ZSIGOVITS LÁSZLÓ

A JÖVŐ RENDŐRE

Reggel felébredsz, arra gondolsz, hogy jó lenne egy tojásrántotta, máris beindul a 3D nyomtató és kinyomtatja a tojásrántottát, azt a házi robot ágyba viszi. Megjelenik egy drón, kinyílik az okos házad okos ablaka, és feltölti a 3D nyomtatód tároló rekeszeit ételpor kapszulákkal. Rosszul alakulnak az életkörülményeid, azon töprengesz, hogyan lehetne, nem éppen tisztességes módon haszonhoz jutni. Nemsokára megjelenik egy robotrendőr és elvisz. Ezek a víziók a disztópikus világképbe illő fikciók vagy valósággá válhatnak? Az írást végigolvasva, talán választ kapunk a kérdésre.

Az emberiségnek mindig is léteztek a fenti víziókat szimbolizáló vágyai, amelyek a tudományos fantasztikus művekben sorra napvilágot láttak, de a gyakorlati megvalósításuknak technikai akadályai voltak. A 2000-es évek elejére azonban a tudomány eljutott arra szintre, amely a kibertérrel és a kibertér mindennemű adattípusainak gyors, automatikus megszerezhetőségével, az óriási digitális adat tárolási és számítógép feldolgozási sebességgel, a gyors mobil kommunikációval és a robotizálással, mesterséges intelligenciával képes egy új digitális világ megteremtésére. A fejlődés nem áll meg, rohamléptekkel halad előre, amelynek mozgatórugói szinergiát alkotnak. Egyrészt van a kínálati oldal, amelyet a profitszerzés, hatalomvágy hajt, a tudós uralni akarja a világot, a hacker meg akarja mutatni, hogy mire képes, másrészt van a befogadó oldal, amely a kényelemszeretet, státuszszimbólum kinyilvánítás, egzisztenciális alapon vágyik az új dolgokra. A főbb fejlődési tendenciák az alábbiakban foglalhatók össze:

- az IKT[1] alkalmazása egyre inkább életfeltétellé válik, amely felgyorsuló fejlődésen megy keresztül (digitális élettér, digitális társadalom stb.);
- robotizálás megállíthatatlanul tör előre;
- mesterséges intelligencia (MI) kifejlesztéséhez a technológia adott (AI – Artificially Intelligent);
- IoT,[2] M2M[3] technológiák behálózzák az egész életteret;
- Web3[4] egyre nagyobb szerepet nyer, a szupergyors internet és az 5G mobil adatátvitel biztosítja a valósidejű és online kommunikációt;
- kialakult a kibertér a virtuális térrel[5] és a hatalmas mennyiségű digitális nyommal;
- a globális elektronikai adat- és információgyűjtéssel (GEAI) megvalósul a hagyományos élettér és a kibertér minden adatának megszerezhetősége;
- a BigData technológiával, a szuperszámítógépekkel, gridekkel, az informatikai felhővel, az óriási tárolókapacitásokkal és processzor műveleti sebességgel

[1] IKT – infokommunikációs technológia.
[2] IoT – internet of things kifejezés mozaikszava. Magyarul: tárgyak internete.
[3] M2M – machine-to-machine, azaz gép és gép közötti kommunikáció rövidítése.
[4] Web3 –az ipar4, IoT és M2M internete, szemantikus web.
[5] Virtuális tér – térinformatikai számítógép program alapján szimulált 3D térmodell és objektum, illetve az interneten összekapcsolt személyek, közösségek élettere.

lehetővé válik a nagyszámú és különböző típusú digitális adatok egységes rendszerben történő valós idejű kezelése;
- a szkenner alapú biometrikus jellemzőket gyűjtő automatikus eszközök a digitális hazugságvizsgáló technológián keresztül egyre inkább képessé válnak az adott személy pillanatnyi érzelmeinek, vágyainak kimutatására;
- a mesterséges intelligencián alapuló algoritmikus elemzéssel a személyiséget jól kifejező profil alkotható, lehetővé válik az összes digitális adatformátum egységes rendszerben való feldolgozása, a prediktív információképzés.

