Lohner Klaudia – Csomós István

A KOCKÁZATELEMZÉS ALKALMAZHATÓSÁGÁNAK KÉRDÉSEI AZ ELHÁRÍTÁSBAN

BEVEZETŐ

A mai terrorizmusnak az országok politikai, gazdasági, vallási és társadalmi helyzetére gyakorolt óriási hatása világszerte egyre nagyobb aggodalomra ad okot. Számos terrorista szervezet aktív, és több országban is tevékenykedik. A terrorizmussal kapcsolatos viselkedéskutatások úgy jelölik őket, mint egyedi vagy csoportszintű szervezeteket, amelyek politikai, vallási, társadalmi, forradalmi és etnikai-nacionalista meggyőződések alapján alakultak ki. Minden terrorszervezetnek sajátos ideológiái és propagandái vannak, amelyekre a működése épül. A közelmúltban készült tanulmányokban a terrorizmus különböző okait figyelték meg, vagyis a szociális és vallási motivációjú csoportokat, a külföldiekkel szembeni társadalmi attitűdök által megfélemlített bevándorlókat, a bosszúvágyra ösztökélt embereket, valamint a jövedelmi egyenlőtlenségeket és a nélkülözést. A terrorszervezet műfaja határozza meg a támadások típusait, a célországokat, a célzott embercsoportot és a támadások jellegét. Ezek a szervezetek nemcsak erőszakos terrortámadásokat kereteznek, hanem ideológiájukat is terjesztik, hogy befolyásolják az átlagembereket.[1]

Mind a terrorista hálózatok, mind a terrorelhárító szervezetek társadalmi struktúrái és dinamikája együtt fejlődtek ki, és folytatják kölcsönös alkalmazkodásukat a változó környezethez és az innovatív technológiákhoz.[2] Tanulmányunkban egy áttekintést adunk arra vonatkozóan – a teljesség igénye nélkül –, hogy milyen módszerek és eszközök alkalmazhatók a terror elleni harc során annak megelőzésére és felderítési szakaszára koncentrálva, kiemelten a kockázatelemzési módszerekre.

[1] Chaudhary–Bansal 2022.
[2] Knoke 2015.

DOI: https://doi.org/10.36250/01259_08

A MEGELŐZÉS JELENTŐSÉGE

A terrorellenes stratégiák[3] közismert négy eszköze: (1) üldözés, amelynek keretében megakadályozzák a terrorcselekményeket, (2) megelőzés: amelynek keretében megelőzik, hogy valaki terroristává váljon vagy erőszakos szélsőségeket támogasson, (3) védekezés: a terrorcselekmények elleni védekezés megerősítését célozza, és végül (4) felkészülés: ha egy terrortámadást nem lehet megelőzni, a káros hatásait kell minimalizálni.[4] Almoqbelék tanulmányukban különböző technikai módszereket mutattak be a terrorista tevékenységek négy szakaszára vonatkozóan: (1) a bevezető szakaszra, (2) a támadást megelőző szakaszra, (3) a támadás kezdetére (4) és a támadás utáni szakaszra vonatkozóan.[5] A támadás előtti szakaszban a közelgő támadások előrejelzését célozzák meg a terroristák megfigyelésével, a kommunikáció lehallgatására tett kísérletekkel, valamint adatgyűjtéssel és adatbányászattal a rejtett trendek felkutatására és a terroristák hálózatainak felfedezésére a terroristák által az interneten hagyott tervezési és cselekvési nyomok alapján. Az ezt megelőző, bevezető szakasz visszalép a terroristává válás és radikalizálódás indikátorainak vizsgálatához, illetve ahhoz, hogy mit tehetünk e jelenség megszüntetése vagy az attól való elrettentés érdekében. Ez a szakasz még azelőttre nyúlik vissza, hogy egy támadást megterveztek volna, egy ideológiát elfogadtak volna, vagy egy személy csatlakozott volna ilyen gyűlölködő csoportokhoz.[6]

A klasszikus büntetőjogi megközelítés keretei között elsődlegesen az üldözés eszközét alkalmazzák, ugyanakkor a 2005-ös londoni terrortámadás megmutatta, hogy a terrorizmus nem valamilyen távoli ország honosaihoz köthető csupán, hanem ugyanúgy elkövethetik radikalizálódott saját állampolgárai is.[7] Ezért célszerű nagyobb hangsúlyt fektetni a megelőzésre, illetve bizonyítékok mindenáron való beszerzése helyett a hatékony megelőzéshez szükséges információ megszerzésére.[8] Innes és Thiel tanulmányukban szintén megállapítják – elsősorban az iszlamista terrorizmusra fókuszálva –, hogy a megelőzésnek központi szerepet kell kapnia minden terrorizmusellenes stratégiában, amelyeknek a következőkre kell törekedniük: (1) az erőszakos iszlamizmus különböző szintű támogatását vagy az abban való részvételt elősegítő társadalmi, pszichológiai, politikai és/vagy gazdasági feltételek kialakulásának elkerülése, (2) pontos információszerzés az erőszakos

[3] Lásd az Európai Unió terrorizmus elleni stratégiáját.
[4] Sabjanics 2019: 37–40; Walker 2008.
[5] Almoqbel–Xu 2019; Chaudray–Bansal 2022.
[6] Almoqbel–Xu 2019.
[7] Walker 2008.
[8] Walker 2005.

iszlamizmusban részt vevő vagy annak veszélyével fenyegetett személyekről és (3) az erőszakos iszlamizmusra fogékony egyének ellenőrzése vagy eltérítése az erőszakos iszlamizmustól.[9] A fentieket – némileg más aspektusból – alátámasztják Feinstein és Kaplan kutatási eredményei, amelyek azt mutatják, hogy amellett, hogy az egyes terrorszervezeteknek van egy természetes növekedési ütemük, a sikeres támadások végrehajtása növeli egy szervezet méretét. Továbbá a terrorszervezetek a méretüket egyre inkább kihasználják, aminek okán a terrorelhárítás akkor lesz a leghatékonyabb, ha az adott szervezetet nem hagyják növekedni, azaz sikeres támadást végrehajtani. A támadások kudarcba fulladhatnak azok sikertelen végrehajtása vagy az elhárítótevékenység miatt.[10]

Tanulmányunkban a megelőzéssel, így a bevezető és a támadás előtti szakasszal foglalkozunk, azonban nem kizárólag technológiai, hanem más nyomozást és felderítést támogató eszközök és módszerek bemutatásával is, különös tekintettel a kockázatelemzésre.

Információ gyűjtése, feldolgozása és értékelése

A következőkben olyan eszközöket, módszereket mutatunk be, amelyek a terrorizmus elleni harcban, elsősorban annak felderítési, illetve prevenciós szakaszában az elhárító szolgálatok segítségére lehetnek. Ebbe beleértünk az információk gyűjtésére, illetve azok feldolgozására és elemzésére-értékelésére alkalmas módszereket is. Természetesen az információgyűjtés után annak feldolgozása, majd értékelése és elemzése történik, fontos megjegyezni, hogy az egyes eszközök alkalmazása nem válik el élesen egymástól. Egy felderítési vagy hírszerző akció támogatása több módszer együttes alkalmazását igényelheti.

Nyílt forráskódú hírszerzés (Open Source Intelligence – OSINT)[11]

Az internet és a média lehetőséget biztosít a terroristáknak és terrorszervezeteknek céljaik előmozdítására, a propaganda és képzési tartalmak megosztására, illetve virtuális működésre,[12] hiszen nincs már szükségük fizikális csoportképző helyekre a szerveződéshez. Az ISIS például jelentős erőfeszítéseket tett arra, hogy a közösségi

[9] Innes–Thiel 2008.
[10] Feinstein–Kaplan 2010.
[11] Open Source Intelligence (OSINT): nyílt forráskódú hírszerzés.
[12] Chaudhary–Bansal 2022.

