ORBÁN JÓZSEF

A BŰNÜGYI JÁTSZMA ESÉLYEINEK MEGFORDÍTÁSA – VALÓSZÍNŰSÉG, HIHETŐSÉG ÉS MEGBÍZHATÓSÁG A TERRORCSELEKMÉNYEK ELŐREJELZÉSÉBEN

1. Bevezetés

A bűnügyi sakkjátszma reaktív, ahol az elkövető lép először.[1] A jó sakkozó felkészül az ellenfeléből, elemzi korábbi játszmáit, megtett lépéseiből prognosztizálja taktikáját, s kibontakozása előtt ad mattot. Ha lehet, bolondmattot![2] Éppen ezért a bűncselekmények előkészületi fázisában tett elhárítást – a sakk-analógiával élve a megnyitáskor adott mattot – tekinthetjük a felkészült kriminalisták igazi sikerének.

Korunk egyik legnagyobb veszélyforrása a terrorizmus, amint azt számos elemző megállapította.[3] A terrorcselekmények[4] az állampolgárok személyes érintettsége nélkül is rontják a köznyugalmat, így megelőzésük és megakadályozásuk a bűnügyi eredményesség demonstrálása mellett a társadalom közérzetére is kedvező hatással van. Előrejelzése az elkövetők ráutaló cselekményeinek és szándékainak helyes értelmezésén keresztül lehetséges.

A nemkívánatos események kockázatának valószínűségi becslése több évtizedes múlttal rendelkezik. A valószínűségi előrejelzés a mindennapok időjárásjelentéseitől kezdve az űrkutatás kockázati becsléséig mindenütt jelenlevő módszerek csoportja. Ipari felhasználásának népszerűségét egyrészt az erőforrások optimális kihasználása adja, másrészt az, hogy reális ráfordításokkal a lehetséges veszélyek nagysága elviselhető értékre csökkenthető, mivel a veszélyek teljes kiküszöbölése nem lehetséges. A teljesség igénye nélkül: a valószínűségi döntési fa az érzékeny információk azonosításához,[5] a hibafa-elemzés,[6] a Bayes-háló,[7] a gyökérok-elemzés és a bayesi oksági háló[8] példaként említhető. Egy terrortámadás lehetősége és egy súlyos baleset kockázatának elfogadható mértékű csökkentése közötti párhuzam belátható. Egy lehetséges terrortámadás teljes

---

[1] Fenyvesi Csaba: Bűnügyi sakkjátszma a kriminalisztikai princípiumok tükrében. Belügyi Szemle, 2016/11. 40-57. o.

[2] A bolondmatt a sakkjátszmában legkevesebb lépéssel adható matt, ahol két lépéssel, a lépéshátrányban lévő sötéttel játszó játékos nyer. Amint a kifejezés következtetni engedi, a vesztes aktív közreműködése is szükséges a nyeréshez.

[3] Kovács László: Biztonságpolitika. Nemzeti Közszolgálati Egyetem. Budapest, 2014. Forrás: https://lipusz.hu/pedagogia_tanulas/nke_eiv/biztonsagpolitika.original.pdf (Letöltés ideje: 2020.07.23.)

[4] A Büntető Törvénykönyvről szóló 2012. évi C. törvény (Btk.) 314.§ (1) bek.

[5] Liu, Shuang – Yang, Ziheng – Li, Yi – Wang, Shuiqing: Decision Tree-Based Sensitive Information Identification and Encrypted Transmission System. Entropy. February 2020. www.mdpi.com/journal/entropy (Letöltés ideje: 2020.07.10.)

[6] Clemens, P.: Fault tree analysis, Fourth edition, Lecture presentation, Sverdrup Technology, 1993.

[7] Orbán József: Terrorfenyegetettségi Bayes-hálós kockázatbecslés – Valószínűségszámítási módszerek a terrorizmuselleni küzdelemben. Pécsi Határőr Tudományos Közlemények XIX. Pécs, 2017. 150-154. o.

