DOI: 10.38146/BSZ.2018.7-8.4

FAZEKAS ISTVÁN

A mesterségesintelligencia-kutatás eredményei a kriminalisztika néhány vonatkozásában

A kultúrtörténet során akkor következtek be a legnagyobb változások, amikor egyfajta információs forradalom zajlott. Ilyen volt az írás feltalálása, a könyvnyomtatás megjelenése vagy éppen a mobilkommunikáció térhódítása. Minden egyes ilyen alkalommal a korábban meglévő tudás megsokszorozódott, éreztetve áldásos hatását – és olykor átkos következményeit is. Az információrobbanás – a számítógépek tömeges elterjedése nyomán bekövetkező adatsokszorozódás – napjainkban is tartó folyamata az ismeretek korábban nem tapasztalt mértékű gyarapodását idézte elő. A mennyiségi növekedésen túl (éppen az informatika és társtudományai hihetetlen fejlődésének köszönhetően) azonban egy minőségi ugrás is bekövetkezett karnyújtásnyira hozva a tanulni képes, esetenként már kreatív gépek korát.

A digitális kor és a big data

Az International Data Corporation (IDC) által immár több mint harminc éve folyamatosan végzett és a világ digitális fejlődésére vonatkozó adatgyűjtő kutatások egyre megdöbbentőbb eredményeket tárnak a nagyközönség elé. A szervezet 2018 februárjában közzétett legfrissebb kutatási dokumentumainak tanúsága szerint 2020-ra mintegy 44 zettabyte mennyiségű felhalmozott adattal számolhatunk.[1]

De mennyi adat is ez?

Nos, ha az egyes után leírandó – és aztán azt csak sok ezer kilométeres távolságokban kifejezni képes – analógiát szeretném segítségül hívni, aligha sikerülne szemléletesen érzékeltetnem ezt az adatmennyiséget. Ezért más utat választok – tegyük fel, hogy az olvasó szereti a filmeket, méghozzá jó minőségben nézni.

A 4K felbontás már csodás vizuális élményt nyújt, a képpontok száma olyan nagy egy meglehetősen kis felületen (ennek megfelelően a méretük is

1 https://www.emc.com/leadership/digital-universe/2014iview/executive-summary.htm

roppant kicsi), hogy két egymás melletti pontocskát közvetlen közelről még erős nagyítóval is igencsak nehézkes megkülönböztetni. Az interneten fellelhető 4K nagyfilmes tartalmak (itt kilencvenperces filmekre kell gondolni) átlagosan negyven gigabyte méretűek, vagyis kb. kilenc DVD-re férne el egy alkotás. Ilyen filmeket valamivel több mint négymillió évig nézhetnénk megszakítás nélkül. Hát ennyi az annyi.

Gyaníthatóan kérdések tömkelegét veti fel ez a kis számolás és a végeredménye az emberben, ezek közül én most csak egyet ragadok ki: honnan ez a rengeteg adat?

A teoretikusok nagyjából megegyeznek abban, hogy a digitális korszak valamikor a 2000-es évek legelején vette kezdetét. Az időpont meghatározása nem önkényes, annak során azt vették alapul, amikor a digitális tárolási kapacitás mértéke meghaladta az ugyanazon időpontban rendelkezésre álló analóg tárolási kapacitást.[2] Azóta az „adattermelés" éves üteme folyamatosan nő, 2011-ben valamivel több mint hatvan százalékkal volt nagyobb az előző évinél, napjainkra pedig egyes becslések szerint minden évben megduplázódik. Szintén az IDC felméréséből derül ki az, hogy két év múlva egy ember másodpercenként 1,7 megabyte adatot fog előállítani, és akkor még nem beszéltünk az üzleti jellegű adatdömpingről, az emberi beavatkozás nélkül létrejövő szenzorikus adatgyűjtésből származó nullák és egyek garmadájáról és a ma még nem is létező technológiák szolgáltatta adatáradatról.[3] Az adattermelés immár önálló technológiává vált, ennek a neve a sokat emlegetett big data. Ez a technológia (más megközelítésben a kifejezés a digitális kor szinonimája) legegyszerűbben úgy jellemezhető, hogy óriási adatmennyiség, amely a korszerű informatikai eszközökön keresztül közvetlen kapcsolatba hozható a mindennapi életünkkel, és képes azt befolyásolni. Egyfajta új természeti erőforrás ez, egyúttal számtalan kockázat forrása is.[4]