médián keresztül erőszakos vizuális tartalmakat állítson elő és terjesszen, hogy ismertséget szerezzen és pénzt gyűjtsön.[13] A terrorszervezetek olyan tagokat is toboroznak, akik nem vesznek részt semmilyen erőszakos támadásban, hanem kizárólag az online propaganda terjesztésére vonják be őket. Az internet térhódítása a világ lakosságának nagy részénél tehát óriási mennyiségű információ terjedéséhez vezetett a digitális térben, beleértve a terrorizmushoz kapcsolódó információkat is. Az interneten folytatott beszélgetések, tranzakciók, sugárzott médiatartalmak, közösségimédia-alkalmazások, elektronikus feljegyzések, nyilvános fórumok, adatbázisok és a dark web oldalainak jelentős része felhasználható a terrorizmussal kapcsolatos hírszerzéshez. Az ilyen nyilvánosan elérhető források törvényes hírszerzési célú kiaknázását a *nyílt forráskódú hírszerzés* (OSINT) kifejezéssel illetik. A terroristák tevékenységének visszaszorítása érdekében az interneten keresztül terjedő információkat elemezni kell, hogy azokat fel lehessen használni a terror elleni küzdelem megfelelő intézkedéseihez. Az OSINT módszere és eszköztára megoldást kínálhat ezekre a jelenségekre.[14]

Az OSINT folyamata alapvetően három fázisból áll: (1) adatgyűjtés, (2) adatbővítés, (3) megszerzett információkból való következtetés.[15] A terrorizmusra vonatkozó nyilvánosan elérhető információknak számos és változatos forrása és formája létezik. A releváns szöveges adatok értelmes összegyűjtése a szerteágazó forrásokból hatalmas mennyiségben különböző technikai kihívásokat jelent. Az adatbányászat és a nyelv feldolgozásának új technikái képesek az adatok heterogén keverékének kiaknázására és a hírszerzéshez elengedhetetlenül fontos összetett összefüggések megtalálására. Az eszközök – például a fejlett keresőmotorok, a felhasználói profilok kinyerése a nevek, a közösségimédia-fiókok, az e-mail-címek, az IP-címek stb. felhasználásával – a legkülönfélébb információkat nyerhetik ki a gyanús webhelyekről és felhasználói fiókokból.[16] Az internet, annak kihívásai és kockázatai mellett, lehetőséget nyit az elhárító és rendvédelmi szervek felderítési és elemzési platformjának bővítésére.

Emberi kapcsolatokra épülő hírszerzés (HUMINT – Human Intelligence)[17]

Az emberi kapcsolatokra épülő hírszerzés, a HUMINT történhet fedetten (a klasszikus kémkedés, a beépülés különböző válfajai), titkosan (például egy külföldi

[13] Awan 2017.
[14] Chaudhary–Bansal 2022.
[15] Chaudhary–Bansal 2022.
[16] Pastor-Galindo et al. 2020.
[17] Human Intelligence (HUMINT): emberi kapcsolatokra épülő hírszerzés.

követség munkatársán keresztül, aki tudja, kinek ad át információkat) és nyíltan (például diplomáciai tárgyalás útján vagy kihallgatás során). A HUMINT jövőjét és jelentőségét igen eltérően, sőt ellentétesen ítélik meg a biztonságkutatás különböző szereplői. Vannak, akik úgy vélik, az elektronikai eszközök térhódítása és fejlődése, a SIGINT (Signal Intelligence) különböző válfajai előbb-utóbb feleslegessé teszik vagy ellehetetlenítik a kockázatosabb és nehezebben kiépíthető, emberi források útján történő információszerzést. Míg mások épp ellenkezőleg, a hatékony terrorelhárítás előtt álló elsődleges feladatnak tekintik a HUMINT adta lehetőségek jobb kihasználását, akár helyzetek és összefüggések feltárásához, akár műveletek támogatásához. Azok, akik úgy gondolják, hogy a titkos vagy fedett emberi forrásokon keresztül történő hírszerzést vissza kell emelni eredeti, „hidegháborús" rangjára, azzal érvelnek, hogy a titkosítási technológiák, titkos alkalmazások elterjedése miatt a terroristákat egyre nehezebb megtalálni a költséges SIGINT-eljárásokkal. Ezért fokozottan kell befektetni a HUMINT fejlesztésébe, nem csupán szövetségi, hanem állami és helyi szinteken is, érvelnek például amerikai vonatkozásban.[18] Talán kijelenthetjük, hogy minden információ- vagy hírszerző metódusnak megvan a maga szerepe és jelentősége. Az OSINT és HUMINT használatának arányait, alkalmazási területeit nagyban befolyásolják a rendelkezésre álló erőforrások és az adott szituáció vagy felderítési kihívás, amellyel az elhárító és titkosszolgálati szervek szembekerülnek.

„Ötletbörze" (Crowdsourcing)

A crowdsourcing egy viszonylag új problémamegoldó technika (magát a kifejezést 2006-ban használták először), amely nagy segítséget nyújthat például a magányos terroristák azonosításában. A módszer lényege, hogy emberek tömegei járulnak hozzá tudásukkal, szakértelmükkel az egyes feladatok megoldásához, ami által olyan eredményeket lehet elérni, amelyeket csak emberi vagy csak számítógépes módszerekkel nem lehet.[19] Daren Brabham úgy határozta meg a metódust, mint egy online problémamegoldó és termelési (production) modell, amely az online közösségek kollektív intelligenciáját használja fel konkrét célok érdekében.[20] Tulajdonképpen két részből áll, az első az adatok gyűjtése (emberi forrásokból), a második pedig a szerzett információ összeállítása és elemzése. Mindkét folyamat nagyon hasznos, hiszen ezen módszer rekordidő alatt képes megtalálni az elszigetelt egyéneket,

[18] Mayer 2016; valamint Hankiss 2018.

[19] Howe 2006: 1–4.

[20] Brabham 2013.

mindemellett pedig rendkívüli gyorsasággal feldolgozza és sűríti a különböző forrásokból származó anyagokat, hogy végül egy egységes képet adjon. Ezen tulajdonságai miatt jól alkalmazható a magányos farkas taktikát alkalmazó terroristák felkutatására és azonosítására. Szintén a módszer előnye, hogy mivel az állampolgárok együttműködő részvételével zajlik, így tulajdonképpen olyan, mint egyfajta rendőrségi bűnügyi forródrót, amelyet többek között az Egyesült Államokban is évtizedek óta problémamentesen használnak.[21]

Sokan gondolják úgy, hogy ha egy információ nem titkos, akkor nem megfelelő hírszerzési szempontból, vagyis a lakosság által önkéntesen szolgáltatott információk felhasználását nem feltétlenül tartják valóban megbízható hírszerzési formának. Például Mark Lowenthal, a CIA és az amerikai külügyminisztérium korábbi elemzője szerint a tömegek nem rendelkeznek kellő bölcsességgel, csupán zavargásokat okoznak, ezért is nem hatékony a módszer. Azonban ezen állítások megfogalmazói olyan módszereket, mint például az OSINT is haszontalannak tekintenek (mivel az információ a lakosság nagy része számára szabadon hozzáférhető).[22]

Viszont fontos megjegyezni, hogy a crowdsourcing vitathatatlanul a HUMINT vagy az OSINT gyűjtésétől különálló gyűjtési diszciplína, hiszen nem teljesen fedi egymást a többi szakterülettel. Például nem tartalmazza a diszkréció dimenzióját (sem a gyűjtés formájában, sem a megszerzett információk típusában), és nem korlátozódik az „egy az egy elleni" (ügynök kontra operátor) interakciókra, mint a humán hírszerzés a klasszikus formájában. A crowdsourcing nem felel meg pontosan az OSINT elveinek sem, amelyek többek között azt feltételezik, hogy az adatgyűjtés passzív (azaz az információ a gyűjtési folyamattól független forrásból származik, és „várja", hogy összegyűjtsék). Ez az új tudományág egyesíti a HUMINT emberi és az OSINT nyilvános dimenzióját.[23]

Elemző-értékelő tevékenység

Az elemző-értékelő tevékenység szerepe mind a bűnügyi, mind a nemzetbiztonsági területen felértékelődött. Az elemzés az információk sikeres felhasználásának kulcsa, a nyers adatokat operatív információvá alakítja át. Ez a hírszerzési folyamat öt szakasza – gyűjtés, értékelés, összevetés, elemzés, tájékoztatás – közül a negyedik. A hatékony elemzői eljárások nélkül a hírszerzési folyamat egyszerű tárolási

[21] Coultas 2015.
[22] Lowenthall 2012: 112–113.
[23] Herhkovitz 2020.

és visszakeresési rendszerré silányul.[24] A növekvő információmennyiség feldolgozására nem elegendő tehát az adatok strukturált tárolása, ahogy a megfelelő szoftverek alkalmazásának képessége sem. Az adatok, információk összefüggéseit hozzáértő szakembereknek kell értékelniük és elemezniük annak érdekében, hogy az így kapott eredmények felhasználhatóvá váljanak. Az elemzői területhez számos elemzési módszer, technika és eszköz kapcsolódik, amelyek közül csak az elhárítás és a terrorfelderítés szempontjából leginkább jelentősekről teszünk említést.

