ZSIGOVITS LÁSZLÓ

A KÖZBIZTONSÁGOT, A KÖZRENDET ÉS AZ ÁLLAMHATÁR RENDJÉT ALAPVETŐEN VESZÉLYEZTETŐ KIHÍVÁSOK A KIBERTÉR ÉS A VIRTUÁLIS TÉR DIMENZIÓJÁBAN

A tudomány és a technika fejlődésének az emberiségre kifejtett hatása mindig is kétirányú volt, mely magában hordozza az életminőség javítása mellett az iszonyatos erejű pusztító modern technológiákat is és a 2000-es évekre már-már az apokalipszis ötödik lovasa szerepét ölti magára.[1] A közbiztonság a komplex értelemben vett biztonság egyik fontos alkotó eleme, mégpedig a belső biztonságé. A biztonság ugyanis egy összetett viszonyrendszer, amely külső, belső, gazdasági-pénzügyi, ellenőrzött termékek-technológiák, kritikus infrastruktúra, élelmiszer-mezőgazdaság, egészség, ökológiai, informatikai biztonságból épül fel.

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 kezeléséhez fel kell tárni 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. Ezen intézkedéssorozat nem más, mint a rend megteremtése a biztonság dimenziójában.

Néhány külföldi példa a biztonság és az azt szavatoló virtuális biztonság, kellő szintjének megteremtéséhez nélkülözhetetlen technológiák, eszközök, módszerek alkalmazására: a schengeni térséghez[2] és a világ sok más államához hasonlóan, az Oroszországi Föderáció (OF) határbiztonságának szavatolásához, és a terrorizmus elleni küzdelemében[3] is magasan fejlett informatikai technológiájú és többfunkciós határőrkomplexumok létrehozása zajlik.[4,5]

A határbiztonság szavatolása mellett, fejlett informatikai technológiák alkalmazásával történik évtizedek óta az OF kozmikus védelmének tökéletesítése is.[6,7] Erre

---

[1] Deák József: A szputnyik-rémtől az „űrszemétig" – A kozmosz orosz „váll-laposítása". Pécsi Határőr Tudományos Közlemények XVI. Pécs, 2015. 344. o.

[2] Deák József – Gáspár Szabolcs – Háncs Tivadar – Révai Róbert: A migráció rendészeti és egészségügyi aspektusai napjainkban. Belügyi Szemle 2016/9. 5-15. o.

[3] Deák József: A terrorizmus természete és az ellene történő fellépés nehézségei Oroszországban a Szovjetunió szétesésétől napjainkig. Belügyi Szemle 2015/7–8. 137-151.o.

[4] Deák József: Az Oroszországi Föderáció határőrizeti kihívásai napjainkban. Hadtudomány 2016. 8. o. Forrás: http://mhtt.eu/hadtudomany/2016/2016_elektronikus/1_deak%20jozsef.pdf (Letöltés ideje: 2018.07.29.)

[5] Deák József: Az Oroszországi Föderáció válaszai a biztonsági kihívások közül a migrációra. Innováció, elektronizáció, tudásmenedzsment. Magyar Rendészettudományi Társaság Vám- és Pénzügyőri Tagozata. Budapest, 2018. 71-86. o.

[6] Deák József: Az orosz lég- és űrvédelmi csapatok. Felderítő Szemle. http://knbsz.gov.hu/hu/letoltes/fsz/2015-1.pdf letöltve: 2018. július 29.

technológiai válaszként születtek, készülnek az USA, napjainkban ismét elővett csillagháborús tervei.[8]

A belső biztonság területei a következőek: nemzetbiztonság, közbiztonság, közlekedés biztonság, határbiztonság[9], 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 közbiztonság egy eredmény állapot, mely a személyek, közösségek testi és szellemi épségének, értékeik, vagyontárgyaik védelmének a szintjét mutatja az erőszakos emberi cselekményekkel szemben. A közgondolkodásban ez azt jelenti, hogy az embert nem fenyegeti az a veszély, hogy személyét bántalmazzák (megverik, megerőszakolják, fogva tartják, sanyargatják, kényszerítik), életét kioltják, értékeit ellopják, elrabolják, vagyontárgyait megrongálják, betörnek a lakásába, kirabolják.