Ezek a kockázatok nem új keletűek, van azonban valami, ami napjainkban új szintre emeli őket – a kibertér kialakulása. A sci-fi szerző *William Gibson* által 1982-ben alkotott fogalom bejárta a világot és mára általánosan elfogadott megnevezése lett annak a virtuális térnek, amelyben az elektronikusan létrehozott adatok tárolódnak, és amelyben az online kommunikáció folyik. Ebben a virtuális térben öltenek formát azok a szándékok is, amelyek

2 Martin Hilbert – Priscilla López: The World's Technological Capacity to Store, Communicate, and Compute Information. Science, vol. 332, no. 6025, 2011

3 https://www.newgenapps.com/blog/big-data-statistics-predictions-on-the-future-of-big-data

4 Zsigovits László: A Big Data mint a rendvédelem egyik nagy kihívása. In: Gaál Gyula – Hautzinger Zoltán (szerk.): Tanulmányok „A változó rendészet aktuális kihívásai" című tudományos konferenciáról. Pécs, 2013 [Pécsi Határőr Tudományos Közlemények XIV.]

egyre több fejtörést okoznak a bűnüldözés szakembereinek. A számítógépes bűnözés vélhetően egyidős a digitális korral, az ellene való védekezésnek mára hatékony formái jöttek létre. Alapjuk, hogy a szakemberek a tapasztalatok fényében egy konzekvens és jól áttekinthető rendszerbe szervezik a megelőzés, felderítés és ellenállás módszereit, és ezeket nemzetközi joghatással párosítják[5] (a kiberbűnözés elleni fellépés dokumentumai). Az elkövetés stratégiája alapján a digitális bűnelkövetéssel foglalkozó tudományok *(Digital Forensic Science)* három területet különítenek el. A számítógép-központú, a számítógéppel segített és a járulékos számítógépes bűnözés területét. Az első esetben célpontként a számítógépes rendszer, hálózat, adattároló, vagy egyéb eszköz jelenik meg (például kereskedelmi weboldal tartalmának módosítása). Ez egyben tekinthető egy új bűncselekménytípusnak is, amely új eszközrendszert használ (tudniillik a számítógépet). A számítógéppel segített bűnözés esetében a számítógépet mint eszközt használja az elkövető a cselekmény során, ami „segíti" a tevékenységét, de nem feltétlenül szükséges hozzá. Itt hagyományos bűncselekményekről beszélhetünk, új módszerek alkalmazása mellett. Végül az a terület, amelyben a számítógépes rendszer a bűncselekmény szempontjából mellékes, lényegében valamely létező hagyományos eszköz kiváltását jelenti (például könyvelés számítógéppel, papíralapú dokumentáció helyett).

A fenyegetések formáinak és módszereinek feltérképezése mellett fontos az elkövetés kategóriáinak tisztázása, hiszen a büntetés – a visszatartó erőt jelentő hatás – ennek alapján határozható meg. Az cybercrime egyezmény[6] kiemel számos bűncselekménycsoportot, amelyeket a kiberbűncselekmények (a kibertérben elkövetett törvényellenes cselekmények) fogalmi körébe sorol, majd az egyes bűncselekményeket ezeken belül tipizálja:

1. Számítástechnikai rendszer és számítástechnikai adat hozzáférhetősége, sérthetetlensége és titkossága elleni bűncselekmények
   a) jogosulatlan belépés,

5 Például az Európai Parlament és a tanács rendelete az elektronikus hírközlés során a magánélet tiszteletben tartásáról és a személyes adatok védelméről, valamint a 2002/58/EK irányelv hatályon kívül helyezéséről (elektronikus hírközlési adatvédelmi rendelet javaslata, 2017); az Európai Parlament és a tanács 2002/58/EK irányelve (2002. július 12.) az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről (elektronikus hírközlési adatvédelmi irányelv); az Európai Parlament és a tanács 2011/92/EU irányelve (2011. december 13.) a gyermekek szexuális bántalmazása, szexuális kizsákmányolása és a gyermekpornográfia elleni küzdelemről, valamint a 2004/68/IB tanácsi kerethatározat felváltásáról.

