HADMÉRNÖK
VÉDELEMINFORMATIKA

20. évfolyam (2025) 1. szám 105–119.
DOI: 10.32567/hm.2025.1.6

Hankó Viktória[1]

Mesterséges intelligencia alkalmazása a kiberműveletekben

The Use of Artificial Intelligence in Cyber Operations

Absztrakt

A tanulmány a mesterséges intelligencia (MI) kiberbiztonsági alkalmazásait vizsgálja, kiemelve annak szerepét a modern kiberműveletekben. Az MI-technológiák lehetővé teszik a fenyegetések gyors azonosítását, az incidenskezelés hatékonyságának növelését és a védelmi folyamatok automatizálását. Az offenzív alkalmazások között megjelennek az MI-alapú támadási módszerek, például a deepfake technológia és az adaptív adathalászat. Az esettanulmány egy kitalált ország, Novaterra példáján keresztül mutatja be az MI integrációját a kritikus infrastruktúrák védelmébe, beleértve az energia-, víz- és pénzügyi rendszerek biztonságát. Az MI-alapú szimulációk jelentős védelmi potenciált hordoznak, ugyanakkor etikai kérdéseket is felvetnek. A kutatás rámutat, hogy az MI és a kiberbiztonság közötti szoros kapcsolat alapvető a fenntartható digitális társadalom megteremtéséhez. A technológia jövője az innováció és az etikus alkalmazás egyensúlyának megteremtésében rejlik.

Kulcsszavak: mesterséges intelligencia, kiberbiztonság, kiberműveletek

Abstract

The study examines the applications of artificial intelligence (AI) in cybersecurity, highlighting its role in modern cyber operations. AI technologies enable rapid threat identification, improve incident management efficiency and automate defence processes. Offensive applications include AI-based attack methods such as deepfake technology and adaptive

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola, e-mail: viktoria.hanko@protonmail.com

phishing. The case study uses the example of a fictional country, Novaterra, to illustrate the integration of AI into the protection of critical infrastructure, including energy, water and financial systems. AI-based simulations have significant defence potential but also raise ethical issues. The research shows that the close link between AI and cybersecurity is essential for creating a sustainable digital society. The future of the technology lies in balancing innovation and ethical application.

Keywords: artificial intelligence, cyber security, cyber operations

Bevezetés

A mesterséges intelligencia (a továbbiakban: MI) és a kiberbiztonság napjaink két meghatározó technológiai és társadalmi témája, amelyek szorosan összefonódnak, és alapvető hatást gyakorolnak életünk minden területére. Az MI forradalmi módon alakítja át az információfeldolgozást, a döntéshozatalt és a problémamegoldást, miközben a kiberbiztonság egyre fontosabbá válik a digitális térben való biztonságos működéshez. Az MI előnyei közé tartozik, hogy hatalmas mennyiségű adatot képes elemezni és értelmezni, így gyorsabb és pontosabb eredményeket produkál, mint bármely emberi erőfeszítés. Például az egészségügyben az MI segítségével gyorsabban diagnosztizálhatók bizonyos betegségek, mint például a rák korai stádiumai, ami életeket menthet. Ugyanakkor az MI kiberbiztonsági alkalmazásai is lenyűgözők: képes felismerni a hálózati forgalomban rejlő anomáliákat, és valós időben kiszűrni a potenciális fenyegetéseket. Azonban ugyanilyen hatékony lehet a támadói oldalon is: például az úgynevezett *deepfake* technológiával rendkívül hiteles hamis videók és hangfelvételek készíthetők, amelyek félrevezethetik a közvéleményt vagy manipulálhatják a döntéshozókat. A kiberbiztonság ezzel szemben arra hivatott, hogy megvédje az adatainkat, rendszereinket és magánszféránkat a rosszindulatú támadásoktól. Példa erre a banki szektor, ahol a kiberbiztonsági megoldások elengedhetetlenek az ügyfelek pénzügyi adatainak védelmében. A két terület szimbiózisban működik, hiszen az MI-alapú rendszerek növelik a kiberbiztonság hatékonyságát, míg a kiberbiztonság védi az MI-rendszereket a manipulációtól és a támadásoktól. Ennek ellenére az MI alkalmazása önmagában hordoz bizonyos kockázatokat, például olyan etikai kérdéseket, mint a magánszféra megsértése, míg a kiberbiztonság területén az egyre kifinomultabb támadások folyamatos kihívást jelentenek. Ezért létfontosságú, hogy mind a két fronton proaktív megközelítést alkalmazzunk, amely nemcsak a technológiai előnyökre épít, hanem figyelembe veszi a lehetséges veszélyeket is. Összekapcsolásuk és szinergiájuk kihasználása kulcsfontosságú a jövő digitális társadalmának biztonságos és fenntartható működése érdekében, ugyanakkor meg kell találni az egyensúlyt az innováció és a biztonság között. Ez különösen fontos olyan korban, amikor az adatok és az információk védelme alapvető emberi joggá válik, miközben a technológiai fejlődés lehetőséget teremt a globális problémák megoldására is. Az MI és a kiberbiztonság tehát nemcsak technológiai eszközök, hanem olyan alapvető építőelemek, amelyek meghatározzák társadalmunk jövőjét.

A kutatás célja, hogy feltárja a mesterséges intelligencia szerepét és lehetőségeit a kiberműveletekben, különös tekintettel a védelmi és támadó alkalmazásokra,

valamint a kritikus infrastruktúrák védelmére. A tanulmány módszertana kvalitatív jellegű, azaz irodalmi áttekintésen, valamint egy szimulációval alátámasztott esettanulmányon – a fiktív Novaterra állam példáján – keresztül elemzi az MI gyakorlati alkalmazását a kiberbiztonság területén.

