ON THE DIGITAL THRESHOLD: NATO'S RESPONSE TO MODERN SECURITY POLICY CHALLENGES

A DIGITÁLIS KÜSZÖBÖN: A NATO VÁLASZA A MODERN BIZTONSÁGPOLITIKAI KIHÍVÁSOKRA

PÁL ANITA[1]

Abstract

The article presents NATO's responses to modern security policy challenges by reviewing the historical background from Cold War military research to the transformation of global society, and then analyzes in detail NATO's cyber defense strategies and the development of AI integration, taking into account ethical and legal issues. It highlights significant cases and examples from the field of cyber defense, as well as the benefits and risks of AI integration in defense strategies. AI integration adds a new dimension to defense strategies, but also raises many ethical and legal concerns, such as automated decision-making. Linking the societal impact of technological innovations with security policy is critical for NATO to understand and address modern challenges. Finally, we link the social impacts of technological innovations with security policy to get a comprehensive picture of NATO's responses to modern challenges.

Keywords

NATO, cyber security, information warfare, artificial intelligence, security policy

Absztrakt

A cikk bemutatja a NATO válaszait a modern biztonságpolitikai kihívásokra, azáltal, hogy áttekinti a hidegháború katonai kutatásaitól kezdve a globális társadalom átalakulásáig terjedő történelmi hátteret, majd részletesen elemzi a NATO kibervédelmi stratégiáit és az AI integrációjának fejlődését, figyelembe véve az etikai és jogi kérdéseket. Jelentős eseteket és példákat emel ki a kibervédelem területéről, valamint az AI integráció előnyeit és kockázatait a védelmi stratégiákban. Az AI integráció új dimenziót ad a védelmi stratégiáknak, ugyanakkor számos etikai és jogi aggályt is felvet, például az automatizált döntéshozatalt illetően. A technológiai innovációk társadalmi hatásainak összekapcsolása a biztonságpolitikával kritikus fontosságú a NATO számára a modern kihívások megértése és kezelése szempontjából. Végül összekapcsoljuk a technológiai innovációk társadalmi hatásait a biztonságpolitikával, hogy átfogó képet kapjunk a NATO válaszairól a modern kihívásokra.

Kulcsszavak

NATO, kiberbiztonság, információs hadviselés, mesterséges intelligencia, biztonságpolitika

[1] pal.anita@phd.uni-obuda.hu | ORCID: 0000-0003-4750-193X | PhD Candidate at the Doctoral School for Safety and Security Sciences Óbuda University | Doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

A DIGITÁLIS KÜSZÖBÖN: A NATO VÁLASZA A MODERN BIZTONSÁGPOLITIKAI KIHÍVÁSOKRA

A modern világ biztonságpolitikai kihívásai között egyre nagyobb szerepet kapnak a kiberfenyegetések és a mesterséges intelligencia alkalmazása. Ezen technológiák rohamos fejlődése és integrációja a védelmi stratégiákba olyan új dimenziókat nyitnak, amelyekre a NATO-nak és tagállamainak egyaránt reagálniuk kell. A technológia és a geopolitikai viszonyok változásának üteme magával hozta a biztonságpolitikai paradigmák átalakulását is. A hidegháború vége óta eltelt évtizedek során a katonai szövetségek és védelmi stratégiák egyre inkább az információs technológiák köré szerveződtek, kiemelve az innováció és a hálózatépítés fontosságát.

A kibervédelem és a mesterséges intelligencia kérdésköre nem csupán technikai vagy technológiai kihívásokat jelent, hanem etikai, jogi és politikai dilemmákat is magában foglal. Ezek a technológiák új lehetőségeket és veszélyeket hoznak magukkal, amelyek megértése és kezelése elengedhetetlen a modern kori biztonságpolitikai stratégiák szempontjából. Az információs társadalom és a transznacionális kereskedelem kibontakozása globális szintű összekapcsolódást eredményezett, amely meghatározó befolyást gyakorol a nemzetközi kapcsolatokra és a biztonsági politikákra.

A NATO mesterséges intelligencia stratégiájában a szövetségesek és a NATO kötelezettséget vállaltak amellett, hogy biztosítják, hogy az általuk kifejlesztett és bevetésre szánt mesterséges intelligencia-alkalmazások megfeleljenek a Felelős Felhasználás hat Alapelvének: törvényesség; felelősség és elszámoltathatóság; magyarázhatóság és nyomon követhetőség; megbízhatóság; kormányozhatóság; és az elfogultság mérséklése. Ez a felelős megközelítés biztosítja, hogy a mesterséges intelligencia alkalmazása összhangban legyen a nemzetközi jogi normákkal és támogassa a NATO kollektív védelmi és biztonsági céljait, miközben felkészül a kihívásokra és a technológiai változásokra a biztonságpolitikai környezetben.[1]

Ebben a kontextusban a NATO szerepe és reakciói kulcsfontosságúak. A szövetség a hidegháború óta jelentős változásokon ment keresztül, amelyek középpontjában a technológiai adaptáció és a kiberbiztonság erősítése állt. A NATO-nak mint intézménynek szembe kell néznie a kibervédelem új kihívásaival, beleértve a szövetséges országok közötti koordináció javítását, a kiberfenyegetésekkel szembeni védekezési képesség fokozását, valamint a mesterséges intelligencia etikai és jogi kereteinek kidolgozását.