A közrend fenntartása az alapja a közbiztonság megteremtésének, mely folyamatos aktivitást jelent két ellenpólus (rendbontó-rendfenntartó) között, cselekvések sorozata, két ellentétes folyamat eredője. A közgondolkodásban az emberi magatartás írott és íratlan szabályainak a betartását jelenti. Mindezek alapján filozófiai értelemben a biztonság a rend és a káosz közötti állapot kifejeződése. A biztonság jövőbeli főbb veszélyteyezői az Európai biztonsági stratégia (The European Agenda on Security[10]) alapján az alábbiakban azonosíthatók:

- infokommunikációs technológia (IKT) a bűnelkövetők szolgálatában:
  - jelentős anyagi forrás;
  - nem kell közbeszerzés;
- kiber bűnözés (Europol IOCTA értékelés);
- súlyos és szervezett bűnözés (Europol SOCTA értékelés);
- nagy méreteket öltő migráció[11];
- környezetkárosítás;
- terrorizmus (Europol TE-SAT értékelés).

A felsorolt veszélyteyezőkben az IKT számos formában ölt testet, melynek főbb elemei az alábbiak:

- kibertér;
- virtuális tér;
- virtuális valóság;
- kiterjesztett valóság;
- kibővített valóság;

[7] Deák József: Russia's space defence from its beginning to the present time. Forrás: http://yadda.icm.edu.pl/yadda/element/bwmeta1.element.desklight-1426f0af-a1e6-429f-a8a6-3ac603fe6cca (Letöltés ideje: 2018.07.29.)

[8] Deák József: Oroszország válaszainak rövid története az űrhadviselés, a migráció és a terrorizmus biztonsági kihívásaira. Hadtudományi Szemle 2018/1. 414-426. o.

[9] A fejlett infokommunikációs technológiák határbiztonság fenntartásában, növelésében játszott szerepét lásd Kui László: Technikai lehetőségek a magyar–szerb viszonylat határőrizetében. Határrendészeti Tanulmányok 2018/4. 32-35. o.

[10] Forrás: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf (Letötlés ideje: 2018.07.19.)

[11] Ritecz György – Sallai János: A migráció trendjei, okai és kezelésének lehetőségei 2.0 Hanns Seidel Alapítvány. Budaörs, 2016.

- kevert valóság;
- vizualizáció;
- intelligens tér.

A kiber kifejezés az Internettel összefüggő események, dolgok kapcsán nyert értelmezést. Ebből fakadóan a kibertér[12] (cyberspace) az internet (világháló) által egyetemessé tett digitális élettér, metaforikus (immateriális, virtuális) tér, az egymástól kölcsönösen függő, összekapcsolt információs rendszerek, a rajtuk áramló digitális információk, valamint az ezen információkkal és információs rendszerekkel kölcsönhatásba lépő felhasználók összessége. A kibertér a számítógép rendszerek és -hálózatok által és az azokban tárolt digitális adatok, az online adatforgalom, valamint a kommunikáció alapján, az idő és tér szerepét megváltoztatva jön létre. A globális kibertér (global cyber space) az interneten az egész Földre kiterjedő globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttese.

Az Európai biztonsági stratégia három fő prioritása (terrorizmus, súlyos és szervezett bűnözés, illetve a kiber bűnözés elleni küzdelem) a kibertérhez kapcsolódik. Ugyanezen stratégia a 2. fejezetében a kibertér fontosságát az információcsere szempontjából elemzi. Az információcsere főbb eszközei az alábbiak: Schengen Information System (SIS, Schengeni Információs Rendszer), Stolen and Lost Travel Documents (SLTD, Lopott és Elveszett Dokumentumok adatbázisa), Anti-Fraud Information System (AFIS, Csalás Elleni Információsrendszer), Prüm framework DNA (Prümi DNS megállapodás), Europol's Secure Information Exchange Network Application (SIENA, Europol Biztonságos Adatcserélő Hálózat Alkalmazás), EU Passenger Name Record (PNR, Utas-információs Adatbázis), European Criminal Records Information System (ECRIS, Európai Bűnügyi Nyilvántartási Információs Rendszer), European Police Record Index System (EPRIS Európai Rendőrségi Nyilvántartási Információs Rendszer), Maritime Common Information Sharing Environment (CISE, Tengeri Környezeti Közös Információ-megosztás), Visa Information System (VIS, Vízum Információs Rendszer), EURODAC – EUROpean DActylographic Comparison system, menedékjogot kérő személyek ujjnyom összehasonlító adatbázisa.