A mesterséges intelligencia fogalmi keretei, alkalmazási területei

A mesterséges intelligencia egy digitális számítógép vagy számítógép-vezérelt robot azon képessége, hogy olyan feladatokat végezzen, amelyeket általában intelligens lényekkel társítanak. A kifejezést gyakran alkalmazzák az olyan rendszerek fejlesztésére irányuló projektekre, amelyek rendelkeznek az emberre jellemző intellektuális folyamatokkal, mint például az érvelés, az értelem felfedezése, az általánosítás vagy a múltbeli tapasztalatokból való tanulás képessége. Az 1940-es évekbeli kifejlesztésük óta a digitális számítógépeket úgy programozták, hogy nagyon összetett feladatokat – például matematikai tételek bizonyítását vagy sakkjátékot – nagy szakértelemmel végezzenek. A számítógépek feldolgozási sebességének és memóriakapacitásának folyamatos fejlődése ellenére még mindig nincsenek olyan programok, amelyek szélesebb területeken vagy a mindennapi tudást igénylő feladatokban teljes emberi rugalmasságot tudnának felmutatni. Másrészt egyes programok bizonyos speciális feladatok végrehajtásában elérték az emberi szakértők és szakemberek teljesítményszintjét, így a mesterséges intelligencia ebben a korlátozott értelemben olyan különböző alkalmazásokban is megtalálható, mint az orvosi diagnosztika, a számítógépes keresőmotorok, a hang- vagy kézírás-felismerés és a chatbotok.[2] Mára a technológiai fejlődés egyik legfontosabb hajtóerejévé vált, jelentős hatással az iparra, a társadalomra és a mindennapi életre.

Egy teljes körű, végponttól végpontig terjedő MI-megoldás képes az emberi szintű tudás befogadására (például gépi olvasás és számítógépes látás révén), és ezen információk felhasználásával olyan feladatok automatizálására és felgyorsítására, amelyeket korábban csak emberek végeztek.[3] Az Alan Turing (1950) által javasolt Turing-tesztet gondolatkísérletként alkották meg annak érdekében, hogy empirikus módon igazolható választ adjon a „Gondolkodhat-e egy gép?" kérdésre, elkerülve a kérdés filozófiai értelmezésének bizonytalanságait. A számítógép akkor megy át a teszten, ha egy emberi kérdezőbiztos néhány írásbeli kérdés feltevése után nem tudja megállapítani, hogy az írásbeli válaszok egy embertől vagy egy számítógéptől származnak-e. A számítógépnek a következő képességekre lenne szüksége:

- *Természetes nyelvfeldolgozás* (*natural language processing,* NLP), hogy sikeresen kommunikáljon emberi nyelven. Az NLP az emberi nyelv megértésére és generálására összpontosít. Az olyan technológiák, mint a chatbotok, a szövegfordítók vagy a hangvezérelt asszisztensek, az NLP eredményeire épülnek.
- *Tudásreprezentáció (knowledge representation)* ahhoz, hogy el tudja tárolni, amit tud vagy hall. Kulcsszerepet játszik a mesterséges intelligenciában, mivel

[2] Copeland [é. n.].
[3] Taddy 2018.

lehetővé teszi a rendszerek számára az információk strukturált formában történő tárolását és feldolgozását, ezáltal támogatva a döntéshozatalt és a problémamegoldást. Például a gyógyászatban található diagnosztikai rendszerekben kifejezetten az onkológiák használják a betegségek osztályozására és kezelésére.

- *Automatizált következtetés (automated reasoning)* a kérdések megválaszolásához és új következtetések levonásához. Ez lehetővé teszi a mesterségesintelligencia-rendszerek számára, hogy logikai szabályok és algoritmusok alapján önállóan vonjanak le következtetéseket, ezzel segítve a komplex problémák gyors megoldását. Használatos jogi dokumentumok elemzésére, például szerződések feltételeinek és ellentmondásainak automatikus azonosítására, ami megkönnyíti a jogi szakemberek munkáját és csökkenti a hibalehetőségeket.
- *Gépi tanulás* (*machine learning,* ML) az új körülményekhez való alkalmazkodáshoz, valamint a minták felismeréséhez és extrapolálásához. Az ML része, amely a legnagyobb nyilvánosságot kapja – olyannyira, hogy gyakran összekeverik az egész MI-vel. Emellett az egyik legfontosabb ága is, amely lehetővé teszi a rendszerek számára, hogy adatokból tanuljanak, és idővel egyre pontosabb döntéseket hozzanak. A gépi tanulási algoritmusok különféle típusai közé tartoznak a felügyelt tanulás, a felügyelet nélküli tanulás és a megerősítéses tanulás. Ennek egyik ága a *mélytanulás (deep learning),* az ML egy speciális formája, amely mély neurális hálózatok segítségével tanul és értelmez összetett mintákat. Az ilyen rendszerek különösen jól alkalmazhatók képfelismerésre, beszédfelismerésre és természetes nyelv feldolgozására.

A teljes Turing-teszt teljesítéséhez a robotnak a továbbiakra van szüksége:

- *Számítógépes látás (computer vision)* és *beszédfelismerés (speech recognition)* a világ értékeléséhez. Ezek az MI azon ágai, amelyek a vizuális adatok, például képek és videók elemzésére és értelmezésére szolgálnak. A számítógépes látás technológiáit használják például önvezető autókban, arcfelismerésben és orvosi képalkotásban.
- *Robotika,* amely a tárgyak manipulálásához és a mozgáshoz szükséges. Az MI-vezérelt robotok képesek az érzékelésre, az elemzésre és az autonóm cselekvésre. A robotika egyesíti az MI-t a mechanikai rendszerekkel, és alkalmazási területei között megtalálható a gyártás, az egészségügy és a mezőgazdaság.

Ez a hat részterület alkotja a mesterséges intelligencia nagy részét. A mesterséges intelligencia kutatói mégis kevés erőfeszítést fordítottak a Turing-teszt teljesítésére, mivel úgy vélik, hogy fontosabb az intelligencia mögöttes elveinek tanulmányozása.[4]

A mesterséges intelligencia szinte minden iparágban és társadalmi területen megjelent, és számos konkrét alkalmazási lehetőséget kínál, többek között a következő területeket:

[4] Russell–Norvig 2020.