A cikkben részletesen akartam tárgyalni a hidegháború óta eltelt időszak katonai kutatásait, a globalizáció hatásait, a NATO kibervédelmi stratégiáinak evolúcióját, valamint a mesterséges intelligencia integrálását a biztonságpolitikába. Mindezek mellett kitérünk az interdiszciplináris megközelítések fontosságára is, amelyek ötvözik a technológiai, társadalomtudományi és biztonságpolitikai elemzéseket. A cikk célja, hogy átfogó képet nyújtson arról, hogyan alakítják és formálják ezek a tényezők a modern világ biztonságpolitikai döntéseit, és milyen kihívásokkal és lehetőségekkel kell szembenézniük a jövőben a NATO és tagállamai számára, valamint, hogy mik azok a történelmi, technológiai és politikai dimenziók, amelyek meghatározóak a NATO jelenlegi és jövőbeli biztonságpolitikai szerepvállalása szempontjából.

A HIDEGHÁBORÚ ÉS A KATONAI KUTATÁSOK KEZDETEI

Az időszak, melyet a hidegháború határozott meg, az Amerikai Egyesült Államok és a Szovjetunió közötti geopolitikai, ideológiai és katonai feszültségekről szólt. Ez a korszak 1945-től, a második világháború lezárásától egészen 1991-ig tartott, amikor is a Szovjetunió felbomlásával véget ért ez a globális vetélkedés. A két szuperhatalom és szövetségeseik a katonai technológiák, különösen az atomfegyverek és hosszú távú ballisztikus rakéták fejlesztésére összpontosítottak, amelyek meghatározták a katonai egyensúlyt és az elrettentés politikáját.

A katonai fejlesztések ezen felül magukban foglalták a légi és űrkutatásokat is. Az űrverseny kulcsfontosságú állomásai voltak a 1957-ben felbocsátott Szputnyik műhold és az 1969-es Apollo 11 holdra szállás, amelyek döntő mérföldköveket jelentettek a hidegháború idején. Ezek a technológiák nemcsak katonai szempontból voltak jelentősek, hanem számottevő hatást gyakoroltak a civil technológiákra és az ipari fejlődésre is. Mi sem példázza jobban az akkori kutatásfejlesztések fontosságát, mint az a tény, hogy napjainkra bekrült a kibertér is a NATO 5. műveleti területei közé, amelyre kiterjesztette az 5. cikkelyének vonatkozásait is.

A katonai kutatásokon túl, a számítástechnika és a kriptográfia fejlődése is előtérbe került, ami alapjaiban formálta át a hírszerzést, a katonai kommunikációt és a kiberháború kezdeti lépéseit. Az elektronikus hadviselés és a kiberbiztonság kérdései a hidegháború idején váltak kiemelt fontosságúvá, és napjainkban is kulcsfontosságú elemei a nemzetbiztonsági stratégiáknak.[2]

A biztonságpolitikai környezet átalakulása drasztikusan csökkentette a katonai tényezők szerepét. A hagyományos államok közötti háború kitörésének veszélye a közeljövőben minimálisra csökkent, bár a katonai konfliktusok és regionális válságok továbbra is jelentős kockázatot jelentettek az euroatlanti régió számára. A közép- és kelet-európai politikai rendszerváltozásokkal a hidegháborús korszak kétoldalú politikai és katonai ellentéteken alapuló rendszere, valamint annak ideológiai alapjai is megszűntek. Ezt a viszonylag stabil, bár magas katonai kockázatokkal járó helyzetet váltotta fel a politikai, gazdasági és társadalmi átalakulások által kiváltott új és régi feszültségek okozta instabilitás.[3] Ebben a megváltozott biztonságpolitikai környezetben új kockázati tényezők is megjelentek. A nem katonai jellegű kihívások - mint a terrorizmus, a tömeges migráció, a tömegpusztító fegyverek terjedése, és a nemzetközi bűnözés - súlya megnőtt, így annak következményei kihatottak mind a katonai, mind a polgári biztonságra egyaránt. A globalizáció jelensége azt eredményezte, hogy a korábban távolinak tűnő nemzetközi feszültségek mára közvetlenül megrengethetik az egyén biztonságról alkotott képét.[4]

A GLOBALIZÁCIÓ ÉS AZ INFORMÁCIÓS TÁRSADALOM KIALAKULÁSA

A hidegháború vége után a világ hatalmas léptékkel transzformálódott a globalizáció kényelme felé, ami egyszerre hozott előnyöket és kihívásokat a világgazdaságnak, politikának és kultúrának. A globalizáció ezen korszakában központi szerepet kapott az információs technológia, különösen az internet és a kommunikációs eszközök gyors fejlődése. Az 1990-es évek elején az internet kereskedelmi felhasználásának liberalizálása új dimen-

ziókat nyitott meg az információs társadalom előtt, lehetővé téve az információ és a kommunikáció korábban elképzelhetetlen mértékű áramlását, valamint a tér és az idő közötti korlátok megszűnését.

Az információs társadalom fejlődésével párhuzamosan növekedett a transznacionális kereskedelmi kapcsolatok és a gazdasági integráció fontossága. A nemzetközi üzleti tevékenységek és a globális ellátási láncok expanziója jelentős hatást gyakorolt a világgazdaságra, átformálva azokat a dinamikákat, amelyek korábban meghatározták a nemzetközi gazdasági rendszert. Ezek a változások nem csak gazdasági, hanem biztonságpolitikai következményekkel is jártak. Új típusú kihívások és fenyegetések jelentek meg, mint például a kibertámadások és az információs háborúk új formái, amelyek nemcsak új kockázati tényezőket hoztak a nemzetközi kapcsolatokban, de megváltoztatták az elrettentés politikájában és a szövetségi rendszerek egymáshoz való viszonyulásában és függőségi viszonyokat is.