TERRORIZMUS ÉS SZERVEZETT BŰNÖZÉS

Számos tanulmány foglalkozik a terrorizmus és a szervezett bűnözés kapcsolatával.[25] Shelley és Picarelli szerint bár a terroristák és a szervezett bűnözők indítékai a legtöbbször eltérnek egymástól, ez nem minden esetben igaz, ugyanis a terrorizmus és a szervezett bűnözés közötti kölcsönhatás egyre mélyebb és összetettebb.[26] A szervezett szinten működő terrorizmus elemzésénél a szervezett bűnözés területén már bejáratott elemzői módszerek és technikák alkalmazhatók. A leggyakoribb ezek közül a hálózatelemzés és az elkövetői csoport elemzése. Amennyiben kifejezetten elemzési technikáról beszélünk, akkor a különböző áramlási ábrák bírhatnak relevanciával, illetve a hívásforgalmi és banki tranzakciós adatok elemzését érdemes kiemelnünk.

Elkövetői csoport elemzése

Az elkövetői csoport elemzése képet ad az elkövetői csoportok tevékenységéről, dinamikájáról, valamint egymáshoz és a bűncselekményhez való kapcsolatukról. A nyomozó hatóság a rendelkezésre álló eszközök, módszerek és erők bevezetése során a kapott információkat feldolgozva térképezheti fel a bűnözői csoportot vagy akár a bűnszervezetet. Az elemzés célja:

- a kulcsfigurák meghatározása;
- meghatározni a személyek ellen bevethető technikai eszközöket (megfigyelés, telefonlehallgatás);
- a gyenge láncszemek meghatározása a bűnszervezetben (azok a személyek, akik hajlandóak a nyomozó hatósággal együttműködni és információt

[24] Sparrow 1991.
[25] Pulido Gragera – Sanso 2014.
[26] Shelley–Picarelli 2005.

szolgáltatni a bűnszervezet működéséről, felépítéséről, tagjairól és az általuk elkövetett vagy elkövetni kívánt bűncselekményekről);
- pénzáramlás és áruforgalom meghatározása, az esetleges pénzügyi vizsgálat kezdeményezése érdekében;
- meghatározni, mely információval rendelkeznek, melyek lehetnek fontosak az eljárás sikeres lefolytatásához;
- meghatározni, hogy szervezett bűnözői csoport-e a csoport;
- meghatározni, ki a csoportvezető;
- meghatározni a szervezeten belüli viszonyokat;
- meghatározni a tagok számát, a tagokat, hogy azok milyen kapcsolatban vannak egymással, hogyan épül fel a munkamegosztás, milyen bűncselekményeket követnek el, egyes bűncselekmények rendelhetőek-e személyekhez.

Az elemzés szemléltethető jelentésben, táblázatban, kapcsolati, cselekmény-, esemény- és áramlási ábrákon.[27]

Hálózatelemzés

A nemzetközi bűnszervezetek – legyenek azok terroristák vagy nemzetközi szervezett bűnözők – gyakran hálózati struktúrát használnak. A szeptember 11-i, a World Trade Center (WTC – Világkereskedelmi Központ) tornyai és a Pentagon elleni támadást végrehajtó elkövetők egy nagyobb szervezet különálló sejtjei voltak, amelyek mindegyike egymástól elkülönülten és függetlenül működött.[28] Az ilyen hálózati struktúra nem egyedülálló, sőt, számos más terrorista csoportot és számos új nemzetközi szervezett bűnözői csoportot is jellemez. A hagyományos maffiatípusú szervezetek hierarchikus, felülről lefelé irányuló struktúrájával ellentétben a szervezett bűnözői csoportok, például a kolumbiai drogkartellek és az orosz nyelvű szervezett bűnözés lazán szervezett sejtek hálózataként működnek. A sejtek szervezeti rugalmasságot biztosítanak, csökkentik a bűnüldözés behatolásának lehetőségét, és nagyobb hatékonyságot biztosítanak. A hálózati struktúrák megnehezítik a vezetők azonosítását, miközben csökkentik az egyes szervezeteken belüli vezetőség méretét. Így a modern szervezett bűnözői csoportok és a vezető terrorista szervezetek inkább hasonlítanak a modern, „lapos" üzleti struktúrákra, mint a régebbi vállalatoknál, például a Ford Motor Companynál és az acéliparban megtalálható többrétegű szervezetekre.[29]

[27] Nyitrai 2015: 141–147.
[28] Hedges 2001: B10.
[29] Williams 1998.

Social Network Analysis – Kapcsolatháló elemzés (SNA)[30]

A társadalmi viselkedés elsősorban a társadalmi kapcsolatokon keresztül jön létre. A más emberekkel való kapcsolataink alakítják a világról alkotott képünket, megerősítik identitásunkat, és az interakciók mindenféle lehetőséget és erőforrást biztosítanak számunkra ahhoz, hogy a dolgokat véghez vigyük. A hálózatokhoz kapcsolódó társadalmi tőke egyben a bűnözés elősegítésének egyik elsődleges módja is.[31] A nemzetközi terrorizmus tendenciáinak nyomon követése során kulcsfontosságú kérdés a szociális hálózatelemzés hasznossága mind elméleti szempontból, mind módszertani eszköztárként, a terrorszervezetek megértéséhez és értékeléséhez, valamint a terrorellenes politikák és gyakorlatok kidolgozásához a terrortámadások felderítése és megszakítása érdekében. A jelenlegi terrorista hálózatok decentralizált, rejtett jellege időszerűvé teszi az SNA alkalmazását.[32] A terrorizmus kutatásában elért előrelépések hatással vannak a titkos, titkos és illegális hálózatok más típusainak – például a fegyverkereskedelem, a gyémántcsempészet, az ember- és szexkereskedelem, a nukleáris fegyverek elterjedése, a mérgező hulladékok ártalmatlanítása és a veszélyeztetett fajokkal való kereskedelem – vizsgálatára és meghiúsítására. A matematikusok, játékelméleti szakemberek és informatikusok matematikai modelleket és számítógépes algoritmusokat dolgoznak ki, hogy felmérjék a terrorista tevékenységek felderítésének és megzavarásának lehetőségeit különböző körülmények között, valamint olyan stratégiákat, amelyek támogathatják a terrorelhárító szervezeteket a terrorista szerveződések destabilizálásában. A jövőbeli hálózatkutatás kulcskérdései közé tartozik:

- a modern terrorizmus négy történelmi hullámának szigorú összehasonlító elemzése a jelenlegi és a jövőbeli hullámokra vonatkozó támpontok érdekében;
- átfogóbb, koherensebb és integráltabb elméleti modellek létrehozása, amelyek képesek magyarázatot adni a terrorista hálózatok kialakulására, szerkezetére és hatásaira;
- új módszerek kidolgozása a terroristák közötti hálózati kapcsolatok mérésére;
- több laboratóriumi kísérlet elvégzése a nehezen hozzáférhető és veszélyes helyszíni megfigyelési adatok gyűjtésének alternatívájaként;
- valamint nagy méretű, jó minőségű kapcsolati adathalmazok létrehozása a terrorizmussal kapcsolatos társadalmi hálózatelméletek tesztelésére.[33]

[30] Social Network Analysis (SNA): szociális hálózatelemzés.
[31] Hulst 2009.
[32] Malm–Nash–Moghadam 2016.
[33] Hulst 2009.

A szerveződés szintje és a fellépés módja

A terrorizmusnak számos osztályozási rendszere létezik, amelyek közül egy magányos és szervezett elkövetőkre bontja szét őket. A terroristák csoportokba való szerveződése ugyanúgy nem egységes, mint ahogy nem azonosak intellektuális képességeik, képzettségük és szociális hátterük sem. Beszélhetünk egy hatalmi láncolatba illeszkedő terrorista sejtről, mint az al-Káida vagy az Iszlám Állam; irányított sejtekről, amelyek a „szuperszervezetektől" függetlenül jönnek létre; önálló sejtekről, amelyek nem tartanak fenn formális kapcsolatot terrorhálózatokkal; és magányos terrorista elkövetőkről.[34]

A szerveződés szintje természetesen jelentős mértékben befolyásolja azt, hogy milyen elemzési vagy információgyűjtő technikát alkalmazzunk egy adott helyzet, kihívás felderítése vagy megoldása érdekében.