A GEAI a klasszikus nyílt és titkos adatgyűjtés mellett megjelenő harmadik féle adat és információszerzési forrás. Azért egy harmadik mód, mivel a globális kibertérben mindenütt digitális nyomok keletkeznek, az egyén életének az elektronikus tevékenységekhez kapcsolódó minden egyes megnyilvánulása digitális nyomot generál és ezen digitális nyomok folyamatosan megszerezhetők bárki által, aki rendelkezik a digitális nyom rögzítésére és feldolgozására alkalmas eszközzel. Korábban is léteztek telefon lehallgatások, titokban készített videofelvételek, adatbázisokban tárolt érzékeny adatok, még ha azok digitalizálva is lettek, nem tudták őket egységes rendszerben kezelni. A 2000-es évek elejére azonban kifejlődött az az infokommunikációs technológia, amely képes az óriási mennyiségű és különböző formátumú adatokat egységes rendszerben kezelni, mint például a BigData[6], Hadoop[7], szuperszámítógép, grid, felhő. A BigData rendszerek alkalmasak az integrált adatfeldolgozásra, az algoritmikus elemzésre. Az algoritmikus elemzés során, például egy szövegfájlban, azaz egy Word dokumentumban a keresőrobot megtalál egy érzékeny szót, amely lehet egy feltételezett terrorista neve, akkor ez az algoritmus a keresést ezzel a kulcsszóval képes az adatbázisokban is lefolytatni. Ha valamely adatbázisban talál megegyező nevet és a képmezőben rögzítésre került a személy fényképe, akkor az algoritmus fájlformátum váltást tud végrehajtani és a biztonsági kamerák felvételeiben futtat le képazonosítási eljárást. Ha hangminta is rendelkezésre áll, akkor az algoritmus újra fájlformátumot vált és a hangminta alapján a hangfájlokban hajt végre keresést. Az algoritmikus elemzés nemcsak a fájlformátumok közötti váltásra képes, hanem a logikailag összefüggő adatkapcsolatokon is egy fa gráf modell segítségével feldolgozást, kutatást tud végrehajtani. Például, ha az egyik dokumentumban a megtalált érzékeny név mellett rendszám, telefonszám is szerepel, akkor az algoritmus leképezi a fa gráf első csúcspontját, aminek egyik éle a rendszám lesz, a másik éle a telefonszám. Először ezen rendszámmal hajt végre keresést, ha talál más adathordozón lévő fájlban egy azonos rendszámot, akkor generálja a fa gráf második elágazását (csúcspontját) és annyi élet, amennyi kapcsolódó adatot talál (újabb név, rendszám, időpont, helyiség stb.). Ezt a műveletet addig végzi, amíg el nem jut az összes adatforrás végére. Innen visszalép a fa gráf utolsó csúcspontjára és a következő él mentén végzi el a kutatást. Egy rekurzív eljárást folytat az összes létező adatforrás átvizsgálására.

A Prediktív Profilalapú Elektronikus Személyazonosítás a személyazonosítás három funkciójának biztosítására szolgáló digitális automatikus adatgyűjtési és értékelési rendszer. Funkciói: 1. Személy kilétének megállapítása (főként személyi okmányok / más adatok és az adatbázisokban tárolt adatok alapján). 2. Személy helyszínen tartózkodási és

[6] Zsigovits László: A Big Data, mint a rendvédelem egyik nagy kihívása, Pécsi Határőr Tudományos Közlemények XIV. Pécs 2013. 180. o.

