Dr. Németh András – Virágh Krisztián***

Mesterséges intelligencia és haderő – További katonai alkalmazási lehetőségek VIII. rész

A mesterséges intelligencia alkalmazása számos területen óriási lehetőséget kínál a mindennapi élet megkönnyítésében, ugyanakkor önfejlesztő képessége és ártó célú felhasználása egyre nagyobb kockázatot is jelent. A szerzők, tanulmányuk előző részeiben bemutatták a legjelentősebb polgári alkalmazási lehetőségekben rejlő potenciált, és átfogó képet festettek a terület komplexitásáról. A cikksorozat zárásaként a MI haderőben betölthető szerepét mutatják be néhány kulcsfontosságú területre, elsősorban a harcszimulációs rendszerekre, és a felderítésre fókuszálva.

Harcszimulátorok

A mesterséges intelligencia egyik fontos katonai alkalmazási területe a harcszimulátorokhoz kapcsolódik. Négyféle harcszimulátor-megoldást különböztethetünk meg egymástól a résztvevők szerepe, és az alkalmazási környezet alapján: az élő, a virtuális, a konstruktív és a játékszimulátorokat [171], amelyek jellemzőit a *4. táblázatban* foglaltuk össze.

Az MI az egyes harcszimulátor-csoportok esetében a lehető legrealisztikusabb környezet kialakításához is képes hozzájárulni. Például élő szimulátorrendszerekben, a szenzorokkal felszerelt fegyvermodellek által szolgáltatott adatok mesterséges intelligencia alapú feldolgozásával pontosabban kiszámítható az imitált lövedékek ballisztikája, ami lényegesen realisztikusabb végrehajtást eredményezhet, mint egy egyszerűbb, lézeres érzékelésű fegyvermodell alkalmazása esetén. Különböző szimulációs gyakorlatok kivitelezésekor, ha az ellenséges erőket mesterséges intelligencia irányítja, kiküszöbölhetők a kezelői hibák, ráadásul a gyakorlat lebonyolításához szükséges állomány létszáma is csökkenthető. A katonák felkészítése a jövőben ugyanakkor – véleményünk szerint – integrált kiképzési környezetben zajlik (ITE – Integrated Training Environment), ami egyesíti mind a négy szimulátor típus képességeit. Ezalatt nem egy teljesen új, különféle funkcióval kiegészített szimulátor értendő, hanem különböző szimulátorok egymással szabványos interfészeken összekapcsolt hálózata, amely közösen képes hatékonyan hozzájárulni egy-egy katona vagy alegység teljes körű, egységes követelményrendszer alapján értékelhető kiképzéséhez. Az alternatív valóság technológiák (VR – Virtual Reality, AR – Agmented Reality, MR – Mixed Reality) fejlődési tendenciái alapjaiban befolyásolják a jövőben az ITE-koncepciójának gyakorlati megvalósíthatóságát. Az egyre több érzékszervet manipulálni képes technikai megoldások [172] közül a legjobb példát maguk a HMD[22]-eszközök jelentik, amelyek ma már magas immerzivitású vizuális élményt képesek nyújtani a felhasználók számára, ami elengedhetetlen feltétele annak, hogy a katonák reakciói is a lehető leghasonlóbbak legyenek a valós körülményekhez.

A harcszimulátorok közül – amelyekkel a tanulmány korábbi részeiben már részletesebben foglalkoztunk –, ezúttal a VBS3 játékszimulátort emeljük ki, amely rendkívül változatos feladatok – mint például a lőgyakorlatok felkészítő foglalkozásai, a térképészeti ismeretek, az alegységek tevékenységeinek bemutatása különböző körülmények között, vagy a C-IED (Counter Improvised Explosive Devices – rögtönzött robbanóeszközök elleni védelem) képzés tudásanyagának készségszintű begyakorlását teszi lehetővé. Ezek alapján egyaránt felhasználható akár az altiszt- és a tisztképzésben, akár az alapkiképzés, a missziós felkészítések, a nemzeti és nemzetközi CAx- (Computer Assisted Technology – számítógép által támogatott technológia) szimulációs gyakorlatok lebonyolítására. [173] A szimulátorban a mesterséges intelligencia úgy jelenik meg, mint egy, a virtuális egységeket – főként ellenséges egységeket és a civil lakosságot – irányító entitás, amely az előzetes beállításokat követően már önállóan képes elvégezni feladatait. [174] A szimulátor újabb verziója a VBS4, amely a VBS3 összes moduljával rendelkezik, ugyanakkor annál fejlettebb működésre képes. A legjelentősebb újítás a VBS Blue IG grafikus motor, amely lehetővé