6 Az Európa Tanács Budapesten, 2001. november 23-án kelt számítástechnikai bűnözésről szóló egyezménye (ETS 185).

b) jogosulatlan kifürkészés,
c) számítástechnikai adat megsértése,
d) számítástechnikai rendszer megsértése,
e) eszközökkel való visszaélés;
2. Számítógéppel kapcsolatos bűncselekmények
a) számítógéppel kapcsolatos hamisítás,
b) számítógéppel kapcsolatos csalás;
3. Számítástechnikai adatok tartamával kapcsolatos bűncselekmények
a) gyermekpornográfiával kapcsolatos bűncselekmény;
4. Szerzői vagy szomszédos jogok megsértésével kapcsolatos bűncselekmények.[7]

A kiberbűnözés e keretei a továbbiakban már megfelelő alapot adnak az ellene való hatékony fellépéshez, illetve rugalmasságánál fogva lehetővé teszik az újabb törvényellenes jelenségek rendszerszintű asszimilálását az azok elleni harchoz. Szükség is van erre a fajta proaktív magatartásra, hiszen a technológia rohamos fejlődése az elkövetés módozatainak és célterületeinek bővülését hozta magával.

Eddig a kártékony kódok hálózati rendszereket fenyegető réme, a kiskorúak tapasztalatlanságával és védtelenségével való visszaélés legkülönbözőbb formái és az adatmanipuláció jelentette a legtöbb kapacitást lekötő veszélyeket. Az okoseszközök elterjedése (okostelefonok, -órák, -tévék, legújabban -porszívók, -hűtők és már erotikus segédeszközök is) roppantmód kiszélesítette a támadható célpontokat egyelőre még a klasszikusnak számító elkövetés módszerei mellett. Van azonban a fejlődésnek – amit gyakran negyedik ipari forradalomként is emlegetnek – egy olyan szegmense, amely már nem csupán mennyiségi, hanem minőségi változásokat képes generálni a kiberbűnözésben. Ez pedig a mesterségesen létrehozott kognitív képességek (gyűjtőnevén mesterséges intelligencia; AI) bűnelkövetés területén való felhasználásának lehetősége.

7 Máté István Zsolt: Az igazságügyi informatikai szakértő a büntetőeljárásban. PhD-értekezés. Pécsi Tudományegyetem Állam- és Jogtudományi Kar Doktori Iskola, Pécs, 2017

A mesterségesintelligencia-kutatások rövid áttekintése és jelene[8]

A mesterségesintelligencia-kutatások kezdete egészen az 1940-es évek elejére nyúlik vissza. Az első hivatalosan is a területhez sorolt eredmény *W. McCulloch* és *W. Pitts* nevéhez fűződik, akik 1943-ban ez első mesterségesneuron- (a neuron természetes körülmények között az idegrendszer elemi építőköve) modellt javasolták, és kimutatták, hogy az ezekből felépített háló képes a tanulásra. A mesterséges intelligencia elnevezés *(Artificial Inteligence) John McCarthy*tól származik 1956-ból. Ez után a töretlen lelkesedés és az elvárások fokozódása jellemezte azokat a kutatási területeket (számítógépes nyelvészet, játékelmélet, alakzatfelismerés és gépi tanulás stb.), amelyek megalapozták a mesterséges intelligencia fejlődését. Jelentősebb sikereket azonban nem igazán tudtak felmutatni a szakemberek. Az áttörést a szakértői rendszerek kifejlesztése hozta meg, amelyek többnyire specializált folyamatok szabályokkal jól leírható feladatait hajtották végre (ilyen például a számítógéprendszerek komponenseit tartalmazó megrendelések konfigurálása). A nyolcvanas évek elején az AI-kutatások eredményeinek felhasználása ipari méreteket öltött. Aztán egy évtizeddel később a túlzottan optimista várakozások tükrében tett ígéretek teljesíthetetlensége miatt beköszöntött az „AI tele", amikor a kutatások finanszírozása szinte teljes mértékben megszűnt, a felhasználói oldalon alakult cégek nagy része pedig tönkrement.