[8] Brown , Laura E. – Tsamardinos, Ioannis: A Strategy for Making Predictions Under Manipulation. in: Guyon, I. et al.: Causation and Prediction Challenge, Challenges in Machine Learning, Volume 2, Microtome Publishing Brookline, Massachusetts 2008. 31-46.

kiküszöbölésére irányuló törekvés az anyagi terhek rendkívüli megnövekedése mellett a jogállamiság szabadságfokainak kevéssé tolerálható megcsorbítását is eredményezné. A lehetséges elkövetők cselekmény előtti azonosítása és ártalmatlanítása az eredményesség mérőszáma is lehet. Az ártalmatlanítás személyre szabott eszköze az anyagi források elzárásától a letartóztatásig széles skálán mozoghat.

Mindezek alapján, társadalmi szinten a kutatóktól elvárható egy olyan optimális helyzet megtalálása, ahol a terrorkockázat és a személyi szabadság korlátozása egyensúlyban van. A tanulmány egy korábban megkezdett gondolatsor folytatásának tekinthető.[9]

2. A terrortámadások előrejelzéseinek kihívásai

Ahogy bűncselekmény, úgy terrorcselekmény is lesz a jövőben. Az események és az áldozatok száma, a megelőzésre, a felderítésre, a védekezésre tett erőfeszítések, és a kárelhárítása fordított összeg nagysága azonban nem mindegy. A terrorizmus indítékában, tartalmában és céljában is eltér a köztörvényes bűnözéstől.[10] A bűncselekmények elkövetésénél jellemzően vélt vagy valós előnyszerzés a cél úgy hogy az események lehetőség szerint ne, vagy minél később derüljenek ki. Az anyagi károkozás, vagy az élet veszélyeztetése csak járulékosan jelentkezik, az elkövető pedig a legkevésbé sem kívánja saját magát feláldozni. A terrorcselekményeknél mindez fordítottan jelentkezik, és az elkövető életének feláldozása tekinthető járulékos veszteségnek. Az elkövető szempontjából nem az anyagi nyereség, hanem a kár, a megfélemlítés mértéke és az elért nyilvánosság tekinthető a terrorcselekmény eredményességi mutatójának. A késes támadást leszámítva a terrorcselekmény jelentős előkészületi munkálatokat igényel, ami viszont esélyt ad a velük szembeni védekezésre.

A gyenge jelzések érzékeléséhez a kriminológiai, és a kriminalisztikai módszerek és ismeretek mellett számos tudományterület komoly együttműködése szükséges. Ilyen az információs technológia hírközlési és adatfeldolgozási, rendszerezési, a mintakeresési, a hálózatkutatási, a és szándékbecslési szakterülete., továbbá szükség van pszichológiai és a szociológiai területek ismeretére is. A Big Data,[11] az adatbányászat, a képfeldolgozás,[12] a mesterséges intelligencia (MI),[13] a gépi tanulás – így különösen a mélytanulássá[14][15] továbbfejlődött területe – együttes alkalmazása szükséges a ritkán előforduló és eltérő elektronikus lábnyomokon induló cselekmények észleléséhez. Az említett gyenge jelzések

[9] Orbán József: (2017) i.m.
[10] Hautzinger Zoltán: A terrorizmus elleni küzdelem idegenjogi eszközei. Pécsi Határőr Tudományos Közlemények XVI. Pécs, 2015. 204. o.
[11] Zsigovits László: A Big Data mint a rendvédelem nagy kihívása. Pécsi Határőr Tudományos Közlemények XIV. Pécs, 2013. 177-184. o.
[12] Angyal Miklós: Biztonsági és térfigyelő kamerafelvételek az igazságügyi személyazonosításban. Pécsi Határőr Tudományos Közlemények XIV. Pécs, 2013. 375-378. o.
[13] S P Maniraj, Deep Chaudhary, Vankayala Hari Deep, Vishesh Pratap Singh: Data Aggregation and Terror Group Prediction using Machine Learning Algorithms. International Journal of Recent Technology and Engineering (IJRTE) Volume-8 Issue-4, November 2019. 1467-1469.
[14] Mobilhálózati menedzsment eszközök öntanulásával a csalás, a gyanús tevékenységek, az informatikai DDoS támadás felismerésén keresztül előre jelezhető az alkalmazás.
[15] Gyires-Tóth Bálint Varga Pál – Tóthfalusi Tamás: Utilizing Deep Learning for Mobile Telecommunications Network Management. 2019 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), Arlington, VA, USA, 2019. 575-580.

