

RENDESZETTUDOMÁNY BIZTONSÁGI KIHÍVÁSAI A FEJLŐDÉSI TRENDEK TÜKRÉBEN

A biztonság az egyik legfontosabb tényező az emberiség életében. A biztonság egy folyamatosan változó állapot, amelyben két ellentétes folyamatrendszer működik. Az egyik a biztonság ellen hat, mint agresszív, dinamikus, időnként konspirált folyamat, a biztonság szintjének csökkentésére törekszik, réseket keres a biztonsági hálón, a másik ezen romboló folyamatot igyekszik felderíteni, semlegesíteni.

A biztonság a létezés, működés káros befolyásoló hatásoktól és a veszélytényezőktől kellően mentesített, védett állapota. A biztonság kellő állapotának, szintjének megteremtéséhez kockázatelemzéssel a fenyegetéseket, veszélyforrásokat azonosítani kell, azok megelőzésére, elhárítására, bekövetkezésük esetén a helyzet kezelésére meg kell alkotni a szükséges ismereteket, ki kell dolgozni az adminisztratív védelem követelményeit, a rezsimintézkedéseket és a protokollokat, fel kell készíteni az emberi erőforrásokat, biztosítani kell a szükséges technológiákat és eszközöket.

A biztonság egy komplex viszonyrendszer, amely összetevődik külső, belső, gazdasági-pénzügyi, ellenőrzött termékek-technológiák, létfontosságú (kritikus) infrastruktúra, élelmiszer-mezőgazdaság, egészség, ökológiai és informatikai biztonságból. A belső biztonság területei a következők: nemzetbiztonság (belbiztonság, titkosszolgálati eredményállapot), közbiztonság, közlekedés biztonság, határbiztonság, szervezett bűnözés- és kábítószer terjedéssel szembeni biztonság, terrorfenyegetettség elleni biztonság, fogvatartotti biztonság, járvány és fertőzésterjedés elleni biztonság, ipari és természeti katasztrófákkal szembeni biztonság, magán- és önkormányzati biztonság, igazgatásrendészeti és idegenrendészeti biztonság.

A feltörekvő technológiák egyaránt szolgálják a biztonság elleni és a biztonságot védő folyamatokat, amelyek nagyon széles spektrumot ölelnek fel és állandó változásban vannak. Ezen állandó változás felfedése, értékelése, figyelembevétele a védelmi stratégiák kidolgozásánál fontos kormányzati, rendvédelmi feladat, rendészettudományi kihívás.

Az állandó változásokra történő reagálás szükségességét és gyakorlatát jól példázza, hogy 2022. március 25-én az Európai Unió Tanácsa elfogadta a „Biztonsági és Védelmi Stratégiai Iránytűt” (Strategic Compass for Security and Defence), amelynek célja az EU biztonság- és védelempolitikájának 2030-ig történő megerősítése. A dokumentum leírja a meghozandó „elsőbbbségi intézkedéseket” több területen annak érdekében, hogy megerősítse képességét a jelenlegi és gyorsan megjelenő fenyegetések és kihívások előrejelzésére, elrettentésére és reagálására, valamint az EU biztonsági érdekeinek védelme érdekében. Ilyenek, hogy növelni kell a hírszerzési elemzési kapacitást és a hibrid eszköztárat a különböző hibrid fenyegetések széles körének észlelésére és reagálására, tovább kell fejleszteni a kiberdiplomáciai eszköztárat, ki kell dolgozni a külföldi információk megfelelő felhasználási és interferencia módjait, meg kell alkotni az EU

biztonsági és védelmi űrstratégiáját, meg kell erősíteni az EU tengerbiztonsági tényezőként betöltött szerepét.¹

Ezek a feltörekvő technológiák egymással szinergiát képezve, még erősebben tudják kifejteni hatásukat, melyeket a külföldi angol nyelvű szakirodalom disruptive technologies névvel illet, amely szétszakítót jelent, valóban szétszakítja az eddigi életvitelünket. Még számtalan új kifejezés kerül a látóterbe a fejlődési trendeket vizsgálva, úgymint: globális elektronikai adatgyűjtés, digitális nyom, prediktív és előíró elemzés, gépi látás, gépi tanulás, mélytanulás, neurális hálózat, virtuális – kiterjesztett – vegyes – kibővített valóság, ipar 4.0, IoT, M2M, big data analytics, cloud computing industry² (tárgyak internete, gép-gép közötti kapcsolat, nagy adat elemzés, ipari számítási felhő), intelligent cloud which includes features like machine learning and advanced analytics³ (intelligens számítási felhő gépi tanulással és kiterjesztett/fejlett elemzéssel), intelligent agents (intelligens asszisztensek), Web5 stb.