Claire Ellis és munkatársai 2019-es tanulmányukban három csoportra osztják az ISIS nevében merényleteket elkövetőket:

- egyedüli elkövetők, akiket az ISIS valamely propagandaanyaga vagy üzenete inspirált, ihletett az elkövetésre, de nem kap konkrét utasítást vagy iránymutatást a cselekménye elkövetéséhez;
- távolról irányított terrorista, aki instrukciókat, távoli irányítást kap a cselekményhez;
- távoli irányítást és távolról szervezett logisztikai támogatást kap, mégis a hálózattól elszigetelten működik annyira, hogy letartóztatása esetén ne veszélyeztesse azt.

Kenyon és munkatársai szerint a terrorizmus elleni elhárító munka talán legnagyobb problémáját a magányos terroristák elleni fellépés jelenti. Mivel egyéni elkövetőkről van szó, ezért hiányzik az a szélesebb hálózat, amelynek tagjai által esetlegesen elkövetett hibák vagy botlások felhívnák a csoportra a figyelmet. Egyik kutatásuk az 1994–2014 közötti merényletek felderítési eredményességét vizsgálta, amelyben arra a következtetésre jutottak, hogy az egyszereplős akciók 30%-át derítették fel, szemben a csoportosan szervezett elkövetések 81%-ával.[35]

A magányos elkövetők vizsgálatára és felderítésére tehát kevéssé használhatók azok az eszközök és módszerek, amelyek a szervezetszerű működésnél bevethetők (például hálózatelemzés, elkövetői csoport elemzése).

[34] Haller–Ivaskevics 2020.
[35] Kenyon–Baker-Beall–Binder 2021.

KOCKÁZATELEMZÉS

A kockázatelemzés valamilyen sérülés, hátrány, veszteség bekövetkezésének a valószínűségét igyekszik meghatározni oly módon, hogy az esemény bekövetkezését (vagy adott esetben az egyén viselkedését) befolyásoló tényezőket összegyűjti és elemzi.[36] A terrorizmus kockázatának mérésére számos eszközt fejlesztettek ki. Ezek azon alapulnak, hogy azonosítják azokat a kockázati faktorokat, amelyek segítségével annak valószínűségét vizsgálják, hogy adott személy aggodalomra okot adó magatartást tanúsít-e. Például radikalizálódni fog-e, vagy elkövet-e egy merényletet.

Pszichológiai szempontú kockázatelemzés

Az erőszak pszichológiai szempontú kockázatértékelési vizsgálata előtt lényeges, hogy megismerjük általánosságban az agresszív, erőszakos viselkedés pszichológiai és magatartás-tudományi értelmezéseit. Az agresszió kifejezés a latin „aggredior" az „ad-gredi" szóból származik, jelentése: „odalépek", „közelítek". A mai szóhasználatban: „agresszív" – támadó, testi vagy lelki ellenségeskedő magatartás. A tudományos szakirodalomban a terrorizmushoz hasonlóan az agressziót is nagyon sokféleképpen definiálták. A legtöbb meghatározás a másoknak okozott fizikai, pszichikai károkat, szenvedéseket hangsúlyozza. Az agresszió magyarázatában lényeges a destruktív aspektus és az elkövető szándéka a viselkedés agresszióként való meghatározásának szempontjából.

A különböző elméleti megközelítések a konkrét esetekre, az egyéni szintre vonatkoztatva nem minden esetben adnak magyarázatot. A témával kapcsolatos kutatások ismerete nélkül viszont nehezebb megérteni, milyen indítékok késztetnek arra embereket, hogy kegyetlen módon cselekedjenek másokkal szemben.

A terrorizmus pszichológiájáról sokféle elmélet született, de viszonylag kevés a kontrollált, empirikus tanulmány. A terrorizmust korábban pszichológiai és viselkedési deviancia patológiás megnyilvánulásának tekintették. A pszichoanalitikus felfogásmód alapján úgy gondolták, hogy a terrorizmus pszichopatológiájának hátterében a gyermekkorból eredő öntudatlan indítékok húzódnak. A pszichológiai szempontú kockázatértékelés ugyanakkor lényeges, mert a terrorista elkövetők temperamentuma, ideológiája, gondolkodása és kognitív képességei nagyon változatosak lehetnek.

[36] HERRINGTON–ROBERTS 2012.

Erőszakkockázat-felmérés

Az erőszakkockázat-felmérés számos beszámolója Paul Meehl[37] kanonikus megkülönböztetésére támaszkodik a „klinikai" és a „tényszerű" (néha statisztikainak nevezett) predikció között.

A klinikai módszerben az értékelő egyesíti vagy feldolgozza az információkat a fejében. A kockázati tényezőkre vonatkozó adatokat személyes megítélés útján kombinálják. A tényszerű vagy statisztikai módszerben az emberi tényezőt kiküszöbölik, és a következtetéseket kizárólag az adatokat és a kulcseseményeket tartalmazó diagramokba vezetik be, amelyek tapasztalati (empirikus) úton szerzett háttér-információkat tartalmaznak.

Az elmúlt években számos olyan kockázatértékelési eszközt fejlesztettek ki, amelyekre nem jellemző az egyszerű klinikai-aktuáriusi dichotómia. Helyette a kockázatértékelési folyamat skálán helyezhető el: a teljesen strukturálatlan („klinikai") értékelés a kontinuum egyik pólusát foglalja el, a teljesen strukturált („aktuáriusi") értékelés pedig a másikat, a részben strukturált és részben strukturálatlan értékelés pedig a kettő között található.

A klinikai megközelítés tehát az, amelyben a klinikus választja ki és kombinálja a kockázati tényezőket szakmai megítélése alapján. A módosított klinikai becslésnél ezt annyiban változtatják, hogy a folyamat egyik elemét (a tényezők kiválasztását) empirikus úton határozzák meg. A tisztán statisztikai, tényszerű kockázatbecslés a tényezők azonosítását, mérését és kombinációját is strukturálja. Ennek módosított megközelítése, amikor a statisztikai pontszámokat – az egyedi esetek miatt – klinikus által végzett felülvizsgálat alá vonják.

Kiran M. Sarma[38] a kockázatelemzés módszerére vonatkozóan három megközelítést foglal össze: (1) a segítség nélküli/önálló szakmai megközelítés, (2) strukturált szakmai megközelítés (SPJ), (3) tényszerű (statisztikai) megítélés. A három kockázatelemzési módszert ő is az alapján különíti el egymástól, hogy a kockázatok kategorizálása mennyire történik szubjektíven vagy objektíven. Sarma az SPJ-módszert tartja a leghasznosabbnak, amely a kockázati tényezők azonosítását és mérését is magába foglalja. A HCR-20[39] strukturált szakmai megközelítésű kockázatértékelési eszközben például húsz kockázati tényezőt sorolnak fel, és minden egyes kockázati tényező kap egy értéket: 0-t, ha hiányzik az értékelt faktor, 1-et, ha esetleg vagy korlátozott mértékben fennáll, és 2-t, ha határozottan jelen van.

[37] Meehl 1954.
[38] Sarma 2017.
[39] Webster et al. 1997.

A meglévő kutatások alapján úgy tűnik, hogy az erőszak kockázatának négy közös, egymást átfedő dimenziója közül – *büntetett előélet, felelőtlen életmód, pszichopátia és bűnözői attitűdök, visszaélés kábítószerrel* – egyik sem kizárólagos jellemzője a terroristáknak. Ezenkívül kevés empirikus bizonyíték támasztja alá a terrorizmus egyéb feltételezett kockázati tényezőinek érvényességét, amelyek meghaladják a már nyilvánvalókat (életkor, nem, családi állapot). Valójában a legerősebb empirikus megállapítások teljesen negatívak: a terroristákra általában nem jellemző az, hogy szegények, elmebetegek, szerhasználók, pszichopaták vagy bűnözők lennének. Az öngyilkos merényleteket elkövetők sem hajlamosak klinikai értelemben az öngyilkosságra. A mai napig egyetlen tanulmányozott társadalomban sem találtak olyan személyiségjegyeket, amelyek megkülönböztetik a terrorizmusban részt vevőket azoktól, akik tartózkodnak tőle.[40]

Az erőszakkockázat-felmérés pszichiátriai módszereinek alkalmazhatóságát a terrorizmussal összefüggésben azonban nem lehet teljesen figyelmen kívül hagyni annak ellenére, hogy a mentális betegség önmagában nem tekinthető terrorizmuskockázatnak. Egy terrorcselekmény elkövetési kockázatának elsődleges értékelésekor azonban lényeges szempont lehet az adott személy erőszakkockázati mintáinak megismerése arra vonatkozóan, hogy az élettörténetében előfordult-e, és ha igen, akkor milyen körülmények hatására alakult ki az erőszakos magatartás.