1. *Egészségügy:* az MI megjelenése forradalmasíthatja az egészségügyi diagnosztikát és kezelést. Például az MI-alapú rendszerek képesek korai stádiumú betegségeket, a rákot felismerni radiológiai képek elemzésével. A gyógyszerkutatásban az alkalmazása felgyorsíthatja az új gyógyszerek kifejlesztését és tesztelését.
2. *Közlekedés:* meghatározó szerepet játszik az önvezető járművek fejlesztésében, amelyek a környezetük érzékelésére és az autonóm navigációra képesek. Ezenkívül az MI-alapú forgalomirányító rendszerek optimalizálhatják a közlekedést, csökkentve a dugók számát.
3. *Pénzügy:* segítségével hatékonyabbá válhat a csalásfelderítés, a hitelképesség-elemzés és az algoritmikus kereskedés. A bankok és a pénzügyi intézmények olyan rendszereket alkalmazhatnak, amelyek valós időben elemzik az ügyfelek tranzakcióit és azonosítják a gyanús tevékenységeket.[5]

A fentiek alapján elmondható, hogy előnyei között szerepel a hatékonyság növelése, az emberi munkaerő tehermentesítése és az új innovációs lehetőségek megnyitása. Az MI-rendszerek képesek olyan mennyiségű adatot feldolgozni, amely az ember számára kezelhetetlen lenne, így gyorsabb és pontosabb döntéseket hoznak. Például egy MI-vezérelt diagnosztikai rendszer több millió beteg adatait elemezve képes egyedi, személyre szabott kezelési javaslatokat nyújtani. Ugyanakkor az alkalmazása jelentős etikai és társadalmi kérdéseket vet fel. A magánélet védelme, az adatok biztonsága és az algoritmusok elfogultsága mind olyan problémák, amelyeket nem szabad figyelmen kívül hagyni. Az MI-vezérelt rendszerek bevezetése emellett munkahelyek elvesztéséhez járulhat hozzá az automatizáció miatt, ami különösen érzékeny téma bizonyos iparágakban. Jövőjét tekintve tele van lehetőségekkel, de a felelős fejlesztés és alkalmazás elengedhetetlen ahhoz, hogy a technológia pozitív hatásai érvényesüljenek. Az MI folyamatos fejlődése új megoldásokat hozhat az egészségügy, a közlekedés és a fenntarthatóság területén, miközben egyre fontosabbá válik az etikai kérdések kezelése.[6] Ezek a kérdések rávilágítanak annak jelentőségére, hogy átlátható, etikus gyakorlatok figyelembevételével történő tervezés és használat szükséges. Az a tény, hogy az MI által működtetett védelmi intézkedések hatalmas mennyiségű adatot képesek összegyűjteni és nyomon követni, az egyik legfőbb aggodalom napjainkban. Az ezekből a képességekből eredő lehetséges adatvédelmi incidensek az egyik fő aggály. Az etikai problémák azonnali felismerése érdekében egyidejűleg védenünk kell a felhasználók személyes adatait is. A kiberbiztonság esetében a fenyegetések felismerése elfogult lehet, ami egyes emberek téves azonosításához vagy mások igazságtalan jellemzéséhez vezethet. Az etikai normák betartása és az esetleges igazságtalan hatások lehetőségének csökkentése szempontjából kulcsfontosságú annak biztosítása, hogy az MI-védelmi megoldásokat tisztességesen hozzák létre és használják fel. Problémák akkor merülnek fel, ha a döntéshozatali folyamat nem egyértelmű.[7]

[5] Zhang–Lu 2021.
[6] Shukla–Jaiswal 2013.
[7] Kaushik et al. 2024.

A mesterséges intelligencia és a kiberbiztonság kapcsolata

Ahogy az a korábbi fejezetben olvasható, az MI-nek számos területen rengeteg előnye és felhasználási lehetősége van, ezek közül az egyik a kiberbiztonság. A kibertámadások gyors fejlődése és az eszközök elterjedése miatt ez a technológia segíthet lépést tartani a kiberbűnözőkkel, automatizálni a fenyegetések észlelését és hatékonyabban reagálni, mint a hagyományos szoftveres vagy ember által vezérelt módszerek. A kiberbiztonságban való felhasználás néhány előnye és felhasználási módja:

- *Újonnan felmerülő fenyegetések azonosítása:* az MI felhasználható a kibertérből érkező kockázatok és a potenciálisan káros tevékenységek azonosítására. Mivel a hagyományos szoftverrendszerek nem képesek lépést tartani a hetente keletkező új vírusok óriási mennyiségével, ez az a terület, ahol az MI valódi segítséget nyújthat. Ezeket a rendszereket úgy tervezték, hogy összetett algoritmusok felhasználásával azonosítsák a rosszindulatú szoftvereket, előrejelző modellezést végezzenek, és még a legkevésbé kompakt rosszindulatú szoftvereket vagy zsarolóvírusos támadásokat is képesek legyenek azonosítani, mielőtt azok bejutnának a rendszerbe.
- *Botok elleni küzdelem:* a botok ma már az internetes forgalom jelentős részét teszik ki, és veszélyesek lehetnek. A botok valódi fenyegetést jelenthetnek, a lopott jelszavakkal történő fiókátvételtől kezdve a hamis fiókok létrehozásán át az adatlopásig. Az automatizált fenyegetéseket nem lehet csak kézi válaszokkal legyőzni. Az MI segít a webhelyforgalom átfogó ismereteinek kialakításában és a jó botok (például a keresőmotorok) megkülönböztetésében a káros botoktól és emberektől. Továbbá megkönnyíti a hatalmas mennyiségű adatok elemzését, és lehetővé teszi a kiberbiztonsági szakemberek számára, hogy a folyamatosan változó fenyegetettségi környezethez igazodva módosítsák módszereiket, védelmi mechanizmusaikat.
- Kockázat-előrejelzés: az MI-rendszerek segítenek az IT-eszközleltár meghatározásában, amely egy átfogó és pontos lista az összes eszközről, felhasználóról és alkalmazásról, amelyek különböző mértékben hozzáférnek a különböző rendszerekhez. A jelenlegi helyzetben ezek a rendszerek képesek előre jelezni, hogy a vállalati irányítással és a fenyegetések kitettségével kapcsolatban hogyan és mikor a legvalószínűbb, hogy feltörik őket, ezért a vezetés átirányíthatja az erőforrásokat a legveszélyeztetettebb régiókba.[8]