A synergia hatást csak egy példával illusztrálva. „In this article, we tell you how the digital currency market works if cryptocurrency is espoused with computer vision – Ebben a cikkben elmondjuk, hogyan működik a digitális valutapiac, ha a kriptovalutát számítógépes látással támogatják”.⁴ A blokklánc technológia kiegészül a számítógépi látással, mindez az MI irányítása alatt. Ez azt jelenti, hogy egységes rendszerben kerül alkalmazásra több korszerű technológia, amelyek rendkívüli módon tudják fokozni egymás hatásosságát.

A robotok egy új generációját hozta létre az MI és a nanotechnológia. Eddig a robotok az elkészített program alapján működtek, az MI hatására önállóak, kvázi gondolkodók lesznek. Példaként említhető a Google LaMDA (Language Model for Dialogue Applications – nyelvi modell párbeszédés alkalmazásokhoz)⁵ – csetbot⁶, amely a cikk szerint már rendelkezik érzelmekkel, de lélekkel még nem. Ha valóban így van, akkor egy gondolkodó gép, lélek nélkül mire képes?

A csetbotok annyira emberszerűek, hogy bárkit könnyen megtévesztenek, melynek kapcsán már megjelentek a bűncselekmények is, például az avatar képes volt egy vezető nevében utasítást adni egyik helyettes vezetőnek nagy összegű pénz átutalásra a hacker számlájára. Két csetbot a beszélgetése során saját nyelvezetet alakított ki.

A csetbotokhoz szorosan kapcsolódik a deepfake technológia, egy algoritmus, amellyel (mozgó)képeken szereplő személy arcképét élethűen másvalakire lehet cserélni. Gépi mélytanulási (deep learning) algoritmus segít a hamis (fake) mozgókép létrehozásában, innen ered az angol neve.⁷ Emberek, közösségek megtévesztésére alkalmas, főleg, ha egy fake politikus vészhelyzetet jelent be, amely óriási pánikhoz vezethet. Az online kommunikációt vizsgáló kutatók szerint az online hírek gyorsan és nagy szétszórtsággal (penetrációval) terjednek, de még ennél is aggasztóbb, hogy nagy tömegek

¹ Forrás: <https://www.consilium.europa.eu/en/press/press-releases/2022/03/21/a-strategic-compass-for-a-stronger-eu-security-and-defence-in-the-next-decade/> (Letöltés ideje: 2022.06.25.)

² Forrás: <https://www.analyticsinsight.net/exclusive-interview-with-sunil-kardam-supply-chain-and-logistics-sbu-head-and-client-partner-gramener/> (Letöltés ideje: 2022.06.25.)

³ Forrás: <https://www.analyticsinsight.net/pr-microsofts-intelligent-cloud-revenue-worldwide-up-7-8-in-q222/> (Letöltés ideje: 2022.06.25.)

⁴ Forrás: <https://www.analyticsinsight.net/computer-vision-and-cryptocurrency-a-unique-combination/> (Letöltés ideje: 2022.06.25.)

⁵ Forrás: <https://www.wired.com/story/blake-lemoine-google-lamda-ai-bigotry/> (Letöltés ideje: 2022.06.25.)

⁶ A csetbotok olyan programok, amik többé-kevésbé élő ember illúzióját keltve képesek írásban csevegni.

⁷ Forrás: <https://www.szomagyarito.hu/szocikk.php?id=17151> (Letöltés ideje: 2022.06.30.)

feltétel nélkül hisznek is benne. A nanorobotok olyan kisméretűek, hogy az emberi testbe juttathatók be.