A virtuális dimenzió egy anyagilag nem létező, képzeletbeli módon megalkotott konstelláció, melynek alapján a virtuális tér számítógépi eszközökkel létrehozott digitális tér egy valós tér modelljeként, illetve fikciók alapján, a virtuális valóság a számítógépes környezet által megalkotott, akár a valóságban reprezentálható digitális világ, melyben a felhasználó is szerepet játszik. A virtuális tér egyrészt a számítógépi 3D alkalmazások és a kibertér hatásai által szimulált térként, másrészt az internet által összekötött személyek, közösségek életteréként jelenik meg, a Web3/Internet3 közössége, egy immateriális tér, amelyben földrajzi területtől független események zajlanak az idő és távolságtényezők kiiktatásával.

A virtuális tér, mivel a számítógépi 3D szimulációval és a multimédia elemek hatékony alkalmazásával szinte határtalan és felmérhetetlen hatású személyiségrombolásra képes, jelentős veszélyforrásként jelenik meg, ugyanakkor az alternatív helyzet

[12] A kibertér fogalmat William Gibson tudományos-fantasztikus (sci-fi) szerző alkotta meg az 1982-ben megjelent "Burning Chrome" című novellájában és 1984-es Neurománc című regényében a kibernetika és tér szavakból, mely egy olyan mátrix, amely színes, elektronikus, karteziánus adattájkép, amelyben az egyének és a cégek interaktív kapcsolatba lépnek az információval, sőt kereskednek vele.

szimulációkkal a rendvédelmi tevékenységeket is segíti. A gyakorlatban a virtuális tér megjelenése a térinformatikai alkalmazásokban (digitális térkép, számítógépi tervezés és 3D modellezés) is szerephez jut.[13]

A kiterjesztett valóság (augmented reality, AR) a valóság virtuális (látszólagos) elemekkel való kibővítése. Ilyen például az okostelefon helyfüggő szolgáltatása, mely során megjeleníthetők a közelben lévő üzletek és azok nyitva tartása, árukészlete stb., vagy az okos szemüveg szolgáltatásai, melyekkel az internetről azok a releváns információk közvetíthetők melyek a tekintet irányába esnek. A rendvédelemben is jól alkalmazható az AR, például egy akció során kivetíthető az épület tervrajza, a különböző távérzékelési módokkal az épületben lévő élőlények helyzete, tevékenysége követhető nyomon.

A kibővített valóság, Extended Reality (XR) a kiterjesztett valóság és a virtuális valóság kiszélesítése az interaktivitással és a mesterséges intelligenciával. A kevert valóság dimenziójában az előző valóságfajták egymást kiegészítik, illetve a felhasználó is, mint kvázi virtuális entitás az eseményeknek a részesévé válhat, mely technológia a rendvédelmi felkészítésben tartogat számos újdonságot.

A vizualizáció az egyik olyan eszközrendszer, mely a kibertér érzékelhetőségét teremti meg, azaz az elképzelések, logikai modellek, leíró és tevékenység generáló algoritmusok képi megjelenítésének, láthatóvá tételének számítástechnológiai eljárása. Az MIT[14] kutatói egy Normannak elnevezett (nyilván a Psycho főhőse után) mesterséges intelligencia alkalmazásnak a Redditen posztolt erőszakos és beteg képeket mutattak meg, majd elvégeztettek vele egy Rorschach-tesztet, mely nagyon negatív eredményre vezetett.

Az intelligens tér a fizikai térben elhelyezett nagyszámú információ-kibocsátó és információfogadó eszköz számítógépi vezérlésével, az interneten történő egymással való összekötésével a fizikai tér minden szegmensére kiterjedő információkezelés megteremtésével valósul meg. Az intelligens tér (mindenütt jelenlévő számítástechnika) fogalma a 2004.évi Szolnoki Térinformatikai Konferencián hangzott el először Detrekői Ákos (az akkori Budapesti Műszaki és Gazdaságtudományi Egyetem rektora) előadásában, aki azt új paradigmaként jellemezte. Az intelligens térben az automatikus állapotváltozási, adat és információ kibocsátó szerepet a különböző intelligens- és okos eszközök töltik be. Az állapotváltozási jelzések, adatok és információk fogadását, felfogását az intelligens- és az okos eszközbe épített szenzorok, robotok végzik az élőlények biometrikus kisugárzásának illetve fizikai megnyilvánulásainak érzékelésével együtt, ami által az intelligens tér háromdimenziós adatszerkezetként a tér egyes pontjainak állapotáról folyamatosan rendelkezik információval az abban megjelenő entitásokról és azok viselkedéséről. A felfogott adatok és információk feldolgozását a számítógép programok és a mesterséges intelligencia alapján működő számítástechnikai eszközök végzik.