miatt egyes, máshol már bevált módszerek – akárcsak az általunk többször is hivatkozott ROC[16] – bűnügyi tudás-transzplantációja[17] szükséges.[18]

Az események megtörténtét követően számos olyan tény, információ kerül a nyomozás kirakójátékába, amelyről kiderül, hogy a különböző bűnügyi munkával foglalkozó szervek számára ismert volt, de az információ súlyozása, vagy továbbítása nem úgy történt, ahogy a bekövetkezett események indokolták volna.[19]

A terrortámadás előrejelzésével kapcsolatos feladatok az alábbi öt pontban fogalmazhatók meg:

1. Milyen legyen az előrejelzés?
2. Mekkora az esemény valószínűsége?
3. Hogyan előzhető meg?
4. Ha bekövetkezik, milyen következményekkel jár?
5. Milyen előzetes kárenyhítési feladatok becsülhetők meg?

Terjedelmi korlátok miatt jelen tanulmány csak az első pont részleges megválaszolására szorítkozik a valószínűség, a hihetőség és a megbízhatóság háromszögének szempontjából.

Az előrejelzésekhez szükséges nagymennyiségű adat sokszintű átvilágítása, mintegy átrostálása alappal vethet fel a digitális magánélettel kapcsolatos adatvédelmi kérdéseket.[20] Mindezt érdemes előre tisztázni, mert számos kutatás gyakorlati hasznosulását lehetetlenítette el a humán mikro-, vagy makro környezet hatástanulmányának mellőzése. A GDPR elvek, továbbá az emberi jogok szigorú kezelése, a terrorbecslés megbízhatóságának, a túlzott lazítás pedig a személyes adatok céltól eltérő önkényes és jogellenes felhasználásának aggályát veti fel.[21] A mélytanulási módszerek a „mélyben" kikristályosítanak olyan megállapításokat, amelyek az előkészületi információk alapján, a valóság megtapasztalásának eredményeként valószínűsítenek fajra, nemre, életkorra, iskolázottságra, hajszínre, stb. vonatkozó adatokat. Amennyiben ezen adatbázis információtartalmát bármilyen szinten cenzúrázzák, úgy az eredmény – az előrejelzés – értéke nagymértékben csökken. Hasonlóan kedvezőtlen hatást eredményezhet egy önkényesen megállapított döntési szint – bias – beépítése. A jogi szabályozási környezet és a terrorcselekmények előrejelzésének harmóniája, az MI normáinak megteremtése[22] elengedhetetlen. Alapelvnek kell tekinteni a "Több adat jobb modellt épít" megállapítást.[23]

[16] ROC: Receiver Operating Chart, amely a valós pozitív megtapasztalások és a téves pozitív vakriasztások arányfüggését mutatja meg.
[17] A tudás-transzplantáció különböző tudományterületek közötti ismeretanyag átvitelt jelent, továbbá a tudás-transzferrel szemben vizsgálja az új környezet befogadó képességét is.
[18] Orbán József: Evidence, Probability and ROC In Crime Cases. Towards a Better Future: Democracy, EU Integration and Criminal Justice, Bitola, 2019 55-64.
[19] A 2001. szeptember 11-én elkövetett terrortámadás következtében 2002-ben az Interpol döntött az lopott vagy elveszett úti okmányok nemzetközi adatbázisának létrehozásáról, amely azóta már bizonyította megelőzésben betöltött szerepét. Lásd: Hegyaljai Mátyás: Az Interpol lopott és elveszett úti okmányok adatbázis (SLTD) használatának felértékelődése. Pécsi Határőr Tudományos Közlemények XVI. Pécs, 2015. 183-189. o.
[20] The right to privacy in the digital age. Forrás: https://undocs.org/A/RES/68/167 (Letöltés ideje: 2020.07.10.)
[21] Mckendick, Kathleen: Artificial Intelligence Prediction and Counter Terrorism. Chatham House. The Royal Institute of International Affairs. 2019. 12. o.
[22] Uo. 12. o.
[23] Uo. 19. o.