49. ábra. VR-alapú harcászati kiképzés [176]

* Alezredes, tanszékvezető, egyetemi docens, NKE Hadtudományi és Honvédtisztképző Kar, Elektronikai Hadviselés Tanszék, ORCID: 0000-0003-2397-189X

** Cybersecurity Architect, Thyssenkrupp Components Technology Hungary, Product Cybersecurity Department, ORCID: 0000-0003-4184-9492

 DOI: 10.23713/HT.57.2.01

4. táblázat. A harcszimulátorok jellemzőinek összefoglalása (A szerzők szerkesztése)

	Résztvevő	Környezet	Végrehajtás	Példa
Élő szimulátor	Valódi	Valódi	Valós személy imitálja	MILES[17]
Virtuális szimulátor	Valódi	Virtuális	Valós személy imitálja és / vagy Virtuális egységeket irányítva	EST[18] 2000, DSTS[19], Kronos
Konstruktív szimulátor	Virtuális	Virtuális	Virtuális egységeket irányítva	Marcus, MILSIM[20]
Játék szimulátor	Virtuális	Virtuális	Valós személy imitálja és / vagy Virtuális egységeket irányítva	VBS3[21]

teszi, hogy a Föld bármely pontján, és a műveletek teljes spektrumában (szárazföld, vízfelszín, levegő) hajthassanak végre szimulációs gyakorlatokat. Tovább növelték a szoftver AR-/VR-kompatibilitását is a CIGI- (Common Image Generator Interface – számítógépes képgenerátor interfész) szabvány segítségével. [175] Az MI által támogatott funkciókat is bővítették (például a gépjármű-menetoszlop tevékenységének vezérlése), így kevesebb alájátszó szükséges egy szimulációs gyakorlat lebonyolításához. Tekintettel arra, hogy a VBS4 egy hosszú fejlődési folyamat eredménye, amelynek során felhasználták a korábbi verziók gyakorlati alkalmazása során szerzett tapasztalatokat, érdemes lenne megvizsgálni, hogy képezhetné-e központi elemét a Magyar Honvédség számára a jövőben kialakítandó integrált kiképzési környezetnek.

Hírszerzés, célpontkutatás, összadatforrású felderítés

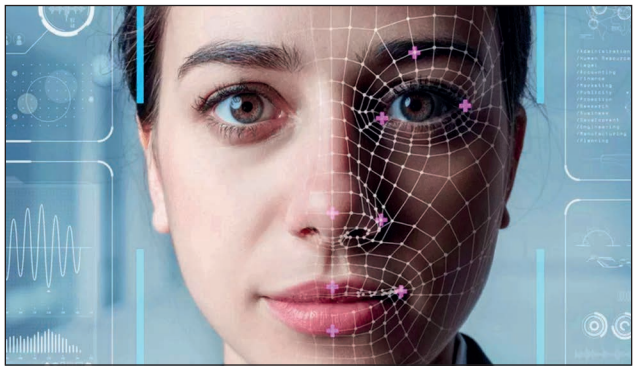
Komoly perspektívával rendelkezik a mesterséges intelligencia az ISTAR- (Intelligence, Surveillance, Target Acquisition, and Reconnaissance – hírszerzés, célpontkutatás, felderítés) feladatok legszélesebb spektrumában is. A hírszerzési, célpontkutatási és felderítési tevékenységek során lehetőség szerint minél több adat-, illetve információszerzési módszert alkalmaznak, így többek között igénybe veszik a HUMINT (Human Intelligence – emberi erővel végzett felderítés), IMINT (Image Intelligence – képi felderítés), a MASINT (Machine Intelligence – műszeres felderítés), az OSINT (Open Source Intelligence – nyílt forrású felderítés), a SIGINT (Signal Intelligence – rádióelektronikai felderítés) és a TECHINT (Technological Intelligence – technológiai felderítés) eszközrendszerét, módszereit. [177] A különböző forrásokból származó információk feldolgozása során, illetve a HUMINT kivételével minden más területen külön-külön is, a mesterséges intelligencia hatékonyan alkalmazható. Az IMINT és OSINT területeken történő alkalmazás lehetőségeivel részletesebben foglalkozunk.

