HADMÉRNÖK
VÉDELEMINFORMATIKA

17. évfolyam (2022) 3. szám 97–107.
DOI: 10.32567/hm.2022.3.7

Bihaly Barbara[1]

A mesterséges intelligencia felhasználása az információs és kibertérműveletekben – az orosz minta

Use of Artificial Intelligence in Information and Cyberspace Operations – The Russian Way

Napjainkban a legnagyobb veszély nem a kinetikus, hanem az információs térből érkezik. Az orosz hadsereg számára a védelmi eszköztár fő fegyvere az információ. Az információs műveletek koncepciója különleges helyet foglal el az orosz (és előtte a szovjet) katonai gondolkodásmódban. A mesterséges intelligencia mint a következő meghatározó technológia már a hadviselésben is megjelent. Az orosz hadsereg a mesterséges intelligencia katonai felhasználására való fejlesztésével beszállt az új típusú fegyverkezési versenybe, sajátos gondolkodásmódjával pedig új szintre léptette azt.

Kulcsszavak: **mesterséges intelligencia, hadviselés, Oroszország**

Nowadays, the biggest danger is not kinetic, but comes from the information space. For the Russian army, the main weapon of the defence toolbox is information. The concept of information operations occupies a special place in the Russian (and before that Soviet) military mindset. Artificial intelligence, as the next defining technology, has already appeared in warfare. By developing artificial intelligence for military use, the Russian army entered a new type of armaments race and took it to a new level with a specific way of thinking.

Keywords: **artificial intelligence, warfare, Russia**

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola, e-mail: bihaly.barbara@hm.gov.hu

1. Bevezetés

A mesterséges intelligencia (MI) napjaink meghatározó technológiája lett, bár még sok kérdést felvet.

A 2019-ben kiadott orosz mesterségesintelligencia-stratégia a következőképpen definiálja a mesterséges intelligenciát:

„[t]echnológiai megoldások összessége, amely lehetővé teszi az emberi kognitív funkciók szimulálását (beleértve az öntanulást és a megoldások keresését előre meghatározott algoritmus nélkül), és olyan eredmények elérését, amelyek olyan konkrét feladatok elvégzése során érhetők el, amelyek legalább összehasonlíthatók az emberi szellemi tevékenység eredményeivel. A technológiai megoldások komplexuma információs és kommunikációs infrastruktúrát, szoftvereket (beleértve a gépi tanulási módszereket is használó szoftvereket), adatfeldolgozási és megoldáskeresési folyamatokat és szolgáltatásokat tartalmaz."[2]

Az orosz stratégia az MI hivatalosan elismert meghatározását úgy mutatja be, mint

„olyan technológiai megoldások összességét, amelyek lehetővé teszik az emberi kognitív funkciók szimulálását […], valamint olyan eredmények elérését a konkrét feladatok elvégzése során, amelyek legalább összehasonlíthatóak az emberi szellemi tevékenység eredményeivel. Ez a technológiai megoldáskészlet információs és kommunikációs infrastruktúrából, szoftverekből […], valamint adatkezelési eljárásokból és szolgáltatásokból áll".[3]

A stratégia hangsúlyozza a mesterséges intelligencia stratégiai jelentőségét, amely előfeltétele annak, hogy Oroszország bekerüljön a gazdasági világvezetők csoportjába, valamint az ország függetlensége és technológiai versenyképessége is nagyban függ tőle. Annak ellenére, hogy Oroszország jelenleg nem számít vezetőnek a mesterséges intelligencia területén (hisz az USA-t számítjuk ebben is vezető hatalomnak), a dokumentum kijelenti, hogy Oroszországnak lehetősége van arra, hogy „nemzetközi vezetővé váljon a mesterségesintelligencia-technológiák fejlesztésében és használatában".[4]

Az MI felhasználása elég széles körű lehetőségeket mutat az élet mindennapi területein és az ipari vagy a katonai szektorban egyaránt. Ennélfogva nem túlzó az állítás, miszerint az MI területén folyamatos nemzetközi fegyverkezési verseny zajlik. De amíg a nyugati katonai szervezetek a mesterséges intelligenciát elsősorban a taktikai terület elemének tekintik, az orosz hadsereg az MI legnagyobb hasznát stratégiai szinten látja. Az orosz fókuszpont a mesterséges intelligenciával továbbfejlesztett információs

