31. évfolyam (2021) 3. szám 73–87. • DOI: 10.32562/mkk.2021.3.5

MŰSZAKI KATONAI KÖZLÖNY

Fehér András Tibor[1] – **Négyesi Imre**[2]

Mesterségesintelligencia-alapú kibertértámadási modellek

Artificial Intelligence–based Cyberattack Models

Az infokommunikációs rendszerek biztonságát fenyegető veszélyek egy egészen új generációját jelentik azok a kibertámadások, amelyeknél a támadók a mesterséges intelligencia erejét is felhasználják. Az alábbiakban néhány konkrét támadási modell bemutatását tűztük ki célul, hogy érzékeltessük a veszély nagyságát, és javaslatokkal szolgáljunk a veszély elhárításának megszervezéséhez.

Kulcsszavak: *mesterséges intelligencia, kibertér, kibertámadás, rajvírus, deeplocker, CAPTCHA*

A whole new generation of threats to the security of computer systems are cyberattacks in which attackers also use the power of artificial intelligence. In the following, we aim to present some specific attack models to illustrate the magnitude of the threat and provide suggestions for organising its prevention.

Keywords: *artificial intelligence, cyberspace, cyberattack, swarm virus, deeplocker, CAPTCHA*

[1] Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar, gyakorlati oktató, e-mail: feher.andras@uni-nke.hu

[2] Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar, egyetemi docens, e-mail: negyesi.imre@uni-nke.hu

1. Bevezetés

Bőséges szakirodalom lelhető fel mind a mesterséges intelligencia[3] (MI), mind a kibertéri műveletek[4] szakterületeihez kapcsolódóan külön-külön, még magyar nyelven is. A két terület közös halmazáról azonban magyar nyelven véleményünk szerint nem áll rendelkezésre elegendő publikáció az érdeklődők számára, ezért megpróbáltuk néhány tanulmányban áttekinteni a problémát. Egy írásban bemutattuk annak okait, hogy miért csak az MI-alapú kibervédelem lesz képes a jövő kihívásait teljesíteni.[5] Jelen kutatásban azonban a támadásokra fogunk koncentrálni, ezért először szükséges röviden összefoglalni (azt, amit egy másik, megjelenés alatt álló publikációnkban fejtünk ki), hogy a kibertámadásokban milyen lehetőségei vannak az MI-nek.

Először is, a technológia fejlődésével megnőtt a digitális támadási felület, a nagyobb felületen pedig az MI van előnyben. Újra kell gondolni a sérülékenységek eddigi kezelését is, hogy a sérülékenységi adatbázisokat ne használhassa egyetlen támadó sem az MI tanítására. Ijesztő veszély az is, hogy az IoT és az IIoT[6] eszközrendszerének rései révén támadott MI a fizikai valóságot is veszélyezteti. Ugyanis nem csupán az MI támadhat, hanem az MI és a gigantikus adatbázisfelhők (big data) léte maga is kihasználható, megszerzésük sokféle módon okozhat komoly károkat.[7] Mindezek mellett a digitális szélhámosság különböző fajtái (az úgynevezett *social engineering*) is szárnyakat kaptak, megtáltosodtak az MI révén, és ezek a támadások egyre kifinomultabbá és személyre szabottabbá tudnak válni. Mindezeken felül az MI megsokszorozza a kibertér eddigi aszimmetriáját, és az MI matematikájának fejlődése révén az erre alapozott támadások hatékonysága várhatóan jelentősen megnövekszik. Azonban ezeknél is nagyobb kihívást jelent, hogy a teljesen új, teljesen az MI-n alapuló támadó módszerek kialakulása várható.

Alább két példán keresztül is szemléltetjük ezt a problémát, az MI-n alapuló vírusok újszerűségét és hatékonyságát. Mindkét megoldás az MI-ben lévő rejtőzködési lehetőségek terén újszerű, de eltérő módon. Az egyik a DeepLocker, amely egy lopakodó, tökéletesen álcázott ruhájú, arcú és fegyverű mesterlövészre emlékeztet, aki biztos kézzel iktatja ki a kitűzött célt. A másik a cseh fejlesztésű rajvírus, amely a gyilkos darazsak egy olyan fajára hasonlít, amely képes az ellenük alkalmazott mérgező permetszerre immunissá válni a következő nemzedékében. Harmadik példánk nem vírust mutat be, hanem azt, hogy hogyan tesz elavulttá az MI (a képfelismerés) egy, a közelmúltig bevált robotvédelmi eszközt. Ezeket a lehetőségeket forráselemző módszerrel mutatjuk be, majd felvetünk néhány elgondolást a bemutatott példák gyakorlati használatának lehetőségeiről is. Végül pedig megfogalmazunk egy, az e szakterületet érintő jogszabályok és irányelvek végrehajtási utasításaiban felhasználható javaslatot, amely nem

---

[3] A technológiának nincs szabványos definíciója, számtalan komplementer meghatározás létezik, közös bennük, hogy az emberi gondolkodási képesség számítógépes utánzását (implementációját) célozza, lásd Négyesi Imre: A mesterséges intelligencia és a hadsereg I. *Hadtudományi Szemle,* 10. (2017), 2. 24–28.

[4] A szembenálló fél feletti kiberfölény megszerzésére és megtartására irányuló tevékenység. Haig Zsolt: *Információs műveletek a kibertérben.* Budapest, Dialóg Campus, 2018. 234.

[5] Fehér András Tibor: Mesterséges intelligencia a kibervédelemben. In Szelei Ildikó (szerk): *A hadtudomány aktuális kérdései napjainkban II. kötet.* Budapest, Ludovika Egyetemi Kiadó (megjelenés alatt).

[6] IoT = *Internet of Things*, a dolgok internete; IIot = *Industrial Internet of Things*, ipari dolgok internete.

[7] Zoltan Nyikes – Zoltan Rajnai: *Big data, as part of the critical infrastructure.* SISY: IEEE 13th International Symposium on Intelligent Systems and Informatics. New York, IEEE, 2015. 217–222.

csupán a Magyar Honvédség (MH) tekintetében alkalmazható, de minden nagy informatikai rendszernél is figyelembe vehető.

2. DeepLocker – a láthatatlan mesterlövész

Az IBM Research fejlesztette ki a DeepLockert. Laborkörülmények között hoztak létre egy olyan új malware[8]-fajtát, amely több nyílt forráskódú, tehát könnyen letölthető MI-modellt kombinál ismert malware-technikákkal. A cél az volt, hogy felkészülhessünk hasonló támadási helyzetekre. Ez az MI-alapú kibertámadási eszköz az úgynevezett kitérő támadások (lásd lentebb) új, erősen célzott fajtáját implementálja. Amikor a fejlesztés eredményét Marc Ph. Stoecklin és társai bemutatták a 2018-as Black Hat (USA) konferencián,[9] prezentációjukkal rá akarták irányítani a figyelmet arra, hogy az MI-alapú fenyegetések hamarosan megjelennek, valamint hogy a támadók képesek olyan rosszindulatú programokat létrehozni, amelyek megkerülhetik a manapság általánosan alkalmazott védekezési lehetőségeket.