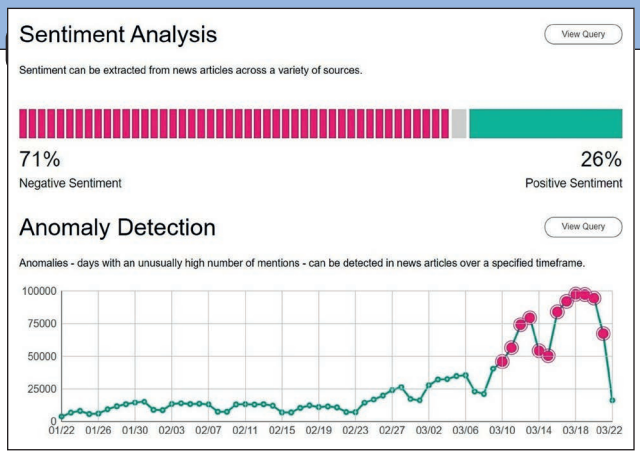
Egy célszemély, vagy az ellenséges erők tevékenységének megfigyelésére gyakran alkalmaznak képi felderítést, amelynek alapvető eszközei a különböző frekvencia-tartományokban (látható fény-, infra-, ultraibolya, radarhullámok) működő képalkotó eszközök, kamerák. [177] Amennyiben a felvételek elemzését, értékelését emberek helyett mesterséges intelligencia segítségével végezzük, gépi látásról beszélhetünk. Ennek lényege, hogy a szoftver jellegzetességek alapján detektál és ismer fel objektumokat, tevékenységeket, esetleg állapotokat. Sok más alkalmazási lehetőség mellett a harcértékbecslést, illetve az arcfelismerést tartjuk leginkább említésre érdemesnek. A harcértékbecslés lényege, hogy az ellenséges alegységekről felülről, különböző szögekből (drónról, vagy műholdról) készített felvételeken a megfelelő tanítóhalmazok segítségével fejlesztett MI lokalizálja és regisztrálja a különböző katonai objektumokat (épületeket, műtárgyakat, járműveket, eszközöket, katonákat). A rendszer komplexitását növelve, a következő szinten megpróbálja azonosítani azokat, meghatározni funkciójukat, típusukat, felszereltségüket, állapotukat, majd statisztikát készít róluk, és egymáshoz képest lévő elhelyezkedésüket is figyelembe véve meghatározza a lehetséges harcrendeket. Amennyiben a folyamatos megfigyelés feltételei biztosítottak, a változások nyomon követésével lehetségessé válik az ellenség szándékának felfedése, tevékenységének előrejelzése is.