[2] „искусственный интеллект – комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые, как минимум, с результатами интеллектуальной деятельности человека. Комплекс технологических решений включает в себя информационно-коммуникационную инфраструктуру, программное обеспечение (в том числе в котором используются методы машинного обучения), процессы и сервисы по обработке данных и поиску решений;" Указ Президента РФ от 10 октября 2019 г. № 490 "О развитии искусственного интеллекта в Российской Федерации" Lásd: www.garant.ru/products/ipo/prime/doc/72738946/

[3] Lásd: www.garant.ru/products/ipo/prime/doc/72738946/

[4] Lásd: www.garant.ru/products/ipo/prime/doc/72738946/

műveleti eszközök alkalmazására irányul (beleértve a kibertéri műveleteket is) abból a célból, hogy mérhető stratégiai hatásokat érjenek el az ellenérdekelt államokkal szemben. Az MI ebben a minőségben való használata „harmadik forradalmat jelent a katonai ügyekben".[5]

Az MI az elkövetkező évek meghatározó technológiai trendje, tagadhatatlan hatása van a gazdaságra, a politikára és a társadalomra. Ezért a világ vezető államaiban kialakult az igény ennek a technológiának a fejlesztésére és felhasználására. Oroszországban nominálisan a hadsereg áll az ilyen témájú K+F élmezőnyében, a nyugati országokban és Kínában a fejlesztés a magánszektor sajátja. Elmondható tehát, hogy Oroszországban a hadsereg vezet jelenleg minden jellegű technológiai fejlesztésben.[6] A kiber- és információs képességeket használó rosszindulatú befolyásoló kampányok jelentős politikai zavart okoztak az egyes államok működésében (például létfontosságú infrastruktúra működésének zavarása, kormányzati rendszerek túlterhelése, dezinformációs kampányok stb.), de a kampányok következő generációja jelentősen károsabb lehet az MI széles körű használata miatt.

A kampányok sikeres lebonyolításának módszerei jelenleg (most még) függenek a mögöttük álló humán erőforrástól. A mesterséges intelligencia bevezetése nagymértékben javítani fogja a tömeges közönség személyre szabott és elfogadható tartalommal való elérése automatizálásának képességeit. Következésképpen még erőteljesebbé teszik a rosszindulatú szereplőket.

Jelen cikk célja bemutatni a mesterséges intelligencia információs és kibertér műveleti felhasználásának módjait az orosz hadviselés kontextusában.

2. A mesterséges intelligencia és lehetőségei a katonai szektorban

Ez a szakasz csupán néhány kiragadott példát mutat be, ahol az MI alkalmazható a katonai képességek fokozására.

Első példa a felderítés. A tengeri felügyeletet rögzített radarállomások, járőrrepülőgépek, hajók, valamint az utóbbi években az automatikus azonosító rendszert használó tengeri hajók elektronikus nyomon követését végzi az MI. Ezek az információforrások nagy mennyiségű adatot szolgáltatnak a hajók mozgásáról, ami illegális, nem biztonságos, fenyegető és rendellenes viselkedést tárhat fel. A hajómozgásokkal kapcsolatos nagy mennyiségű információ azonban megnehezíti az ilyen viselkedés észlelését, ha csupán emberi erőforrásra támaszkodunk. Ehelyett a gépi tanulási megközelítéseket használják arra, hogy különböző modelleket hozzanak létre a hajómozgások adataiból. A modellektől eltérő bármilyen egyéb mozgást rendellenesnek tekintik, és ellenőrzés céljából bemutatják az üzemeltetőknek.[7]

[5] Rod Thornton – Marina Miron: Towards the 'Third Revolution in Military Affairs'. The Russian Military's Use of AI-Enabled Cyber Warfare. *The RUSI Journal,* 165. (2020), 3. 12–21.

[6] Vooruzhennyye Sily RF Vnedryayut Tekhnologii Iskusstvennogo Intellekta. *Voenniye Materialy,* 2018. március 15.

[7] Peter Svenmarck et al.: Possibilities and Challenges for Artificial Intelligence in Military Applications. In *Proceedings of the 2018 NATO Big Data and Artificial Intelligence for Military Decision Making Specialists' Meeting*. 2018.

A modellek lehetővé teszik azoknak a hajóknak a felismerését, amelyek irányt váltanak, tengeri sávokat kereszteznek, ellentétes irányba vagy nagy sebességgel haladnak. A legújabb megközelítések a Bayes-hálózatokkal[8] fedezik fel a hamis hajótípust, valamint a szakaszos, lehetetlen és lebegő hajómozgást.[9] A tengeri anomáliák felderítése jövőbeli fejlesztéseinek figyelembe kell venniük a környező hajókat és a több hajó közötti kölcsönhatást is.