[7] Az Apache Hadoop nagy mennyiségű, akár több terabájtnyi strukturált vagy strukturálatlan adat tárolására és elemzésére szolgáló, nyílt forráskódú szoftver.

tevékenységi jogosultságának eldöntése. 3. Személy rendvédelemre való veszélyességének, kockázatának előjelzése, megítélése, valószínűsítése. A rendszer egyik elemét a bázis adattár képezi, amelynek az összetevői a rendvédelmi és más kormányzati adatbázisok, a GEAI -val megszerzett kibertér digitális nyomai, illetve az ezeket kezelő üzleti logika (BigData és más kereső elemző algoritmusok). Lehetőséget teremt az okmánybeli személyi adatok és más biometrikus jellemzők alapján történő elsődleges személyazonosításra. A rendszer második eleme az általános bűnelkövetési módok és személyiségjellemzők kriminológiai, kriminalisztikai, szociológiai, pszichológiai aspektusai alapján megalkotott általános bűnözői profil, egy digitalizált referenciamodell. A rendszer harmadik eleme a helyszíni biometrikus kisugárzás detektáló berendezés, amelyben egy MI kezeli a hazugságvizsgálat elvén működő digitális kamera által felfogott biometrikus kisugárzásokat és a kamerakép kiértékelését, a kapott eredményt hasonlítja az általános bűnözői referenciamodellel, amelyből létrehozza a prediktív megítélését. A digitális hazugságvizsgáló kamera képes felismerni a célszemély rejtett érzelmeit, szorongását, az elvárható viselkedési módtól eltérő megnyilvánulásait, amelyből felépíti az aktuálszemélyi digitális prediktív modellt. Ez a prediktív modell kerül összevetésre az általános bűnözői profillal. Ha az értékelő algoritmus talál bizonyos azonosságot, figyelmezteti a rendvédelmi szervet a felmerült gyanúokra. Ennek folytán a másodlagos személyazonosítás képes olyan rendvédelemre veszélyes személyekre utalást adni, akik nem szerepelnek sem a SIS, sem egyéb más rendvédelmi adatbázisokban, illetve fiktív személyi okmányokkal fedik el valódi kilétüket. Az eljárás nagy valószínűséggel utalást ad a megfigyelt vagy az ellenőrzött személy rejtett szándékára, fedett viselkedésére.

A robotkérdést két szempontból kell vizsgálni. Először, mint a rendőrrobotot, másrészt a rendőr viszonyát a robotokhoz. Az Isaac Asimov által megalkotott robotika három törvénye értelmében a rendvédelmi robot nem alkalmazhat kényszerítő eszközöket, nem használhat fegyvert, ez viszont ellentmond a rendvédelmi funkciót megtestesítő szerepének. A rendőrnek a biztonságérzet sugárzása, a bizonytalansági helyzetekben szolgáltatás nyújtása és adott esetben a belső rend védelme a hivatása. Ezen utóbbi általában félelmet vált ki az emberekből. A rendőrrobot olyan eszköz lesz, amely e félelem kiváltást megszünteti? Felismeri-e az ember az emberszabású, érzelmeket kifejező, környezet változásaira reagáló robotot? Fél tőle? Engedelmeskedik egy gépnek? A rendőrrobot korruptálható lesz a hacker által, védhető a hackertámadásoktól, méltányosságot tud-e alkalmazni, avagy érzéketlen vastömeg lesz? (Korrupció: Egyébként nem járó ellenszolgáltatás fejében előny biztosítása vagy hátránytól mentesítés). A vezető nélküli autó gyorshajtása, nem megengedett helyen való parkolása, drón általi károkozás hogyan kezelhető a rendőr által? A rendőr, illetve a robotrendőr a robottal hogyan kommunikál? Robotviadalok hogyan harmonizálnak a közrenddel? Robot okozta balesetért ki felel (gyereket gázolt a Szilícium-völgy robotzsaruja 2017.06.24.)? Isaac Asimov törvényeit ki kell egészíteni egy negyedik törvénnyel? Jelesül: A robot tevékenysége során nem szeghet meg jogszabályt vagy más közrendre vonatkozó előírást, illetve szabályszegés észlelése esetén köteles figyelmeztetni a szabálysértő magatartás befejezésére, értesítenie kell a releváns rendvédelmi szervet. Ha a rendőrrobot fel lesz ruházva kényszerítő eszközök alkalmazásának jogával, akkor fontos törvényként kell alkalmazkodnia a szükségesség és arányosság elvéhez.