A katonai és civil technológiák közötti együttműködés, valamint a kibertér és az információs infrastruktúrák védelme kiemelten fontossá vált. A NATO és más nemzetközi szervezetek számára ez azt jelentette, hogy újra kellett gondolniuk és adaptálniuk kellett védelmi stratégiáikat, hogy megfeleljenek az új, digitalizált világ kihívásainak. Az információs társadalom kialakulása így nem csak technológiai forradalmat jelentett, hanem mélyreható politikai és társadalmi változásokat is előidézett, amelyek ma is jelentősen befolyásolják a világ globális biztonságpolitikáját. [5]

Ez a folyamat alapvetően átalakította az államok közötti interakciókat, erősítve a nemzetek közötti függőségeket, miközben növelte azokat a lehetőségeket, amelyek révén a kisebb államok is részt vehetnek a globális piacon. Ugyanakkor a fokozott összekapcsolódás új sebezhetőségeket is teremtett, amelyek kezelése kulcsfontosságú a nemzetközi stabilitás fenntartása szempontjából. Az információs kor hajnalán a biztonságpolitikai tervezőknek és döntéshozóknak újra kell gondolniuk stratégiáikat, hogy képesek legyenek kezelni a digitalizált világ rendkívül összetett és gyorsan változó fenyegetéseit.[6]

A technológiai trendek jelentős változásokat hozhatnak, mivel a fejlett algoritmusok (például gépi tanulás) egyre jobban kihasználják a rengeteg digitális adatot (big data) emberihez hasonló viselkedés és tevékenységek (mesterséges intelligencia) létrehozására. A gépek sok feladatban hatékonyabbak lehetnek az embereknél, ami az interakciók exponenciális növekedéséhez vezethet. A vállalatok egyre inkább a szoftverekre és digitális tartalmakra támaszkodnak új termékek gyors fejlesztéséhez. Hasonlóképpen, az algoritmusok online vásárlási pontosságának javulása az online vásárlás dominanciájához vezethet, ahol a szoftverek autonóm módon szállítják a szükséges termékeket a vásárlók digitális nyilvántartásai alapján. Ezek a változások nagy hatással lesznek az üzleti tevékenységekre és a versenyre.[7]

A NATO KIBERVÉDELMI STRATÉGIÁINAK EVOLÚCIÓJA

Ahogy a digitális kor fejlődött, úgy vált egyre nyilvánvalóbbá, hogy a kiberfenyegetések jelentős kihívást jelentenek a nemzetek biztonságára. A NATO, mint transzatlanti katonai szövetség, kénytelen volt szembenézni azokkal a kihívásokkal, amelyek az információs kor hajnalán kezdődtek és napjainkra egyre összetettebbé váltak. Amint a tagállamok kormányzati, katonai és infrastrukturális rendszerei egyre inkább célpontjává váltak a

kibertámadásoknak, úgy vált maga a kibervédelem egyre kiemeltebb prioritássá a szövetség számára.

Az elmúlt évtizedekben a NATO számos lépést tett a kiberbiztonsági kapacitásának megerősítése érdekében. Ezen folyamat során több jelentős eset is bekövetkezett, amelyek rávilágítottak a kollektív védelem kiberdimenzióinak fontosságára. Például, 2007-ben Észtország ellen indított kibertámadás, amelyet állami szponzorált orosz hackereknek tulajdonítanak, széles körű zavart okozott az ország kormányzati, pénzügyi és hírközlési rendszereiben. Ez az eset katalizátorként szolgált a NATO számára, hogy felgyorsítsa saját kiberreakciós erőinek fejlesztését, és 2008-ban létrehozta a NATO Kiberbiztonsági Kiválósági Központját (CCDCOE) Tallinnban, amely a kibervédelmi kutatás és képzés központja lett.[8]

2021 novemberében Tallinn adott otthont a „Cyber Coalition 21" nevű hadgyakorlatnak, amely a NATO legnagyobb kibervédelmi eseménye, és világviszonylatban is kiemelkedő jelentőségű. célja a NATO és szövetséges országok kiberbiztonsági szakértőinek felkészültségének és együttműködési képességeinek tesztelése volt. A gyakorlaton 21 tagállam több mint 1000 szakértője vett részt, beleértve Svájc, Finnország, Írország és Svédország képviselőit is. A gyakorlat különféle válság-szcenáriókat tartalmazott, amelyek valós fenyegetéseket szimuláltak, mint például gázvezeték szolgáltatók elleni kiber- és információs támadások. Ezek a szcenáriók a valósághűségre és a geopolitikai realizmusra törekedtek, például a 2021 eleji amerikai Colonial Pipeline támadásra reagálva. A résztvevők nem versengtek egymással, hanem együttműködve oldották meg a feladatokat, fejlesztve a NATO-tagállamok közötti kooperációt és vészhelyzeti információcserét. A gyakorlat kiemelt figyelmet fordított a modern információs hadviselésre, beleértve a közösségi média platformokon végzett kognitív támadásokra való felkészülést.[9]

Az Adat- és Mesterséges Intelligencia Felülvizsgáló Testület (DARB-Data and Artificial Intelligence Review Board) a szövetségesek fórumaként és a NATO azon erőfeszítéseinek fókuszpontjaként szolgál, amelyek a mesterséges intelligencia felelős fejlesztésének és használatának szabályozására irányulnak. A DARB-on keresztül a szövetségesek és a NATO olyan felelől mesterséges intelligencia (RAI-Responsible AI) használatokon és gyakorlatokaon (fog csiszolni, amelyek megbízhatóbb, interoperábilis és biztonságosabb rendszereket biztosítanak, elősegítve minőségi előnyök elérését a stratégiai versenytársakkal és a potenciális ellenfelekkel szemben.[10]

A NATO válasza a kiberfenyegetésekre nem csupán technikai védekezésre korlátozódik. A szövetség a tagállamok közötti információmegosztást és együttműködést is ösztönzi, amely elengedhetetlen a gyorsan változó kiberfenyegetések hatékony kezeléséhez. Az intézkedések között szerepel a kiberháborús gyakorlatok rendszeres végrehajtása, a kiberbiztonsági politikák harmonizációja, valamint a kiberbűnözéssel szembeni fellépés koordinálása. Ezek a lépések biztosítják, hogy a NATO képes legyen védelmet nyújtani nem csak a hagyományos, hanem a digitális fenyegetésekkel szemben is.