Második példa a gépi látás és a mély neurális hálózatokat (*deep neural network,* DNN) alkalmazó technológiák gyakorlati felhasználásának lehetősége a mélytengeri aknák felderítésében.

A víz alatti aknák komoly veszélyt jelentenek a tengeri hajókra, a mozgás irányítására vagy a korlátozott vizeken való áthaladás megakadályozására szolgálnak. Az aknakeresést egyre inkább autonóm víz alatti járművekkel (*autonomous underwater vehicle,* AUV) hajtják végre, amelyek olyan szintetikus apertúrájú szonárral (*synthetic aperture sonar,* SAS) vannak felszerelve, amelyek centiméteres felbontású akusztikus képeket nyújtanak a tengerfenékről. Mivel az AUV-k nagy mennyiségű SAS-képet gyűjtenek, az automatikus célosztályozás hasznos a potenciális aknák és más objektumok megkülönböztetéséhez. Míg az aknák automatikus célbesorolását hosszú ideje tanulmányozták, a DNN-ek nagy teljesítménye a képosztályozás során felvetette annak lehetőségét, hogy miként lehetnek alkalmasak az aknák automatikus észlelésére.

A DNN megtanítható az AUV- és az SAS-rendszerek által gyűjtött adatokkal, hogy milyen formájú egy próbaakna, milyen egy aknaszerű célpont, illetve milyen ember alkotta tárgyak találhatók meg a tengerfenéken. Az eredmények azt mutatják, hogy a DNN szignifikánsan nagyobb teljesítménnyel rendelkezik, nagyobb valószínűséggel észleli az aknák alakjait, és alacsonyabbak a téves riasztási arányok, mint egy hagyományos célosztályozó esetén.[10]

Harmadik példa a kiberbiztonság. A behatolásfelismerés a kiberbiztonság fontos része a rosszindulatú hálózati tevékenységek felderítéséhez. Erre fejlesztették ki az úgynevezett behatolásészlelő rendszert (*intrusion detection system,* IDS), amely a hálózati forgalmat elemzi és jelez a normálistól eltérő forgalom esetén. Mivel azonban a normális hálózati forgalomnak gyakran hasonló jellemzői vannak, mint a tényleges támadásoknak, ezeket szakemberek külön elemzik. Ugyanakkor, amíg az aláírás-alapú IDS-ek gyakran alkalmasak az ismert támadási minták észlelésére, nem képesek korábban nem látott támadásokat észlelni, ezért az aláírás-alapú észlelés fejlesztése gyakran lassú és költséges.[11] Ennek eredményeképpen ez akadályozza a rendszerek alkalmazkodóképességét a gyorsan fejlődő kiberfenyegetésekkel szemben.

[8] A bayesi hálózat (más néven a Bayes-hálózat, hiedelemhálózat, vagy döntési hálózat) egy valószínűségi grafikus modell, amely változók halmazát és azok feltételes függőségeit ábrázolja egy irányított aciklusos grafikonon (DAG) keresztül. A bayesi hálózatok ideálisak egy bekövetkezett esemény felvételére és annak valószínűségének előrejelzésére, hogy a lehetséges ismert okok bármelyike a hozzájáruló tényező. Lásd: https://hu.wiki4maps.com/438896-bayesian-network-CTDYOZ

[9] Steven Mascaro – Ann E. Nicholso – Kevin B Korb: Anomaly Detection in Vessel Tracks Using Bayesian Networks. *International Journal of Approximate Reasoning,* 55. (2014), 1. 84–98.

[10] David P. Williams: Underwater Target Classification in Synthetic Aperture Sonar Imagery Using Deep Convolutional Neural Networks. In *Pattern Recognition (ICPR), 2016 3rd International Conference,* Cancún, 2016. 2498–2503.

[11] Gulshan Kumar – Krishan Kumar – Monika Sachdeva: The Use of Artificial Intelligence Based Techniques for Intrusion Detection: A Review. *Artificial Intelligence Review,* 34. (2010), 4. 369–387.

Sok fejlesztés során használnak gépi tanulási (*machine learning,* ML) és más MI-hoz köthető technológiákat az ismert támadások osztályozási pontosságának növelésére, a rendellenes hálózati forgalom észlelésére (mivel ez új támadási mintákat jelezhet, amelyek eltérnek a normál hálózati forgalomtól), és automatizálják a modell felépítését.

