkalmazásokban. 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. Emellett az MI számára elegendő tanulási adatot kell rendelkezésre bocsátani.

A nemzetbiztonsági rendszerekbe való adatbeáramlás növekvő mennyisége és sebessége bizonyos fokú gépi tanulást és mesterséges intelligenciával támogatott döntéshozatalt igényel főként az elemzések fontossági sorrendjének meghatározásához. Az adatok automatizált elemzése azonban nem fogja megszüntetni az emberi megítélés szükségességét a nemzetbiztonsági döntéshozatal több szintjén, sőt megköveteli az ember-gép interakciók lehető leghatékonyabbá tételét.

Felhasznált irodalom

Carroll, Jami: OSINT Analysis using Adaptive Resonance Theory for Counterterrorism Warnings. In *Artificial Intelligence and Applications. AIA '2005, Innsbruck,* 2005. 756–760.

Cherry, Kendra: What Is General Intelligence (G Factor)? *Verywell Mind,* 2021. április 25. Online: www.verywellmind.com/what-is-general-intelligence-2795210

European Commission: *European Defence Industrial Development Programme (EDIDP)* (2020. július 23.). Online: https://ec.europa.eu/research/participants/data/ref/other_eu_prog/edidp/wp-call/edidp_call-texts-2020_en.pdf

Evangelista, João Rafael Gonçalves – Renato José Sassi – Márcio Romero – Domingos Napolitano: Systematic Literature Review to Investigate the Application of Open Source Intelligence (OSINT) with Artificial Intelligence. *Journal of Applied Security Research,* 16. (2021), 3. 345–369. Online: https://doi.org/10.1080/19361610.2020.1761737

Glassman, Michael – Min Ju Kang: Intelligence in the Internet Age: The Emergence and Evolution of Open Source Intelligence (OSINT). *Computers in Human Behavior,* 28. (2012), 2 673–682. Online: https://doi.org/10.1016/j.chb.2011.11.014

Izsa Jenő: *Nemzetbiztonsági alapismeretek.* Jegyzet. Budapest, ZMNE, 2009. Online: https://docplayer.hu/47243533-Nemzetbiztonsagi-alapismeretek.html

Lakomy, Miron: *Military Application of Open-Source Intelligence on the Internet.* 85-915 Bydgoszcz, Polska, 2021. Online: https://cdissz.wp.mil.pl/en/articles/news-2021/globstate-2021-new-operational-domains/

National Security Commission on Artificial Intelligence: *Final Report* (2021). Online: www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf

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

NATO: *NATO Open Source Intelligence Handbook* (2001). Online: www.academia.edu/4037348/NATO_Open_Source_Intelligence_Handbook

NATO: *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

Resperger István (szerk.): *A nemzetbiztonság elmélete a közszolgálatban.* Budapest, Dialóg Campus, 2018.

Saalman, Lora (szerk.): *The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk,* Volume II, East Asian Perspectives. SIPRI, 2019.

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

Tonin, Matej: *Artificial Intelligence: Implications for NATO Armed Forces.* Report. NATO Parliamentary Assembly, 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

Van Puyvelde, Damien – Stephen Coulthart – M. Shahriar Hossain: Beyond the Buzzword: Big Data and National Security Decision-Making. *International Affairs,* 93. (2017), 6. 1397–1416. Online: https://doi.org/10.1093/ia/iix184

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), 2. 265–288. Online: https://doi.org/10.1007/s13347-019-00382-7