Az 1. táblázat mutatja, hogy Blazsek és Wernigg[41] szerint melyek az agresszió/erőszak kockázatértékelésének általános szempontjai és kérdései.

1. táblázat: Agresszió/erőszak kockázata a rövid kockázatbecslő skála alapján

Statikus (anamnesztikus) faktorok	**Dinamikus (jelenlegi) rizikófaktorok**
Erőszakos cselekmények a közelmúltban	környezetre irányuló agresszív szándék
Korábbi fegyverhasználat (bármilyen fegyverrel)	fegyverhez való hozzáférés (bármilyen fegyverhez)
Férfi nem	paranoid gondolatok, téveszmék
35 év alatti életkor	erőszakos imperatív hallucinációk
Bűnügyi előzmények	düh, agitáció, frusztráció
Korábbi veszélyes cselekmények	erőszakos gondolatok
Gyermekkori abúzus	nem megfelelő szexuális magatartás
Szerepzavar/szerepkonfliktus	önkontroll képességének csökkenése
Anamnézisben kóros alkohol-/szerhasználat	jelenlegi kóros alkohol-/szerhasználat

Forrás: a szerző szerkesztése

[40] Monahan 2011.
[41] Blazsek–Wernigg 2015.

1. Korábbi erőszakos magatartás, cselekmények (a jövőbeni, potenciálisan előforduló erőszakos megnyilvánulások legvalószínűbb előjelei):

- Fenyegette-e a személy környezetét fizikálisan, és járt-e ez mások bántalmazásával?
- A személy múltbeli vagy mostani viselkedése utalt-e azon szándékára, hogy másokat fenyegessen, és ezen szándékát szóban vagy másképpen kifejezte-e?
- Felbujtott-e másokat erőszakos cselekményekre?
- Fenyegetett-e másokat pszichológiai nyomásgyakorlással?
- A fenyegetések gyakorisága és intenzitása?

2. A korábbi fegyverhasználat szerepe:

- Használt-e lőfegyvert a személy a korábbiakban? Ha igen, milyen lőfegyvert? Milyen körülmények között?
- Használt-e szúró-/vágóeszközt a személy a korábbiakban? Ha igen, milyen eszközt? Milyen körülmények között?
- Használt-e a személy közönséges tárgyakat fegyverként?

3. Másokat fenyegető vagy másoknak ártalmat okozó szándék kifejezése (szóban vagy írásban):

- Van-e jele annak, hogy a személy másoknak ártani akar?
- Ha igen, milyen módon?
- Fenyeget-e konkrét személyeket vagy csoportokat?
- Van-e utalás a tervezett elkövetés módjára?

Borum[42] a terrorizmusban való részvétel kockázatértékelésének kidolgozásához nyolc lehetséges klaszter kidolgozására tesz javaslatot: Affektus/Emóció, Viselkedés, Kognitív stílus, Hiedelmek/ideológia, Attitűdök, Szociális tényezők, Identitások és Képességek. Az első három a gondolkodás, az érzelem és a viselkedés alapvető pszichológiai konstrukcióinak felel meg. A klaszterek nem a kockázati tényezők egyszerű számbavételét szolgálják, hanem sokkal inkább azt, hogy az értékelő elegendő releváns információval rendelkezzen ahhoz, hogy használható véleményt tudjon adni a kockázat jellegére és valószínűségére a terrorizmusban való egyéni részvétellel összefüggésben. A terrorizmusban való részvétel kockázatának konceptualizációja – az orvosi és pszichológiai esetek megfogalmazásához hasonlóan – a 2. táblázatban látható lépéseken keresztül történhet.

[42] Borum 2011; Dean 2014.

2. táblázat: A terrorizmusban való részvétel kockázatának konceptualizációja

1.	**Viselkedés-történeti elemzés**	**A személy tevékenységéhez kapcsolódó múltbeli minták vizsgálata. Kulcsfontosságú az egyéni élettörténet kritikus eseményeinek és viselkedéseinek azonosítása, amelyek a terrorizmusban való részvételre utalhatnak.**
2.	**Motivációs elemzés**	Azoknak a támogató, illetve elkerülő motivációknak, érzelmeknek, attitűdöknek, meggyőződéseknek és szituációs tényezőknek az azonosítása, amelyek jelentősek lehettek az egyén döntéseiben vagy viselkedésében, valamint azoknak, amelyek esetleg felerősíthetik vagy csökkenthetik a kockázatot. Fontos figyelembe venni az emberi motiváció bonyolultságát, ezért ritkán lesz egyedi vagy egyszerű válasz arra, hogy miért „történt meg" az adott viselkedés.
3.	**Sebezhetőségi elemzés**	A kulcsfontosságú sebezhetőségek – belső vagy szituációs – meghatározása, amelyek az adott időpontban növelhették az egyén érdeklődését a motivációs tényezők iránt. A terrorizmusban való részvétellel összefüggésben Horgan[43] a sebezhetőségeket olyan tényezőként határozza meg, amelyek oda vezetnek, hogy „egyes emberek nagyobb nyitottságot mutatnak a fokozottabb részvételre, mint mások". Egy közelmúltbeli esemény felkeltheti az igazságtalanság érzését, az elszenvedett veszteség kétségbeesett igényt vált ki a személyközi összetartozásra, vagy olyan krízis történt, amely megzavarja az egyén önérzetét. Ezen sérülékenységek bármelyike felerősítheti bizonyos push és pull tényezők befolyásos hatásait.
4.	**Összefoglaló elemzés**	Az összefoglalás részletezi a releváns viselkedéseket/döntéseket befolyásoló tényezőket és kölcsönhatásokat.[44]

Forrás: a szerző szerkesztése

Az erőszakos szélsőségesség kockázati tényezőinek meghatározásában jelentős problémát jelent a bázistényezők hiánya. Clemmow és munkatársai[45] tanulmányukban a bázistényezők kialakításához online kutatást végeztek, amelynek során a magányos elkövetői kategóriába tartozó (n = 125) minta adatait hasonlították össze az általános populáció (n = 2108) mintájával. Az összehasonlítás számos jelentős különbséget azonosított: a magányos terroristák a bűncselekmények vagy erőszak elkövetését támogató erkölcsre vonatkozóan fokozottabb kognitív hajlandóságot és szituációs indikátorokat mutattak, ugyanakkor az általános minta gyakrabban mutatott védő tényezőket. Az eredmények arra utalnak, hogy mérhető különbségek vannak a kockázati tényezők prevalenciájában a magányos terroristák és az általános népesség között. Véleményük szerint egyetlen tényező sem jelzi előre az erőszakos

[43] Horgan 2005.
[44] Persons 2008.
[45] Clemmow 2020.

szélsőségesség magatartást, és ez befolyásolja a kockázati és védelmi tényezők kölcsönhatásának megértését, valamint az erőszakos szélsőségesség kockázatértékelését.

Az erőszakos szélsőségesség viselkedési mutatói

Az erőszakos szélsőséges viselkedésáltal jelentett kockázat értékelésének másik gyakori megközelítése az, hogy a viselkedési mutatókra összpontosít. A kutatók a radikalizálódási folyamat viselkedésbeli megnyilvánulásaiban olyan közös elemeket kívántak találni, amelyekre a kockázatértékelési döntések meghozatalát alapozni lehetett. Borum[46] a radikalizálódási folyamatot vizsgáló kutatások közül kiemelte Gartenstein-Ross, Goodman és Grossman munkáját, amely a radikalizálódás folyamatának viselkedési megnyilvánulásaira összpontosított az Egyesült Államokból és az Egyesült Királyságból származó 117 dzsihádista terrorista esetében.

A kutatók hat olyan tényezőt azonosítottak, amelyek szignifikánsan gyakoribbak voltak a mintában:

- az iszlám szabályalapú értelmezése;
- kizárólag a vallási hatóságokba vetett bizalom;
- az iszlám és a Nyugat közötti összeegyeztethetetlennek vélt szakadék;
- alacsony tolerancia és személyre szabott reakció az érzékelt teológiai eltérésekkel szemben;
- a vallási meggyőződések másokra való ráerőltetésének kísérlete;
- politikai radikalizálódás (nyugati összeesküvés az iszlám leigázására).