E rendszerek közül azonban keveset használnak operatív módon. Ennek az oka, hogy az olyan kérdések, mint például a behatolások észlelése, olyan speciális kihívásokat jelentenek, mint az MI tanításához szükséges adatbázisok hiánya. Másik probléma általában a hálózati forgalom nagy változatossága, de a szükséges értékelések elvégzését is sokszor akadályozza a megfelelően képzett és mennyiségű szakértő hiánya. Noha nagy mennyiségű hálózati forgalom gyűjthető, az információk gyakran érzékenyek és csak részben névtelenek.[12]

A szimulált adatok használata egy másik lehetőség, de ezek gyakran nem elég valósághűek. Az adatokat kategorizálni kell a felügyelt tanuláshoz, azért, hogy eldönthető legyen, a minták a normális mintának megfelelnek-e, vagy behatolásnak számítanak-e. Végül a modelleknek átláthatóknak kell lenniük, hogy a kutatók megértsék a jellemzők észlelési határait és jelentőségét.[13]

A kiberbiztonság növelésének másik módszere a behatolási tesztek (*penetration test,* penetrációs teszt) elvégzése. A biztonsági auditok során a potenciálisan kihasználható biztonsági gyengeségeket azonosítják ezekkel a tesztekkel. A behatolási tesztek gyakran automatizáltak, mivel sok hálózat bonyolult és nagyszámú gazdagépet tartalmaz.

Jörg Hoffmann tanulmánya azt vizsgálta, hogyan lehet az MI-technikákat felhasználni szimulált penetrációs tesztelésre a hálózat logikai modelljeivel, nem pedig a tényleges hálózattal.[14] A hálózatot gyakran ábrázolják támadási grafikonok vagy fák, amelyek azt mutatják, az ellenfél hogyan tudja kihasználni a sebezhetőségeket, hogy behatoljon egy rendszerbe.

Hoffmann azonban leírja, hogy a modellek hogyan különböznek azok jellemzői alapján: a) a támadás függ az absztrakt sikertől, az észlelési valószínűségektől és a hálózati állapot bizonytalanságától, és b) a támadó cselekedetei függenek az ismert pre- és posztfeltételektől, az általános érzékeléstől és az eredmények megfigyelésétől.[15]

Ezenkívül a hálózatok és a gazdagépek formális modelljeivel lehetőség van a különböző mérséklési stratégiák elemzésére. A behatolási tesztelés jövőbeni kutatása valószínűleg kognitív módon érvényes modelleket fog felhasználni a támadó és a védő közötti interakcióról, például mélyreható tanulási módszerrel a lehetséges támadások nagy problématerületének feltárására.

[12] Carlos A. Catania – Carlos García Garino: Automatic Network Intrusion Detection: Current Techniques and Open Issues. *Computers & Electrical Engineering,* 38. (2012), 5. 1062–1072.

[13] Robin Sommer – Vern Paxson: Outside the Closed World: On Using Machine Learning for Network Intrusion Detection. In *2010 IEEE Symposium on Security and Privacy (SP).* IEEE, 2010. 305–316.

[14] Jörg Hoffmann: Simulated Penetration Testing: From "Dijkstra" to "Turing Test++". In *Proceedings of the International Conference on Automated Planning and Scheduling (ICAPS).* 25. (2015), 1. 364–372.

[15] Hoffmann (2015): i. m.

3. A mesterséges intelligencia katonai felhasználása Oroszországban

Nem volt meglepetés, hogy a mesterséges intelligencia megjelenésével Oroszország is beszáll a versenybe, hogy először használhassa katonai célokra az új képességet. Bár kezdetben az orosz beruházás mértéke elmaradt versenytársaiétól (Amerikai Egyesült Államok, Kína), a 2008-ban megkezdett szélesebb körű védelmi modernizációs erőfeszítések részeként az Orosz Katonai Ipari Bizottság célul tűzte ki, hogy a katonai felszerelések 30%-a 2025-re robotizálódjon.[16] 2016-ban az orosz kormány létrehozott egy védelmi kutató szervezetet, amely az Alapítvány a Haladó Tanulmányokért (Фонд перспективных исследований[17]) nevet viselte, és éves konferenciát kezdeményezett az „Orosz Föderáció fegyveres erőinek robotizálása" témában.[18] 2017-ben Oroszországból regisztrált a negyedik legtöbb felhasználó a Kaggle-re, a nyílt forráskódú platform mesterségesintelligencia-kutatásra.[19] Ez jól jelzi, amellett, hogy az orosz kockázati tőkések aktívan keresik a lehetőségeket a mesterségesintelligencia-piacon külföldön, hogy milyen komolyak az orosz szándékok a fegyverkezési versenyben.