A NATO folyamatosan fejleszti kiberbiztonsági stratégiáit, hogy megfeleljen a modern kihívásoknak, és védelmezze tagállamai digitális infrastruktúráit a növekvő kiberfenyegetésekkel szemben. A szervezet kiberbiztonsági politikája a tagállamok közötti együttműködésen és az új technológiák bevonásán alapul, ami kulcsfontosságú a kollektív biztonsági rendszer fenntartásához a 21. században. A NATO válasza a kiberfenyegetésekre így

nem csupán a jelenlegi veszélyekre ad választ, hanem a jövő kihívásaira is felkészül, biztosítva, hogy a szövetség tagjai közötti védelmi kötelék ellenálló maradjon a digitális korban.

A MESTERSÉGES INTELLIGENCIA A BIZTONSÁGPOLITIKÁBAN

A technológia gyors fejlődése három fő irányban halad előre. Először is, a processzorok teljesítménye olyan ütemben növekszik, hogy a következő években nagyobb számítási kapacitás lesz elérhető, mint eddig valaha. Másodszor, a szoftverek nem csak a világot hódítják meg, hanem alapvetően átalakítják a számítástechnika területét, különösen a mély neurális hálózatok fejlődésének köszönhetően. Harmadszor, a hordozható eszközök elterjedésével az elektronikus tartalom mennyisége 24 havonta megduplázódik, és a jelenlegi digitális adatok 90%-a az elmúlt két évben jött létre. Ez az exponenciális növekedés várhatóan a közeljövőben is folytatódni fog.[11]

Az elmúlt években a mesterséges intelligencia (MI) fejlődése átformálta a védelmi stratégiákat és újra értelmezte a biztonságpolitikai paradigmákat. A technológia előretörése jelentős hatással van a katonai műveletekre, a hírszerzésre és a kibervédelemre, megváltoztatva ezzel a nemzetek közötti erőviszonyokat és a globális biztonsági környezetet.

Az MI integrációjának kulcsfontosságú területei közé tartozik a hírszerzési tevékenységek optimalizálása, ahol az MI képes óriási adathalmazokat feldolgozni és értelmezni, lehetővé téve ezzel a gyorsabb és pontosabb döntéshozatalt. A kibervédelemben az MI alapú rendszerek előre láthatják és automatikusan reagálhatnak a fenyegetésekre, így növelve a hálózatok biztonságát és ellenálló képességét. Továbbá, a robotizált és autonóm hadviselési technológiák fejlesztése új dimenziókat nyit meg a harctéri műveletekben, amelyek potenciálisan minimalizálhatják az emberi veszteségeket.[12]

Az MI technológiai előnyei mellett azonban számos etikai és jogi kihívás is felmerül: a döntések átláthatósága, a felelősség kérdésköre, valamint a teljesen autonóm fegyverrendszerek használatának morális vetületei mind olyan témák, amelyek komoly vitákat váltanak ki a szakértők és a döntéshozók körében. A nemzetközi jogi szabályozások kialakítása és az etikai normák meghatározása lassan halad a gyors technológiai fejlődéshez képest, ami kihívásokat jelent a globális biztonság és alkalmazhatóság szempontjából.

A NATO mesterséges intelligencia stratégiájának keretein belül a szövetségesek és a NATO elkötelezték magukat amellett, hogy az általuk fejlesztett és alkalmazott mesterséges intelligencia rendszerek megfeleljenek a Felelős Felhasználás hat alapelvének (PRU-Principles of Responsible Use): törvényesség; felelősség és elszámoltathatóság; magyarázhatóság és nyomon követhetőség; megbízhatóság; kormányozhatóság; valamint az elfogultság csökkentése.[13]

2022-ben a NATO-szövetségesek további lépéseket tesznek a mesterséges intelligencia, az adatok, az autonómia és a digitális átalakítás felelős használatára. Az Igazgatóság első feladata egy felhasználóbarát felelős mesterséges intelligencia tanúsítási szabvány kidolgozása lesz, beleértve a minőség-ellenőrzést és a kockázatcsökkentést is, amely elősegíti az új mesterségesintelligencia- és adatprojektek összehangolását a NATO 2021 októberében jóváhagyott felelősségteljes felhasználási elveivel.[14]

A NATO Adat- és Mesterséges Intelligencia Felülvizsgáló Testülete (DARB) létrehozásának alapvető célja, hogy elősegítse a mesterséges intelligencia felelős fejlesztését

és alkalmazását a védelmi szektorban. A DARB központi szerepet tölt be a bizalom építésében a nyilvánosság, az innovátorok és a végfelhasználók között, miközben irányítást biztosít a felelős védelmi innovációkhoz a nemzetközi normák és jogi előírások szerint. A testület fontos szerepet játszik abban, hogy a mesterséges intelligencia alkalmazásait a NATO és a szövetséges államok számára elfogadható, megbízható és interoperábilis módon alakítsa át, csökkentve a kockázatokat és ellenőrizve a minőséget. A DARB fórumként is szolgál, ahol a szövetségesek megoszthatják a legjobb gyakorlatokat és véleményeket cserélhetnek, ezzel támogatva a kollektív védelmi erőfeszítéseket. A testület munkája eredményeként a NATO és tagállamok gyakorlati mesterséges intelligencia eszközkészleteket dolgoznak ki, melyek a NATO és a szövetségesek számára is elérhetők. Ezek az eszközök és eljárások a tapasztalatokra, a NATO érdekelt felei által adott bemenetekre és a nemzetközi gyakorlatokra épülnek, beleértve a köz-, magán-, akadémiai szektort és a civil társadalmat is. A testület agilis módon irányítja a mesterséges intelligencia megvalósítását a NATO-n belül, alkalmazkodva a változó körülményekhez és technológiai fejlődéshez. Célja, hogy támogassa a szövetségeseket a mesterséges intelligencia eszközkészletek nemzeti szintű használatában és a felelős tervezési gyakorlatok alkalmazásában, erősítve a NATO kollektív védelmi képességeit a stratégiai versenytársakkal és potenciális ellenfelekkel szemben.[15]