Fenyvesi Csaba által felépített kriminalisztika piramis adatmodelljét[8] az IKT három tekintetben kibővíti: digitális nyomok; GEAI; helyszíni biometrikus kisugárzás detektálás. A mediátorok nyomok halmazának a digitális nyomok jelentős részhalmazát képezik, amelyet jól bizonyít a biztonsági kamerák felvételeinek elemzésével történt bűncselekmény elkövetők azonosítása[9] és más bűncselekmény elkövetők felderítése. Digitális anyagmaradványt képeznek a számítógéprendszerek által készített naplófájlok. Digitális vallomást eredményez a helyszíni biometrikus kisugárzás detektálás, amely a poligráfos hazugságvizsgálat elvét követve a személy pillanatnyi gondolatait, elrejtett vágyait képes felfedni.[10]

A fejlődést jól szemlélteti a különböző rendszerek kialakulása. A tudásalapú rendszerek egy célszámítógépen keresztül a tudásbázisukban tárolt adatok és információk óriási halmazából egy belső üzleti logikán keresztül képesek mindig a felmerülő problémahelyzet megoldásához azonnal adatokat, információkat szolgáltatni. Az okos rendszerek már tartalmaznak egy automatikus környezeti adatgyűjtő egységet a kibertérből származó összes formátumú digitális adat megszerzéséhez és az egyes elemei a weben keresztül az IoT és M2M technológia alapján egymással kapcsolatban állnak, melynek következtében emberi beavatkozás nélkül, de az ember tájékoztatásával, esetleg megkérdezésével folyamatokat indítanak el, robotokat aktivizálnak. A folyamatokat a kibertér meghatározott állapotváltozásaihoz rendelt beprogramozott protokollok és szabályrendszerek alapján kezelik. Az intelligens rendszerekben a működtető üzleti logika kel önálló életre az MI által. A protokoll és a szabályrendszer a tapasztalat feldolgozáson és öntanulási képesség folytán állandóan változik. Amíg az okos rendszer csak az előre kidolgozott helyzetekre vonatkozóan képes cselekedni, addig az intelligens rendszer nincsen korlátozva a kezdetként számára meghatározott helyzetek kezelésére, az MI folytán új helyzeteket képes felismerni és erre reagálni.

Joggal feltételezhető, hogy a bevezetőként felvillantott víziók nem fikciók. A mesterséges intelligencia alapján működő elemzőrendszer elkészíti a személyiségprofilt a GEAI által gyűjtött szokásjellemzők, cselekedetek, megnyilvánulások alapján, a házi robot pillanatnyi hangulat, titkos vágyak biometrikus kisugárzását kutató szenzorjai figyelnek, a felfogott jeleket a mesterséges intelligencia azonosítja a személyiségprofillal, a levont következtetés alapján kiadja a parancsot a 3D ételnyomtatónak. Ha a 3D ételnyomtató valamely ételpor kapszulája kifogyóban van, a nyomtató az M2M technológia folytán értesíti az ételpor ellátót, amely útba indít egy drónt a szükséges kapszulával. Az IoT folytán a ház, az ablak is okos objektumként, az interneten keresztül egy rendszerben folytat kommunikációs tevékenységet, ezért az ablak a drón közeledtével kinyílik. A GEAI folyamatosan adatot gyűjt a személy helyzetéről, körülményeinek változásairól, annak minden mozgását, megnyilvánulását rögzíti, aktualizálja a profilját, a pillanatnyi hangulat, titkos vágyak biometrikus kisugárzását kutató robotok szenzorjai által képzett információkat a mesterséges intelligencia összeveti a profillal és prediktív értékítéletet képezve ki tudja következtetni, hogy a személy bűncselekmény elkövetésére készül.