Az orosz hadsereg számos védelmi alkalmazási módot kutat az MI felhasználására, nagy hangsúlyt fektetve az autonóm járművekre és a robotikára. 2017. november 1-jei hivatalos nyilatkozatában ezt alátámasztotta Viktor Bondarev, a Föderációs Tanács Védelmi és Biztonsági Bizottságának elnöke, amikor kijelentette, hogy „a mesterséges intelligencia képes lesz helyettesíteni a katonát a harctéren, a pilótát pedig a repülőgép pilótafülkéjében", és később bejelentette, hogy „közeleg a nap, amikor a járművek mesterséges intelligenciát kapnak".[20]

Bondarev ezeket a megjegyzéseket közvetlenül a Nerehta pilóta nélküli földi rendszer sikeres tesztje után tette. A moduláris jármű, amely a teszt során állítólag „felülmúlta a már meglévő ember vezette harci járműveket", képes egy 7,62 mm-es géppuska hordozására, és használható harci, hírszerzési vagy logisztikai célokra. Az orosz hadsereg azt tervezi, hogy a Nerehtát az MI kutatási és fejlesztési platformjaként használja, amely potenciálisan magában foglalja az autonóm célfelismerési képességet.[21]

Ezek a fejlemények aggodalmat ébresztettek a nemzetközi helyzetelemzőkben, akik azt is megjegyzik, hogy az orosz hadsereg sokféle autonóm járműkoncepciót kutat, beleértve a harckocsi méretű eszközöket is, míg az ellenérdekelt hadseregek eddig csak a támogató funkciókra fókuszáltak. Ugyanakkor a versenytársakhoz hasonlóan az orosz hadsereg azt tervezi, hogy beépíti a mesterséges intelligenciát pilóta nélküli légi járművekbe, haditengerészeti eszközökbe és személyzet nélküli tengeralattjárókba, a rajképességek integrálása érdekében.[22]

Ezenkívül egyes elemzők úgy vélik, hogy az orosz hadsereg valószínűleg a kémkedés és a propagandacélú mesterségesintelligencia-alkalmazásokat is kutatja. Ezen

[16] Tom Simonite: For Superpowers, Artificial Intelligence Fuels New Global Arms Race. *Wired,* 2017. szeptember 8.
[17] Lásd: https://fpi.gov.ru
[18] Samuel Bendett: Red Robots Rising: Behind the Rapid Development of Russian Unmanned Military Systems. *The Strategy Bridge,* 2017b. december 12.
[19] Leon Bershidsky: Take Elon Musk Seriously on the Russian AI Threat. *Bloomberg,* 2017. szeptember 5.
[20] Samuel Bendett: Should the US Army Fear Russia's Killer Robots? *The National Interest,* 2017a. november 8.
[21] Patrick Tucker: Russia Says It Will Field a Robot Tank that Outperforms Humans. *Defense One,* 2017. november 8.
[22] Sydney J. Freedberg Jr.: Armed Robots: US Lags Rhetoric, Russia. *Breaking Defense,* 2017. október 18.

elemzők feltételezése szerint Oroszország olyan eszközöket vizsgálhat, amelyek az eredeti forrásanyag kis mintamérete alapján nagy pontosságú videó- és hanghamisításra képesek.[23]

4. Mesterséges intelligencia vezette orosz információs és kibertérműveletek

Az orosz hadsereg számára a védelmi eszköztár fő fegyvere az információ. Az információs műveletek koncepciója különleges helyet foglal el az orosz (és előtte a szovjet) katonai gondolkodásmódban.

Geraszimov a közelmúltban többször hangsúlyozta az információ növekvő jelentőségét az állami ellenfelek semlegesítésének érdekében. „Az információs technológiák (…) az egyik legígéretesebb fegyvertípussá válnak, amelyet más országokkal szemben lehet használni."[24] Ebből következik, hogy az információs műveletek előkészítése és lebonyolítása kérdéseinek tanulmányozása a hadtudomány legfontosabb feladata napjainkban.

Geraszimov e kijelentéséből az is kitűnik, hogy az információs műveletek elsődlegesek, és az ehhez tartozó eszköztár fejlesztése nagyobb prioritást élvez az orosz hadseregben, már csak abból is kiindulva, hogy az ilyen jellegű műveleteket támogató technológiai fejlesztések középpontjában jelenleg a mesterséges intelligencia áll.