Egyetlen dolog maradt töretlen, a hit, hogy a mesterséges intelligencia létrehozása nem csupán álom. Ettől az erőtől hajtva megszállott tudósok az egyes részterületekre fókuszálva gyötrelmes, apró lépésekben valódi tudományos eredményeket produkáltak (ellenőrzött körülmények között létrejött, reprodukálható eredmények) olyan területeken, mint a beszédfelismerés, a robotika, a gépi látás vagy éppen a tudásreprezentációk. Az elért eredményeken felbátorodva a szakemberek a kilencvenes évektől egy új problémakörre összpontosítottak, amit a „teljes ágens" fogalmával jelöltek. Ezen a valós környezetbe ágyazott, folytonos szenzorikus adatokat fogadó mesterséges entitást értették. Az ilyen intelligens ágensek szempontjából az egyik legfontosabb működési környezet az internet. Mára a világhálós alkalmazásokban az AI-rendszerek mindennaposak lettek (spamszűrés, vírusdetektálás, online-magatartás-vizsgálatokra épülő ajánlórendszerek, interaktív csevegőalkalmazások, weboldal-optimalizálás, keresőgépek stb.), olyannyira, hogy a 'bot'[9]

8 http://mialmanach.mit.bme.hu/aima/ch01s03

9 A robot szó végéről „levált" 'bot' kifejezés az automatikus, felügyelet nélküli programot jelöli.

szóvégződés már a mindennapi nyelvbe is beépült. A korrektség kedvéért idekívánkozik, hogy a teljes ágens és az intelligens robot nem ekvivalens kifejezések. Az integrált, szintetikus egyedeken belüli általános mesterséges intelligenciára (AGI) valójában még nincs példa. A rendszer azon elemei, amelyek az előzőkben felsorolt területeken működnek, úgynevezett szűk tudásterű AI-megvalósulások.[10]

A kockázatok felmérése

A mesterséges intelligenciához, még inkább a gondolkodó és érző robotok víziójához kapcsolódó félelmek gyakran tárgyalt jelenség. Regények, filmek és a tudomány prominens alakjai foglalkoznak azzal, hogy mit is jelent majd az AGI megjelenése, ha egyáltalán sor kerül rá. Van tehát egy általános viszonyulás a közvélemény részéről, amelyet a média által közvetített hírek alakítanak, és amely többnyire valamiféle szerves–szintetikus szembenállás formájában ölt testet, miközben van egy másik megközelítés, amely kevésbé körvonalazódott. Ez pedig a kibertérben végrehajtott bűncselekmények oldaláról közelít a területhez. A korábban tárgyalt számítógépes bűnözés új formáinak megjelenését a mesterségesen létrehozott kognitív entitások, a szűk tudásterű AI térhódítása idézi elő, amellyel a kiberbűnözés mintegy szintet ugrik.

Az új helyzetben a kockázatok és fenyegetések felmérése sokkal nagyobb mértékű szervezettséget és együttműködést kíván a törvényesség védelmében munkálkodók és a tudományos közösség tagjai között, miközben a tájékoztatás irányába is nagyobb aktivitást feltételez. 2018 elején egy 26 szerző által (tudósok, rendvédelmi szakemberek, jövőkutatók) jegyzett tudományos értekezés jelent meg[11]. A tanulmány a jelenleg már használatos AI-eredményekre fókuszál, illetve felveszi a repertoárba az öt éven belül várható fejlődés eredményeit is. A dokumentumban a szerzők megpróbálnak képet adni a mesterségesintelligencia-kutatások eredményeinek szándékosan rosszindulatú felhasználása esetén meglévő kockázatokról és veszélyekről, illetve javaslatot tesznek a megelőzésre és a már bekövetkezett biztonsági események okozta károk enyhítésére. Az együttműködés szükségességének felismerését tehát gyorsan követte a tett, ami mind az együttműködés szorosabbra vonó-

10 Martin Ford: Robotok kora. Milyen lesz a világ munkahelyek nélkül? HVG Kiadó Zrt., Budapest, 2017, 250–251. o. [HVG-könyvek]