Az arcfelismerő rendszerek az emberi arc jellegzetes jegyeit, geometriai elrendezését, egyes pontok (például a szemek) távolságát vizsgálják, éppen emiatt egy kellően szofisztikált rendszer akár arra is alkalmas, hogy az arc jelentős részének a kitakarása esetén is beazonosítson személyeket. Mivel ma már arra is van lehetőség, hogy egy több szögből lefotózott emberi arcból háromdimenziós modellt alkossunk, így nem feltétel, hogy az emberi arc minden részlete szemből látható legyen a felvételen. A mesterséges intelligencia össze tudja hasonlítani a modell arcvonásait a megfigyelt területen lévő emberek arcvonásaival, rangsorolja az egyezéseket, ami alapján nagy megbízhatósággal detektálható a célszemély. [178] A felismerés során a fals negatív, vagy fals pozitív (amikor nem ismer fel, vagy tévesen azonosít) eredmények aránya csökkenthető, ha az arcvonások mellett más jellegzetességeket is vizsgálunk, ami lehet például mimika-, gesztus-, vagy mozgásfelismerés, de az infravörös, vagy akusztikus tartomány bevonásával tovább bővíthetjük a vizsgált jellegzetességek körét (pl. beszédfelismerés). A cél az, hogy a fejlesztett rendszer ellenálló legyen akár a szándékos megtévesztéssel szemben is (pl. fénykép, okostelefon-, vagy tabletkijelzőjén visszajátszott, illetve manipulált videó, álarc viselése).

Ugyanakkor a személyazonosság meghatározásán túl lehetőség nyílik MI segítségével viselkedéselemzés elvégzésére is, amelynek segítségével akár nem azonosítható, idegen személyek szándékára vonatkozóan is vonhatunk le

50. ábra. Az arcfelismerő rendszer működése [179]





51. ábra. A Watson Discovery elemzései az angol „coronavirus” kifejezésre [182]

következtetéseket, ismerhetünk fel idő előtt például támadásra utaló jeleket. Nagyobb kiterjedésű rendszerek esetén (pl. térfigyelő rendszerek), ahol kamerák hálózata áll rendelkezésre, az információhalmaz kiegészíthető idő- és helyadatokkal, amelyek ismeretében további funkciókkal is kiegészíthető a struktúra (pl. célpontkövetés városi környezetben, vagy objektumon belül). A fentiek alapján az ilyen rendszerek felhasználhatók például a katonai objektumok védelmére akár beléptetőrendszerekben, akár missziós környezetben a katonai táborok külső környezetének megfigyelésére, a lehetséges támadások előrejelzésére (magányos, vagy csoportos elkövetők azonosítása). Természetesen a hasonló megoldások támogathatják a rendőrség bűnmegelőzési és bűnüldözési, illetve a büntetés-végrehajtási szervezet objektumvédelmi, vagy a külső helyszínen foglalkoztatott fogvatartottak megfigyelési tevékenységét, valamint a nemzetbiztonság és a terrorelhárítás területén feladatot ellátó szervezetek munkáját is jelentősen megkönnyíthetik.

A nyílt forrású felderítés legfőbb színtere maga a világháló, ahol különböző internetes oldalakon, nyilvános platformokon, közösségimédia-felületeken magánszemélyek, különböző szervezetek, érdek-, illetve értékközösségek, állami és vállalati szereplők, társadalmi és vallási csoportok osztanak meg tudatosan, vagy kevésbé tudatosan magukról, illetve másokról, valós, manipulált, vagy teljesen hamis, valós idejű, vagy archív információkat felhasználói fiókok milliárdjain keresztül. Néhány érdekes adat: csak a Facebook naponta 4 PB[23] adatot generál, a YouTube-ra percenként 3,5 évnyi felvételt töltenek fel, egy személy másodpercenként átlagosan 1,7 MB[24] adatot hoz létre és havonta 49,8 GB internetforgalmat generál, az összes keletkező adat 85%-a pedig más adatok másolata. Míg 2020-ban a világ digitális adatmennyisége „mindössze” 44 ZB[25]-ra rúgott, 2022-re ez több mint duplájára növekedve elérte a 97 ZB-ot (egy átlagos internetelőfizetőnek nagyságrendileg 2 Mrd évig tartana letölteni), három év múlva ez várhatóan 175 ZB-ot fog kitenni. [180] A jelenleg hozzáférhető „Big Data” eljárások már alkalmasak arra, hogy nagy mennyiségű adatot dolgozzanak fel. Az IBM Watson Discovery szolgáltatása is ilyen eljárásokra épül, azaz a különböző digitális formátumokban rendelkezésre álló strukturált és strukturálatlan adatokat gépi tanulási algoritmusok segítségével elemzi, rendszerezi és NLP-eljárásokon keresztül vizsgálja meg, hogy az adott forrásban a számunkra szükséges információ milyen kontextusban van jelen. [181] Jó példa a Watson Discovery működésére egy, a koronavírus-járvány idején a demóverzióval végzett teszt eredménye, ami az *51. ábrán* látható. A rendszer – a beállításoknak megfelelően – csak a járvány terjedésének kezdetén kijelölt 2 hónapos terminus forrásait vette figyelembe, amelyeken elvégezte az elemzést.