Az okos eszköz (smart device) a számítógépi funkciókkal kiegészített, egyébként más célra (telefonálásra, időmérésre, látásjavításra, ételtárolásra stb.) létrehozott mechanikus vagy elektronikus eszköz, mint például az okostelefon, okos óra, okos

[13] A Nemzeti Közszolgálati Egyetemen minden évben megrendezésre kerül a Közös Közszolgálati Gyakorlat, amelynek eseményei a levezetésének tervei alapján a valóságos és a kibertérben játszódnak. Lásd: KOVÁCS Gábor: Az egyetemi közös közszolgálati gyakorlatok hatása az Államtudományi és Közigazgatási Kar hallgatóinak vezetői felkészítésére In: Auer Ádám, Berke Gyula, György István, Hazafi Zoltán (szerk.) Ünnepi kötet a 65 éves Kiss György tiszteletére. Liber Amicorum in honorem Georgii Kiss aetatis suae LXV. Dialóg Campus Kiadó. Budapest, 2018. 577-590. o.
Kovács Gábor (szerk.): VÁNDOR2017. A Nemzeti Közszolgálati Egyetem Közös Közszolgálati Gyakorlat Alap- és Indító Feladata. oktatói példán. Nemzeti Közszolgálati Egyetem. Budapest, 2017.

[14] Forrás: http://norman-ai.mit.edu/ (Letöltés ideje: 2018.07.24.)

szemüveg, okos hűtőszekrény, vagy az okos betörésvédelmi berendezés (természetes, rajtuk kívül még számos okos eszköz létezik). Az okos eszközben a beépített célszámítógép az eszköz eredeti funkciójának az alkalmazási környezetének meghatározottsága alapján való kiterjesztésére szolgál.

Az intelligens eszköz (device of intelligent) egy fizikai egységben tartalmazza a szolgáltatás minden elemét, melyet többnyire célszámítógép program vagy mesterséges intelligencia vezérel. Az intelligens eszköz nagymértékben hasonlít az okos eszközhöz, de az intelligens eszköz alapvető funkciója a környezeti hatások gyűjtése az intelligens térből. Az előrejelzések szerint 2020-ig több, mint 15 milliárd intelligens eszköz kapcsolódik majd egymáshoz világszerte.[15] Ezen eszközök kommunikációját az 5. generációs vezeték nélküli hálózat (5G) fogja megteremteni, mely 1 négyzetkilométeres körzetben 1 millió eszköznek átlagosan 100 Mbps adatátviteli sebességet fog biztosítani.

Az intelligens és az okos eszközök alkotják a tárgyak internetét (Internet of Things, IoT) és a gép-gép közötti kommunikáció (Machine-to-Machine, M2M) dimenzióját. Az eCall eszközök az Európai Útbiztonsági Akcióterv alapján 2020-ra 50 százalékkal csökkenthetik a közúti elhalálozások számát. Az intelligens és az okos eszközök azonban potenciális veszélyforrások is lehetnek. Néhány példa:

- vírus volt a bontatlan mobiltelefonokon, már a gyárban kártevő kerül az Androidra,[16]
- a telefonhívások és üzenetek eltérítésére használható kémfelszerelést találtak Washingtonban – közölte az amerikai kormány,[17]
- az akváriumon keresztül hatolt be a kaszinó rendszerébe egy hekkercsapat, egy nem túl okos okos-hőmérőből szívták le az ügyfelek titkos adatait,[18]
- az okostelefon a hangulatelemzéssel, nyomkövetéssel és más hasznos szolgáltatásával egyidejűleg veszélyes kémeszközzé válhat.