11 Miles Brundage et al.: The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. February 2018. https://www.eff.org/files/2018/02/20/malicious_ai_report_final.pdf

sában és elmélyítésében, mind a széles körű tájékoztatás gyakorlatában jelentős előrelépés. Az értekezés olyan stratégiai gondolatokat fogalmaz meg, mint a lehetséges célterületek klaszterezése (digitális, fizikai és politikai biztonság) vagy a várható fenyegetések módszertani besorolása (a tradicionális célpontok, módszerek és elkövetői kör bővülése, az „új típusú fenyegetések" megjelenése, a már meglévő fenyegetések jellegének megváltozása). További erénye a dokumentumnak, hogy – bár kiveszi a rosszindulatú felhasználás köréből – kitér az AI mint technológiai fejlődési jelenség által okozott (munkaerőpiac, vásárlói szokások átalakulása stb.) problémákra, illetve az AI-kutatás és -innováció területén a versenyelőny megszerzésére tett lépésekből származó veszélyekre (nemzetbiztonsági és titokvédelmi kockázatok). A vázolt megállapítások figyelembevételével immár kísérlet tehető arra, hogy a fenyegetettség forrásait, mértékét és célterületeit is számba lehessen venni.

Általánosítható és elsődleges jellegét tekintve a kockázat a világ digitalizált és globális mivoltából fakad. Ezt tovább súlyosbítja az a jellegzetesség, hogy eszközeink nagyobb része immár mobilis, multifunkcionális és hálózatba kötött, így bármikor, bárhol és bárhonnan, nem utolsósorban pedig bárki – már amennyiben birtokában van a megfelelő kapacitásoknak – által elérhetővé válhat.

Ha ez a „valaki" képességeinek megsokszorozására mesterségesintelligencia-elemeket használ, akkor olyan előnyhöz jut, amelynek birtokában a ma rendelkezésre álló védelmi rendszerek többsége hatékonyan kijátszható.

A falnak is szeme van

Az AI-kutatások kezdete óta foglalkoztatja a szakembereket a gépi látás problémája. Hogyan lehetne az emberi érzékelés (érzékszervek) analógiájára a környezetet a mesterséges entitások részére is érzékelhetővé tenni. Az már régen ismert és kihasznált tény, hogy a napi információáradat feldolgozásában a szemnek jut a legnagyobb szerep. Óvatos becslések szerint is a minket érő információs hatások több mint nyolcvan százaléka vizuális természetű. A gépi intelligencia működése során a környezet felfogása, az abban való tájékozódás kiemelt fontosságú. Ez pedig azt jelenti, hogy fel kell készíteni a gépeket a vizuális ingerek felfogására és feldolgozására. A kezdeti alakfelismerési problémák megoldása után a képfelismerési algoritmusoknak köszönhetően a gépi látás most már olyan összetett feladatok ellátására is képes, mint a valós időben való alakfelismerés és -követés akár több célobjek-

tum esetében is, vagy éppen a nézőponthalmazok elemzése után való vizuális 3D-rekonstrukció (mozgóképes felvételek esetében egy-egy nézőpontban látható tárgy vagy személy térbeli képének rekonstrukciója még gyengébb minőségű felvételek esetén is). A biometrikus azonosítás területén egyre nagyobb teret hódít az arckép-/arcvonás-detektálás módszere, amelyben a tanulóalgoritmusok szintén jelentős szerepet kapnak. A Google arcképazonosító algoritmusa nagyobb pontossággal ismeri fel az arcokat, mint az ember, és a fejlődés még csak az elején tart. Némi képzelőerő és az előbbi tények ismeretében nem ördöngösség felmérni a kockázatokat. A hálózatba kötött köztéri vagy magánüzemeltetésű biztonságikamera-rendszerek a nap huszonnégy órájában folyamatosan pásztázzák a teret, a műholdak funkciójuktól függően szintén képi információval látják el az üzemeltetőiket vagy bérlőiket. Az autonóm rendszerek – legyen szó önvezető járművekről, vagy éppen egy raktár készleteinek elrendezését végző rendszerről, nem is beszélve némely katonai alkalmazásról – szintén jelentős mértékben támaszkodnak a környezetből érkező vizuális természetű információkra.

Az ezekhez való illetéktelen hozzáférés után – amelyhez talán már valamely AI-komponenst használt az elkövető – a behatoló képessé válik akár az irányítás átvételére, vagy olyan adatok megszerzésére, amelyeket egy későbbi alkalommal használ fel (azonosítás megtévesztése, megfigyelési rendszerek kijátszása stb.)[12]. A már ma is működő retinaszkennerek esetében egy webkamera feletti irányítás átvételét követően, a szemről készített megfelelő felbontású képek AI „tisztítása" és a retina rekonstrukciója után rendelkezésre áll egy klón, amely lehetővé teszi egy biztonsági rendszer feltörését. A pénzszállító járművek mozgásának és útvonaljellemzőinek kameraképeit neurális háló segítségével elemezve megtalálhatók a sikeres támadást lehetővé tevő rések.