A „Sentiment Analysis”, azaz hangulatelemzés rész tartalmazza, hogy a keresett kifejezést a szöveg pozitív vagy negatív kontextusban szerepelteti-e. Az „Anomaly Detection”, azaz a rendellenesség-észlelés részben a rendszer azt emeli ki, hogy az adott időszakban melyik napokon szerepelt kiugró esetszámban a kifejezés. A fenti grafikonok különböző trendek elemzésére is alkalmasak, hiszen segítségükkel lemérhető egy adott hír, vagy esemény társadalmi fogadtatása, vagy akár egy szervezet pillanatnyi megítélése is. Ez a megoldás lehetővé teszi tehát a Magyar Honvédség társadalmi kapcsolatrendszerének vizsgálatát is, amely alapján meghatározható a helyes kommunikációs stratégia, a katonai pálya elismertségének erősítése a stabil utánpótlásbázis kialakítása érdekében. Az ehhez szükséges elemzéseket másodpercek alatt elvégzi a Watson Discovery, a felhasználónak csak azt kell megadnia bemeneti paraméterként, hogy milyen forrásokból dolgozzon a rendszer, és milyen időszakot vizsgáljon. A szoftver magyar nyelven jelenleg nem kínál szolgáltatást, ugyanakkor a Magyar Honvédség számára hasonló megoldás fejlesztése a fenti lehetőségen kívül számos további előnnyel is járhatna, például missziós területeken a CIMIC (Civil-Military Cooperation – Civil-Katonai Együttműködés), vagy a PSYOPS- (Psychological Operations – lélektani hadviselés) műveletek támogatása során.

A felderítés korábban említett területei a 21. században már nem választhatók szét markáns határvonalak mentén, a kapcsolódó tevékenységek hatékonyságát a különböző módszerekkel begyűjtött adatok integrált feldolgozása jelentősen fokozza. Ez az összadatforrású felderítés koncepciójának lényege, amely fogalom alatt azon komplex felderítési módszereket kell érteni, amelyek a hozzáférhető adat- és információforrások lehető legszélesebb körét, és a kapcsolódó technikai eljárásokat használják fel a cél elérése érdekében. A különböző módon megszerzett, eltérő formátumú adatok egységes rendszerbe foglalását úgynevezett fúziós adatfeldolgozás segítségével lehet megtenni, csak azt követően tudunk belőlük hatékonyan használható információkat kinyerni. [183] Ebben az információfeldolgozásban napjaink mesterséges intelligencia rendszerei már jelentős segítséget nyújtanak, illetve nyújthatnak, ezek fejlődése pedig alapjaiban fogja befolyásolni a jövő fegyveres konfliktusaiban az információs fölény kivívása érdekében végzett tevékenységek eredményességét.