Az IBM laborkártevője kétféle módon is kiaknázza az MI erejét: a cél azonosításához és a rejtőzködéshez. A DeepLockerben a cél azonosításához az MI-modell olyan triggereket (eseményindítókat) használ, mint például az arcfelismerés és a hangfelismerés, továbbá képes ez a vírus helymeghatározás alapján is aktiválódni, vagy akár a rendszer típusa alapján, de egy konkrét eszköz valamely azonosítója is lehet az aktiválódás kiváltója. Egy durva hasonlattal élve, a hagyományos kártevők úgy érik el a célszemélyt, hogy egy lángszóróval mindenki mást is letarolnak, a DeepLocker pedig úgy, mint egy rejtőzködő mesterlövész. Sőt, még hatékonyabban, mivel egyszerre több millió rendszert megfertőzhet anélkül, hogy valaki észrevenné – és csak akkor lép működésbe, ha a célokat ezek közül bármelyiken azonosítja. (Tehát ha az adott hangmintát érzékeli, és/vagy ha a fertőzött eszköz egy adott helyszínre kerül, és/vagy ha mondjuk éjszaka van stb.) Ezek alapján világos, hogy igen jelentős fenyegetés egy ennyire célzott módszer mind állami-katonai, mind céges szempontból.

A DeepLocker egyik fő újdonsága a kitérés (elrejtőzés) eddiginél hatékonyabb módszerében van. Ennek megértéséhez pár szóban tekintsük át, mit is jelent ez a kitérés, honnan fejlődött a mai állapotáig. A kitérőtechnikák olyan módszerek, amelyeket a számítógépes támadások használnak a rosszindulatú tevékenységek elrejtésére. A támadások hagyományosan különböző kitérőtechnikákat használnak a biztonsági védelmi rétegek (behatolásmegelőző rendszerek, biztonsági webes átjárók, homokozórendszerek stb.) elkerülésére. A támadó alkalmazhat egy vagy több kitérőtechnikát (például a tartománygeneráló algoritmust, a lassú kommunikációt vagy a véletlenszerű kérési útvonal technikáit).[10]

Már az 1980-as évek vírusainál elkezdték használni a kitérőtechnikákat. Az 1990-es évektől jelent meg a kód kártékony részének titkosítása, ami lehetetlenné tette a kódrészletek keresésének hagyományos, összehasonlításos módszerét. (Ez ellen hozták létre a biztonsági

[8] A malware a *malicious software* rövidítése, magyarul rosszindulatú számítógépes program.

[9] Marc Ph. Stoecklin – Jang Jiyong – Dhilung Kirat: DeepLocker, How AI can power a stealthy new breed of malware. *Security Intelligence,* 2018.

[10] Radware Malware Protection Service: *Evasive Attack Techniques Overview.* Radware, 2018.

oldalon a virtuális környezeteket, ahol következmény nélkül el lehet érni, hogy a kártevő aktiválódjon. A virtuális védelmi környezet, más néven *sandbox* („homokozó") egy védelmi módszer arra, hogy „kiugrasszuk a nyulat a bokorból": a vírust vizsgálat céljára ebben a zárt környezetben aktiváljuk, így igazi rendszerünkben nem képes kárt okozni.) A 2000-es évekre a vírusok már képessé váltak érzékelni, hogy speciális virtuális környezetben (homokozóban) futnak-e, vagy éles rendszeren. Egy 2018. májusi tanulmány[11] kimutatta, hogy az elemzett malware-minták 98%-a kitérőtechnikákat alkalmaz. Viszont az IT-biztonság fejlődése ezt a módszert kezdi felszámolni azzal, hogy homokozó helyett úgynevezett „csupasz fém" környezetben tesztelnek (ahol a kártevő nem képes rájönni, hogy tesztkörnyezetben van).[12]

Így a támadók újabb stratégia felé hajlanak: a támadás *célzásával* érik el, hogy kártevőjük rejtve maradjon. A rosszindulatú kód csak akkor töltődik le vagy csomagolódik ki, tehát csak akkor hajtódik végre, ha a célpontot „tisztának" találja. Ennek a „mesterlövész" módszernek egy korai (2010-es), igen hírhedett példája a Stuxnet féreg, amelyet úgy programoztak, hogy csak egy adott gyártótól származó specifikus hardver- és szoftverkonfiguráció jelenlétében aktiválódjon.[13] Csakhogy ehhez is szükséges valami trigger, a védekező oldal pedig ezentúl ennek felismerére koncentrált. (Vagyis a védelmi program automatikusan rákeres a „ha ez történik, akkor hajtsd végre ezt" típusú kódsorokra, azt megtalálva jelez, a szakemberek pedig megtalálhatják a probléma forrását.)

Visszatérve a DeepLockerre, ennél a kártevőnél nem lehet ezt a triggert megtalálni, mivel ugyanúgy titkosítva van, mint a kód kártevő része. Az MI használata teszi szinte lehetetlenné már a „kiváltó körülmények" meglétének felismerését is. Ezt egy mély neurális hálózat (DNN[14]) alkalmazásával éri el.

Három fő összetevőt kell tehát alaposan elrejteni: nem csupán a támadás úgynevezett „hasznos terhét"[15], mint korábban, hanem az indító feltételt (feltételeket) és a feltétel jellegét (típusát) is. Technikailag ezért a DeepLocker három réteggel fedi el magát (lásd 1. ábra):

1. Az első réteg elrejti, hogy *mi* váltja ki a támadást (arc, hang, hely, rendszer?).
   A réteg feladata a cél *típusának* elrejtése (milyen jellegű a támadás célja: személy, szervezet, hardver, szoftver).
2. A második elrejti, hogy konkrétan *kire* irányul a támadás.
   A réteg feladata a konkrét cél elrejtése (pontosan *ki* a támadás célja, vagy *hol* következzen be, netán minden X típusú gépet tönkre kell tennie, vagy csak egy konkrét eszközt stb).
3. A harmadik réteg elrejti, hogy *mi is fog történni,* ha bekövetkezik a támadás.
   A réteg feladata a kártevő titkosítása, vagyis annak álcázása, *hogyan* hajtódik végre a támadás.