Figyelemmel kísérve a robot technológiát, a következő hírekre lehet bukanni: A robot, amely érzi a fájdalmat; Hangokkal fejezhetik ki az érzelmeiket a robotok; Budapestre látogatott Sophia a szuperintelligens robot; Sikeresen repül a harvardi robotrovar; Okostelefon vezérléssel repül a robot szitakötő⁸.

Az MI által vezérelt drónok gyilkológépekké váltak. Személyfelismeréssel (nem csak az arcfelismerést alkalmazza, hanem a viselkedés és megjelenés azonosítást is – nőnek öltözött férfit azonosított az MI a mozgása, viselkedése alapján) kiválasztják az adott politikust, vezetőt és likvidálják. Kis méretű drónok rajokban való támadásra is alkalmasak, amelyek hatalmas pusztításra képesek.

Ha ezek a robot és drón képességek a terrorizmust szolgálják, illetve tömegesen alkalmazza őket valamely állami vagy más szervezet, az óriási veszélyhelyzetek kialakulásához vezethet.

Az adattudomány előretörésével a globális elektronikai adatgyűjtés, a bigdata adatfeldolgozás, a prediktív és előíró elemzés a személyiség identitását képes teljesen lerombolni. A globális elektronikai adatgyűjtéssel a személy minden mozdulata, tevékenysége az általa generált digitális nyomok (biztonsági kamera, internet alkalmazás, bankkártya és vásárlói kártya használat, okostelefon kommunikáció, műhold felvétel) kapcsán megfigyelhető, érzékelhető. A bigdata adatfeldolgozási technológia képes minden adatfajt, legyen az mozgókép, hang, írott szöveg, internet használat vagy más digitális nyom, egységes rendszerben az algoritmos elemzés során feldolgozni és a célszemély teljes élettevékenységét reprodukálni. A prediktív és előíró elemzés lehetőséget ad az egyén jövőbeli cselekvéseinek előrejelzésére és befolyásolására. Ezáltal a személyiség identitás manipulálható. Tömeges alkalmazás során vezetők, politikusok tehetők munkaképtelenné.

Az adattudomány eredményei a rendvédelemben is jól hasznosíthatók. Az adattudományra épül az intelligencia led policing (intelligencia vezérelt rendfenntartás) is. „Az intelligencia vezérelt rendfenntartás lehetővé teszi a rendőrségi szervek számára, hogy adatokat és információkat használhassanak fel a bűnözési trendek és problémák jobb értékelése érdekében, ezáltal lehetővé téve a vezető döntéshozók számára, hogy hatékonyan és eredményesen allokálják az erőforrásokat és dolgozzanak ki bűnözés elleni stratégiákat.” Az intelligencia szót az angolban két vonatkozásban is használják, úgymint ész, értelem és hírszerzés, hírek. Ezért gyakran az intelligencia led policing kifejezést hírszerzés vezérelt rendfenntartásnak is értelmezik, de helyesebb az intelligencia vezérelt rendfenntartás megnevezés, mert a szövegkörnyezet egyértelműen az adattudomány alkalmazását sugallja, nem pedig a titkosszolgálati tevékenységet.⁹ A Chicagói Egyetem adattudósai által kifejlesztett új bűn-előrejelző algoritmus valószínűsíti a bűncselekmények elkövetési helyét és időpontját és 90%-os pontossággal képes meghatározni az erőszakos bűncselekményeket egy hétre előre.¹⁰

Az Európai Unió a 2021. évben vizsgálta a „The OSCE Project on Project Report Intelligence Led Policing 2017–2020” projekt végrehajtásának eredményeit.¹¹

⁸ Forrás: <https://www.robotvilag.hu/nanorobotok> (Letöltés ideje: 2022.06.25.)

⁹ Forrás: <https://study.com/academy/lesson/intelligence-led-policing-definition-lesson.html> Letöltés ideje: (2022.06.30.)

¹⁰ Forrás: <https://www.analyticsinsight.net/this-ai-tool-is-biased-but-still-can-predict-crime-locations-with-90-accuracy/> (Letöltés ideje: 2022.06.30.)

¹¹ Forrás: <https://www.osce.org/tntd/482610> (Letöltés ideje: 2022.06.25.)