A megtévesztés mesterei

A másik olyan terület, amely napjainkra kiemelkedően jó színvonalon képes működni, a beszédfelismerés és a beszédszintézis. A számítógépes nyelvészet alapjaiból kifejlődő tudományág mára szintén életünk számos területére belopódzott. Ezekre építenek az intelligens asszisztensek (Siri), a chatbotok és

12 Kevin Townsend: The Malicious Use of Artificial Intelligence in Cybersecurity. Security Week, March 28, 2018. https://www.securityweek.com/malicious-use-artificial-intelligence-cybersecurity

még számtalan online alkalmazás. Ma már az ügyfélszolgálatok, a helpdesk szolgáltatásokat nyújtó szervezetek vagy éppen az online termékajánlatok készítői is előszeretettel használják ezt a technológiát. Az emberi természetes beszéddel való vezérlés már nemcsak a számítógépek – erre már az angol nyelvű Windows XP is képes volt – sajátja, szóbeli utasításokkal vezérelhetjük a porszívónkat, vagy éppen a garázskaput. A gépek értik és válaszolnak is, a válaszok pedig már régen nem a klasszikus szintetikus robothangok, hanem kifinomult emberi vokalitások. Nem nehéz elképzelni azt a helyzetet, amelyben a mesterséges intelligencia nemes egyszerűséggel ismerősünk hangján csevegve átveri a vonal túlsó végén gyanútlanul vele társalgó embert. De ugyanígy egy hangazonosítás alkalmával is kiválóan teljesíthet, hozzáférve védett tartalmakhoz, vagy egyéb értékekhez. Ha mindehhez hozzátesszük, hogy ezek az alkalmazások a nyelvek közötti átjárhatóság (fordítók, szinkrontolmács alkalmazások) területének vezető megoldásai, akkor nyilvánvalóvá válik, hogy a globális kibertérben a veszélyek is globálisan jelentkeznek.

Szegregáció kontra aggregáció

Az új, intelligens algoritmusok kínálta lehetőségek egyik kiemelkedően fontos jellemzője, hogy túllépnek az adatok egyszerű felhalmozásán (aggregáció). Bonyolult számítástudományi, statisztikai, hálózatelméleti és genetikus kódoláson alapuló elemzési módszereket alkalmazva összefüggéseket, rejtett kapcsolatokat tárnak fel. Más alkalommal az adatok elkülönítésének technikájával (szegregáció) dolgoznak, aminek eredményeképpen képesek kiszűrni az eltérő, egyedi jellegzetességeket és ezzel leszűkíteni egy keresés találatainak körét és számát. Ezeket a technikákat napjainkra a bűnmegelőzés és a bűncselekmények felderítése során is egyre gyakrabban alkalmazzák a szakemberek.

A védekezés területei és módszerei

A rendvédelem területén dolgozók, a biztonsági szolgálatok és az érzékeny adatokkal foglalkozó szervezetek már az AI-kutatások első kézzelfogható és használható eredményeinek megjelenése óta igyekeznek azokat munkamódszereikbe integrálni. Napjainkban már olyan stratégiai területeken vetik be a

mesterségesintelligencia-kutatások vívmányait, mint a vírusvédelem, a spamszűrés, a profilalkotás, az intelligens térfigyelő rendszerek és ezekkel összefüggésben a képjavítási technológiák és az azonosítás. A kifejezetten a bűnmegelőzés irányába mutató kezdeményezések mind Európa országaiban, mind a tengerentúl egyre nagyobb szerepet kapnak. Ezek közül kiemelkedő a statisztikai jellegű klaszterezés, amelyben az információs rendszerek szolgáltatta adatokat feldolgozva elkészítik egy-egy terület bűnmegelőzési szempontok alapján érzékenyített térképét. Ez mintegy előrejelzi a várható elkövetések lehetséges és legvalószínűbb helyszíneit, a szóba jöhető elkövetők személyét és a veszélyeztetettek körét is. Hasonló elvek alapján szerveződnek a legmodernebb adatbiztonsági rendszerek és védelmi struktúrák is. Élő példaként említhető az AI-alapú automatikus védelmi rendszer, a Vectra Cognito, amelyről a terület kiemelkedő szakemberei a következő jellemzést adták: *„A Cognito automatikusan, valós időben elemzi, rangsorolja, összeveti egymással és priorizálja a vállalaton belüli aktív fenyegetéseket, így jelentősen csökkenti a biztonsági elemzők túlterhelését."* Ez lehetővé teszi a biztonsági csapatok számára, hogy a legkritikusabb fenyegetésekre összpontosítsanak anélkül, hogy elárasztanák őket az alacsony kockázatú eseményekre vonatkozó állandó riasztások.[13]