---

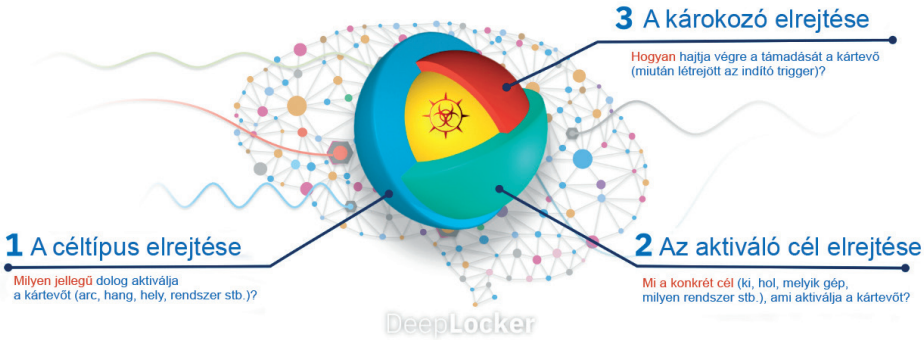
[11] Siggi Stefnisson: Evasive malware now a commodity. *Security Week,* 2018.

[12] Dhilung Kirat – Giovanni Vigna – Christopher Kruegel: BareBox: efficient malware analysis on bare-metal. *Proceedings of the 27th Annual Computer Security Applications Conference.* Orlando, 2011. 403–412.

[13] Ezek a konkrét rendszerek a Stuxnet esetében iráni urándúsítók voltak, tehát egy pontosan meghatározott ipari vezérlőrendszer.

[14] *Deep Neural Network.*

[15] Egy vírus esetében a hasznos teher nyilván valami kártékony kód.



1. ábra. A DeepLocker rétegei

Forrás: a szerzők szerkesztése az idézett Stocklin–Jiyong–Kirat-cikkben közölt ábra alapján

A DeepLockerben az MI-modell végzi el ezt az álcázást, maga a neurális hálózat egy feketedobozként rejti el a három kártékony réteget. Csak akkor állítja elő az „indítókulcsot" (triggert), amikor minden elvárt körülmény együtt áll – ám akkor már késő detektálni. Ráadásul olyan sokféle attribútumot használhat a cél azonosításához, hogy a kódelemzőknek gyakorlatilag még az MI-modell ismeretében is lehetetlen kitalálni, hogy melyek a lehetséges kiváltási körülmények: valaki arca vagy más vizuális nyomok, hely, rendszerinformáció, vagy több dolog együttesen? Tehát a szokásos kérdések is megválaszolatlanok maradnak: mit fog egyáltalán aktiválni a támadás, és hol lehet az elrejtve.

A kutatócsoport a fentiek demonstrálására az ismert WannaCry vírust (zsarolóvírust) álcázta a DeepLockerrel, egy jóindulatú videókonferencia-alkalmazásba rejtve el a kártevőt. Az antivírusprogramok még homokozók használatával[16] sem vették észre a fertőzést.

Kiváltó körülményként az MI-modellt úgy képezték ki, hogy felismerje egy adott személy arcát, és csak ennek hatására bontsa ki és indítsa be a vírust. Képzeljék el, hogy ezt a videókonferencia-alkalmazást több millió ember tölti le, ami manapság sok nyilvános platformon valószínűsíthető forgatókönyv. Indításkor az alkalmazás rejtett módon fényképezőgép-pillanatképeket adagol a beágyazott MI-modellbe, de egyébként minden felhasználó számára normálisan viselkedik – kivéve a kívánt célszemélyt. Amikor az áldozat a számítógép elé ül, és használja az alkalmazást, az arcát észlelve (amely az előprogramozott kulcs volt a feloldásához) a rosszindulatú hasznos teher titokban végrehajtódik.

Noha a DeepLockerhez hasonló malware-programot a mai napig nem detektáltak, a készítéséhez használt MI-eszközök nyilvánosan elérhetők, ahogy az alkalmazott malware-technikák is. Csak idő kérdése, mikor jön hír ilyen akcióról. Sőt a vázolt hatékony rejtőzködés miatt akár az is lehetséges, hogy ilyen támadás akár most is folyamatban van.

[16] A dokumentáció nem említi, de a technológia jellegéből adódóan képes lehet a „csupasz fém" környezetek átverésére is.

3. Támadás öngyógyító rajintelligenciával

Nulladik Neumann-elvnek vehetnénk fel, hogy „másoljuk le az élő szervezetek működési elveit". A híres magyar tudós is tanulmányozta az emberi agy működését, azt vizsgálva, hogyan használhatja fel azt számítógépek tervezéséhez. Később az első MI-modelleket is az emberi agy idegsejtjeinek kapcsolatrendszere ihlette. Azonban a műszaki tudományok nem csupán az agy működéséből próbálnak ötleteket meríteni, a biológia számtalan felfedezését sikerült már felhasználni, sőt egy új tudomány, a bionika kifejezetten az ilyen lehetőségek számbavételére koncentrál. A mesterséges intelligencia fejlődésével ezek az ötletek „virágba borultak", és az MI újabb és újabb irányzatai nyílnak meg ily módon. Ezen belül az úgynevezett populációs modellek területe etológiai megfigyeléseken alapul, a hatékonyan működő állatközösségek világából merít.

Az így ihletett MI-irányzat ijesztően ígéretes. A populációs modellek közül a „rajintelligencia" egy olyan új paradigma, amelynek egészen biztos, hogy óriási jövője van. Elsősorban optimalizációs feladatok megoldására kínálnak az eddigieknél sokkal hatékonyabb megoldást. A hangyaboly-intelligenciát[17] alapvetően az útvonal-optimalizációs problémákkal kapcsolatban fejlesztik, a méhraj-intelligenciát[18] pedig a naperőművek optimalizálására. Megemlíthetjük még a mesterséges halrajalgoritmust[19] vagy a szentjánosbogarak (fénylegyek) párzási motivációját használó modellt,[20] de számos egyéb ígéretes kutatás is folyik.[21] Itt azonban csupán arra koncentrálunk, hogy a rajintelligencia rendkívül alkalmas kibertámadások elvégzésére is.

A raji intelligencia lényege, hogy nem sejtekből épül fel, mint az élő szervezetek vagy a többi MI – hanem egyedekből áll, amelyek önmagukban is működő entitások. Ezek az entitások együtt, közösségben sokkal sikeresebben és hatékonyabban képesek a környezeti kihívásoknak megfelelni. Ugyanez a célja ezeknek az informatikai modelleknek is, hogy az entitások egymást segítsék „tapasztalataikkal", egymástól tanuljanak. A közös tapasztalatokból csiszolódik ki a cél elérésének leghatékonyabb módja. A raj hatékonysága azért is nagy, mert lényegtelen, melyik entitás ér el eredményt, ha valamelyik eléri (például az új táplálékforrást), akkor az egész közösség elérte. Sőt ezek az entitások utódjaikban akár saját (genetikai vagy program-) kód-

---

17 Lubomir Sikora: *Swarm Malware – Hejnový virus*. Diplomamunka. Osztravai Műszaki Egyetem, 2017.

18 Dervis Karaboga – Bahriye Akay: A survey: Algorithms simulating bee swarm intelligence. *Artificial Intelligence Review,* 31. (2009), 1–4. 61–85.