3. A terrorizmus azonosítása és a terrorcselekmények becslése

A Btk. a terrorcselekmény céljától, az előkészületen, a finanszírozáson keresztül az elkövetési módig mindenre szabatos választ ad. Az előrejelzésre ez esetben különösen igaz a tű keresése a szénakazalban kifejezés, ezért minden, a keresendő tevékenységre, előkészületre, az anyagi háttér biztosítására, vagy személyre vonatkozó információ segíti az azonosítás hatékonyságát. A keresés algoritmizálásához, számítógépes feldolgozáshoz az alap meghatározások, az elhatárolási pontok, a felismerést segítő főbb jegyek megadása a tévutak számának csökkentése miatt szükséges. A történetileg folyamatosan változó meghatározás[24] kiindulópontja lehet a XX. századi négy fő frontvonal: [25] a politikai, a katonai, az igazságügyi, és a pénzügyi terület, amit XXI. század informatikai fejlődésének sötét oldala ötödikként egészített ki a kiber harcvonallal.[26] Az elméleti tudományos tevékenység ezeket kellene, hogy egységbe foglalja.[27] A szervezett politikai erőszak formájaként a terrorizmus megjelenhet az állam vagy az állampolgár oldaláról egyaránt, amely túlmutat a büntetőjogi értelmezésen.[28] Előrejelzés szempontjából az állami terrorizmus nehezen érhető utol a finanszírozáson keresztül. A nem állami terrorfinanszírozás az adományokon és a felhasználási módszereken keresztül esélyt ad a leleplezésre. Ugyanakkor el kell ismerni, hogy a nem túl bonyolultan elérhető dark web,[29] és a feketepiaci vásárlás, a virtuális pénzek a források és a felhasználás elrejtését támogatja.[30] Ugyanakkor egyre több sikert mondhat magának a bűnüldözés a dark web illegális tranzakcióinak felderítésében, így reményt keltő lehet egy olyan módszer, ami tippadó a bűnfelderítésben.[31] A legváltozatosabb képet a kiber terrorizmus mutatja. Kezdve attól, hogy az internetet, mint médiát használja rémhírterjesztésre, megfélemlítésre, reklámcélokra,[32] egészen a fizikai támadásig úgy, hogy az elektronikus infrastruktúrán keresztül dolog elleni erőszakkal közvetlen kárt okoz.

A cselekmény és az elkövető motivációja szempontjából lényeges lehet a pszichológia háttér felderítése is.[33] A fenyegetettség mértékének becslése a múltbeli adatokból indul ki.[34] Az adatokból alakzat, mintázat vagy tulajdonság kereséssel, avagy

[24] OHCHR: Human Rights, Terrorism and Counter-terrorism. Fact Sheet No. 32, Office of the United Nations High Commissioner for Human Rights. Forrás: https://www.ohchr.org/documents/publications/factsheet32en.pdf (Letöltés ideje: 2020.07.10.)

[25] Vass György: Egységes meghatározás a terrorizmusra. Hadtudományi Szemle. 2009/4. 10-16. o.

[26] The Use of the Internet for Terrorist Purposes. United Nations Office on Drugs and Crime, 2012. Forrás: https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf (Letöltés ideje: 2020.07.10.)

[27] Vass György idézett meghatározása ötödikként említi a tudományos kutatói tevékenységet. Ide ékelődik be a kiberterrorizmussal kapcsolatos harcvonal. Mindez összhangban áll azzal az állításával, hogy a kutatóknak rendszeresen felül kell vizsgálniuk a korábbi elméleti megállapításokat.

[28] Kaiser Ferenc – Tálas Péter: Politikai erőszakformák. Nemzet és Biztonság 2012/5-6. 133-156. o.