Egyéb területek

Napjainkra a valós anyagi világgal párhuzamosan szinte teljesen kiépült egy digitális világ is, amelyben a valós szereplők mellett számos fiktív entitás is megjelenik. Így az a dimenzió egyfajta alternatív valóságnak is tekinthető, amelynek kollektív emlékezete nem feltétlenül kötődik szigorúan a valósághoz. Az ebben spontán kialakuló, vagy szándékosan létrehozott véleménybuborékok jelentősen képesek torzítani az egyének véleményét, súlyosabb esetben személyiségét, ezáltal komoly társadalmi változások generálására is alkalmasak. A kibertér szereplőinek egy része ezt a lehetőséget ki is használja politikai, vagy gazdasági céljai elérése érdekében. Ugyanakkor mindenki, aki bármilyen formában megjelenik a kibertérben – így minden állami vagy gazdasági szereplő – egyúttal fenyegetettségnek is ki van téve. Az onnan érkező különböző támadások céljától és módszereitől függően, akár a jelentős károkozás veszélye is fennáll. Ennek megelőzése, saját informatikai rendszereink védelme a kibervédelem alapvető feladata, amelynek technikai dimenziójában a mesterséges intelligenciák egyre komolyabb szerephez jutnak. Képesek észlelni a kibertámadásokat, azokat azonosítani és kategori-

zálni tudják, segítséget nyújthatnak a támadások forrásainak azonosításában, és az ellentevékenységek lebonyolításában. Felmérések szerint az MI-t leggyakrabban csalások, rosszindulatú szoftverek (malware) és zsarolóvírusok ellen, biztonsági rések osztályozásában, felhasználói és gépi viselkedéselemzésnél alkalmazzák. [184][185] Bár számos célszoftver elérhető a piacon, a nemzetbiztonsági szempontból kritikus – például a katonai rendszerek védelme érdekében –, érdemes lenne hosszú távon nemzeti fejlesztésekben is gondolkodni a kiberbiztonság területén.

A mesterséges intelligenciák alkalmazásának egy újabb fontos területe, amelyen komoly előrelépést lehetne elérni, a Magyar Honvédség nyilvántartási (pl. személyügyi, pénzügyi, logisztikai), valamint ügyviteli rendszere. Ezeken a területeken a hagyományos papír alapú megoldások aránya még mindig irreálisan magas, amely kezelésének humánerőforrás-igénye jelentős a haderő teljes létszámához képest. Természetesen a kapcsolódó fejlesztéseknél kiemelt figyelmet kell szentelni a kezelt adatok szenzitivitásának, ugyanakkor a rendszer reagálóképességének csökkentése érdekében ezt mindenképpen megoldandó problémaként kell kezelni.

Összegzés

A mesterséges intelligenciák tevékenyége – ha legtöbbször láthatatlanul is –, fokozatosan növekvő mértékben van jelen mindennapi életünkben, és befolyásolja például az elérhető szolgáltatások színvonalát. Ennek ellenére még nem beszélhetünk igazi áttörésről, ami többek között technológiai, technikai, gazdasági, jogi és morális okokkal magyarázható. Ugyanakkor a fejlődés ütemét figyelve nem lehetnek kétségeink afelől, hogy a következő évtizedekben alapjaiban változtatják majd meg gondolkodásunkon keresztül egész világunkat. Az MI számos területen óriási lehetőséget jelent a mindennapi élet megkönnyítésétől az emberiség legjelentősebb problémáinak megoldásáig, ugyanakkor önfejlesztő képessége és ártó célú felhasználása egyre nagyobb kockázatot is jelent. Jelen tanulmányunkban az MI-nek a haderő egyes elemeinek, képességeinek fejlődésében játszott szerepét mutattuk be néhány kulcsfontosságú területre fókuszálva. Az ismertetett forgatókönyvek alapján arra a következtetésre juthatunk, hogy a fegyveres konfliktusok kimenetele a jövőben egyre kevésbé mennyiségi, mint inkább minőségi kérdéssé válik, és az összecsapás nem feltétlenül a hadszíntér fizikai dimenzióiban fog eldőlni. A globális katonai erőviszonyokat a következő évtizedekben alapjaiban fogja meghatározni, hogy ki milyen ütemben, és milyen mértékben képes a mesterséges intelligenciát saját szolgálatába állítani, az általa kínált lehetőségeket, technikai megoldásokat fegyver- és vezetés-irányítási, valamint döntéstámogató rendszereibe integrálni.