19 Kuan-Cheng Lin – Sih-Yang Chen – Jason C. Hun: Botnet detection using support vector machines with artificial fish swarm algorithm. *Journal of Applied Mathematics (Hindawi),* (2014). 1–9.

20 Kása Richárd: *Döntéselmélet*. Diplomamunka. Miskolc, Miskolci Egyetem, 2014.

21 Az érdekesség kedvéért például a pillangóalgoritmus – Iztok Fister et alii: A comprehensive review of firefly algorithms. *Swarm and Evolutionary Computation,* 13. (2013). 34–46.; a kakukk tojásrakása a Kakukk-keresésben – Xin-She Yang: *Nature-inspired metaheuristic algorithms.* Cambridge, Luniver Press, 2010. 105–116. A farkasvadászat a Szürke Farkas Optimalizálóban – Faris Hossam et alii: Grey wolf optimizer: a review of recent variants and applications. *Neural Computing and Applications,* 30. (2018), 2. 413–435.; valamint érdekes ezek rendszerezése is: S. Arockia Panimalar: Nature inspired metaheuristic algorithms. *International Research Journal of Engineering and Technology (IRJET),* 4. (2017), 10. 306–309.

jukat is módosítják, optimálisabbá teszik a közösség tapasztalatai alapján. A természetben is megfigyelhető az ilyen alkalmazkodás, amikor néhány generáció alatt az adott faj egyedeinek képességei valami új helyzethez alkalmazkodnak, például a táplálék változásával átalakul a csőrük, a hőmérséklettel összefüggésben a szőrzetük, vagy egyes belső szerveik erősebbek lesznek, mint más populációban. Az ilyen átalakulás nem a falkavezértől vagy hangyakirálynőtől függ, sok állatfajnál nincs is ilyen vezér. Tehát ennek számítógépes implementációja egy teljesen elosztott rendszer lesz, amely a jelenlegi központi vezérlésű informatikai módszerekkel szemben sokkal életképesebbnek tűnik.

Amikor ezt az elvet kibertámadásokra használják, akkor a környezetükhöz alkalmazkodó víruskódok jönnek létre. A különféle hátráltató tényezőket a vírusraj entitásai közlik egymással, és a szükséges módosulásokat maga az MI hozza létre. Ráadásul ez a módszer képes a rajintelligencia közös tudását felhasználni a kártékony kódok elrejtéséhez (mimikrijéhez) is. Tehát a támadó kód, mint egy kaméleon, az adott környezetnek megfelelő legoptimálisabb technikát alakítja ki az ellen, hogy megtalálják.

Ezek alapján már világos, hogy egy ilyen vírusrajjal hatékonyan lehet tömeges (robusztus) kárt okozni egy vagy sok rendszerben, hiszen:

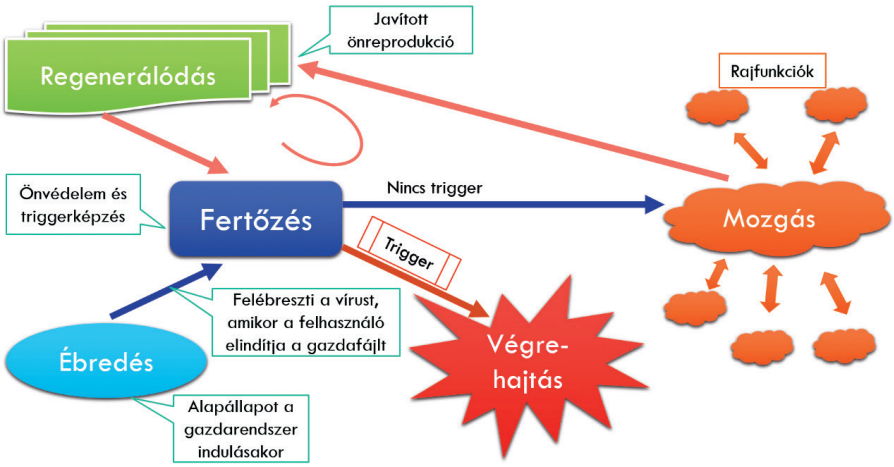
- a rajnak nincs központi vezérlőegysége;
- a rajnak lehet kollektív emlékezete, megoszthatja tudását valamilyen stratégiáról (sikeres/sikertelen), és „tanulhat belőle";
- így a raj egyfajta közösségi és kommunikációs hálózatot hoz létre, és minden tag különféle módon kommunikálhat másokkal (az információ átadódhat közvetlenül, kiválasztott egyéneken keresztül, egyénről alpopulációra stb.);
- a raj alkalmazkodási képességét rejtőzködésre lehet hasznosítani.

Tehát ha nagy nehezen észre is vesz a védelmi rendszer néhány víruspéldányt, azokat hiába távolítja el, mert az nem érinti a teljes raj működését. Nyilván egy ilyen támadás korábbi más, már bevált rosszindulatú technológiák (férgek, malware-ek) módosításával készül, azok ártó tulajdonságait nagyíthatja fel óriási mértékben.

Egy cseh kutatócsapat az osztravai egyetemen Ivan Zelinka vezetésével publikált is egy olyan vírusstruktúrát, amely ilyen elven működik.[22] Laboratóriumukban kísérleti mintát hoztak létre egy rajmalware megvalósítására. Konkrétan egy „klasszikus" botnet-[23] (nem féreg, nem trójai) vírusból indultak ki. Ezt alakították át egy önjavító-önreplikáló kártevőstruktúrára. A célhoz három technológiát ötvöztek: a számítógépes vírus alapelveit, a raj intelligenciáját és a komplex hálózati elemzési képességet. A modell egy néhány állapotból álló véges automata, az alábbiakban ennek lényegét vázoljuk. A kísérleteik során használt vírus állapotainak szerkezete a 2. ábrán látható.

[22] Ivan Zelinka et alii: Swarm virus – Next-generation virus and antivirus paradigm. *Swarm and Evolutionary Computation,* 43. (2018). 207–224.

[23] Botnet – a „robot network" összevonása. A támadó vírussal fertőzött számítógépek seregét használva támad.