A blokklánc alapú virtuális valuta hozzájárul a pénzmosáshoz, az illegális üzletek, a terrorizmus finanszírozásának elrejtéséhez. A kommunikáció titkosítás 5G, 6G mobilkommunikáció esetén védi a személyiségi jogokat, de elősegíti a szervezett bűnözés és a terrorizmus rejtett szerveződését, tevékenységét.

Az okos és intelligens települések, rendszerek létrehozása elengedhetetlen az életminőség javítása érdekében, de számtalan veszélyforrást hordoznak magukban, főként azért, mert az informatika nem csak kiegészítő szerepet játszik a létükben, hanem ezen alapul a működésük. A vezérlőrendszer és az információellátó rendszer műszaki vagy hackerek által történő megzavarása beláthatatlan rendkívüli helyzetek kialakulásához vezethet. Ha minden közlekedési lámpát pirosra állít valamely külső erő, abból óriási közlekedési dugók keletkeznek, de még rosszabb lehet a helyzet, ha ezek egyidőben zöldet mutatnak, amely hatalmas tömegbalesetekhez vezethet. Az áram, víz, gázszolgáltatás is az információtechnológia (a továbbiakban: IT) hatalmában áll, ezért ezek is érzékenyek az informatikai támadásokra, de más természeti csapás is károkat okozhat bennük.

Az alapinformáció ellátás szüneteltetése is zavarokat okozhat a napi életvitelben, ha elérhetlenné válik az internet, sok alapszolgáltatás is megbénul. Főként a Z és alfa generáció a lexikális tudás helyett az algoritmikus tudást (tudja hogyan zajlanak a folyamatok és ezekhez mit, hol kell keresni az interneten) tartja hasznosnak, amely viszont teljesen kiszolgáltatja őket az IT -nek. Az alapinformáció ellátás szüneteltetése a legnagyobb problémát a bankrendszer működésében és az egészségügyben okozza. A létfontosságú (alapvető/kritikus) infrastruktúrák is IT függőek, így ezek is jelentős kockázati tényezőt képviselnek.

Az önvezető járművek és a repülő autók, motorok vezérlésének megzavarása, elromlása is komoly veszélyhelyzeteket idézhet elő.

Az internet térhódítása is rendkívüli helyzetek forrása lehet. Ahogy az internet az érzelmi és virtuális irányba tendál és mindez ötvözve az adattudománnyal és az MI -vel, az emberi életvitelre jelenthet katasztrofális hatást. A kibertérben megjelent az érzékek és a tapintás internete, a metaverzum, valamint az influenzek és a hackerek is hathatós tevékenységet fejtenek ki. Az érzékek és a tapintás internete a személyről képes érzékeny információkat szerezni, amellyel adott esetben vissza lehet élni. A közösségi háló is öntanulóvá válik, üzleti intelligenciával felvértezett robot asszisztensek fognak ügyeket intézni.

A metaverzum (metaverse) napjaink kialakuló entitása, amely a kiterjesztett és a virtuális valóságot (AR/VR) mesterséges intelligenciával és blokkláncal ötvözve viszi az egyéni a virtuális térbe és azonosul annak minden elemével. A metaverzum is számos új veszélyforrást teremt. Alig kezdett a metaverzum trend közismertté válni, máris megtörtént az első bűncselekmény a metaverzumban. A sértett blogbejegyzésében az esetről azt írta, hogy egy perc sem telt el a belépést követően, három-négy férfi avatárjai zaklatni kezdték az övét, körbevették, verbálisan inzultálták és fotókat is készítettek.¹² Mindez felveti annak a szükségességét, hogy vizsgálni kell, hogy mi az online bűn. Ha a videójátékban nem bűn embert ölni, akkor az online molesztálás sem bűn? Az avatárok manipulálása, megölése, reinkarnációja hova helyezhető el a virtuális etikában?