Hivatkozott irodalom

[171] Virágh Krisztián. *Harcszimulátorok integrálásának lehetőségei a hazai katonai kiképzés rendszerébe, Tudományos Diákköri Dolgozat,* Budapest: Nemzeti Közszolgálati Egyetem, 2019.;

[172] Dr. Németh András, Virágh Krisztián. *Virtuális valóság és haderő – technológiai háttér II. rész, Haditechnika, LV. évf. 3. sz.,* pp. 8–16., 2021. DOI: 10.23713/HT.55.3.02;

[173] Dr. Németh András, Virágh Krisztián. *Virtuális valóság és haderő – katonai alkalmazási lehetőségek IV. rész, Haditechnika, LV. évf. 5. sz.,* pp. 2–7., 2021. DOI: 10.23713/HT.55.5.01;

[174] *VBS Control Behavior Pack: Breakthrough AI Behaviors at Your Command*, Bohemia Interactive Simulations, 2018.03.18. https://www.youtube.com/watch?v=RwDaom_KIkY (Letöltve: 2022.4.15.);

[175] *VBS BLUE IG*, Bohemia Interactive Simulations, https://bisimulations.com/products/vbs-blue-ig (Letöltve: 2022.10.25.);

[176] Forrás: https://www.roadtovr.com/the-gulf-between-high-end-military-vr-and-consumer-vr-is-rapidly-shrinking/; https://bisimulations.com/sites/default/files/website_1920x700_header_vbs4_20_1.jpg (Letöltve: 2022.11.5.);

[177] Haig Zsolt, Kovács László, Ványa László, Vass Sándor, Németh, András (szerk.). *Elektronikai hadviselés*, Budapest, Nemzeti Közszolgálati Egyetem, 2014. ISBN: 9786155305870 https://opac.uni-nke.hu/webview?infile=&sobj=9276&source=webvd&cgimime=application%2Fpdf%0D%0A (Letöltve: 2022.10.15);

[178] Kovács Tibor, Miklós Gellért. *A biometrikus adatok kezelésének jogi szabályozása,* Hadmérnök XIV. évf. 1. sz., pp. 8–16., 2019.;

[179] Forrás: *Facebook settles facial recognition dispute*, 2020.01.30. https://www.bbc.com/news/technology-51309186 (Letöltve: 2022.10.24.);

[180] *How Much Data Is Created Every Day in 2022*, Web tributal, 2022.10.07. https://webtribunal.net/blog/how-much-data-is-created-every-day/#gref (Letöltve: 2022.11.6.);

[181] IBM. *Watson Discovery*, https://www.coursera.org/learn/ai-with-ibm-watson/lecture/GF4X5/watson-discovery (Letöltve: 2022.10.24);

[182] Forrás: https://discovery-news-demo.ng.bluemix.net/ (Letöltve: 2020.3.20.);

[183] Kovács László. *Az elektronikai felderítés korszerű eszközei, eljárásai és azok alkalmazhatósága a Magyar Honvédségben*, Doktori (PhD) értekezés, Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem, 2003.;

[184] Louis Columbus. *Why AI Is The Future Of Cybersecurity*, Forbes, 2019.07.14. https://www.forbes.com/sites/louiscolumbus/2019/07/14/why-ai-is-the-future-of-cybersecurity/#70b243b0117e (Letöltve: 2022.10.24);

[185] Ronan Murphy. *With Watson, I can reduce response times to cybersecurity breaches by more than 50%*, IBM, https://www.ibm.com/watson/ai-professionals/smarttech/ (Letöltve: 2022.10.24).

Jegyzetek

17 MILES: Multiple Integrated Laser Engagement System – többcélú integrált lézeralkalmazású rendszer.
18 EST: Engagement Skills Trainer – lövészkatonák kiképzését elősegítő rendszer
19 DSTS: Dismounted Soldier Training System – gyalogos katona kiképző rendszer.
20 MILSIM: Military Simulation – katonai szimuláció.
21 VBS: Virtual Battlespace – virtuális hadszíntér.
22 HMD: Head Mounted Display – fejre illeszthető kijelző.
23 1 petabyte = 10^{15} byte.
24 1 megabyte = 10^{6} byte.
25 1 zettabyte = 10^{21} byte.