A mesterséges intelligencia (MI) az emberi gondolkodás és memória számítógépi programmal való megalkotását végzi, mesterségesen létrehozott tudat által képviselt, ez emberi gondolkodás, tanulás, reagálás reprodukálására törekvő intelligencia. A mesterséges intelligencia bonyolult szoftver, adathalmaz és üzleti logika elemeiből összetevődő rendszer, mely az emberi ingerfeldolgozást, emlékezőtehetséget, szabályalkotási, kognitív (gondolkodáson alapuló megismerő) és döntéshozó tevékenységet emulálja. Az előrejelzések szerint 2030-ra a számítógépek okosabbak lesznek, mint az emberek. A mesterséges intelligencia gyakorlati megjelenését a 2020-as évektől egyre terjedő önvezető gépjárművek forgalomba kerülésében lehet majd nyomon követni. A Moodies Emotions Analytics (Rosszkedvű Érzelem Analitika) okostelefonra letölthető web applikáció is a mesterséges intelligencia alapján működik, mely 20 másodpercnyi beszéd után az informatikai felhőbe telepített üzleti logika (analitikai motor) segítségével elemzi a beszélő hangulatát. A hazugságvizsgáló kamera szintén a mesterséges intelligencia alapján működik, mely távérzékeléssel a biometrikus jellemzőket (arckifejezés, szemöldök mozgás,

[15] Forrás: https://index.hu/tech/2011/09/13/2020-ra_15_milliard_intelligens_eszkoz_kapcsolodik_egymashoz/ (Letöltés ideje: 2018.07.24.)
[16] Forrás: https://index.hu/tech/cellanaplo/2017/03/13/virus_volt_a_bontatlan_mobilokon/ (Letöltés ideje: 2018.07.24.)
[17] Forrás: https://www.bbc.com/news/technology-43639709 (Letöltés ideje: 2018.07.24.)
[18] https://index.hu/tech/2018/04/17/az_akvariumon_keresztul_hatolt_be_a_kaszino_rendszerebe_egy_hekkercsapat/ (Letöltés ideje: 2018.07.24.)

nézés, rándulás stb.), kisugárzásokat fogja fel és elemzi azokat. Szakértői vélemények szerint hamarosan elérhetjük a szingularitást – azt az állapotot, amikor a gépek okosabbak lesznek, mint az ember – ez pedig száz év alatt húszezer évnyi fejlődést hozhat.

Az algoritmikus elemzés egy olyan prediktivitást, profilalkotást biztosító eljárás, mely összetett kapcsolatok, mély összefüggések feltárására alkalmas, a különböző adathordozókon lévő más és más fajú adatok egységes feldolgozásával. Az algoritmikus elemzést lehetővé tevő IKT az alábbi:

- digitális adatfajok kialakulása;
  - számítógépi natív;
  - digitalizált nyomtatott szöveg és hang;
  - kép/képfolyam digitalizálása;
  - biometrikus jellemzők digitalizálása;
  - téradatok;
- digitális nyomok keletkezése;
- globális elektronikai információgyűjtés;
- BigData;
- IoT.

A fentiekben elemzett IKT -éknak a szingularitás irányába mutató fejlődése jelentősen befolyásolja a közbiztonság, határbiztonság állapotának alakulását, a bűnözés növekedését vagy csökkenését. A biztonság alapja a már elemzett veszélytényezők feltárhatósága és a semlegesíthetőségük elérhetősége, mely folyamatban alapvető szerepet játszik az infokommunikációs technológiák bűnözői–bűnüldözői alkalmazási szintje. Mindkét oldal tevékenységének fontos eleme az információszerzés, az elemzés, a korai reagálás, a tervezés-szervezés, a kommunikáció, az irányítás és vezetés hatékonysága. Aki uralja a kiberteret a benne lévő dimenziókkal együtt, az lesz a győztes. Ebből fakadóan a rendvédelmi képzésnek két irányt kell vennie:

- a rendvédelmi szerveket képessé kell tenni a folyamatosan fejlődő infokommunikációs ismeretek megszerzésére;
- el kell érni, hogy a rendvédelmi szervek időben felismerjék a bűnözői oldal infókommunikációs tevékenységét és azt hatékonyan semlegesíteni tudják.

A szingularitásnak van egy nem bűnözői oldala is, mégpedig a munkanélküliség jelentős megnövelése, mely végül is a bűnözés emelkedéséhez vezethet. Az egyik leggyakoribb kérdés, ami a téma kapcsán felmerül, az, hogy vajon a gépek elveszik-e az emberek munkáját. Tera Allas, a McKinsey Global Institute vezető kutatója arra hívta fel a figyelmet, hogy már ma az állások 50 %-a esetében automatizálni lehetne a munkafolyamatok két ötödét. Pintér Róbert, az eNet kutatási vezetője szerint a mesterséges intelligencia egy új civilizációs hullámot hoz. Az automatizáció következményeként strukturális munkanélküliség alakul majd ki, például az önvezető autók terjedése miatt biztosan sokkal kevesebb sofőrre lesz majd szükség. Az Egyesült Államokban például 3,5 millióról 1 millióra csökkenhet a számuk.