Az orosz hadsereg gondolkodását arról, hogyan lehetne a legjobban használni az MI-t ebben a tekintetben, Losev 2018-as *A katonai mesterséges intelligencia* című cikke részletezte az *Arsenal Otechestva* című folyóiratban. A cikk bemutatja, hogy az MI milyen előnyökkel járhat a fegyveres erők törekvéseiben. A lista élén nem írt az MI szerepéről az autonóm rendszerekben vagy más kifejezetten katonai technológiában. Inkább annak információstér-beli funkcióját vizsgálta, konkrétan a nagy stratégiai szintet megcélozva.[25]

Polyakova a *Weapons of the Weak* című cikkében a következőképp fogalmazott: „Az MI potenciálisan felerősítheti Oroszország dezinformációs műveleteinek hatását, valamint a hamis és félrevezető információk szándékos terjesztésének sebességét a politika és a társadalmak befolyásolása céljából."[26] Azonban az orosz gondolkodás az MI használatáról az információs környezetben sokkal tovább megy, mint pusztán a befolyásolás. Ha a mesterséges intelligenciának a „harmadik forradalmat kell képviselnie a katonai ügyekben",[27] akkor sokkal többet kell tennie, mint pusztán befolyásolni, következésképpen az MI-vel támogatott információs hadviselésnek is képesnek kell lennie a pusztításra. Ahogy Ilnitsky és Losev kifejezik, a mai konfliktusokban, „ahol a forró háború annyira valószínűtlen, ott az ellenség pusztításának fő

[23] Samuel Bendett: Red Robots Rising. *RealClear Defence,* 2017c. december 12.
[24] Gerasimov, 'Vektory Razvitiya Voyennoy Strategii' ['The Vectors of Military Strategic Development'], 11.
[25] Aleksandr Losev: Voennii Iskusstvenii Intellekt ['Military Artificial Intelligence']. *Arsenal Otechestva,* 6. (2018), 32. 12–21.
[26] Alina Polyakova: Weapons of the Weak: Russian and AI-Driven Asymmetric Warfare. *Brookings Institution,* 2018. november 15.
[27] Thornton–Miron (2020): i. m.

eszköze az [ellenségen belüli] nagy fokú instabilitás megteremtése, az információk manipulálása és kiberhatások révén".[28]

Az orosz katonai gondolkodásban a kiberhadviselés az információs hadviselés részhalmaza. E gondolat logikájának mentén megállapítható, hogy az MI által támogatott kibertérműveletekből fakadó stratégiai fenyegetés mélyreható.

Orosz szempontból a kibertéri műveleteknek pszichológiai és technológiai vonatkozásai egyaránt vannak.[29] A pszichológiai vonatkozás magában foglalja azon számítógépes (kiber-) eszközöket, amelyeket olyan információk terjesztésére használnak, amelyek célja a nagymértékű befolyás generálása, akár propaganda, akár álhírterjesztés (hoaxkampányok) formájában.

A mesterséges intelligenciával kapcsolatos fejlemények arra mutatnak, hogy alapvetően fokozzák az orosz kibertérműveletek ezen formájának hatásait. Az MI-t támogató eszközök képessé válhatnak igen valósághű, hamis információk létrehozására (például *deepfake* videók révén). Ahogy Losev leírja, az MI „nagy mennyiségű, mesterségesen előállított adattal töltheti be az információs teret, ez a »virtuális igazság« megzavarja a potenciális ellenfeleket".[30]

Egy ilyen művelet káros hatással lenne az ellenérdekelt állam döntéshozatalára, mivel nagyon kevés megbízható információ állna rendelkezésre. Alapvetően képes lenne aláásni a kormányokba és a demokratikus működésbe vetett hitet. Az információkba vetett hit nélkül a kormányok, a társadalmak és a katonai szervezetek nem tudnak hatékonyan működni. Az állami funkciók egyszerűen összeomolhatnak, mivel nem képesek felismerni az igazságot.[31] Ezzel elérkezne a kognitív háború kora a kibertérben.

A kibertérműveletek másik eleme a technológiai infrastrukturális háttér.[32] Ennek középpontjában egyaránt állnak a rosszindulatú programok, az alkalmi pusztítás és a felderítés a számítógépes rendszerek gyengeségeinek felkutatásában.