A MESTERSÉGES INTELLIGENCIA A VÉDELMI STRATÉGIÁKBAN

A mesterséges intelligencia integrációja a védelmi stratégiákba az elmúlt évtizedek egyik legmeghatározóbb technológiai fejlődése. Az MI alkalmazása a katonai és biztonságpolitikai területeken számos új lehetőséget nyitott meg, így a hírszerzési tevékenységek hatékonyságának növelésétől kezdve a kibervédelmi rendszerek fejlesztésén át a robotizált hadviselésig. Az MI lehetővé teszi, hogy a védelmi rendszerek gyorsabban és pontosabban reagáljanak a fenyegetésekre, miközben csökkenthetik az emberi tényezőből adódó hibák és az azokból adódó késedelmek számát. Ezekben az eszközökben és műveletekben mindig is fontos szerepet játszott a nyílt forrású információszerzés (OSINT), amely az internet elterjedésével és a világhálón tárolt adatok feldolgozásával jelentős mértékben átvette a hagyományos emberi hírszerzés (HUMINT) szerepét. Az MI alkalmazása az OSINT-ben növeli az információszerzés sebességét és hatékonyságát, legyen szó szövegbányászatról, képfelismerésről vagy összefüggések elemzéséről.[16]

A mesterséges intelligencia integrációja a hírszerzési műveletekbe forradalmasította a modern hadviselést és biztonságpolitikát. Az MI képessége, hogy hatalmas adatmennyiségeket dolgozzon fel és elemezzen gyorsasággal és pontossággal, lehetővé teszi a hírszerző szervezetek számára, hogy az eddiginél sokkal hatékonyabban azonosítsák és értékeljék a fenyegetéseket. Ez a technológia kritikus döntéshozatali támogatást nyújt a biztonsági erőknek, lehetővé téve számukra, hogy gyorsan reagáljanak és megfelelő intézkedéseket hozzanak.[17]

Az MI a hírszerzés terén elsősorban képfelismerésre, nyelvi feldolgozásra és viselkedési minták elemzésére használható. Például, a drónok és műholdak által gyűjtött képi adatokat MI algoritmusok elemzik, azonosítva a fontos objektumokat és mozgásokat olyan helyzetekben, ahol az emberi elemzőknek napokba telne a feldolgozás. Az MI segítségével a hírszerzés képes lépést tartani a folyamatosan változó és fejlődő kibertérrel, ahol a fenyegetések gyorsan változhatnak és evolválódhatnak.[18]

A hírszerzési MI alkalmazásai közé tartozik a szociális média és nyílt források monitorizálása is, ahol az algoritmusok képesek felismerni a különleges eseményeket, hangulati változásokat vagy radikalizálódási jeleket. Ezen technológiák integrációja lehetővé teszi a döntéshozók számára, hogy jobban megértsék a globális politikai és társadalmi trendeket, és előre lássák a potenciális zavarokat vagy konfliktusokat.

Ezek az MI alkalmazások tehát alapvetően növelik a hírszerzési képességeket, miközben új kérdéseket vetnek fel a magánélet védelmével és az adatkezeléssel kapcsolatban. Az AI által vezérelt hírszerzés hozzájárul a nemzetbiztonsági célkitűzések hatékonyabb eléréséhez, miközben biztosítja a gyors és alapos adatelemzést, amely elengedhetetlen a modern biztonsági kihívások kezelésében.

A MESTERSÉGES INTELLIGENCIA SZEREPE A KIBERFENYEGETÉSEK KEZELÉSÉBEN

A mesterséges intelligencia (MI) alapvető szerepet játszik a kiberfenyegetések azonosításában és kezelésében, mivel az AI technológiák képesek a hálózati forgalom mintáinak folyamatos elemzésére és a rendellenes viselkedés azonosítására. Az MI rendszerek gyorsan reagálnak a potenciális biztonsági incidensekre, automatizált védelmi protokollokat aktiválva, amelyek azonnali lépéseket tesznek lehetővé a fenyegetések elhárítására, még mielőtt azok kárt okoznának.

Az MI segítségével a kibervédelmi rendszerek képesek adaptálni és tanulni a különféle támadási technikákból, így növelve a védelmi stratégiák hatékonyságát az idő előrehaladtával. Az incidensreagálási stratégiák automatizálása, mint például a sebezhetőségek gyors javítása vagy a támadási vektorok elszigetelése, kulcsfontosságúak az információs infrastruktúrák védelmében. Az mesterséges intelligencia tehát nélkülözhetetlen eszközzé vált a kiberbiztonsági szakértők számára, amelyek íly módon képesek lépést tartani a folyamatosan változó kiberfenyegetésekkel és proaktívan védekezni ellenük.[19]

Automatizált harci rendszerek: Autonóm fegyverek és járművek

Az MI integrációja a védelmi stratégiákba kiterjed az automatizált harci rendszerekre is, amelyek középpontjában az autonóm fegyverek és járművek állnak. Ezek a rendszerek képesek önállóan döntéseket hozni és végrehajtani különböző műveleteket emberi beavatkozás nélkül, bonyolult és veszélyes környezetben is. Az MI által vezérelt döntéshozatal lehetővé teszi a harci műveletek gyorsaságának és hatékonyságának növelését, miközben csökkenti a katonák életveszélyes helyzetekben való kitettségét.