A bűncselekmények felderítésekor a tanulóalgoritmusok bevetése a nyomszakértésben, a DNS-vizsgálatokban és a kapcsolati rendszerek feltérképezésében jelentősen növeli a hatékonyságot. Sőt, a jövő fenyegetéseinek előrejelzésében és a rájuk való felkészülésben is egyre nagyobb szerepet játszanak, mint arra az előzőekben bemutatott módszerek utalnak. Az önvezető járművek, a csomagszállító drónok, az orvoslásban a nanotechnológia térhódítása olyan kihívások elé állítja a törvényesség védelmezőit, amelyeknek a hagyományos eszközökkel és felkészültséggel már nagyon nehéz megfelelni. A jövő a tudásalapú szervezetek előtt nyit nagyobb távlatokat, amit a rendvédelem területén sem szabad figyelmen kívül hagyni.

Kitekintés

1997-ben a Deep Blue elnevezésű nagy teljesítményű számítógép[14] legyőzte *Garri Kaszparov* sakknagymestert. A sakk azonban olyan játék, amelyben minden állás egzakt módon betáplálható egy gépbe, egy ilyen mérkőzés ki-

13 https://info.vectra.ai/hs-fs/hub/388196/file-1918923738.pdf
14 A Deep Blue 1997-ben a világ 259. legerősebb szuperszámítógépe volt.

menetele csak a tárolt adatokhoz való hozzáférés és azok feldolgozásának sebességén múlik. Az AI kezdetekben valójában azokon a területeken teljesített jól, ahol nagy mennyiségű adat feldolgozása vált szükségessé, de jól definiálható szabályok és állapotok, valamint a bizonytalanság kizárása mellett. Mára a helyzet gyökeresen megváltozott. A tanulóalgoritmusok túllépnek ezen a fajta hatékonyságon. Teljesítményük attól függően változik, hogy a felügyelt, a felügyelet nélküli vagy a részben vagy félig felügyelt tanulási szisztéma szerint működnek-e. Mindhárom esetben a kiinduló állapot azonos, a szoftver úgynevezett tanuló-adatbázisok adatait kapja meg. A különbség abban van, hogy kap-e ezekhez az adatokhoz azokat a megoldással összekötő közvetlen információkat, vagyis van-e jól definiált cél. Ha nincs ilyen egyértelmű kimenet, az algoritmusnak magának kell azt meghatároznia a rendelkezésre álló adatok halmazának elemzése alapján. Ekkor beszélünk felügyelet nélküli tanulásról. A mesterséges intelligencia ezen a szinten válik igazán önálló, mintegy intuitív és kreatív entitássá és ebben a formájában hordozza a legtöbb kockázatot.

Húsz évvel a Deep Blue győzelme után az AI újabb bravúrt hajtott végre immár a felügyelet nélküli tanulás algoritmusával felruházva[15]. Az algoritmusnak mindössze a sakk alapvető szabályait, a felállást, a lépéseket tanították meg, illetve azt, hogy mi számít győzelemnek (azaz mattnak). Alpha Zero ezután négy óra alatt nagymesteri szinten kezdett játszani, teljesen új nyerési stratégiákkal előállva. Hogy ezt diadalként, vagy a vészharang első kondulásaként értékeljük-e, az – jelen pillanatban még – rajtunk áll.

15 NAK: Új sakknagymestere van az emberiségnek. Index, 2017. december 8. https://index.hu/tech/2017/12/08/uj_sakknagymestere_van_az_emberisegnek_egy_gep/