Schmid[47] átfogóan összegezte a radikalizálódási folyamat és a viselkedési mutatók kapcsolatát, amely alapján Brandenburg német szövetségi tartomány meghatározta a potenciális viselkedési indikátorokat:

- látható változások az öltözködési stílusban és a viselkedésben;
- szakítás a saját családdal és új barátok felé fordulás;
- állandó hivatkozás a vallásra, amely mindenre magyarázattá válik;
- azokat a muszlimokat, akik nem követik a szigorú vallási gyakorlatot, elítélik, mint a hitetleneket;
- harci sportokban és túlélő tréningeken való részvétel;
- csalás és más bűncselekmények a nem hívők ellen;
- részvétel radikális prédikátorok vallási szemináriumain;

[46] Borum 2011.
[47] Schmid 2013; Dean 2014.

- dzsihádista honlapok látogatása és dzsihádista videók megtekintése;
- nyelvi képzések után külföldi utazások;
- a felderítés elkerülésére irányuló erőfeszítések (útlevél elvesztése stb.);
- hirtelen visszaváltás nyugati ruházatra, bulizás a támadás előtt.

A radikalizálódásról, deradikalizálódásról és radikalizálódás elleni küzdelemről szóló szakirodalom Schmid[48] kiterjedt és átfogó áttekintése szerint a következő nyolc pontot széles körben viszonylag jól megalapozott tudásnak tekinti a radikalizálódott személyek terrorizmus felé fordulásáról:

- A legtöbb terrorista klinikailag normális, bár tetteiket széles körben úgy tekintik, hogy erkölcsi értelemben normán kívüliek.
- A terroristák háttere nagyon változatos; a terrorizmushoz sokféle út vezet, és nincs egyetlen terroristaprofil.
- A radikalizálódás általában fokozatos, szakaszos folyamat.
- Az egyéni szegénység önmagában nem okoz radikalizálódást a terrorizmus irányába, de a munkanélküliség szerepet játszhat.
- A sérelmek szerepet játszanak, de gyakran inkább mozgósító eszközként, mint személyi okként, élményként.
- A társadalmi hálózatok/környezetek döntő szerepet játszanak abban, hogy a kiszolgáltatott fiatalok a terrorizmushoz vonzódjanak.
- Az ideológia gyakran fontos szerepet játszik abban, hogy az igaz hívők számára biztosíthat „engedélyt a gyilkolásra".
- A terrorizmustól való elszakadás gyakran deradikalizáció nélkül történik.

Geoff Dean (2014)[49] a *Neurokognitív kockázatértékelés az erőszakos szélsőségesek korai felismeréséhez* című könyvében beszámolt azokról a kihívásokról, amelyek a gyakorlatban nehézséget jelentenek a kockázatok értékelése során.

A kognitív idegtudomány egy viszonylag új tudományos kutatási terület, amely a kognitív pszichológia és általában az idegtudomány együttműködéséből jött létre, és nem meglepő módon „kognitív idegtudománynak" nevezik. Ward szerint „a kognitív idegtudomány egy áthidaló tudományág egyrészt a kognitív tudomány és a kognitív pszichológia, másrészt a biológia és az idegtudomány között".[50]

Dean az erőszakos szélsőséggel összefüggő neurokognitív folyamatok figyelembevételével vizsgálta a kockázati mutatókat. Szerinte az észlelés módja összefügg az erőszakos eszmék kialakulásával. Az agy neuroplaszticitása a tapasztalatok hatására

[48] Schmid 2013.
[49] Dean 2014.
[50] Ward 2010: 4; Dean 2014.

kölcsönhatást eredményez a kognitív folyamatok és az agyi neuromechanizmusok között. A szélsőséges felfogásokkal való azonosulás ismételt megerősítése hozzájárulhat az erőszakos és szélsőséges nézetek elfogadásával kapcsolatos szilárd meggyőződések kialakulásához, és ez radikális gondolkodásmódhoz vezethet. Ennek hatására az egyén felkészül az erőszakos cselekedetekre, és a szélsőséges viselkedés racionalizálásával és igazolásával védekezik. A folyamat ciklikus jellege miatt előfordulhat, hogy a csalódás befolyásolhatja az elkövető gondolkodásmódját. Ebből azonban nem következik a radikalizálódás megszűnése, leginkább egy spirális folyamathoz hasonlítható, amely átmenetileg szünetelhet, és ismételten megjelenhet.

A „megfelelő feltételek"[51] mellett az idegi aktivitás a szinaptikus kapcsolatok megerősödéséhez vezethet. A neuroplaszticitás jelentősége az erőszakos szélsőséges gondolkodással kapcsolatban azzal függ össze, hogy az agy működésére hatással vannak az alábbi tapasztalatok:

- *ismétlés* (az erőszak ismételt megtekintése a valóságban vagy virtuálisan videójátékokban, a *Korán* erőszakot kiváltó verseinek szokatlan tanulása, agymosás stb.);
- *érzelmi izgalom* (traumatikus események átélése; erőszakos videók megtekintése; tragikus hírek; a terrorizmus elleni háború médiavisszhangja stb.);
- *újdonság* (a véletlenszerű erőszakos cselekmények durva megtekintése új és különböző módokon);
- *a figyelem gondos összpontosítása* (erőszakos eszközök tanulmányozása és gyakorlása, például céllövöldözés fegyverekkel, bombakészítés; erőszakos videók nézése; elmélkedés szent szövegekből kiragadott részleteken, sorokon, mint például a felbujtás hitetlenek megölésére stb.).

A gondolkodásmód kulcsfontosságú jellemző az egyén erőszakos és szélsőséges cselekedetekre és viselkedésekre való hajlama mögött meghúzódó motivációs rendszer megértése szempontjából. Ha egy személy arra a szilárd meggyőződésre (hitrendszerre) jutott, hogy a gondolkodását egy bizonyos irányba tereli, akkor ez a mentális attitűd egy önerősítő, szokásformáló kognitív konstrukció, amely előre meghatározza, hogy az illető hogyan fogja „értelmezni" a jelenlegi és a jövőbeni helyzeteket, és azokra milyen módon fog reagálni.

[51] Siegel 2010; Dean 2014.

Az Erőszakos Szélsőségesek Kockázatértékelése (Violent Extremist Risk Assessment, VERA[52]) egy, az erőszakos szélsőségesek kockázatértékeléséhez használható modell.

A Terrorista Elkövetők Európai Adatbázisából (European Database of Terrorist offenders, EDT) származó adatok felhasználásával a VERA-2R alapján összehasonlították egy emberölésért elítélt 21 dzsihádista elkövetőből álló csoport és egy 30, más terrorcselekmény miatt elítélt dzsihádista elkövetőből álló kontrollcsoport jellemzőit.[53] Az eredmények azt mutatják, hogy számos kockázati és védő mutatóban különbözik a két csoport. Mindkét terrorista csoport gyakran fogalmazott meg sérelmeket a vélt igazságtalanság miatt, de az emberölésért elítélt csoport gyakrabban fejezte ki haragját, erkölcsi felháborodását vagy gyűlöletét az észlelt igazságtalanság miatt, mint a kontrollcsoport. Az emberölésért elítélt csoportot ritkábban motiválta terrorcselekmény elkövetésére a csoporthoz tartozás a kontrollcsoporthoz képest. A védő mutatók tekintetében a kontrollcsoportba tartozó személyek gyakrabban utasítják el az erőszakot mint a célok elérésének eszközét.

3. táblázat: Terrorista Elkövetők Európai Adatbázisa: VERA-2R indikátorok

	A VERA-2R indikátorai
Hiedelmek, attitűdök és ideológia	Elkötelezettség az ideológia mellett, amely igazolja az erőszakot.
	Vélt sérelmek és/vagy vélt igazságtalanságok.
	Az igazságtalansággal kapcsolatos célpontok kijelölése és dehumanizálása.
	A demokratikus társadalmi értékek elutasítása.
	Érzelmek kifejezése az észlelt igazságtalanságra adott válaszként.
	A nemzeti identitással szembeni ellenségesség.
	Empátia hiánya a saját csoporton kívüliek iránt.
Szociális kontextus és szándék	Erőszakos szélsőséges anyagok keresője, felhasználója vagy fejlesztője.
	A támadás célpontjának azonosítása.
	Személyes kapcsolat erőszakos szélsőségesekkel.
	Kifejezett szándék erőszakos szélsőséges cselekmények elkövetésére.
	Hajlandóság arra, hogy meghaljon egy ügyért/meggyőződésért.
	Erőszakos szélsőséges cselekmények tervezése, előkészítése.
	Befolyásolhatóságra, irányíthatóságra vagy indoktrináció iránti fogékonyságra való hajlam.