2. ábra. A cseh rajvírusmodell

Forrás: a szerzők szerkesztése Zelinka (2018) i. m. 13. ábra alapján

A vírus entitásainak fontosabb állapotai a következők:

1. Felébredési állapot: Ez az állapot akkor aktív, ha a többi víruspéldány még nem működik. A felhasználó által végrehajtott gazdafájl jelzésére ébred fel.
2. Fertőzés állapota: Ez részben a végrehajtási állapothoz kapcsolódik, részben pedig egy önvédelmi funkció. Tehát egyrészt itt jön létre a trigger, amely majd aktiválja a hasznos terhet (kártékony kódot). Ezáltal a vírus a végrehajtási állapotba kerül. Másrészt ez az állapot egy önvédelmi funkció. Abban az esetben, amikor az antivírus felismer néhány víruspéldányt, és karanténba küldi vagy törli őket, ez az állapot idézi elő újabb víruspéldány generálását a gyógyulási állapot segítségével, amelynek eredményeként fenntartható az állandó, optimális víruslétszám.
3. Gyógyulási (regenerálódási)[24] állapot: Ennek a műveletnek köszönhető, hogy a raj számossága állandó. Itt a vírus módosítja (megtisztítja) régi példányát a mozgás állapot segítségével, mielőtt egy másik gazdagépre költözik.
4. Mozgás állapot: Ebben az állapotban hajtja végre a rajelveket, itt zajlik a tapasztalatok generálása és átvétele.
5. Végrehajtási állapot: Ez a vírus „robbanótöltete", ennek van látható (kártékony) hatása. De csak akkor jön működésbe, ha egy trigger aktiválva van – különben figyelmen kívül hagyja, és „lopakodó módban" maradva a mozgás állapotba kerül.

A raj egy adott állapotban kezdi meg futtatását azon állapot alapján, amelyben egy víruspéldány már elindult. Ha ez volt az első végrehajtás az operációs rendszer indítása után, akkor a végrehajtás felébredési állapotban kezdődik. Ha a víruspéldányt más víruspéldány felébresztette,

[24] A modell *heal* (gyógyulás) állapotnak hívja, pedig a regenerálódás szó eredeti jelentése sokkal jobban utalna az állapot lényegére, hogy „újjászületik" a kód, hiszen tényleg új (módosult) kód jön létre.

akkor a fertőzés állapotban kell futtatnia. Ha egy létező víruspéldány a mozgás állapotában tapasztalatokat adott vagy kapott (tehát a rajtudás érvényesült), akkor a gyógyulási (regenerálódási) állapotba kerül, átalakul, és majd már más módon fertőz. Nyilvánvaló, hogy bonyolultabb vírusviselkedés is létrehozható, de ez is jól példázza a módszer lényegi újdonságát.

Sajnos a rajintelligencia használati módjának alaposabb kifejtésére terjedelmi korlátok miatt nincs lehetőség, de még két dolgot meg kell itt említenünk, ami nem közvetlenül kapcsolódik a kibertérhez, azonban katonai szempontból fontos. Az egyik, hogy a harci robotok (drónok, harckocsik, hajók) vezérlése is megvalósítható rajintelligenciával, ami megsokszorozza azt a harcértéket, amely pusztán a raj létszámából adódna. A másik pedig, hogy a rajintelligencia a pszichológiai hadviselés terén is fegyverré válhat. Ha az emberekből és gépekből álló tömeg hatékonyan képes választási eredményeket jósolni, akkor ezt a jóslatot módosítani is képes lehet úgy, hogy megmondja, mit kell tenni, hogy másképp alakuljon az a bizonyos végeredmény. A módszerre jó példa az év embere választás megjóslásának elemzése: Egy UNU nevű rendszer, amelyben az MI és sok ember véleménye együtt dolgozik, nagyon pontos közvéleményjóslásra volt képes.[25] (Megjegyzendő, hogy az Indiában fejlesztett MogIA nevű rendszer, amely nem rajintelligenciát használ, az amerikai elnökválasztást is többször jól megjósolta[26] – tehát más modellek is hatékonyak ilyen téren.)

4. A CAPTCHA-védelem áttörése az MI segítségével

A CAPTCHA[27] egy máig használt módszer arra, hogy a webes felületeket megvédjék azoktól a támadásoktól, amelyek automatikusan próbálnak meg fiókokat létrehozni, hozzászólni a fórumokhoz (például reklámokkal szórják teli a kommenteket), tehát kéretlen tartalmakkal zavarják a portál működését. Ehhez az embernek kell bizonyítania, hogy ő valóban ember: olyan feladványt kap, amit gép nem képes megfejteni. Körülbelül 1997-től 2007-ig, tehát 10 éven át szöveges CAPTCHA-védelmet használtak, amelyben a felhasználónak egy eltorzított szöveg karaktereit kell helyesen megadnia, vagy valamilyen egyszerű (például matematikai) kérdésre kell válaszolnia.

Az alábbi példán keresztül jól be tudjuk mutatni a klasszikus, szövegtorzításos CAPTCHA-védelmek feltörhetőségét. A kiberbűnözők már régen képesek erre, ezt saját munkájukban jelen cikk szerzői is megtapasztalhatták. Az általuk üzemeltetett Drupal-alapú portálon két év zavartalan működés után le kellett védeniük a hozzászólásokat CAPTCHA-val, de pár év múlva (körülbelül 2009-ben) új, még erősebb reklámkomment-támadás érte az oldalt. Ha úgy állították be a szöveg torzítását, hogy az ember számára mindig megfejthető legyen, akkor özönlöttek a reklámhozzászólások is. Ha viszont több homályosító effektet, képpontokból és vonalakból álló zavarásokat adtak hozzá, akkor a reklámposztok ugyan megszűntek, de emberként sem

[25] Dom Galeon: A swarm intelligence correctly predicted TIME's Person of the Year. *Futurism,* 2017.

[26] Arjun Kharpal: Trump will win the election and is more popular than Obama in 2008, AI system finds. *CNBC,* 2016.

[27] *Completely Automated Public Turing test to tell Computers and Humans Apart* vagyis egy teljesen automatizált nyilvános Turing-teszt a számítógép és az ember megkülönböztetésére.

lehetett mindig kitalálni, mi is a megfejtése a képrejtvénynek, és igen nehéz lett belépni az oldalra (ami nem felhasználóbarát dolog).