Losev rámutat, hogy a technológiai szférában az MI megjelenése most sokkal könnyebbé teszi a sebezhetőségek felkutatását az ellenfél informatikai rendszereiben. Az MI-vel, ahogy ő fogalmaz, a gyengeségekre való vadászat hatalmas méreteket fog ölteni.[33] Ez azt jelenti, hogy a kibertámadások sokkal összetettebbé és nagyon veszélyessé válnak a megcélzott állam számára. Továbbá valós lehetőségét látja annak, hogy néhány jövőbeli „harmadik világháború" néhány másodpercen belül ténylegesen véget érjen, ha az egyik állam átveszi az irányítást a riválisországok kritikus (információs) infrastruktúrái felett, az MI segítségével. Ugyanakkor, amint egy másik orosz forrás kifejezi, „minden katonai szervezet, amely ilyen módon használja az MI-t, világvége *(doomsday)* technológiát hozhat létre".[34]

[28] Thornton–Miron (2020): i. m.
[29] Timothy Thomas: Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts. *Journal of Slavic Military Studies,* 27. (2014), 1. 101–130.
[30] Losev (2018): i. m. 2.
[31] Andrei Bezrukov: Vyklyuchit' Svet v Kremle: Chego Zhdat' ot Kibervoyn [Turn off the Lights in the Kremlin: What to Expect from Cyberwar]. *Gazeta,* 2018. október 13.
[32] Thorton–Miron (2020): i. m. 17.
[33] Losev (2018): i. m. 2.
[34] Tekhnologii "Sudnogo Dnya": Vooruzhennyye Sily Rossii Vnedryayut Iskusstvennyy Intellekt ['Doomsday Technologies': Russia's Armed Forces Introduce Artificial Intelligence]. *Yandex,* 2018. március 16.

5. Összegzés, következtetések

„Jelenleg a csatákat nem a csatatéren vívják, hanem először az információs térben" – fogalmazta meg Jurij Boriszov egykori miniszterhelyettes 2018-ban.[35]

Oroszországban a mesterséges intelligenciával támogatott információs és kibertérműveletek stratégiai szinten való használata a legmagasabb szintű politikai támogatást élvezi. Oroszország végső célját ismerve – az információs tér végső és kizárólagos kontroll alá vonása – az is megjegyezhető, hogy a mesterséges intelligencia fejlesztése lehetővé tenné az információs térben a hatékony ellentevékenységet, és elősegítené a végső győzelmet – legalábbis a fegyverkezési versenyben mindenképp.

Az Oroszországból érkező legnagyobb fenyegetés a Nyugatra nézve nem kinetikus, sokkal inkább technológiai és pszichológiai lesz.

Másrészről komoly intézkedéseket vezet be Oroszország az információstér-beli védelem növelésének, a sérülékenységi lehetőségek minimalizálásának, valamint a szuverenitás megőrzésének érdekében.

Az MI támogatta kiberfenyegetés már nem csupán elmélet. Akár rosszindulatú programokról, akár álhírekről van szó, a kiber- és információstér-beli fenyegetések és támadások lerombolhatják a nemzeti kritikus (információs) infrastruktúrákat és alááshatják a demokráciát.

Amíg a nyugati lineáris gondolkodásban az MI csak kiegészítője a meglévő katonai technológiáknak és műveleteknek, az orosz hadsereg gondolkodása az állandó stratégiai előnyre való törekvés kultúrája miatt nem korlátozódik ennyire: a hadviselés új módjait igyekszik kialakítani az új technológiák alkalmazásával. Ezt a gondolkodást érdemes elsajátítani, nem csak megfigyelni.

Felhasznált irodalom

Bendett, Samuel: Should the US Army Fear Russia's Killer Robots? *The National Interest,* 2017a. november 8. Online: http://nationalinterest.org/blog/the-buzz/should-the-us-army-fear-russias-killer-robots-23098

Bendett, Samuel: Red Robots Rising: Behind the Rapid Development of Russian Unmanned Military Systems. *The Strategy Bridge,* 2017b. december 12. Online: https://thestrategybridge.org/the-bridge/2017/12/12/red-robots-rising-behind-therapid-development-of-russian-unmanned-military-systems

Bendett, Samuel: Red Robots Rising. *RealClear Defence,* 2017c. december 12. Online: www.realcleardefense.com/articles/2017/12/12/red_robots_risin_112770.html

Bershidsky, Leon: Take Elon Musk Seriously on the Russian AI Threat. *Bloomberg,* 2017. szeptember 5. www.bloomberg.com/view/articles/2017-09-05/take-elon-musk-seriously-on-the-russian-ai-threat

[35] Iskusstvennyi Intellekt: Puti i Resheniya [Artificial Intelligence: Problems and Solutions]. *Arsenal Otechestva,* 2018. március 27. 1.