A robotok rendvédelmi alkalmazása már hosszabb időre nyúlik vissza, de az egyik speciális robot, a drón (pilóta nélküli, kisméretű repülő eszköz) szinte elképzelhetetlen lehetőségeket rejt magában, főként abból adódóan, hogy már a gyermekjátéknak szánt DJI Mavic Air drón is olyan felderítő képességekkel, személy- és tárgykövetési funkcióval rendelkezik, mely a személyiségjogok komoly megsértésére alkalmas. A drónok a kiváló

felderítő és csempészeszköz adottságok mellett egyre inkább veszélyes gyilkoló eszközökké válnak, főként, ha rajokban alkalmazzák őket. Kísérlettel bizonyították, hogy a hang és arcfelismerő okos eszköz a mesterséges intelligenciája alapján azonosítani képes a célszemélyt, kiadja a parancsot a drónnak, a drón felkutatja a célszemélyt és megsemmisíti. Például az AI real selfie a szelfizés során 296 ponton érzékeli az arcot, és elemzi azt nem, kor, bőrszín, bőrtónus és bőrállapot alapján, hogy a feldolgozott információkat a minőség javításához használja fel, melyek jó alapot adnak a drón arcfelismerő rendszerének. A drónok ellen több intézkedés került bevezetésre, Svájcban kiképzett rendőr sasokat vetnek be a drónok ellen.

A robotrendőr alkalmazása is számos etikai, jogi problémát vet fel. Például milyen mértékben kelthet félelmet, alkalmazhat erőszakot, méltányosságot, reagálása értelmi, érzelmi, erkölcsi alapú-e, ki a felelős azért, ha balesetet okoz, jogsértést követ el, meddig mehet el az öntanulásban, mikor vonható újra emberi felügyelet alá, hogyan intézkedik egy önvezető autóval szemben, mi lehet a sérült robottal szembeni eljárás, hackertámadás kivédése hogyan történhet stb.

Az infokommunikációs technológiák folyamatos fejlődése úgy tűnik, hogy jobban segíti a bűnelkövetőket, mint a bűnüldözőket. A szervezett bűnözői körök hatalmas vagyona, szemben a rendvédelmi szervek anyagi lehetőségeivel és a közbeszerzés miatti elavulási ráta fokozódásával, párosulva a korrupcióval, a hatalomvággyal, a meggazdagodási vággyal óriási szinergiahatást kiváltva szolgálja a veszélyteményezők fokozódását.

A bűnözői körök a globális kibertérben, a digitális nyomok követésével, a globális elektronikai adatgyűjtéssel és a BigData, prediktív és a mesterséges intelligenciát használó információképzési alkalmazásokkal, jól képzett hekkerek megfizetésével bárhová eljuthatnak, bármely számítógép program alapján működő okos és intelligens eszközt, robotot irányításuk alá vonhatnak.

Az Europol TE-SAT, IOCTA, SOCTA elemzéseiből, értékeléseiből nyomon követhetők a kibertérből származó veszélyforrások. A TE-SAT 2018. évi értékelése[19] jól mutatja a szociális média szerepét a toborzásban, kampányban, az online rendszerek kihasználását a kommunikációban, pénzmozgásban. A kibertérben zajló bűncselekmények felfedése érdekében szorgalmazza több kormány a titkosítási eljárások tiltását. A hekker támadásokról készült statisztikák egyre több kibertérben történt támadásról számolnak be[20]. 2017-ben az FBI is vészjelzést adott ki[21].

A szándékos bűnelkövetéseken túl az informatikai biztonsági követelmények sérülése, a környezetszennyezés, a fertőzésterjedés és a tömeges migráció generál még számos veszélyforrást. Egyik piacvezető álláskereső portál önéletrajz-adatbázisához bárki hozzáférhetett, ezzel számos személyes adat védetlenné vált.