Autonóm rendszerek alkalmazása jelentős előnyöket kínál, mint például a reakcióidő drasztikus csökkentését és a műveletek precizitásának növelését. Az MI képes „real-time" adatok alapján elemzéseket végezni, így optimalizálva a célzási és támadási protokollokat. Emellett, az autonóm járművek, mint drónok és robotizált földi járművek, képesek felderítő és megfigyelő feladatokat ellátni, kritikus információkat szolgáltatva a döntéshozóknak.[20]

Azonban ezeknek a technológiáknak a bevezetése komoly etikai kérdéseket is felvet. Az AI által vezérelt döntéshozatal, különösen a harci környezetben, számos aggodalmat generál a felelősség és az elszámoltathatóság terén. Ezért fontos, hogy a fejlesztés és alkal-

mazás során szigorú etikai keretek között mozogjunk, biztosítva, hogy az autonóm rendszerek használata összhangban legyen a nemzetközi jogi előírásokkal és humanitárius normákkal.

Etikai és jogi kihívások

Bár az MI technológia jelentős előnyöket kínál a védelmi stratégiákban, számos etikai és jogi kérdést is felvet. Ezek között a legfontosabbak:

- A mesterséges intelligencia védelmi alkalmazása etikai és jogi dilemmákat vet fel, amelyek kezelése elengedhetetlen a technológia felelős integrálásához a katonai stratégiákba. Az MI vezérelte *döntéshozatali folyamatok átláthatóságának kérdése* kulcsfontosságú, mivel az ilyen rendszerek gyakran zárt, nehezen érthető algoritmusokon alapulnak. A "fekete doboz" jelenség, amely az MI által hozott döntések mögötti logikát homályban hagyja, komoly kihívásokat jelent a biztonságpolitika számára. A védelmi döntéshozóknak és a hadseregnek meg kell birkózniuk azzal a tényezővel, hogy hogyan biztosítható az elszámoltathatóság, amikor az MI részt vesz a kritikus döntések meghozatalában. A modern háborúkban alkalmazott MI technológiák növelik a hadműveletek hatékonyságát, de ezeknek a rendszereknek a döntései mögötti logika megértése és ellenőrzése létfontosságú marad.[20]
- Az autonóm fegyverrendszerek etikai vetületei további aggodalmakat vetnek fel. Amikor a gépek képesek önállóan dönteni élet és halál kérdéseiről, felmerül a kérdés, hogy vajon a technológia felelősségteljesen használható-e. A nemzetközi közösség már évek óta küzd azzal, hogy meghatározza azokat a kereteket, amelyek között az autonóm fegyverek bevetése elfogadható lenne. Ezek a viták gyakran az emberi felügyelet szükségességére koncentrálnak, ahol a döntő kérdés, hogy *az MI által hozott döntések mekkora mértékben igényelnek emberi beavatkozást vagy ellenőrzést*. A nemzetközi jogi normák és a hadviselésre vonatkozó etikai előírások nehezen tartják lépést a technológia fejlődésével, ami késlelteti az egyértelmű szabályozások kialakulását.[21]
- Végül, a *szabályozás és felügyelet kérdésköre* is elengedhetetlen a biztonságpolitikai szempontból releváns MI alkalmazások esetében. A nemzeti és nemzetközi szabályozó testületeknek folyamatosan értékelniük kell az MI technológiák fejlődését, hogy megfelelő kereteket állíthassanak fel az etikus használathoz. A katonai MI alkalmazások szigorú felügyelete kulcsfontosságú a biztonságos és felelős technológiai integráció érdekében. Az ilyen rendszerek bevezetésével járó kockázatok kezelése érdekében szükséges egy átfogó jogi és etikai infrastruktúra kiépítése, amely képes alkalmazkodni a gyors technológiai változásokhoz és azok új kihívásaihoz.[22]

Ezek a kérdések alapvető jelentőséggel bírnak a modern biztonságpolitikai döntéshozatalban, és létfontosságúak a mesterséges intelligencia katonai alkalmazásainak jövőjére nézve. Az átláthatóság, az etikai felelősség és a hatékony szabályozás kulcsfontosságúak az MI technológiák biztonságos és felelős használatának biztosításához.

Ezen kihívások kezelése érdekében szükség van a nemzetközi jogi keretek továbbfejlesztésére és a nemzetközi együttműködés erősítésére. A NATO és az ENSZ együttműködése például kritikus a kibervédelem és az információs biztonság területén, mivel ezek a területek közvetlenül érintik a tagállamok nemzeti biztonságát és a nemzetközi stabilitást

vagy akár az autonóm döntéshozatal kérdéskörét. Ezen kihívások kezelése érdekében szükség van a nemzetközi jogi keretek továbbfejlesztésére és a nemzetközi együttműködés erősítésére.

A mesterséges intelligencia integrációja a védelmi stratégiákba tehát nem csupán technológiai, hanem etikai, jogi és politikai dimenziókat is magában foglal. A felelős MI alkalmazás biztosítása érdekében a nemzetközi közösségnek együtt kell működnie a technológiai fejlődés és az emberi jogok tiszteletben tartása közötti egyensúly megteremtése érdekében.