Az influenzek főként a Z és alfa generációt ragadják magukkal, amely a megfélemlés, önkifejezés reménytelenség érzése folytán öngyilkossághoz is vezethet. Több

¹² Forrás: <https://www.vice.com/en/article/3abpg3/woman-says-she-was-virtually-gang-raped-in-facebooks-metaverse> Letöltés ideje: (2022.06.25.)

kutató szerint sok fiatal lelkét rombolja az Instagram.¹³ Egyes kutatások olyan módszert is tesztelnek, amely egy személy írott posztjain alapul, hogy kiderüljön, tinédzserként vagy felnőttként ír-e, bár előfordult, hogy sok felnőtt az Instagramon úgy írt, mintha tinédzser lett volna.¹⁴ De az MI is képes szövegalkotásra. A GPT-3 -t arra utasították, hogy írjon egy akadémiai dolgozatot saját magáról és adjon hozzá tudományos hivatkozásokat, idézeteket, melyet sikeresen megvalósított.¹⁵

Az internet számos bűncselekmény hordozója lehet, többek között csalások, zsarolóvírusok alkalmazásai, adatlopások fordulhatnak elő. A kibertérben folyó agresszív tevékenység kirobbanhat egy globális kiberháborút, amely a létfontosságú infrastruktúrák számítástechnikai működtetését teszi lehetetlenné és ezáltal a fenyegetettségét magas szintre emeli. Évekkel ezelőtt a biztonsági szakemberek reményüket fejezték ki, hogy a hackertevékenység nem emelkedik állami szintre és nem kerül a szervezett bűnözés hatókörébe. De ez nem váltotta be a reményeket, a számtalan eset közül csak kettőt említve, jól érzékelhető a veszélyes tendencia. A stuxnet vírussal a 2010. évben blokkolták az iráni nukleáris programot.¹⁶ Az orosz hackerok elérhetlenné tették több norvég kormányzati weboldalt.¹⁷

Az egyre fogyó minőségi munkaerő is számtalan olyan állapotot idézhet elő, amely rendkívüli helyzethez vezethet. Az éltechnológiák elvonhatják a szolgáltatástól a munkaerőt, illetve az MI felügyeletéhez, az adattudományhoz, a kibertér uralásához nem lesz elég szakképzett munkaerő.

A fertőzések új formái is előfordulhatnak. Még le sem lett küzdve a koronavírus járvány, máris új fenyegetések sejljenek fel. A szaporodó új vírusok, a sarki jegek olvadása során is életre kelhetnek lefagyasztott kórokozók.

Mindezek alapján a rendészettudománynak számolnia kell azzal, hogy az életvitelt egy sok pólusú hatásrendszer, paradigma fogja meghatározni. A Z és alfa generáció mérhetetlen szabadság- és önmegvalósulás vágya, amely jórészt a metaverzumba tevődik át igényli az online környezet, a kibertér gyorsuló fejlődését. Az üzleti és gazdasági élet törekvése a tömegtermelés (minél többet – minél olcsóbban) és eladhatóság tükrében az egyén személyiségének, vágyainak megismerése a célzott reklámtevékenység végzése érdekében, melynek következtében felgyorsul a globális elektronikai adatgyűjtéssel a digitális nyomok megszerzése, a bigdata technológiával azok feldolgozása, az érzelmek és a tapintás internetének létrehozásával, a metaverzum kialakításával, a prediktív és előíró elemzéssel a potenciális vevőkör meghatározása, amely az adattudományban ölt testet. A jogvédő szervezetek küzdenek a személyiségi jogok, személyes adatok védelméért. A szervezett bűnözés és a terrorizmus kihasználja az adatvédelem lehetőségeit a konspiráció miatt, ezért támogatja a jogvédő szervezetek törekvéseit a titkosított kommunikáció és a blokklánc technológia megvalósítása érdekében, természetes, mindezek mellett azonnal kiaknázza a fejlődési trendek eredményeit. A rendvédelem célkitűzése a gyanús személyek

¹³Forrás: https://hvg.hu/360/202139__toxikus_instagram__titkolozo_facebook__ertelem_es_erzelem__szenvedely_betegseg (Letöltés ideje: 2022.06.25.)

¹⁴ Forrás: <https://www.analyticsinsight.net/artificial-intelligence-helps-instagram-to-verify-your-age-with-your-face/> (Letöltés ideje: 2022.06.30.)

¹⁵ Forrás: <https://www.analyticsinsight.net/ai-writes-an-academic-paper-about-itself-and-researchers-try-to-publish-it/> (Letöltés ideje: 2022.07.05.)