A migráció valakinek, valaminek a mozgása az élettér tartós megváltoztatása céljából. Az informatikában is migrációnak nevezik azt a folyamatot, amikor például egy alkalmazást áttelepítenek az egyik szerverről a másikra. Ezek alapján a migráció formálisan nem lehet illegális vagy legális, a migráció egy adott entitás. Az emberi migráció lehetősége is egy alapjogon nyugszik, így az nem lehet illegális, mert minden embernek joga van a

[19] Forrás: https://www.europol.europa.eu/activities-services/main-reports/european-union-terrorism-situation-and-trend-report-2018-tesat-2018. (Letöltés ideje: 2018.07.24.)

[20] Forrás: https://www.trendmicro.com/en_us/business.html, ITBN konferenciák előadásanyagai https://www.itbn.hu/index.php/hu (Letöltés ideje: 2018.07.24.)

[21] Forrás: https://pdf.ic3.gov/2017_IC3Report.pdf (Letöltés ideje: 2018.07.24.)

helyváltoztatásra.[22] A helyváltoztatás folyamata viszont lehet törvényes vagy jogszabálysértő.[23] A migráció folyamata például törvényes az országon, illetve az Schengen térségen belül, de már jogszabályok betartásához kötött a harmadik országok állampolgárai tekintetében ezen térségbe való belépéshez. Mindenkinek joga van elindulni Európa felé, de az adott európai országba történő belépés szabályait be kell tartania, azaz megfelelő úti-okmányokkal kell rendelkeznie, ennek hiányában a legrövidebb időn belül a megfelelő hatósághoz kell fordulnia. Ha a migráns nem így cselekszik, akkor jogsértést követ el, melyet az adott ország szankcionálhat, visszafordíthatja, eljárást indíthat vele szemben, kiutasíthatja területéről stb.[24] Az az adott ország belügye, hogy méltányosságot gyakorolva a migránst befogadja. Ha a migránst valaki üzletszerűen segíti a jogtalan államhatár átlépésben, az elköveti a szintén büntetendő embercsempész tevékenységet.

A menekülő nem fogható fel migránsként, mivel ő nem önszántából akar életteret változtatni, hanem kényszer hatására végszükségből cselekszik,[25] ezért a nemzetközi jog alapján az első biztonságos országnak be kell fogadnia és megfelelő emberi körülmények között kel elhelyeznie. Ezzel viszont a menekülő joga véget ér, ha az első biztonságos országból tovább indul, akkor már migránsnak minősül.[26]

A kibertér és a virtuális tér szerepe megnő a menekülő valódi menekült státuszának megállapítása során, főként akkor, ha a menekülő nem rendelkezik okmányokkal, illetve valamely bűnszervezeten keresztül megszerezte egy korábbi menekültnek minősített személy részére kiadott okiratokat. Információtechnológiailag minden feltétel adott, melyet többnyire a jogi környezet is támogat, hogy a migráns és a menekülő azonosítása, származási, kiindulási országa, élettere, szándéka felderíthető, azonosítható legyen.

A tömeges migráció életre keltése, szervezése, lebonyolítása jórészt a kibertérben történik. A toborzás, tájékoztatás, pénzmozgás, kommunikáció igénybe veszi az internetet és az egyéb távközlési szolgáltatásokat, melyek a digitális nyomok sokaságát generálják. A prediktív analitika, profilalkotás, informatikai robotalkalmazás jelentősen elősegíti a gyanúsított kör azonosítását. A globális elektronikus információgyűjtéssel a rejtett tevékenységek áruló jelei jól felfedhetők, a begyűjtött különböző forrású információkat a BigData alkalmazás megfelelő módon képes értékelni. Mindezek által a tömeges migráció előkészítése már a kiindulási helyszínen felfedhető, meghozhatók azok az intézkedések, amelyekkel az szabályozható. Nem kétséges, hogy Európának szüksége van az emberi erőforrása megújítására, a humanitárius követelményeknek is eleget kell tennie, ezért szükséges lenne, hogy a kiindulási, szerveződési környezetben tudja szabályozni a migrációt, ne utólagos, többnyire nehezen végrehajtható intézkedésekkel próbálja a bekövetkezett helyzetet valamelyest javítani.[27]

---

[22] 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.

[23] Lásd Ritecz György: A Migráció a XXI. század kezdetén. Globe Edit. Saarbrücken, 2017. 16-20. o.

[24] Balla József (2017): Határőrizeti intézkedések a migrációs válság kezelésére és megszüntetésére. In.: TÁLAS Péter (szerk.): Magyarország és a 2015-ös migrációs válság. Dialóg Campus Kiadó. Budapest, 83-100. o.