[52] Pressman 2009.
[53] Alberda et al. 2022.

	A VERA-2R indikátorai
Élettörténet, cselekvés és képesség	Az erőszakot támogató, militáns ideológiának való korai kitettség.
	Az erőszakos szélsőségességben részt vevő családtagok és barátok hálózata.
	Büntetett előélet erőszakos bűncselekmények miatt.
	Stratégiai, félkatonai és/vagy robbanóanyag-használati kiképzés.
	Szélsőséges ideológiai képzés saját országban vagy külföldön.
Elkötelezettség és motiváció	Vélt vallási kötelesség/dicsőítés.
	Bűnözői megalkuvás.
	Bajtársiasság, a csoporthoz tartozás.
	Erkölcsi kötelesség, erkölcsi felsőbbrendűség.
	Izgalom és kaland.
	Erőszakos szélsőségességben való kényszerű részvétel.
	Státusz megszerzése.
	Értelem/jelentőség keresése.
Védő és kockázatcsökkentő mutatók	Az ideológia újbóli értelmezése.
	Az erőszak mint a célok elérése eszközének elutasítása.
	Az ellenségről alkotott elképzelés változása.
	Aktív résztvevője az erőszakos szélsőségesség elleni programoknak.
	Közösségi támogatás az erőszakmentességért.
	Támogatás a családtagoktól az erőszakmentességhez.

Forrás: a szerző szerkesztése

A Terrorist Radicalization Assessment Protocol (TRAP-18)[54] 18 kódolt viselkedési mintából áll. A TRAP-18 a célzott erőszakra fókuszál – olyan cselekményekre, amelyek szándékosak, és amelyeknek célja van –, és nem az általános erőszakos cselekményekre, hanem a magányos elkövető terroristára, akit megkülönböztet az olyan terroristától, akit kívülről irányítanak. Illetve javasol egy temporális (időbeli) megkülönböztetést az olyan indikátorok esetében, amelyek indukálhatják az aktív kockázatkezelést egy esetlegesen időben közeli terrorcselekménnyel kapcsolatban, és az olyan távolabbi karakterisztikájúak között, amelyek esetében esetlegesen csak aktív megfigyelésre van szükség. A 18 viselkedési minta *8 proximális* figyelmeztető magatartásból és *10 disztális* jellemzőből áll (lásd 4. táblázat).

[54] Meloy–Gill 2016.

4. táblázat: Proximális faktorok a TRAP-18 kockázatelemzési rendszerben[55]

Proximális faktorok	**„közelebbi"**
Viselkedés figyelmeztető folyamata	egy támadás kutatása, megtervezése, előkészítése vagy végrehajtása
Fixáció	patológiás elváltozás, amelyet a társadalmi és a szakmai élet romlása kísér
Azonosulás	katonai vagy rendészeti kellékekkel szoros kapcsolat, azonosulás korábbi támadókkal
Újfajta agresszió	erőszakos előzmény nélkül az alany teszteli tényleges erőszakos képességét
„Energiatörés/szakadás"	célhoz kapcsolódó bármely feljegyzett tevékenység gyakoriságának növekedése
„Szivárgó" magatartás	harmadik fél felé történő kommunikáció a támadás szándékáról
Végső megoldás	amikor az alany úgy dönt, csak az erőszakos viselkedés lehet a megoldás
Közvetlenül közölt fenyegetés	a támadás előtti kommunikációja a célponttal vagy a bűnüldöző szervekkel

Forrás: a szerző szerkesztése

5. táblázat: Disztális faktorok a TRAP-18 kockázatelemzési rendszerben[56] – Disztális „távolabbi" faktorok

Személyes sérelem és erkölcsi felháborodás
Ideológiai keret
Szélsőséges csoporttal való kapcsolattartás elmulasztása
Függőség a virtuális közösségtől
A foglalkozási célok meghiúsítása
A gondolkodás és az érzelem változásai
A szexuális-intim kapcsolat kudarca
Mentális rendellenességek
Kreativitás és innováció
Korábbi erőszakos bűncselekmény

Forrás: a szerző szerkesztése

[55] Meloy–Gill (2016).
[56] Meloy–Gill (2016).

Ezeknek a proximális és dinamikus jellemzőknek a változása vagy megjelenése a célzott erőszak kockázatának fokozódását jelezheti.[57]

John Reid Meloy és Paul Gill az Egyesült Államokból és Európából származó 111 magányos elkövetőből álló nyílt forráskódú mintán tesztelték a TRAP-18-at. A terroristákból álló minta 70%-ánál előre jelezte az elkövetést a rendszer. Amikor a mintát iszlám szélsőségesekre, jobboldali szélsőségesekre és egyéni terroristákra osztották, négy indikátor esetében volt szignifikáns különbség a csoportok között. A sikeres és a sikertelen támadók összehasonlításakor arra jutottak, hogy a sikeres támadók jobban rá voltak „szűkülve", fókuszálva az eseményre, kreatívabbak, innovatívabbak voltak, és kevésbé volt rájuk jellemző, hogy intim kapcsolatban, párkapcsolatban lettek volna valakivel, ezen túl kevésbé függtek a virtuális közösségtől. Összességében azt állapították meg, hogy a TRAP-18 ígéretes kockázatbecslő eszköz, elsősorban magányos elkövetők kockázatértékelésére.

ÖSSZEGZÉS

Megállapítható, hogy a különböző kockázatelemzési módszerek fontos részét képezik a terrorizmus elleni harcnak. A konkrét módszerek alkalmazásával, fejlesztésével kapcsolatban fontosnak gondoljuk, hogy azok hatékonyan elősegítsék a gyakorlatban a terrorcselekmények megelőzését. A tanulmányban megfogalmazott gondolatok bemutatják, hogy nagyon sokoldalú módszerekről van szó.

Fontosnak tartjuk megjegyezni, hogy az internet és a globalizáció elterjedésével egyre több potenciális terrorista, radikalizálódó személy kerül a hírszerző, elhárító szolgálatok látókörébe. Ahogy azt Meloy és Hoffmann[58] megfogalmazta, „a kockázat fokozott tudata mindenütt jelen van". Véleményünk szerint a kockázatelemzési módszerek fejlesztése során a pszichológiai szempontoknak lényeges szerepe lesz a jövőben is, tekintettel arra, hogy egy terrorcselekmény elkövetése mindig egy szélsőségesen erőszakos emberi magatartás eredményeként jön létre.

FELHASZNÁLT IRODALOM

Alberda, Daphne L. et al. (2022): Identifying Risk Factors for Jihadist Terrorist Offenders Committing Homicide: An Explorative Analysis Using the European Database of Terrorist Offenders. *Frontiers in Psychology,* (13), 1–16. Online: https://doi.org/10.3389/fpsyg.2022.1000186

[57] Meloy–Gill 2016.

[58] Meloy–Hoffmann 2014.

ALMOQBEL, Mashael – XU, Songhua (2019): Computational Mining of Social Media to Curb Terrorism. *ACM Computing Surveys,* 52(5), 1–25. Online: https://doi.org/10.1145/3342101

AWAN, Imran (2017): Cyber-Extremism: ISIS and the Power of Social Media. *Society,* 54(2), 138–149. Online: https://doi.org/10.1007/s12115-017-0114-0

BLAZSEK Péter – WERNIGG Róbert (2015): *Kockázatbecslés és kockázatkezelés a pszichiátriában.* Budapest: Oriold és Társai.

BORUM, Randy (2011): Radicalization into Violent Extremism: A Review of Social Science Theories. *Journal of Strategic Security,* 4(4), 7–36. Online: https://doi.org/10.5038/1944-0472.4.4.1

BRABHAM, Daren C. (2013): *Using Crowdsourcing in Government.* Washington: IBM Center for the Business of Government.