[8] Fenyvesi Csaba: A kriminalisztika alapkérdései, Pécsi Határőr Tudományos Közlemények XIV. Pécs 2013. 177-183. o.

[9] Teréz körút Király utcai kereszteződésében 2016. szeptember 24-én elkövetett robbantás gyanúsítottjának beazonosítása.

[10] Hexium Kft terméke, hivatalos URL: http://www.hexium.hu/ (Letöltés ideje: 2017.07.19.)

A fejlődési tendenciák mellett a belső biztonságot veszélyeztető főbb kihívások is hatnak a jövő rendőrére, amelyek az alábbiak:

- tömegméretű migráció és a migráció új jellemvonásainak megjelenése;[11]
- terrorcselekmények elszaporodása, módszereinek megváltozása;
- az IKT legfejlettebb generációinak a bűnözés szolgálatába állítása;
- kibertér elleni támadások.

A tömeges méretű migráció alapvető okaként említhető egyrészt a megélhetési biztonságot veszélyeztető tényezők, mint a harcok, üldöztetés, éhínség, vízhiány előtérbe kerülése, másrészt a globalizációból fakadóan a propaganda hatására a jobb élet reményében és a nyugat-európai elöregedés, munkaerőhiány hatására a gazdasági migráció felerősödése, harmadrészt az embercsempészetből fakadó haszon motivációja. A 2000-es éveket megelőzően a migrációra az egyedi vagy szórvány jellegű (kis csoport), önállóan, esetleg segítővel (embercsempész) történő lezajlás volt a jellemző. Ehhez adódott hozzá a spontán, ad hoc jellegű, nagyobb létszámú, valamely jelentősebb veszélytényező hatására (háború, természeti csapás stb.) meginduló élettérváltás.

A 2000-es évek elejétől új jelenségként kialakult, első sorban a propaganda és az embercsempész szervezetek hatására a lappangó, látens, kiváró gazdasági migráció. Az életkörülmények megváltoztatása érdekében az élettér váltás tervezésének hatásaként az Európába jutni akarók, többnyire sátortáborban várakozó nagy létszámú csoportjai alakultak ki. Egyes számítások szerint a közeljövőben akár 10 millió migráns is megindulhat embercsempészek, különböző emberjogi szervezetek segítségével Európa felé.

A 2000-es évek migrációjában három markánsan tetten érhető új jellemvonás fedezhető fel. Egyrészt új segítőként különböző emberjogi szervezetek karolták fel a migrációt, az embercsempészési bűncselekményektől elhatárolódván, azt nyílt, különböző nemzetközi szerződésekre való hivatkozás alapján a migráció segítését kötelező emberbaráti segítségként deklarálva. Másrészt felerősödött a rejtett, embercsempész szervezetek és más titokban segítő csoportosulások, mint például az egyéb csempésztevékenységet folytatók, terrorcselekményre készülők aktivitása. Harmadrészt a migránsok cselekedeteire, magatartására az alázatosság, a valóban segítségre szorulás igényének kinyilvánítása helyett a követelődzés, a fejlett Európába jutás jogának hangoztatása és mindezek mellett az erőszakosság (2017.06.26. Olasz–francia határon mindegy 400 fő migránst, többnyire fiatal szudániakat csak könnygázzal tudták megállítani), a telepített határzárak fizikai megrongálása lett a jellemző.