Azonban már a korábbi szakaszban, a hálózatépítés során is megjelenhet az MI mint megoldás, hiszen a hálózat tervezői nem feltétlenül találják meg a hálózati topológia sebezhetőségét és bizonytalanságát. A hálózat használatának folyamatában a nem egyenletes adatáramlás, amely feltárja a hálózat helyzetét, előre érzékeli a hálózat gyenge láncszemét, alapot biztosít a hálózat kiigazításához, így szükség van a hálózati helyzetismeret használatára. A hálózati helyzetfelismerés folyamatában az összetett hálózatokat modellezni kell, szükséges elemezni a hálózat biztonsági helyzetét, és végül meg kell adni a hálózati helyzetfelismerés mennyiségi eredményeit. Ennek

[8] Mohammed 2020.

a folyamatnak az eléréséhez szükséges, hogy a helyzetfelismerési modell erős tudásbázissal rendelkezzen, amelyből gyorsan felismeri és hozzáigazítja a hálózati helyzetet. Ugyanakkor a modellnek képesnek kell lennie a jellemzők kinyerésére.[9] Emellett az 5G megjelenésével néhány kutató elkezdte tanulmányozni az 5G-technológiák anomáliaérzékelését. Például egyes kutatók egy adaptív mélytanuláson alapuló 5G-hálózati anomáliafelismerő rendszert javasoltak. Ebben a keretrendszerben két réteg mélytanulási modellt használtak: az egyik a hálózati áramlás aggregációs észlelésének módszerére összpontosított a rendellenes jelek gyors keresésével, főként mély neurális hálózatot használtak a feldolgozáshoz, a másik az idővonal és a kapcsolódó jellemzők közötti viszonyon alapult a hálózati anomáliák azonosítására, és közvetlenül kommunikált a felügyeleti és diagnosztikai modullal az anomáliák megtalálása érdekében. A hosszú rövid távú memóriát (LSTM) az idősorok jó kezeléséhez implementálták.[10]

Ezek a módszerek mind pozitív megközelítései az MI és a kiberbiztonság kapcsolatának. Azonban nem szabad elmennünk amellett, hogy ma már számos kifinomult, mesterséges intelligencia által vezérelt kibertámadási módszer áll a kiberbűnözők rendelkezésére, amelyekkel problémákat okozhatnak a kormányzatnak, a szervezeteknek, a vállalkozásoknak és az egyéneknek. Az MI által vezérelt kibertámadások az utóbbi években egyre nagyobb számban fordulnak elő. Még ha sok szervezet át is tér a biztonságosabb kibertérbe, például a felhőalapú tárolási szolgáltatások bevezetésére, erőforrásaik továbbra is sebezhetők maradnak. Általánosságban elmondható, hogy ezek a támadástípusok csak súlyosbodni fognak, majd a hagyományos kiberbiztonsági eszközök számára szinte lehetetlen lesz felismerni azokat. Ez egyszerűen a gépi hatékonyság vs. emberi erőfeszítés kérdése. Ennek a növekvő trendnek a komplexitása és mérete további kihívások elé állítja a kiberbiztonsági szakembereket. Ezzel szemben a fenyegetés sikeres elhárításához szükséges, magasan képzett szakemberek egyre drágábbak és nehezebben találhatók meg. Az újonnan megjelenő támadási technikák következményei károsak lehetnek. Egyes kutatók szerint az MI által vezérelt kibertámadási technikák képesek lesznek alkalmazkodni ahhoz a környezethez, amelyben végrehajtják őket. A kontextuális adatokból vagy információkból tanulva kihasználhatják a sebezhetőségeket, vagy megbízható rendszerjellemzőknek álcázhatják magukat.[11]

Az MI és a kiberbiztonság szoros kapcsolata a korábban bemutatott, civil életben tapasztalt előnyök mellett a katonai műveletekben is kiemelkedő fontosságú. A modern hadviselés egyre inkább támaszkodik a kibertéri műveletekre, ahol az MI-technológiák gyorsítják az adatfeldolgozást és a döntéshozatalt, míg a kiberbiztonság védi az érzékeny rendszereket az ellenséges beavatkozásoktól. E kettő kombinációja alapvetővé vált a hadseregek stratégiájában, biztosítva a technológiai fölényt és a működési stabilitást a digitális térben.

[9] Zhang et al. 2022.
[10] Maimó et al. 2018.
[11] Guembe et al. 2022.

Kibertéri műveletek

A mesterséges intelligencia és a kiberbiztonság szoros összefonódása különösen jelentőségteljes a kiberműveletek területén, ahol az adatvezérelt döntéshozatal és a valós idejű fenyegetéskezelés alapvető követelmény. Az MI-technológiák lehetővé teszik a kiberműveletek hatékonyságának növelését, például az anomáliaészlelés, az automatizált válaszlépések és az ellenséges hálózatok elemzése terén. Eközben a kiberbiztonság szavatolja, hogy ezek a fejlett rendszerek védettek maradjanak az ellenséges manipulációval szemben, amely aláásná a műveletek sikerét. Emellett az MI egyre fontosabb szerepet tölt be a hadviselésben, mivel növeli a kiberműveletek hatékonyságát, támogatja az autonóm fegyverrendszerek fejlődését, és előmozdítja az ember és gép közötti kapcsolat kialakítását. Azonban nem csupán a hatékonyságot fokozó erőszorzóként *(force multiplier)* értelmezhető, hanem önálló eszközként is, amely képes stratégiai és taktikai döntéseket meghozni.[12]

A kibertéri műveletek a modern hadviselés és biztonságpolitika kulcsfontosságú elemeivé váltak, mivel az információs technológia fejlődése új dimenziót nyitott a konfliktusok és a védelem terén. Haig Zsolt értelmezése szerint a kibertéri műveleteket a következőképpen definiálhatjuk:

„A kibertéri műveletek a kibertérben érvényesülő információs képességek integrált, összehangolt és koordinált alkalmazására irányuló tevékenységek összessége, amelyek a műveletek célkitűzéseinek elérése érdekében, a kibertéri hálózatos infokommunikációs rendszereket felhasználva, a kognitív képességekkel közvetlenül, illetve a technikai képességekkel közvetetten hatásokat gyakorolnak a műveletekben részt vevő célközönség szándékára, helyzetértelmezésére és képességeire."[13]