[25] Ritecz György: Minden legyen az ami, a krumplileves legyen krumplileves … Pécsi Határőr Tudományos Közlemények XVII. Pécs, 2016. 119-126. o.

[26] 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.

[27] Balla József – Kui László: A határőrizeti célú ideiglenes biztonsági határzár és határőrizetre gyakorolt hatásai. Hadtudományi Szemle 2017/1. 223-225. o. Balla József: A Magyar Honvédség helye és szerepe a határőrizeti rendszerben. Hadtudományi Szemle 2017/1. 354-364. o.

A menekülő státusz eldöntéséhez alkalmazható a DNS azonosítás, a digitális hazugságvizsgáló kamera, a beszédelemzés, a menekülő eredeti életterének jellemzőire vonatkozó kérdések feltétele és mikro nyomainak vizsgálata.[28]

Az Európai Uniónak megvannak a sajátos szervezetei és eszközei is a tömeges migráció kezeléséhez. Csak pár példát említve, rendelkezik a műholdas felderítő rendszerrel, a megfelelő informatikai robotokkal és drónokkal, amelyekkel végre tudja hajtani a globális elektronikai információgyűjtést, a Külügyi Szolgálat képes a tagállamoktól kapott titkos információk alapján és az OSINT segítségével a hatékony elemzésre és javaslattételre. Az Europol Információs Rendszer (Europol Information System, EIS), az Elemzési Projektek (Analysis Projects), a Frontex Kockázatelemzési Hálózat (Frontex Risk Analysis Network, FRAN), a kiberhírszerzés (CYBINT)[29] megfelelő lehetőséget ad a további információszerzésre és azok értékelésére. A különböző szervezeti egységek, mint az Európai Terrorelhárító Központ (European Counter Terrorism Centre - ECTC), az Europol Kiberbűnözés Központ (Europol Cybercrime, EC3), az Európai Tengerészeti Biztonsági Ügynökség (European Maritime Safety Agency), a Pénzügyi Hírszerző Egységek és a Vagyon-visszaszerzési hivatalok (Financial Intelligence Units FIUs and national Asset Recovery Offices (AROs), a Rendőri és Vám Együttműködési Központ (Police and Customs Cooperation Centres PCCCs), az Embercsempészés Elleni Európai Központ (European Migrant Smuggling Centre, EMSC) a hatékony tevékenységeket biztosítják. Az EMPACT műveletek (European Multidisciplinary Platform against Criminal Threats, Európai Bűnügyi Fenyegetettség elleni Multidiszciplináris Platform), a Terrorizmus Finanszírozásának Felderítését célzó EU-USA Program (Terrorist Financing Tracking Programme TFTP) szintén hozzájárulnak a migráció kezelhetőségéhez.

Befejezésként felvetődik néhány kérdés, mely elgondolkodtató. Jó-e az emberfeletti világ? Az agy kívülről vezérelhetővé válik? Csevegő robotok kerítenek hatalmukba a hangulatelemzést követően? Meddig lehet elmenni az ember szerepének elvonásával (amíg segíti az emberi tevékenységet, amíg kiterjeszti az ember képességeit)? Szabad-e megfosztani az embert a gondolkodástól? Szabad-e az embert kikapcsolni a döntések meghozatalából? Titkok hálózata vesz körül bennünk? Jobban jár, aki digitális analfabéta (7,5 milliárd ember közül pont engem?…hát, ha az emberi szerv kereskedőnek pont a te veséd kell!). Ami információ a kibertérben van, az meg is szerezhető, mert mindig lesznek árulók, szabályszegő munkatársak, rések a védelmi rendszerben, innováció hekker-lovasok.

[28] Angyal Miklós – Mészáros Bence: Egyek vagyunk, de nem ugyanazok – személyazonosítás és európai bevándorlás. In. Hautzinger Zoltán (szerk.): A migráció bűnügyi hatásai. Magyar Rendészettudományi Társaság Migrációs Tagozata. Budapest, 2016. 107-120. o.

[29] Forrás: http://knbsz.gov.hu/hu/letoltes/fsz/2016-3.pdf Lakatos Zsolt alezredes: Az EU felderítő-információs rendszer kihívásai és szerepe a válságkezelésben 94.o. (Letötlés ideje: 2018.06.09.)