¹⁶ Forrás: <https://hu.atomiyme.com/12-legnagyobb-hacker-tamadasok-a-vilag/> Letöltés ideje: 2022. június 25.

¹⁷Forrás: https://hvg.hu/tudomany/20220701_orosz_hackertamadas_norvegia_ddos_tamadas_tulterheleses_tamadas Letöltés ideje: (2022.06.25.)

tevékenységének figyelemmel kísérhetősége érdekében az üzleti élet technológiai eredményeinek adaptálása, amely ellentmond a jogvédők elképzeléseinek. A szakképzett munkaerőhiány az MI és az IT rohamos fejlődésével lehetővé teszi az új generációs autonóm műszaki-technikai-neurális eszközrendszerek általánossá válását, úgymint a „gondolkodó” robotok, kobotok – kollaboratív robotok, önvezető és repülő járművek, intelligens/okos települések, ipar 4.0, avatárok, csetbotok egyre nagyobb térnyerését. Mindezek alapján elengedhetetlen a rendszerben való gondolkodás és a különböző jelenségek synergia hatásának vizsgálata. Számolni kell az emberek kényelemszeretetével, az új iránti fokozott érdeklődésével, a kifinomult csalási technológiákkal, amelyek a biztonság, főként az informatikai biztonság rombolóivá válhatnak.

A szakképzett munkaerőhiány miatt és a megfelelő intézkedési képesség kialakítása érdekében a rendvédelemnek, a rendészettudománynak is fel kell készülnie a robotok, önvezető és repülő járművek, az MI és az adattudomány egyre szélesebb körű igénybevételére. Alkalmazni kell a robotjárórt, robotkutyát, az MI által vezérelt, hazugságvizsgálatra is alkalmas intelligens beléptető és ellenőrző rendszereket, főként a határellenőrzésben. Az informatikai védelemben kobotokkal, botokkal (informatikai robotokkal) kell részt venni. Az irodai és szolgáltató tevékenységet robotokkal (csetbotokkal) kell kiváltani. Elképzelhető a robot tűzoltó, vagy az önvezető mentőben utazó robotorvos alkalmazása?

A rendvédelem jelentős része átkerül a kibertérbe a metaverzum és más kiberbűncselekmények kezelése, a kriptovaluta bűncselekmények nyomozása, a titkosított kommunikáció ellenére a szerveződő és zajló bűncselekmények, terrortámadások felfedése érdekében. Az intelligens rendszerek zavara esetén való teendők nagy része is a kibertérben zajlik.

Az ember-gép viszony is számos kérdést vet fel. Hogyan intézkedik az emberi rendőr az önvezető és repülő járművekkel, más robotokkal szemben, hogyan tud a rendőr egy önvezető járművet megállítani? Milyen lesz a rendőr robot viszonya az intézkedés tárgyához? Megijed tőle az ember? Fél, hogy elromlik, aggasztja, hogy nincsek érzelmei? Milyen lesz a rendőr robot viszonya egy másik robothoz?

A korszerű vezetésemélet (agilis vezetés, coaching, adattudomány, a prediktív és előíró elemzés alkalmazása) is kihívás elé állítja a rendészettudományt. Már most el kell kezdeni a felsővezetés oktatását, felkészítését a várható jövőre és mindezeket be kell építeni a képzési tematikákba. A rendészettudománynak azonban van honnan merítenie, hiszen a hadtudomány és a határőrizet tudománya már évtizedekkel ezelőtt alkalmazta ezen üzleti élet vezetési újdonságait. Az agilis vezetés elmélete szinte leutánozza a harcászati parancsnoki munkákat, a coaching a katonai főiskolán alkalmazott gyakorló alparancsnok, a térképes feladatok, hadijátékok üzleti életre átszabott változata. Az adattudomány is alkalmazásra került, mert nem csak a tiltott határátlépést elkövetők adatai kerültek gyűjtésre és feldolgozásra, hanem a környezeti és befolyásoló adatok (terep, időjárás, rendezvények stb.) is. A prediktív elemzést fedte le a határsértők valószínű mozgási idejének és irányának meghatározása, vagy a harcászatban a helyzetértékelés, a mennyiségi és minőségi erőviszony számvetés.