A kibertéri műveletek és a kiberhadviselés szorosan összefonódnak, mivel mindkettő az információs technológia alkalmazásával befolyásolja a katonai és biztonsági műveletek kimenetelét. A kibertéri műveletek magukban foglalják a számítógépes hálózatok védelmét, támadását és kihasználását, míg a kiberhadviselés ezen tevékenységek katonai kontextusban történő alkalmazását jelenti. A modern hadviselésben a kiberhadviselés integrálása elengedhetetlen, hiszen a kibertérben végrehajtott támadások képesek megbénítani kritikus infrastruktúrákat, kommunikációs rendszereket és egyéb létfontosságú szolgáltatásokat. Ezért a kibertéri műveletek hatékony végrehajtása és a kiberhadviselési képességek fejlesztése kulcsfontosságú a nemzetbiztonság szempontjából. A NATO is felismerte a kibertér jelentőségét, és 2016-ban műveleti területként ismerte el, hangsúlyozva annak fontosságát a modern hadviselésben.[14] Ezáltal elmondható, hogy általánosan megfogalmazva a kiberhadviselés a kiberműveletek összefüggő sorozataként értelmezhető. Attól függően, hogy ezek a műveletek katonai vagy civil célpontok ellen irányulnak, más típusú műveletek is kapcsolódhatnak

[12] Boda 2024.
[13] Haig 2018: 15.
[14] Kassai 2022.

hozzájuk. Idetartozhatnak például a médiaműveletek, a pszichológiai műveletek, valamint az elektronikai hadviselés egyes elemei.[15]

A katonai elmélet a háborút három szintre osztja: hadászati (stratégiai), hadműveleti és harcászati (taktikai) szintre. Ezek a szintek összefüggnek egymással, és ami az egyik szinten történik, az befolyásolja a többit. A stratégiai szint a „hogyan nyerjünk háborút?" kérdéseivel foglalkozik. Számos államközi kibertéri művelet stratégiai szinten zajlik. A legtöbbjüket szándékosan úgy tervezték, hogy a fegyveres támadás küszöbértéke alatt maradjanak, hogy elkerüljék a hagyományos konfliktusba való eszkalálódást. A mai napig nem történt olyan összehangolt, stratégiai kiberháborús hadjárat egy másik állam ellen, amely elérte volna a fegyveres támadás szintjét, vagy könnyen háborúnak minősíthető lett volna. Ehhez a legközelebb az amerikai kiberparancsnokság által Irán ellen tervezett Nitro Zeus művelet áll, amelyet 2016-ban lepleztek le. Ez egy vészterv volt arra az esetre, ha elődje, az Olimpiai Játékok művelet, ismertebb nevén a Stuxnet, és az iráni atomprogram korlátozására irányuló diplomáciai erőfeszítések kudarcot vallanak. A hadműveleti szintre egy kitűnő példa az Orchard hadművelet (más néven Operation Outside the Box), amely 2007-ben zajlott Szíriában, és amelynek során izraeli hackerek Tell-Abjadban hatástalanítottak egy szíriai légvédelmi radart, majd gyors egymásutánban kinetikus légicsapást mértek. Az izraeli légierő ezután megsemmisített egy nukleáris kísérleti telepet az észak-szíriai Deir ez-Zórban. A műveletek sikeresek voltak, és a digitális komponens jelentős szerepet játszott abban, hogy az izraeli F–15-ös repülőgépek észrevétlenül léphessenek be a légtérbe. A taktikai szintről nem sokat lehet tudni, azonban Shane Harris újságíró kiterjedt kutatást végzett a 2007-es iraki felkelésellenes műveletek során alkalmazott támadó taktikai kiberműveletekről. Ennek a műveletnek három összetevője volt:

- Az NSA az iraki internetszolgáltatók telefonos metaadatait földrajzi térképekkel hozta összefüggésbe, így meg tudta határozni a rögtönzött robbanószerkezetek beindítására használt mobiltelefonok földrajzi helyét. Az NSA képes volt ezek egy részét távolról megsemmisíteni, vagy a közelben lévő felkelők tartózkodási helyét megtudni.
- Rosszindulatú szoftverek alkalmazása a felkelők számítógépes rendszerei ellen. Itt két változatot használtak. Az elsőben számos iraki felhasználót fertőztek meg nagy mennyiségben manipulált adathalász-e-maileken keresztül. A második a számítógépek célzott megfertőzését jelentette USB-n keresztül, amelyeket a terepen lévő taktikai kiberegységek vittek magukkal.
- Felkelők elleni információs műveletek. Az iraki telefonhálózathoz való hozzáféréssel az amerikai csapatok hamis szöveges üzeneteket küldtek a felkelőknek, hogy demoralizálják őket, vagy csapdát állítsanak.[16]

Ahogy azt a fejezet elején hangsúlyoztam, a mesterséges intelligencia kiemelt szerepet képvisel a kiberműveletek terén – kifejezetten a védelmi oldalon. Azonban ahogy arra egyes kutatók rámutatnak, az MI fejlődése mind a kiberbiztonságban való felhasználását, mind a visszaélést elősegítette. A hagyományos kibertámadásokkal ellentétben az új

[15] Kovács 2023.
[16] Schulze 2020.

formák az MI-rendszereket célozzák meg a viselkedés manipulálására, megkérdőjelezve az MI robusztusságában és ellenálló képességében rejlő lehetőségeket. Az adatok megfertőzése, a modellek manipulálása és a *backdoorok* nyitása az irányítás megszerzésének elsődleges módszerei. A mesterséges intelligencia fegyverként felhasználható olyan összetett kibertámadások indítására, mint a APT-támadások, az adathalászat és a *social engineering* támadások, amelyek jelentős kiberbiztonsági kihívásokat jelentenek. A rosszindulatú programok javítására vagy elrejtésére való felhasználása komoly fenyegetést jelent, mivel az olyan technikák, mint a kód meghamisítása és az adaptív viselkedés felvétele, kikerülik a jelenlegi észlelési módszereket. Az offenzív MI célzott kiválasztás, hitelesítéseltávolítás, gyors adathalászüzenet-készítés és összehangolt művelettervezés révén növelheti a rosszindulatú programok teljesítményét.[17]

Esettanulmány

Az előző fejezetekben bemutattuk az MI szerepét a kiberműveletekben, különös figyelmet fordítva az offenzív és defenzív alkalmazásokra. Ez a technológia képes felgyorsítani a fenyegetések felismerését, javítani az incidenskezelést, valamint automatizálni a védelmi folyamatokat. Kiemeltük, hogy az offenzív oldalon az MI-eszközökkel hatékonyan lehet manipulálni információkat és kihasználni a rendszerek gyenge pontjait – például *social engineering* támadásokon keresztül. Ugyanakkor a defenzív oldalon a mesterségesintelligencia-alapú rendszerek, mint például az anomáliaészlelés vagy az automatizált reagálás, jelentős védelmi potenciállal bírnak.