2017 szeptemberében nyilvánossá is vált, hogyan lehet ilyen támadást megvalósítani. Adrian Rosenbrock nem csupán publikált egy ilyen módszert könyve egyik fejezetében,[28] de python-kódokat is mellékelt ehhez. Egy bizonyos webhely CAPTCHA-védelmét törte fel az etikus hacker úgy, hogy nagy mennyiségű CAPTCHA-mintakép letöltésével képezett ki egy mélytanuló modellt. Nem sokkal később egy kínai–angol egyetemi együttműködésben készült tanulmány általánosabb kiberfegyversémát mutatott be, sokféle CAPTCHA-védelmen tesztelve azt. Ezt a példát vizsgájuk meg alaposabban: hogy hogyan törte át a tesztlaborban a különböző CAPTCHA-típusú védelmeket az ellene bevetett mesterséges intelligencia.[29]

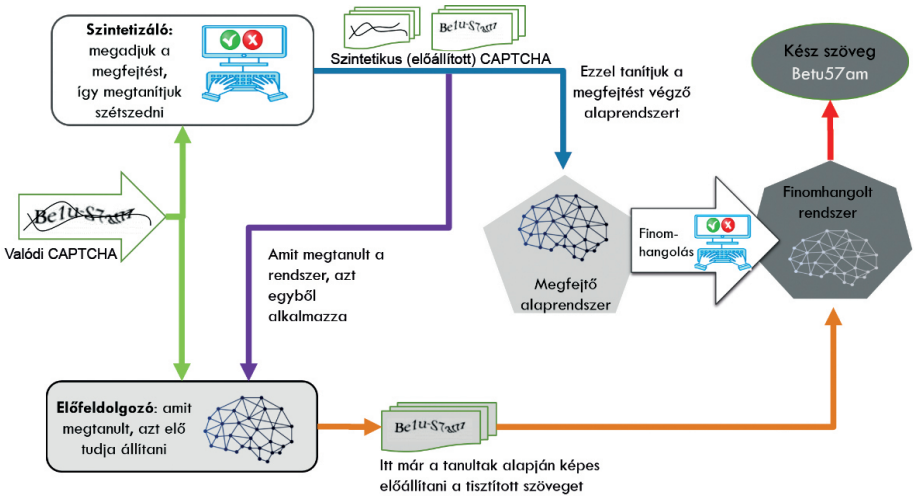
Nem egy tökéletes, minden esetben működő CAPTCHA-törő rendszer elkészítése volt a cél. Csupán azt vizsgálták, hogy meg lehet-e tanítani az erre létrehozott MI-t úgy, hogy nagyobb eséllyel tudja helyes szövegként értelmezni a torzított szöveget, mint amilyen eséllyel sikertelen marad. Ez a cél megvalósult. Minden vizsgált rendszernél sikerült több-kevesebb lépésben elérni, hogy az esetek legalább 60%-ában képes legyen a helyes karakterek visszaadására. Sőt, több rendszerrel szemben sikerült a 100% elérése. A kutatásban a világ 32 (+1) valaha is legnépszerűbb portáljának szövegtorzító eljárását, annak felismerhetőségét vizsgálták. 20 ezer különféle típusú CAPTCHA-szövegképpel tanították a rendszert, figyelembe véve a portálokon tapasztalható torzítási módszereket.

A folyamat röviden így foglalható össze (lásd a 3. ábrán):

1. A szintetizáló modul megpróbálja utánozni a kapott valódi CAPTCHA-típust. Kap egy valódi Captchát, megmondjuk neki a megfejtést, és próbál hasonlót generálni. Először addig próbálgatja torzítani a kapott betűket, míg azok olyanok nem lesznek, mint a kapott, torzított képen. A modul ezáltal egyre inkább „rájön" arra, *hogyan* keletkezett a kép, és képes az eredetihez hasonló, szintetikus CAPTCHA-kat előállítani. Ezt a tudását egyrészt átadja egy előfeldolgozó modellnek, másrészt CAPTCHA-képeket szolgáltat a megfejtő alaprendszer tanításához.
2. Az előfeldolgozó MI-modellje a szintetizálótól kapott algoritmus segítségével fejlődik. Már emberi tanítás nélkül képes lesz a kapott valódi CAPTCHA-ban elkülöníteni a pont,- felhő-, vonal- és egyéb torzításokat, valamint megállapítani a betűtípust. Az így kapott eredmény a rendszer finomhangolásánál használható fel.
3. A szintetizáló és az előfeldolgozó nagyszámú képet generál. A szintetizáló képeivel megtanítjuk a megfejtő alaprendszert, hogyan torzítsa a képszöveget úgy, hogy utána majd képes legyen felismerni.
4. Még finomhangolásra is szükség van, mivel a megfejtő alaprendszer egy tisztább, de még torz szöveget ad eredményül. Ehhez használjuk az előfeldolgozó modelltől kapott képeket, és azokkal addig taníthatjuk (finomhangoljuk) rendszerünket, míg a kívánt 50%

[28] Adrian Rosebrock: *Deep Learning for Computer Vision with Python*. Philadelphia, PyImageSearch, 2017. 287–307.
[29] Guixin Ye – Zhanyong Tang et alii: Yet another text captcha solver: A generative adversarial network based approach. *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security.* 2018. 332–348.

feletti felismerési rátát el nem érjük. Azzal, hogy a támadásnak nagyobb esélye van arra, hogy áttöri a védelmet, mint arra, hogy nem töri át, bebizonyítottuk, hogy a módszer nem alkalmas a védelemre.



3. ábra. CAPTCHA-feltörés MI-vel

Forrás: a szerzők szerkesztése Zhanyong (2018) i. m. 2. ábra alapján

A régebbi oldalak ilyen védelmét alig több mint 10 finomhangolási lépés után 100%-ban áttörték. A Yahoo! eredményei a legjobbak, de a támadó rendszer ott is átlépte az 50%-os határt 19 finomhangolási lépés után.[30] Tehát (bár néhol nehezebben és még tökéletlenül) már ez a prototípus MI is elbánt minden betűképtorzító védelemmel. Levonhatjuk a tanulságot: ez egyértelműen a képszövegfelismerés-alapú robotellenes védelmi technika végét jelenti.

A példa szemlélteti és előrevetíti azt is, hogy új alapokra kell helyezni sok más védelmi megoldást is a közeljövőben.

A teljesség kedvéért azonban megjegyezzük, hogy ez az új alapokra helyezés már régen zajlik, és a CAPTCHA egyelőre beláthatatlan ideig képes lesz kiszűrni a robotokat. A fejlettebb CAPTCHA-technikákat ugyanis nem vizsgálta ez a módszer, csak a szövegtorzítást. Mikorra fejlődnek fel olyan szintre a támadó MI-k, hogy képesek legyenek megmondani, például „melyik képen nincs ház"? Ha ezt majd tudni fogja, akkor ki lehet találni újabb és újabb ilyen feladatokat. Kérhetünk egérműveleteket válaszként, hiszen egérmozdulat-utánzásra egyelőre nem képesek az offenzív rendszerek. (Erre a legjobb példa, amit láttam, hogy dobozokat kell sorrendbe pakolni drag&drop technikával.)

A portálok üzemeltetői tehát még jó néhány éven át használhatnak olcsó és jó CAPTCHA-védelmet az automatizált, nem célirányos támadások ellen.

[30] Roberto Iriondo: Breaking CAPTCHA using machine learning in 0.05 seconds. *Towards Ai,* 2018.