[29] Bischoff, Paul: Step by step guide to safely accessing the dark web. Forrás: https://www.comparitech.com/blog/vpn-privacy/access-dark-web-safely-vpn/ (Letöltés ideje: 2020.07.10.)

[30] Ezért került az FBI és az EUROPOL célkeresztjébe a dark weben működő Silk Road kiber-feketepiac, amit 2014-ben sikeresen felszámoltak.

[31] Az Operation Disarray akcióban résztvevő FBI ügynök szerint a dark web már nem biztosít anonimitást a drogkereskedőknek. Forrás: Operation Disarray: Shining a Light on the Dark Web Nationwide Law Enforcement Action Targets Online Drug Trafficking. Forrás: https://www.fbi.gov/news/stories/operation-disarray-040318 (Letöltés ideje: 2020.07.10.)

[32] Itt említhető az Iszlám Állam internetes propagandája.

[33] Borum, Randy: Psychology of Terrorism Initiative. Psychology of Terrorism. University of Florida, Tampa, 2004. 9-17. o.

[34] Tálas Péter A terrorfenyegetettségről a számok tükrében. Nemzet és Biztonság 2011. szeptember 83-92. o.

cselekmény-vektor meghatározással lehet előszűrést végezni. Azonosítási (identifikációs – egy a sokhoz) algoritmusokkal szűrik ki a tulajdonság vektorokat. Előnye, hogy az azonossági (verifikációs – egy az egyhez) adatokhoz személyiségi jogi kifogások nélkül lehet eljutni.[35] A terrorizmus egyik finanszírozási formája a kábítószer kereskedelem. Felfedezésében az illegális internetcsatornák észlelése és a felhasználók valószínűsítése jó támpontot adhat más társadalomra veszélyes bűncselekmény leleplezéséhez is.

A becslés egy adott információ, vagy információ halmaz nem, vagy nem kellően ismert elemeinek valószínűsítésére irányuló folyamat. Ez a folyamat irányulhat múltbeli tények rekonstruálására, a jelen idejű, de más helyen történő esemény vélelmezésére, avagy egy jövőbeli cselekmény előrejelzésére. A becslés megbízhatósága a hihetőségi tényezővel arányos. A vélelem lehet statikus – hol lehetett, hol lehet és hol lesz pontokat ad meg – avagy dinamikus – honnan jöhetett, hol mozoghat, és hová mehet – ívet jelöl ki. A statikus és a dinamikus vélelmezés nem választható el egymástól, ugyanakkor a múltbeli események feltárására inkább a statikus, a jövőbeli feltételezésekre a dinamikus becslés a jellemzőbb.

4. A Bayes-módszerektől a mélytanulásig

A tömegjelenségek leírásához a pénzfeldobási esélyeket vizsgáló gyakorisági valószínűség használatos. Tömegjelenségek valószínűsége alapján az egyedi esemény, tény vagy cselekmény, de még a következmény is csak nagy hibával írható le. Ilyen egyedi felvetéseknél a Bayes-féle valószínűség használható. A Bayes tétel egyszerűsített megközelítése egy hipotézis valószínűségét adja a rendelkezésre álló bizonyítékok ismeretében. Hasonlóképp az egyes bizonyítékok valószínűsége is megadható a többi bizonyíték ismeretében. A való élet összetett jelenségeinek eredménye az elemi tényezők valószínűségéből, és azok kapcsolati rendszeréből adódik. A kapcsolati rendszert leíró, az elemi tényezőkhöz – csomópontokhoz – rendelt valószínűségi gráf a Bayes-háló. A csomópontok eseményeihez a tömegjelenségekkel és a tapasztalati eloszlási függvényével súlyozott feltételes valószínűségi tábla tartozik. Az elemi események valószínűségi lánca szorzatban adja az eredményt. A valószínűség várható értéke nulla és egy közé esik. A lánc hosszának növelésével – azaz a teljes esemény egymással logikai kapcsolatban álló tényezői számának gyarapodásával – az eredmény jellemzően a nulla felé tolódik el. Érdemes ugyanilyen módon az esemény elmaradásának valószínűségét is megvizsgálni. Az esemény bekövetkezési valószínűségének és a bekövetkezés elmaradásának hányadosa a likelihood arány, amely a különbségeket felnagyítja. A kutatási témakörre vonatkozó szemléltetéssel élve: egy terrorcselekmény bekövetkezésének valószínűsége kicsi, ezért kell az elmaradás esélyei is vizsgálni.