Ez a fejezet a korábban bemutatott alapelveket ülteti gyakorlatba egy fiktív ország, Novaterra példáján keresztül. Részletesen elemezzük, hogyan használja az MI-t az ország a kibervédelmi stratégiáiban, különös tekintettel a kritikus infrastruktúra védelmére.

Novaterra környezeti bemutatása

Novaterra egy fejlett technológiával rendelkező kis közép-európai állam, amely jelentős mértékben függ digitális infrastruktúrájától. Az ország gazdasága elsősorban az energiatermelésre, a fintechiparra és a technológiaorientált szolgáltatásokra épül, amelyeket kiterjedt villamosenergia-hálózat és fejlett kommunikációs rendszerek támogatnak. Ugyanakkor ezek az infrastruktúrák kiemelt célpontjai a kibertámadásoknak, legyen szó állami vagy nem állami szereplőkről. A kormány felismerte a digitális fenyegetések jelentőségét, és egy átfogó kiberbiztonsági stratégiát dolgozott ki, amelyben kulcsszerepet kapott a mesterséges intelligencia. Az MI-alapú rendszerek telepítése nemcsak a kritikus infrastruktúra védelmét szolgálja, hanem a folyamatos fenyegetések azonosítását és az incidensekre történő gyors reagálást is lehetővé teszi. Novaterra kiemelten épít a gépi tanulási algoritmusokra, amelyek képesek adaptálódni az állandóan változó fenyegetésekhez.

[17] Nobles 2024.

Az MI alkalmazása kritikus infrastruktúrák területén

Villamosenergia-hálózat: a villamosenergia-hálózat Novaterra gazdaságának gerince, amely szélerőműveket, naperőműveket és hagyományos erőműveket integrál. Ezáltal az MI-alapú rendszerek itt képesek valós időben monitorozni a hálózati forgalmat, érzékelni a szokatlan adatforgalmat és azonosítani a potenciális fenyegetéseket. Egy neurálishálózat-alapú anomáliaészlelési rendszer például felismeri, ha egy adott csomópontot szokatlanul nagy adatforgalom ér, ami DDoS-támadásra utalhat. Ezenkívül az MI képes optimalizálni az energiaelosztást, megelőzve az áramszolgáltatás megszakadását, amelyet egy kártékony támadás okozhatna. Ezek az előrejelzési modellek lehetővé teszik a hálózati terhelés dinamikus szabályozását is, amely csökkenti a meghibásodások kockázatát. Ez a megközelítés nemcsak a támadások hatékony kezelését biztosítja, hanem hozzájárul a rendszer hosszú távú fenntarthatóságához is. Az energiaiparban alkalmazott MI így egyszerre szolgálja a megelőzést és a válságkezelést.

Honvédelem: Novaterra hadseregében az MI az információgyűjtés és -elemzés kulcsfontosságú eszköze. Ennek segítségével folyamatosan elemzik az ellenséges kommunikációs csatornákat, és azonosítják a potenciális fenyegetéseket. Továbbá a kibertérből érkező támadásokat valós időben blokkolják, miközben az MI-rendszerek javaslatokat tesznek a műveleti egységeknek a megfelelő válaszintézkedésekre. Az MI közreműködésével szimulációkat futtatnak, hogy felkészüljenek az esetleges támadási forgatókönyvekre, és csökkentsék a valós konfliktusok kockázatait. Az autonóm rendszerek, például drónok és robotok, szintén MI-vezérelt megoldásokkal működnek, amelyek gyors adatfeldolgozásra és önálló döntéshozatalra képesek. Az MI ilyen integrációja jelentősen növeli a hadsereg hatékonyságát, miközben minimalizálja az emberi beavatkozás szükségességét. Ezáltal Novaterra védelmi stratégiája korszerű és alkalmazkodóképes marad a változó fenyegetésekkel szemben.

Rendvédelem: a rendvédelemben az MI-technológiákat főként a bűnügyi elemzésben és a kibertámadások elleni védekezésben alkalmazzák. Egy prediktív elemzési modell segít megállapítani, hogy mely szervezetek lehetnek a leginkább kitettek egy támadásnak, így lehetőség nyílik a proaktív védekezésre. Az MI-alapú rendszerek gyorsan elemezhetik a nagy mennyiségű bűnügyi adatot, segítve a minták felismerését és a gyanús tevékenységek azonosítását. Emellett az online csalások elleni harcban is hatékony eszközként jelennek meg, valós időben azonosítva a gyanús tranzakciókat. További alkalmazási terület az arcfelismerő rendszerek fejlesztése, amelyek az MI segítségével pontosabbak és gyorsabbak a gyanúsítottak azonosításában. A rendvédelemben az MI tehát nemcsak a bűnüldözés gyorsaságát növeli, hanem a megelőzésben is jelentős szerepet játszik. Ez a technológia segíti a rendfenntartó erők munkáját, miközben hozzájárul a lakosság biztonságának növeléséhez.