Interdiszciplináris Perspektívák

A modern katonai stratégiák és biztonságpolitikai intézkedések megértése egyre inkább igényli az interdiszciplináris megközelítést, amely ötvözi a technológiai, társadalmi, és politikai elemzéseket. A mesterséges intelligencia terjedése és annak integrációja a védelmi rendszerekbe olyan komplex kihívásokat vet fel, amelyek kezelése különböző tudományágak együttműködését igényli. Az MI hatása a biztonságpolitikára nem korlátozódik pusztán a technológiai fejlődésre; széleskörű társadalmi és etikai kérdéseket is felvet, beleértve a munkaerőpiacra, a jogi szabályozásra és a nemzetközi kapcsolatokra gyakorolt hatásokat.[23]

A technológiai fejlődés által indukált társadalmi változások megértése érdekében a biztonságpolitikai elemzéseknek széleskörűen kell vizsgálniuk a társadalomtudományi összefüggéseket. Az MI, mint a kiberhadviselés és hírszerzés eszköze, új kérdéseket vet fel az információs háborúk etikájáról és a kibertér nemzetközi szabályozásáról.

Az interdiszciplináris perspektívák fontosságát jól mutatja, hogy a technológiai innovációk hogyan alakították és alakítják a társadalmi struktúrákat, különösen a biztonságpolitika területén. A mesterséges intelligencia fejlődése például jelentős hatással van a munkaerőpiacra, a magánélet védelmére és az állampolgári jogokra, amelyek mind a társadalmi szerkezet alapvető elemei. Az MI alkalmazása a katonai technológiákban, mint amilyeneket a NATO használ, új kihívásokat és lehetőségeket teremt, amelyek a hagyományos védelmi stratégiákon túlmutatnak. A robotizált harci rendszerek és a hírszerzési technológiák fejlődése, melyek az MI-t integrálják, nem csupán a hadviselés módját változtatják meg, hanem a nemzetek közötti diplomáciai és társadalmi dinamikákat is befolyásolják. [24]

Az interdiszciplináris megközelítések tehát nem csupán a technológiai fejlesztések és azok társadalmi hatásainak megértését segítik, hanem a nemzetközi jogi és etikai keretek megszilárdítását is elősegítik a biztonságpolitika területén. Az MI hatása a biztonságpolitikára és a társadalomra kiterjedő tanulmányozása nélkülözhetetlen a felelős és fenntartható technológiai integráció szempontjából.

ÖSSZEGZÉS

Az informatika vívmányai egyre inkább átszőtték a mindennapjainkat, valamint a katonai rendszereket is. A katonai irányítórendszerek és az intelligens fegyverek hálózatba kapcsolódva fognak hosszú távon működni, ami kétélű fegyver, hiszen ezáltal egy sor biztonsági kockázatnak vannak kitéve. Fel kell készülnünk arra, hogy a jövő konfliktusaiban az ellenséges országok egyre nagyobb hangsúlyt helyeznek majd nem csak a katonai, hanem polgári használatban lévő hálózatok, elektronikus információs rendszerek és kritikus infra-

struktúrák támadásaira. Jelentős hátrányba kerülhetnek azok az országok, amelyek nem fejlesztik ki a védekezésre való a képességeiket, mivel önmagában csak a kibervédelem nem biztos, hogy elegendő lesz egy konfliktus során.

A jelenlegi technológiai korszak jelentős kihívásokkal szembesíti a NATO-t, amelynek kulcsszerepe van a kollektív védelemben és a tagállamok biztonságának fenntartásában. Ahogy a mesterséges intelligencia és egyéb digitális technológiák egyre inkább részévé válnak a katonai stratégiáknak és műveleteknek, úgy a NATO-nak adaptálnia kell a hagyományos védelmi megközelítéseit, hogy kezelni tudja a kibertér által előidézett új fenyegetéseket és kihívásokat. Az MI alkalmazása a hírszerzésben, kibervédelemben és robotizált harci rendszerekben lehetőséget nyújt a NATO-nak, hogy növelje a hatékonyságát és a reakcióképességét. Ugyanakkor ezek a fejlesztések komoly etikai és jogi kérdéseket is felvetnek, különösen az autonóm fegyverrendszerek és a döntéshozatali folyamatok átláthatósága terén.

A technológiai innovációk gyors üteme komoly kihívást jelent a jelenlegi nemzetközi jogi keretek számára. A NATO-nak és tagállamainak folyamatosan értékelniük kell az új technológiák biztonságpolitikai következményeit, és aktívan részt kell venniük a nemzetközi szabályozási folyamatokban. Az MI és más fejlett technológiák katonai alkalmazásának szabályozása alapvető fontosságú a nemzetközi béke és biztonság fenntartása érdekében. A hatékony szabályozási keretek kialakításához elengedhetetlen a nemzetközi együttműködés, különösen az ENSZ és más regionális szervezetek bevonása.

A jövőbeli kutatások irányai közé tartozik az MI technológiák biztonsági alkalmazásainak részletesebb elemzése, a kibervédelem erősítése és az információbiztonság javítása. Emellett szükséges a technológiai fejlesztések társadalmi és etikai hatásainak folyamatos figyelemmel kísérése a felelős használat biztosítása érdekében. A nemzetközi együttműködés erősítése és a globális biztonsági kihívásokra adott közös válaszok kidolgozása kulcsfontosságú cél kell hogy legyen a jövőben. A katonai és civil szektorok közötti együttműködés, valamint az interdiszciplináris kutatások támogatása segíthet a komplex biztonsági problémák hatékonyabb kezelésében.

Összegzésül, a NATO-nak és a nemzetközi közösségnek alkalmazkodnia kell a gyorsan változó technológiai környezethez. A folyamatos innováció és a nemzetközi együttműködés támogatása, valamint a jogi és etikai keretek erősítése elengedhetetlen a jövőbeli biztonsági kihívások kezelésében. A technológiai fejlődés lehetőséget nyújt a védelmi képességek javítására, ugyanakkor szükség van a kritikus infrastruktúrák védelmének és a társadalmi stabilitás megőrzésének biztosítására. A NATO és a tagállamok feladata, hogy a technológiai fejlődést a biztonság és stabilitás növelésére használják, miközben tiszteletben tartják az etikai és jogi normákat.