A gyenge jelzések további problémája, hogy az értékes adatok besüllyednek az információs zajba. A cselekmény elmaradásának esélyével összevetve az információs zajok csökkennek, mintegy kioltják egymást. Az információs zajkioltást követő arányvizsgálat után a releváns válaszok kontrasztosabbak lesznek.

A terrorcselekmény becslése folyamatos kockázatelemzést igényel ezért az online elemzés elsődlegessége nem vitatható. A módszerek közötti választás befolyással lesz az eredményekre is.[36]

[35] Grother, Patrick - Ngan, Mei – Hanaoka, Kayee: Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, National Institute of Standards and Technology. 2019. 5-6. o.

[36] Ratnapinda, Parot – Druzdzel, Marek J.: Learning discrete Bayesian network parameters from continuous data streams: What is the best strategy? Journal of Applied Logic 13. 2015. 628-642. o.

Minden információ esetében felmerül a valóságtartalom elemzésének szükségessége, az álhírek és a megbízhatatlan adatok kiszűrésének igénye. Ez különösen igaz az interneten terjedő információra,[37] amely erősen kitett a manipulációknak. Az adattömeg nagyága miatt kognitív modellezésen[38] alapuló MI nélkül a szűrés megvalósíthatatlan. A valószínűsítés megbízhatóságát annak hihetősége a – credibility – adja. A hihetőség vizsgálatot minden információforrásra – így a meta adatokra is – szükséges elvégezni. Ebből adódóan a Bayes-háló minden csomópontjának valószínűségi értékét súlyozni kell a forrás hihetőségével.

Hasonlóan fontos a megbízhatóság a – reliability – is. A terrorizmus elleni küzdelemben a katonai és a forenzikus értelmezés közelítése érdekében javasolt a megbízhatóságra vonatkozó már meglévő fogalmak közös használata.[39]

A valószínűség, az információ hihetőségi és megbízhatósági nyomkövetése az MI „mélyebb" szintjét, a mélytanulást (Deep Learning) igényli. A tanulási folyamatban feladatként adódik az emberi viselkedés, a döntések, a terrorizmus felé tévelyedés, a terror sejteken belüli és egymás közötti kommunikáció megértése és változási folyamatainak nyomon követése. Az előrejelzés megbízhatósága és a kitekintés időtartama függ a bekövetkezett események adatainak folyamatos visszacsatolásától, amelyben a sikerek és a tévedések egyformán helyet kell, hogy kapjanak.

5. Néhány módszertani hiba: a digitális előítélet és a morfológiai támadás

A döntéseket gyorsítja a logikai súlypont eltolás – durván egyszerűsítve az előítélet – amit ember alkotta szoftverek esetében, így az egyszerűbb MI-re épített rendszerekben el kell kerülni.[40] A tanulmány írásakor fellelt friss információ, hogy a Black Lives Matter mozgalom tiltakozott a MI-re alapozott arcfelismerő szoftverek használata ellen, arra hivatkozva, hogy az algoritmusok a színes bőrűekkel és a nőkkel szembeni előítéletes döntési mechanizmusokat tartalmaznak.[41] [42]Kutatások megerősítették, hogy a színes bőrűek azonosításánál a fals pozitív és a fals negatív értékek számottevően magasabbak, mint a fehérbőrűek arcfelismerésénél.[43] Módszertani hibának tekinthető az is, hogy az algoritmus származási helyének populációjára kisebb fals pozitív érték adódik, mint a nem odavalósiak esetében. Ez a terrorcselekménytől védendő helyen az eredményezi, hogy idegenek esetében nagyobb lesz a vaklárma, miközben az alappal gyanúsítható személyek közül többen kerülnek át a rostán. Feltehető, hogy a gépi tanulás tanítási fázisában elkövetik

[37] Javasolt figyelembe venni az idevágó szociológiai kutatásokat is. Vö. Kriscautzky, Marina – Ferreiro, Emilia: The credibility of information on the Internet: criteria stated and criteria used by Mexican students. Forrás: https://www.scielo.br/pdf/ep/v40n4/en_04.pdf (Letöltés ideje: 2020.07.12.)