Pénzügy: a fintech szektorban az MI alkalmazása kulcsfontosságú a csalásfelderítés és a tranzakcióbiztonság terén. Novaterra bankjai MI-alapú rendszereket használnak a szokatlan tranzakciós minták azonosítására, amelyek között lehetnek gyanús pénzmozgások vagy adatlopási kísérletek. Ezen a területen prediktív elemzést alkalmaznak, hogy előre jelezzék az esetleges pénzügyi fenyegetéseket, minimalizálva a pénzmosás és egyéb illegális tevékenységek kockázatát. Továbbá a technológia hozzájárul az önkiszolgáló banki rendszerek biztonságának növeléséhez, valós időben védelmet nyújtva

az adathalász-támadások ellen. Az MI-alapú chatbotok gyorsan felismerik a gyanús interakciókat, és automatikusan értesítik a biztonsági csapatot. A pénzügyi szektorban nemcsak a biztonságot növeli az MI alkalmazása, hanem az ügyfélélményt is javítja, mivel gyorsabb és pontosabb kiszolgálást tesz lehetővé. Ezáltal a fintechipar képes lépést tartani a növekvő fenyegetésekkel és ügyféligényekkel egyaránt.

Vízszolgáltatás: a vízszolgáltatás kulcsfontosságú Novaterra lakossága számára, és a mesterséges intelligencia itt is jelentős védelmi szerepet tölt be. Az MI-alapú rendszerek folyamatosan monitorozzák a vízhálózat működését, észlelik a nyomáscsökkenéseket vagy a szennyezés jeleit, amelyek esetleg támadásra vagy rendszerhibára utalhatnak. A technológia által lehetőség nyílik valós időben reagálni az incidensekre, megelőzve a lakosságot érő súlyos károkat. Emellett prediktív modellezéssel előre jelezhetők a karbantartási igények, így biztosítható a szolgáltatás folyamatossága. Az MI-alapú rendszerek továbbá lehetővé teszik a vízfogyasztási minták elemzését, ami segíthet a vízkészletek hatékonyabb kezelésében. Ezáltal elmondható, hogy nemcsak a védelemben, hanem a fenntarthatóságban is kiemelt szerepet játszik az MI, tehát a vízszolgáltatás hatékonyabbá és biztonságosabbá válik, megfelelve a modern kihívásoknak.

A kiberhadviselés aspektusa

Novaterrában az MI kiemelkedő szerepet tölt be a kiberhadviselés területén, különösen az összetett támadások és védekezési mechanizmusok hatékony kezelésében. Támadói oldalon az MI alkalmazásával automatizálják a sérülékenységfelderítési folyamatokat, amelyek során az algoritmusok képesek gyorsan azonosítani a rendszerek gyenge pontjait, még azelőtt, hogy azokat manuális vizsgálatok felfedeznék. A dezinformációs kampányokban az MI-alapú generatív modellek, például a *deepfake* technológiák, hamisított vizuális és hanganyagok előállításával növelik a pszichológiai hadviselés hatékonyságát. Ezek az eszközök különösen akkor hatásosak, ha az ellenfél közvéleményének befolyásolása vagy belső instabilitás előidézése a cél. Védekezési oldalon is elengedhetetlen az MI alkalmazása a modern kibervédelmi rendszerek hatékonyságának biztosításához. Az országban adaptív biztonsági algoritmusokat alkalmaznak, amelyek valós időben elemzik a hálózati forgalmat, és azonosítják a gyanús tevékenységeket, például a szolgáltatásmegtagadási támadások (DDoS) korai jeleit. Az MI továbbá támogathatja a prediktív elemzési rendszereket, amelyek képesek előre jelezni az ellenséges támadások valószínűségét, lehetővé téve a proaktív védekezést. Például egy neurális hálózat segítségével modellezhetők az ellenséges aktorok viselkedési mintái, így azonosíthatók a potenciális célpontok és a támadási stratégiák. Mindemellett az MI-alapú szimulációk lehetőséget adnak arra is, hogy a kiberhadviselési forgatókönyveket valósághűen modellezzék. Ez segíti a döntéshozókat abban, hogy optimalizálják a védelmi stratégiákat, miközben minimalizálják az emberi hiba lehetőségét. A mesterséges intelligencia tehát a kiberhadviselés mindkét oldalán nélkülözhetetlen, mivel lehetővé teszi a gyors alkalmazkodást és a stratégiai előnyök kihasználását egy folyamatosan változó digitális környezetben.

Forgatókönyv: DDoS-támadás egy villamosenergia-hálózat ellen

A szimuláció alapvető célja, hogy tesztelje Novaterra villamosenergia-hálózatának védelmi mechanizmusait egy DDoS-támadás ellen. A szimuláció további célja, hogy azonosítsa a rendszer azon gyenge pontjait, amelyek kihasználhatók lennének egy valós támadás során, miközben javítja a reagálási időt.

A forgatókönyvben az MI-alapú szimulációs rendszer virtuális környezetben modellezi a villamosenergia-hálózatot. A szimuláció részeként az alábbi fő elemek jelennek meg:

- Támadási szcenárió: az MI generál egy széles körű DDoS-támadást, amelyben az adatcsomagok nagymértékű áradata irányul az erőműveket felügyelő rendszerekre.
- Védelmi reakció: az MI-alapú védelmi rendszer valós időben elemzi a beérkező adatforgalmat, azonosítja a legitim és illegitim csomagokat, majd automatikusan blokkolja a rosszindulatú adatokat.
- Hatékonyság mérése: a rendszer méri a reagálási időt, a sikeresen blokkolt csomagok arányát, valamint az üzemzavarok hatását a hálózat stabilitására.

A szimuláció kimutatta, hogy a védelmi rendszer 95%-os hatékonysággal blokkolta a támadási adatcsomagokat, miközben minimális késlekedést okozott a legitim forgalomban. Az anomáliaészlelési rendszer korábban nem ismert mintákat is felfedezett, amelyek a jövőbeni finomhangolás alapjául szolgálhatnak. Emellett a szimuláció során felismerték, hogy egyes adatcsomagok dinamikus blokkolása további optimalizálást igényel, hogy teljes mértékben elkerüljön minden működési zavart. Emellett ez a forgatókönyv bemutatja, hogy az MI-alapú szimulációk hogyan segíthetik Novaterra kiberbiztonsági stratégiájának fejlesztését. Az ilyen technológiák nemcsak az azonnali fenyegetések elhárításában hatékonyak, hanem hozzájárulnak a hosszú távú védelmi stratégiák optimalizálásához is. A szimuláció alapján kidolgozott javaslatok támogatják a rendszerszintű ellenálló képességek kiépítését és a nemzetgazdasági stabilitás fenntartását egyre komplexebb kiberfenyegetések közepette.