Bezrukov, Andrei: Vyklyuchit' Svet v Kremle: Chego Zhdat' ot Kibervoyn [Turn off the Lights in the Kremlin: What to Expect from Cyberwar]. *Gazeta,* 2018. október 13. Online: www.gazeta.ru/comments/2018/10/12_a_12018991.shtml

Catania, Carlos A. – Carlos García Garino: Automatic Network Intrusion Detection: Current Techniques and Open Issues. *Computers & Electrical Engineering,* 38. (2012), 5. 1062–1072. Online: https://doi.org/10.1016/j.compeleceng.2012.05.013

Freedberg Jr., Sydney J.: Armed Robots: US Lags Rhetoric, Russia. *Breaking Defense,* 2017. október 18. Online: https://breakingdefense.com/2017/10/armed-robots-us-lags-rhetoric-russia/

Hoffmann, Jörg: Simulated Penetration Testing: From "Dijkstra" to "Turing Test++". In *Proceedings of the International Conference on Automated Planning and Scheduling (ICAPS).* 25. (2015), 1. 364–372. Online: https://doi.org/10.1609/icaps.v25i1.13684

Kumar, Gulshan – Krishan Kumar – Monika Sachdeva: The Use of Artificial Intelligence Based Techniques for Intrusion Detection: A Review. *Artificial Intelligence Review,* 34. (2010), 4. 369–387. Online: https://doi.org/10.1007/s10462-010-9179-5

Losev, Aleksandr: Voennii Iskusstvenii Intellekt ['Military Artificial Intelligence']. *Arsenal Otechestva,* 6. (2018), 32. 12–21.

Mascaro Steven – Ann E. Nicholso – Kevin B. Korb: Anomaly Detection in Vessel Tracks Using Bayesian Networks. *International Journal of Approximate Reasoning,* 55. (2014), 1. 84–98. Online: https://doi.org/10.1016/j.ijar.2013.03.012

Polyakova, Alina: Weapons of the Weak: Russian and AI-Driven Asymmetric Warfare. *Brookings Institution,* 2018. november 15. Online: www.brookings.edu/research/weapons-of-the-weak-russia-and-ai-driven-asymmetric-warfare/

Simonite, Tom: For Superpowers, Artificial Intelligence Fuels New Global Arms Race. *Wired,* 2017. szeptember 8. Online: www.wired.com/story/for-superpowers-artificial-intelligence-fuels-new-global-arms-race/

Sommer, Robin – Vern Paxson: Outside the Closed World: On Using Machine Learning for Network Intrusion Detection. In *2010 IEEE Symposium on Security and Privacy (SP).* IEEE, 2010. 305–316. Online: https://doi.org/10.1109/SP.2010.25

Svenmarck, Peter – Linus Luotsinen – Mattias Nilsson – Johan Schubert: Possibilities and Challenges for Artificial Intelligence in Military Applications. In *Proceedings of the 2018 NATO Big Data and Artificial Intelligence for Military Decision Making Specialists' Meeting. 2018.* 1–16.

Tekhnologii "Sudnogo Dnya": Vooruzhennyye Sily Rossii Vnedryayut Iskusstvennyy Intellekt' ['Doomsday Technologies': Russia's Armed Forces Introduce Artificial Intelligence'], *Yandex,* 2018. március 16. Online: https://bit.ly/3slQkU6

Thomas, Timothy: Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts. *Journal of Slavic Military Studies,* 27. (2014), 1. 101–130. Online: https://doi.org/10.1080/13518046.2014.874845

Thornton, Rod – Marina Miron: Towards the 'Third Revolution in Military Affairs'. The Russian Military's Use of AI-Enabled Cyber Warfare. *The RUSI Journal,* 165. (2020), 3. 12–21. Online: https://doi.org/10.1080/03071847.2020.1765514

Tucker, Patrick: Russia Says It Will Field a Robot Tank that Outperforms Humans. *Defense One,* 2017. november 8. Online: www.defenseone.com/technology/2017/11/russia-robot-tank-outperforms-humans/142376/

Vooruzhennyye Sily RF Vnedryayut Tekhnologii Iskusstvennogo Intellekta. *Voenniye Materialy,* 2018. március 15. Online: https://warfiles.ru/176763-vooruzhennye-sily-rf-vnedryayut-tehnologii-iskusstvennogo-intellekta.html

Williams, David P.: Underwater Target Classification in Synthetic Aperture Sonar Imagery Using Deep Convolutional Neural Networks. In *Pattern Recognition (ICPR), 2016 23rd International Conference,* Cancún, 2016. 2498–2503. Online: https://doi.org/10.1109/ICPR.2016.7900011