CHAUDHARY, Megha – BANSAL, Divya (2022): Open Source Intelligence Extraction for Terrorism-Related Information: A Review. *WIREs Data Mining and Knowledge Discovery,* 12(5), e1473. Online: https://doi.org/10.1002/widm.1473

CLEMMOW, Caitlin et al. (2020): The Base Rate Study: Developing Base Rates for Risk Factors and Indicators for Engagement in Violent Extremism. *Journal Forensic Sciences,* 65(3), 865–881. Online: https://doi.org/10.1111/1556-4029.14282

COULTAS, Bryan T. (2015): *Crowdsourcing Intelligence to Combat Terrorism: Harnessing Bottom-Up Collection to Prevent Lone-Wolf Terror Attacks.* Monterey: Naval Postgraduete Schoool. Online: https://apps.dtic.mil/sti/pdfs/ADA620622.pdf

DEAN, Geoff (2014): *Neurocognitive Risk Assessment for the Early Detection of Violent Extremists.* New York: Springer. Online: https://doi.org/10.1007/978-3-319-06719-3

FEINSTEIN, Jonathan S. – KAPLAN, Edward H. (2010): Analysis of a Strategic Terror Organization. *Journal of Conflict Resolution,* 54(2), 281–302. Online: https://doi.org/10.1177/0022002709355438

HALLER József – IVASKEVICS Krisztián (2020): *Terrorizmus.* In HALLER József (szerk): *Bűntettek kriminálpszichológiája.* Budapest: Dialóg Campus, 237–264.

HANKISS Ágnes (2018): HUMINT-RETRO – lélektani vonzatok. *Arc és Álarc,* 2(1–2), 195–227.

HEDGES, Chris (2001): A European Dragnet Captures New Clues to Bin Laden's Network. *The New York Times,* 2001. október 12. B10. Online: https://www.nytimes.com/2001/10/12/world/nation-challenged-search-european-dragnet-captures-new-clues-bin-laden-s-network.html

HERHKOVITZ, Shay (2020): Crowdsourced Intelligence (Crosint): Using Crowds for National Security. *The International Journal of Intelligence. Security, and Public Affairs,* 22(1), 42–55. Online: https://doi.org/10.1080/23800992.2020.1744824

HERRINGTON, Victoria – ROBERTS, Karl (2012): Risk Assessment in Counterterrorism. In KUMAR, Updesh – MANDAL, Manas K. (szerk.): *Countering Terrorism: Psychosocial Strategies.* New Delhi: SAGE, 282–304.

HORGAN, John (2005): *The Psychology of Terrorism.* London: Routledge. Online: https://doi.org/10.4324/9780203496961

HOWE, Jeff (2006): The Rise of Crowdsourcing. *Wired,* 14(6), 1–4.

HULST, Renée C. van der (2009): Introduction to Social Network Analysis (SNA) as an Investigative Tool. *Trends Organ Crime,* 12(2), 101–121. Online: https://doi.org/10.1007/s12117-008-9057-6

INNES, Martin – THIEL, Darren (2008): *Policing Terror.* In NEWBURN, Tim: *The Handbook of Policing.* Cullompton: Willan. Online: https://www.police-foundation.org.uk/2017/wp-content/uploads/2017/06/terrorism_review.pdf

KENYON, Jonathan – BAKER-BEALL, Christopher – BINDER, Jens (2021): Lone-Actor Terrorism – A Systematic Literature Review. *Studies in Conflict & Terrorism,* 46(10), 1–24. Online: https://doi.org/10.1080/1057610X.2021.1892635

KNOKE, David (2015): *Emerging Trends in Social Network Analysis of Terrorism and Counterterrorism.* In SCOTT, Robert A. (szerk.): *Emerging Trends in the Social and Behavioral Sciences.* New York: John Wiley and Sons, 1–15. Online: https://doi.org/10.1002/9781118900772.etrds0106

LOWENTHALL, Mark M. (2012): *Intelligence: From Secrets to Policy.* Washington: CQ Press.

MALM, Aili – NASH, Rebecca – MOGHADAM, Ramim (2016): Social Network Analysis and Terrorism. In LAFREE, Gary – FREILICH, Joshua D.: *The Handbook of the Criminology of Terrorism.* Hoboken: Wiley–Blackwell, 221–231. Online: https://doi.org/10.1002/9781118923986.ch14

MAYER, Matt A. (2016): *Enhanced Human Intelligence is Key to Defeating Terrorists.* American Enterprise Institute (AEI). Online: https://www.aei.org/research-products/report/enhanced-human-intelligence-is-key-to-defeating-terrorists/

MEEHL, Paul E. (1954): *Clinical Versus Statistical Prediction: A Theoretical Analysis and a Review of the Evidence.* Minneapolis: University of Minnesota Press. Online: https://doi.org/10.1037/11281-000

MELOY, John Reid – HOFFMANN, Jens (2014): *International Handbook of Threat Assessment.* New York: Oxford University Press.

MELOY, John Reid – GILL, Paul (2016): The Lone-Actor Terrorist and the TRAP-18. *Journal of Threat Assessment and Management,* 3(1), 37–52. Online: https://doi.org/10.1037/tam0000061

MONAHAN, John (2011): The Individual Risk Assessment of Terrorism. *Public Law and Legal Theory Working Paper Series,* (2011–34). Charlottesville: University of Virginia. Online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1928722

NYITRAI Endre (2015): Bűnelemzés a nyomozásban. In GAÁL Gyula – HAUTZINGER Zoltán (szerk.): *Modern kori veszélyek rendészeti aspektusai.* Pécs: Magyar Hadtudományi Társaság, 141–147.

PASTOR-GALINDO, Javier et al. (2020): The not yet Exploited Goldmine of OSINT: Opportunities, Open Challenges and Future Trends. *IEEE Access,* 8, 10282–10304. Online: https://doi.org/10.1109/ACCESS.2020.2965257

PERSONS, Jacqueline B. (2008): *The Case Formulation Approach to Cognitive-Behavior Therapy.* New York: Guilford Press.

PRESSMAN, D. Elaine (2009): *Risk Assessment Decisions for Violent Political Extremism.* Ottawa: Her Majesty the Queen in Right of Canada.

PULIDO GRAGERA, Julia – SANSO, Daniel (2014): A Phenomenological Analysis of Terrorism and Organized Crime from a Comparative Criminological Perspective. *Journal of Law and Criminal Justice,* 2(2), 113–131.

SABJANICS István (2019): *A terrorizmus hatásai és megjelenése a demokratikus jogrendben.* Budapest: Pázmány Péter Katolikus Egyetem Jog- és Államtudományi Doktori Iskola. Online: https://jak.ppke.hu/uploads/articles/12332/file/Sabjanics_Istvan_dolgozatv.pdf.

SARMA, Kiran M. (2017): Risk Assessment and the Prevention of Radicalization from Nonviolence Into Terrorism. *American Psychologist,* 72(3), 278–288. Online: https://doi.org/10.1037/amp0000121

SCHMID, Alex P. (2013): Radicalisation, De-Radicalisation and Counter-Radicalisation: A Conceptual, Discussion and Literature Review. *International Centre for Counter-Terrorism (ICCT) – The Hague,* 4(2). Online: http://dx.doi.org/10.19165/2013.1.02

Shelley, Luise L. – Picarelli, John T. (2005): Methods and Motives: Exploring Links between Transnational Organized Crime and International Terrorism. *Trends Organ Crime,* 9(2), 52–67. Online: https://doi.org/10.1007/s12117-005-1024-x.

Siegel, Daniel J. (2010): *Mindsight: The New Science of Personal Transformation.* New York: Random House.

Sparrow, Malcolm K. (1991): The Application of Network Analysis to Criminal Intelligence: An Assessment of the Prospects. *Social Networks,* 13(3), 251–274. Online: https://doi.org/10.1016/0378-8733(91)90008-H

Walker, Clive (2005): Intelligence and Anti-Terrorism Legislation in the United Kingdom. *Criminal Law & Society Change,* 44(4–5), 387–422. Online: https://doi.org/10.1007/s10611-006-9030-8

Walker, Clive (2008): Know Thine Enemy as Thyself: Discerning Friend from Foe under Anti-Terrorism Laws. *Melbourne University Law Review,* 32(1), 275–301.

Ward, Jamie (2010): *The Student's Guide to Cognitive Neuroscience.* Hove: Psychology Press.

Webster, Christopher D. et al. (1997): Assessing Risk of Violence to Others. In Webster, Christopher D. – Jackson, Margaret A. (szerk.): *Impulsivity: Theory, assessment, and treatment.* New York: The Guilford Press, 251–277.

Williams, Phil (1998): The Nature of Drug-Trafficking Networks. *Current History,* 97(618), 154–159. Online: https://doi.org/10.1525/curh.1998.97.618.154

Egyéb forrás

Az Európai Unió terrorizmus elleni stratégiája. Online: https://www.consilium.europa.eu/hu/policies/fightagainst-terrorism/eu-strategy