A fent leírtakat figyelembe véve elmondható, hogy Novaterra esete rávilágít a mesterséges intelligencia fontosságára a defenzív kiberműveletekben, különös tekintettel a kritikus infrastruktúrák védelmére. Az MI alkalmazása lehetővé teszi a fenyegetések gyors felismerését, a rendszerek adaptálását és az automatizált reagálást, ezáltal növelve az állami és gazdasági stabilitást. Ugyanakkor nem csupán technológiai, hanem etikai kihívásokat is felvet az alkalmazása, amelyeket meg kell oldani a biztonság fenntartása érdekében. Novaterra példája megmutatja, hogy a mesterséges intelligencia nemcsak hatékony védelmi eszköz, hanem a digitális jövő egyik meghatározó eleme.

Összegzés és következtetések

A mesterséges intelligencia alkalmazása a kiberműveletekben jelentős lehetőségeket és kihívásokat hordoz. Az MI a kiberbiztonság védelmi oldalán kiemelkedő

hatékonyságot nyújt az anomáliaészlelésben, fenyegetések valós idejű kezelésében és az automatizált válaszlépések kidolgozásában. Ugyanakkor az offenzív oldalon az MI-támogatott támadások, például a *deepfake* technológia és az adathalászat, új fenyegetési dimenziókat nyitnak. Az etikai és biztonsági kockázatok hangsúlyozzák a felelősségteljes fejlesztés szükségességét. A cikk esettanulmánya, Novaterra példája bemutatja az MI alkalmazásának stratégiai szerepét a kritikus infrastruktúrák védelmében, amely képes gyorsan alkalmazkodni a változó fenyegetésekhez. Az MI szimbiózisa a kiberbiztonsággal kulcsfontosságú a digitális jövő megbízhatóságának biztosításában, ugyanakkor kiegyensúlyozott megközelítés szükséges az innováció és a biztonság között.

További kutatási irányként lehetőséget látok abban, hogy a jelenlegi fikcióalapú modell egy virtuális környezetben megvalósított, konkrét gyakorlati tesztelés formáját öltse, amelyben az MI-rendszerek működését különböző tudományos módszerekkel, például kvantitatív elemzésekkel, szimulációs modellezéssel és értékelési keretrendszerekkel vizsgálnám.

Felhasznált irodalom

Boda Mihály (2024): A kockázatkerülő háború és a bátorság a 20–21. század fordulóján. *Honvédségi Szemle,* 152(3), 113–125. Online: https://doi.org/10.35926/HSZ.2024.3.9

Copeland, B. J. [é. n.]: Artificial Intelligence. *Britannica*. Online: www.britannica.com/technology/artificial-intelligence

Guembe, Blessing et al. (2022): The Emerging Threat of Ai-Driven Cyber Attacks: A Review. *Applied Artificial Intelligence,* 36(1). Online: https://doi.org/10.1080/08839514.2022.2037254

Haig Zsolt (2019): *Információs műveletek a kibertérben*. Budapest: Dialóg Campus Kiadó.

Kassai Károly (2022): A kibertér műveleti képesség szerepének, jelentőségének és fókuszának evolúciója a NATO stratégiai dokumentumai alapján. *Military and Intelligence CyberSecurity Research Paper,* (9), 1–38. Online: http://hdl.handle.net/20.500.12944/100742

Kaushik, Keshav et al. (2024): Ethical Considerations in AI-Based Cybersecurity. In Kaushik, Keshav – Sharma, Ishu (szerk.): *Next-Generation Cybersecurity. AI, ML, Blockchain*. Singapore: Springer, 437–470. Online: https://doi.org/10.1007/978-981-97-1249-6_19

Kovács László (2023): *Hadviselés a 21. században: kiberműveletek*. Budapest: Ludovika Egyetemi Kiadó.

Maimó, Lorenzo Fernández et al. (2018): A Self-Adaptive Deep Learning-Based System for Anomaly Detection in 5G Networks. *EEE Access,* 6, 7700–7712. Online: https://doi.org/10.1109/ACCESS.2018.2803446

Mohammed, Ishaq Azhar (2020): Artificial Intelligence for Cybersecurity: A Systematic Mapping of Literature. *International Journal of Innovations in Engineering Research and Technology,* 7(9), 172–176. Online: https://repo.ijiert.org/index.php/ijiert/article/view/2797

Nobles, Calvin (2024): The Weaponization of Artificial Intelligence in Cybersecurity: A Systematic Review. *Procedia Computer Science,* 239, 547–555. Online: https://doi.org/10.1016/j.procs.2024.06.206

Russell, Stuart – Norvig, Peter (2020): *Artificial Intelligence. A Modern Approach. 4th Edition.* London: Pearson.

Schulze, Matthias (2020): Cyber in War: Assessing the Strategic, Tactical, and Operational Utility of Military Cyber Operations. *12th International Conference on Cyber Conflict (CyCon),* 183–197. Online: https://doi.org/10.23919/CyCon49761.2020.9131733

Shukla, Shubhendu S. – Jaiswal, Vijay (2013): Applicability of Artificial Intelligence in Different Fields of Life. *International Journal of Scientific Engineering and Research*, 1(1), 28–35. Online: www.doi.org/10.70729/1130915

Taddy, Matthew Alan (2018): The Technological Elements of Artificial Intelligence. *NBER Working Paper,* w24301. Online: www.nber.org/system/files/working_papers/w24301/w24301.pdf

Zhang, Caiming – Lu, Yang (2021): Study on Artificial Intelligence: The State of the Art and Future Prospects. *Journal of Industrial Information Integration,* 23, 100224. Online: https://doi.org/10.1016/j.jii.2021.100224

Zhang, Zhimin et al. (2022): Artificial Intelligence in Cyber Security: Research Advances, Challenges, and Opportunities. *Artificial Intelligence Review,* 55, 1029–1053. Online: https://doi.org/10.1007/s10462-021-09976-0