[38] Schaffer, J. et al: Truth, Lies, and Data: Credibility Representation in Data Analysis. Forrás: https://sites.cs.ucsb.edu/~holl/pubs/Schaffer-2014-CogSIMA.pdf (Letöltés ideje: 2020.07.12.)

[39] A források megbízhatóságát a MIL-STD-6040 katonai szabvány a százalékos értékekhez rendelt kódokkal értelmezi.

[40] A problémakör szempontjából egyszerűbb MI-nek tekinthető az a rendszer, ahol az öntanulás mellett döntést befolyásoló mértékben jelen van az emberi tanítás. Önfejlődőnek nevezhető az a rendszer, amely a tanítási folyamat hibáit felismerve algoritmusait folyamatosan javítja.

[41] Alalouff, Ron: Why AI and facial recognition software is under scrutiny for racial and gender bias. IFSEC GLOBAL, July 20, 2020. Forrás: https://www.ifsecglobal.com/video-surveillance/why-ai-and-facial-recognition-software-is-under-scrutiny-for-racial-and-gender-bias/?elq_mid=4183&elq_cid=1480874 (Letöltés ideje: 2020.07.21.)

[42] Számos vállalat óriás, köztük az Amazon és az IBM felfüggesztette az MI alapú algoritmusok használatát.

[43] Grother et al. im. 6-7. o.

Lombroso sokszor idézett – börtönre szűkített – mintavételezési hibáját.[44] Valószínűleg a valós negatív minták nagyobb száma csökkentené a vakriasztások és a küszöb alatt átcsusszanó elkövetők számát.

Morfológiai támadás leginkább akkor fordulhat elő, ha a személyazonosító dokumentum hamisított fényképét az állampolgár szolgáltatja. A képet az igénylő és egy másik személy fotóiból keverik össze úgy, hogy hogy a kép egy nem létező harmadik személyt ábrázol. Azonosításkor a nem egyező pontokat a kép készítési hibájának, és nem pedig hamisításnak tekintik. Ezért mindazon dokumentumokat fenntartással kell kezelni, ahol a kibocsátó hatóság nem maga készíti az azonosítás fényképét.

A morfológiailag hamisított dokumentumok felismerésére csak úgy van esély, ha minden okmányellenőrzésnél – még a közúton is – az okmány birtokosának arcát számítógép veti egybe a dokumentumon szereplő képpel. Ehhez új okmányellenőrzési folyamatra, szélessávú adatátvitelre és megfelelő mélytanulási módszereket is használó központi informatikai háttér kiépítésére van szükség.

6. Összegzés

A terrorcselekmények előrejelzéséhez a múltbeli ismeretek mellett az aktuális események széleskörű online értékelésére van szükség. A reprezentatív elemi forrásinformáció értékélésére a valószínű, a hihető és a megbízható súlyozási kategóriákat kell alkalmazni. A súlyozott forrásokat a közöttük fennálló összefüggéseket leíró hálóba rendezve szorzatsorozatokként kell kiszámítani. A vaklárma, a téves elengedés, az információ hamisítás esélyének meghagyása elértékteleníthetí az eredményeket. Javasolt az anomáliás tevékenységek, így különösen a kritikus anyagok, emberek, szervezetek, banki tranzakciók, infokommunikációs események együttes nyomon követése, valamint a személyazonosítási módszerek újragondolása.

[44] Egy tetszőleges statisztikára igaz, hogy forrás adatok reprezentativitásának hiánya téves következtetésekhez vezet.