Viszont ha ilyen ütemben felfejlődik az MI, és már mindent képes megoldani, eljutunk oda, hogy a CAPTCHA-technika lehet a Turing-teszt egyik utódja. Akkor definiálható lesz egy olyan „szuper-CAPTCHA", amely az adott rendszerről meg tudja mondani, hogy ember-e – mégpedig oly módon, hogy a feladvány ember számára túl nehéz lesz, tehát ember nem lesz képes megoldani, viszont az MI igen, így leleplezi magát.[31]

5. Lehetséges támadások az ismertetett technológiákkal

A fentebb elemzett konkrét támadó megoldások rávilágítottak arra, hogy a technológiában rejlő potenciálok már nem csupán végtelenek, mint mostanáig – a támadók lehetőségei az MI használatával, immár „végtelenszer végtelenek". Az újdonságokat a támadók kombinálhatják bevált technikákkal. Alább néhány gondolatindító felvetést fogalmazunk meg arról, hogy néhány ismert támadási technika hogyan erősödhet meg az MI használatával, az eddig bemutatott ötletekből merítve.

Az említett rajintelligencia az elosztott rendszer remek megvalósítása, tehát használata elosztott támadásokra, ezen belül az elosztott túlterhelésekre (DDoS)[32] kézenfekvő.[33] Ismert technika, hogy valami időzár alapján egyszerre aktiválódnak a DDoS-t kiváltó zombivírusok, de a fentebb elemzett modellek ötleteit is alkalmazva, egy ilyen támadásnál az MI segítségével sokkal jobban álcáznák a támadást, ahogyan erre a lehetőségre a DeepLockernél rávilágítottunk. Olyasmire lehetne számítani, hogy egy fejlett tartós támadás (APT)[34] vagy egyéb negyedik generációs infokommunikációs támadás[35] részeként valósulna meg egy MI-alapú DDoS. Egy rajvírusnak például megadhatók olyan triggerek, amelyek egy bizonyos fertőzöttségi szintnél jeleznek. Ráadásul ez a szint lehet külső-belső: a rendszeren kívül százezer kliens, a rendszeren belül minden szerver és munkaállomás – főleg ez utóbbi által lényegesen nagyobb a hatás, mint ha a támadást felfedezik egy-egy részrendszernél, és ott eliminálják a fertőzést. Tehát nem csupán a szerverek fagynának le, hanem a beavatkozáshoz használható terminálokat is használhatatlanná tennék, sőt a helyiséget vagy épületet is lezárhatnák, vagy minden ajtót lezárhatatlanná tehetnének.

Másik példaként gondoljuk át, hogy milyen valószínű olyan katonai kártevők fejlesztése, amelyek az ellenség vezetés-irányítási rendszereit, infokommunikációs eszközeit, járműveit vagy egyéb harci technikáit fertőzik meg. Így azokat kellő időben használhatatlanná tennék, vagy átvennék fölöttük az irányítást. Ennek eredményeképpen a szuperfejlett technológiák szuperdrága fémhalmazzá válnának, vagy akár a saját erők ellen fordulhatnának. A fentebb vázolt MI-alapú rejtőzködési technikák egészen bizonyos, hogy használhatók lennének ilyen célokra. Ezek segít-

---

31 Roman V. Yampolskiy: AI-complete CAPTCHAs as zero knowledge proofs of access to an artificially intelligent system. *International Scholarly Research Notices Artificial Intelligence,* (2012). 1–6.

32 *Distributed Denial of Service*. A feldolgozhatatlan mennyiségű kérés sok helyről érkezik a szerverre.

33 Például www.networkworld.com/article/3289108/the-rise-of-artificial-intelligence-ddos-attacks.html

34 *Advanced Persistent Threat,* észrevétlenül, hosszú időn keresztül zajló, akár többlépcsős rendszertámadás. Lásd Kovács László: *A kibertér védelme*, Budapest, Dialóg Campus, 2018. 141–166.

35 Jobbágy Szabolcs: A negyedik generációs hadviselés infokommunikációs aspektusai – fogalmi kitekintő. *Hadmérnök,* 12. (2017), 1. 203–213.

ségével bármely rendszerelem (fegyver, gép, irányítóközpont), amelybe számítógépet építettek, nyomtalanul megfertőzhető lenne. A fertőzés azért is nyomtalan marad, mivel a triggerek, amelyek aktiválják, lehetnek olyan tényezők együttesen, amelyek talán soha nem aktiválódnak. Például, ha x darab megfertőzött ellenséges eszköz egyszerre lépi át a fertőzést elhelyező ország határát, és valami egyéb megerősítő jelzés is érkezik. Ez a megerősítő jel lehet egy adott frekvencián sugárzott jelsorozat, vagy el lehet rejteni akár egy (várhatóan nem zavart) zenés civil rádióban úgy, hogy három adott zeneszámot egymás után játszanak le. Trigger lehet a támadási alakzat felvétele is, a lehetőségek határtalanul finomíthatók, beépíthető számtalan biztonsági lépcső is.

6. Következtetések

Nem szeretnénk sok ötletet adni az esetleges támadóknak, ezért további példák helyett inkább arra a kérdésre adunk választ, hogy mennyi időnk van felkészülni erre a veszélyre és megtenni a megfelelő ellenlépéseket. Ehhez keretet ad hazánk nemzeti biztonsági stratégiája,[36] amely említi a problémát, ám az elhárításához szükséges konkrét lépések rögzítése nem ilyen jogszabályok szintjén történik. E mellett Magyarország MI-stratégiája is foglalkozik több pontban a kérdéssel, kijelöli a katonai nemzetbiztonsági célú MI-képességek fejlesztéséért felelős szervezetet (a Katonai Nemzetbiztonsági Szolgálatot),[37] tehát a helyzet biztató. Az MH hadrendjében egyelőre nem létezik kibertámadásra szakosodott alegység, ezért a védelem szempontjából vizsgáljuk meg a kérdést. Látnunk kell, hogy a bemutatott példák egyelőre csak demonstrációk, tehát éles környezetben számos probléma adódhat a támadó oldaláról, amelyek miatt a leírt látványos hatás mégsem következik be. Az MH felhasználói és informatikai állományában a biztonságtudatosság az utóbbi időben jelentősen nőtt, a kibervédelmi eszközpark nem marad el a hasonló erőforrásokkal rendelkező szövetségeseinké mögött – elkerülhetetlen azonban néhány éven belül az MI-alapú kibervédelemre áttérni. Alább javaslatot teszünk egy lehetséges forgatókönyvre.