A terrorcselekmények elszaporodása mellett, azok elkövetési módjában is lényeges változás állt be (lásd: 2017.tavasz-nyár eseményei). Szinte hetente számolnak be a híradások merényletek elkövetéséről, amelyeket többnyire nem beszivárgó terroristák hajtanak végre, hanem másod vagy harmadgenerációs bevándorlók, akikre a virtuális szocializáció a jellemző. A radikalizálódó közösségek a kibertérben szerveződnek. Nehezen felderíthető módszereket alkalmaznak, olyanokat, amihez nem kell fegyver, robbanóanyag beszerzése, köznapi, gyanúokon felül álló eszközökkel és módon vitelezhetők ki, mint például gépjárművel történő tömegbe hajtás, késes támadás.

[11] Kovács Gábor: A migráció bűnügyi hatásai a magyar határrendészet kockázatelemzési rendszerére. In: Hautzinger Zoltán (szerk.) A migráció bűnügyi hatásai. Magyar Rendészettudományi Társaság Migrációs Tagozat. Budapest, 2016. 141-150. o. Kovács Gábor: A rendőrség vezetésirányítási rendszerének sajátosságai a migrációs válsághelyzet kezelése során. In: Tálas Péter (szerk.). Magyarország és a 2015-ös európai migrációs válság. Dialóg Campus Kiadó. Budapest, 2017. 125-148. o.

Az IKT és az egyéb műszaki eszközök legfejlettebb generációinak a bűnözés szolgálatába állítása szintén jelentős kihívásként jelenik meg a rendvédelem, a rendészeti kutatások terén. A szervezett bűnözői csoportok többször jelentősebb anyagi erőforrásokkal rendelkeznek, mint a rendvédelmi szervek, így azok képesek azonnal átállni a legmodernebb technológiára, amíg a rendvédelmi szerveknek erre nincsen forrásuk. Ha lenne is forrásuk, egy új technológia bevezetése (pályáztatás, közbeszerzés – amire a bűnöző nem kötelezett) akár egy évbe is telhet, mire az már lehet, hogy nem is a leg korszerűbb technológia lesz.

A kibertér elleni támadások jelentősége is határozottan megnőtt. A kibertér kialakulásával a számítástechnika és a kommunikációs hálózatok rendszere a társadalmi létezés alapjává vált, egy „Z" generációs élettér, életminőség alakult ki, amely az IKT nélkül összeomlik. A kibertér ellen elkövethető támadás a könnyűnek tűnő pénzszerzési lehetőség reményét villantja fel (WannaCry zsarolóvírus), alkalmas a politika befolyásolására (USA választások), jól szolgálja egyes kormányok titkosszolgálati céljait, a bűncselekmények kivitelezését. Többek között a drónokat az embercsempészek a határőrizeti rendszer felderítésére, a csempészek cigarettaszállításra használják.

A fejlődési tendenciák és a veszélytényezők a belső biztonság megteremtésének törvényszerűségeit kiegészítik az alábbiakkal:

- a belső biztonságot szándékosan veszélyeztető folyamatok a rendvédelem technológiai képességeinek felülmúlására törekszenek, többnyire azt felül is múlják;
- a belső biztonságot veszélyeztető folyamatok sajátos morfológiai jellemzőkkel rendelkeznek, a hálózatelmélettel kapcsolatrendszereik jól modellezhetők;
- az IKT legújabb eredményeinek felhasználási képessége döntően befolyásolja a belső biztonság fenntartásának állapotát (kibertér uralása);
- a belső biztonság szintje attól függ, hogy a rendvédelem milyen mértékben képes a veszélyeztető folyamatok azonosítására, azok korai felismerésére és kezelésére;
- minden konspirált, rejtett folyamatnak vannak áruló jelei, azok digitális nyomokat generálnak, amelyek a GEAI –vel felderíthetők.

A jövő rendőrét az eddigiekben elemzett fejlődési tendenciák és veszélytényezők határozzák meg, amelynek pár jellemzőjét az alábbiak fejezik ki:

- uralnia kell a kiberteret;
- képesnek kell lennie az új kihívások kezelésére, a folyamatos megújulásra;
- integrálódnia kell a robotvilágba;
- digitális rendőrré kell válnia.