FELHASZNÁLT IRODALOM

[1] https://www.nato.int/cps/en/natohq/opinions_224836.htm?selectedLocale=en
[2] D. Shree,. A Review on Cryptography, Attacks and Cyber Security. International Journal of Advanced Research in Computer Science, 2017, Vol 8, Issue 5, pp. 239, ISSN: 0976-5697
[3] Z. Martinusz, Felelősség és lehetőség, MHTT XI. évfolyam 1. szám https://www.mhtt.eu/hadtudomany/1999/ht-1999-1-1.html

[4] C. Kollár and B. Z. Vinárné, “Terrorism and the information security of media content with special regard to ISIS, the Balkans and Russia,” *SOCIOECONOMIC CHALLENGES*, vol. 1, no. 1, pp. 13–19, 2017.
[5] C. Kollár, “A mesterséges intelligencia és a kapcsolódó technológiák bemutatása a biztonságtudomány fókuszában,” in *Kiberbiztonság – Cybersecurity 2.*, vol. 2, 2019, pp. 47–61.
[6] M. Barsy: A digitális gazdaságról, In: Pintér István (szerk.) Műhelymunkák: A virtuális tér geopolitikája. 367 p. Budapest: Geopolitikai Tanács Közhasznú Alapítvány, 2016. pp. 131-142. (ISBN:978-963-9816-34-3) http://mek.oszk.hu/16100/16182/16182.pdf
[7] H. J. Wilson, P. Daugherty: Human and machine: Reimagining work in the age of AI., Harvard Business Review Press 2018, https://hbsp.harvard.edu/product/10163-PDF-ENG
[8] L. Kovács: Cyber security policy and strategy in the European Union and NATO. *Land Forces Academy Review*, 2018, Vol. XXIII, No 1(89), 2018, pp. 16-24., DOI: https://doi.org/10.2478/raft-2018-0002
[9] G. Nyári: Kiber koalíció 21 – a NATO legfontosabb éves kibervédelmi hadgyakorlatát rendezték meg Észtországban, E-Gov hírlevél, Közigazgatás és Informatika 2021. https://hirlevel.egov.hu/2021/12/13/kiber-koalicio-21-a-nato-legfontosabb-eves-kibervedelmi-hadgyakorlatat-rendeztek-meg-esztorszagban/
[10] https://www.nato.int/cps/en/natohq/official_texts_208374.htm?selectedLocale=en
[11] D. Ryding, J. Reinsel, J. Gantz: The digitization of the world from edge to core. *Framingham: International Data Corporation*, 2018, 16: pp. 1-28., https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-data-age-whitepaper.pdf
[12] I. Szabadföldi. "A mesterséges intelligenciával támogatott nyílt információszerzés (OSINT): evolúció és kihívások." *Nemzetbiztonsági Szemle* 10.1 (2022), pp. 30-51., https://folyoirat.ludovika.hu/index.php/nbsz/article/view/5953
[13] https://www.nato.int/cps/en/natohq/official_texts_208374.htm?selectedLocale=en
[14] https://www.nato.int/cps/en/natohq/news_208342.htmkiber
[15] https://www.nato.int/cps/en/natohq/official_texts_221777.htm?selectedLocale=en
[16] I. Szabadföldi. "A mesterséges intelligenciával támogatott nyílt információszerzés (OSINT):–evolúció és kihívások." *Nemzetbiztonsági Szemle* 10.1 (2022), pp. 30-51. https://folyoirat.ludovika.hu/index.php/nbsz/article/view/5953/4997
[17] G. Berki: Kiberháborúk, kiberkonfliktusok, In: Pintér István (szerk.) Műhelymunkák: A virtuális tér geopolitikája. 367 p. Budapest: Geopolitikai Tanács Közhasznú Alapítvány, 2016. pp. 246-282. (ISBN:978-963-9816-34-3) http://mek.oszk.hu/16100/16182/16182.pdf
[18] J. Carroll: OSINT Analysis using Adaptive Resonance Theory for Counterterror-ism Warnings, *Artificial Intelligence and Applications*, Innsbruck, 2005., pp. 756–760.
[19] T. Kőkuti, "Társadalmi hatások és MI!", 2022, pp. 312-324.
[20] A. Németh: "A katonai alkalmazású autonóm terepjáró járművek fejlesztésének egyes kérdései I. rész." *HADITECHNIKA* 53.4 (2019), pp. 11-16.

[21] P. Scharre, *Army of none: Autonomous weapons and the future of war, Future Weapons*. WW Norton & Company, 2018. pp. 34, ISBN-szám:9780393608991, 0393608999

[22] F. Mező, "A mesterséges intelligencia téma megjelenése a „Tanulás és Társadalom" Interdiszciplináris Nemzetközi Konferencián - The Appearance of the Topic of Artificial Intelligence in the" Learning And Society" Interdisciplinary International Conference." *MESTERSÉGES INTELLIGENCIA: INTERDISZCIPLINÁRIS E-FOLYÓIRAT* 4.2 (2022): pp. 89-107., https://real.mtak.hu/155963/1/MI_2022_2_089_Mezo.pdf

[23] K. Mező, Zs. Mándy. "BESZÁMOLÓ A 4. NEMZETKÖZI INTERDISZCIPLINÁRIS KONFERENCIÁRÓL." *Különleges Bánásmód-Interdiszciplináris folyóirat* 5.2 (2019), pp. 71-81.

[24] H. Harlow, Ethical concerns of artificial intelligence, big data and data analytics, *European conference on knowledge management*. Academic Conferences International Limited, 2018. pp. 316. Ethical Concerns of Artificial Intelligence, Big Data and Data Analytics - ProQuest