Első körben megoldást jelent, ha a fejlesztések jövőben tervezett ütemeiben olyan termékeket szerzünk be (akár ugyanattól a hardver- vagy/és szoftvergyártótól), amelyek frissítéseihez a cég MI-t vesz igénybe. A következő ütemben azonban szükségessé fog válni az ilyen rendszerek szervezetre szabott tanítása, amelyhez olyan speciálisan szakképzett humán erőforrás szükséges, amelynek képzése hazánkban még sehol sem kezdődött meg. (Kiberbiztonsági és mesterségesintelligencia-képzések zajlanak, azonban egy MI-alapú kibervédelem folyamatos tanításához a kettő együttes ismerete szükséges.) A katonai üzemeltető állomány akkor vonható be ilyen feladatba, ha a gyártók az ilyen rendszerek tanítását leegyszerűsítik annyira, hogy az operátori szinten is használható legyen – ez azonban egyelőre nincs a látóhatáron. Egyelőre tehát nem vagyunk elkésve, bízhatunk abban, hogy az elmúlt években tapasztalható gyors fejlődés lendületével az ilyen új generációs kibervédelem is idejében megvalósul mind a védelmi szféra, mind pedig az állami szféra szintjén.

---

[36] 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról, 160–162. pont. 106.

[37] Mesterséges Intelligencia Koalíció: *Magyarország Mesterséges Intelligencia Stratégiája, 2020–2030.* Budapest, Innovációs és Technológiai Minisztérium, 2020. 52.

Felhasznált irodalom

Dervis, Karaboga – Bahriye Akay: A survey: Algorithms simulating bee swarm intelligence. *Artificial Intelligence Review,* 31. (2009), 1–4. 61–65. Online: https://doi.org/10.1007/s10462-009-9127-4

Fehér András Tibor: Mesterséges intelligencia a kibervédelemben. In Szelei Ildikó (szerk.): *A hadtudomány aktuális kérdései napjainkban. II. kötet.* Budapest, Ludovika Egyetemi Kiadó (megjelenés alatt).

Fister, Iztok – Xin-She Yang – Janez Brest: A comprehensive review of firefly algorithms. *Swarm and Evolutionary Computation,* 13. (2013). 34–46. Online: https://doi.org/10.1016/j.swevo.2013.06.001

Galeon, Dom: A swarm intelligence correctly predicted TIME's Person of the Year. *Futurism,* 2017. Online: https://futurism.com/swarm-intelligence-correctly-predicted-times-person-of-the-year

Haig Zsolt: *Információs műveletek a kibertérben.* Budapest, Dialóg Campus, 2018.

Hossam, Faris – Ibrahim Aljarah – Mohammed Azmi Al-Betar – Seyedali Mirjalili: Grey wolf optimizer: A review of recent variants and applications. *Neural Computing and Applications,* 30. (2018), 2. 413–435. Online: https://doi.org/10.1007/s00521-017-3272-5

Iriondo, Roberto: *Breaking CAPTCHA using machine learning in 0.05 seconds.* Towards AI, 2018. Online: https://medium.com/towards-artificial-intelligence/breaking-captcha-using-machine-learning-in-0-05-seconds-9feefb997694

Jobbágy Szabolcs: A negyedik generációs hadviselés infokommunikációs aspektusai – fogalmi kitekintő. *Hadmérnök,* 12. (2017), 1. 203–213.

Kása Richárd: *Döntéselmélet.* Diplomamunka. Miskolc, Miskolci Egyetem, 2014.

Kharpal, Arjun: Trump will win the election and is more popular than Obama in 2008, MI system finds. *CNBC,* 2016. Online: www.cnbc.com/2016/10/28/donald-trump-will-win-the-election-and-is-more-popular-than-obama-in-2008-ai-system-finds.html (Magyarul: https://hvg.hu/tudomany/20161029_donald_trump_lesz_az_elnok_josolja_a_mesterseges_intelligencia)

Kirat, Dhilung – Giovanni Vigna – Christopher Kruegel: BareBox: Efficient Malware Analysis on Bare-Metal. Proceedings of the 27th *Annual Computer Security Applications Conference.* Orlando, 2011. Online: https://doi.org/10.1145/2076732.2076790

Kovács László: *A kibertér védelme.* Budapest, Dialóg Campus, 2018.

Lin, Kuan-Cheng – Sih-Yang Chen – Jason C. Hun: Botnet detection using support vector machines with artificial fish swarm algorithm. *Journal of Applied Mathematics (Hindawi),* (2014). 1–9. Online: https://doi.org/10.1155/2014/986428

Mesterséges Intelligencia Koalíció: *Magyarország Mesterséges Intelligencia Stratégiája, 2020–2030.* Budapest, Innovációs és Technológiai Minisztérium, 2020. Online: https://digitalisjoletprogram.hu/files/2f/32/2f32f239878a4559b6541e46277d6e88.pdf

Négyesi Imre: A mesterséges intelligencia és a hadsereg I. *Hadtudományi Szemle,* 10. (2017), 2. 23–34.

Nyikes, Zoltan – Zoltan Rajnai: *Big data, as part of the critical infrastructure*. SISY: IEEE 13th International Symposium on Intelligent Systems and Informatics. New York, IEEE, 2015. 217–222. Online: https://doi.org/10.1109/SISY.2015.7325383

Panimalar, S. Arockia: Nature inspired metaheuristic algorithms. *International Research Journal of Engineering and Technology,* 4. (2017), 10. 306–309.

Radware Malware Protection Service: *Evasive Attack Techniques Overview*. Radware, 2018. Online: https://downloads.seculert.com/documents/Evasive%20Attack%20Techniques%20Overview.pdf

Rosebrock, Adrian: *Deep learning for computer vision with Python*. Philadelphia, PyImageSearch, 2017.

Sikora, Lubomir: *Swarm Malware – Hejnový virus.* (Diplomamunka.) Osztravai Műszaki Egyetem, 2017.

Stefnisson, Siggi: Evasive malware now a commodity. *Security Week,* 2018. Online: www.securityweek.com/evasive-malware-now-commodity

Stoecklin, Marc Ph. – Jang Jiyong – Dhilung Kirat: DeepLocker, How MI can power a stealthy new breed of malware. *Security Intelligence,* 2018. Online: https://securityintelligence.com/deeplocker-how-ai-can-power-a-stealthy-new-breed-of-malware

Ye, Guixin – Zhanyong Tang et alii: Yet another text CAPTCHA solver: A generative adversarial network based approach. *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security.* 2018. 332–348. Online: https://doi.org/10.1145/3243734.3243754

Yang, Xin-She: *Nature-inspired metaheuristic algorithms.* Cambridge, Luniver Press, 2010.

Yampolskiy, Roman V.: AI-complete CAPTCHAs as Zero Knowledge Proofs of Access to an Artificially Intelligent System. *International Scholarly Research Notices Artificial Intelligence,* (2012). 1–6. Online: https://doi.org/10.5402/2012/271878

Zelinka, Ivan – Swagatam Das – Lubomir Sikora – Roman Šenkeřík: Swarm virus – Next-generation virus and antivirus paradigm. *Swarm and Evolutionary Computation,* 43. (2018). 207–224. Online: https://doi.org/10.1016/j.swevo.2018.05.003

Jogi forrás

1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról