Szerkesztette

Taller János
Erdős Ákos
Kuszi Viktória
Rémai Dániel

SZEMELVÉNYEK A XXI. SZÁZADI TERRORIZMUS KIHÍVÁSAIBÓL

Magyar
Rendészettudományi
Társaság

Szerkesztette

TALLER JÁNOS – ERDŐS ÁKOS – KUSZI VIKTÓRIA – RÉMAI DÁNIEL

SZEMELVÉNYEK A XXI. SZÁZADI TERRORIZMUS KIHÍVÁSAIBÓL

Magyar Rendészettudományi Társaság

Budapest, 2025.

Szakmai lektor

Rémai Dániel

Szerkesztette

Taller János
Erdős Ákos
Kuszi Viktória
Rémai Dániel

A kötet szerzői

Petruska Ferenc
Forró Tamás
Jasenszky Nándor
Csepregi Zsolt
Viszkocsil László
Kiss Nikoletta

Kiadja a Magyar Rendészettudományi Társaság
A kiadásért felel: Korinek László elnök

Székhely: 1089 Budapest, Diószeghy Sámuel u. 38-42.
Kapcsolat: mrtt@uni-nke.hu

ISBN 978-615-6456-43-4 (ePDF)

A kötet, a TKP 2021-NVA-18 számú projekt („XXI. századi biztonsági kihívások nemzetbiztonsági hangsúlyai”) keretében, a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból nyújtott támogatással, a TKP2021-NVA pályázati program finanszírozásában valósult meg valósult meg.

NEMZETI KUTATÁSI, FEJLESZTÉSI ÉS INNOVÁCIÓS HIVATAL
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROJEKT

Tartalomjegyzék

VÁKÁT OLDAL

Előszó

A XXI. század biztonsági környezetét alapvetően formálja a terrorizmus állandó és sokrétű fenyegetése. Az elmúlt évtizedek tapasztalatai is rávilágítottak arra, hogy a terrorizmus nem statikus jelenség, hiszen folyamatosan alkalmazkodik a politikai, társadalmi és technológiai változásokhoz. A globális és regionális szinten egyaránt tapasztalható fenyegetések nemcsak a hagyományos biztonsági dimenziókat érintik, hanem új kihívások elé állítják az államokat, a nemzetközi szervezeteket és a társadalmakat is. Ennélfogva a kötet célja, hogy betekintést adjon a terrorizmus jelenlegi és jövőbeni kihívásainak egyes elemeiről.

A kötet tanulmányai széles spektrumot ölelnek fel. Kiemelt témaként jelenik meg a mesterséges intelligencia, amely kettős természetéből fakadóan egyszerre kínál új lehetőségeket a terrorelhárítás számára, miközben eszközként szolgálhat a szélsőséges csoportok kezében is. A hírszerző szolgálatok közötti nemzetközi együttműködés kérdésköre szintén meghatározó, hiszen a globalizált fenyegetések hatékony kezeléséhez elengedhetetlen az információmegosztás és a koordináció.

A kritikus infrastruktúra sebezhetősége és a kibertérben zajló támadások veszélyei különös aktualitást nyernek napjainkban, amikor a kiberterrorizmus már nem csupán elméleti lehetőség, hanem valós kockázat lehet. A radikalizáció folyamatának elemzése pedig rámutat arra, miként használják ki a szélsőséges mozgalmak a társadalmi feszültségeket és az identitásválságokat, míg a terrorizmus finanszírozásának változó módszerei új szabályozási és ellenőrzési megközelítéseket tesznek szükségessé.

A kötet nem csupán a jelen problémáira reflektál, hanem a jövő kihívásaira is tekint. E szemelvények célja, hogy gondolatébresztőként és tájékozódási pontként szolgáljanak mindazok számára, akik a terrorizmus komplex kihívásainak megértésére és kezelésére törekszenek. A feladat összetett és hosszú távú, de éppen ezért elengedhetetlen, hogy a tudomány és a gyakorlati szakemberek közösen keressék a megoldásokat.

Köszönet illeti a kötet szerzőit, akik szakértelmükkel és elkötelezettségükkel járultak hozzá e munkához. Írásaik révén olyan tudományos szemelvények kerülnek az olvasó elé, amelyek nemcsak a meglévő ismeretek bővítését szolgálják, hanem a további kutatásokhoz is alapot biztosítanak.

Dr. Rémai Dániel

Nemzeti Közszolgálati Egyetem
Rendészettudományi Kar
Terrorelhárítási Tanszék vezetője

VÁKÁT OLDAL

Petruska Ferenc

A mesterséges intelligencia alkalmazásának lehetőségei a terrorizmus kutatásában

1. BEVEZETÉS

A 21. század a világ biztonsági helyzetét erősen rontja a terrorizmus folyamatos és erőteljes jelenléte. A terrorista csoportok – a kiterjedt és hierarchikus szervezetektől a decentralizált, sejtszerű hálózatokig és a magányos elkövetőkig – változatos módszereket használnak. A mesterséges intelligencia viszont minden elkövetési forma (internetes propaganda és toborzás, közösségi média stb.) ellen fegyvert ad a terrorelhárítás kezébe. A hagyományos hírszerzési és elemzési módszerek nehezen birkóznak meg a szünet nélkül keletkező, elképesztő mennyiségű adattal, amely a nyílt forrásoktól (OSINT) a lefoglalt digitális eszközökig és a megfigyelési rendszerekből származó információkig terjed.[1] Ezeket sem manuálisan, sem vizuálisan nem lehetséges sem átvizsgálni és pláne nem lehet feldolgozni és kiértékelni. Különösen igaz ez a rejtett mintázatokra, a gyenge jelekre és a kialakulóban lévő fenyegetések azonosítására.

Ebben a komplex és dinamikusan változó környezetben jelent meg a mesterséges intelligencia, mint forradalmi technológia, amely forradalmasíthatja a terrorizmus elleni küzdelmet és annak tudományos vizsgálatát. A mesterséges intelligencia, és különösen a gépi tanulás, a természetes nyelvfeldolgozás és a számítógépes látás, olyan képességekkel ruházza fel az elemzőket és a kutatókat, amelyekről korábban nem is tudtak. E technológia lehetővé teszi a hatalmas mennyiségű és gyorsan változó adatok elemzését, a terrorista narratívák valós idejű észlelését az online térben, a támadások valószínűségének és lehetséges célpontjainak előrejelzését, valamint a terrorista hálózatok rejtett struktúráinak feltárását. A technológia kettős felhasználású (terrorizmus és terrorelhárítás), amely komoly aggályokat is felvet, hiszen a terroristák is egyre kifinomultabban alkalmazzák a mesterséges intelligenciát multimodális támadóeszközként.

A tanulmány célja, hogy átfogó betekintést nyújtson a mesterséges intelligencia terrorizmuskutatásban való alkalmazásának lehetőségeiről, kihívásairól és jövőbeli irányairól. A tanulmányom az elmúlt fél évtized tudományos eredményeire, nemzetközi szervezetek

[1] FARKAS– VIKMAN (2024)

jelentéseire és szakpolitikai elemzésekre támaszkodva keresi a választ a következő kutatási kérdésekre. Milyen konkrét MI-technológiák és módszerek bizonyulnak a leghatékonyabbnak a terrorizmus jelenségének megértésében és a fenyegetések elhárításában? Milyen gyakorlati alkalmazási területeken hozhatnak áttörést ezek a technológiák a radikalizáció online felderítésétől a prediktív analitikán át az operatív támogatásig? Milyen mélyreható etikai, jogi és társadalmi kihívásokat vet fel az MI alkalmazása a terrorelhárításban, különös tekintettel az algoritmikus torzításra, a magánélet védelmére és az emberi felügyelet kérdésére? Első hipotézisem szerint a mesterséges intelligencia technológiák, különösen a gépi tanulás és a természetes nyelvfeldolgozás, jelentős mértékben javíthatják a terrorista fenyegetések korai felismerését és előrejelzését, amennyiben megfelelő adatminőség és emberi felügyelet mellett alkalmazzák őket. Második hipotézisem azt állítja, hogy a mesterséges intelligencia (MI) alkalmazása a terrorelhárításban elkerülhetetlenül etikai és jogi dilemmákat vet fel, amelyek kezelése – még ha az MI-t alapvetően metajurisztikus jelenségnek is tartom – új szabályozási keretek kidolgozását teszi szükségessé. Harmadik hipotézis szerint a terrorista csoportok saját MI-képességeinek fejlődése egy sajátos technológiai fegyverkezési rivalizálást, sőt versenyt indít el. Mindez megítélésem szerint új típusú fenyegetéseket teremtett. A tanulmány újdonsága abban rejlik, hogy nem csupán a technológiai aspektusokra fókuszál, hanem holisztikus megközelítést alkalmaz, amely egyaránt figyelembe veszi a műszaki, és jogászként különösen a jogi dimenziókat. Különös hangsúlyt fektet a terrorista csoportok saját MI-felhasználására, amely gyakran alulreprezentált a szakirodalomban.

2. ALKALMAZOTT KUTATÁSI MÓDSZEREK

Jelen tanulmányom egy kvalitatív, szisztematikus szakirodalmi áttekintésen alapul, amely a mesterséges intelligencia és a terrorizmuskutatás metszetében született. A legfrissebb, főként az elmúlt fél évtized időszakára fókuszáló tudományos publikációkat, nemzetközi szervezetek által kiadott jelentéseket, valamint releváns szakpolitikai dokumentumokat és kutatóintézeti elemzéseket szintetizálja. A módszertan célja nem új empirikus adatok előállítása, hanem a meglévő tudás strukturált bemutatása, a legfontosabb technológiai trendek, alkalmazási területek és kritikai diskurzusok azonosítása. A tanulmány egy „technológiai taxonómiát” is magában foglal, amely a terrorizmuskutatás szempontjából leginkább releváns MI-területek köré szervezi az írásom. A taxonómia négy fő kategóriát különböztet meg: gépi tanulás, természetes nyelvfeldolgozás, számítógépes látás, valamint big data analitika.

A gépi tanulás az MI azon ága, amely lehetővé teszi a számítógépes rendszerek számára, hogy adatokból, külön manuális programozás nélkül tanuljanak és következtetéseket vonjanak le. A terrorizmuskutatásban ez a képesség különösen értékes a nagy, strukturált és strukturálatlan adathalmazokban rejlő mintázatok azonosítására. A prediktív analitika gépi tanulási modelleket alkalmaz a jövőbeli események valószínűségének előrejelzésére. A leggyakrabban használt modellek közé tartoznak a felügyelt tanulási algoritmusok, mint például a Random Forest[2] és az XGBoost[3], amelyek több döntési fa kombinálásával hoznak létre pontos előrejelzéseket. Ezeket a modelleket gyakran terrortámadásokat rögzítő adatbázisok elemzésére használják. A mélytanulás, amely komplex, többrétegű neurális hálózatokon alapul, még kifinomultabb elemzést tesz lehetővé.

A természetes nyelvfeldolgozás (NLP) az MI azon területe, amely a számítógépek és az emberi nyelv közötti interakcióval foglalkozik. Ez az interdiszciplináris tudományterület azzal foglalkozik, hogy az MI értelmezni, sőt generálni tudja az emberi nyelvet. A terrorizmuskutatásban a természetes nyelvi feldolgozás kulcsfontosságú az online térben zajló radikalizáció, propaganda-terjesztés és toborzás megértésében és felderítésében. A módszertan magában foglalja a szövegek előfeldolgozását, majd a szövegek numerikus reprezentációját. A hagyományos módszerek, mint a Bag-of-Words a szavak gyakoriságán alapulnak. A modell egy szövegmodell, amely rendezetlen szavak gyűjteményét (egy „zsákot") használ. Természetes nyelvfeldolgozásban és információkeresésben alkalmazzák. Nem veszi figyelembe a szavak sorrendjét (és így a szintaxis vagy a nyelvtan nagy részét), de rögzíti a többszörösséget. A modernebb megközelítések, mint a Word2Vec, a szavakat sűrű vektorokként ábrázolják, megragadva a szemantikai kapcsolatokat. Magyarul azok a szavak, amelyek hasonló összefüggésben szerepelnek, azok azonos irányú vektornak is minősülnek. A transzformermodellek, különösen a BERT[4] és annak variánsai, forradalmasították az NLP-t azáltal, hogy a szavak jelentését a teljes kontextusuk alapján értelmezik. Ezek a modellek rendkívül hatékonyak a szélsőségbe hajló tartalmak pontos minősítésében és felismerésében, és képesek a többnyelvű tartalmak elemzésére is.

A számítógépes látás célja, hogy a számítógépek képesek legyenek a vizuális világ megértésére, azaz digitális képekből és videókból származó információk feldolgozására és értelmezésére. A terrorelhárításban ez a technológia a fizikai biztonság és a megfigyelés területén játszik kiemelt szerepet. Az alapját a neurális hálózatok képezik, amelyek rendkívül

[2] IBM (2025)
[3] KAVLAKOGLU – RUSSI (2024)
[4] GOOGLE AI BLOG (2018)

hatékonyak a képi mintázatok felismerésében. Az alkalmazások skálája széles: az arcfelismerő rendszerek a határellenőrzési pontokon vagy a tömegben képesek azonosítani a körözött személyeket. A technológia kiterjed a drónokról és műholdakról származó felvételek elemzésére is, lehetővé téve a távoli és nehezen megközelíthető területeken lévő kiképzőtáborok vagy gyanús mozgások azonosítását.[5]

A terrorizmuskutatás egyre inkább big data problémává válik, ahol hatalmas és heterogén adathalmazokat kell feldolgozni, beleértve a közösségi média posztokat, pénzügyi tranzakciókat, telefonhívásokat, utazási információkat és térfigyelő kamera felvételeket. A big data analitikai platformok lehetővé teszik ezen adatok integrálását és együttes elemzését. A hálózatelemzés különösen fontos módszertan a terrorista sejtek és hálózatok feltérképezésében.

3. MESTERSÉGES INTELLIGENCIA GYAKORLATI ALKALMAZÁSA A TERRORELHÁRÍTÁSBAN

A mesterséges intelligencia elméleti lehetőségei a terrorizmuskutatásban egyre inkább kézzelfogható, gyakorlati alkalmazásokban öltenek testet. A bűnüldöző és hírszerző szervek, valamint a kutatóintézetek világszerte fejlesztenek és implementálnak olyan MI-alapú rendszereket, amelyek a fenyegetések teljes spektrumát lefedik, az online radikalizáció korai felismerésétől a támadások előrejelzésén át az operatív műveletek támogatásáig.

3.1. ONLINE RADIKALIZÁCIÓ ÉS PROPAGANDA FELDERÍTÉSE

Az online tér vált a modern terrorizmus egyik legfontosabb hadszínterévé, ahol a propaganda terjesztése, a toborzás és a radikalizáció zajlik. Az MI, különösen a természetes nyelvfeldolgozás, kulcsfontosságú eszköz ezen tevékenységek felderítésében. Az EU által finanszírozott INSIKT projekt[6] keretében kifejlesztett platform például természetes nyelvfeldolgozás, hálózatelemzés és gépi tanulás segítségével monitorozza a nyílt és zárt online csatornákat, hogy valós időben azonosítsa a dzsihadista propaganda megjelenését és a titkosított toborzási párbeszédeket.[7]

A gyakorlati eredmények lenyűgözőek. Már létezik olyan többnyelvű klasszifikációs rendszer 91,1%-os pontosságot ért el az extremista tartalmak azonosításában arab, angol és francia nyelvű szövegeken. A modell képes volt felismerni a finom nyelvi jelzéseket, amelyek

[5] RÉMAI (2024)
[6] INSIKT INTELLIGENCE S.L. (2020b)
[7] INSIKT INTELLIGENCE S.L. (2020a)

megkülönböztetik a radikális ideológiai tartalmakat a mainstream vallási vagy politikai diskurzusoktól.[8]

A kutatók fejlett hálózatelemzési technikákat alkalmaznak, hogy feltérképezzék a felhasználók közötti kapcsolatokat és azonosítsák a befolyásos csomópontokat a radikalizációs hálózatokban. Ez lehetővé teszi a hatóságok számára, hogy célzott beavatkozásokat hajtsanak végre a legveszélyesebb propagandisták ellen.

3.2. FENYEGETÉS-ELŐREJELZÉS ÉS HOT SPOT ANALÍZIS

A prediktív analitika egyik legígéretesebb alkalmazási területe a jövőbeli terrortámadások valószínűségének, helyszínének és jellegének előrejelzése. A kutatók mélytanulási modelleket alkalmaznak kiterjedt adatbázisokon, mint például a Global Terrorism Database.[9] Évek óta használnak olyan modelleket, amelyek a támadások idősoros adataiból tanulva képesek előre jelezni a jövőbeli események jellemzőit.[10]

A gyakorlatban a prediktív rendészet koncepciója jelent meg, ahol az MI-algoritmusok „forró pontokat" azonosítanak, ahol a támadások kockázata a legmagasabb. Izraelben a hatóságok hasonló, térbeli klaszterezésen és idősoros modellezésen alapuló algoritmusokat használtak a kockázatosnak ítélt egyének preventív őrizetbe vételére. Bár ez a megközelítés hatékonynak bizonyult a támadások megelőzésében, komoly etikai kérdéseket vet fel az ártatlanság vélelmével és az emberi jogokkal kapcsolatban.

Szingapúr „Safe City" platformja egy még integráltabb megközelítést alkalmaz: a biometrikus adatok, a lövésdetektorok, a közösségi média hangulatelemzése és az IoT szenzorok adatait egyesítve óránkénti kockázati pontszámot generál a város minden kerületére. A platformja a város biztonságát növelő, fejlett technológiára és kiterjedt megfigyelőrendszerre épülő kezdeményezés. A platform célja a bűnmegelőzés, a közbiztonság fenntartása és a gyors reagálás a vészhelyzetekre. A platform központi eleme a kiterjedt kamerarendszer, amely az egész várost behálózza. Ezek a kamerák valós időben rögzítenek minden fontos eseményt, és a mesterséges intelligencia segítségével képesek azonosítani a gyanús viselkedést vagy a bűncselekményeket. Ezenkívül a rendszer képes riasztást küldeni a rendőrségnek és a mentőszolgálatoknak is, ha a kamerák vészhelyzetet észlelnek. Ez a rendszer képes valós időben reagálni a változó biztonsági helyzetekre és optimalizálni a rendőrségi járőrözést.[11]

[8] ZERROUKI – BENBLIDIA (2024): 121-135.
[9] START (2025)
[10] SAIDI – TRABELSI (2022): 34320-34331.
[11] PRESTIGE ONLINE SINGAPORE (2025)

3.3. OPERATÍV ÉS TAKTIKAI TÁMOGATÁS

A számítógépes látás technológiája forradalmasítja a hírszerzési, megfigyelési és felderítési tevékenységeket. Az amerikai Védelmi Minisztérium Project MAVEN nevű kezdeményezése az egyik legkiemelkedőbb példa erre. A projekt keretében neurális hálózatokat tanítottak be arra, hogy a konfliktusövezetek felett gyűjtött, petabájtos (1 000 000 000 000 000 bájt) nagyságrendű videóanyagot automatikusan elemezzék.[12] A rendszer képes felismerni és megjelölni a releváns objektumokat, járműveket, fegyvereket, személyeket, ezzel akár 70%-kal csökkentve az emberi elemzők leterheltségét és felgyorsítva a kritikus információk feldolgozását. A technológia különösen hatékony a nagy területek folyamatos megfigyelésében, ahol az emberi elemzők gyorsan kifáradnának vagy figyelmetlenné válnának.

A határellenőrzés területén a mélytanuláson alapuló arcfelismerő rendszerek több mint 99%-os pontossággal képesek azonosítani a keresett személyeket a figyelőlistákról, még kedvezőtlen fényviszonyok vagy részleges takarás esetén is. Az Európai Unió Entry/Exit System (EES) projektje ilyen technológiákat alkalmaz a schengeni térség külső határain, jelentősen javítva a biztonsági ellenőrzések hatékonyságát.[13]

3.4. HÁLÓZATELEMZÉS ÉS KAPCSOLATFELTÁRÁS

Az MI-alapú hálózatelemzés forradalmasította a terrorista sejtek és támogató hálózatok feltérképezését. Az indiai Innefu Labs által fejlesztett Prophecy Alethia™ platform[14] integrált megközelítést alkalmaz, amely a hívásadatokat, térfigyelő kamera felvételeket és nyílt forrású hírszerzési adatokat egyetlen gráf-adatbázisban egyesíti a militáns sejtek viselkedési mintázatainak felismerésére.

A platform képes azonosítani a rejtett kapcsolatokat a látszólag független egyének között, feltárni a pénzügyi támogatási láncokat és előre jelezni a sejtek aktivitásának növekedését. Egy konkrét esetben a rendszer sikeresen azonosított egy 15 fős terrorista sejtet Kelet-Indiában azáltal, hogy elemzte a tagok kommunikációs mintázatait és mozgási szokásait.

Hasonló eredményeket ért el a francia DGSI (Direction Générale de la Sécurité Intérieure) is, amely MI-alapú hálózatelemzést alkalmazott a 2015-ös párizsi támadások utáni

[12] PORTFOLIO (2024)
[13] EURÓPAI BIZOTTSÁG (n.d.); EUROPEAN COMMISSION (n.d.)
[14] INNEFU LABS. (2025)

nyomozásban. A rendszer képes volt rekonstruálni a támadók kapcsolati hálóját és azonosítani a korábban ismeretlen támogatókat, ami további letartóztatásokhoz vezetett.[15]

3.5. PÉNZÜGYI NYOMKÖVETÉS ÉS FINANSZÍROZÁS-ELEMZÉS

A terrorista finanszírozás felderítése az egyik leginkább kihívásokkal teli feladat a terrorelhárításban. Az MI-technológiák, különösen a gépi tanulás és a hálózatelemzés, új lehetőségeket nyitnak ezen a területen. A pénzügyi tranzakciók elemzésére fejlesztett algoritmusok képesek azonosítani a gyanús pénzmozgásokat, még akkor is, ha azok kis összegekben, több lépcsőben történnek.

Az Egyesült Államok Pénzügyminisztériumának Financial Crimes Enforcement Network (FinCEN) részlege fejlett MI-rendszereket alkalmaz a Suspicious Activity Reports (SAR) elemzésére. Ezek a rendszerek képesek felismerni a terrorista finanszírozásra jellemző mintázatokat, mint például a hawala rendszerek használata, a kriptovaluták alkalmazása vagy a jótékonysági szervezeteken keresztüli pénzmosás.[16]

3.6. TERRORISTA CSOPORTOK ÁLTALI ROSSZINDULATÚ MI-FELHASZNÁLÁS

A mesterséges intelligencia kettős felhasználású technológia, ami azt jelenti, hogy ugyanazok az eszközök, amelyeket a terrorelhárítás használ, a terrorista csoportok kezében is hatékony fegyverré válhatnak.

A rosszindulatú felhasználás nem korlátozódik a propagandára: a terroristák MI-t alkalmazhatnak autonóm támadóeszközök, például drónrajok fejlesztésére, kritikus infrastruktúrák elleni kibertámadások[17] végrehajtására, vagy akár a terrorelhárító szervek MI-rendszereinek megtévesztésére és adatainak „megmérgezésére”. Ez utóbbi egy olyan típusú támadás, amelynek során rosszindulatú szereplők manipulálják a képzési adatokat, hogy sebezhetőségeket, torzításokat vagy hátsó ajtókat vezessenek be a modellbe. Ez a manipuláció káros kimenetekhez, teljesítményromláshoz, vagy akár biztonsági résekhez is vezethet. Az adatmérgezés előfordulhat az előképzés, a finomhangolás, vagy akár a beágyazási folyamat során is, a nagy nyelvi modell életciklusának különböző szakaszait célozva meg. Ezek a fenyegetések pedig egy folyamatos technológiai fegyverkezési versenyt vetít előre.

Különösen aggasztó a deepfake technológia terrorista alkalmazása. A Hamas és a Hezbollah már használt szintetikus videókat dezinformációs kampányokban. Ezek a chatbotok képesek személyre szabott radikalizációs tartalmakat generálni, amely növeli a

[15] MINISTÈRE DE L’INTÉRIEUR (2025)
[16] THOMSON REUTERS (2025)
[17] KELEMEN (2024)

propaganda hatékonyságát, hiszen így több mindenkit személyre szabott formában közvetlenül érhetnek el.[18]

3.7. KIBERTÉRBEN ZAJLÓ TERRORIZMUS

A kibertérben zajló terrorizmus egy új dimenzió, ahol az MI mind a támadó, mind a védekező oldalon kulcsszerepet játszik.[19] A terrorista csoportok egyre kifinomultabb kibertámadásokat hajtanak végre kritikus infrastruktúrák ellen, és ezekben a támadásokban egyre gyakrabban alkalmaznak MI-technológiákat.

A védekezés oldalán az MI-alapú kibervédelmi rendszerek képesek valós időben detektálni és elhárítani a fejlett perzisztens fenyegetéseket. Ezek a rendszerek viselkedési analitikát alkalmaznak a normálistól eltérő hálózati aktivitás azonosítására, és képesek előre jelezni a támadások következő lépéseit.

3.8. KÖZÖSSÉGI MÉDIA MONITORING

A közösségi média platformok monitorozása kritikus fontosságú a radikalizációs folyamatok megértésében és a fenyegetések korai felismerésében. Az MI-alapú sentiment analízis[20] eszközök képesek valós időben elemezni a millió számra érkező posztokat, kommenteket és üzeneteket, azonosítva a radikális tartalmakat és a potenciálisan veszélyes egyéneket.

A Facebook Meta AI csapata fejlett neurális hálózatokat alkalmaz a platform 3 milliárd felhasználójának tartalmainak valós idejű moderálására.[21] Ezek a rendszerek képesek azonosítani a terrorista toborzási kísérleteket, még akkor is, ha azok ártatlannak tűnő tartalmak mögé rejtve jelennek meg. 2024-ben Magyarországon a közösségi média platformok felhasználóinak száma elérte a 7,29 millió főt, ami a teljes lakosság 72,4%-át jelenti.

A legnépszerűbb platform a YouTube, amelyet 7,29 millióan használnak, így a magyar lakosság 78,9%-a érhető el rajta hirdetésekkel. A Facebook 5,35 millió felhasználóval rendelkezik, ami a lakosság 53,1%-át fedi le, míg a TikTok 3,24 millió, az Instagram 2,7 millió, a Pinterest 2,09 millió, a LinkedIn pedig 1,6 millió magyar felhasználót számlál. Az X (korábban Twitter) 1,46 millió, a Snapchat pedig 1,16 millió regisztrált felhasználóval van

[18] JONES (2025)
[19] KÁDÁR (2023)
[20] KUGLER (2022)
[21] ZŐDI (2024)

jelen Magyarországon. Ezek az adatok jól mutatják, hogy a közösségi média platformok továbbra is meghatározó szerepet töltenek be a magyar internetezők mindennapjaiban is.[22]

3.9. PREDIKTÍV POLICING ÉS TERÜLETI ELEMZÉS

A prediktív rendészet alkalmazása a terrorelhárításban új lehetőségeket nyit a támadások megelőzésében. Az MI-algoritmusok képesek elemezni a már megtörtént támadási adatokat, a társadalmi-gazdasági mutatókat, az időjárási viszonyokat és más környezeti tényezőket, hogy előre jelezzék, hol és mikor várható a legnagyobb valószínűséggel terrorista aktivitás.

Hasonló eredményeket ért el London is, ahol a Metropolitan Police MI-alapú kockázatértékelési rendszert alkalmaz a nagy tömegeket vonzó események biztosításához. A rendszer képes valós időben elemezni a közösségi média aktivitást, a híreket és más nyílt forrású információkat, hogy azonosítsa a potenciális fenyegetéseket. A Metropolitan Police e technikát elsősorban arcfelismerő rendszerek formájában integrálta a mindennapi működésébe, főként nyomozati célokra. Emellett folyamatosan vizsgálják és értékelik a chatbot technológiák lehetséges előnyeit, illetve más MI-alapú megoldásokat is fontolóra vesznek a rendőrségi munka hatékonyságának növelése érdekében. A jövőben a chatbotokat különböző rendőrségi szituációkban is hasznosnak tartják, és nyitottak az együttműködésre külső technológiai partnerekkel vagy kutatóintézetekkel a biztonságos és ellenőrzött bevezetés érdekében. Az MI alkalmazására vonatkozóan léteznek irányelvek és szabályzatok, amelyek nyilvánosan is elérhetők, és a rendőrség kiemelt figyelmet fordít az etikai és jogi megfelelőségre.[23]

3.10. BIOMETRIKUS AZONOSÍTÁS ÉS VISELKEDÉSELEMZÉS

A biometrikus technológiák és az MI kombinációja forradalmasította a személyazonosítást és a viselkedéselemzést a terrorelhárításban. A fejlett arcfelismerő rendszerek már nem csupán a statikus képek alapján működnek, hanem képesek valós idejű viselkedéselemzésre is.

Néhány repülőtéren alkalmazott rendszer például nemcsak az arcokat ismeri fel, hanem elemzi a járás módját, a testtartást és a mikro-arckifejezéseket is, hogy azonosítsa a gyanús viselkedést. A viselkedéselemzés kiterjed a tömegek dinamikájának elemzésére is. Az MI-algoritmusok képesek azonosítani a pánik jeleit, a tömeg szokatlan mozgását vagy a gyanús csoportosulásokat, amelyek egy készülő támadásra utalhatnak. Ezek a rendszerek már

[22] ONLINE SPECIALISTA (2024)
[23] METROPOLITAN POLICE (2023)

több nagy sporteseményen és fesztiválon bizonyították hatékonyságukat. A mesterséges intelligencia megfelelő alkalmazása jelentősen növelheti a rendőrség hatékonyságát, ugyanakkor elengedhetetlen a szabályozás és az átláthatóság biztosítása.[24]

4. MESTERSÉGES INTELLIGENCIA ALKALMAZÁSÁNAK KOCKÁZATAI A TERRORIZMUSKUTATÁSBAN ÉS TERRORELHÁRÍTÁSBAN

A mesterséges intelligencia terrorizmuskutatásban és terrorelhárításban való alkalmazása kétségtelenül hatalmas potenciált rejt. Az MI képes felgyorsítani az adatelemzést, feltárni a rejtett mintázatokat, és új képességekkel ruházza fel a biztonsági szerveket. Azonban a technológia bevezetése nem mentes a komoly kihívásoktól és dilemmáktól.

4.1. FELTANÍTÓ ADATOK HIÁNYA ÉS MÓDSZERTANI KIHÍVÁSOK

Az MI-modellek hatékonysága nagymértékben függ a rendelkezésre álló adatok minőségétől és mennyiségétől. A terrorizmuskutatás területén ez számos problémát vet fel. Az egyik legfőbb kihívás az adatritkaság és a kiegyensúlyozatlanság. A terrortámadások, bár rendkívül súlyos következményekkel járnak, statisztikailag ritka események a mindennapi emberi tevékenységek milliárdjaihoz képest.

További jelentős probléma a „concept drift”, azaz a jelenség folyamatos változása. A terrorista csoportok tudatosan és gyorsan adaptálódnak: új kódnyelveket, szimbólumokat, kommunikációs platformokat és taktikákat alkalmaznak, hogy elkerüljék a lelepleződést. Egy MI-modell, amelyet a múltbeli adatokon tanítottak, gyorsan elavulttá válhat, ha nem frissítik és tanítják újra folyamatosan a legújabb trendeknek megfelelően.

A modellek általánosíthatósága is kérdéses. Egy adott régióban vagy nyelvi kontextusban sikeresen működő modell nem biztos, hogy hatékony lesz egy másik kulturális vagy nyelvi környezetben, különösen az alacsony erőforrású nyelvek esetében, ahol kevesebb a rendelkezésre álló tanítóadat. Ez különösen problematikus a globális terrorista fenyegetések kezelésében, ahol a csoportok gyakran több kultúrában és nyelvben is aktívak.

Az adatminőség kérdése szintén kritikus. A terrorizmuskutatásban használt adatok gyakran hiányosak, torzítottak vagy megbízhatatlanok. A nyílt forrású adatok esetében nehéz megállapítani a hitelességet, míg a titkosított vagy kormányzati adatok esetében a hozzáférés korlátozott. Ez befolyásolja a modellek teljesítményét és megbízhatóságát.

[24] MÄKELÄ (2024)

4.2. ERKÖLCSI, JOGI ÉS TÁRSADALMI DILEMMÁK

Az MI terrorelhárítási alkalmazása talán a legkomolyabb kérdéseket az alapjogok területén veti fel. Az egyik leggyakrabban hangoztatott aggodalom az algoritmikus torzítás. Ha a modelleket elavult adatokon tanítják, amelyek maguk is tükrözik a múltbeli társadalmi vagy intézményi előítéleteket, az MI-rendszerek nem csupán reprodukálhatják, hanem fel is erősíthetik ezeket a torzításokat. Ez oda vezethet, hogy bizonyos etnikai, vallási vagy politikai csoportokat aránytalanul nagy mértékben jelölnek meg gyanúsként, ami súlyos diszkriminációhoz és a közösségek megbélyegzéséhez vezet. Az izraeli „Lavender" MI-rendszer esete, amely a sajtó szerint több ezer palesztint azonosított tévesen ellenséges harcosként, drámai példája ennek a veszélynek.[25]

A magánélethez való jog és a tömeges megfigyelés kérdése szintén központi dilemma. Az MI képessége a hatalmas adatmennyiségek feldolgozására eltörölheti a gyakorlati korlátokat, amelyek eddig gátat szabtak a totális megfigyelésnek. Szigorú jogi keretek, az arányosság és szükségesség elvének betartása, valamint átlátható adatvédelmi szabályozás nélkül a célzott megfigyelés könnyen átcsaphat válogatás nélküli, a teljes lakosságot érintő adatgyűjtésbe.

A „fekete doboz" probléma az átláthatóság és az elszámoltathatóság hiányára utal. Sok fejlett mélytanulási modell annyira komplex, hogy még a fejlesztőik sem tudják pontosan megmagyarázni, miért hozott egy adott döntést. Ez aláássa a jogorvoslathoz való jogot, hiszen az érintett nem tudja, milyen alapon született a rá nézve hátrányos döntés, és így vitatni sem tudja azt.

A Tom Cruise főszereplésével készült Különvélemény (Minority Report) című film[26] fiktív példát szolgáltat arra, hogy milyen veszélyeket rejt magában, ha a rendvédelmi szervek minden gépi javaslatot megkérdőjelezhetetlennek tekintenek. A filmben a jövőben játszódó történet szerint a rendőrség egy olyan prediktív rendszert alkalmaz, amely előre jelzi a bűncselekményeket, így azokat még elkövetésük előtt megakadályozzák. Idővel azonban a rendőrök kritikátlanul elfogadják a rendszer döntéseit, és nem kérdőjelezik meg azok helyességét, ami súlyos igazságtalanságokhoz vezet. Ez a helyzet jól rávilágít az elszámoltathatóság problémájára is: hiba esetén ki a felelős – a fejlesztő, az üzemeltető, a döntést jóváhagyó emberi felügyelő, vagy a szakpolitikát alkotó szerv? Ez a bizonytalanság különösen veszélyes, ha az MI-rendszer téves döntése ártatlan emberek letartóztatásához vagy akár életének elvesztéséhez vezet. A prediktív rendészet és az autonóm rendszerek

[25] HVG (2025)
[26] *Különvélemény* (2002)

alkalmazása alapvető jogállami elveket, például az ártatlanság vélelmét és a bűncselekmény utáni felelősségre vonást is megkérdőjelezi. Ha egy algoritmus előre jelzi, hogy valaki terrorista támadást fog elkövetni, felmerül a kérdés: milyen alapon és milyen mértékben korlátozhatók ennek a személynek a jogai? Ez a dilemma különösen éles a preventív őrizetbe vétel és a célzott megfigyelés esetében, ahol az emberi jogok védelme és a közbiztonság közötti egyensúly megtalálása rendkívül nehéz feladat.

4.3. TECHNOLÓGIAI FEGYVERKEZÉSI VERSENY

A terrorista csoportok saját MI-képességeinek fejlődése egy technológiai fegyverkezési versenyt indított el. Ahogy a terrorelhárító szervek egyre kifinomultabb MI-eszközöket fejlesztenek, a terroristák is adaptálódnak és saját technológiai képességeiket építik ki. Ez egy dinamikus, folyamatosan változó környezetet teremt, ahol mindkét oldal igyekszik technológiai előnyre szert tenni. A generatív MI, különösen a nagy nyelvi modellek és a deepfake technológiák, különösen veszélyesek a terroristák kezében. Ezek az eszközök lehetővé teszik rendkívül meggyőző propaganda-tartalmak tömeges előállítását, hamis hírek terjesztését és a közvélemény manipulálását. A technológia demokratizálódása azt jelenti, hogy ezek az eszközök egyre könnyebben elérhetők még a kisebb, kevésbé erőforrásokkal rendelkező csoportok számára is. Az adversarial machine learning, azaz az MI-rendszerek elleni támadások tudománya, szintén komoly fenyegetést jelent. A terroristák megtanulhatják, hogyan „mérgezzék meg” a terrorelhárító MI-rendszereket hamis adatokkal, vagy hogyan kerüljék el a detektálást speciálisan kialakított tartalmakkal. Ez egy macska-egér játékot eredményez, ahol a védekezők folyamatosan frissíteniük kell rendszereiket az új támadási módszerekre.

4.4. NEMZETKÖZI EGYÜTTMŰKÖDÉS ÉS SZABÁLYOZÁSI KIHÍVÁSOK

A terrorizmus globális jelenség, amely nem ismer határokat. Az MI-alapú terrorelhárítás hatékonysága nagymértékben függ a nemzetközi együttműködéstől és az adatmegosztástól. Azonban a különböző országok eltérő jogi keretei, adatvédelmi szabályozásai és politikai érdekei gyakran akadályozzák ezt az együttműködést. Az Európai Unió GDPR szabályozása[27] például szigorú korlátokat szab a személyes adatok feldolgozására, ami megnehezíti az MI-alapú terrorelhárítási rendszerek működését. Másrészt az Egyesült Államok és Kína közötti technológiai verseny befolyásolja az MI-technológiák megosztását és fejlesztését a biztonsági területen. A szabályozási környezet fragmentáltsága

[27] *Az Európai Parlament és a Tanács 2016. április 27-i (EU) 2016/679 sz. rendelete.*

azt jelenti, hogy nincs egységes nemzetközi keret az MI terrorelhárítási alkalmazására. Ez problematikus, mivel a terroristák kihasználhatják ezeket a jogi réseket és a kevésbé szabályozott területekre helyezhetik át tevékenységüket.

4.5. ALKALMAZÓI HIÁNYOSSÁGOK

Az MI-rendszerek hatékonysága nagymértékben függ az emberi szakértelemtől és felügyelettől. A terrorizmuskutatás komplex, kontextusfüggő terület, ahol a kulturális, vallási és politikai árnyalatok megértése kritikus fontosságú. Az MI-algoritmusok, bármilyen kifinomultak is, nem helyettesíthetik teljesen az emberi intuíciót és szakértelmet. A „human-in-the-loop" megközelítés, ahol az emberi szakértők és az MI-rendszerek együttműködnek, bizonyult a leghatékonyabbnak. Ez a hibrid modell lehetővé teszi az MI gyorsaságának és skálázhatóságának kihasználását, miközben megőrzi az emberi ítélőképesség és kontextuális megértés előnyeit. Azonban ez a megközelítés új kihívásokat is teremt. A szakértők képzése és folyamatos továbbképzése kritikus fontosságú, mivel az MI-technológiák gyorsan fejlődnek. Emellett a kognitív torzítások, mint például az automatizációs bias, ahol az emberek túlzottan bíznak az algoritmusok döntéseiben, szintén veszélyt jelenthetnek.

4.6. JÖVŐBELI KUTATÁSI IRÁNYOK

A mesterséges intelligencia terrorizmuskutatásban való alkalmazása még mindig egy fejlődő terület, ahol számos kutatási lehetőség vár feltárásra. Az egyik legígéretesebb irány a multimodális MI-rendszerek fejlesztése, amelyek képesek egyidejűleg elemezni a szöveges, vizuális és audio tartalmakat. Ez holisztikusabb megértést tesz lehetővé a terrorista kommunikációról és propagandáról.[28] A gépi tanulás egy másik izgalmas terület, amely exponenciálisan növelheti az MI-rendszerek számítási kapacitását. Ez lehetővé teheti a jelenleg feldolgozhatatlanul nagy adathalmazok elemzését és a komplex optimalizálási problémák megoldását a terrorelhárításban. A federated learning, azaz az elosztott tanulás, megoldást jelenthet az adatmegosztási és magánélet-védelmi kihívásokra. Ez a megközelítés lehetővé teszi, hogy a különböző szervezetek együttműködjenek az MI-modellek fejlesztésében anélkül, hogy megosztanák az érzékeny adataikat.

4.7. SZAKPOLITIKAI AJÁNLÁSOK

A kutatási eredmények alapján több szakpolitikai ajánlás fogalmazható meg az MI terrorelhárítási alkalmazásának optimalizálására. Először is, szükséges egy átfogó,

[28] RÉMAI – HEGEDŰS (2024)

nemzetközi szintű szabályozási keret kidolgozása, amely egyensúlyt teremt a biztonsági szükségletek és az emberi jogok védelme között. Másodszor, a transzparencia és elszámoltathatóság növelése érdekében kötelezővé kellene tenni az explainable AI technológiák alkalmazását a kritikus biztonsági döntésekben. Harmadszor, a nemzetközi együttműködés erősítése érdekében közös adatmegosztási protokollokat és technológiai standardokat kellene kidolgozni. Negyedszer, a szakértői képzés és továbbképzés rendszerének fejlesztése kritikus fontosságú. Az MI-technológiák gyors fejlődése megköveteli, hogy a terrorelhárítási szakemberek folyamatosan frissítsék tudásukat és készségeiket. Végül, az akadémiai közösség és a teljes civil társadalom bevonása és a nyilvános vita ösztönzése szükséges az MI terrorelhárítási alkalmazásának társadalmi elfogadottságának növelése érdekében. A technológia csak akkor lehet igazán hatékony, ha a társadalom támogatja és megérti annak szükségességét és korlátait.

5. TÁRSDALMI KÜLÖNBSÉGEK ÉS KULTURÁLIS ADAPTÁCIÓ

A mesterséges intelligencia terrorizmuskutatásban való alkalmazása nem egységes globális jelenség. Jelentős regionális különbségek figyelhetők meg mind a technológiai fejlettség, mind a szabályozási környezet, mind pedig a társadalmi elfogadottság tekintetében. Ezek a különbségek befolyásolják az MI-technológiák hatékonyságát és alkalmazhatóságát. Az Egyesült Államokban a technológiai innováció és a magánszféra bevonása jellemzi a megközelítést. A szilícium-völgyi technológiai óriások, mint a Google, a Microsoft és az Amazon, szorosan együttműködnek a kormányzati szervekkel az MI-alapú terrorelhárítási megoldások fejlesztésében. Ez gyors innovációt eredményez, de etikai kérdéseket is felvet a magánszféra és a kormányzat közötti határok elmosódásával kapcsolatban. Európában a GDPR és más adatvédelmi szabályozások szigorúbb keretet teremtenek az MI alkalmazására. Ez lassíthatja a technológiai fejlődést, de erősebb védelmet nyújt az állampolgári jogoknak. Az európai megközelítés hangsúlyozza az „etikus MI” koncepcióját és a technológiai szuverenitást. A fejlődő országokban az erőforrások hiánya és a technológiai lemaradás jelenti a fő kihívást. Ezek az országok gyakran függnek a fejlett országok technológiai támogatásától, ami függőségi viszonyokat teremt és korlátozza a szuverenitást.

6. KÉPZÉS, KÉPZÉS ÉS MÉG TÖBB GYAKOLATI KÉPZÉS

A mesterséges intelligencia terrorizmuskutatásban való sikeres alkalmazása nagymértékben függ a megfelelően képzett emberi erőforrásoktól. Ez egy új típusú

szakértelem iránti igényt teremt, amely kombinálja a technológiai ismereteket a biztonsági szakértelemmel és a társadalomtudományi megértéssel. A hagyományos terrorelhárítási szakembereknek meg kell tanulniuk az MI-technológiák eljárásmódjait, trükkjeit, hogy hatékonyan tudjanak együttműködni az autonóm rendszerekkel. Ez magában foglalja az algoritmusok működésének megértését, a modellek korlátainak felismerését és a hamis pozitív eredmények kezelését. Másrészt az MI-szakértőknek meg kell érteniük a terrorizmus komplexitását, a kulturális és vallási kontextusokat, valamint a biztonsági műveletek sajátosságait. Ez interdiszciplináris képzést igényel, amely ritkán található meg a hagyományos egyetemi programokban. A képzési kihívásokat súlyosbítja a technológia gyors fejlődése. Az MI-területen a tudás gyorsan elavul, ami folyamatos továbbképzést tesz szükségessé. Emellett a terrorista taktikák is folyamatosan változnak, ami megköveteli a biztonsági szakemberektől a rugalmasságot és az adaptációs képességet.

7. TECHNOLÓGIAI STANDARDIZÁCIÓ ÉS ÁTJÁRHATÓSÁG

A mesterséges intelligencia terrorizmuskutatásban való hatékony alkalmazása megköveteli a különböző rendszerek közötti interoperabilitást és a technológiai standardok kidolgozását. Jelenleg a különböző szervezetek és országok gyakran inkompatibilis rendszereket használnak, ami akadályozza az információmegosztást és a koordinált fellépést. A NATO már elindította a Defence Innovation Accelerator for the North Atlantic (DIANA) programot[29], amely célja az MI-technológiák standardizálása a szövetséges országok között. Hasonlóképpen, az Európai Unió a Digital Europe Programme[30] keretében dolgozik az MI-alapú biztonsági rendszerek harmonizálásán. A standardizáció kihívásai nemcsak technológiai, hanem jogi és politikai természetűek is. A különböző országok eltérő adatvédelmi szabályozásai, biztonsági protokolljai és politikai érdekei gyakran akadályozzák az egységes standardok kidolgozását.

8. ÖSSZEFOGLALÁS

Jelen tanulmány átfogó elemzést nyújtott a mesterséges intelligencia terrorizmuskutatásban való alkalmazásának lehetőségeiről, kihívásairól és jövőbeli irányairól. A kutatás eredményei megerősítik mindhárom hipotézisünket, miközben árnyalt képet festenek a technológia potenciáljáról és korlátairól. Az első hipotézis, amely szerint az MI-technológiák jelentős

[29] NATO (2025)
[30] EU4DIGITAL (2025)

mértékben javíthatják a terrorista fenyegetések korai felismerését és előrejelzését, teljes mértékben igazolódott. A bemutatott feljhasználói formák és esettanulmányok mind azt bizonyítják, hogy az MI forradalmasíthatja a terrorelhárítást. A technológia képes feldolgozni és elemezni olyan mennyiségű adatot, amely emberi erővel kezelhetetlen lenne, miközben rejtett mintázatokat és kapcsolatokat tár fel. A második hipotézis, amely az etikai és jogi dilemmákra vonatkozott, szintén beigazolódott. A tanulmány részletesen bemutatta az algoritmikus torzítás, a magánélet megsértése, az átláthatóság hiánya és az elszámoltathatóság problémáit. Ezek a kihívások nem csupán elméleti aggályok, hanem konkrét, gyakorlati problémák, amelyek már most is befolyásolják az MI-rendszerek alkalmazását. Az izraeli „Lavender" rendszer esete vagy a prediktív rendészet vitatott alkalmazása jól illusztrálja ezeket a dilemmákat. A harmadik hipotézis, amely a technológiai fegyverkezési versenyre vonatkozott, szintén igazolást nyert. A terrorista csoportok, különösen az ISIS és kapcsolt szervezetek, egyre kifinomultabban alkalmazzák az MI-technológiákat saját céljaikra. A deepfake propaganda-videóktól az adversarial machine learning technikákon át az autonóm támadóeszközökig, a terroristák gyorsan adaptálják a legújabb technológiákat. Ez valóban egy folyamatos versenyt eredményez a terrorelhárító szervek és a terrorista csoportok között.

8.1. KÖVETKEZTETÉSEK

A kutatás során több kulcsfontosságú megállapítás kristályosodott ki. Először is, az MI nem csodaszer a terrorizmus ellen, hanem egy hatékony eszköz, amely megfelelő alkalmazás esetén jelentősen javíthatja a terrorelhárítás hatékonyságát. A technológia legnagyobb erőssége a nagy adathalmazok gyors feldolgozásában és a mintázatok felismerésében rejlik, de nem helyettesítheti teljesen az emberi szakértelmet és ítélőképességet.Másodszor, a sikeres MI-alkalmazás megköveteli a technológiai, jogi, etikai és társadalmi szempontok egyidejű figyelembevételét. A tisztán technológiai megközelítések, amelyek figyelmen kívül hagyják az emberi jogokat és a társadalmi elfogadottságot, hosszú távon kudarcra vannak ítélve. Harmadszor, a nemzetközi együttműködés kritikus fontosságú. A terrorizmus globális jelenség, amely globális válaszokat igényel. Az MI-technológiák hatékonysága nagymértékben függ az adatmegosztástól és a koordinált fellépéstől, ami megköveteli a nemzeti szuverenitás és a biztonsági érdekek közötti egyensúly megtalálását. Negyedszer, a folyamatos adaptáció és tanulás szükségessége. Mind a terrorista csoportok, mind a terrorelhárító szervek gyorsan adaptálódnak az új technológiákhoz. Ez megköveteli a rugalmas, gyorsan frissíthető rendszerek fejlesztését és a folyamatos kutatás-fejlesztési befektetéseket.

8.2. JAVASLATOK

A jövőre nézve több fontos trend rajzolódik ki. A multimodális MI-rendszerek, amelyek képesek egyidejűleg elemezni a különböző típusú adatokat, még hatékonyabbá tehetik a fenyegetés-detektálást. A gépi tanulás exponenciálisan növelheti a számítási kapacitásokat, míg a federated learning megoldást jelenthet az adatmegosztási dilemmákra. A jövő MI-rendszereinek nemcsak hatékonyaknak, hanem érthetőeknek és elszámoltathatóaknak is kell lenniük. A szabályozási környezet fejlődése szintén kulcsfontosságú. Szükség van olyan nemzetközi keretekre, amelyek egyensúlyt teremtenek a biztonsági szükségletek és az emberi jogok között, miközben ösztönzik az innovációt és a nemzetközi együttműködést.

9. ZÁRÓ GONDOLATOK

A mesterséges intelligencia alkalmazása a terrorizmuskutatásban és terrorelhárításban egy kettős kihívást jelent: egyrészt hatalmas lehetőségeket kínál a biztonság növelésére, másrészt komoly kockázatokat hordoz az emberi jogok és a demokratikus értékek szempontjából. A siker kulcsa a felelős innováció, amely maximalizálja a technológia előnyeit, miközben minimalizálja a kockázatokat. Ez megköveteli a technológiai fejlesztők, a biztonsági szakemberek, a jogalkotók, az etikusok és a civil társadalom szoros együttműködését. Csak egy ilyen holisztikus megközelítés biztosíthatja, hogy az MI valóban a biztonság és a szabadság szolgálatában álljon, nem pedig azok rovására. A terrorizmus elleni küzdelem hosszú távú sikere nem csupán a technológiai fölényen múlik, hanem azon is, hogy mennyire sikerül megőrizni azokat az értékeket és elveket, amelyeket védeni kívánunk. Az MI ebben a küzdelemben hatékony szövetséges lehet, de csak akkor, ha bölcsen és felelősségteljesen alkalmazzuk, és szinte mindenki képes alkalmazni. A jövő kihívásai megkövetelik, hogy folyamatosan újragondoljuk az MI szerepét a terrorelhárításban. A technológia fejlődésével párhuzamosan fejlődniük kell a jogi kereteknek, az etikai irányelveknek és a társadalmi normáknak is. Csak így biztosíthatjuk, hogy az MI valóban szolgálja az emberiség érdekeit a terrorizmus elleni küzdelemben.

FELHASZNÁLT IRODALOM

Az Európai Parlament és a Tanács 2016. április 27-i (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet)

EU4DIGITAL (2025): *A Digital Europe Programme céljai és prioritásai*. Online: https://eufordigital.eu/discover-eu/the-digital-europe-programme/ (Letöltve: 2025. június 6.)

EURÓPAI BIZOTTSÁG (n.d.): *Entry/Exit System (EES). Travel Europe*. https://travel-europe.europa.eu/en/ees

EUROPEAN COMMISSION (2025): *Entry/Exit System (EES) – Information for travellers*. Online: https://travel-europe.europa.eu/en/ees (Letöltve: 2025. június 15.)

European Commission (n.d.): *Entry/Exit System (EES) – Information for travellers*. https://travel-europe.europa.eu/en/ees

FARKAS Ádám – VIKMAN László (2024): Information Operations as a Question of Law and Cyber Sovereignty. *ELTE Law Journal*, 2024(2), 187–202. Online: https://doi.org/10.54148/ELTELJ.2024.2.187 (Letöltve: 2025. június 15.)

GOOGLE AI BLOG (2018): *Open sourcing BERT: State-of-the-art pre-training for natural language processing*. Online: https://ai.googleblog.com/2018/11/open-sourcing-bert-state-of-art-pre.html (Letöltve: 2025. június 15.)

HVG (2025. április 3.): *Totális megfigyelést készül indítani Izrael: ijesztően alapos mesterséges intelligenciát engednek a palesztinokra*. Online: https://hvg.hu/tudomany/20250403_izraeli-palesztin-haboru-mesterseges-intelligencia-palesztinok-megfigyeles-lehallgatas (Letöltve: 2025. június 15.)

IBM (2025): *Random forest. In Think: Topics*. Online: https://www.ibm.com/think/topics/random-forest (Letöltve: 2025. június 15.)

INNEFU LABS. (2025): *Innefu – Artificial Intelligence, Cyber Security & Big Data Analytics*. Online: https://innefu.com/ (Letöltve: 2025. június 15.)

INSIKT INTELLIGENCE S.L. (2020a): *Novel Social Data Mining Platform to Detect and Defeat Violent Online Radicalization (INSIKT) (H2020 projekt, 767542)*. CORDIS – EU research results. Online: https://cordis.europa.eu/project/id/767542 (Letöltve: 2025. június 15.)

INSIKT INTELLIGENCE S.L. (2020b): *Periodic Reporting for period 2 – INSIKT (Novel Social Data Mining Platform to Detect and Defeat Violent Online Radicalization) (Projektazonosító: 767542).* CORDIS – EU research results. Online: https://cordis.europa.eu/project/id/767542/reporting (Letöltve: 2025. június 10.)

JONES, Mared Gwyn (2025): *Tényellenőrzés: az izraeli és iráni légicsapásokat bemutató videók hitelességéről*. Euronews. Online: https://hu.euronews.com/my-europe/2025/06/17/tenyelenorzes-az-izraeli-es-irani-legicsapasokat-bemutato-videok-hitelessegerol (Letöltve: 2025. június 15.)

KÁDÁR Pál (2023): A *kibertér és a kibertérműveleti képességek jelentősége a védelmi és biztonsági tevékenységek összehangolásának fejlesztés*ében. In FARKAS Ádám – KELEMEN Roland (szerk.): *A fejlődés fogságában? Tanulmányok a kibertér és a mesterséges intelligencia 21. századi állam- és jogfejlesztési, társadalmi, biztonsági kapcsolódásai köréből*. Budapest: Gondolat Kiadó, 149–165.

KAVLAKOGLU, Eda – RUSSI, Erika (2024): What is XGBoost? In Think: Topics. *IBM*. Online: https://www.ibm.com/think/topics/xgboost (Letöltve: 2025. június 15.)

KELEMEN Roland (2024): *Kibertér és (kiber)biztonság: A digitális kihívások evolúciója a globális trendek szorításában*. In FARKAS Ádám – KELEMEN Roland (szerk.)*: Kibertér és biztonság egyes jogtani és államtani kérdései.* Győr: Universitas-Győr Nonprofit Kft., 15–29.

KUGLER Péter (2022): *A szentimentelemzés alapjai I. – Áttekintés és szövegelemzés*. Ludovika Cyberblog. Online: https://www.ludovika.hu/blogok/cyberblog/2022/06/22/a-szentimentelemzes-alapjai-i-attekintes-es-szovegelemzes/ (Letöltve: 2025. június 15.)

Különvélemény (2002). Rend. Spielberg, S. 20th Century Fox; DreamWorks Pictures. Online: https://www.imdb.com/title/tt0181689/

MÄKELÄ, Marianna (2024): *Artificial intelligence in policing [Szakdolgozat, Laurea University of Applied Sciences]*. Theseus. Online: https://www.theseus.fi/bitstream/handle/10024/854179/Makela_Marianna.pdf?sequence=2 (Letöltve: 2025. június 10.)

METROPOLITAN POLICE (2023): *Information about AI models (FOI request reference no: 01.FOI.23.031755).* Online: https://www.met.police.uk/foi-ai/metropolitan-police/disclosure-2023/september-2023/information-ai-models/ (Letöltve: 2025. június 15.)

MINISTÈRE DE L'INTÉRIEUR (2025): *Direction générale de la sécurité intérieure (DGSI)*. Online: https://www.interieur.gouv.fr/ministere/direction-generale-de-securite-interieure (Letöltve: 2025. június 17.)

NATO (2025): *Key elements of NATO's digital strategy*. Online: https://www.nato.int/cps/en/natohq/topics_216199.htm (Letöltve: 2025. augusztus 6.)

ONLINE SPECIALISTA (2024): *A legfontosabb közösségi média platformok Magyarországon 2025-ben.* Online: https://onlinespecialista.hu/kozossegi-media/a-legfontosabb-kozossegi-media-platformok-magyarorszagon-2025-ben/ (Letöltve: 2025. június 12.)

PORTFOLIO (2024): *Villámgyorsan vásárolt be a NATO: egy hónapon belül működőképes lesz a MavEN*. Online: https://www.portfolio.hu/global/20250414/villamgyorsan-vasarolt-be-a-nato-egy-honapon-belul-mukodokepes-lesz-a-maven-754925 (Letöltve: 2025. június 19.)

PRENTICE, Sheryl – TAYLOR, Paul J. – RAYSON, Paul – HOSKINS, Andrew – O'Loughlin, Ben (2011): Analyzing the semantic content and persuasive composition of extremist media: A case study of texts produced during the Gaza conflict. *Information Systems Frontiers*, 13(1), 61–73.

PRESTIGE ONLINE SINGAPORE (2025): *Singapore ranks 2nd safest city in Southeast Asia's safety rankings*. 2025. . július 18. Online: https://www.prestigeonline.com/sg/lifestyle/southeast-asia-safety-rankings-safest-city-2025/ (Letöltve: 2025. június 25.)

RÉMAI Dániel – HEGEDŰS Judit (2024): *Innovatív adatvizualizációs eszközök alkalmazása a modern felsőoktatásban*. In CZENE-POLGÁR Viktória – MAGASVÁRI Adrienn – ZSÁMBOKINÉ FICSKOVSZKY Ágnes: *Hatósági munka, szolgáltatások és tanulás támogatása modern eszközökkel*. Budapest: Magyar Rendészettudományi Társaság Határrendészeti Tagozat. 225–236. Online: http://doi.org/10.37372/mrttvpt.2024.1.19 (Letöltve: 2025. június 17.)

RÉMAI Dániel (2024): *Vizualizáljunk adatot!* Online: https://www.ludovika.hu/blogok/kreativity-blog/2024/03/04/vizualizaljunk-adatot/ (Letöltve: 2025. június 11.)

SAIDI, R. – TRABELSI, Z. (2022): A hybrid CNN-LSTM model for terrorism prediction. *IEEE Access*, 10, 34320–34331.

START (2025): *Global Terrorism Database*. Online: https://www.start.umd.edu/gtd (Letöltve: 2025. június 5.)

THOMSON REUTERS (2025): *What is a Suspicious Activity Report (SAR)?* Online: https://legal.thomsonreuters.com/en/insights/articles/what-is-a-suspicious-activity-report (Letöltve: 2025. június 25.)

ZERROUKI, N. – BENBLIDIA, N. (2024): Multilingual extremist content detection using transformer models. *Expert Systems with Applications*, 238, 121–135.

ZŐDI Zsolt (2024): A Facebook tartalom- és fiókkorlátozási gyakorlata: szabályok, eljárások, algoritmusok és statisztikák. Néhány empirikus adalék a „szólásszabadság a platformokon" diskurzushoz. *Fontes Iuris*, 10(3–4), 5–28. Online: https://ojs.mtak.hu/index.php/fontesiuris/article/view/19548 (Letöltve: 2025. június 5.)

VÁKÁT OLDAL

Forró Tamás

A kritikus információs infrastruktúra fenyegetettsége kiberterrorizmus szempontjából

1. BEVEZETÉS

Napjainkban az információ hasonlóan fontos és értékes szerepet tölt be a világ működésében, mint például a nyersanyagok vagy az energiahordozók, lényegében a társadalom egyik alappillérévé vált. Felértékelődését jól mutatja, hogy Magyarországon 2021-ben a témának dedikált jogszabály[1] született a nemzeti adatvagyonról és annak kezeléséről, védelméről. „Fejlett korunkban a társadalmi, a gazdasági, illetve a rendvédelmi szektor működésében az információ központi szerepet tölt be, így annak szükséges mennyisége és megfelelő minősége elengedhetetlenül fontos ahhoz, hogy a döntés-előkészítő, a döntéshozó, illetve a végrehajtó folyamatok hatékonysága az elvárásoknak megfelelő legyen.”[2] Ugyanakkor értékének növekedésével párhuzamosan jelennek meg a különböző információk megszerzésére, vagy az ezeket kezelő és feldolgozó rendszerek megzavarására irányuló támadások is, melyek elsősorban a kibertérben zajlanak.

1.1. A KIBERTÉR

A kibertér alapvetően az információs környezet fontos, hálózatos tartománya, de bővebb, kiterjedtebb, mint a klasszikus számítógép-hálózatok. Maga a kifejezés a görög kyber (hajózni, navigálni, kormányozni) szóból származik, és eredeti értelmében hajózásra alkalmas teret jelent. William Ford Gibson használta először a mai tartalmával, az 1982-es Izzó króm című novellájában, de alapvetően az 1984-ben napvilágot látott Neuromancer című novellája révén terjed el. Ebben használja ezt a fogalmat a hálózatba kapcsolt, számítógép-terminálokról közvetlenül elérhető digitális, navigálható tér meghatározására. Napjainkra alapvetően azt a mesterségesen létrehozott, összetett, dinamikus, tehát állandóan változó és fejlődő környezetet jelenti, mely magában foglalja az internetet, a számítógépes rendszereket, globális kommunikációs hálózatokat, továbbá tágabb értelmezésben azokat a gazdasági, társadalmi, politikai folyamatokat is, melyek ebben a virtuális térben zajlanak.

---

[1] *2021. évi XCI. törvény a nemzeti adatvagyonról.*
[2] PAPP (2018)

Napjainkban a kibertér gyakorlatilag megkerülhetetlen, a modern, információs társadalom működése jelentősen összefonódik vele. Az internet elterjedése és a digitális eszközök használata forradalmasította az információhoz való hozzáférést, lehetővé téve a globális kommunikációt, valamint az információk gyors és hatékony megosztását. E fejlődés hatására kialakult az információs társadalom, melyben az adatok és az információk a gazdasági és társadalmi élet középpontjába kerültek.

Az Amerikai Egyesült Államok Védelmi Minisztériumának Katonai és kapcsolódó kifejezések szótárában[3] az alábbi értelmezését találhatjuk: „Egy globális tartomány az informatikai környezeten belül, amely tartalmazza az egymással összefüggő informatikai hálózatok infrastruktúráit, beleértve az internetet, a távközlési hálózatokat, a számítógépes rendszereket, valamint beágyazott processzorokat és vezérlőket."[4] Magyarország Nemzeti Kiberbiztonsági Stratégiájáról szóló 1139/2013. (III. 21.) Korm. határozat (a továbbiakban: Kiberbiztonsági Stratégia) is hasonlóan fogalmaz: „A kibertér globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét jelenti." Fontos azonban észrevenni azt, hogy a Kiberbiztonsági Stratégia által használt bővebb értelmezésben már megjelennek a társadalmi és gazdasági folyamatok is. A kiberterrorizmus szempontjából még ennél is bővebb az értelmezése és ezzel igen hasonló a napjainkban elterjed katonai értelmezéséhez, ami a számítógép-hálózati hadviselésnél egy jóval bővebb kört fed le. A modern megközelítésben ide tartozik a „navigációs és kommunikációs hálózatok pusztítása, lehallgatása, zavarása, a rendszerek elleni elektronikai ellentevékenység különböző formái, a számítógép-hálózatok feltérképezése, az azokba történő behatolás, az ott található adatbázisok, vagy az azokban lévő adatok tönkretétele, manipulálása, elérhetetlenné tétele, valamint az infrastruktúrák elemeinek túlterhelése, továbbá a támogató infrastruktúrák támadása is. E módszereken túl ide értendők még az információs infrastruktúrákat működtető személyzet különböző módszerekkel – akár a kibertérben, akár a fizikai térben történő – támadása, »zaklatása« is, mivel ezeknek hatása megjelenik a kibertérben."[5] Az elmúlt évek nyugat-európai terrortámadásaiban jelentős szerepet játszott a kibertér, bár az elkövetők mindezidáig elsősorban a kommunikációra, a propagandájuk terjesztésére, toborzásra és a működésük, cselekményeik finanszírozására

[3] U.S. DEPARTMENT OF DEFENSE (2010)
[4] MUHA– KRASZNAY (2022); A definíció angolul: „*A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.*"
[5] PAPP (2018)

használták; látható tehát, hogy valóban még a katonai értelmezésnél is tágabb ez a megközelítés.

1.2. A KIBERTERRORIZMUS

Papp Zoltán szerint a kiberterrorizmus az alábbi definícióval írható le: „A kiberterrorizmus a terrorizmus azon megjelenési formája, amikor a terrorcselekmény célpontjai az információs infrastruktúrák, illetve ezek rendszerelemei, a bennük kezelt adatok, funkciók és meglévő képességek, és/vagy a terrorcselekmény előkészítése, támogatása, végrehajtása során az elkövetők tevékenységében az információs infrastruktúrák egyes szolgáltatásai olyan hangsúlyos szerepet kapnak, mely nélkül a jogellenes cselekmény egyáltalán nem, vagy csak aránytalanul nagy nehézségek árán valósulhatott volna meg."[6] Véleményem szerint a definíció inkább a terroristák által végrehajtott kibertámadást írja le, nem pedig a kiberterrorizmust, ami szerintem a fentieknél egy sokkal jobban körülhatárolt dolog. Jordan Plotnek és Jill Slay kutatók a kiberterrorizmust előre megfontolt támadásként, illetve nem állami szereplők támadásaival való fenyegetésként határozzák meg, akik a kiberteret fizikai, politikai, gazdasági, ökológiai vagy egyéb károk okozására kívánják használni. Az elkövetők célja, hogy félelmet keltsenek, illetve olyan cselekvésekre kényszerítsék a kormányzati vagy nem kormányzati szerveket, amelyek elősegítik a terroristák társadalmi, pénzügyi vagy ideológiai céljait.[7]

A kiberterrorizmus azonosításához az alábbi kulcselemek megvalósulása szükséges egy cselekmény során:

- Az elkövetők egy nem állami hátterű, terrorista csoport tagjai.
- Az indítékuk vallási, ideológiai, társadalmi, gazdasági vagy politikai.
- Konkrét követelést fogalmaznak meg egy állammal, annak képviselőjével, vagy egy nemzetközi szervezettel szemben, valamilyen cselekvés előidézésére vagy kikényszerítésére, további célok elérésére.
- A cselekmény elkövetéséhez elsősorban a kiberteret használják és az elsődleges célpont is abban helyezkedik el, vagy azon keresztül érhető el.
- A cselekmény hatása közvetlenül, vagy közvetve halált, vagy súlyos sérülést, jelentős fizikai, gazdasági károkat okoz, illetve szolgáltatási zavarokat idéz elő.
- A támadás célpontjai pedig leggyakrabban civilek, a kritikus (információs) infrastruktúra, nyilvántartások, kormányzati, vagy nemzetközi szervek, szervezetek.

[6] PAPP (2018)
[7] PLOTNEK – SLAY (2021)

Ugyanakkor ezzel a megközelítéssel teljesen kizárnánk a kiberterrorizmus úgynevezett „soft” formáját (melyről a későbbiekben még szó lesz), továbbá a magyar és az európai uniós jogalkotás is ennél bővebben kezeli a témakört. Hasonló problémával szembesült *Bőczné Neparáczki Anna Viktória,* miszerint: „A kiberterrorizmus a terrorizmus egyik új megjelenési formája, a felhasznált eszközöket tekintve jelenik meg külön kategóriaként: a számítógépes rendszereket, hálózatokat és azok adattartalmát támadja, illetőleg használja fel saját céljai eléréséhez, kiberterrorizmus esetén tehát a kiberbűncselekményhez terrorista célzat társul. Ezen álláspont szerint a kiberterrorizmust el kell határolni a terroristák egyéb internetes tevékenységétől, mint a propaganda, pénzgyűjtés, információterjesztés, biztonságos kommunikáció, hírszerzés. Más álláspont szerint a kiberterrorizmus azokat a terrorista cselekményeket is magában foglalja, amelyek az interneten vagy a számítógépes hálózatokon jelentkeznek és itt kívánják céljukat elérni. Álláspontom szerint a kiberterrorizmus fogalma – hasonlóan a kiberbűnözéshez – gyűjtőfogalom. A kiberterrorizmus szűkebb értelemben informatikai környezettől függő bűnözési forma, az ún. tisztán kiberbűncselekmény terrorista célú elkövetését jelenti, amely az információtechnológia »hard« típusú felhasználásával valósul meg. A kiberterrorizmus tágabb értelemben magában foglalja az informatikai környezet által elősegített terrorista cselekményeket, azaz az információtechnológia »soft« típusú terrorista célú felhasználásának büntetendő formáit. Ezek a terrorista cselekmények az információtechnológia felhasználása nélkül is bűncselekményt valósítanak meg, de elkövetésüket segítheti, lényegesen megkönnyítheti, vagy akár egyáltalán lehetővé teheti az információs rendszer felhasználása.”[8]

1.3. A KIBERTÉR HASZNÁLATÁNAK ELŐNYEI ELKÖVETŐI SZEMSZÖGBŐL

A bevezetőben ugyan már néhány szó esett a kibertér előnyeiről, azonban érdemes összefoglalni azokat, abból az okból, hogy láthatóvá váljon, hogy milyen jelentős előnyöket jelent a használata az egyes elkövetői köröknek és ebből fakadóan mennyire megnehezíti a rendvédelmi szervek tevékenységét.

A kibertér talán egyik legjelentősebb előnye, hogy használatával eltűntek a fizikai országhatárok, egy támadás a világ bármely pontjáról végrehajtható anélkül, hogy fizikailag a célpont közelében kellene tartózkodni. Korábban igen komoly kihívást jelentett a terroristák számára, hogy lehetőleg észrevétlenül a támadásuk helyszínére érkezzenek, feltérképezzék azt, az elkövetéshez szükséges (többnyire illegálisan birtokolható) eszközöket beszerezzék, majd az elkövetés után távozzanak, vagy rejtve maradjanak. Ugyanakkor mind az eszközök

[8] BŐCZNÉ (2020)

beszerzése, mind az utaztatás, az elszállásolás, a képzés jelentős anyagi ráfordítást jelentett, mely szintén megváltozott. A kibertérben viszonylag kis befektetéssel, akár önképzés keretében, vagy egy a fentiekhez képest nagyságrendekkel olcsóbb szolgáltatás megvásárlásával lehet jelentős károkat okozni. További jelentős változás, hogy ezekhez az internet világában nincs szükség személyes találkozásokra, megfelelő technikai felkészültség és háttér esetén gyakorlatilag szinte teljesen biztosított az anonimitás, sőt az úgynevezett „false flag”[9] műveletek végrehajtása is jelentősen egyszerűsödött. A fentiek mellett az információszerzést is jelentősen megkönnyítette, lényegében forradalmasította az internet. Elképesztő mennyiségű információ érhető el rajta keresztül például a kritikus információs infrastruktúráról, az ott használt rendszerekről, eszközökről, sőt akár a védelemben részt vevő egyes konkrét személyekről is, köszönhetően a közösségi média dedikált portáljainak (pl.: LinkedIn[10]). Az előbbieken túl ugyancsak kiváló információforrás a támadóeszközökről is, amik alatt nem csak a kibereszközöket kell érteni, hanem a fizikaiakat is (például fegyverek, robbanóanyagok működésének leírása). A 2001. szeptember 11-ei terrortámadások után az Egyesült Államokban legalább 13 szövetségi ügynökség és három tartományi kormány távolított el anyagokat weboldalaikról, a terroristák számára hasznosítható, korábban közzétett információkkal kapcsolatos aggodalmakra hivatkozva.[11]

2. A KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRA

„A kibertértől való függőségünknek van egy másik oldala is, amely legalább olyan mértékű, mint maga a digitalizáció teremtette függőség. Ez nem más, mint a digitális szolgáltatásokat lehetővé tevő infrastruktúra, illetve azok együttese. Ezeket ma kritikus infrastruktúráknak, illetőleg kritikus információs infrastruktúráknak, […] létfontosságú elemeknek és rendszereknek is nevezzük. Kritikus rendszereink olyan szoros kapcsolatban vannak egymással, hogy egy-egy rendszer vagy rendszerelem kiesése negatív hatással van egy vagy akár több kritikus rendszerre.”[12]

[9] Magyarul: Hamis zászló alatt végrehajtott művelet. Azt a jellemzően katonai műveletet nevezzük így, amely során álcázott egységek szándékosan más erők nevében tevékenykednek, követnek el támadást.
[10] A LinkedIn a világ egyik legnagyobb üzleti közösségi hálózata. 2003-ban indult útjára és napjainkra közel 800 millió felhasználója van. Az oldal sajátossága, hogy a regisztrált személyek meglehetősen sok szakmai információt osztanak meg magukról önkét, kedvezőbb állásajánlatok reményében. Az oldalról elért információk már több esetben kerültek felhasználásra kibertámadások elkövetése során, valamint az oldal maga is több alkalommal került kompromittálásra.
[11] PEW RESEARCH CENTER (2002)
[12] KOVÁCS (2018)

1. ábra: *A kritikus infrastruktúra elemei*.
Forrás: Cybersecurity and Infrastructure Security Agency (2021).

A kritikus infrastruktúra fogalmát, jelentőségét a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló a 2012. évi CLXVI. törvény létfontosságú rendszerelem definíciójának nyomán lehet megérteni. Ez alapján a létfontosságú rendszerelem olyan „szolgáltatás, eszköz, létesítmény vagy rendszer olyan rendszereleme, továbbá azok által nyújtott szolgáltatások, amelyek elengedhetetlenek a létfontosságú társadalmi feladatok ellátásához – így különösen az egészségügyhöz, a lakosság személy- és vagyonbiztonságához, a gazdasági és szociális közszolgáltatások biztosításához, az ország honvédelméhez, – és amelynek kiesése e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna” (1. ábra). Az fentiek alapján látható, hogy ez gyakorlatilag definíció szerint tökéletes célpont lehet a terroristák számára, hiszen az esetlegesen sikeres támadásuk bizonyosan jelentős következményekkel járna a társadalom számottevő részére nézve, valamint az terrorizmushoz köthető zavar- és félelemkeltés is megvalósulhat.

A társadalom és a lakosság kitettségét jól tükrözi a Colonial Pipeline ellen intézett támadás[13], mely kezelésére az amerikai kormányzatnak vészhelyzeti rendelkezést[14] kellett kiadnia, annak érdekében, hogy az érintett államokban biztosíthassák a szállítás és ellátás zavartalanságát.

[13] TURTON – KARTIKAY (2021)
[14] THE GUARDIAN (2021)

Amennyiben az információs rendeltetésű kritikus infrastruktúrákat vizsgáljuk, úgy megállapíthatjuk, hogy azok nem feltétlenül egyeznek meg a kritikus infrastruktúrával. Várhegyi István és Makkay Imre definíciója alapján „az információs társadalom működéséhez szükséges információk előállítására, szállítására és felhasználására különböző rendeltetésű, funkciójú és típusú infrastruktúrarendszerek, hálózatok állnak rendelkezésre. Ezek összessége képezi az információs társadalom komplex információs infrastruktúráját."[15] A létfontosságú infrastruktúrák védelmére vonatkozó európai programról szóló Zöld Könyv szerint azokat az infokommunikációs technológiákat értjük a kritikus infrastruktúra alatt, melyek önmagukban kritikus infrastruktúrák, vagy amelyek létfontosságúak a kritikus infrastruktúrák működése szempontjából (ilyenek például: távközlés, számítógépek/szoftverek, internet, műholdak stb.).[16] Már a bevezetőben is említésre került, hogy mennyire meghatározza a mindennapjainkat az informatika fejlődése és az internet elterjedése. Ez alapján is megállapítható, hogy egy állam információtechnológiára támaszkodó infrastruktúrája joggal sorolható be a kritikus (információs) infrastruktúra közé. E gondolatmenet alapján „pl. egy ország nyilvános mobil távközlési hálózatai, mint önmagukban is kritikus infrastruktúrák, egyben kritikus információs infrastruktúráknak is minősülnek, illetve pl. az energiaellátó rendszert irányító, vezérlő számítógép-hálózat is ez utóbbiak közé sorolandó."[17] Haig Zsolt és Kovács László tanulmánya szerint egy ország kritikus információs infrastruktúrái közé legalább az alábbiak tartozhatnak:

- „energiaellátó rendszerek rendszerirányító számítógép-hálózatai;
- kommunikációs hálózatok (vezetékes, mobil, műholdas);
- közlekedés szervezés és irányítás számítógép-hálózatai;
- pénzügyi-gazdasági rendszer számítógép-hálózatai;
- védelmi szféra riasztási, távközlési, számítógép-hálózatai;
- egészségügyi rendszer számítógép-hálózatai;
- kormányzati és önkormányzati számítógép-hálózatok."[18]

A kritikus infrastruktúrák a létezésük óta kiemelt célpontjai voltak a hadviselő feleknek és a különböző támadóknak, támadásoknak. Kezdetben viszonylagos védelmet jelentettek az országhatárok, hiszen a támadások a fizikai térben valósultak meg, így, ha a tényleges megrendelőknek nem is feltétlenül, de az elkövetőknek mindenképpen jelen kellett lenniük.

[15] VÁRHEGYI – MAKKAY (2000)
[16] „ICT systems that are critical infrastructures for themselves or that are essential for the operation of critical infrastructures (telecommunications, computers/software, Internet, satellites, etc.)." EURÓPAI BIZOTTSÁG (2005)
[17] HAIG (2007)
[18] HAIG – KOVÁCS (2012)

A kibertér penetrációjával azonban ez gyökeresen megváltozott. A különböző és egyre bővülő potenciális elkövetői kör számára lényegesen kisebb ráfordítással is lehetővé vált a támadások végrehajtása, így a klasszikus háborús fenyegetettség mellett napjainkra előtérbe került ez az aszimmetrikus fenyegetés is. „E tekintetben kijelenthetjük, hogy a katonai és polgári természetű fenyegetések közötti hagyományos határvonal egyre inkább elmosódik."[19]

3. A KIBERTERRORIZMUS MÓDSZEREI ÉS ESZKÖZEI A KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRA BEFOLYÁSOLÁSÁRA

A tanulmányban mindezidáig elsősorban a kiberterrorizmus azon módszereiről volt szó, melyben a terror fogalmának megfelelően az erőszak és a rombolás kiemelt jelentőséggel bír. A kibertér, illetve annak előnyeinek bemutatása során azonban már látható volt, hogy az internet jóval több lehetőséget hordoz magában annál, hogy pusztán a támadások újabb célpontjait biztosítsa. Ennek megfelelően egyes szakirodalmak[20] az információtechnológia és a kibertér terrorista célú felhasználásának két csoportját különböztetik meg. Az úgynevezett „hard" típus esetében a terroristák „klasszikus" kibertámadásokat követnek el, a „soft" típus esetén pedig azokat a működésükhöz, fejlődésükhöz szükséges egyéb tevékenységeiket (például: kommunikáció, toborzás, finanszírozás, propaganda terjesztése stb.) végzik, amelyeket ezt megelőzően jellemzően a fizikai térben tevékenykedve végeztek, lényegesen nagyobb ráfordítások és kockázat mellett. A következőkben ezeket a tevékenységeket, módszereket és a felhasznált eszközeiket szeretném röviden bemutatni, elsősorban a „hard" módszerek és annak eszközkészlete fókuszálva.

3.1. HARD MÓDSZEREK

Az információtechnológia „hard" jellegű felhasználásakor a terroristák kifejezetten „klasszikus" kibertámadásokat hajtanak végre, felhasználva annak teljes eszköztárát. Jelenleg viszonylag alacsony az ilyen jellegű támadások száma, de a technológia további fejlődése (például a negyedik ipari forradalom vagy az 5. generációs vezeték nélküli hálózat elterjedése) jelentősen fokozza a rendszerek, hálózatok kitettségét.

3.2. A KIBERTERRORIZMUS ESZKÖZEI

A kiberterrorizmus esetében nem a fizikai dimenzióban működő, a valódi fegyverek hatásmechanizmusához hasonló eszközökre kell gondolnunk, hanem olyan szoftver- és

[19] HAIG (2007)
[20] BŐCZNÉ (2020)

hardvereszközökre, valamint ezek kibertéri alkalmazására, amelyekkel a kijelölt célpontok kompromittálhatóak, vagy számára valamilyen mértékű kár okozható. Ilyen fegyverek bevetésére már számos esetben volt példa.[21]

A rosszindulatú számítógépes programokat összefoglaló néven „Malware"-nek (Malicious Software) nevezzük, ami egy gyűjtőkategória, több kártevő tartozik ide. Közös jellemzőjük, hogy anélkül kerülnek a számítógépre, hogy arra a felhasználó engedélyt adott volna, vagy a program valódi célja és működése egyáltalán ismert lenne számára. Felkerülése után az alkalmazás erőforrást foglalhat le, adatszivárgást, adatvesztést eredményezhet, a számítógép fizikai hibáját okozhatja. Ide tartoznak a vírusok, trójai programok, rootkitek, keyloggerek, zsarolóprogramok, kémprogramok stb. Ezen eszközök közül szeretném röviden bemutatni azokat, melyek a kibertámadások és különösen a kiberterrorizmus szempontjából kiemelt jelentőséggel bírnak.

3.2.1. Zsarolóvírusok

„Zsarolóvírus (ransomware) alatt olyan kártékony szoftvert értünk, amelynek célja valamilyen módon »túszul ejteni« a felhasználók informatikai eszközein tárolt adatokat, amelyeket csak váltságdíj megfizetése esetén tesz újra elérhetővé. Az ilyen típusú károkozók néhány közös jellemzője, hogy:

- titkosítják az állományokat;
- zsaroló üzenetet jelenítenek meg;
- határidőt szabnak a váltságdíj kifizetésére;
- törlik az állományok egy részét;
- az idő múlásával egyre több állományt tesznek végleg visszaállíthatatlanná."[22]

A leggyakoribb esetben a fertőzés egy kéretlen e-mail káros csatolmányának útján kerül a megtámadott számítógépére. A melléklet megnyitása után lefut az abban található kód és megtörténik az állományok titkosítása, valamint néhány esetben a felhasználó kizárása is a rendszerből. A zsarolóvírusok általában kifejezetten erős titkosítást alkalmaznak, így a kódolt állományok visszafejtése szinte lehetetlen. Az ilyen jellegű támadások számra továbbra is igen magas és egyre komolyabb problémát jelent. 2020-ban, egy német korházat ért támadás halálos áldozattal is járt.[23] 2021-ben az Egyesült Államok (vélhetően a Colonial Pipeline támadás hatására is) a zsarolóvírus támadásokat a terrorizmushoz hasonló prioritással kezdte

[21] KOVÁCS (2018)
[22] NEMZETI KIBERVÉDELMI INTÉZET (2019)
[23] HAJDÚ (2020)

kezelni.[24] A fentiek alapján látható, hogy ez az eszköz több szempontból is alkalmas a terroristák számára. Egyrészt a befolyó váltságdíjakból biztosítható a működésük finanszírozása, másrészt a kritikus (információs) infrastruktúra támadásával, vagy az azzal való fenyegetéssel valóban kiválható a társadalomból a félelem, megvalósítható a zavarkeltés és a fenti sajnálatos példa igazolja, hogy emberélet kioltására is alkalmas lehet.

3.2.2. DoS, DDoS támadások (túlterheléses támadás)

A szolgáltatásmegtagadással járó támadás (Denial of Service vagy DoS), vagy más néven túlterheléses támadás, valamint az elosztott szolgáltatásmegtagadással járó támadás (Distributed Denial of Service, DDoS) célja bizonyos informatikai szolgáltatások teljes, vagy részleges megbénítása. DoS támadás eseten egy (jellemzően erős) támadó vesz részt a folyamatban, a DDoS támadásokat pedig egy hálózat gépei hajtják végre. A folyamat célja, hogy az adott eszközt, szolgáltatást a használatára feljogosított felhasználó ne tudja elérni, igénybe venni. Ilyen lehet, ha például egy elektronikus választási rendszerbe nem tudunk belépni, mert az oldal nem elérhető a választás napján, nem tudjuk használni a banki szolgáltatásokat, mert az oldal nem tölt be, vagy például nem tudjuk időben beadni az adóbevallásunkat, mert az erre szolgáló weboldal a határidő napján nem elérhető. Jól látható, hogy amennyiben a támadás zsarolással is kiegészül (váltságdíj fejében a terroristák beszüntetik a támadást), úgy ez a módszer is alkalmas a terrorfinanszírozásra, valamint még inkább megfelel például az államba vetett bizalom gyengítésére. Kritikus információs rendszerek támadása esetén pedig ez is alkalmas lehet az élet kioltására.

3.2.3. Wiper (törlő) kártevők

Az úgynevezett „wiper” (magyarul: törlő) kártevők a ransomware-hez hasonló módon viselkednek, de a titkosítás helyett törlik a fájlokat. Ebből fakadóan ilyen esetekben nem kínálnak helyreállítási lehetőséget és nem is kérnek váltságdíjat; a cél a pusztítás. Ezeket a rosszindulatú programokat a 2010-es évek elején kezdték el használni az iráni és szaúdi olajtársaságok, energiaipari cégek elleni támadásokhoz. 2017-ben több országban (leginkább Ukrajnában) megfertőzte a számítógépeket a Petya ransomware egy változata, amelyet úgy módosítottak, hogy az adatok egy részét titkosítsa, a többit viszont törölje. További érdekessége, hogy bár továbbra is váltságdíjat követelt, a kód módosítása miatt valójában nem volt lehetőség a fájlok visszaállítására még akkor sem, ha a kért összeget sikeresen megfizették. 2022 elején az ukrán-orosz konfliktus során ismét a wiper kártevők számos változatát fedezték fel az Ukrajnához köthető számítógépes rendszereken, jelentősen eltérő

[24] BING (2021)

kódstruktúrával, ami azt sugallja, hogy külön erre az alkalomra hozták létre őket különböző vélhetően államilag támogatott szereplők.

3.2.4. Website defacement (honlaprongálás)

A honlaprongálásos támadás során a támadók hozzáférnek a weboldalt futtató szerverhez és azon található fájlokat törlik, módosítják. Ennek során jellemzően a nyitóoldalt a saját tartalmukra módosítják, amin különböző üzeneteket, ideológiai mondanivalót tesznek közzé. Ilyen támadásra hazánkban is többször volt már példa. [25]

A fenti rövid ismertető után fontos kitérni arra, hogy az így létrehozott kiberfegyverek használatuk után nem tűnnek el. Működésük megismerése után módosíthatóak és újra felhasználhatóak. További gondot jelenthet, ha az eszközök egy hibás módosítási kísérlet után önálló életre kelnek, vagy ha egyszerűen csak rossz kezekbe kerülnek. Hasonló történt például a Stuxnettel is: a kódja, illetve annak egyes részletei elterjedtek a számítógépes bűnözők és hackerek között szerte a világon. Jelenleg nehéz megállapítani, hogy a nem állami támogatású csoportok képesek-e hatékonyan módosítani a kiberfegyverek kódjait, ugyanakkor rendkívül kézenfekvő megoldás lenne számukra, így a jövőben mindenképpen számolni kell ezzel a lehetőséggel is.

Hasonló a helyzet a hacktivisták eszközeivel is. „Az egyik korai, de pont emiatt az egyik legnagyobb visszhangot kiváltó kiberfegyver a már ismertetett Anonymous hacktivistacsoporthoz köthető. Az Anonymous a Wikileaks támogatása érdekében vetette be ezt a fegyvert 2010-ben, amikor a kiszivárogtatások miatt több pénzügyi szolgáltató – köztük a PayPal és a Mastercard – zárolta a Wikileaks számláit. Ezeket a támadásokat az Anonymous egy nem túl kifinomult, de annál hatásosabb fegyverrel, az úgynevezett Low Orbit Ion Cannon szoftver segítségével valósította meg, amely: tömeges DDoS-támadást idéz elő, azaz a nyers erőt használja a briliáns programozói megoldások helyett. Maga a program nyilvánosan elérhető és bárki által letölthető az internetről, azóta, hogy megalkotója – a Praetox Technologies – 2008 év végén […] a Project Chanology akció után közzétette.”[26] Az ukrajnai orosz invázió kapcsán szintén több csoport jött létre, melyek különböző támadásokat szerveznek és az ezekhez való csatlakozásra biztatják a szimpatizánsaikat. A felhasznált eszközök működése, a cselekmények valós célja azonban az átlagos felhasználók számára gyakran nem látható, illetve a biztosított eszköz paramétereinek módosítása után más célokra is felhasználható.

[25] INDEX (2006); SZABOLCSHÍR (2017)
[26] KOVÁCS (2018)

4. A KRITIKUS INFRASTRUKTRA ELLEN INTÉZETT (KIBER)TERRORTÁMADÁSOK

„Az információs társadalom ideghálózatának is tekinthető kritikus információs infrastruktúrák ellenei támadások előkészítése, megszervezése és végrehajtása – a kibertérben végrehajtott műveletek keretében – rendkívül összetett és összehangolt tevékenységet feltételez, mely alatt egyrészt technikai, másrészt pedig humán oldali összetevőket kell érteni. Ebből következik, hogy a kibertámadók az akcióik sikeressége érdekében az alábbiakra építhetnek:

- az információs infrastruktúrát alkotó elemek, részegységek műszaki hibáira, sérülékenységére;
- az adminisztrációs, fizikai, logikai és elektronikai védelem gyengeségeire;
- a védelmi intézkedések elhanyagolására;
- valamint a rendszerben foglalkoztatott humánerőforrások jelentette kockázatokra."[27]

Az alábbi fejezetben néhány olyan kibertámadást mutatok be, melyek a kritikus (információs) infrastruktúra ellen irányultak és a médián, vagy az okozott hatásain keresztül széles társadalmi rétegekhez jutott el. A rövid elemzések célja, hogy megismerjük a ténylegesen alkalmazott módszereket, eszközöket, valamint, hogy az eddigi ismeretek és információk alapján kísérletet tegyek a cselekmény pontosabb bekategorizálására, elsősorban abban a tekintetben, hogy nevezhetjük-e őket kiberterrorista támadásnak.

2007-ben egy akkor 14 éves lengyel tinédzser, Adam Dabrowski a kíváncsiságtól hajtva elkezdte tanulmányozni szülővárosa, a lengyelországi Lodz közúti villamos vasút hálózatának működését. Hónapokig tartó online kutatással és az iskolai elektronikai szakkörön szerzett tudásával 2008 elején sikerült átalakítania egy tévétávirányítót, úgy, hogy azzal vezérelni is tudta a villamosok váltóit. A fiú ki is használta ezt a képességét, mely eredményeként négy szerelvény siklott ki és tizenkét személy sérült meg.[28]

A célpont a kritikus infrastruktúra volt, a támadás eszköze belefér a tágabb értelemben vett kibertér fogalmába, a cselekménye okán emberek sérültek meg és vélhetően a félelem és zavarkeltés is megvalósult. Teljesen hiányzik azonban a politikai, ideológiai motiváció, valamint az ehhez kapcsolódó követelések megfogalmazása is. Látható, hogy egy meggondolatlan diákcsíny és egy kiberterror támadás mennyire hasonló lehet jellemzőiben,

[27] PAPP (2018)
[28] DINGODY (2008)

azonban úgy gondolom, hogy ebben az esetben nem kifejezetten merült fel bárkiben is, hogy az utóbbi elkövetésével gyanúsítsa meg az iskolás fiút.

2010 őszén a sajtó a Stuxnettől volt hangos (2. ábra). Egy olyan kártevőről érkeztek a hírek, ami nem az átlagos, otthoni felhasználókat vette célba, hanem egy ipari létesítmény vezérlő szoftvereit támadta.

2. ábra: *Stuxnet megjelenés a médiában.*
Forrás: Kovács – Sipos (2010).

A későbbi elemzések során bebizonyosodott, hogy még ennél is konkrétabb célpontja volt, ugyanis a Simatic WinCC SCADA-kat kereste, melyek az iráni urándúsító centrifugák vezérlését végezték. A rosszindulatú szoftver működése során az IR–1-es centrifuga fordulatszámát emelte meg rövidebb fázisokra annyival, hogy azok meghibásodjanak, ezzel lényegében sikeresen szabotálva az iráni atomprogramot és egyben új fejezetet nyitva a kiberhadviselésben. Ismét a kritikus infrastruktúra került tehát célkeresztbe, valamint a fizikai pusztítás is adott volt. Mégsem nevezhetjük az eseményt kiberterror támadásnak. A Stuxnet célja az volt, hogy megzavarja és szabotálja az iráni kormány nukleáris programját. Nem fenyegettek meg további dúsító üzemeket, vagy államokat, hogy hagyjanak fel a tevékenységükkel, sem pedig a lakosságot, hogy ne használjanak atomenergiából származó áramot. A támadás célzott volt és mint később kvázi kiderült állami szereplő(k) állt(ak) mögötte. Könnyen elképzelhető, hogy amennyiben a kibertérben elkövetett támadás nem jár

eredménnyel, akkor izraeli részéről egy jóval konvencionálisabb, az Opera-hadműveletthez[29] hasonló akció következett volna.

„2021. április 29-én a DarkSide bűnszervezet hackerei megtámadták a Colonial Pipeline vállalatot, amely az Egyesült Államok legnagyobb üzemanyag-vezetékét üzemelteti, és a keleti parton felhasznált üzemanyag körülbelül 45%-át szállítja. Ennek eredményeként a vállalat ideiglenesen leállította teljes hálózatát, ami súlyos üzemanyaghiányhoz és a gázárak megugrásához vezetett."[30] A támadás hozzávetőleg 50 millió embert érintett, a helyreállítás több mint két hétig tartott és mindemellett 4,4 millió dollár váltságdíj megfizetése kellett hozzá.

Az esemény igen komoly zavart és vélhetően félelmet is okozott a társadalomban, kritikus infrastruktúra ellen irányult, ugyanakkor az elkövetői vélhetően nem terroristák voltak, hiszen a támadást egy ismert kiberbűnözői csoporthoz tudták kötni és semmilyen politikai, ideológiai cél nem jelent meg, kizárólag a nyereségvágy.

Az ismertetett támadások minden esetben fizikai károkat okoztak, illetve a kritikus infrastruktúrát értek, azonban egyik sem tartalmazta a kiberterrorizmus összes jellemzőjét. Ezeket a kibertámadásokat az elkövetői körön kívül elsősorban az különbözteti meg a kiberterrorizmustól, hogy a terrorizmus erőszakának eredendően drámai célja van, azaz félelmet, rettegést és zavart kelteni egy szélesebb közönségben, vagy a teljes társadalomban, ez pedig egyik esetben sem volt cél. Ugyancsak fontos tényező, hogy egyik támadást sem kísérték nyilvános bejelentések, vagy hangzatos felelősségvállalás az elkövetők részéről, akik utána további támadásokkal fenyegetőztek volna, pedig az ilyen nyilatkozatok még megfélemlítőbbé tették volna a támadásokat, ha ez lett volna a támadók célja.

5. A VÉDEKEZÉS LEHETŐSÉGEI

A kibertámadások elkövetőinek és a támadásokhoz felhasznált eszközeik megismerése után mindenképpen szükséges a védekezés lehetőségeit is áttekinteni.

5.1. A POTENCIÁLIS CÉLPONTOK FELADATAI

Ezen területen a potenciális célpontok védekezésének alapja egy komplex információbiztonsági irányítási rendszer (a továbbiakban: IBIR) kiépítése lehet. Ennek célja az, hogy lényegesen megnehezítse, vagy akár el is lehetetlenítse a támadások jelentős részét. Egy jogszabályoknak, vagy egyéb információbiztonsági szabványoknak (pl.: ISO 27000-es

[29] MILITAVIA (2021)
[30] MWT SOLUTIONS (2021)

család) megfelelően, helyesen kiépített, üzemeltetett, auditált IBIR-rel megelőzhető lett volna az elmúlt évek információbiztonsági incidenseinek túlnyomó többsége. A fentiek mellett az eddiginél is nagyobb hangsúlyt szükséges a tudatosításra fektetni, hiszen a terület komplexitása és a fejlődés üteme valóban roppantul megnehezíti egy átlagos felhasználó számára a biztonságtudatos viselkedést a munkavégzése során.

Ugyancsak javasolt lenne, hogy a kritikus információs rendszerek és a kritikus infrastruktúra kialakítása során már a tervezés fázisában megjelenjenek az információbiztonsági szempontok és igények, hiszen az elmúlt 20 év tapasztalatai alapján a későbbiekben sok esetben csak az eredeti fejlesztés teljes költségével összemérhető ráfordítás árán érhető el a kívánt biztonsági szint, ha egyáltalán elérhető. A javítást ilyen esetekben jellemzően tovább nehezíti a sokszor előforduló forráshiány is.

A hatóságokkal történő együttműködés szintén fejlesztendő terület lehet. A támadási vektorok tanulmányozása és megosztása lehetővé tenné a további célpontok számára a védekezésre történő felkészülést és így adott esetben a támadás meghiúsítását is.

5.2. HATÓSÁGI FELADATOK

Természetesen a potenciális célpontok mellett az államnak, illetve a hatóságoknak is kiemelt szerepe van a védekezés során. A hard módszerek tekintetében ez jelenthet egy a jelenleginél sokkal erősebb támogatást, valamint akár kontrollt a kritikus infrastruktúra tekintetében. Jól látható azonban, hogy az előremutató és korszakukat megelőző intézkedések mellett (mint például az Ibtv. életre hívása) legalább ennyire fontos lenne a védelem kiépítéséhez szükséges források (legalább részleges) biztosítása, vagy bizonyos védelmi képességek szolgáltatásként történő nyújtása a kritikus (információs) infrastruktúra számára. A jövőben bizonyosan jelentősebb erőforrásokat kell allokálni annak érdekében, hogy felderítésre kerüljenek és a lehetőségekhez képest nyomon követhetőek legyenek a nem állami szereplők által felhasznált rosszindulatú kódok, kiberfegyverek.

Szükségesnek tartom kiemelni, hogy ezek a tevékenységek a kibertér jellegénél fogva nem feltétlenül történhetnek meg csak nemzeti szinten, így a nemzetközi, vagy akár a globális összefogás elengedhetetlen a kiberbiztonság megteremtése, vagy legalább növelése érdekében. A fenti megközelítés helyességét bizonyítja, hogy Európa a NIS 2 (Network and In-formation Systems Directive) keretében arra törekszik, hogy egy egységes szintet állapítson meg a fontosabb információbiztonsági elvárások tekintetében, annak érdekében, hogy a nemzetállamok szintjén ne legyenek lényeges eltérések a védelem alapkérdéseiben. Az Európai Unió által alapított számos információbiztonsággal foglalkozó szervet közül az

ENISA (European Network and Information Security Agency) az egyik legfontosabb ezen a téren, mely tanácsadó ügynökségként különféle ajánlásokkal, eljárásrendekkel segíti a tagállamokat a saját információbiztonsági szabályozásuk kialakításában.

Kifejezetten előremutató irányt jelent a tanulmány készítése során társadalmi egyeztetésen lévő, Magyarország kiberbiztonságáról szóló törvénytervezet, mely egységesíti a kibertámadások elleni védelem jogi szabályozását és összhangba hozza azt az európai uniós jogi keretrendszerrel. Emellett egy új, hatékony védelmi struktúrát alakít ki, amely egyszerűsíti az állami információs rendszerek védelmét, miközben iránymutatást nyújt a piaci szereplők számára is.

6. ÖSSZEGZÉS, KÖVETKEZTETÉSEK

A fentiek alapján kijelenthetjük, hogy a kritikus információs infrastruktúrák ideális célpontjai lehetnek egy terrorista támadásnak. Sikeres támadásuk bizonyosan jelentős hatással járna a társadalom számottevő részére nézve, valamint a terrorizmus egyik lényegi elemét jelentő zavar- és félelemkeltés is megvalósulhat.

Különösen súlyos következményekkel járna egy összehangolt, a célpontok körültekintő kiválasztásával megvalósított támadás. Ebben az esetben számolni kell a hatásalapú műveletek lényegével, miszerint első csapással törvényszerűen további közvetett károsító hatásokat lehet elérni, amely a teljes rendszerre negatív hatást fejt ki. Ennek oka az infokommunikációs rendszerek közötti interdependencia, ahol a különböző létfontosságú infrastruktúrák – például a távközlési hálózatok és az energiahálózatok – kölcsönös függőségi viszonyban állnak. Ebből fakadóan egy rendszer működésének zavarai más rendszerekben is súlyos következményeket okozhatnak, azaz a támadások nemcsak közvetlen hatásokat váltanak ki, hanem tovagyűrűző másodlagos, harmadlagos és akár további szintű hatásokkal is járhatnak, amelyek a teljes hálózat működését veszélyeztetik.

A korábbi, nem feltétlenül kiberterror támadások során használt eszközök, megoldások (bizonyos esetekben különösebb szakértelem nélkül) újra felhasználhatóak, továbbá felnövőben van egy olyan generáció mely a kibertérben elérhető eszközöket lényegében születése óta készségszinten használja.

Ezek alapján kijelenthetjük, hogy napjainkra jelentős veszélyt jelent a kritikus információs infrastruktúrák elleni kiberterrortámadások lehetősége, mely a hagyományos, fizikai térben végrehajtott terrortámadásokkal kombinálva eddig nem látott hatásokat érhet el. A kibertérben

folytatott terrorizmus belátható időn belül egyenértékűvé válhat a nehezebben kivitelezhető és csak lokális eredményekkel kecsegtető „hagyományos” fegyveres támadásokkal.

FELHASZNÁLT IRODALOM

2021. évi XCI. törvény a nemzeti adatvagyonról.

BING, Christopher (2021): *Exclusive: U.S. to give ransomware hacks similar priority as terrorism*. Online: https://www.reuters.com/technology/exclusive-us-give-ransomware-hacks-similar-priority-terrorism-official-says-2021-06-03/

BŐCZNÉ Neparáczki Anna Viktória (2020): A kiberterrorizmus büntető anyagi jogi megítélése. *Ügyészek Lapja*, 22(1), 71–85. Online: https://ugyeszeklapja.hu/?tag=boczne-neparaczki-anna-viktoria

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (2021): *Guidance on the Essential Critical Infrastructure Workforce*. Version 4.1. Washington, D.C.: U.S. Department of Homeland Security. Online: https://www.cisa.gov/resources-tools/resources/guidance-essential-critical-infrastructure-workforce

DINGODY (2008): *Metro: Genius boy takes over city's trams*. Online: https://wrongplanet.net/forums/viewtopic.php/feed.php?f=21&t=53881

EURÓPAI BIZOTTSÁG (2005): *Green Paper on a European Programme for Critical Infrastructure Protection.com* (2005) 576 final. Online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52005DC0576

HAIG Zsolt – KOVÁCS László (2012): *Kritikus infrastruktúrák és kritikus információs infrastruktúrák*. Budapest: Nemzeti Közszolgálati Egyetem. Online: https://www.uni-nke.hu/document/uni-nke-hu/kritikus_infrastrukturak.pdf

HAIG Zsolt (2007): Az információs társadalmat fenyegető információalapú veszélyforrások. *Hadtudomány*, 17(3), 37-56. Online: https://tudasportal.uni-nke.hu/xmlui/bitstream/handle/20.500.12944/2201/hadtud_2007_3_haig.pdf

HAJDÚ Gábor (2020): *Halálos áldozattal járt a kórházat ért zsarolóvírusos támadás*. Online: https://www.pcwplus.hu/pcwlite/halalos-aldozattal-jart-a-korhazat-ert-zsarolovirusos-tamadas-284552.html

INDEX (2006): *Eger közelében a török hekkerek*. Online: https://index.hu/tech/biztonsag/hax0215/

KOVÁCS László – SIPOS Marianna (2010): A Stuxnet és ami mögötte van: Tények és a cyberháború hajnala. *Hadmérnök*, 5(4), 163–172. Online: https://hadmernok.hu/2010_4_kovacs_sipos.pdf

KOVÁCS László (2018): *A kiberbiztonság stratégiai megközelítése*. MTA Doktori Értekezés. Nemzeti Közszolgálati Egyetem.

MILITAVIA (2021): *Opera Hadművelet – Izraeli légicsapás az iraki atomprogramon*. Online: https://militavia.blog.hu/2021/06/07/opera_hadmuvelet

MUHA Lajos – KRASZNAY Csaba (2022): *Az elektronikus információs rendszerek biztonságának menedzselése.* Budapest: Nemzeti Közszolgálati Egyetem, Online: http://hdl.handle.net/20.500.12944/18030

MWT SOLUTIONS (2021): *A Colonial Pipeline ransomware támadás*. Online: https://mwtsolutions.eu/hu/cikk/a-colonial-pipeline-ransomware-tamadas-leckek-a-kiberbiztonsagi-csapatok-szamara/

NEMZETI KIBERVÉDELMI INTÉZET (2019): *Zsarolóvírus (Ransomware)*. Online: https://nki.gov.hu/it-biztonsag/tudastar/zsarolovirus-ransomware-v2/

PAPP Zoltán István (2018): *A kiberterrorizmus módszerei, lehetséges eszközei és az ezek ellen történő védekezés alternatívái*. Doktori értekezés. Nemzeti Közszolgálati Egyetem, Katonai Műszaki Doktori Iskola.

PEW RESEARCH CENTER (2002): *One year later: September 11 and the Internet*. Online: https://www.pewresearch.org/internet/2002/09/05/one-year-later-september-11-and-the-internet-2/

PLOTNEK, Jordan J. – SLAY, Jill (2021): Cyber terrorism: A homogenized taxonomy and definition. *Computers & Security*, 102(2), Online: https://doi.org/10.1016/j.cose.2020.102145

SZABOLCSHÍR (2017): *Meghekkelték Nyíregyháza honlapját*. Online: https://szabolcsihir.hu/hir/meghekkeltek-nyiregyhaza-honlapjat

THE GUARDIAN (2021): *US invokes emergency powers after cyber-attack on fuel pipeline*. https://www.theguardian.com/us-news/2021/may/10/us-invokes-emergency-powers-after-cyberattack-shuts-crucial-fuel-pipeline

TURTON, William – MEHROTRA, Kartikay (2021): *Hackers Breached Colonial Pipeline Using Compromised Password*. Online: https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password?embedded-checkout=true

U.S. DEPARTMENT OF DEFENSE (2010): *Joint Publication 1–02: Department of Defense Dictionary of Military and Associated Terms*. Washington, DC: Joint Chiefs of Staff.

VÁRHEGYI István – MAKKAY Imre (2000): *Információs korszak, információs háború, biztonságkultúra*. Budapest: OMIKK.

VÁKÁT OLDAL

Jasenszky Nándor ny. r. ezredes

A hírszerzések együttműködése, különösen a hivatásos (állami) és az üzleti (magán) hírszerzés területén

1. BEVEZETÉS

A biztonság az egyének, az emberi közösségek, a különböző társadalmak egyik legrégibb igénye és vágya. Éppen ezért nem könnyű olyan meghatározást alkotni, amely minden korra és helyzetre érvényes és megkérdőjelezhetetlen. Ezt meg sem kísérelném, inkább arra törekszem, hogy a biztonság fejlődését egy folyamat részeként mutassam be.

Az emberi fejlődésben még csak csoportok vagy kisebb közösségek léteztek, amikor már megfogalmazódott az igény arra, hogy tudják merre jár a „táplálék", merre van az iható víz, és hogy lehet ezekhez hozzá jutni. Így lettek a vadászok, a nyomkeresők, nyomolvasók, akiket bizton tekinthetünk a mai hírszerzők őseinek.

A közösségi fejlődés, a társadalmak kialakulása nemhogy megőrizte, hanem egyre magasabb szintre emelte a közösségek információ igényét. Egyre szélesedett a paletta – az élelmiszer beszerzéstől, a termelésen, a gazdálkodáson át az egyén és közösség biztonságának szavatolásához vezető információk megszerzéséig. Egyre inkább vált önálló „szakmává" a hírszerzés, bár ekkor még a leggyakoribb megnevezésnek a kémet és a kémkedést tekinthetjük.

A hírszerzés gyökereit igazolandó, gyakran a világ második legrégebbi foglalkozásaként említik. Tény, hogy már a Bibliában is olvasható a „kémkedés" kifejezés. Emellett írásos dokumentumok számolnak be ókori birodalmak katonai hódításai előtt alkalmazott hírszerzési tevékenységről. Persze akkoriban még nem így hívták, de a tevékenység céljai hasonlóak voltak a mai hírszerzési munkához. Az egyik legrégebbi írásos forrás, amely tanulmányozza, elemzi és értékeli a hírszerzést az Szun Tzu legendás hírű kínai hadvezér könyve: The Art of War (A háború művészete). Ez a könyv több ezer évvel ezelőtt íródott, de a mai szerzők is előszeretettel idéznek a szerző megállapításaiból. A kínai generális nemcsak felismerte a hírszerzés fontosságát – amelyet az „előre tudás művészetének" nevezett –, hanem tanulmányozta az alkalmazási lehetőségeit is különböző helyzetekben.

A több évszázados fejlődés során a hírszerzés sokáig egységes tevékenységként volt értelmezhető. Természetesen a hatalom, a politika, az állam kiszolgálása, az egyre erősödő

katonai igények adtak egy belső szakosodást. Hosszú ideig a gazdasági, különösen az üzleti hírszerzés nem jelent meg önálló szakterületként. Ez természetesen nem azt jelentette, hogy találmány, termék, iparvédelem terén ne lettek volna kémkedési akciók, de szervezetszerű gazdasági hírszerzési és elhárítási tevékenységről a XX. század második feléig nem nagyon beszélhetünk.

Az embercsoportok, társadalmak biztonságigényét a korábban megtörtént, vagy folyamatosan jelen lévő, nem kívánatos veszélyes események megtörténte vagy történése váltja ki. A közösség igyekszik tenni azért, hogy a helyzet megváltozzon és a kívánatos rend helyreálljon. Ebből a cselekménysorból, az adott válaszokból alakult ki a védelem maga. A védelmi intézkedések a konkrét, azonnal kezelendő eseményekre adott direkt válaszok. Az ilyen jellegű, állandósuló feladatok hívták életre azokat a védelmi, nemzetvédelmi és rendvédelmi szervezeteket, amelyek hivatásszerűen foglalkoznak a problémák kezelésével. Ezektől a szakmai közösségektől elvárható volt, hogy ne csak az akkutan jelentkező nem kívánatos eseménnyel foglalkozzanak, hanem azt összefüggéseikben, rendszerben vizsgálják.

Ehhez arra volt szükség, hogy folyamatosan álljanak rendelkezésre, releváns, értékelhető adatok. Ez az igény hozta létre az önálló hírszerzéssel foglalkozó szervezeteket.

Nézzük meg, hogyan fogalmazza meg a Rendészettudományi Szaklexikon a hírszerzés fogalmát:

Hírszerzés: (1) politikai, katonai, gazdasági és más fontos → információk tervszerű gyűjtése nyílt és titkos eszközökkel, valamint módszerekkel. A ~ az → állam speciális funkciója, amelyet az e feladatra létrehozott speciális → szervezetek (szolgálatok, hivatalok) látnak el. (2) Leplezett vagy titkostevékenység, az ellenérdekelt félre vonatkozó, korábban saját erőink által nem ismert → adatok és információk megszerzésére. (3) A katonai felderítő szerveknek békében és háborúban, megszakítás nélkül, minden lehetőség felhasználásával folytatott tevékenysége az ellenséges vagy várhatóan ellenséges ország katonapolitikai helyzetére, hadigazdasági potenciáljára, fegyveres erőire, valamint a hadszínterekre vonatkozó adatok megszerzése és tanulmányozása céljából.

Jól látható, hogy ez a forrás csak az állam és annak hatóságait teszi szereplőjévé a hírszerzésnek.

A **hírszerzés** egy dinamikusan változó fogalom, amelynek nincs egyetlen meghatározott definíciója vagy alkalmazása. Viszont a folyamatosan végzett hírszerzési munka valódi célja, hogy biztosítson előnyt a döntéshozók számára. Ezt számtalan titkos szervezet, szolgálat a saját profiljának, feladatrendszerének megfelelően egészíti ki, illetve árnyalja, de a lényeg mit sem változik.

Vizsgáljuk meg, hogyan és miképpen jelenik meg ez az alapvetés a gazdasági, üzleti szférában:

Az **üzleti hírszerzés** a vállalat aktív és passzív gazdasági biztonságának (kialakításának és fenntartásának) eszköze stratégiai és operatív szinten egyaránt. Az üzleti hírszerzés a piaci környezet lehetőségeinek és fenyegetéseinek felismeréséhez, elemzéséhez és az e folyamatokhoz kapcsolódó döntések előkészítéséhez nyújt segítséget. Az üzleti hírszerzés modern vezetői, döntéshozói gondolkodást jelent a vállalat rugalmasságának növelése és a meglepetések, a kockázati tényezők iránti érzékenység csökkentése érdekében.

A mai globalizált világban, világgazdaságban elkerülhetetlen, hogy valamilyen szinten ne kerüljünk kapcsolatba az üzleti hírszerzéssel és persze az állami szolgálatokkal, az egyre fokozódó gazdasági hírszerzési igényeikből kifolyólag. Ebből a következtetésből egyértelműen látszik, hogy állami és üzleti hírszerzés együttműködésre van utalva. A gyakorlati megvalósulásáról és annak lehetséges formáiról a továbbiakban részletesebb információt nyújtunk.

Fontos résztvevőként kell tárgyalnunk a bűnügyi szolgálatokat, az általuk végzett felderítési tevékenységet és azon belül is **bűnügyi hírszerzést**.

A bűnüldözés egy rendkívül összetett jelenség és szerteágazó tevékenység. Természetes társadalmi igény, hogy az állam nyújtson biztonságot polgárainak, biztosítsa számukra életük, testi épségük és javaik védelmét, a bűncselekményeket derítse fel, az elkövetőket vonja felelősségre. A rendőrség, mint az állam által létrehozott szervezet a bűnüldözés területén meghatározó szerepet tölt be.

2. A TITKOS INFORMÁCIÓGYŰJTÉS - BŰNÜGYI HÍRSZERZÉS

Az államok bűnüldöző szervei a bűncselekmények felderítése érdekében ősidők óta alkalmaznak olyan leplezett személyeket, módszereket és eszközöket. Ezek segítségével a bűnüldöző tevékenységük egy részét titokban végzik. A bűnözés természetéből adódóan titokban zajló tevékenység, ezért az ellene való harcban is természetes a hasonlóan titkos módszerek felhasználása. A nemzetközi és hazai bűnüldözési tapasztalatok azt igazolják, hogy a bűnelkövetők cselekményük sikere és leplezése érdekében maguk is rendszeresen végeznek titkos információgyűjtést. A szervezett, országhatárokon átlépő bűnözés a tudomány és a technika legújabb vívmányait alkalmazza. Azonos vagy fejlettebb módszerek és eszközök hiánya a bűnözés számos területét a rendőrség számára hozzáférhetetlenné tenné, a bűncselekmények és elkövetőik jelentős hányadának felderítését hiúsítaná meg.

A titkos információszerzés, a bűnügyi hírszerzés a bűnüldözés fegyvertárának nemzetközileg is elismert és alkalmazott eleme. A bűnüldözés területén végzett titkos információgyűjtés, a bűnügyi hírszerzés fő szabály szerint részben eseménykövető. Emellett bizonyos csoportok, szervezett bűnözéssel kapcsolatba hozható személyek, hozzájuk köthető múltbéli események felderítésével, a bizonyítékok beszerzésével foglalkozik. Alapvető feladata, hogy bűn ne maradhasson felderítetlen és teljesüljön a társadalom azon jogos elvárása, hogy a bűnös felelősségre vonása történjen meg. A feladatköréből fakadóan a hírszerzések közötti együttműködésből inkább az akciószerű, műveleti tartalmúak a gyakoriak. Az egy bizonyos területhez, ágazathoz, objektumokhoz kötött hosszabb távú, stratégiai együttműködés kevésbé fordul elő. Az általuk biztosítandó területek, esetleges objektumok gyakrabban változnak, ami részben a szervezett bűnözés konjunktúraérzékenységével, továbbá a célszemélyi kör mobilitásával is magyarázható.

A bűnügyi szolgálatokkal történő együttműködés jellemzői általában: a konkrét feladatokhoz, személyekhez kötöttség, a szűkebb időtényező és adott esetben egy nyílt rendőri intézkedésben vagy büntetőeljárásban való részvétel esetleges igénye. Ebből fakad, hogy az együttműködés titkossága, a forrás(ok) védelme kiemelt figyelmet kell, hogy kapjon és így megfelelően fedett maradjon. Különösen speciális együttműködést és szakmai egyeztetést igényel az a feladat, amikor egy nemzetbiztonsági elhárítási területhez tartozó gazdasági szereplőnél – ahol saját üzleti hírszerzés is működik – a bűnügyi szolgálatnak bevezetést, beépülést vagy bármilyen fedett műveletet kell végrehajtania. Például: az energetikai szektor egyik stratégiai gyártelepén (MOL DUFI, Százhalombatta, 2005) végrehajtott, szervezett és folyamatos lopás megszakítása és felderítése ilyen együttműködést igényelt.

3. A BŰNÜGYI ÉS A NEMZETBIZTONSÁGI HÍRSZERZÉS, MINT A TERRORFELDERÍTÉS KULCSELEME

Az új ellenséggel szembeni küzdelem új felderítési és elhárítási stratégiát és taktikát, erőket és eszközöket, módszereket igényelt. Nem elhanyagolható szempont, hogy megváltozott az időtényező szerepe. A biztonság veszélyeztetése továbbra is stratégiai perspektívába helyezte a fenyegetéseket. Ugyanakkor a hidegháborús kémjátszmákra jellemző, évtizedekre előre gondolkodó tervezési-szervezési szemléletet felváltotta – vagy inkább kiegészítette – az azonnali reagálás igénye. A válságkezelés, a megszakítás, az elhárítás és a megelőzés parancsoló, jelen idejű szükségletté vált. Az agresszív, türelmetlen, offenzív beállítottságú, az állampolgárok életét közvetlenül veszélyeztető, váratlan – de

bármikor bekövetkezhető – terrorcselekményekre leplezetten készülő ellenséggel szemben csak hasonló jellegű és intenzitású ellenintézkedésekkel lehet felvenni a harcot.

A terrorizmus elleni küzdelemben a hagyományos katonai vagy rendőri módszerek korlátozott hatékonyságúnak bizonyulnak. A bűnüldöző szemlélettel szemben itt már nem egyértelmű és mindenekfelett álló igényként jelenik meg a törvény elé állítás, a büntetéskiszabás illetve -végrehajtás követelménye. Nem minden esetben célszerű a büntetőeljárási jog szabályainak megfelelően lezárni az ügyet. Előfordulhat, hogy az elkövető szabadlábon hagyása, rejtett megfigyelése, félrevezetése vagy manipulálása révén a nemzetbiztonsági szolgálatok még veszélyesebb potenciális elkövetőkhöz juthatnak el, meghiúsíthatnak egy újabb, pusztítóbb terrorcselekményt, vagy akár egy egész terrorszervezetet is felszámolhatnak. Hasonlít ez a szervezett bűnözés elleni fellépés módszertanához, amely már nem kizárólag és nem is elsősorban a bűnelkövetőt, hanem a mögötte álló szervezetet veszi célba. A szervezettség ugyanis olyan „erősokszorozó" tényező, amely az elkövetői csoportot – ha az szembehelyezkedik a társadalommal és annak alapértékeit veszélyezteti – valósággal „idegen hatalommá" avatja, és a nemzetbiztonsági szolgálatok, valamint a különleges rendeltetésű rendőri szervek hatáskörébe utalja.

„Tisztán kell látni, hogy szervezett bűnözés ellen csak a megfelelő szervezeti, személyi és technikai feltételek biztosításával, azok koncentrált igénybevételével lehet a kívánalmaknak, elvárásoknak megfelelő eredményes, offenzív bűnüldöző tevékenységet végezni."[1] Ez az igény 1986-ban már testet öltött, de megelőzte korát, mert a szervezett bűnözés elismerésére is várni kellett még 4–5 évet nem beszélve az offenzív információ szerzésről.

Mindhárom szakterületen – a bűnüldözésben, a nemzetbiztonságban és a terrorelhárításban – egyértelműen előtérbe kerül a minőségi és offenzív információszerzés, nevén nevezve: a hírszerzés. Ebben a megközelítésben itt a hírszerzés – mint titkos információgyűjtés – nem cél, hanem eszköz. Nagyon fontos, hogy tisztán lássuk, hogy a terrorfelderítés senkinek sem a kizárólagos „birtoka". Régen sem volt az, de napjainkban már végképp nem. Ezt többen vitatják, igyekeznek ezt a tevékenységet kizárólagosan titkosszolgálati munkának beállítani. Egyes vélemények szerint a különleges eszközök és módszerek kizárólag a titkosszolgálatokhoz köthetők, mivel csak ott áll rendelkezésre a szükséges szakértelem. Ez finoman fogalmazva – téves megközelítés és következtetés. Nélkülözi a jelenlegi, sőt a korábbi helyzet ismeretét.

A terrorfelderítés területén sajátos kettősség uralkodik:

[1] JASENSZKY (1987)

1) A terrorszervezetek, azok vezetőinek és irányítóinak kiléte, általános célkitűzéseik, stratégiájuk, taktikájuk, finanszírozásuk, a toborzási módszereik felderítéséhez igényelt munka közelebb áll a klasszikus *titkosszolgálati munkához.*
2) A tervezett, konkrét terrorcselekmények megelőzése, megszakítása, felderítése, a csoportok feltérképezése, bomlasztása, felszámolása, az általuk elkövetett bűncselekmények operatív szakban történő bizonyítása, az abban részt vevő személyek törvény elé állítása, a büntetőeljárások előkészítése kifejezetten a *szervezett bűnözés elleni felderítő tevékenység* jellemzőit mutatja.

Természetesen a nemzetbiztonsági és a bűnügyi titkos felderítések metodikája között sok a hasonlóság, ám céljaikban minden hasonlóság mellett is van egy lényeges különbség: a szervezett bűnözés elleni küzdelemben a cél a mélyen konspirált csoportok és személyek bűnös tevékenységének *felderítése és bizonyítása.* A terrorizmus elleni küzdelemben a cél: a mélyen konspirált csoportok és személyek bűnös tevékenységének *felderítése és elhárítása.*

A célok elvi különbözősége (bizonyítékok megszerzése a büntető eljáráshoz vagy információszerzés az elhárítás érdekében) visszatükröződik a titkos információgyűjtés végrehajtásának társadalmi, jogi és politikai feltételrendszerében is. A külső engedélyhez kötött eszközök alkalmazását bűnüldözési cél esetében bíró, nemzetbiztonsági cél esetében az igazságügy miniszter engedélyezi.

Egyértelmű alapvetésként leszögezhetjük, hogy az érintett szervezetek az eredményes és alapos információszerzés és felderítés érdekében egymásra vannak utalva. Ha elfogadjuk, hogy az információigények – legyenek azok állami titkosszolgálati, bűnüldözési vagy üzleti jellegűek – szétterülnek és beleágyazódnak a társadalom teljes rendszerébe, akkor világossá válik: az érintett szervezeteknek együtt kell működniük. A különböző szereplők általános feladataikból adódóan jellemzően bizonyos területekre koncentrálják hírszerző kapacitásaikat. Egy-egy szervezettől nem várható el, hogy lefedje az esetleges igényként megjelenő teljes területet. Ez egyszerűen lehetetlen, továbbá cél- és ésszerűtlen. Meg kell találni azt a partner szervezetet, szolgálatot, amely az általunk érdekelt területen a legjobb pozíciókkal, forrásokkal és lehetőségekkel rendelkezik. Természetesen bizonyos esetekben a forrás és a saját érdekek védelme kereteket és határokat szabnak az együttműködés mélységének, de főszabályként fogadjuk el az együttgondolkodás lehetőségét és szükségességét. Kerüljük az indokolatlan titokzatoskodás misztériumjátékát. Nem emeli az ázsiónkat, viszont ellehetetlenítheti az érdemi együttműködést.

Ennek a gondolatiságnak a terjedéséhez, elmélyítéséhez át kell értékelni (tapasztalataim és véleményem szerint) a korábbi, sok esetben több évtizedes megszokásainkat, szakmainak ítélt

fő „ökölszabályainkat”. Számoljunk le és lehetőleg ne adjunk kontroll nélkül további teret – a szakmai sovinizmusra oly jellemző – a „magasabb érdekeknek”, a bizonyos szervezetek nevéből adódó feltétlen elsőbbségnek, és főleg ne a „kizárólagos igazságoknak”, amelyek egyetlen alapja adott esetben az, hogy ők mondják.

Törekedjünk egymás munkájának a kölcsönös megismerésére, fontosságának elismerésére. Az együttműködés emberi alapja mindig legyen a:

- tisztelet, tisztesség;
- megbecsülés;
- szakmai alázat;
- közös érdek;
- egyenrangúság;
- korrektség;
- kölcsönösség.

Ezek a fogalmak – véleményem szerint – nem igényelnek külön magyarázatot. Közel 50 év munka tapasztalata mondatja velem, hogy az együttműködések az emberi kapcsolatok így működnek jól és hatékonyan.

Az együttműködési szabályokat a szakterületi előírások meghatározzák, és természetesen ezek irányadóak. Ennek az anyagnak nem feladata, hogy a szakterületi szabályokat a teljesség igényével ismertesse.

Célom a gyakorlati végrehajtás elveinek összegyűjtése és megosztása volt, mivel ezekhez való igazodás határozza meg a megvalósítás sikerét. Az együttműködésbe vont szereplők közül vizsgáljuk meg egy kicsit az indokolatlanul és méltánytalanul megítélt „szegény rokont”.

Amennyiben felidézzük az üzleti hírszerzés korábban idézett fogalmát azt tapasztalhatjuk, hogy a meghatározásban olyan kulcsszavak szerepelnek, mint gazdasági biztonság, piaci lehetőség és fenyegetettség, döntés-előkészítés, vezetői gondolkodás. Ezek a kifejezések kiragadva a definícióból, átültetve más szövegkörnyezetbe egy vállalat fejlődésének, piaci szereplésének, gazdaságos üzemelésének, nyereségességének feltételeit is jellemezhetik. Valóban szoros az összefüggés. Napjainkban az üzleti hírszerzés a globális piacon egyet jelent a fenti kondíciókkal.

A meghatározásnak egyik központi eleme a modern vezetői, döntéshozói gondolkodás kialakítása. A mai piaci versenyben egy vállalat sikerét vagy kudarcát nem a gazdasági adottságaiban, körülményeiben kell keresni elsősorban, hanem a döntéshozók attitűdjében, a piaci versenyhez, szerepléshez való hozzáállásában.

Tételezzük fel, hogy ugyanazon a piacon – földrajzi és ágazati szempontból egyaránt – a piacvezető két-három vállalat mögött tucatnyi szereplő küzd a középmezőnyben, és várhatóan további két-három új vállalkozás próbál betörni ugyanerre a piacra. Mind az élvonalat, mind a középmezőnyt képviselő cégek a kategóriájukon belül megközelítőleg azonos képességekkel, lehetőségekkel, pénzügyi háttérrel, kapacitással, technológiával és technikával rendelkeznek. A cél minden esetben a nyereségesség, a növekedés, a piaci részesedés növelése, a terjeszkedés. De vajon hogyan sikerül ezeket a célokat megvalósítani, mi fogja őket a céljaik eléréséhez hozzásegíteni? Úgy is feltehetnénk a kérdést: mi az, amit kihasználhatnak, hogy a versenyben eredményesek legyenek, mi az a hatékony eszköz, ami megkülönbözteti majd egyiket a másiktól?

Ahhoz, hogy megválaszolhassuk a kérdést, azt is ismerni kell, milyen kihívásokkal néz szembe a mai piaci versenyben egy vállalat.

Ezek a kihívások a következők lehetnek:

- A konkurencia aktivitása.
- Az ágazat meghatározó szereplőinek üzleti politikája.
- A beszállítók és vásárlók árpolitikája, ár alku pozíciója.
- Más ágazatok folyamatainak hatása.
- A környezeti tényezők – piaci, szociális, jogi, gazdasági szabályzási rendszerek – változása, módosulása.
- Nemzetközi gazdasági folyamatok.
- Nemzetközi – kormányközi és nem kormányközi – szervezetek aktivitása.
- Nemzetközi politikai folyamatok.

(Ha elemezzük a felsorolt kihívásokat, meg kell állapítanunk, hogy ezek az állam szintjén is jelen lévő stratégiai kérdések, így folyamatos hírigényként fogalmazódnak meg az állami szolgálatok irányába is.)

Csoportosítva a kihívásokat, két fő kérdéskörben érdemes őket megvizsgálni, az ágazati és konkurencia-összefüggéseket, valamint a környezeti tényezőket és változásaik jellemzőit. Ezekre kell a vállalat vezetésének reagálnia. A környezeti tényezők változásai, valamint az ágazati és versenytársi folyamatok fogják azokat a lehetőségeket és/vagy fenyegetéseket felvetni, melyek meglepetésként érhetik a vállalatokat. Emiatt a rájuk történő reagálásnak nagy lehet a kockázata. A mai menedzserek két kritikus kérdéssel találják szemben magukat ezzel a témával kapcsolatban:

1) Képesek-e ellenállni annak a kísértésnek, hogy a közelmúlt – akár a jelen – trendjeire, folyamataira építsék következő stratégiájukat?

2) Képesek-e megtalálni a jövő trendjeinek, folyamatainak indikátorait, és így felmérni azok irányát és hatásait?

A döntéshozónak mindkét kérdésre választ kell adnia, felismerve, hogy ezek szorosan összefüggenek. Ezek megválaszolása az első lépés a kihívások azonosítása felé. Az a vezető, aki minkét kérdésre igennel válaszolt, nagy valószínűséggel alkalmazza az üzleti hírszerzés valamilyen formáját.

Azért fogalmaztunk így, mert bár a magyar nyelv ezt nem fejezi ki igazán, az angol szakirodalom az üzleti hírszerzés több változatát, fajtáját tárgyalja. Ilyenek például:

- *Strategic intelligence for businesses* – stratégiai hírszerzés vállalatoknál;
- *Competitive intelligence* – üzleti hírszerzés, amely a piaci versenyre koncentrál;
- *Competitor intelligence* – üzleti hírszerzés, amely a versenytársakra koncentrál,
- *Business intelligence* – üzleti hírszerzés általában;
- *Corporate intelligence* – üzleti hírszerzés, amely kifejezetten a vállalati csúcsirányítás döntéshozatalát támogatja;
- *Benchmarking* – az üzleti hírszerzés egy szűkebb, összehasonlító formája.

Említésképpen csak: az üzleti hírszerzés egy másik speciális ága a *knowledge management*, amely, mint döntéshozási, döntéselőkészítési tevékenység érdemel figyelmet. A legelterjedtebb elnevezés azonban a *competitive intelligence*, amely alatt ma már az átfogó üzleti hírszerzési tevékenységet is értik.

A kihívásoknak való megfelelés szükségessé teszi az üzleti hírszerzés alkalmazását. Az azonos képességű és feltételekkel rendelkező cégek közül azok tudják céljaikat elérni és érvényesülni a piacon, amelyek képesek felismerni, értékelni és kezelni a jövő bizonytalansági tényezőit. Ehhez elengedhetetlen, hogy a vezető felmérje a kockázatokat, és azok ismeretében hozzon döntést. A már említett lehetőségek és fenyegetések a bizonytalansági tényezőkön kívül értékelendők. Vagyis míg a bizonytalansági faktort a gazdasági célok, a stratégia tervezésénél veszik figyelembe, a lehetőségek és veszélyhelyzetek a stratégia végrehajtása során merülnek fel. Mindkét kérdéskörre lehetséges a hatékony felkészülés az üzleti hírszerzés segítségével. Az első esetben a bizonytalansági faktort a kockázati elemek iránti érzékenység csökkentéséel érheti el egy vállalat. A második esetben a rugalmasság növelésével és korrekt ismeretekkel. A kulcs ezekhez minden esetben az információ, mégpedig az időben elemzett és ellenőrzött információ.

Az üzleti és állami hírszerzés és elhárítás közötti kapcsolatok többfélék lehetnek:

1. az egymást támogató, kölcsönös érdekeken alapuló együttműködés, amelyben:
   1.1. az állami szolgálatok támogatják a vállalati szervezeteket;

1.2. az üzleti szervezetek támogatják az állami szolgálatokat;

1.3. rendszeresen egyeztetett és kölcsönös az együttműködés.

2. az ellentétes érdekek alapján kialakuló és egymás ellen irányuló tevékenység, amely a gyakorlatban a következő módon jelenik meg:

2.1. az állami hírszerzés gyűjt adatot – általában külföldi – vállalatról, ahol az üzleti hírszerzés defenzív részlege védekezik az idegen állami hírszerzés akciója ellen;

2.2. az állami hírszerzés védelmet biztosít saját vállalatoknak idegen vállalatok üzleti hírszerző tevékenysége ellen, ahol az idegen vállalati és a védekező állami hírszerzés között léphet fel konfrontáció;

2.3. az üzleti hírszerzés folytat offenzív tevékenységet külföldön, hogy információt szerezzen a kormány gazdasági, kereskedelmi szándékairól, szabályzórendszerének változtatási szándékáról, amikor az állami hírszerzés az állami érdekeket védve lép fel az offenzív üzleti hírszerzés ellen.

Mint látható, az üzleti és állami hírszerzés között akár komoly együttműködés vagy ellenkezőleg, veszélyes konfrontáció alakulhat ki. Nyilván ezek a kapcsolatok nem egy közepes vagy kisvállalat információ szükséglete és az állami hírszerzés információ igénye között figyelhetők meg, hanem a transznacionális, multinacionális vállalatok és a nemzetgazdaság kapcsolatában.

Ha valakiben felmerül, hogy Magyarország esetében is érdemes-e ezzel a kérdéssel foglalkozni, a válasz határozott igen. Egyrészt Magyarországon is jelen vannak már a világ, a globális piac vezető multinacionális és transznacionális vállalatai. Másrészt az integrációs folyamatoknak köszönhetően hazánk EU[2] és NATO[3] tagsága is hatással bír a geopolitikai folyamatokra, régiónk gazdasági, kereskedelmi helyzetére.

A vállalati gazdasági biztonság nemzeti szinten része a nemzeti biztonságnak, míg vállalati szinten egyet jelent a vállalat létezésével. A kérdés az, hogy mikor és hogyan egyeztethető össze egy nemzeti és egy vállalati szinten jelentkező gazdasági biztonsági kérdés? Ha a két szintet hasonló célok motiválják – például egy vállalat üzleti céljai egyben a nemzetgazdaság érdekeit is szolgálják –, akkor a hírszerző és elhárító szervezetek közötti kapcsolat várhatóan együttműködő.

Ha viszont az érdekek ellentétesek, akár belföldi, akár nemzetközi szinten, a két szervezet valószínűleg egymással szemben fog tevékenykedni.

[2] Európai Unió.
[3] North Atlantic Treaty Organisation – Észak-atlanti Szerződés Szervezete.

Magyarországon a vállalatok – kivéve a multinacionális és transznacionális vállalatok magyarországi képviseleteit, leányvállalatait – nagyságuk, piaci jelentőségük miatt nem engedhetik meg maguknak önálló üzleti hírszerző vagy elhárító részleg kiépítését. A megoldás az ilyen feladatokra szakosodott konzultációs irodák felkérése. Ezek az irodák azért is érdekesek lehetnek, mert kényes helyzetben képesek a hivatalos állami hírszerzés és a vállalati érdekek között fennálló ellentéteket a megfelelő módon kezelni. Ilyen irodák sikerrel működnek számos országban.

Az állami és üzleti hírszerzés kapcsolatát vizsgálva azt is fontolóra kell venni, tulajdonképpen melyik hírszerzési forma a jelentősebb, befolyásosabb? Pontosabban: a mögöttük álló nemzeti gazdasági érdekek bírnak nagyobb jelentőséggel vagy a magántulajdont képviselő privát szféra gazdasági biztonsága a súlyosabb tényező? Természetesen a CIA[4], az NSA[5], az FBI[6] mint hírszerző és biztonsági szolgálatok, valamint az Egyesült Államok – USA[7]) gazdasága nem hasonlítható össze egyetlen transznacionális vállalattal – ebben az esetben eltérő nagyságrendekről van szó. Ugyanakkor léteznek azonban kisebb nemzetek, akár egyes régiók is, ahol transznacionális és multinacionális vállalatok komoly befolyással rendelkeznek. A gazdaság mára már olyan önálló hatalmi tényezővé vált, hogy könnyedén gyakorol nyomást egy adott ország nemzeti politikájára. Ez a folyamat olyan, biztonsági szempontból instabil helyzetet eredményezett, hogy bátran kijelenthetjük: egy adott ország, így Magyarország nemzetbiztonságát is legkönnyebben gazdasági érdekeinek csorbításával lehet veszélyeztetni.

Magyarország gazdaságbiztonságának megértéséhez szükséges, hogy megmagyarázzuk, mit jelent a nemzetgazdaság fogalma. A nemzetgazdaság alatt, mint biztonsági fogalom, azokat a stratégiai gazdasági ágakat értjük, melyek védelme szükséges ahhoz, hogy az ország gazdasági biztonsága semmilyen formában ne szenvedjen csorbát. Ezek közé a gazdasági ágazatok közé tartozik: közlekedés, kommunikációs technológia, az ország jelentősebb ipari komplexumai és bankjai, kutató és fejlesztési intézetek és az ország energia előállításáért felelős vegyipari és egyéb állami, illetve részben, vagy teljesen magánkézben lévő cégek. A nemzetgazdaság biztonsági fogalma magában foglalja az ország közép- és hosszú távú gazdasági stratégiájára vonatkozó információk védelmét is. Meg kell említenünk továbbá, hogy a gazdaságbiztonság alatt nemcsak azt értjük, hogy az adott ország nemzetgazdasága a lehetőségekhez mérten, védett a negatív külső és belső hatásoktól, hanem azt is, hogy az adott

[4] Central Intelligence Agency – Központi Hírszerző Ügynökség.
[5] National Security Agency – Nemzetbiztonsági Ügynökség.
[6] Federal Bureau of Investigation – Szövetségi Nyomozóiroda.
[7] United States of America – Amerikai Egyesült Államok.

ország érdekeit korlátozás nélkül tudja kifejteni úgy külföldön, mint belföldön egyaránt. Vagyis a gazdaságbiztonság fogalma nemcsak állapot, hanem az arra vonatkozó tevékenységet is magában foglalja.

Napjaink gazdasági viszonyai mind az államok, mind a vállalatok részéről olyan stratégiát várnak el, mely alapvetően az információk birtoklására épül. Nap mint nap olyan kihívások érik az országokat és vállalatokat a gazdaság dimenziójában, melyekre, ha nem képesek megfelelő választ adni, az komoly veszteséget, vagy akár pénzügyi összeomlást is okozhat számukra. Állami szinten a szükséges információk beszerzését a megfelelő döntések támogatására, a gazdasági és külügyi forrásokon túl, a sokkal komplexebb gazdasági hírszerzés biztosítja, míg a versenyszférában hasonló szerepet tölt be az úgynevezett üzleti hírszerzés és a bűncselekménynek számító ipari kémkedés. A gazdasági hírszerzés alatt minden országban – így Magyarországon is – az állami titkosszolgálatok tevékenységét értjük. A tevékenység alapvetése, hogy nem csak az információk, megszerzésére kell koncentrálni, hanem azok tényleges védelmére is. Hazánk gazdasági hírszerzését a Magyar Köztársaság Információs Hivatala, illetve a Magyar Köztársaság Katonai Nemzetbiztonsági Szolgálata (korábban a Katonai Felderítő Hivatal), látja el. Feladatuk, hogy a rájuk jellemző módszerekkel szerzett információk révén kellő időben felismerhetővé tegyék a politikai vezetés számára a negatív vagy pozitív gazdasági tendenciákat és így segítsék a döntéshozatalt. Feladatuk továbbá olyan információk megszerzése, amelyek segítik:

- az ország gazdasági érdekeinek az érvényesülését;
- a gazdasági-pénzügyi veszély elhárítását, a nemzetgazdaság működését;
- a pénzügyi egyensúly fenntartását;
- a kormány foglalkoztatás politikai céljainak megvalósulását;
- a külföldi befektetések ösztönzését;
- jelentős tőke kivonások megakadályozását;
- valamint a magyar technikai-, tőkeexportot veszélyeztető kockázatok felismerését.

Ezen túl még olyan feladatok tartoznak hozzájuk a gazdasági hírszerzés terén, mint a gazdasági globalizációs tendenciák figyelése, a pénzügyi válságok elemzése, a multinacionális szereplők és külföldi szervezett bűnözői csoportok megfigyelése és végül az exportellenőrzés.

Magyarország gazdaságbiztonsági, és az arra vonatkozó információk védelmét az Alkotmányvédelmi Hivatal (jogelődje a Nemzetbiztonsági Hivatal) és a Katonai Nemzetbiztonsági Szolgálat (korábban a Katonai Biztonsági Hivatal) látja el. Feladatuk a veszélyeztető tényezők felderítése és azok elhárítása. Ilyen fenyegetésnek számít az

ellenérdekelt országok gazdasági hírszerzési tevékenysége és a nemzetgazdaságot érintő egyéb ipari kémkedési esetek. Nem képezi a jegyzet központi témáját, de gazdaságbiztonsági kihívásnak számít még a korrupció, a feketegazdaság, pénzmosás és a szervezett bűnözés bizonyos aspektusai is.

A versenyszféra információs igényeit az erre a területre szakosodott üzleti hírszerzőcégek, vagy ami egyre jellemzőbb manapság, a nagyobb vállalatok saját hasonló osztályai látják el, a vezetés közvetlen alárendeltségében. A nemzetközi szintű ipari kémkedés szerepe sem elhanyagolható. A fenti sorok hallatán felmerülhet bennünk a kérdés, hogy alapvetően a versenyszférára jellemző információs háború, az ellenérdekelt állami hírszerzés tevékenységével szemben, mennyiben befolyásolhatja az ország gazdaságbiztonságát? A válasz igen egyszerű: nagyban! Ez a háború közvetlenül érinti a magyar nemzetgazdaságot, kriminalizálhatja azt az ipari kémkedés végett, továbbá a nemzetgazdaság keretein belüli cégek hátrányt szenvedhetnek mind az ipari kémkedés, mind az üzleti hírszerzés következtében, nemzetközi versenytársaikkal szemben.

Először is tisztázni kell, hogy gazdasági kémkedés és ipari kémkedés nem ugyanazt takarja. E két tevékenység élesen elkülönítendő hírszerzési gyakorlatot jelent. Megfogalmazásuk segít a megkülönböztetésben. Elsőként a gazdasági kémkedés definícióját nézzük.

A **gazdasági kémkedés** illegális, titkos, kényszerítő vagy félrevezető eszközök alkalmazása külföldi kormányok vagy azokat támogató szervezetek részéről gazdasági vonatkozású információk megszerzése céljából. Túl az információgyűjtésen, a technológiai titkok eltulajdonításán, egyéb illegális tevékenység kapcsolódása gazdasági előny megszerzése érdekében.

A gazdasági kémkedés alapvető ismertetőjegye, hogy állami szinten folyik, és elsősorban nemzeti gazdasági érdekek feltérképezése, megértése, esetleg rombolása a célja. Nyilván a mai gazdasági helyzetben, amikor transznacionális és multinacionális vállalatok befolyásos szereppel bírnak a globális piacon, ezek kereskedelmi, technológiai, szervezeti vagy működési titkai szintén vitálisak lehetnek nemzeti szempontból, különösen Magyarországhoz hasonló kis nemzetek esetében.

Az **ipari kémkedés** megfogalmazása egyszerűbb, gyakorlatát tekintve azonban természetesen nem sokban különbözik az állami szinten alkalmazott gazdasági kémkedéstől. Az ipari kémkedés illegális, titkos, kényszerítő vagy félrevezető eszközök alkalmazása a privát szektorban gazdasági információk gyűjtése céljából.

Tehát a definíciókból kitűnik, hogy a két kémkedési forma hasonló eszközöket alkalmaz, a különbség használatuk szintjében van, vagyis, hogy állami vagy vállalati keretek között történik-e. Pontosabban: a gazdasági és ipari kémkedés megkülönböztetésében az az irányadó, hogy ki végzi ezt a tevékenységet.

Minden ágazatban komoly harc folyik a piaci pozíció megtartásáért, új piacok szerzéséért. Sok esetben ez új technológia, technika bevezetésétől függ – akár termelési, akár kereskedelmi vonatkozásban. Az új technológia azonban mindig drága, ezért sokan döntenek olcsóbb, ugyanakkor illegális megoldás mellett, azaz lopnak, ipari, gazdasági kémkedés útján jutnak vitális titkokhoz. Hasonlóan fontos faktor a képzett munkaerő. A kifejezetten tudásigényes ágazatokban a belső vállalati továbbképzések, tréningek, az úgynevezett emberi erőforrás fejlesztését szolgáló módszerek, elképzelések kiemelt szerepet kaptak az ipari kémkedésben. Szintén a kiemelt fontosságú területek közé sorolják a vállalatvezetők szakmai és magánéletének ismeretét. Az ipari kémkedéssel, mint etikátlan, illegális eszközöket alkalmazó hírszerzéssel akkor találják szembe magukat a vállalatvezetők, amikor legféltettebb, legfontosabb titkaikat éri támadás.

Érdemes egy pillanatra megállni és elgondolkodni egy bonyolult ipari kémkedéssel kapcsolatos nemzetközi, kormányközi szintre emelkedett ügyről. A kilencvenes évek elején ipari kémháború folyt a General Motors (GM) európai szekciója, az Opel és a Volkswagen (VW) konszern között. A GM európai leányvállalata azzal vádolta a VW vezetését, hogy fontos fejlesztési és kereskedelmi adatokat, információkat lopott el a vállalattól. Az ügy akkor pattant ki, amikor az Opel nyíltan fellépett a Volkswagen egyre agresszívabb kémkedési tevékenysége ellen.

Látható tehát, hogy az ipari kémkedés lehet egyszerűen a piaci küzdelem etikátlan eszköze, de lehet nemzeti szinten jelentkező, gazdasági, kereskedelmi érdekeket érintő kérdés is.

Szeretnék két nagyon jellemző és tanulságos ügyet bemutatni, az információ szerzés és a hírszerzések együttműködésének, vagy éppen azok hiányának hatásairól.

4. BOEING ÉS AZ AIRBUS „HÁBORÚ”

A Boeing és az Airbus közötti „kémkedési háború” a több évtizeden át tartó, titokban zajló versenyt jelenti a két óriásrepülőgép-gyártó között. A két vállalat, amelyek a világ két legnagyobb repülőgépgyártói, számos alkalommal vádolták meg egymást ipari kémkedéssel és információk megszerzésével, amelyek célja a másik cég versenyelőnyének csökkentése volt.

- Korai évek és kezdeti verseny (1970-es évek): A Boeing és az Airbus már a 70-es években is versenyzett a globális repülőgéppiacon. Bár kezdetben nem voltak közvetlenül riválisok, a verseny fokozódott, ahogy az Airbus – mint európai konszern – egyre nagyobb piaci részesedést szerzett a légitársaságok körében. A Boeing a 747-es Jumboval uralta a nagy távolságú, szélestörzsű, nagy kapacitású piacot, míg az Airbus A300-as típusa a közepes távolságú járatokra koncentrált.
- Boeing és Airbus ipari kémkedési vádjai (1990-es évek): Az 1990-es évek közepén a verseny fokozódásával együtt egyre több vád és gyanú merült fel a két cég között ipari kémkedés terén. A Boeing és az Airbus közötti piaci harc a közép- és nagy távolságú repülőgépek piacán vált kiemelkedővé, és a két vállalat között fokozódó rivalizálás jellemezte.
- 1996: A Boeing elleni vádak: A Boeing ellen egy olyan vád merült fel, miszerint egyes alkalmazottai titkos adatokat szivárogtattak ki az Airbus számára. A vádak szerint a Boeing mérnökei és dolgozói szándékosan átadták a vállalat szabadalmi és tervezési adatait, amelyek segíthették az Airbus termékfejlesztését. Bár a vádak sosem kaptak komoly következményeket, a titkos információk megszerzésével kapcsolatos gyanú továbbra is fennmaradt.
- 1997: A „Boeing Man” és a szivárogtatás: 1997-ben egy Boeing mérnököt letartóztattak, miután azzal vádolták, hogy szándékosan adatokat adott át az Airbus számára. Az ügyet titkosították, és részletes információkat nem hoztak nyilvánosságra. Az eset tovább növelte a két cég közötti feszültséget.
- A „Davis-Wright” és az Airbus manipulációs vádjai (2000-es évek): A 2000-es évek elején a két vállalat közötti verseny élesedett. Az Airbus A380-as programja a Boeing 747-esét célozta meg, és komoly kárt okozott a Boeingnak, mivel az Airbus hamarabb elérte a piacot, és jelentős szerződéseket nyert a legnagyobb légitársaságokkal.
- 2003: A „Davis-Wright” ügy: 2003-ban egy Boeing mérnöke, Robert Davis-Wright, és az Airbus egyik vezető mérnöke közötti titkos levelezés került napvilágra,

amelyben a két fél ipari titkokat és tervezési információkat osztott meg. Az ügy kiváltotta a Boeing és az Airbus közötti jogi eljárásokat, és jelentős nyomás alá helyezte mindkét céget, hogy erősítsék meg adatvédelmi és információs biztonsági rendszereiket.

4.1. AZ A380 ÉS 787-ES PROJEKTEK ÉS A VERSENY 2000-ES ÉVEK VÉGÉN

A Boeing és az Airbus közötti verseny a nagy távolságú, nagy kapacitású repülőgépek piacán 2000 végén ismét élesedett, amikor az Airbus bemutatta az A380-as szuperjumbo, két szintes, szélestörzsű repülőgépet, míg a Boeing a 787-es Dreamliner-t fejlesztette. Mindkét projekt hatalmas technológiai kihívások elé állította a cégeket, és a verseny következményeként tovább nőtt az ipari kémkedési vádak száma.

- **2005:** A Boeing és az Airbus dokumentumok szivárogtatása2005-ben kémkedéssel kapcsolatos vádak merültek fel, miután egyes dokumentumok szivárogtak ki a Boeingtől az Airbus számára. Az Airbus mérnökei állítólag hozzáfértek a Boeing 787-es tervrajzaihoz, amelyeket a Boeing egy titkos adattároló rendszeren keresztül kezelt. Az ügyet vizsgálták, de a nyilvános kimenetele nem volt egyértelmű.
- **2007:** Boeing 787-es vs. Airbus A380A Boeing 787-es és az Airbus A380-as közötti verseny folytatásaként számos technológiai titok és innováció került a két cég közötti rivalizálás középpontjába. A Boeing azzal vádolta meg az Airbus-t, hogy ipari kémkedés révén szerezték meg a Dreamliner kulcsfontosságú tervezési elemeit. Az ügyet azonban nem bizonyították, és mindkét cég folytatta fejlesztéseit.

4.2. A KÉT ÓRIÁS KÖZÖTTI JOGI CSATÁROZÁSOK ÉS AZ IPARI KÉMKEDÉSI VÁDAK VÉGSŐ HATÁSA

Az Airbus és a Boeing közötti verseny 2010-re elérte csúcspontját, amikor a Boeing végül kiadta a 787-es Dreamliner-t, míg az Airbus az A380-as programot próbálta befejezni. Bár a kémkedés vádjai továbbra is ott voltak a háttérben, az ipari titkok és a szabadalmak védelme egyre fontosabbá vált a két vállalat számára.

- **2010:** A titkos tervezési információk megszerzése. 2010-ben több incidensről is beszámoltak, amelyekben mindkét vállalat tervezési információit szivárogtatták ki. Az egyik nagy eset az volt, amikor az Airbus szándékosan beszerzett titkos

adatokat a Boeing egyik szállítójától, ami az egész iparágat felkavarta. Az ügyben sem a Boeing, sem az Airbus nem hozott nyilvánosságra konkrét adatokat.

A Boeing és az Airbus közötti „kémkedési háború" folyamatosan formálódott a két vállalat közötti éles verseny hatására. Bár konkrét jogi következmények nem mindig voltak, az ipari kémkedés vádjai több évtizedes versenyt kísérték. A legfontosabb ügyek a tervezési titkok, a szabadalmak, és a műszaki innovációk megszerzése köré épültek. Az ipari kémkedés és az üzleti titkok megsértése mindkét fél számára komoly következményekkel járt volna, és a verseny a repülőgéppiacon továbbra is folytatódik.

Vizsgáljuk meg, talán csak a címszavak szintjén, hogy ilyen méretű, országukban és a világpiacon meghatározó cégek harcában – a saját üzleti hírszerzésükön túl – érdekeltek voltak-e anyanemzeteik titkosszolgálatai.

A Boeing és az Airbus közötti verseny, különösen az ipari kémkedéssel kapcsolatos vádak tükrében, sokkal bonyolultabb, mint pusztán két magánvállalat rivalizálása. Az amerikai és európai titkosszolgálatok, különösen az Egyesült Államok és Franciaország hírszerző ügynökségei, a geopolitikai és gazdasági érdekek védelme érdekében biztos, hogy figyelemmel kísérték a két óriás közötti versenyt, és bizonyos esetekben aktívan befolyásolták is a folyamatokat.

4.3. GEOPOLITIKAI ÉS GAZDASÁGI ÉRDEKEK

A Boeing és az Airbus közötti verseny nem csupán két magánvállalat küzdelme, hanem komoly gazdasági és geopolitikai kérdéseket is felvetett. Mindkét cég az országuk gazdaságának kulcsszereplője, és az ipari verseny befolyásolása komoly politikai és nemzetbiztonsági következményekkel járhat.

Az Egyesült Államok, mint a Boeing szülőhelye, minden bizonnyal érdekelt abban, hogy a Boeing globálisan dominálj on a repülőgépiparban. A Boeing nemcsak az amerikai munkahelyeket és gazdaságot támogatja, hanem a katonai szektorban is kulcsfontosságú szereplő, mivel a Boeing a legnagyobb katonai repülőgépgyártó is (pl. F–15, F/A–18, KC–46A). A Boeing piaci pozíciójának védelme nemcsak gazdasági, hanem biztonságpolitikai szempontból is fontos az USA számára.

Az amerikai titkosszolgálatok (pl. CIA, NSA, FBI) érdekeltek abban, hogy információkat gyűjtsenek vagy adatokat szivárogtassanak ki, amelyek segíthették a Boeing előnyhöz juttatását az Airbus-szal szemben. Bár konkrétan nem bizonyították, hogy a titkosszolgálatok aktívan támogatták a Boeingot, az Egyesült Államok gazdasági és nemzetbiztonsági érdekek védelme erősen befolyásolhatta a háttérben zajló folyamatokat.

Franciaország, mint az Airbus székhelye és egyik fő támogatója, szintén nemcsak gazdasági, hanem politikai érdekek mentén támogatta a vállalatot. Az Airbus nemcsak gazdaságilag fontos szereplő a francia iparban, hanem stratégiai tényező is, különösen a védelmi és a nemzetközi diplomáciai szintéren. Az Airbus az Európai Unió számára is kulcsfontosságú szereplő, és a francia kormány (valamint az EU) számára létfontosságú volt, hogy biztosítsák a vállalat globális versenyképességét, hogy ne csak gazdasági, hanem politikai súlyt is gyakoroljanak a globális piacokon.

Franciaország titkosszolgálatai, mint az DGSE (Direction Générale de la Sécurité Extérieure) a gazdasági hírszerzés terén is aktívan működnek. Biztos, hogy a francia hírszerzés figyelemmel kísérte az Airbus működését, és mindent megtett, hogy megvédje az európai ipari érdekeket, különösen akkor, amikor a Boeing szoros versenyt támasztott az Airbus számára.

A francia kormány érdekei és a biztonságpolitikai kérdések közvetve befolyásolták a titkosszolgálatok tevékenységét is.

Az ipari kémkedés vádjait az Airbus és a Boeing között nemcsak a cégek közötti rivalizálás táplálta, hanem a globális verseny, amely olyan titkos adatokat érintett, mint a fejlesztési terveket, műszaki innovációkat és a szabadalmakat. Az információk megszerzése és az ipari titkok védelme a titkosszolgálatok számára is kiemelten fontos, mivel az ipari kémkedés befolyásolja, veszélyezteti a gazdasági és katonai szektort egyaránt.

A Boeing és az Airbus közötti harc azzal, hogy egy-egy vállalat információkat szerzett a másik fejlesztéseiről, potenciálisan nemcsak a gazdasági versenyt befolyásolta, hanem a nemzetbiztonsági szintű kockázatokat is jelentett.

A Boeing és az Airbus közötti verseny, különösen a 2000-es évek vége felé, kiberfenyegetésekkel és digitális támadásokkal is párosult. Az amerikai és francia titkosszolgálatok mindkét vállalat számára biztosíthattak informatikai biztonságot, és valószínű, hogy a kibertámadások ellen is tevékenykedtek a háttérben, segítve a cégeket a digitális kémkedés elleni védekezésben.

Mindkét kormány nemcsak hírszerzési, hanem jogi eszközökkel is támogatta saját ipari óriásait. Az Egyesült Államok és Franciaország szoros kapcsolatban álltak a saját hírszerző ügynökségeikkel, és bár a titkosszolgálatok nem közvetlenül irányították a cégeket, a politikai és gazdasági érdekek védelme miatt valószínű, hogy informálisan támogatták a Boeingot vagy az Airbus-t a versenyben.

Összegezve, bár ismereteink szerint nincs kézzelfogható bizonyíték arra, hogy az amerikai vagy a francia, illetve más, a beszállításban érdekelt nemzetek titkosszolgálatai közvetlenül

beavatkoztak volna a Boeing és az Airbus közötti ipari kémkedési harcba, a gazdasági, politikai és nemzetbiztonsági érdekek mindkét ország számára fontos tényezőt képeztek. Az állami titkosszolgálatok figyelemmel kísérték a versenyt és támogatták a saját ipari óriásaikat a háttérből, de valószínűleg nem hoztak nyilvános vagy hivatalos döntéseket, amelyek kifejezetten ipari kémkedéshez vezettek volna. Az ipari titkok és a kémkedés szerepe azonban kétségtelenül egyre fontosabbá vált, ahogy a két cég globális piacon vívott harcában a nemzeti érdekek és a gazdasági hatalom is érintetté vált.

5. A MÁSODIK TÖRTÉNETÜNK: A NOKIA ÉS A MOBILPIAC, VALAMINT AZ OKOSTELEFON!

2002 februárjában, a Cannes-ban megtartott konferencián hadat üzent egymásnak a Microsoft és a Nokia. A háború végső célja a mobilpiac feletti dominancia volt. A mobiltechnológia fejlődése eddigre eljutott abba a fázisba, amikor a meglévőknél sokkal szofisztikáltabb szoftvert igényelt, s ezzel lényegében egy miniszámítógéppé vált. Ez magyarázza, hogy az eddig viszonylag távoli piacokon arató két óriás összeütközésbe kerülhetett. A Microsoft a szoftver, a Nokia a mobiltelefon irányából érkezett ahhoz a szituációhoz, amelyben e kettő egyesítése történik.

A Microsoft bejelentette, hogy az Intellel és a Texas Instruments nevű céggel kidolgoznak egy referenciatervet a mobilpiac számára. Ennek jelentősége abban rejlett, hogy megcéloztak egy olyan nemzetközi szabványt (természetesen nem jogi értelemben), amelynek segítségével később a piac nagy részét saját ellenőrzésük alá vonhatták volna. Az elképzelés lényegében lekopírozta azt, ami korábban a személyi számítógépek terén történt. Ott a Microsoft, a Windows operációs rendszerek (és más szoftverek), míg az Intel a Pentium chip-ek útján szerzett dominanciát a piacon, hagyva, hogy – bizonyos korlátok között – a hardver terén verseny alakuljon ki.

Ekkor a mobilpiacon azonban más volt a helyzet. A két óriás eltérő irányból, de lényegében egy időben érkezett el a problémához. A Nokia jelentős tőkeerővel, szellemi kapacitással és piaci tapasztalattal, ekkor még jól működő üzleti hírszerzéssel bír. Ráadásul nem reagált a Microsoft lépéseire, hanem bizonyos értelemben előtte járt. Alapvetően meg volt neki az a szoftver, amellyel harcba indulhatott, és harcmodora jelentősen eltért az amerikaiakétól. A Nokia ugyanis egyrészt engedélyezte szoftverei beépítését más társaságok készülékeibe, másrészt rendelkezésükre bocsátotta forráskódot, ami azt jelentette, hogy a termék szabadon fejleszthetővé vált. Ettől sok szakember nagyobb mozgékonyságot, nagyobb

dinamikát remélt, s azt, hogy gyorsabban jönnek létre a megfelelő alkalmazások, ráadásul így a fejlesztési források is jobban mobilizálhatók voltak.

A küzdelem tehát a szabványért folyt, pontosabban azért, amit a piac később szabványként fogad el. Nincsenek azonban még termékek. A Microsoft egyelőre a nemrég piacra dobott PocketPC nevű kézi számítógépével járt legközelebb a célhoz. Ennek a szoftverét használták kiindulópontként. Ennek ismertségét és kompatibilitását tervezték felhasználni a legnagyobb erőként. A Nokia viszont ekkor már termékeiben igyekezett az internetes eszközök telefonba integrálásával, igaz, inkább technológiai (pl.: NOKIA Communicator 9210i), mintsem üzleti sikerrel. Legnagyobb előnye azonban az volt, hogy ekkor öt telefonból kettőt ő gyártott, így eleve negyvenszázalékos előnyt élvezett a Microsofttal szemben. Ez a szoftveres rugalmasság hozzáadódott a már meglévő piaci fölényhez.

Természetesen egy ilyen szinte kizárólagos hegemónia megszerzése komoly harcot sejtetett a háttérben. Az idő igazolta, hogy ebből a harcból a Nokia jól és hatékonyan működő rendszerei miatt ekkor még győztesen került ki. Nem mondhatjuk el ugyanezt az okostelefonok megjelenése kapcsán.

A Nokia „mélyrepülése” általában a 2010-es évek elejétől a mobiltelefon-piacon tapasztalható folyamatos hanyatlására utal. Ez a „mélyrepülés” érthető módon a Nokia mobilos üzletágának csökkenő teljesítményéből fakadt, amit a konkurenciaként megjelenő okostelefonok növekvő népszerűsége okozott. (Az Apple 2007 júniusában mutatta be az iPhone-t, majd évente a fejlesztett új készüléket és operációs rendszert, 2010-re már a iPhone 4S-nél tartottak.)

A Nokia az okostelefonok piacán – különösen az Apple és a Samsung megjelenése után – nem tudott kellőképpen alkalmazkodni a változó piaci trendekhez. A Nokia saját, kevésbé népszerű operációs rendszere, a Symbian, nem volt képes felvenni a versenyt az Androiddal és az iOS-szel. Az okostelefonok gyorsan növekedő népszerűsége miatt a Nokia piaci részesedése rohamosan hanyatlott. A vállalat értékelése és árfolyama jelentősen csökkent, ami a befektetői bizalom romlását tükrözte.

A Nokia mobil divíziója folyamatosan veszteséges volt, ami még inkább rontotta a cég általános helyzetét.

- A Nokia mobil divízióját 2014-ben a Microsoft vette át.
- A Nokia a mobiltelefon-gyártástól visszalépett, és a hálózati technológiákra és az infrastrukturális projektekre koncentrált.
- A Nokia a hálózati technológiák piacán, például az 5G-vel kapcsolatban, újra növekedési pályára került.

Sajnálatos módon a Nokia vesszőfutásának konkrét magyarországi kihatásai is voltak.

A Nokia 2000-ben kezdte meg komáromi tevékenységét, építette fel és üzemelte be összeszerelő üzemét, mely akkor a világon a legnagyobb volt. Árbevétele alapján a legnagyobb magyar cégek közé tartozott. Az Opten cégtárának adatai szerint a Nokia Komárom Kft. 2010-ben 1017 milliárd forintnyi, vagyis a magyar GDP 3,6 százalékát kitevő árbevételt ért el. 2009-ben 1075 milliárdot, 2008-ban, a válság előtt, 1292 milliárd forintot könyvelt el árbevételként. A 2014 novemberében történt megszűnésével 1620 munkahely szűnt meg.

Egy konkrét eset vázlatos ismertetésén keresztül szeretném bemutatni a vállalati, a privát szaktanácsadói, majd a büntetőeljárás előkészítésében az állami rendvédelmi szervek együttműködését.

A komáromi Nokia összeszerelő üzem – akkoriban a legnagyobb létesítmény – a 2000-es évek közepén élte fénykorát. Közel kétezer alkalmazott dolgozott itt a környékről, Magyarország távolabbi vidékeiről és részben csekélyebb számban, egy-kétszáz fő Szlovákiából. A munkáltató, a finn vállalati kultúrának megfelelően kiemelt munkafeltételeket és környezetet biztosított a dolgozók számára. Ők a mai napig, mint életük legjobb munkahelyét emlegetik.

A cég biztonsági igazgatója ebben az időszakban vette fel a kapcsolatot egy privát szakértői céggel, amely üzleti hírszerzéssel foglalkozott. A rövid problémafelvetés azt mutatta, hogy hosszabb ideje, nagyobb mennyiségben kerülnek ki a gyárból illegálisan a mobiltelefonok központi elemét képező chipek. Ezek a kisméretű lapkák, műanyag szalagra vannak rögzítve és tekercsben kerülnek tárolásra, majd később így kerülnek gyártásba a szalagokon. A speciális termékre tekintettel kiemelt károkozásról számolt be. Az elsődleges problémafeltáró megbeszélés után a gyári finn menedzsmenttel kialakítottuk a végrehajtandó feladatok sorát. Gyártási, folyamatellenőrzési és egyben biztonsági rendszer audit lett elrendelve. Értelemszerűen a konkrét káreseményekre való hivatkozás és célzás nélkül. Ennek a folyamatnak a végrehajtásában, illetve a céljainak megbeszélésében a finn vezetőkön, a biztonsági igazgatón kívül csak az őrzésvédelemért felelős biztonsági cég területi igazgatója került bevonásra.

Az őrzés-védelemért felelős multinacionális cég oldaláról érdekes momentum volt, hogy a londoni központ olyan fontosságot tulajdonított a komáromi felderítésnek, hogy a külső szakértői iroda teljes költségét és díját ők finanszírozták. Ugyanis egy ekkora cég sem engedhette meg magának, hogy elveszítse a magyarországi Nokiát. Egy ilyen szintű

bizalomvesztés a Nokiával szemben akár teljes körű nemzetközi szerződésbontással is járhatott volna.

A teljeskörű audit feltárt néhány hiányosságot, de a konkrét bűncselekmény vonatkozásában nem szolgáltatott érdemi, az elkövetésre, annak módszerére, illetve az elkövetőkre vonatkozó információkat. A kiértékelés után a konzultációs iroda javaslata egy „új munkatárs" telepítése volt olyan munkakörben, amely a legtöbb mozgási lehetőséget biztosította. Az iroda jelezte, hogy rendelkezik megfelelő humán erőforrással a bevezetéshez és a szükség szerinti, folyamatos kapcsolattartáshoz is A végrehajtás időtartamát első körben három hónapra tervezték. A javaslatot a finn menedzsment elfogadta, kellő előkészítés után az új munkatárs a megfelelő civil, általános HR felvételi úton megérkezett, felvételre került. A cég által biztosított munkásszálláson nyert elhelyezést, hiszen ekkor már elég nagy számban dolgoztak Komáromban az ország alföldi régióiból is. A kiválasztott munkatárs rendelkezett termelőüzemi gyakorlattal, speciális jogosultságokkal, például gépkezelői végzettség, targoncavezetői jogosítvány. Ebből fakadóan megfelelő idő elteltével nagy mobilitás volt számára biztosítható. Ki lett alakítva a személyes, rendszeres kapcsolattartás rendje. Különös figyelmet kellett fordítani a kisvárosi, meglehetősen belterjes környezetre, a konspiráció fenntartása érdekében.

A megindított akció az első eredményeit körübelül egy-másfél hónap elteltével kezdte meghozni. A körvonalazódó elkövetői csoport további, üzemen kívüli ellenőrzése elkerülhetetlennek látszott, különös figyelemmel egy megjelenő és erősödő szlovák vonalra. A konzultációs iroda a rendvédelmi hatósági együttműködés érdekében a Központi Bűnüldözési Igazgatóság győri kirendeltségével vette fel a kapcsolatot. A KBI-nek minden lehetőség a rendelkezésére állt, hogy további eredményes felderítéssel készítse elő a későbbi nyílt büntetőeljárást. A KBI – mint bűnügyi hírszerző szervezet – aktív együttműködést folytatott nemcsak a szomszédos, de az európai bűnügyi felderítő szervezetekkel egyaránt így eséllyel indult a nemzetközi szélesítésben.

A Nokián belüli felderítő munka folyamatos volt a korábbi feltételekkel és felállással. A harmadik hónapra konkretizálódtak a belső személyek, sikerült megállapítani az elkövetés módszerét, feltárni a szlovák orgazda vonalat, sőt egy végértékesítésként azonosított horvát kapcsolatot is. Az iroda által bevezetett kapcsolatot egy „ittasan munkába érkezés" miatt eltávolíttatták a gyárból, így a kivonása dekonspirációmentesen megtörtént. Kis idő elteltével KBI, a Győr-Moson-Sopron Megyei Rendőr-főkapitánysággal és a Komáromi Rendőrkapitánysággal közösen realizálást hajtott végre. A nyílt eljárásban a vádemelések után a bíróság az elkövetőket 6–8 évi szabadságvesztéssel díjazta.

Természetesen a belső eljárás vége a lehetővé tévő körülmények teljes körű feltárása, a javítóintézkedések kidolgozása és bevezetése volt. Ez a komplex együttműködés szerintem tökéletes példája volt az akció és ügyszerű együttműködésnek a felsorolt és résztvevő szervezetek között.

A példák után vizsgáljuk meg a hírszerzéssel foglalkozó szereplők tipikus együttműködési formáit. A korábbiakban már külön-külön is vizsgáltuk, hogy melyik önálló területnek mi a feladata. Aránylag tiszta képletet lehet látni a bűnügyi és az üzleti hírszerzés területén, hiszen a bűn üldözésében döntően a múltban megtörtént események felderítése a feladat. Természetesen ettől összetettebb és árnyaltabb a szervezett bűnözés elleni felderítő munka, de itt is a megtörtént vagy a megtenni tervezett kriminális cselekmény megelőzése, megakadályozása a fő csapás iránya. Egyszerűbben leírhatónak és behatárolhatónak tűnik az üzleti hírszerzés területe, hiszen vagy konkrét céghez, területhez, ágazathoz vagy már megtörtént eseményhez köthető. A nemzetbiztonsági szervezetek, a polgári és katonai titkosszolgálatok sokkal szélesebb körben, területeken, adott esetben külföldön, és a globális gazdaság világában, a termelő és szolgáltató szektorban egyaránt kell, hogy tevékenykedjenek ahhoz, hogy a törvényben rögzített feladataikat ellássák. Ebből vezethető le, hogy a titkosszolgálatok számára a felsorolt területekre előírt kötelezettségekhez stratégiai együttműködések szükségesek.

Talán nem hibázunk nagyot, ha megállapítjuk, hogy általánosságban a hírszerzések együttműködése lehet:

- stratégiai hosszú távú és
- akció vagy műveleti, rövidebb távú.

Természetesen ezek nem kőben vésett dolgok, az aktuális operatív helyzet hozhat létre változásokat. Egy stratégiai partner területén is fordulhat elő más, erőket és módszereket igénylő műveleti végrehajtás, míg egy korábbi műveleti partnerből is lehet később stratégiai együttműködő. Ez a hírszerzési, felderítési, és elhárítási terület folyamatos mozgásban van, változások alatt áll. Egy új pénzügyi válság, egy új válságövezet, egy új migrációs hullám, mind-mind olyan mértékben befolyásoló körülmények, amelyek aktív hatást fejtenek ki a hírszerzések működésére. Nem beszélve persze arról a teljesen jogos állami, megrendelői, megbízói igényről, hogy ezek a szervezetek tudják előre jelezni ezeket a váratlannak tűnő eseményeket. Ezért nem győzzük hangoztatni, hogy a folyamatos információ áramlás, a magasszintű értékelő-elemző munka az egyetlen záloga a sikeres munkavégzésnek.

6. A HÍRSZERZÉSEK STRATÉGIAI ÉS MŰVELETI JELENLÉTE

6.1. A MAGYAR LÉGIKÖZLEKEDÉSI VÁLLALAT (MALÉV) AZ II. ÖBÖL-HÁBORÚ IDEJÉN

A könnyebb érthetőség miatt igyekszem az akkor még működő nemzeti légitársaságon, a Malév példáján keresztül mutatom be a hírszerzések stratégiai és műveleti jelenlétét, valamint egy konkrét nemzetközi helyzet generálta válságkezelést.

Magam 2002-től vállalkozásbiztonsági igazgatóként dolgoztam a légitársaságnál, majd 2006 után külső szakértőként folytattam a munkát szerződéses formában. Ahhoz, hogy tisztán lássuk és értsük a Malév helyzetét, súlyát, szerepét a 2000-es évek gazdasági térképén, indokolt áttekinteni röviden a cég történetét.

Alapítás és korai évek (1946–1968):

- 1946. március 29-én alapították Magyar–Szovjet Polgári Légiforgalmi Rt. (Maszovlet) néven. Kezdetben 50-50%-os magyar-szovjet tulajdonban.
- 1946-ban belföldi vonalak (pl. Budapest–Szeged, Debrecen, Szombathely).
- 1954. november 25-én a magyar állam kivásárolta a szovjet részesedést – ettől kezdve működött Malév néven.

A szocialista korszak és expanzió (1968–1989):

- A Malév hosszú időre a keleti blokk egyik fontos légitársaságává vált.
- Flottája főként szovjet gyártmányú repülőgépekből (pl. Il–18, Tu–154) állt.
- Nyugat-Európába is üzemeltetett járatokat, de erősen korlátozott kapacitással.
- A nyolcvanas években megkezdődött a nyugati technológiára való áttérés (pl. Boeing 737-es típusok vásárlása).

Rendszerváltás utáni időszak (1990–2000):

- A Malév állami vállalatból részvénytársasággá alakult.
- Kihívások a liberalizált piac miatt: fokozódó verseny, pénzügyi nehézségek.
- Privatizációs próbálkozások: több lépcsőben részleges privatizáció történt, de a cég mindig visszakerült az államhoz.

A 2000-es évek a modernizáció és a piacgazdasági kihívások időszaka volt, de végül a csőd felé sodródásé is.

Flotta és desztinációk:

- 22–27 repülőgép között mozgott, túlnyomórészt Boeing 737–600, –700 és –800 típusok, valamint Bombardier Q400 regionális gépek.
- Kb. 50–60 város Európában, Észak-Afrikában és a Közel-Keleten.

- Fontos csomópontok: London, Párizs, Frankfurt, Moszkva, Tel-Aviv, Brüsszel, Amszterdam.

Utasszám:

- 2000-ben: kb. 2 millió fő.
- 2005-ben: kb. 3,1 millió fő.
- 2007-ben (csúcspont): kb. 3,5 millió fő.
- 2011-ben (utolsó teljes év): kb. 2,89 millió fő.

Járatszám:

- Évente kb. 23 000 – 28 000 induló járat (oda-vissza duplázva kb. 50 000 járat évente).
- Naponta átlagosan 70–80 járat, csúcsszezonban ennél több is.

Dolgozói létszám:

- 2000 körül: kb. 3 000 fő.
- 2007-ben: kb. 2 800 fő.
- 2011-re: kb. 2 600 fő – létszámleépítések, kiszervezések után.

Nemzetközi kereskedelmi, szövetségi együttműködések:

- 2007-ben a Malév csatlakozott a Oneworld légiszövetséghez, amely reményt adott a nemzetközi integrációra.
- Codeshare-megállapodások többek között a British Airways, Finnair, Iberia, American Airlines társaságokkal.

Gazdasági nehézségek:

- A vállalat folyamatosan veszteséges volt, jelentős adósságállománnyal küzdött.
- Az Európai Bizottság 2010–2012 között vizsgálta az állami támogatásokat, és jogellenesnek minősítette őket.
- A 2007-es év látszólag sikeres fordulatot hozott: nyereséget termelt, csatlakozott nemzetközi légiszövetséghez és bővült a forgalom. Ennek ellenére az üzemi veszteség magas maradt, ami a fenntarthatóságot kérdésessé tette.
- 2011-re a helyzet újra romlott**:** az állami mentőövek és anyagi injekciók ellenére sem sikerült tartósan talpra állni, a veszteségek folytatódtak, ami 2012-es csődhöz vezetett.
- **2012. február 3.** – A Malév hivatalosan beszüntette működését, miután nem tudta tovább finanszírozni napi működését.

A társaság történetéből is kitűnik, hogy az első perctől fogva kiemelt érdeklődést és együttműködést kapott a korábbi állambiztonsági, majd később titkosszolgálatok részéről. Hosszú út vezetett a félkatonai szervezettől a kétezres évekig. A stratégiai együttműködés alapja a teljesség igénye nélkül:

- Kiemelt külföldi utasforgalom.
- Kiemelt külföldi áruforgalom.
- Mindenkori kormányzati utazások teljesítése.
- Konkrét műveleti akciók támogatásának biztosítása.
- A légitársaság külföldi kirendeltségeinek irodahálózatának fel és kihasználása.
- A külföldi területeken keletkezett információkhoz történő hozzájutás.

A Budapest Ferihegyi Repülőtéren a 2000-es évek elején a Malév sajátos szimbiózisban élt a Nemzetbiztonsági Hivatallal, a Vám és Pénzügyőrséggel, a Légügyi Hatósággal, a Repülőtéri Rendőrséggel, a Határőrséggel. Ebből joggal gondolhatjuk, hogy ebben a közösségben kialakult kultúrája volt az együttműködésnek.

6.2. A KONKRÉT VÁLSÁGKEZELÉSI KOMPLEX ELJÁRÁS 2002-2003-BÓL – A II. ÖBÖLHÁBORÚT MEGELŐZŐ ÉS A KIROBBANÁSÁT KÖVETŐ IDŐSZAK

Ahhoz, hogy a nemzetközi helyzet mindenki számára érthető legyen, röviden felidézném az események okait és állomásait:

6.2.1. A kialakulás körülményei

Az Öböl II. háború közvetlen kiváltó oka az Egyesült Államok és szövetségesei részéről az az állítás volt, hogy Irak tömegpusztító fegyvereket (WMD) birtokol, illetve azokat rejtegeti.

<u>Háttér és politikai okok:</u>

- A szeptember 11-i terrortámadás (2001) után az amerikai kül- és biztonságpolitika „megelőző csapás” doktrínáját hirdette meg.
- Az iraki rezsimet azzal is gyanúsították, hogy kapcsolatban állt az al-Kaida terrorszervezettel.
- Gazdasági és stratégiai szempontból Irak jelentős olajtartalékai, valamint a Közel-Kelet katonai és politikai befolyásolása is motivációként szolgált.

<u>Diplomáciai környezet:</u>

- Az ENSZ Biztonsági Tanácsa nem adott felhatalmazást a háború megindítására.
- Franciaország, Németország és Oroszország ellenezte a beavatkozást, míg az USA, Nagy-Britannia és több szövetséges támogatta azt.

<u>A háború kezdete és időtartama:</u>

- Kezdete: *2003. március 20.* (az amerikai „Shock and Awe” légitámadási kampány
- Formális befejezés: *2011. december 18.* (az amerikai csapatok kivonulása)

2002 őszén a Malév Vállalkozásbiztonsági Igazgatósága vizsgálni kezdte az Egyesült Államok és az Irak között egyre feszültebbé váló helyzetet. A vizsgálatnak egyszerű oka volt,

a légitársaság a kérdéses körzetben több olyan járatot üzemeltetett, amelyek üzemelési kockázatát nagyban befolyásolhatta a körzet általános biztonsági helyzete. Az elvégzett elemzések azt mutatták, hogy nem zárható ki egy esetleges háborús konfliktus. Ennek a lehetőségnek az üzemelésre gyakorolt hatásának elemzéséhez az 1991. évi Sivatagi Vihar, I. Öböl háborút tekintettük benchmarknak. Az események légi közlekedésre gyakorolt hatásait tanulmányoztuk és ebből készítettünk egy előzetes figyelemfelhívó anyagot a menedzsment számára. Tisztán látszott, hogy egy esetleges háború nagyon széles körben fogja érinteni a Malév működését. Sajnos a vállalaton belül nem álltak rendelkezésre a 1991 évi eseményeket üzemeltetési hatások szempontjából elemző anyagok. A felkészülési irányoknál, mint várható veszélyt a járatok törlésében, az utazási kedv visszaesésében, az utasszám csökkenésében, az emelkedő kerozin árakban, valamint az alkalmazott légtérzárlatok okán kialakuló hosszabb útvonalakban és bonyolultabb és költségesebb üzemanyag menedzsmentben jelöltük meg.

Idézet a Malév VBI (Vállalkozásbiztonsági Igazgatóság) 2002. október 30.-i kockázati jelentéséből:

„[…]

Az iraki válság charter-ágazatra gyakorolt lehetséges kockázatai:

- a téli charter piac meglehetősen korlátozott Magyarországon és igen érzékenyen reagál a külpolitikai eseményekre;
- a W02 időszakban 5 középtávú- (Európán kívüli) és 3 hosszú távú láncra van szerződésünk, ezek várható összforgalma a teljes időszakban kb. 1,4 Mrd Ft;
- Fenti láncok közül egyedül a TFS (Kanári-szigetek) lánc nem érintett közvetlenül a háborús térség eseményei által, de az utazási (repülési) kedv általános visszaesése hatással lehet erre is;
- A közel-keleti térségben eszkalálódó helyzet nem csak az arab világba irányuló forgalmat érinti, mint HRG, SSH (Egyiptom), AQJ (Jordánia) MIR/DJE (Tunézia), de a légtér érintettsége révén az MBA (Kenya) és BKK (Thaiföld) láncaink realizálását is veszélyezteti;
- Amennyiben bármiféle tényleges háborús tevékenység kezdődik, úgy hasonlóan a tavaly szept. 11. utáni időszakhoz, a charterláncok teljes lemondásával lehet számolni; ezt a szerződések vis maior záradéka kötbérmentesen lehetővé is teszi a partnereknek; a várható forgalom kiesés közel 1 Mrd Ft;
- az esetleges háborús helyzet további kockázata az üzemanyag árak emelkedése.

Az üzemanyag-menedzser részletes információval szolgált a várható tendencia tekintetében, amelyet röviden az alábbiakban foglalok össze:

A világpiacon jelenleg nyersolaj és kerozin elegendő mennyiségben állrendelkezésre, a tartalékok jelentősek, tényleges beszerzési nehézségek az iraki háború kitörése esetén sem várhatók.

Ebből következően az áremelkedésnek nem *fundamentális*, hanem »pszichológiai« okai vannak; az áremelések kapcsán »risk premium«-ról illetve »war-risk premiumról« beszélhetünk.

A Malév Rt. kerozin-felhasználásának döntő részét a monopol-helyzetben lévő eladótól, vagyis a MOL Rt.-től szerzi be, amely kőolajat Oroszországtól vásárol. A kerozint légitársaságunknak »Jet FOB Rotterdam« világpiaci árbázison értékesíti. Vagyis az olajtársaság az árait nem költségalapú árképzéssel alakítja ki, hanem a legközelebbi alternatív beszerzési forrás áraihoz igazítja. Ez az árbázis az év jelenlegi időszakára tervezett 240 USD/tonna körüli árszint helyett már most meghaladja a 270 USD/tonna árat.

Az iraki konfliktus vonatkozásában egyes világpiaci elemzések alapvetően három – eltérő valószínűségű – forgatókönyvvel számolnak:

- diplomáciai rendezés (30%);
- erős iraki válaszcsapás, elhúzódó súlyos konfliktus (10%);
- gyors, sikeres USA/NATO intervenció (60%).

Az első esetben a Brent nyersolaj ára fokozatos emelkedés után 240 USD/tonna körüli áron tetőzik és lassan, kb. 10 hónap alatt ereszkedik vissza a normálisnak tekinthető 200 USD/tonna körüli szintre.

A második esetben a nyersolaj ára gyors ütemben felszökhet akár 400 USD/tonnára is és a konfliktus időtartama alatt a jelzett árszint környékén mozog.

A harmadik esetben a nyersolaj legmagasabb ára – 270 USD/tonna - valamelyest meghaladja diplomáciai rendezés esetére becsült értéket, de messze elmarad az »elhúzódó válság« variációjában jósolt szinttől és igen gyorsan, kb. 2 hónap alatt visszatér a normál szintre.

A Malév egy hónap alatt kb. 17 000 tonna kerozint használ fel, vagyis egy 10 USD/tonna összegű áremelkedés havi kb. 170 000 USD összegű többletkiadást jelent.

A Hungarocontroll »elméleti« információt adott, az öböl-válság ismétlődése esetén Magyarországon sem teljes, sem részleges légtérzárlat nem várható. Ugyanakkor várható, hogy az európai átrepülések területén *katonai okból, vagy a térségbe irányuló polgári repülésekkel összefüggő* ***közvetett*** *okból* lesznek járatkésések. Az öböltérségre vonatkozó konkrét zárlatokat várhatóan csak igen rövid idővel az esedékesség előtt adják meg. […]”[8]

A Malév VBI részéről – a szükséges információk beszerzése érdekében – felvettük a kapcsolatot az Országos Légügyi Hatósággal és a légiirányításért felelős HungaroControl-lal valamint a Külügyminisztérium biztonsági osztályával és a Katonai Felderítő Hivatal munkatársaival is. Folyamatosan üzemeltettük saját, az érintett külföldi körzetekben dolgozó állomásvezetőinkkel, képviseletvezetőinkkel és régióvezetőinkkel megszervezett folyamatos jelentési rendszert. Közös, személyes munkamegbeszélések során alakítottuk ki azt a naponta, szükség szerint azonnal frissülő információs rendszert, ami biztosította az összes érintett számára a legszélesebb körű tájékozottságot.

[8] MALÉV VBI (2002)

A kialakított együttműködés tartalmilag azt jelentette, hogy a KÜM rendelkezésre bocsátotta az Információs Hivatal részükre biztosított információit. A katonai szolgálatok hagyományosan erős hírszerzési pozíciókkal és kapcsolatrendszerrel rendelkeztek Észak-Afrikában és a Közel-Keleten, és ezeket az információkat meg is osztották velünk. A Malév a kialakuló konfliktus környezetében lévő, telepített munkatársai – állomásvezetők, képviseletvezetők és régióvezetők – által szerzett információkra építhetett. A menetrend szerinti járatokkal érintett területek: BEY – Bejrút, CAI – Kairó, IST – Isztambul, LCA – Larnaka, TLV – Tel-Aviv. Charter járatok által repült desztinációk: MIR – Monastir, HRG – Hurghada, SSH – Sharm El Sheikh, MBA – Mombassa, AQJ – Aquaba, GUW – Atura, BKK. A területek nagysága, összetettsége, a munkatársak információszerzési lehetősége a városi irodákon keresztül, a mindennapi életük helyszínein át a repülőterek és a repülés sajátos világáig tartott.

A felsorolt szolgálati és együttműködő felületek azt jelentették, hogy a kritikus régióból nap mint nap lehetőség volt érdemi, esetenként mélységi híreket szerezni. Ezeknek az információknak a napi riportálási rendszerét kellett kidolgozni, hogy adatok minden időben és mindenkinek megérkezzenek. A teljes körön megjelent információkat, a forrásoktól függetlenül, minden érintett felhasználta a saját szakmai területén. Ez az általunk, a területről beszerzett információ mennyiség lett hozzárendelve a nyílt forrásokból beszerzett adatokhoz. Így alakultak a mindennapok során a döntés előkészítések információs alapjai.

Hasonló információs jelentések készültek szükség szerinti sűrűségben:
a 2003. április 9.-i jelentés kivonata:

„**TLV**

A KÜM információi szerint Sharon kijelentette, ha Izraelt bármilyen támadás éri Irakból, a zsidó állam azt megtorolja.

Az általános készültségi fok továbbra is fennáll, a repülőtéri biztonsági intézkedések megnyugtatóak.

Az állomásvezetői jelentések és a repülésvédelmi kíséret tapasztalatai szerint minden járat üzemel, kivéve a KL-t, amely ismeretlen okból április 8-ig szünetelteti járatait. A kísérés során zavaró tényező nem merült fel, katonai légimozgás nem volt észlelhető.

Katonai vonatkozása lehet annak, hogy az ATC a TMA elhagyásának magasságát minden alkalommal meghatározza. (FL 60, 80, 120,)

A repülésvédelmi tiszt három alkalommal akadályozta meg SOF (XX000 járatszám) szabálytalan postaküldemény felrakását.

Biztonsági szempontból nincs változás, egyre kevesebb a járattörlés, az üzemelés biztonsági kockázata alacsony.

IST

A KÜM információi szerint érdemi változás, hogy a készültség foka magasabb lett Törökországban.

Április 3-án két robbantás történt Isztambulban brit és amerikai érdekeltségek ellen. A brit főkonzulátus hátsó vízumbejáratánál, valamint az UPS (Nemzetközi Futár- és Cargo Szolgáltató) telephelyét körbefogó falnál elhelyezett pokolgépek csupán anyagi károkat okoztak.

Az állomásvezetői jelentések szerint nincs törlés az Európába üzemelő légitársaságok részéről. A repülőtéri forgalom élénk, fokozott utasbiztonsági ellenőrzést vezettek be.

A további üzemelés biztonsági kockázata alacsony.

CAI

A KÜM értékelése szerint Egyiptomot nem tekintik közvetlen veszélyövezetnek, de a háborús konfliktus kihatásai különböző területeken érinthetik a lakosságot, a külföldi állampolgárokat és érdekeltségeket is. Az iszlám ünnepek látványos megmozdulások nélkül zajlottak le. A lakosság körében nőtt az Amerika-ellenesség. A tüntetések országszerte folytatódnak, legutóbb 40000-en gyűltek össze Alexandriában, USA, Nagy-Britannia és ENSZ ellenes jelszavakat hangoztattak. Hasonló, de kisebb megmozdulások voltak más városokban is.

Egy iraki diplomatát kiutasítottak.

A légiközlekedés területén nem észlelhető a háborús helyzetnek tulajdonítható forgalomváltozás, a repülőtér üzemelése normál, fokozott biztonsági intézkedéseket nem vezettek be.

A további üzemelésnek biztonsági biztonsági szempontból nincs akadálya.

BEY

A KÜM információi szerint a háborúellenes tömeghangulat változatlan. 9000 fő tüntetett Szidonban, más városokban is megmozdulások voltak. Az amerikai nagykövetség komolyan tanácsolja állampolgárainak a Libanonból való elutazást.

A honvédelmi miniszter nyilatkozata alapján az önkéntesek személyes szolidaritásuk alapján mennek Irakba, a libanoni kormány ebben semmilyen szerepet nem játszik. Kérte az amerikai nagykövetet, az USA járjon el Izraelben annak érdekében, hogy szünjenek meg a berepülések.

A libanoni lapok bejelentették, hogy Magyarországon felfüggesztették az iraki ellenzékiek kiképzését.

Az állomásvezetői jelentések és a repülésvédelmi kíséret tapasztalatai szerint a repülőtér normál üzemelést folytat.

A flight-plan szerinti útvonal az IST FIR kikerülésével törénik. LCA FIR-ben ismételt azonosítást, majd check-point bejelentkezést kérnek. A megkért magasságot megadják, zavaró légi mozgás nem volt tapasztalható.

A repülésvédelmi tiszt két alkalommal akadályozta meg 5/30 kg, majd 3/20 kg szabálytalan posta berakását.

Az LH ötször üzemel egy héten, az LO, AZ, KL április 15-én újraindítja járatait, a többi légitársaság menetrend szerint üzemel.

A további üzemelésnek biztonsági szempontból nincs akadálya.

LCA

Az állomásvezetői jelentések szerint a repülőtér fokozott rendőri jelenlét mellett, normál üzemmenetben működik. Néhány szigorító intézkedés történt, a 14-es, air-side-ra vezető kaput bezárták, az 1-es kapunál random checket vezettek be a személyzet és kiszolgálás tranzit területre lépésénél.

Minden légitársaság menetrendszerűen üzemel.

A további üzemelésnek biztonsági biztonsági szempontból nincs akadálya.

Egyéb információk:

A brit nagykövetség újabb felhívásban javasolta állampolgárainak, hogy ne utazzanak Kuvaitba. Kuvait április 3-tól csökkentette a biztonsági erők készültségi fokozatát. A bahraini hatóságok kiutasították a manamai iraki nagykövetség első titkárát, aki a jelentések szerint aktív szerepet vállalt az ottani amerikai haditengerészeti bázis elleni robbantásban.

Colin Powell amerikai külügyminiszter a március 30-i amerikai-izraeli konferencián (AIPAC) megfenyegette Szíriát, hogy vállalnia kell a felelősséget, amiért szállítmányokat és önkénteseket enged át Irakba. Az izraeli védelmi miniszter a fenyegetés kommentálása során kijelentette, amennyiben Szíria nem változtat álláspontján, a terrorizmus elleni háborúban Irakot követően a következő célpont lehet.

Az iraki katonai fellépés ellen Tiranában nincsenek tüntetések. A határőrizeti szervek a titkosszolgálat bevonásával akciótervet készítettek a tíltott módon belépni szándékozó kurd és iraki illegális migráció megállítására. A Mother Teresa nemzetközi repülőtéren szigorították a belépés biztonsági ellenőrzését."[9]

Ezek a kezdeti időszakban napi jelentések fontos támogatást jelentettek minden résztvevőnek. A Malév szakterületi felelősei, járat tervezők, üzemanyag menedzserek, navigációs szolgálat, hálózat és menetrend tervezők, megfontoltabb, pontosabb, szakmailag, biztonságilag és üzletileg megalapozott döntéseket tudtak hozni. Nagyon fontos szempont, hogy gyorsan.

A kialakulófélben lévő válság nagyságát, összetettségét jól mutatja az Európai Légitársaságok Szövetségének 2003. január 27.-én kiadott dokumentuma, melynek tartalmi kivonatát beidézem:

„**Az AEA (Európai Légitársaságok Szövetsége) krízis-menedzselési anyaga**

Válságterv az Öböl-konfliktus és esetleges újabb terrortámadások hatásainak kezelésére

Döntés: Krízismenedzsment felállítása

Az alkalmazott megközelítés két részből áll:

1) Az AEA kulcsterületeket érintő álláspontjainak kidolgozása 3 forgatókönyv szerint.

2) Az adatcsere és koordináció területeinek és résztvevőinek meghatározása.

[9] MALÉV VBI (2003)

Az anyag bevezető része számadatokkal alátámasztva igazolja a légi-közlekedési iparág gazdasági súlyát és fontosságát, ezzel alapozva meg a későbbi felvetések jogosságát.

– Európában 125 utasszállító légitársaság és 450 reptér van.
– A kapcsolódó szolgáltatásokkal együtt területenként a GDP 1–5 %-át adja!
– 3–5 millió munkahelyet jelent.
– Napi forgalma 700 millió euro.

Probléma: Az ágazat sebezhetősége a nemzetközi konfliktusokkal és terrorizmussal szemben.

Ebből a szempontból rendkívüli figyelmet érdemlő adat, hogy az európai légitársaságok össz-utasforgalmának közel 70 %-a az Európán kívüli járatokon generálódik. (Az ágazat globális jellege!)

Kockázatok:

– Utazási kedv visszaesése;
– Olajár tartós megemelkedése;
– Légtérzárások – ennek következtében járattörlések, útvonal-módosítások, késések, résidő-kiosztás megváltozása, szervízdíjak növekedése

Ez az anyag három forgatókönyvvel számol:

a) korlátozott háború (gyors U.S. siker)

b) kiterjedt háború

c) kiterjedt háború + terrorcselekmények

Alapelvek:

– *A légitársaságok dolgozzák ki saját kockázatkezelési tervüket*
– *Az a.) és b.) esetekben a légitársaságok nem kérnek közvetlen pénzügyi támogatást*
– *Az európai légi-közlekedés a b.) és c.) esetekben strukturális támogatást igényel speciális területeken, a működőképesség fenntartásához szükséges mértékben*
– *Az európai kormányok és intézmények biztosítsanak egyensúlyt az USA légi-közlekedési piacával*

I. Az európai kormányoktól elvárt azonnali intézkedések

1.) Résidők:

Felfüggeszteni a „használod vagy elveszíted” szabályt azokra az esetekre, ha a használatra az öbölkonfliktus okán nincs módja az érintett légitársaságnak.

2.) Biztosítás:

A már most is törékeny biztosítási piacon várható *a harmadik fél okozta káreseményre vonatkozó felelősség biztosítási kör további szűkítése, a háborús és terror-cselekmény okozta káresemény iránti felelősség teljes kizárása.* Szűkítés várható az utasbiztosításokban is. *Ugyanakkor a megmaradó formákban biztosra vehető a további díjemelés. Kormányzati intézkedésre van szükség ezen események fedezetének biztosítására.*

3.) Biztonság („Security”)

Az AEA ki fogja dolgozni a válságkezelés biztonsági alapelveit.

Követelmények:

– A tagállamok kötelesek vállalni a az általuk meghozott biztonsági előírások költségeit.

– Az érintett kormányok hozzanak létre olyan szakmai testületet, ami az állami és légitársasági oldalt is tartalmazva keretet ad a biztonsági konzultációnak. (intézkedések, új eljárások /biometria/, költséghatékonyság, működési és pénzügyi alkalmazások)

4.) Lobbi-tevékenység nemzeti és nemzetközi szinten, kormányzati és intézményi szférában.

II. További intézkedéseket igénylő területek, aspektusok
(Az anyag elején felvezetésként részben már említett kockázatok.)

1) A légtér korlátozása

2) Üzemanyagár emelkedése

3) Kapacitás-egyeztetés engedélyezése

4) A légi-közlekedés részére nyújtott szolgáltatások (ATC) árainak átmeneti befagyasztása

5) A légi-közlekedésben foglalkoztatottakra háruló negatív szociális hatások kezelése, enyhítése

III. Hosszú-távú intézkedések

Ha a fent felsorolt kockázati területeket nem sikerül – a valóra váló forgatókönyvhöz mérten – kielégítő módon kezelni, az azt fogja jelenteni, hogy a légi-közlekedés fundamentális válságba kerül, fenntarthatósága megszűnik.

Ebben az esetben csak egy speciálisan erre a célra létrehozott Európai Alap jelenthet megoldást. Ennek az alapnak a létrehozását az AEA távlati céljának tekinti. ..."[10]

Egyértelműen fogalmazzák meg, hogy az ágazat, a légi közlekedés biztonságos üzemeltetése, gazdasági súlya, a mindennapi életre gyakorolt hatása, a mobilizáció biztosítása és annak veszélyeztetése olyan probléma, amelynek megoldásához uniós szinten is kormányzati beavatkozások szükségesek.

Az előzetes – 2002 októbere óta tartó – felkészülések és az AEA Krízis-menedzselési anyaga alapján 2003. január 29.-én elkészült a Malév akció terve az iraki háború esetére.
A feladat összetettségét mutatja az alábbi kivonatos idézet:

„AKCIÓ TERV AZ IRAKI HÁBORÚ ESETÉRE

2003. január 29.

Verzió 3.

Háború kitörése előtt (T időpont előtt)

Feladatok:

– A kereskedelmi, gazdasági és biztonsági szempontokat figyelembe véve javasolt (február ?-től) a maximumra való tankolás Budapestről a payload felett. (ezzel Budapestre vagy Budapest közeli repülőtérre repülhető a repülőgép a visszafordított járatok esetén)

[10] AEA (2003)

– felhívni a hajózószemélyzetek figyelmét a kapcsolatfelvétel, kapcsolattartás fontosságára: Stockholm rádió, mobiltelefon. Javasoljuk, hogy mobiltelefon a háború idejére géptartozék legyen. (Megjegyzés: A hajózók saját mobil telefonjaiknak száma ismert, van listánk most is. Ugyanakkor kérdéses, hogy kötelezni lehet-e őket külállomáson való telefonjuk bekapcsolására, mert ez esetben hívottként is ők fizetnék a költségeket.)
– minden külföldi állomás legyen elérhető H-24 órában, különösen az érintett állomások + JFK (New York Kennedy), YYZ (Toronto Pearson), BKK (Bangkok-Szuvarnabhumi).
– a külállomások értesítsék az Üzemeltetésirányítási Központot (ÜIK) ha az adott állomásról a háborús térségbe induló légitársaságok járataikat törlik, illetve az üzemelést alapvetően befolyásoló információ birtokába jutnak.
– az ÜIK-ban folyamatos médiafigyelés (CNN, híradások), a Navigációban ill. az ÜIK-ban a NOTAM-ok (Notice to Airmen vagy Notice to Air Mission egy olyan közlemény, amely a légiközlekedésben résztvevő személyzet számára fontos információkat tartalmaz) folyamatos figyelése elemzése.
– az elsődleges telefonlistán lévő személyek azonnali elérhetőségének biztosítása (bekapcsolt mobil, távollét esetén helyettes – aki lehetőleg tudja miért kap értesítést). Folyamatos (éjjel, nappali) bekapacsolt üzemmód február 1-től.
– esetleges, az érintett térségbe történő üzemeltetés esetére a hajózószemélyzetek munkavégzésének tisztázása (önkéntesség, előzetes felmérés, pótlék nagysága stb.)

<u>Háború kitörése (T időpont)</u>

Feladatok a háborúra vonatkozó első információ beérkezésének idejétől függően:

– 21:00 és 23:00 között – az ügyeletes forgalomirányító tiszt (ÜFI) a térségbe irányuló járatokat törli (lehetséges listát lásd a következő pontnál), és értesíti a telefonlistán szereplőket, összehívja a Válságstábot
– 23:00 és 06:00 között – az ÜFI visszafordítja a járatokat, amennyiben már elérték a célállomást a lehető leghamarabb visszajuttatja Budapestre azokat (hacsak nincs olyan ok, ami lehetetlennél teszi a reptér elhagyását), értesíti a telefonlistán szereplőket, összehívja a Válságstábot
– 06:00 és 21:00 között felfüggeszti az érintett járatok indulását és értesíti a telefonlistán szereplőket, összehívja a Válságstábot
– az ÜFI a Válságstáb működőképességéig beszerzi az elérhető információkat

A válságstáb:

Név	Beosztás	Mobil, lakás:
	Vezérigazgató	
	Elnök	
	Üzemeltetési vezig-h / Válságstáb Vezető	
	Kereskedelmi vezig-h.	
	Pénzügyi és Gazdasági vezig-h	

Jasenszky Nándor	Vállalkozásbiztonsági Igazgató	
	OCC vezető	
	Szóvivő	
	Repülési Igazgató	
	Minőség ügyi és Rep. Biztonsági Igazgató	
	Forgalmi Igazgatóság	
	Kockázatkezelési Vezető	
	GKM Légiközlekedési Főosztály	
	POLÉBISZ	
	Polgári Légiközlekedési Hatóság	

Válságstáb (T+ 1 óra)

A T időpontot követő 1 órán belül a Válságstáb összejön a válság operatív kezelése érdekében

Feladat:

Az automatikusan visszafordított, illetve törölt járatok listájának áttekintése

A Válságstáb javaslatai alapján döntés az első 24 órában a térségbe induló járatok (de még el nem indult járat) törléséről vagy engedélyezéséről. Ellenkező döntés esetén minden a térségbe irányuló járat (az első 24 órában) törlésre kerül

Érintett menetrendszerinti járatok: BEY – Bejrút, CAI – Kairó, IST – Isztambul, LCA – Larnaka, TLV – Tel-Aviv,

Érintett charter járatok: MIR – Monastir, HRG – Hurghada, SSH – Sharm El Sheikh, MBA – Mombassa, AQJ – Aquaba, GUW – Atura, BKK – Bangkok

Az események függvényében döntés az első 24 órában egyéb induló Malév (nem térségbe irányuló) járatok törléséről vagy engedélyezéséről. Például esetleges terrortámadás Nyugat Európában szükségessé teheti az oda irányuló járatok törlését, visszafordítását is. Ellenkező döntés esetén minden nem a térségbe irányuló Malév járat indításra kerül.

Nyilatkozhat: Vezérigazgató - Szóvivő.

Válságinformációs Team (T utáni első nap 8: 00)

A T időpontot követő munkanap kezdetén (8:00 kor) a Válságinformációs team összejön a válsággal kapcsolatos információk elemzése, rendszerezése és döntés előkészítés érdekében. A Válságinformációs Teamet a Kockázatkezelési Vezető hívja össze a T időpontbeli értesítést követően.

Feladat:

A gazdasági és repülési (utaslétszám, esetleges kerülő útvonal lehetősége, légtérzárak, megnövekedett biztosítási díjtételek, stb), valamint a biztonsági szempontok alapján javaslattétel a Válság Teamnek az esetleges járattörlésre, módosításra az első 24 órában

A Vállalkozásbiztonsági Igazgatóság munkatársa az érintett célállomásokkal kialakított folyamatos telefonkapcsolat alapján értékeli az adott célállomások biztonsági helyzetét.

A térségbe járó egyéb légitársaságok reakcióinak figyelemmel kisérése

Szervezeti egységek (T utáni első munkanap)

Az egyes szervezeti egységek a háborút követően elkezdik a területükön előzetesen definiált akcióterv végrehajtását. A végrehajtást a Válságstáb, illetve a Válságinformációs Team utasítása alapján kezdik el. A szükséges döntésekről a Válságinformációs Teamet tájékoztatják, a meghozott döntéseket végrehajtják."[11]

Ez a szabályozott rend a háború kitörését követően 2003. április végéig volt érvényben. Ezt követően folyamatosan értékelve lett a biztonsági és forgalmi helyzet, majd ennek ismeretében születtek meg a vezetői döntések.

Lassú normalizálódás után lehetett enyhíteni a korlátozásokat, de a háború maradandó sérüléseket okozott világszerte a légiközlekedésben.

6.2.2. Az Öböl II. háború közvetlen hatásai a légiközlekedésre

Biztonsági intézkedések szigorítása:

A háború újabb lökést adott a globális légiközlekedési biztonság militarizálásának, főként az amerikai és európai reptereken.

Fokozódott az utas- és csomagellenőrzések mértéke, nőtt a személyes adatgyűjtés. (Pl.: PNR (Passenger Name Record): foglalási adatok pl. fizetési mód, ülésválasztás, repülési útvonal, poggyászinformáció)

A repülésbiztonsági rendszerekbe beépült a háborús tapasztalatokon alapuló profilalapú kockázatelemzés.

Légitársaságokra gyakorolt gazdasági hatás:

A háború és az emelkedő olajárak drámai üzemanyagköltség-növekedést hoztak a légitársaságok számára.

Több kisebb légitársaság csődbe ment 2003–2005 között (különösen Európában és Észak-Amerikában).

A nagy légitársaságok (pl. Delta, United) költségcsökkentésre és járatritkításra kényszerültek.

Légiforgalmi útvonalak átrendezése:

A B-52 Stratofortress bombázók esetén hosszú, közvetlen transzatlanti átrepülések voltak a jellemzőek;

Szállító repülőgépek (C-17, C-130) rendszerint Ramstein/Aviano/Constanța felől indulva jutottak el iraki célpontokra (Bashur, Kirkuk).

[11] MALÉV (2003)

Külön partraszálló/háborús légikapacitás később Qayyarah, Moszul és más előretolt repterekről operált.

A katonai stratégiai útvonalakhoz igazodva polgári légiforgalom gyakran alternatív útvonal terv szerint repült**,** hogy elkerüljék a hadműveleti területeket (Irak, Szaúd-Arábia térsége). A sivatagi térségben lezárt katonai légterek gyakoriak voltak; emiatt a polgári járatok hosszabb úton, például Törökország vagy az Arab-félsziget nyugati légtere felé kerültek (analóg napjaink Irán–Izrael konfliktusával).

A katonai szállítások megsokszorozódtak: a Ramstein–Bashur útvonalon napi 4–5 járat teljesült. Ez túlterhelte az előretolt bázisok infrastruktúráját, ami a polgári repülést korlátozta. Polgári repülőterek (pl. Al Udeid, Prince Sultan) osztoztak a katonai műveletekben.

Több nemzetközi légitársaság elkerülte az iraki légteret, illetve később is csak korlátozottan használta.

A Közel-Kelet tranzitrepülőtereinek (pl. Dubai, Doha) szerepe megnőtt, mivel a háború kitérítette a nyugat-keleti folyosók egy részét.

Az iraki repterek (Bagdad, Basra) civil használatra csak fokozatosan tértek vissza, hosszú ideig csak katonai vagy humanitárius forgalom zajlott.

Az Öböl II. háború messze nem csupán egy katonai konfliktus volt: globális gazdasági, politikai és biztonságpolitikai hatásai is mind a mai napig jelentősek. A légiközlekedés különösen érzékenyen reagált a konfliktus következményeire, mind az üzemanyagárak, mind az útvonalak, mind pedig a biztonsági protokollok szintjén.

Meggyőződésem szerint a Malév 2003-as, Öböl II. háborús válságkezelésénél kialakított és hosszabb időn keresztül eredményesen működtetett, széleskörű együttműködés bizonyította: az érintett állami hatóságok, polgári és katonai titkosszolgálatok, valamint egy civil vállalat üzleti hírszerzése, ha akar, tud és képes a magas szintű közös munkára. Ezt persze segítette a teljes érdekazonosság, továbbá az, hogy mindenki átérezte a munka fontosságát, az emberek biztonságára, életére gyakorolt konkrét hatását. Felülemelkedtek a sok esetben máskor fel-felbukkanó lokális szolgálati érdekeken.

Reményeim szerint a felsorolt és bemutatott gyakorlati példák megerősítették azt a megállapítást, hogy a hírszerzések és az aktuális felderítési területen dolgozó vagy jelenlévő bármely szervezetekkel való együttműködés segítheti és javíthatja eredményességüket.

7. HAZAI ÉS NEMZETKÖZI TAPASZTALATOK ALAPJÁN AZ EGYÜTTMŰKÖDÉS FOKOZÁSÁNAK JÖVŐBENI LEHETŐSÉGEI

A titkosszolgálatok, a terrorelhárítás és a magánbiztonsági, üzleti hírszerzési szolgálatok, irodák, osztályok közötti együttműködés kulcsfontosságú lehet a jövőben a nemzetbiztonság és gazdaság védelme szempontjából, különösen olyan komplex és dinamikus fenyegetések esetén, amelyek hatással lehetnek a társadalom biztonságára és a gazdaság stabilitására. A két szektor közötti együttműködés számos területen előnyös lehet, különösen az információmegosztás, a kockázatértékelés és a gyors reagálás tekintetében.

Információmegosztás és közös hírszerzés:

Az egyik legfontosabb együttműködési lehetőség az információmegosztás. Az titkos felderítéseket végző állami szolgálatok, a titkosszolgálatok, a bűnügyi hírszerzés és a terrorelhárító szolgálat /továbbiakban: Szolgálatok/ és a magánbiztonsági, üzleti hírszerző cégek gyakran szembesülnek hasonló fenyegetésekkel, például terrorista támadásokkal, kibe fenyegetésekkel vagy ipari kémkedéssel. Az együttműködés során a következő lehetőségek merülhetnek fel:

- **Közös hírszerzés és adatmegosztás**: A magánszektor (pl. a pénzügyi, energia- vagy technológiai szektorok) vállalatai gyakran gyűjtenek adatokat, amelyek a Szolgálatok számára is hasznosak lehetnek, például gyanús pénzügyi tranzakciók, nemzetközi összefonódások, vagy ipari kémkedésre utaló jelek formájában. Az ilyen információk megosztása segíthet az állami szolgálatoknak az alaposabb fenyegetések észlelésében.
- **Központi adatbázisok és kommunikációs csatornák létrehozása**: Különböző adatbázisok (pl. kiberfenyegetési információk) és kommunikációs csatornák kialakítása, amelyek lehetővé teszik a gyors és hatékony információáramlást a magánszektor és az állami szolgálatok között.
- Az Amerikai Egyesült Államok **Fúziós Központok**at **(Fusion Centers)** működtet, amelyekben a különböző rendvédelmi, nemzetbiztonsági továbbá a magánbiztonsági szolgálatok emberei is egymás mellett dolgoznak azon, hogy a jelentéseik a lehető legtöbb forrásból megszerzett adatokat tartalmazzák, és a leggyorsabban jussanak el a célzott felhasználókhoz. A központok a terrorizmus elleni küzdelem okán születtek, ám idővel kiterjedt a hatáskörük más területekre is.

Közös kockázatértékelés és megelőzés:

A Szolgálatok és az üzleti hírszerzés közötti együttműködés egyik legfontosabb aspektusa a kockázatértékelés és a megelőzés, mivel mindkét fél számára elengedhetetlen a potenciális fenyegetések felismerése és a megfelelő válaszreakciók kidolgozása.

- **Kockázatfelmérés és sérülékenységvizsgálatok**: A magánszektornak, különösen a kritikus infrastruktúrával rendelkező iparágakban (pl. energiaipar, pénzügyi szektor, közlekedés), fontos szerepe van a saját biztonságuk és védelmük kiépítésében. A Szolgálatok segíthetnek a potenciális támadási formák azonosításában, amelyek a magánszektor számára kritikusak, míg a magáncégek a saját fenyegetettségeikhez kapcsolódó adatokkal támogathatják az állami szervet.
- **Szcenárió alapú gyakorlatok és szimulációk**: Az állami és magánszektori hírszerzők közös gyakorlatokat, asztali szimulációkat végezhetnek, amelyek segítenek felkészíteni mindkét szektort a várható támadásokra, például terrorista akciókra vagy kiberbiztonsági fenyegetésekre. Az ilyen típusú szimulációk lehetőséget biztosítanak a közös reakciótervek tesztelésére, a hatékony kommunikációs csatornák kiépítésére és a koordinált válaszadási képességek fejlesztésére.

Kiberfenyegetések és kibervédelem:

A szervezett bűnözés és a modern terrorizmus, vagy akár a piaci konkurens által megbízott csoportok gyakran kiberfenyegetések révén is támadja a kritikus infrastruktúrát. Az üzleti hírszerzés és a Szolgálatok közötti együttműködés különösen fontos lehet a kiberbiztonság terén.

- **Közös kibervédelmi rendszerek és eszközök**: A magánszektor (különösen az IT és telekommunikációs iparágak) és az állami szervetek közötti szorosabb együttműködés segíthet a kibertámadások megelőzésében. A Szolgálatok az állami szintű, globális kiberfenyegetésekhez való hozzáféréssel segíthetnek a vállalatoknak abban, hogy megvédjék saját rendszereiket és adatbázisaikat.
- **Közös kiberhírszerzési csatornák**: Az állami hírszerzés és a magánvállalatok közötti közvetlen kapcsolat lehetőséget adhat a kiberfenyegetésekkel kapcsolatos gyors információcserére, és segíthet a potenciálisan káros vírusok, malware-ek, vagy kémprogramok gyors felismerésében és semlegesítésében.

Szabályozások és jogi keretek:

Az állami és magán hírszerző szolgálatok közötti együttműködés során fontos, hogy a jogi és etikai normákat minden esetben betartsák. A titkos információk megosztása vagy a vállalati adatvédelmi előírások tiszteletben tartása különös figyelmet igényelhet.

- **Jogi keretek és adatvédelmi szabályozás**: A Szolgálatok és a magánbiztonsági szolgálatok közötti együttműködésnek biztosítania kell, hogy az információk megosztása feleljen meg a hazai, valamint a nemzetközi jogszabályoknak, mint például az EU Általános Adatvédelmi Rendelete (GDPR), vagy az Egyesült

Államok adatvédelmi előírásai. Ezért szükséges a megfelelő jogi és szabályozási alapok megteremtése, hogy a közös munkát a jogi határok betartása mellett végezhessék.

Közvetlen vészhelyzeti válaszadás:

A Szolgálatok és a magánbiztonsági cégek közötti együttműködés különösen hasznos lehet válsághelyzetekben, például egy terrorista támadás, ipari baleset vagy kiberincidens esetén.

- **Koordinált reagálás**: A közvetlen együttműködés lehetőséget biztosít a gyors és koordinált válaszadásra, ahol mind az állami szolgálatok, mind a magánvállalatok biztosítják a szükséges erőforrásokat és szakértelmet. A magánvállalatok rendelkezhetnek speciális technológiai eszközökkel vagy gyorsan mobilizálható erőforrásokkal, míg az állami szervek rendelkeznek a szükséges jogi, operatív és nemzetközi kapcsolatokkal.

Képzés és tudatosságnövelés:

A különböző szektorok közötti együttműködés segíthet abban, hogy mindkét fél felkészüljön a különböző fenyegetésekre.

- **Képzési programok**: A magánszektor és a Szolgálatok közös képzési programokat indíthatnak, amelyek célja a munkatársak felkészítése a különböző típusú fenyegetésekre, beleértve a kibertámadásokat, a fizikai terroristatámadásokat, és a pénzügyi terrorizmus elleni küzdelmet.

8. ÖSSZEGZÉS

A titkosszolgálatok a bűnügyi hírszerzés a terrorelhárítás és a magánbiztonsági, üzleti hírszerzés közötti együttműködés rendkívül fontos a modern fenyegetések kezelésében. Az információmegosztás, közös kockázatfelmérés, kibervédelem, jogi szabályozások és gyors vészhelyzeti reakciók lehetőségei mind hozzájárulhatnak a hatékony védekezéshez. A két szektor közötti együttműködés erősítése nemcsak a társadalom biztonságát növeli, hanem segíthet megvédeni a gazdasági infrastruktúrát és a kulcsfontosságú iparágakat is.

FELHASZNÁLT IRODALOM

AEA (2003): *Válságterv az Öböl-konfliktus és esetleges újabb terrortámadások hatásainak kezelésére*. A szerző tulajdonában lévő irat.

HÖHN, Christiane dr. (2014): *Az európai terrorelhárítási erőfeszítések aktuális kihívásai.* Előadás a Terrorelhárítási Központ 4. születésnapja alkalmából. Budapest, 2014. szeptember 3.

JASENSZKY NÁNDOR – REGÉNYI Kund Miklós – LIPPAI Zsolt (2021): A biztonságtudatosság fogalma fejlődése nemzetbiztonsági, terrorelhárítási és magánbiztonsági szempontból. *Nemzetbiztonsági Szemle,* 9(4), 3–17. Online: https://doi.org/10.32561/nsz.2021.4.1

JASENSZKY Nándor – SOMOSKŐVI Áron dr. (2016): A *terrorelhárítás információéhsége és a „csillapítás" lehetőségei.* In: BEBESI Zoltán dr. (szerk.): *Terrorelhárítási alapismeretek.* Budapest: Dialóg Campus Kiadó, Nordex Kft., 193–212.

JASENSZKY Nándor (1987): *Operatív erők, eszközök és módszerek komplex alkalmazása, illegálisan hazánkban tartózkodó, külföldi bűnözők által elkövetett betörési sorozat felderítésében*. Szakdolgozat. Belügyminisztérium Rendőrtiszti Főiskola.

JASENSZKY Nándor (2015): *Adatszerzés – Információhasznosulás – Biztonságtudatos vállalati kultúra.* In: SZAMOS Tamás (szerk.): *A nyílt információgyűjtés fejlődő területei. Nemzetközi tudományos-szakmai konferencia tanulmánykötet.* Budapest: Belügyi Tudományos Tanács, 55–65.

JENSEN, Carl J. – MCELREATH, David H., – GRAVES, Melissa (2013): *Bevezetés a hírszerzésbe*. Budapest: Antall József Tudásközpont.

KASZNÁR Attila – JASENSZKY Nándor – SOMOSKŐVI Áron (2017): *Az információ szerepe és elemzési lehetőségei a terrorfelderítés aspektusából*. In: KASZNÁR Attila (szerk.): *Bevezetés a terrorelhárítás alapjaiba.* Budapest: Dialóg Campus Kiadó, Nordex Kft., 211–269.

KASZNÁR Attila (szerk.) (2017): *Bevezetés a terrorelhárítás alapjaiba.* Budapest: Dialóg Campus Kiadó.

LOWENTHAL, Mark M. (2017): Hírszerzés – A titkoktól a politikai döntésekig. Budapest: Antall József Tudásközpont.

MALÉV (2003): *Akció terv az iraki háború esetére*. A szerző tulajdonában lévő irat.

MALÉV VÁLLALKOZÁSBIZTONSÁGI IGAZGATÓSÁG (2002): *2002. október 30.-i kockázati jelentés*. A szerző tulajdonában lévő irat.

MARAS, Marié-Helen (2016): A terrorizmus elmélete és gyakorlata. Budapest: Antall József Tudásközpont.

MEZEI József – KONCZ Veronika – JASENSZKY Nándor (2021): Biztonságtudatosság – hazai helyzetkép, hazai gyakorlat és példák I. Biztonságtudatosság – hazai helyzetkép, hazai

gyakorlat és példák 2. *Nemzetbiztonsági Szemle*, 9(4), 48–61. Online: https://doi.org/10.32561/nsz.2021.4.4

NEMES Sándor (1944): *Gyakorlati nyomozás*. Budapest: GRIFF Könyvkiadó.

NYESTE Péter – SZENDREI Ferenc (2019): *A bűnügyi hírszerzés kézikönyve.* Budapest: Dialóg Campus Kiadó – Nordex Kft.

O. GÁBOR László – JASENSZKY Nándor – FORRÓ György – HARMADOS György (2001): *Üzleti hírszerzés.* Budapest: Budapesti Műszaki és Gazdaságtudományi Egyetem, Mérnöktovábbképző Intézet.

ORMOSY Gábor László – HARMADOS György – JASENSZKY Nándor – Forró György (2010): *Üzleti hírszerzési és elhárítási ismeretek.* Egyetemi jegyzet. Budapest: BM Rendőrtiszti Főiskola.

PILCH Jenő szerk. (1937): *A hírszerzés és kémkedés története* I–III. Budapest: Franklin-Társulat.

REGÉNYI Kund – JASENSZKY Nándor – LIPPAI Zsolt (2022): The concept of security awareness, its development from the point of view of national security, counter-terrorism, and private security. *Belügyi Szemle / Academic Journal of Internal Affairs*, 70(Special Issue–1.), 123–137.

RÓDLER Norbert dr. (2021): *Terrorizmus a kibertérben.* Szakdolgozat. Nemzeti Közszolgálati Egyetem, Közigazgatási Továbbképzési Intézet.

ROLINGTON, Alfréd (2015): *Hírszerzés a 21. században, a mozaikmódszer*. Budapest: Antall József Tudásközpont.

TÓTH Gábor (2021): *Az információszerzés és a hírszerzés kapcsolata az ókortól napjainkig.* Szakdolgozat. Nemzeti Közszolgálati Egyetem, Rendészettudományi Kar, Terrorelhárítási Tanszék.

TURCSÁNYI Gyula szerk. (1927): *Modern bűnözés I–II. Budapest*: Rozsnyai Károly Kiadása.

Csepregi Zsolt

Az Izrael–Hamász háború terrorelhárítási tapasztalatainak vizsgálata

1. BEVEZETÉS [1]

A 2023. október 7-i Hamász terrortámadás új szintet jelentett a globális terrorizmus történetében, és így a terrorelhárítás területén is kiemelt vizsgálati kérdéssé vált. Az akció során a Hamász és kisebb radikális szervezetek terroristái a Gázai övezetből kitörve több mint ezerkétszáz izraeli személyt gyilkoltak meg, és 254 főt Gázába hurcoltak túszként.[2] Az izraeli nemzettudat számára a tragikus nap súlyát jelzi – és egyben a reakciók intenzitását magyarázza –, hogy a zsidóság történelmében a Holokauszt óta a legnagyobb áldozattal járó napként hivatkoznak rá.[3] A terrortámadás következtében kirobbant a több mint egy éve tartó Izrael-Hamász háború, az izraeli haderő bevonult a Gázai övezetbe majd a fegyveres konfliktus órákon belül regionális szintre emelkedett.

A Hamász azonban nem egy elszigetelt terrorszervezet, hanem része az Irán által vezetett ellenállás tengelyének és így a közel-keleti nagyhatalmi küzdelemben proxyszereplőként jelenik meg.[4] A harcok az összetett regionális viszonyokból eredően tehát kiterjedtek a Hezbollah terrorszervezet tevékenysége folytán Libanonra, valamint Szíria, Irak, Irán és Jemen mind érintettek a harcokban a Hamász oldalán. Az izraeli oldalon hatásosan lépnek fel az Egyesült Államok, a nagy európai katonai hatalmak, mint az Egyesült Királyság és Franciaország, továbbá egyensúlyozó politikát végeznek folytatnak a szunnita arab államok. A Hamász terrorista akciója tehát átfogó közel-keleti eszkalációhoz és gyakorlatilag egy korlátozott intenzitású, de regionális kiterjedésű háborúhoz vezetett, amely jelentős hatással van a globális viszonyokra is.

Mindezek több mint egy év elteltével szükségessé teszik a terrortámadást lehetővé tevő izraeli mulasztásoknak, a Hamász stratégiájának, a harcok lefolyásának vizsgálatát. Az elemzés során kitérek a háború regionális kontextusára, azonban leginkább olyan tekintetben, hogy az hogyan gátolja a terrorelhárítási művelet lezárását, valamint a terrorelhárítási célok

[1] A tanulmány kézirata 2024. november 30-án került lezárásra.
[2] Egyesült Államok Külügyminisztériuma (2024)
[3] Council on Foreign Relations (2024)
[4] Sobelman (2024)

hogyan segíthették Izrael tágabb biztonsági környezetének kedvező átalakítását. Végezetül az események vizsgálatát követően a legfontosabb célom levonni a tanulságokat, hogy egyrészt hasonló terrortámadások ellen bevethető legjobb módszerekre rávilágítsak, másrészt aláhúzzam, hogy a huszonegyedik században milyen szoros összefüggés létezik a lokális terrorszervezetek tevékenysége, a regionális dinamikák és a globális rend megbillenése között. Mindezek a tényezők Magyarország számára is relevánssá teszik a Hamász terrortámadása és az azt követő események vizsgálatát és a nemzetközileg alkalmazható tanulságok levonását.

A kutatás kvalitatív módszereket alkalmaz a téma feltárása céljából, ezen belül szakértői interjúkra, a háborúval kapcsolatos szakértői elemzésekre és hivatalos, legfőképpen izraeli és amerikai vezetői (politikai és katonai) nyilatkozatokra építve dolgozza fel a kutatási kérdéseket. A konkrét terrortámadást és az azt követő háborút esettanulmánynak tekinti, amelyből általános következtetések vonhatóak le, amelyek a sajátos izraeli, közel-keleti kontextust meghaladva általános, globális tanulságokkal is szolgálnak. A kutatás a fent bemutatott összetett kérdések közül négyet vizsgál kutatási kérdés minőségben.

1) Milyen izraeli tényezők, mulasztások és hibák tették lehetővé, hogy a Hamász képes volt végrehajtani és átmenetileg kiterjeszteni az október 7-i terrortámadását?
2) Mennyiben tekinthető Izrael katonai válasza újszerűnek, vagy az a nemzeti biztonsági stratégiájából egyértelműen következő lépés volt?
3) A kitűzött izraeli háborús célokat mennyiben sikerült izraeli és nemzetközi értékelések szerint teljesíteni, hogyan változtak azok az elmúlt tizenkét hónapban, miért húzódott el a háború több mint egy éven keresztül?
4) Milyen mértékben sikerült Izraelnek elválasztani a lokális terrorszervezettel szembeni harcot annak regionális támogatójával szembeni küzdelemtől?

2. A HÁBORÚ

A 2023. október 7-én kirobbant Izrael–Hamász háború elválaszthatatlan a közel-keleti hatalmi rend folyamataitól és az izraeli-palesztin konfliktus háttérbeszorulásától. Az elemzés kereteit meghatározó külső környezetet röviden összefoglalva: az öt közel-keleti nagyhatalom közötti komplex egyensúlyozás határozta meg, amelyben átfogó normalizációs trend érvényesült egészen 2023 őszéig.[5] Az öt nagyhatalmat, Egyiptomot, Izraelt, Törökországot,

[5] KRASNA – MELADZE (2021) 6–8.

Iránt, Szaúd-Arábiát és Izraelt alapvetően három tengelyre oszthatjuk[6], amelyek közül az Egyesült Államokkal szoros biztonsági partnerséget ápoló Izrael és Szaúd-Arábia és a szunnita arab államok többsége alapvetően status quo politikát követ, Irán és az „ellenállás tengelye" (a szíriai Aszad-rezsim, iraki síita milíciák, a libanoni Hezbollah és a jemeni húszik) ezzel szemben revizionista hatalmi ambíciókkal rendelkeznek és főként Oroszország, kisebb mértékben Kína támogatását élvezik. A harmadik tengely, amely jelenleg leginkább befelé fordul, Törökország, amely a korábbi években megkísérelte Katarral és a Muszlim Testvérekkel közösen egy új közel-keleti rend kialakítása felé törekedni, azonban ambícióit a török belpolitikai és gazdasági nehézségek visszafogták és leginkább a szíriai és iraki kurd erőkkel szembeni harcok kötik le erejét.

Meg kell említeni, hogy negyedik „pszeudo" tengelyként nem feledkezhetünk meg a radikális, dzsihádista terrorszervezetekről, mint az al-Káida és az Iszlám Állam, amelyek bár visszaszorultak, továbbra is kihasználják a hatalmi vákuumot és várják, hogy újra megerősödhessenek, amennyiben a közel-keleti állami struktúra tovább erodálódik. Az államközi kihívásokon túlmenően minden közel-keleti állam alapvető modernizációs kihívással szembesül és a társadalmi szerződés modern körülmények között való újrakötése jelenti a legnagyobb kihívást.[7] A belső feszültségek és modernizáció terhei lekötik ezen államok erőforrásait, ezért kívánatos volt az államközi feszültségek csökkentése. Ennek az igénynek volt az eredménye az a kiegyezési folyamat az Ábrahám-megállapodásoktól kezdődően a török–egyiptomi és az iráni–szaúdi normalizációig.[8] Ezt az alapvetően kényes egyensúlyt és óvatosan kedvező trendet szakította meg a Hamász terrortámadása.

Fontos leszögezni, hogy a Hamász terrortámadásának időzítésének és nemzetközi okainak bemutatása természetszerűleg nem jelenti annak bármifajta legitimálását. Kijelenthetjük azonban, hogy az izraeli-palesztin konfliktus – amelynek bemutatása meghaladja a kutatás kereteit – jelentős mértékben vesztett korábbi relevanciájából.[9] Ennek számos oka volt, egyrészt a közel-keleti egyensúlyozási, normalizációs és modernizációs trendek, másrészt a globális válságok, utóbbiak közé sorolható a teljesség igénye nélkül az orosz-ukrán háború, a COVID-válság és az Egyesült Államok és Kína között folyó hatalmi küzdelem. A palesztin államiság kérdésének leértékelődése sajátos izraeli és palesztin okokra is visszavezethető. Izrael kiemelt gazdasági, technológiai és katonai partnerévé vált a világ államainak többsége

[6] CSICSMANN (2020) 17–18.
[7] CSICSMANN (2020): 23.
[8] SALAMI (2024)
[9] N. RÓZSA (2024): 65.

számára, ebből következően nem kívánták az Izraeltől nyerhető hasznot kockáztatni a palesztin ügy hangsúlyos képviseletével.

A palesztin fél melletti kiállás csekély gazdasági vagy politikai hasznot hozhat, a korábbi béketárgyalások nem jártak sikerrel, továbbá maguk a palesztinok is megosztottak, a Fatah és Hamász közötti egységkormány megalakítását célul kitűző tárgyalások mindig kudarcba torkoltak. Önmagában az a tény, hogy az Izraellel biztonsági és gazdasági tekintetben együttműködő Fatah Ciszjordániában, izraeli katonai jelenlét mellett kormányoz, míg a Hamász Gázát uralja és hivatalosan továbbra is Izrael megsemmisítését tűzi ki célul, garantálta, hogy ne léphessenek fel közösen a palesztin államiság előmozdítása érdekében.[10] Ez nem jelenti azt, hogy a világ közvéleménye, főként a regionális államok, teljes mértékben közömbösek lettek volna a palesztin nép iránt. Ezt már belpolitikai okokból sem tehették meg, mivel különösen a muszlim lakosság természetszerűleg szimpatizál a palesztinok államisági törekvéseivel és az Izraelhez túl közel kerülő állami vezetés rezsimbiztonságát ez erodálhatja. Azonban az Ábrahám-megállapodásokhoz vezető feltételezés 2023. október 7-ig fennmaradt, miszerint az Izraellel folytatott kiegyezés alapvetően függetleníthető a palesztin államiság kérdésében való előrehaladástól.[11]

A fő megmaradt kérdést a palesztinokkal kapcsolatban 2023-ra az jelentette, hogy milyen mértékű engedményt kell Izraelnek tennie, hogy amerikai vezetéssel létrejöhessen az izraeli-szaúdi normalizáció és ennek eredményeként a közel-keleti regionális biztonsági architektúra alappillérei.[12] A fenti folyamatok Hamász víziója, közelítsük azt meg akár a független palesztin állam a Jordán-folyó és a Földközi tenger között, vagy Izrael elpusztítása oldaláról, egyre inkább távoli ábrándnak tűnhetett, ami, mint mára tudható, radikális, azonban semmiképpen nem hosszú évek előkészítését igénylő radikális lépés megtételére sarkallta a terrorszervezetet.

2.1. HÁBORÚ ELŐTTI ÁTFOGÓ STRATÉGIÁK

Az Izrael-Hamász háború előzményeit, kereteit a közel-keleti regionális dinamikák és az izraeli-palesztin konfliktus adták, azonban a két fő harcoló fél háború előtt követett stratégiái tették lehetővé, hogy a terrortámadás a gyakorlatban megvalósulhasson. A következőkben tehát az izraeli politikai és katonai vezetés, valamint a Hamász által követett megközelítéseket mutatom be.

[10] ROBINSON (2024)
[11] CSICSMANN (2020): 26.
[12] EFRON – GOTTESMAN – KOPLOW (2023): 8–9.

Az izraeli katonai stratégia az állam megalapításától kezdődően a létfenyegetésekre koncentrál, amelyre a jelenkorban Iránhoz és az ellenállás tengelyéhez tartozó proxykon, különösen a Hezbollah irányából számított. Izrael a stratégiai tervezés szintjén alapvetően egy északi háborúval tervezett, amelynek során a libanoni és szíriai területek felől érkezett volna a fő támadás, míg az Irak területén működő síita milíciák, a Jemen északnyugati részét uraló húszik, a palesztin terrorszervezetek és az iráni területről indított támadások a földrajzi távolság miatt kiegészítő szerepet játszottak volna.[13] A háborút alapvetően aszimmetrikus eszközökkel végrehajtott támadásként képzelték el az izraeli tervezők, főként az izraeli kritikus infrastruktúra és polgári központok ellen végrehajtott tömeges, túlterheléses ballisztikus rakéta- és dróntámadás keretében, főként a Hezbollah mintegy százötvenezres, részben precíziós rakétaarzenáljára építve, a Hamász azonban másodlagos szerepet játszott volna.[14] A szárazföldi behatolás mint módszer is csak kiegészítő eszközként merült fel, itt is főként a Hezbollah úgynevezett Radwan Erők által végrehajtott betörés képében.[15] A fő kérdés az volt, hogy Irán kizárólag proxykon keresztül támadna, vagy közvetlenül részt venne a támadásban, valamint hogy milyen szerepet játszanának a Forradalmi Gárda erői.[16]

A palesztin front tehát természetesen része volt az izraeli tervezésnek, azonban visszatekintve két alapvető feltételezésük hibás volt. Az első, hogy alapvető doktrinális szinten a döntő katonai győzelem elérése és a megelőző támadásokra építő stratégia helyett az ellenségekkel szembeni elrettentés sikerre vezethet.[17] Ezzel összefüggésben tehát az izraeli vezetés hibásan feltételezte, hogy sikerült elérni a Hamász elrettentését és viszonylagos pacifikálását.[18] Benjamin Netanjahu stratégiája, a „kívülről befelé" zajló közel-keleti békefolyamat részeként alapvető fontosságú cél volt a palesztin megosztottság fenntartása és mindkét fő erő, a Fatah és Hamász pacifikálása. A cél és a valóságérzékelés összekeveredett és az izraeli vezetés nem számolt azzal, hogy a Hamász egyáltalán nincs elrettentve.[19] Ezt jelzi, hogy Cahi Hanegbi, az izraeli Nemzetbiztonsági Tanács feje még a támadást megelőző napokban is kijelentette, hogy a Hamászt a következő másfél évtizedre sikerült elrettenteni.[20] A stratégiai tervezés és hírszerzési tévedések komplex rendszerét kiegészítette, hogy mindezzel együtt nem nevezhetjük teljesen naivnak az izraeli vezetést, hiszen azzal tisztában voltak, hogy a Hamász nem hagyott fel a terrorista szervezkedéssel és tevékenységgel,

[13] MIZRAHI – DEKEL – BAZAK (2021) 14.
[14] MAHMOUDIAN (2023)
[15] LAPIN (2023)
[16] MIZRAHI – DEKEL – BAZAK (2021): 25.
[17] FREILICH (2018): 366.
[18] LUPOVICI (2024): 74–75.
[19] BREUER (2024)
[20] KAHAV (2023)

azonban fő céljuknak a ciszjordániai képességeik kiépítését és a Fatah uralmának megdöntését tartották, nem a közvetlen támadást a Gázai övezettel szomszédos izraeli területekkel szemben. Összességében tehát a Hamász tevékenységét és egy háborúban játszott szerepét Izrael félrekalkulálta, kiegészítő és alapvetően passzív szerepet tulajdonított nekik, nem kezdeményezőkészséget.

A Hamász oldalán ezzel szemben, a terrorszervezet szempontjából sikerült az izraeli katonai és politikai döntéshozókat megtéveszteni. Az első szempont, hogy gyakorlatilag egy „ördögi kört" alkotva a vágyvezérelt izraeli értékelésekkel a Hamász sikeresen hitette el Izraellel, hogy az elmúlt években sikerült kialakítani valamiféle *status quot,* amelyet a Hamász sem kíván kockáztatni. A 2021-es válság idején a Hamász a Templom-hegyen történő izraeli tevékenységre válaszul tizenkét napos rakétatámadás-kampányt indított, amelyet tűzszünet zárt le.[21] Nem volt szárazföldi áttörés, nem jelentek meg azok a képességek, amelyek mindösszesen két év múlva sokkolták az izraeli haderőt. A Hamász látszólag belesimult a Gázai övezet kormányzásának szerepébe és arról érkeztek hírek, hogy milyen kihívást jelentenek a Hamász számára a még radikálisabb dzsihádista szervezetek, mint a Palesztin Iszlám Dzsihád és az Iszlám Állam helyi leágazásai. Mind az izraeli, mind a nemzetközi értékelések döntően azon az álláspontón voltak, hogy a Hamász pragmatikus szervezet, amely a Gázai övezet kormányzása érdekében tartózkodik az önpusztító, tömeges terrortámadások stratégiájától.[22] Annak ellenére tudta a Hamász ezt a képet sugározni, hogy gázai vezetője 2017-ben Jahja esz-Szinvár lett, aki a szervezet radikális szárnyát képviselte, ennek ellenére, vagy mint mára tudjuk éppen ezért, a 2017-2023-ig tartó hat év Izrael szempontjából az egyik legnyugodtabb időszaknak tekinthető.

A gázai fronthoz kapcsolódó „elrettentséget" kiegészítette a Hamász elterelő magatartása, amelyben a Ciszjordániában létrehozott terrorista sejtek elvonták az izraeli haderő figyelmét. Az elterelés éppen azért lehetett sikeres, mert a Hamász szempontjából teljesen logikusnak tűnt a korruptnak tekintett Fatah destabilizálására és megbuktatására irányuló terv és az izraeli telepesek és haderő tevékenysége folytán agitált ciszjordániai palesztinok toborzása az Izrael elleni terrorista harchoz. Feltehetően két célt is szolgált a ciszjordániai tevékenység, egyrészt az említett figyelemelterelést Gázáról, másrészt valós képességeket építeni a tervezett Izraellel szembeni terroroffenzívához, annak érdekében, hogy több frontra széthúzzák az izraeli biztonsági erőket.

[21] FELDMAN (2021)
[22] PARAGI (2024): 80.

Végezetül ki kell emelni, hogy a Hamász támadásra való készülése ugyan titokban folyt, azonban nem sikerült és feltehetőleg nem is volt cél teljes mértékben eltitkolni annak elemeit. Ennek két egymásra épülő oka lehet. Az első, hogy bár az izraeli hírszerzés mulasztása kétségtelen, azonban azt nem feltételezhetjük, hogy minden egyes kiképzési és logisztikai elem elkerülte a figyelmüket. A lényeg a Hamász szempontjából, az volt, hogy az átfogó támadás tervét ne tudják vagy ne akarják az izraeli hírszerzés keretében összerakni, ami sikerült is. Másodsorban nem is lett volna életszerű, hogy a több tízezer fegyveressel rendelkező Hamász éveken át semmilyen katonai kiképzést, gyakorlatozást nem végez. Ezt azonban az izraeliek elkönyvelték hazai fogyasztásra felhasználható tevékenységnek, amelyet a korrupt Hamász vezetés a militáns elemek elhallgattatására, mintegy pótcselekvésként végez. Összességében tehát a Hamász stratégiája nem lehetett volna sikeres az izraeli politikai és katonai vezetés téves kalkulációi és vágyvezért értékelése nélkül, amelyhez azonban a Hamász sikeresen szolgált illeszkedő, megtévesztő alapokat.

A Hamász háború előtti stratégiája kapcsán a legfontosabb azonban leszögezni, hogy nemhogy el lett volna rettentve, de a Hamász célja valójában sosem változott. Minden eltérő jelzés ellenére ugyanaz a terrorszervezet maradt, amely Izrael elpusztítására törekedett. Ez nem jelenti azt, hogy ne lehettek volna, különösen a Katarban élő Hamász vezetők között viszonylag mérsékeltebb hangok. Mindazonáltal Izrael el és megtűrte határai mellett Szinvár radikális vezetése alatt egy terrorszervezet előkészületeit egy nagyfokú mészárlásra. Nem hajtott végre a Hamász erői ellen a Gázai övezetben a szíriai fenyegetések elhárítása érdekében alkalmazott „hadjárat a háborúk között”[23] eljáráshoz hasonló megelőző támadásokat, mivel nem kívánta kockáztatni a *status quot*. Ez a súlyos mulasztás összességében fontos tanulság mind Izrael, mind a világ államai számára.

2.2. A HARCOK LEFOLYÁSÁNAK TANULSÁGAI

A következőkben az Izrael határain és szomszédos területeken lezajló háború tapasztalatait és tanulságait elemzem. A háború kitörését közvetlenül megelőző intézkedésektől, és a csapatmozgásoktól kezdődően a gázai szárazföldi offenzíván át a 2024 november végéig tartó eseményeket vizsgálom. Röviden kitérek a Ciszjordániában és Izrael szuverén területén zajló eseményekre. A konfliktus libanoni és iráni vetületeit a következő, regionális kontextust elemző részben vizsgálom. A jelen kutatás célja nem a háború hadtörténeti szintű dokumentálása, hanem az események olyan mértékű ismertetése, amennyiben azok szorosan kapcsolódnak a terrorelhárítással összefüggő tapasztalatokhoz.

[23] CSEPREGI (2023): 35–48.

2.2.1 A támadást megelőző helyzet

A 2023 őszét megelőző izraeli biztonsági helyzettel kapcsolatban három kulcskérdést kell vizsgálni. Az első, hogy igazak-e azok a vádak, amelyek általános katonai felkészületlenségre mutattak rá Izrael esetében. A második, hogy hol helyezkedtek el az izraeli csapatok, amelyeknek a Hamász egy esetleges betörését kellett volna megállítaniuk. A harmadik, hogy érkezett-e figyelmeztetés a támadásról, és ha igen, akkor ezalapján miért nem rendeltek el magasabb készültségi szintet.

Az első kérdés kapcsán megállapítom, hogy a lecsökkent izraeli katonai képességek kapcsán és ezzel implicit az izraeli belpolitikai válság hatását hangsúlyozó vélemények hibásak. Az izraeli válság 2023 márciusában érte el a csúcsát, amikor az igazságügyi reform miatt egyre több IDF egység tagadta meg különböző formákban a fegyveres szolgálat bizonyos járulékos részeit (például gyakorlatozás). A reformtörekvések biztonságra gyakorolt negatív hatásának nyilvános kritizálása miatt Joáv Gallant védelmi minisztert Benjamin Netanjahu menesztette, aminek hatására nagyszabású tüntetések robbantak ki és a kormánynak meg kellett hátrálnia.[24] Ezt követően 2023 őszéig tehát kényes patthelyzet alakult ki az izraeli belpolitikában, Netanjahu és szövetségesei várták az alkalmat, hogy újra bevezethessék az igazságügyi reformelképzeléseiket, míg az ellenzék igyekezett ettől továbbra is politikai eszközökkel elrettenteni a kormányt. A szolgálatot megtagadó, vagy feltételekhez kötő tartalékosok száma 2023 július végén mintegy tízezer fő volt a négyszázezer fős keretből, tehát nem érte el a három százalékot sem.[25] A Hamász támadása tehát nem a belpolitikai válság csúcsát használta ki, nem lehet ilyen egyszerű választ adni a kudarc okaira. Ugyanakkor egy belpolitikai válság természetesen nem használ a hadseregnek és a nemzetbiztonsági szerveknek, de közvetlen összefüggést nem lehet vonni, hiszen nem arról volt szó, hogy a gázai határ védelmét szolgáló erők vagy az ellenőrzést végző szervek megtagadták volna a szolgálatot és ezért lett porózus a határ.

A második kérdés kapcsán, hogy hol helyezkedtek el a csapatok, három megállapítás tehető. Az első, hogy jelentős részük otthon, családjuknál tartózkodott, mivel Szimhát Tóra ünnepére nagyarányú eltávot engedélyeztek a déli erőknél is. Tehát a Hamász, ha a belpolitikai válság csúcsát nem, a zsidó őszi ünnepi idény alatt mutatott gyengeséget kihasználta a támadás időzítésével. Az izraeli csapatok másik jelentős része a megnövekedett feszültségek, izraeli telepesek és palesztinok között zajló zavargások miatt Ciszjordániába

[24] JEWISH NEWS SYNDICATE (2023)
[25] EBRAHIM – TEL – KREVER (2023)

lettek vezényelve.[26] A ciszjordániai hatalmi vákuum és az izraeli kormány bizonyos elemeinek politikája hozzájárult a konfliktus eszkalálódásához. Így jelentős erők lettek átcsoportosítva a ciszjordániai területek ellenőrzése és pacifikálása céljából, ami valóban elterelte a fókuszt a gázai határról. Ebben a Hamász szerepe indirekt módon mutatható ki, hiszen évek óta hozzájárult a ciszjordániai biztonsági helyzet erodálásához a terrorista sejtek támogatásával, kiépítésével. A ciszjordániai csapaterősítések és az ünnepi eltávok együttesen azt jelentették tehát, hogy elégtelen mennyiségű és minőségű katonai erő maradt volna a gázai határon, hogy a Hamász támadását megállítsák? A végkimenetel szempontjából mindenképpen, hiszen a Hamász képes volt végrehajtani a támadást. A rendelkezésre álló információk szerint azonban nem a mennyiséggel volt az alapvető probléma, hanem az izraeli katonai és biztonsági erők pozícionálásával, készültségével és vezénylésével.[27] Ez pedig arra utal, hogy nem a rendelkezésre álló erőforrásokban, hanem tervezésben, hírszerzési és értékelési és parancskiadási hibák okozták az izraeli oldal kudarcát.

Harmadrészt, tehát ha nem belpolitikai káosz és nem a katonai erő abszolút hiánya tette lehetővé a támadást, akkor miért nem működtek megfelelően az izraeli hírszerzési szervek, miért nem jelezték előre a támadást, hogy a rendelkezésre álló izraeli erők megfelelő felkészültségben várhassák a támadást, vagy akár megelőző csapást mérjenek a Hamászra október 6. éjszaka? A jelenlegi ismereteink szerint az izraeliek tisztában voltak vele, hogy a Hamász erői kiképzést folytatnak és ismerték a támadásra vonatkozó elképzelések körvonalait is.[28] Az október eleji időszakra tervezett Hamász műveletről is rendelkeztek információkkal, azonban mindezen elemek nem álltak össze olyan képpé, amelynek alapján kiadták volna a megfelelő utasításokat, készenlétbe helyezték volna a határvédelmi egységeket és erősítést rendeltek volna a támadás előtt. Látható tehát, hogy alapvetően egy felülről-lefelé történő rendszerhibák alkotta sorozat okozta az október 7-re beérő izraeli tragédiát. Az összegyűlő információk kiértékelése a dogmatikus alapfelvetések miatt nem indította el a teljes kép megszerzéséhez szükséges további részletek megszerzésére irányuló információgyűjtést.[29] Izrael alapvetően egy-egy behatolásra és nem inváziót számított, ennek eredményeként nem alakították ki a megfelelő eljárásokat az október 7-i terrortámadáshoz hasonló műveletek elhárítására.[30] Ez az alapfeltételezés pedig meghatározta a hírszerzési ciklus működését és kódolta a szisztematikus hibák elkövetését.

[26] TARNOPOLSKY – RUBIN (2023)
[27] GAT (2024)
[28] ORTAL (2024): 9.
[29] KIRCHWEGER (2024):5.
[30] LAISH (2024): 4–5.

2.2.2. A Hamász támadás eseményei

Október 7. szombat hajnalban, 6.30-kor a Hamász és kisebb részben Palesztin Iszlám Dzsihád több ezer rakétát indított Izraelre, amelynek ernyője alatt a következő órában megindult a terroristák első hulláma, több ponton áttörve az Izraelt és a Gázai övezetet elválasztó határkerítést, megkezdve a zsidó állam történetének legnagyobb és globális szinten az egyik legjelentősebb terrortámadást. A támadók több hullámban hatoltak be, a beszivárgási szintet jelentősen meghaladva, egyfajta terrorista inváziót végrehajtva. A becslések jelentősen eltérnek a támadók száma kapcsán, kezdetben mintegy 2-3000 főre tették az izraeli források az Izraelbe áttörő erőket, de 2024. augusztusában új izraeli becslések már 7000 főre tették a közvetlenül résztvevő Hamász és PIJ erők számát és mintegy ezer főre, akik a Gázai övezetből végezték a nagyszabású ballisztikus rakétatámadásokat Izraellel szemben.[31] A terroristák célpontjai közül négyet emelek ki, a gázai határ mellett lévő kibucokat, a Re'im katonai bázist, a Nova Fesztivált és Szderót városát. Összességében elmondható, hogy a Hamász támadásának sikerült megvakítania a fejlett izraeli eszközrendszert a határon, fizikailag gyorsan átszakítani a határkerítést és gyorsmozgású erőkkel hamar behatolni a szomszédos izraeli területekre.

Fontos viszont már a támadás vizsgálatának legelején leszögezni, hogy a Hamász és PIJ támadóerők önmagukban nem voltak képesek Izrael létét fenyegetni. Egy közel tízmilliós közel-keleti katonai nagyhatalmat, a világ leginkább militarizált országát néhány ezer terrorista nem képes elfoglalni. A Hamász terrortámadása, hangsúlyozom, hogy önmagában, a hármas szintű izraeli biztonsági fenyegetés skálán a rutin és létért vívott háborús szint között a vészhelyzeti kategóriába esik. Ez azonban nincs ellentétben azzal, hogy Izrael létfenyegetésnek fogja fel a háború egészét, a Hamász terrorakcióját és az ellenállás tengelyének többi tagjának támadásait és feltételezhető offenzíváját egybevéve.[32] Először megvizsgálom az izraeli védelem hibáit, majd bemutatom, hogy milyen kapcsolat áll fenn a kezdeti inváziós terrortámadás és az izraeli létért vívott háború narratívája között.

A korábbiakban ismertettem, hogy az izraeli oldalon alapvető tervezési és hírszerzési hibákat követtek el, amelyek miatt nem voltak megfelelően felkészülve a Hamász támadásának konkrét előrejelzésére és az arra való felkészülésben. Milyen fizikai megjelenési formát öltött ez a mulasztás október 7. reggelén a négy kiemelt izraeli célpont-kategória esetében? Először a kibucokkal kezdem, amelyek már évtizedek óta a cionista ethosz alapvetéseit jelentették és az „Ígéret Földjének" munkával való újra birtokbavételének

[31] JEWISH NEWS SYNDICATE (2024a)
[32] SHAMIR (2024) 3.

szimbólumai. A gázai határon, Izrael szuverén területén, ezek a kis települések jelzik a zsidó állam és nép földrajzi kiterjedését. Ezek a települések rendkívül kitettek mindenfajta támadásnak, ha a határt sikeresen áttörné vagy ott beszivárogna az ellenség. Ennek eredményeként minden közösségnek elvileg lakosokból, fizetett biztonsági személyzetből és sorozott katonákból álló önálló védelmi ereje van, ami feltartja a támadókat, amíg a haderő csapatai megérkeznek felmenteni a települést. Ez a legtöbb helyen nem működött megfelelően és a kibucok lakosai már azt vették észre, hogy a terroristák betörtek a településekre, motorbicikliken érkezve gyilkoltak, kegyetlenkedtek és túszokat ejtettek.[33] Súlyos mulasztás az izraeli hatóságok részéről, hogy a téves helyzetértékelés miatt hagyták, hogy a Gázai övezet melletti kibucok védelme ilyen szinten degradálódjon az évek alatt, miközben tőlük öt kilométerre, a határ túloldalán egy dzsihádista terrorszervezet uralkodott. A mulasztás mértékét nem csak az embertelen pusztítás mutatja, amit a Hamász terroristái elkövettek a szinte védtelen kibucokban, hanem a sikeres védelemhez szükséges korlátozott erőforrások példái is. Sufa kibucában hat fegyveres lakos tartott fel harminc terroristát, amíg a hadsereg megérkezett.[34] Be'eriben háromszoros túlerővel szemben, 340 terrorista ellen harcolt a lakosokból és katonákból álló izraeli védelem, stabilizálták a frontot, amíg a haderő megtisztította a települést.[35] A kibucok védelmének fejlesztését, fenntartását súlyosan elhanyagolta az izraeli állam, ami a jelenlegi ismeretek fényében megmagyarázhatatlan. A védelem elhanyagolása mellett pedig figyelmeztetést sem kaptak időben.

Valójában ugyanerre a hibára lehet rámutatni a másik három kiemelt célpont kapcsán is. A Nova zenei fesztivált soha nem szabadott volna engedélyezni a gázai határ mellett, kérdéses, hogy egyáltalán meg lehetett-e volna védeni a helyszínt, de tekintettel arra, hogy hasonló, Izraelben divatos sivatagi koncertre mennyi hely áll rendelkezésre a Negev-sivatag belsejében, a reális helyzetértékelés rendkívüli hiányát mutatta a Hamász területétől motorral néhány percen belül elérhető helyre tenni egy nagyszabású fesztivált. Szderót városát, amely a Gázai övezet mellett fekvő teleülések központja, ugyancsak lerohanták a terrorista erők, amelyben a rendőrkapitányság szolgált erődként az izraeli védekezők számára. A védelmezők azonban átmenetileg elbuktak és összesen mintegy hetvenkét halálos áldozatot szenvedtek a településen. Az izraeli válasz keménységét jelzi, hogy az elfoglalt rendőrőrsöt végül az izraeli erők buldózerrel elpusztították, megölve benne az összes terroristát.[36] Tekintettel arra, hogy a település harminchárom ezer lakosú volt, ennél jóval nagyobb katasztrófa is történhetett volna.

[33] KINGSLEY – BOXERMAN – SOBELMAN (2023)
[34] YAGNA (2023)
[35] IZRAELI VÉDELMI ERŐK (2023a)
[36] STEINBERG (2024)

Megint csak látható, hogy egy ilyen kitett, határmenti település se rendelkezett megfelelő védelmi rendszerrel. Rá kell mutatni Szderót esetében, hogy a város az izraeli rakétavédelem egyszerre szimbolikus és gyakorlati központja is volt, mindig több és jobb óvóhelyet követeltek a lakosok, azonban látszólag semmibe vették az invázió és beszivárgás jelentette veszélyforrást. Végezetül semmi nem mutatja jobban az izraeli védelem mulasztását, mint a Re'im katonai bázison történt harcok, ahol a magukat a katonákat is meglepte a támadás. A Re'im bázis felkészületlensége a hiba gyökere, hiszen a támaszpont a Gáza hadosztály, valamint a drón és megfigyelőrendszerek egyik központja is.[37] A tizenkét órán át tartó harcokban ismeretlen számú izraeli katonai esett el, jelezve, hogy a viszonylag „puha" célpontok mellett a katonai létesítmények sem voltak felkészülve. A különbségtétel azonban nem lényeges, a valódi tanulság a már bekövetkezett támadásból kiindulva, hogy egy terrorszervezet bázisa mellett semmilyen, sem katonai, sem civil célpont nem lehet „puha".

2.2.3. Háború kibontakozása és a gázai offenzíva

A támadók döntő részét sikerült a Gázai övezethez legközelebb eső településeken feltartóztatni, igaz, igen nagy áldozatok mellett, több mint 1200 izraeli élete és a 250 túsz elhurcolása árán. Az izraeli rendőrség és katonaság fokozatosan, a terrortámadást követő órákban átvette a kezdeményezést, visszaszorította a terroristákat és október 8. estére már csak elszórtan maradtak megbúvó terroristák Izrael területén. A védelem egyik ikonikus példája volt a Hiúz zászlóalj négy Merkava tankból és egy Namer páncélozott csapatszállító harcjárműből álló női egysége, amely azonnal reagált az invázióra és mintegy ötven terroristát öltek meg tizenhét órán át tartó harcok során, jelentős részüket egyszerűen széttaposva a több mint hatvan tonnás harcjárműveik lánctalpaik alatt.[38] Az izraeli sajtót is bejárta a történet, nemcsak a női határvédelmi célú harcoló alakulatok jövőbeli fontosságát aláhúzva, hanem hogy megfelelő felkészülés mellett a katonai nagyhatalom képességei mellett a támadás nem jelenthetett volna komoly kihívást. Ez azonban összességében nem így történt, hanem a kezdeti órák általános kudarcában fedezhetünk fel kiváló egyéni és alegység szintű teljesítményeket.

A felső szinten az izraeli vezetés hadiállapotot hirdetett, visszamenőleg 2023. október 7-én 6:00-tól.[39] Ez lehetővé tette a nagyarányú mozgósítást és a különleges jogi lépések bevezetését.[40] A mozgósítás keretében a reguláris és sorkatonai szolgálatukat töltő katonák

[37] NEW YORK TIMES (2023)
[38] I24NEWS ENGLISH (2023)
[39] IZRAELI MINISZTERELNÖKI HIVATAL (2023)
[40] KONGRESSZUSI KÖNYVTÁR (2023)

mellé a 360 ezer fős jóváhagyott mozgósítási keretből mintegy 220 ezer tartalékos katonát hívták be.[41] Ezzel átmenetileg Izrael rendelkezett a világ egyik legnagyobb fegyverben lévő erejével, ami természetszerűleg meghatározta az ország lehetőségeit. A különleges intézkedések keretében evakuálták a déli határvidéket, majd a libanoni Hezbollah rakétacsapásai és várt eszkalációja kapcsán az északi határ melletti településeket is. Összesen mintegy kétszázezer izraeli polgárnak kellett elhagynia az otthonát. A háborús készültség és mozgósítást lehetővé tevő szabályozás keretében meg kell említeni, hogy a csapatmozgásokat akadályozó személyeket, legyenek azok tüntetők vagy szabotőrök éles lőszerrel is lehet oszlatni, likvidálni. Tekintetbe véve, hogy a kezdeti becslések szerint néhány ezer fős Hamász erő tört be Izraelbe és sikerült őket megállítani a határtól legfeljebb húsz kilométerre, miért váltott Izrael szinte teljes háborús mozgósításra? A válasz, hogy Izrael nem az eredeti, vészhelyzeti szintet elérő terrortámadásra reagált csupán, hanem meg kívánta előzni a létért vívott háború kitörését, illetve erre a forgatókönyvre felkészülni.

Amint tehát a mozgósítás elkezdődött és az első 220 ezer tartalékost behívták, azok jelentős része az északi határra került, egy esetleges Hezbollah és Szíria felől indított offenzíva feltartóztatására. Ciszjordániából se vonták el az erőket, mivel tartottak egyrészt a Hamász helyi terrorista sejtjeinek aktiválódásától, másrészt ezen túlmenően egy általános felkeléstől, akár a harmadik intifáda kitörésétől. Összességében tehát Izrael egy többfrontos, Izrael létét fenyegető támadástól tartott. Az izraeli stratégiai tervezésben nem volt helye egy, a Hamász által önállóan indított nagyszabású terrortámadásnak, csak abban az esetben, ha az el kívánja terelni a figyelmet a többi frontról, elvonni az izraeli erőket, hogy aztán az északi és keleti irányból bénító erejű, adott esetben megsemmisítő támadást indíthasson az ellenállás tengelye. Mindez kiegészülne az izraeli arabság felkelésével, amelyre a kezdeti félelmek ellenére ugyancsak nem került sor a háború alatt. Jelenleg nincsenek ismereteink azzal kapcsolatban, hogy az iráni tengely tervezett volna második, elsöprő erejű támadással a Hamász terrortámadásra építve, azonban mégsem jelenthetjük ki, hogy az izraeli vélekedés hibás lett volna. Amennyiben Izrael ellenségei erő helyett gyengeséget érzékeltek volna az északi és keleti fronton, úgy megkísérelhettek volna építeni a támadásra, ami már a háború kezdeti szakaszában beláthatatlan kimenetelű eszkalációhoz vezethetett volna. Tehát míg a háború előtti és a Gázai övezet melletti izraeli erők fellépését kritikával illettem, addig a többi (részben feltételezett) frontra vonatkozó izraeli reagálást megfelelő és racionális válaszadásnak tartom.

[41] HEIMANN (2024)

A Hezbollah és más Iránhoz hű erők képességeikhez mérten korlátozott mértékben vették ki a részüket a harcokból, szárazföldi támadásra pedig nem került sor más országok felől.[42] A ciszjordániai terrorista tevékenység eszkalációját a későbbiekben röviden elemzem, azonban leszögezhető, hogy nem került sor a gázaihoz hasonló ciszjordániai inváziór, sem harmadik intifádára. Izrael tehát koncentrálhatott az alapvető problémára, a Hamásszal szembeni harcra. A háború célja hivatalosan a Hamász teljes megsemmisítése, a túszok kiszabadítása volt.[43] Mindez alapvető mértékben különbözik a korábbi „fűnyíró" konfliktusköröktől, amelyek célja a Hamász meggyengítése és elrettentése volt, de nem a döntő győzelem.[44] Az október 7-én elkövetett Hamász terrortámadás Izrael vezetése részéről, szimbiózisban a társadalom elvárásával, a terrorszervezet felszámolását tűzte ki célul annak minden járulékos következményével együtt.

Az izraeli vezetés október 7-ét követően komoly döntéshelyzet elé került, miszerint átfogó szárazföldi offenzívát is indítson a Gázai övezet megtisztítása érdekében, vagy csupán korlátozott szárazföldi manővereket alkalmazzon és alapvetően légierővel igyekezzen válaszolni a Hamász támadására. Utóbbi lehetőség nagyban hasonlított volna a korábbi konfliktuskörökhöz, amelyek célja a Hamász meggyengítése és átmeneti elrettentése volt. A háborús cél, azaz a Hamász teljes elpusztítása végső soron azonban kizárta a totális szárazföldi offenzívától eltérő megoldásokat.[45] Itt szükséges megállni és kiemelni, hogy ugyan a háborús cél igen konkrétnak tűnt az első napokban, azonban nem került pontos definiálásra, mit jelent a Hamász teljes elpusztítása. Minden egyes terrorista meggyilkolását jelenti-e, vagy csak a vezetőkét és a Hamász képességeinek felmorzsolásához szükséges élőerő likvidálását? Ha szétbontjuk a Hamászt katonai, gerilla és terrorista képességekkel rendelkező szintekre (ami csak elméletben tehető meg) meddig kell degradálni az erőit, hogy Izrael befejezettnek tekintse a küldetést? Valójában sosem került pontosan definiálva mit is jelent a gyakorlatban a háborús cél megvalósítása, azonban több mint egy év távlatában kijelenthető, hogy az összes vezető meggyilkolása és mint katonai és kormányzati szervezet (utóbbi a Hamász hibrid jellege miatt fontos) elpusztítása és gerilla és terrorszervezetként radikális meggyengítése volt a cél a túszok kiszabadítása mellett.

Az izraeli politikai vezetés tehát a háborús cél megvalósítása érdekében a mozgósítás nyomán közel félmilliósra bővült fegyverben álló erő mintegy egyötödét, négy hadosztályt[46],

[42] MIZRAHI – SCHWEITZER (2024)
[43] SATLOFF – ROSS – MAKOVSKY (2023)
[44] SHABTAI (2024): 1.
[45] LAISH (2024): 6.
[46] GAT (2024)

így akár százezer katonát vont össze a Gázai övezet határainál, majd október 13-án megkezdte a fokozatos bevonulást a Gázai övezetbe. A részletes bemutatástól eltekintek, azonban érdemes kiemelni, hogy egy lépcsőzetes hadművelet zajlott, ahol először elvágták az északi részt, majd azt tisztította meg Izrael, fokozatosan haladva dél felé. Körbevette a nagyobb városi gócokat, ostrom alá vette őket és szisztematikusan semmisítette meg a Hamász élőerejét, erődített állásait és alagútrendszereit. A harcoknak két fontos tanulsága van. Az első, hogy bár, mint említettem a Gázában harcoló katonák gyakorlatilag töredékét teszik ki az IDF mozgósítást követő létszámának, mégis, ilyen mennyiségű jól kiképzett szárazföldi katona bevetése meghaladja a világ legtöbb államának lehetőségeit. A másik kiemelendő tényező, hogy a militáns és terrorszervezetekkel szemben bevetendő haderő nemzetközi mintáitól rendkívül eltér a gázai művelet, legfeljebb az Iszlám Állammal szemben Rakkában és más iraki nagyvárosokban került sor hasonló összecsapásokra. A jellemzőbb, hogy alapvetően vidékies területen végez az adott ország katonai ereje műveleteket, nem pedig betonból épült magasházakkal sűrűn beépített területeken. Gyakran elhangzik, hogy a Gázai övezet nem nagyobb, mint Budapest harmada, ez azonban nem von le a katonai kihívás mértékéből. Jelenleg nem tudunk más hasonlóan sűrűn beépített területről, amely egy adott terrorszervezett uralma alatt állna, azonban a jövőben ez rendkívüli kihívást jelenthet a világ haderői számára, ezért is fontos példa a gázai offenzíva. Az izraeli haderő veszteségei a kezdeti félelmek ellenére viszonylag alacsonyak maradtak, a harcok egy éve során Gázában mintegy 378 izraeli katona vesztette életét.[47] Ez egyrészt jelzi az izraeli haderő felkészültségét, emellett azt, hogy nem szabad fatalista módon megközelíteni a hasonló hadműveletek veszélyességét, ez megfelelő tervezés, felszerelés és vezetés mellett leküzdhető.

Az izraeli haderő műveleti sikerei és aránylag alacsony veszteségei nem jelentik azt, hogy ne lenne a Gázai övezet egy rendkívül összetett és veszélyes műveleti terület. A Hamásznak közel tíz éve állt rendelkezésre, hogy gyakorlatilag zavartalanul erődítse a lakott területeket, berendezze rakétakilövő állomásait, rajtaütési pontokat építsen ki és alagútrendszert, az úgynevezett „gázai metrót” kialakítsa az övezet alatt. Minden arra szolgált, hogy aszimmetrikus eszközökkel valamifajta paritást érjen el harci érték tekintetében az Izraeli Védelmi Erőkkel szemben. Mindez azonban a legkevésbé sem állította meg, legfeljebb csak lassította az izraeli csapatokat. Fontos hangsúlyozni, hogy hosszú hónapok álltak rendelkezésére Izraelnek, hogy saját ütemterve szerint haladjon előre, senki nem

[47] FABIAN (2024)

kényszerítette tűzszünetre és a zsidó állam nem egy nemzetközi koalíció, amely előbb vagy utóbb ki akarja vonni erőit még a térségből is, Izrael léte a Közel-Kelet megkerülhetetlen adottsága. Ez azt is jelenti ugyanakkor, hogy a kezdeti remények a gyors legfolyású büntetőhadjárattal kapcsolatban az események ismeretében teljes fantazmagóriáknak tűnnek. Ez mindenképpen eltérő megközelítésre utal a hagyományosan gyorsan döntő győzelmet elérni kívánó izraeli katonai stratégiához képest és egy viszonylag lassú, szisztematikus, az ellenséget fizikailag megsemmisíteni kívánó eljárás felé való elmozdulást jelent.[48] A szárazföldi offenzíva mellett fontos hangsúlyozni, hogy a légierő és haditengerészet is kivette és a mai napig kiveszi a részét a műveletekben, gyakorlatilag egy fejlett, összhaderőnemi hadműveletet valósítva meg egy városgócokat uralma alatt tartó terrorszervezettel szemben. Az egyik legfontosabb aspektusa a hadjáratnak a Hamász vezetőinek likvidálása, mivel bár a háborús célok kapcsán fogalmaztam meg kritikát a definiálatlanság kapcsán, az nem volt kétséges, hogy Izrael célja az összes gázai Hamász vezető megölése. Ezt a célt gyakorlatilag sikerült elérni az eltelt egy év során.[49]

A kezdeti terrortámadást követően a nemzetközi közösség fókusza hamar az izraeli ellentámadás humanitárius következményeire került át. Meg kell vizsgálni az állítólagos palesztin civil áldozatok számát és arányát, a segélyek kérdését és a civil épületek használatának problematikáját. A halálos áldozatokkal kapcsolatban elmondható, hogy a Hamász irányítása alatt álló, kellő óvatossággal kezelendő gázai források szerint több mint negyvenezer palesztin személy vesztette életét az izraeli offenzívából eredően.[50] Az egyes források eltérnek azzal kapcsolatban, hogy a halottak milyen arányban voltak a Hamász és a PIJ terroristái és mennyi volt a civil áldozat. Izraeli források nagyjából 1:1,4 arányban teszik a militánsok és civil halottak arányát.[51] Az Izraelt kritizáló és elítélő nemzetközi hangot ezzel kapcsolatban a háborús bűnök vádját is felvetik. Izraelt természetszerűleg kötelezi a hadijog még egy terrorszervezettel szemben vívott küzdelem esetén is. Ez azonban nem jelenti, hogy a Hamász megsemmisítése során életüket vesztő civilek száma alapján lehetne következtetni háborús bűnökre, az arányosság elvét kell követni, amely azonban nem egy abszolút szám.[52] Izrael fő szövetségesei, kiemelten az Egyesült Államok bár komoly büntetést nem helyeztek kilátásba Izraellel szemben, azonban a zsidó államnak folyamatos nemzetközi nyomásgyakorlás alatt kell vívnia küzdelmét a Hamásszal szemben. Ez egyrészt természetes

[48] ORION (2024)
[49] BBC (2024)
[50] TÜRK (2024)
[51] HECHT (2024)
[52] YOO – RABKIN (2024): 8.

és normális velejárója minden fegyveres konfliktusnak, másrészt aláhúzza, hogy a terrorellenes küzdelemben is milyen fontos a stabil diplomáciai háttér, amely még a kényes körülmények között is képes biztosítani a külső támogatást és a külső szereplőktől elszenvedhető károk minimalizálását.

A helyzetet bonyolítja a Hamász széles körben alkalmazott és jól dokumentált „élő pajzs" eljárása, amelyben katonai és terrorista infrastruktúráját civil célpontokba vagy azokhoz közel telepíti, legyenek ezek kórházak vagy iskolák.[53] Egy évet követően látható, hogy ez az izraeli hadsereggel szemben kevés elrettentőerőt képvisel (bár nem tudjuk milyen célpontokat nem lőttek az izraeliek, csak arról tudunk, amit eléggé fontosnak értékeltek, hogy vállalják a járulékos károkat). A civil áldozatok számának csökkentése érdekében az izraeli haderő evakuálta a műveleti alterületeket, előbb a Gázai övezet északi részét ürítve ki, majd szisztematikusan, szektoronként irányítva a lakosságot, hogy a Hamász állások „pajzs" nélkül maradjanak. Ez önmagában is a humanitárius helyzet súlyos degradálásához vezet ilyen sűrűn lakott területeken.[54] Továbbá izraeli források szerint[55] a Hamász fegyveresen akadályozta a civilek menekülését.[56] Az élő pajzsok használata minden szinten a jövőben is nehezíteni fogja a demokratikus államok terrorista szervezetekkel szembeni harcát, és bár Izraelt nem tudták a nemzetközi ellenkezések megállítani, egy régión kívüli ország közvéleménye kétséges, hogy hasonló művelet esetén ne fordult volna a kormányával szembe.

Végezetül meg kell említeni a segélyszállítmányok problematikáját, mivel azokat egyrészt Izraelnek kötelessége átengedni a nemzetközi hadijog alapján, azonban másik oldalon ezzel az egyetlen kormányzásra képes erőt, a Hamászt is támogatja, amely gyakran sikeresen szerzi meg a szállítmányokat és használhatja fel hatalmának megőrzése céljából.[57] A nemzetközi közvélemény nagymértékű nyomást helyez Izraelre, hogy tegye lehetővé a szállítmányok eljuttatását, ez a kérdés még az amerikai fegyverszállítmányokat is veszélyezteti.[58] Két fő probléma merül fel. Az első, hogy különösen az élelmiszerbehozatal kapcsán az izraeliek a terrortámadást követően egy gyors Hamász kapituláció reményében, illetve a lakosság terrorszervezetekkel szembeni felkelésének kiváltása érdekében egyfajta teljes ostromban és kiéheztetésben gondolkodtak.[59] Látva azonban a kísérlet kockázatos voltát és a nemzetközi felháborodást, erről a stratégiáról Izrael letett és kiéheztetésről nem, legfeljebb limitálásról,

[53] SCHMITT (2023)
[54] BASHI (2024)
[55] IZRAELI VÉDELMI ERŐK (2023b)
[56] SAID (2023)
[57] MARGOLIN – NEUMANN (2024)
[58] FRANKEL – LEE – MAGDY (2024)
[59] FABIAN (2023)

adott helyzetekben szüneteltetésről beszélhetünk. A másik probléma a kettős felhasználású termékek, mint az üzemanyag bevitele. Egyik oldalon Izraelt kritika érte, amiért a kórházi generátorokat is ellátó üzemanyagot nem engedte be, mivel az a Hamász kezében katonai célokra is felhasználható. A háború első hónapjaiban folyamatosan arról cikkezett a nemzetközi sajtó, hogy „azonnal" elfogy a kórházakban az áramot termelő üzemanyag Izrael „blokádja" következtében. Ez azonban a mai napig nem következett be, ellenben jelentős nyomás nehezedett Izraelre és pattanásig feszítette a zsidó állam és legfontosabb támogatója az Egyesült Államok közötti viszonyt. Izrael igyekszik átláthatóan dokumentálni a segélyszállítmányok beérkezését, annak érdekében, hogy elhárítsa a vádakat.[60] A humanitárius kérdésekre azonban nem sikerült valódi megoldást találni a háború során, mivel a civil lakosságot nem lehet mentesíteni a háború alól, ha egyszer a másik fél élő pajzsként használja és nem lehet a segélyt se hatékonyan elosztani, ha nincs alternatív, kooperáló, vagy negatív jelzővel „kollaboráns" hatóság, amely képes lenne elosztani a segélyt a terrorszervezetet kiiktatva az egyenletből.

Röviden tárgyalom a ciszjordániai és az Izraelen belüli helyzetet a háború során, nem feltétlenül azért, ami történt, hanem sokkal inkább, ami nem. Izrael félelme a többfrontos háború kapcsán részben beigazolódott, azonban a nagyarányú felkelés nem indult meg Ciszjordániából kiindulva[61], Izraelben pedig nem indultak zavargások, ami megbéníthatta volna a háborúban álló országot. A ciszjordániai helyzet természetesen komplex, hiszen szinte folyamatosan zajlott az elmúlt egy évben az alacsony szintű konfliktus, és a rajtaütések a terrorista sejteken az izraeli erők által. Összességében azonban semmifajta harmadik intifádának nevezhető felkelés nem indult meg. Az Izrael területén elkövetett terrormerényleteket többségükben ciszjordániai palesztinok hajtották végre, de ez sem közelítette meg a korábbi intifádák során tapasztaltak szintjét. Az izraeli arabság többségében kategorikusan elítélte a Hamász terrortámadását, ezzel a gyakorlatban stabil hátteret teremtve Izraelnek a háború megvívására.[62] Látható tehát, hogy Izrael alapvető ellensége Irán és az ellenállás tengelye, nem annyira a nagyrészt sikeresen pacifikált ciszjordániai palesztinok és legkevésbé sem Izrael arab polgárai.

2.2.4. Harcok lezárása

Az előző alfejezetben úgy fogalmaztam, hogy az izraeli haderő az előzetes várakozásokkal szemben jóval kevesebb katonai áldozattal hajtotta végre az elmúlt több mint tizenhárom

[60] COGAT (2024)
[61] BYMAN (2023)
[62] RUDNITZKY (2023)

hónapban a gázai hadjáratot. Ugyanakkor azt is hangsúlyozni kell, hogy a másik oldalon nem is tudta elérni az izraeli katonai stratégiában fő pillérként kezelt döntő győzelem kritériumát. A harci sikerek fokozatosan akkumulálódnak, azonban a mennyiségi és minőségi eredmények nem váltottak át sem az ellenfél harci szándékának megtörésébe (ami a döntő győzelem hagyományos izraeli értelmezése), sem a Hamász teljes elpusztításába, amely újszerű követelmény Izrael számára. Mindkét megállapításra egyszerű bizonyítékot szolgáltat, hogy a beszámoló írásának időpontjában a harcok továbbra is zajlanak a Gázai övezetben.

A sikerek terén két fő tényezőt kell kiemelni, az izraeli haderő nagyfokú szabad műveleti szabadságát, valamint a Hamász vezetőinek sikeres likvidálását. A műveleti szabadság hangsúlyozása véleményem szerint azért kiemelt szempont, mivel mutatja, hogy egy terrorszervezet által egy évtizede szinte korlátlanul erődített városi hadszintéren is képes lehet egy modern, nagyszámú haderő összhaderőnemi művelet keretében átvenni a hatalmat, elzárni azt a külvilágtól és ott a kitűzött háborús célok megvalósítására törekedni minden különösebb külső időnyomás, vagy tömeges saját katonai áldozatok árán. Természetesen nem szabad lebecsülni a szinte minden nap életüket vesztő izraeli katonák jelentette belpolitikai nyomást. Ez nem mondható el a Hamászról, amelyet rendkívüli mértékben degradáltak a Gázai övezetet megszállás és ostrom alatt tartó izraeli csapatok, amelyek ismereteink szerint az övezet bármely pontján képesek a precíziós csapásmérésre vagy szárazföldi erőket összevonni és ott likvidálni a felbukkanó és újjá szerveződni kívánó Hamász erőket.

Az összes Hamász és PIJ terrorista likvidálása azonban kilátástalan küzdelem, a tapasztalt harcosokat meg lehet ölni, azonban a több mint kétmilliós gázai övezetben mindig lesz egy újabb fiatal férfi, aki készen áll fegyvert ragadni. Ezért is kiemelten fontos a vezetők likvidálása, amely kiemelt háborús cél volt, ahogy Netanjahu és Gallant fogalmazott.[63] Számos befolyásos vezetőt sikerült az eltelt hónapok alatt likvidálni, kiemelendő Mohammed Deif, a Hamász katonai vezetőjének júliusi halála, azonban a fő cél mindig is Jahja Szinvár, a Hamász gázai feje és a terrortámadás feltételezett szellemi atyja volt.[64] Hosszú hónapokat követően éppen a harcok egy éves évfordulója után sikerült az izraeli haderőnek Szinvárt megölni. Ennek nyilvánvaló üzenete volt, hogy a zsidó állam ellenségei bujkálhatnak, azonban előbb-utóbb elkapják őket, ezzel Izrael tavaly csorbát szenvedett elrettentőerejét és fenyegetését igyekeztek helyreállítani és az izraeli polgárokat megnyugtatni a revans által.

A Hamász likvidálása mellett a másik fő háborús cél kezdetektől a túszul ejtett kétszázötven izraeli kiszabadítása volt. Ez két módon történhet meg, a haderő által

[63] KELLER-LYNN (2023)
[64] NETANYAHU (2024)

végrehajtott mentőakció során vagy a túszok elengedéséről kötött megállapodás által. Az előbbivel kapcsolatban, szemben a Hamász erőinek és vezetőinek likvidálásával, az izraeli haderő rendkívül korlátozott sikereket tudott felmutatni. Összesen nyolc izraeli túszt sikerült élve kiszabadítani, miközben többeket az izraeliek érkezése előtt likvidált a Hamász, és volt példa, hogy izraeli katonák tévedésből túszokat öltek meg. Ezzel szemben a 2023 végén kötött első, és mindezidáig egyetlen tűzszünet idején 105 túsz került szabadon bocsájtásra.[65] A tanulság egyszerűen levonható, míg harcot lehetséges sikeresen vívni rendkívül összetett városi körülmények között is egy jól felkészült terrorszervezettel szemben, addig az ennél is komplexebb túszkiszabadítási akciók még az izraeli haderő képességeit is meghaladják. Az összes túszt azonban csak az izraeli csapatok kivonása esetén engedné el a Hamász, mivel ez az utolsó ütőkártya a kezükben. Ezt a Netanjahu-kormány mindeddig nem fogadta el, hiszen akkor nem lenne képes elpusztítani a Hamászt és megakadályozni az újjászervezését.[66] A két háborús cél tehát egymással ellentétes és ez a kettősség meghatározta az izraeli politikai és katonai elit manőverezését az elmúlt hónapokban.

Összességében azonban a legfőbb probléma, hogy hogyan lehet lezárni egy ilyen konfliktust izraeli oldalról. Említettem, hogy a legnagyobb gond, hogy soha nem került valójában definiálásra, mit jelent a Hamász elpusztítása. Ez a kérdés kevésbé volt jelentős, ameddig Szinvár életben volt és voltak újabb övezetek, városnegyedek, amelyek elfoglalásával és megtisztításával az IDF eredményeket mutathatott fel. Szakértők természetesen igyekeztek meghatározni a győzelem konkrét feltételeit, azonban végső soron a politikai elit mondhatja ki, hogy ezeket sikerült-e elérni vagy hogy bizonyos háborús célokat felad Izrael a tűzszünet, túszok kiszabadítása vagy más érvek mentén. Meggyőző érv ugyanakkor, hogy nem lehet a harcok elején konkrét *exit stratégiát* felállítani, először eredményeket kell elérni és utána a kialakult körülmények mentén alakítani a további lépéseket.[67] Tehát létezett egy átfogó cél, a Hamász elpusztítása és a túszok kiszabadítása, ezekhez társítottak eszközöket és műveleteket. Egy év után a megmaradt Hamász erők szintje mellett szükséges garantálni Izrael biztonságát kevésbé intenzív katonai és nemzetbiztonsági műveletek révén.

Izrael célja, hogy a Hamász soha többet ne tudjon biztonsági fenyegetést jelenteni Izraelre, különösen nem a 2023. október 7-ihez hasonló mértékűt. Ehhez alternatív, Izraelnek a biztonság terén szabad kezet adó gázai palesztin és/vagy nemzetközi kormányzatot akar

[65] SAID-MOORHOUSE et al. (2024)
[66] MAKOVSKY (2024)
[67] SHAMIR (2024): 3.

hatalomra segíteni. Ez a mai napig nem történt meg három okból. Az első, hogy a Hamász melletti egyetlen létező alternatíva a Fatah és a Ciszjordánia önkormányzatát fenntartó Palesztin Nemzeti Hatóság, amelyet viszont Izrael nem kíván megerősíteni, mivel ez egy általa kontrollálhatatlan folyamatot indíthatna el a palesztin államiság felé. A Fatah csak komoly feltételekkel vállalná el a Gázai övezet Hamász utáni kormányzását és a *status quo* megszüntetését várja el Izraeltől, amelyet utóbbi tehát nem vállal fel, a nemzetközi közösség viszont ezt a megoldást támogatná. A második ok, hogy az izraeli megoldás, amely a gázai helyi klánokra építve igyekezett valamilyen limitált helyi önkormányzatiságot kiépíteni a segélyszállítmányok elosztását alapul véve, nem vált be. A Hamász erői egyszerűen visszatérnek a hatalmi vákuumba és megkezdik a kormányzás visszavételét, nyilván azért, mivel 2006 óta nekik van egyedül ilyen tapasztalatuk az övezetben. A harmadik ok, hogy ha sem a Fatah, sem helyi decentralizált erők nem tudnak kormányozni, a Hamász pedig ki van zárva, akkor kellene egy új palesztin politikai erő, amely átvenné a hatalmat. Ilyen erő azonban nem született az elmúlt egy évben, bár nagy reményeket fűztek elemzők a Fatah és Hamászon kívülálló, azonban mindkettőhöz korábban kötődő Mohammed Dahlan szerepéhez.[68]

Összefoglalva tehát nem volt izraeli *exit stratégia*, nem sikerült teljesen megsemmisíteni a Hamászt és továbbra is mintegy száz (élő vagy halott) izraeli túsz van Gázában. Nincs kilátás arra, hogy Izraeli biztonsági érdekeit kiszolgáló palesztin vagy nemzetközi vezetés kerüljön a Gázai övezet élére. Mi marad tehát Izrael előtt nyitva álló megoldás? Az első a teljes izraeli megszállás és katonai uralom, amelyet azonban a feladat összetettségére, nemzetközi ellenállásra és várható áldozatok miatt rendkívül negatív lehetőség. Emellett éppen a Hamász érdekeit szolgálná, mivel az kormányzóerő helyett az izraeli megszállók elleni terrorakciókkal építhetné vissza renoméját, folyamatosan véreztetve a zsidó államot.[69] Második lehetőség, hogy Izrael kivonul a sűrűn lakott területekről a Gázai övezet szélére és stratégiai pontokra, mint az egyiptomi határsáv és az övezetet felező Netzarim korridor és onnan ellenőrzi a területet és hajt végre célzott beavatkozásokat, miközben a civil adminisztrációt a helyi erőkre bízza. A harmadik lehetőség a kivonulás, miközben nem feltételezhető, hogy a jövőben Izrael elkövetné azt a hibát, hogy ne hajtana végre megelőző csapásokat, a „hadjárat a háborúk között” doktrína egy módosított verzióját Gázában. Ha Izraelen múlik ezt egy kooperatív palesztin önkormányzattal teszi, mint Ciszjordániában, de ez csak a preferált, nem szükségszerű feltétel. Amit tehát biztosan állíthatunk, hogy a harcok intenzitása fokozatosan

[68] MEIR AMIT INTELLIGENCE AND TERRORISM INFORMATION CENTER (2024)
[69] DEKEL (2024): 5.

csillapodott az elmúlt hónapokban, de Izrael a tervezettnél hosszabb időre ragadt bent és az új szakaszban, legyenek ennek részletei bármilyenek Izrael továbbra is terrorelhárítási céllal szabad kezet fog követelni magának Ciszjordániához hasonlóan a Gázai övezetben is.

2.3. REGIONÁLIS KONTEXTUS

Az eddigiekben a Hamász terrortámadására és az izraeli ellenoffenzívára fókuszáltam, azonban ezeket nem lehet elválasztani a tágabb közel-keleti dinamikáktól. Az alapvető keretet az Izrael és Irán közötti hatalmi küzdelem határozza meg, amelyben egyik oldalon a zsidó állam áll, amelyet főként az Egyesült Államok támogat, kisebb mértékben a térségi szunnita államok, továbbá Franciaország és az Egyesült Királyság. A másik oldalon az Irán vezette ellenállás tengelye van, amelynek része, azonban nem központi eleme a Hamász.[70] Az ellenállás tengelyének célja az iráni szempontok szerint az ellenfeleinek elrettentése, a stratégiai mélység elérése az úgynevezett „offenzív védelem" stratégiája által. Irán a hagyományos katonai képességeiben meglévő hiányosságokat is kompenzálja az aszimmetrikus eszközökkel, ezen belül a proxyhálózat fenntartásával, amelynek terrorszervezetek, így a Hamász és a PIJ is részei.[71] Fontos hangsúlyozni, hogy minden egyes alkotóelemnek léteznek önálló érdekei, nem beszélhetünk monolit iráni irányításról, mindez megnehezíti a koordinációt. Nem csupán önálló érdekeik vannak a tengelyt alkotó szervezeteknek, hanem különösen a Hamász és a PIJ terrorista jellege miatt az államoktól, de akár a milíciáktól is eltérő kalkulációik megnehezítik Irán számára a szervezetek felhasználását saját céljai előmozdítása érdekében.

Irán alapvető érdeke saját hatalmi pozícióinak erősítése és ellenségeinek elrettentése.[72] Ebben Izrael az egyik fő célpont, amelyet Irán és proxyjai a „frontok egysége" stratégia keretében több irányból fenyegetnek. Izrael számára ez jelenti a létfenyegetést, a több frontos, aszimmetrikus háború veszélyét, amelyben terrorista műveletek, szárazföldi invázió, tömeges drón és ballisztikus rakétacsapások érkeznének minden irányból. Október 7-én, mint bemutattam, Izrael azzal kalkulált, hogy a Hamász terrortámadása figyelemelterelés lehet, az ellenállás tengelye által indított átfogó offenzíva nyitánya. Ez azonban nem következett be, Izrael létét nem próbálták meg Irán és proxyjai eltörölni. Felmerül tehát, hogy a Hamász saját érdekei miatt cselekedett, és erős érvek szólnak amellett, hogy ebben a formában nem is állt Irán érdekében a konfliktus.[73] Azt is határozottan állíthatjuk, hogy Iránnak kihívást jelentett

[70] ZIMMT (2024): 6.
[71] SOBELMAN (2024)
[72] KAM (2021): 20.
[73] SHABAN (2024)

menedzselni szövetségeseit és elérni a számára kívánatos intenzitású csapásokat Izraelre. Leegyszerűsítve, a Hezbollah vonakodott eszkalálni a konfliktust Izraellel, míg a Hamász eredeti támadása szinte öngyilkos jellegű volt. Irán maga is több ponton vonakodott belépni az eszkalációs spirálba, mind a Hamász támadás kezdeti szakaszában, mind a Hezbollah elleni szeptemberi izraeli offenzíva idején.[74] Kérdéses, hogy Irán milyen tanulságokat szűr le a háborúból és hogy fenntartható-e a frontok egysége stratégia vagy új megközelítést kell találnia Iránnak. Ez a kérdés nagymértékben függ a háború pontos kimenetelétől, hogy milyen mértékben gyengülnek meg a proxyk és lesz-e következő izraeli csapásmérés Iránra, továbbá, hogy a Trump-adminisztráció képes lesz-e tartósan térdre kényszeríteni a teheráni rezsimet.

Mint említettem, egy Izrael létét valóban fenyegető támadás nem indult a Hamász eredeti terrorműveletét követően, azonban változó mértékben, de az összes iráni proxy kivette a részét a küzdelemből. Ezeknek a célja az Izraelre és az amerikai blokkra gyakorolt nyomás erősítése volt, nem a Hamász felmentése és különösen nem Izrael elpusztítása. Ez nyilvánvalóan komoly presztízsveszteség az ellenállás tengelye számára. A Hamász felszólításai a felkelésre és Izrael elsöprésére érdemi válasz nélkül maradtak, a zsidó állam pedig az eredeti *casus bellit* felhasználva és kiterjesztve sorra gyengítette meg ellenségeit, ahogy a Gázai övezet után a hadműveleteit kiterjesztette Libanonban, Szíriában, Jemenben és Iránban is. Terjedelmi korlátok miatt itt csak a leginkább releváns tényezőket, a Hezbollah kérdését, majd Iránt tárgyalom.

2.3.1. A libanoni Hezbollahhal szembeni harc

Az Izrael-Hezbollah konfliktus több mint négy évtizedes múltra tekint vissza miután Izrael a keresztény Dél-libanoni Hadsereg oldalán beavatkozott a libanoni polgárháborúba és 2000-ig katonailag jelen volt északi szomszédja területén. Az eltelt évtizedekben több konfliktuskörre is sor került a Hezbollahhal, amely közben Irán regionális proxyhálózatának kiemelt pillérévé vált.[75] Ennek tekintetében problematikus volt, hogy a libanoni terrorszervezet, amely ugyanakkor parlamenti pártként kormányzati pozíciókat is betölt, saját képességeihez mérten szinte csak szimbolikusan vette ki a részét az Izraellel szembeni harcból. Ez ugyanakkor érthető, hiszen sem Irán, sem a Hezbollah vezetői nem kívánták feláldozni a szervezetet a Hamász harcának oltárán. A Hezbollah szerepe legfőképpen az iráni befolyási zóna nyugati szárnyának biztosítása, különösen a polgárháborús Szíriában Irán hatalmának fenntartása, ugyanakkor képes kiváltani az iráni kiképzőerőket és hozzájárulni az ellenállás tengelyét képező proxyhálózat erősítéséhez, kiképzéséhez, a „*franchise*”

[74] GOL (2024)
[75] ZIMMT (2024): 6.

terjesztéséhez. Mindemellett, tekintettel Izraelhez való földrajzi közelségére, több tízezres rakétaarzenáljára a „frontok egysége” stratégia legfontosabb szereplője is. Ugyanakkor éppen emiatt a kiemelt szerep és az iráni és Hezbollah narratíva miatt az se lett volna megengedhető, hogy a Hezbollah semmilyen formában ne csatlakozzon a Hamász harcához, vagy hogy idejekorán kilépjen a konfliktusból.

Izrael határozottan kommunikálta, hogy a Hezbollahnak fel kell hagynia a rakéta és dróncsapásokkal, különben fegyveres erővel fogja visszaállítani az északi határvidékének biztonságát. A Hamásszal szemben vívott küzdelem intenzitásának fokozatos apadása nyomán az izraeli vezetés 2023 decemberétől kezdődően jelezte, hogy északra fog fordulni a harctevékenységének fókusza, amennyiben a Hezbollah nem hátrál meg.[76] Az izraeli formálódó ultimátum szerint a Hezbollahnak be kellett volna szüntetnie a csapásokat és a határtól legalább 15 kilométerrel, a Litáni folyó mögé vonni vissza erőit.[77] Ezzel gyakorlatilag a polgárháborút lezáró 1701. számú ENSZ Biztonsági Tanács határozatot kellett volna megvalósítani, közel két és fél évtizeddel elfogadása után, amelyet sosem sikerült valóban betartatni a Hezbollahhal. A libanoni terrorszervezet ennek az ultimátumnak nem tett eleget, azonban a helyzet további eszkalációjához vezetett, hogy 2024. július 27-én az izraeli fennhatóság alatt álló Majdal Shams település futballpályán becsapódott rakéta tizenkét gyermek életét oltotta ki és negyvenketten sebesültek meg.[78] Az izraeli katonai vezetés a Hezbollahot tette felelőssé a támadásért.[79] Ezt követően az Izrael és a libanoni Hezbollah terrorszervezet közötti addigi korlátozott konfliktus rendkívüli mértékben eszkalálódott.

Az izraeli vezetés szeptember 16-án a hivatalos háborús célok közé emelte a Hezbollah rakétatámadásai nyomán kitelepített több tízezer észak-izraeli civil hazatérésének biztosítását, előrevetítve egy szárazföldi offenzívát.[80] Az új háborús cél kitűzését követő napon, szeptember 17-én több ezer Hezbollah tag gyorshívó készülékét robbantották fel egy koordinált titkosszolgálati akció keretében, amelyet Netanjahu közel két hónappal később ismert el.[81] Az akcióban mintegy háromezer, többségében Hezbollah militáns sebesült meg, jelentősen gyengítve a terrorszervezet harci és koordinációs képességeit. Másnap a Hezbollah több száz walkie talkie készüléke robbant fel, közel ezer főt megsebesítve, hozzájárulva a terrorszervezet további szétzilálásához és a félelem elmélyítéséhez. Szeptember 19-én Izrael átfogó légioffenzívát indított a Hezbollah libanoni állásai ellen, a terrorszervezet vezetőit

[76] DETTMER (2023)
[77] JEWISH NEWS SYNDICATE (2024)
[78] FABIAN (2024)
[79] IZRAELI VÉDELMI ERŐK (2024b)
[80] LUKIV (2024)
[81] BERMAN, Lazar (2024)

sorban likvidálta. Szeptember 27-én a világ közvéleményét és a közel-keleti hatalmi rendet sokkolta a Hasszán Naszrallah, a Hezbollah fejének megölése egy Bejrútban végrehajtott nagyszabású célzott légitámadás során.[82] Az izraeli haderő október első hetében szárazföldi offenzívát indított Dél-Libanonban, az átfogó légihadjárat folytatása mellett, amelyek célja a Hezbollah jelentette fenyegetés felszámolása, Észak-Izrael biztosítása és a közel-keleti hatalmi egyensúly radikális megváltoztatása Izrael javára Iránnal és tengelyével szemben.[83] A Hamásszal szembeni küzdelemről tehát elfordult a fókusz és tágabb, regionális stratégiai célok megvalósítására váltott Izrael. A 2024. november 26. éjszakáján érvénybe lépett tűzszünet keretében a meggyengített Hezbollah hajlandó volt elfogadni az izraeli ultimátum fő pontjait a szervezet maradékának megőrzéséért cserébe.[84]

2.3.2. Iránnal szembeni közvetlen kinetikus konfliktus

Irán, az ellenállás tengelyét vezető regionális nagyhatalom hosszú hónapokon keresztül igyekezett egyszerre felhasználni proxyjait, ugyanakkor maga kimaradni a közvetlen harcokból Izraellel és az Egyesült Államok térségi erőivel szemben.[85] Továbbra is nyitott kérdés, hogy a Hamász terrortámadása mennyiben lepte meg a teheráni rezsimet, azonban az eltelt egy év során az események bebizonyították, hogy Irán nem kívánta, hogy a proxyhálózata a háború áldozata legyen. Ez hatványozottan vonatkozott saját erőire. Ez a politika 2024 tavaszán vált tarthatatlanná az iráni politikai és katonai vezetés számára, miután Izrael légicsapást mért a damaszkuszi iráni nagykövetség épületére, több magas rangú, az ellenállás tengelyének koordinációját végző iráni tisztet megölve.[86] Ezt Irán olyan közvetlen kihívásként értékelte, amire válaszul nagyszabású, eredményében azonban szimbolikusnak tekinthető drón, ballisztikus- és cirkálórakéta-támadást indított Izraellel szemben. A támadás kivédésében példátlan nemzetközi koalíció vonult fel a zsidó állam oldalán.[87] A védelem sikere lehetővé tette, hogy Izraelnek nem volt szüksége pusztító választ adni, mivel az iráni támadásnak nem sikerült, még ha célja is volt, átrendezni a regionális hatalmi viszonyokat.

A második hasonló támadás már egy Teherán területén végzett, feltételezhetően izraeli művelet eredménye volt, mivel 2024. július 31-én éppen az új iráni elnök teheráni beiktatására való látogatása során vált merénylet áldozatává Iszmail Hanije, a Hamász politikai vezetője. Ez súlyos presztízsveszteséget jelentett a teheráni rezsim számára, így a válaszadás nem volt

[82] FOUNDATION FOR DEFENSE OF DEMOCRACIES (2024)
[83] HAZUT– SHELAH (2024)
[84] RADFORD et al. (2024)
[85] ZIMMT (2024): 5.
[86] HAID (2024)
[87] SHAIKH (2024)

kétséges, ugyanakkor komoly kalkulációk előzték meg.[88] Az események azonban 2024 őszén kezdtek még inkább kicsúszni Teherán befolyása alól, a Hezbollah ellen indított, katonai és nemzetbiztonsági eszközöket alkalmazó gyors izraeli felmorzsolóhadjárat eredményeként. Az október elsejei újabb iráni rakétacsapás célja tehát megint csak az volt, hogy megállítsa az ellenállás tengelye és Izrael közötti hatalmi viszonyok teljes átrendeződését az utóbbi javára. A támadás komolyabb eredményeket ért el, mint az első, azonban átütő sikerről nem beszélhetünk. Az izraeli ellencsapás azonban jelenlegi ismeretink szerint súlyos károkat okozott Irán ballisztikus rakétaépítési és részben nukleáris programjában. Emellett bizonyította, hogy Izrael az iráni légvédelmet le tudja küzdeni és szinte szabadon megsemmisíteni a kijelölt célpontokat.[89] A közvetlen összecsapást tehát a Hamász eredeti terrortámadása végső soron kiváltotta a két szembenálló regionális nagyhatalom között, azonban ezek időzítése, intenzitása és különösen az eredménye nem segítették a terrorszervezet céljait, de minden bizonnyal Iránét sem.

A háború kapcsán fontos kiemelni, hogy az regionális szinten aszimmetrikus viszonyok jellemzik és a közel-keleti dinamikák kapcsán más érdekek érvényesülnek, mint a közvetlen Izrael-Hamász harcokban. Az aszimmetriát okozza, hogy regionális szinten az egyik oldalon Izrael, egy nemzetállam áll, a másik oldalon a Hamász és a Hezbollah, egy regionális nagyhatalom, Irán, valamint az ellenállás tengelyének többi tagja van. Az izraeli oldal ebből következően jobban szervezett, kifelé monolit cselekvőként jelenik meg, míg a Hamász oldalán minden egyes lépésnél természetéből következően tökéletlen koordináció és közös fellépés valósul meg. Ehhez az aszimmetriához járul hozzá, hogy a zsidó állam is rendelkezik partnerekkel, amelyeknek nem érdeke a közel-keleti hatalmi viszonyok átrendeződése az iráni oldal javára. Az Egyesült Államok játssza a legfontosabb szerepet, mint Izrael nagyhatalmi garantora, legnagyobb fegyverszállítója és diplomáciai védőernyője. Az Egyesült Államok és Izrael kapcsolata rendkívül szilárd és sokrétű alapokon nyugszik, azonban Washington rendszerszinten is érdekelt Izrael, mint az egyetlen olyan közel-keleti katonai nagyhatalom, amely nem potenciális regionális hegemón, elrettentőerejének fenntartásában és erre építve egy regionális biztonsági architektúra kiépítésében.

A hatalmi egyensúly Irán és tengelye felé való eltolódása ugyanúgy fenyegeti a szunnita arab államokat, így bár ezek az országok kritizálják Izrael gázai és libanoni fellépését, gyakorlatban semmit nem tettek, hogy azt akadályozzák.[90] Szerepük részleges és a

[88] McCabe (2024)
[89] Hokayem (2024)
[90] Khouri (2024)

humanitárius segítségnyújtásra és (Egyiptom és Katar részéről) a tűszüneti tárgyalások közvetítésében merül ki. A regionális biztonsági architektúrában érdekelt, az Egyesült Államokkal és így Izraellel is partnerséget ápoló *status quo* országok nem érdekeltek Irán és partnereinek előretörésében, így nem gyakorolnak jelentős nyomást Izraelre. Ennél továbbmenve, különösen az áprilisi iráni támadás során hathatós regionális koalíciót sikerült az Egyesült Államoknak létrehozni, amely a zsidó állam rakétavédelmét biztosította. Amiben az arab államok azonban nem tudnak és nem is kívánnak egyelőre hatékony segítséget nyújtani az a Hamász utáni gázai stabilitás garantálása, békefenntartók küldése és gyakorlatilag átvállalni Izrael költségeit a gázai háború után, amennyiben az nem kötődik a Palesztin Hatóság megerősítéséhez a Gázai övezetben is.[91] Míg tehát Izrael jelentős mértékben számíthat partnereire az átfogó közel-keleti hatalmi egyensúly számára is kedvező fenntartása szintjén, a jelenlegi konfliktus gyökere, Gázai övezetben a Hamásszal szemben zajló terrorellenes katonai művelet kapcsán nem számíthat egyelőre hatékony segítségre. Ugyanakkor a térség legtöbb állama nem nyújt hathatós segítséget a Hamásznak sem (még az ellenállás tengelye sem tudja megállítani az izraeli offenzívát, nemhogy az Egyesült Államok és Izrael partnerei), így a Hamász és Izrael aszimmetriájából eredően ez inkább kedvező viszonyokat teremt a zsidó állam számára.

3. KÖVETKEZTETÉSEK

A Hamász által 2023. október 7-én elkövetett terrortámadás, a Gázai övezetben több mint egy éve tartó háború és a konfliktus regionális aspektusai kapcsán több fontos tanulságot és tapasztalatot levonhatunk – még ha a teljes kivizsgálásra hosszú hónapok és évek múlva kerülhet csak sor. A négy eredeti kutatási kérdésre az alábbi válaszokat adom:

3.1. MILYEN IZRAELI TÉNYEZŐK TETTÉK LEHETŐVÉ, HOGY A HAMÁSZ BIZONYOS MÉRTÉKŰ SIKERT ÉRHETETT EL AZ OKTÓBER 7-I TÁMADÁSÁVAL?

A kutatás során két fő tényező emelkedett ki a terrortámadást lehetővé tevő izraeli hibák közül. Az első, hogy több összetevő miatt alapvetően félreértelmezték a Hamász stratégiai terveit és szándékait, ezzel vakfoltot képezve az izraeli nemzetbiztonsági szervek elemző-értékelő munkája során és eredően sorozatos hibákat eredményezve az október 7-i védelem kudarcáig bezárólag. A Hamász félreértelmezéséhez egyrészt belső, izraeli okok, másrészt a Hamász sikeres megtévesztése, harmadrészt a közel-keleti biztonsági környezet átalakulása is

[91] MAGID (2024)

hozzájárult. Az izraeli politikai vezetés szempontjából az a feltételezés szolgáltatta a legtöbb előnyt, amely szerint a Hamász érdekelt volt a *status quoban* és a zsidó állam képes azt elrettenteni. Az izraeli vezetés nem kívánt egy gázai „hadjárat a háborúk között" eljárással eszkalációt kockáztatni, amely lehetetlenné tette volna a prioritásként kezelt regionális normalizáció folyamatát.

Ez tehát kizárta a Hamásszal szembeni megelőző izraeli katonai akciókat, azt azonban nem magyarázza, miért nem készültek fel jobban a védelemre, ha feltételezték a Hamász nagyarányú támadását. A válasz kettős. Egyrészt ezek szerint valóban nem tartották valószínűnek a Hamász inváziójá̀t, legfeljebb egy-egy beszivárgó műveletet, amellyel szemben a rendelkezésre álló katonai erő és védelmi képességeknek elegendőnek kellett volna lenniük. Ennél is fontosabb szempont volt, hogy Izrael készült ugyan a háborúra, azonban elsődlegesen nem a Hamásszal, hanem Irán és az ellenállás tengelyének egészével szemben, alapvetően északról kiindulva. Összességében tehát igazoltnak tekintem, hogy az izraeli politikai, katonai és nemzetbiztonsági szervek súlyos elemzési és értékelési hibát okoztak vágyvezérelt feladatmeghatározásaikkal, amelyek megakadályozták a megfelelő megelőző katonai és nemzetbiztonsági műveletek végrehajtását és a védelmi felkészülés kialakítását. Ezzel összefüggésben Izrael készült Gázából a rutin biztonsági fenyegetést jelentő beszivárgásra számított, míg a létét fenyegető háborút más irányból várta – ebben a Hamásznak csupán kiegészítő szerepet tulajdonított. A kettő közötti, a Gázai övezetből kiinduló vészhelyzeti biztonsági fenyegetésre nem voltak felkészülve.

3.2. MENNYIBEN TEKINTHETŐ IZRAEL VÁLASZA ÚJSZERŰNEK, VAGY AZ A NEMZETI BIZTONSÁGI STRATÉGIÁJÁBÓL KÖVETKEZŐ LOGIKUS LÉPÉS VOLT?

Az izraeli katonai válaszcsapás és többfrontos háború igényei szerint való azonnali mozgósítás logikus volt saját szempontjukból, mivel az izraeli stratégiai tervezésben a Hamász támadása csak egy létet fenyegető háború megindításának első lépéseként tűnt racionálisnak, köszönhetően a téves izraeli helyzetértékelésnek. Ugyanakkor elmondható, hogy a kudarcot követően az izraeli vezetés a lehető legnagyobb veszélyt feltételezte, és kárminimalizáló stratégiát követve maximális háborús készültséget rendeltek el. A gázai szárazföldi hadművelet ebben a kontextusban csak akkor újszerű, ha az elmúlt néhány év izraeli stratégiáját vesszük alapul – nem pedig az évtizedek óta a döntő győzelemre törekvő, offenzív izraeli katonai stratégiát. Ha átfogóan nézzük Izraelt, akkor egyértelmű, hogy az október hetedikei nemzeti tragédiára a rendkívül érzékeny biztonságpercepcióval rendelkező és létében magát fenyegetve érző izraeli társadalom radikális választ fog adni. Ennek célja a

hiba kijavítása azáltal, hogy a terrortámadás elkövetőit egyrészt példastatuálás gyanánt likvidálja, ezzel helyreállítva a zsidó állam elrettentőerejét, másrészt leegyszerűsíti a következő, elkerülhetetlennek tartott létért vívott háborút azáltal, hogy a frontok egysége iráni stratégia délnyugati elemét kiiktatja egyszer és mindenkorra.

Két szempontból azonban újszerű az izraeli katonai válasz, mivel a döntő győzelem hagyományos izraeli értelmezésével szemben, amelyben az ellenség, legyen az állami vagy nem állami szereplő, harci akaratát töri meg, a Hamász esetében az ellenség elpusztítása, vezetőinek meggyilkolása vált a konkrét háborús céllá, míg korábban nem volt cél például Egyiptom elnökének likvidálása a háborúk során. Tehát ebben Izrael új magatartást mutatott a terrorelhárítás terén, amit kiegészít, hogy míg korábban a gyors hadműveletek jellemezték Izraelt, addig a jelenlegi háború során minden korábbinál tovább tart az intenzív háborús szakasz. Ennek egyik oka a Hamász elpusztítására fordított idő és a művelet nehézsége (különösen a túszok kérdésének összetettsége miatt), azonban az is, hogy Izrael sikeresen alakította át az eredeti terrorelhárítási céllal indított háborúját a biztonsági környezet radikális megváltoztatása érdekében előbb a Hezbollah, majd részlegesen Irán meggyengítésére, ami megint újszerű elem, hacsak nem megyünk vissza az 1967-es hatnapos háborúig, amikor az ellenséges arab koalíciót egy offenzív megelőző háborúval megtörve Izrael megnégyszerezte területét.

3.3. A KITŰZÖTT IZRAELI HÁBORÚS CÉLOKAT MENNYIBEN SIKERÜLT IZRAELI ÉS NEMZETKÖZI ÉRTÉKELÉSEK SZERINT TELJESÍTENI, HOGYAN VÁLTOZTAK AZOK AZ ELMÚLT TIZENKÉT HÓNAPBAN, MIÉRT HÚZÓDOTT EL A HÁBORÚ TÖBB MINT EGY ÉVEN KERESZTÜL?

A háborús célok kapcsán talán a leginkább lesújtó a kép és a legtöbb figyelmeztetést adja, hogy milyen összetett és egyértelmű siker milyen nehezen érhető el a terrorszervezetekkel szemben vívott harcok során. A két eredeti cél közül megállapítottam, hogy a Hamászt nem sikerült teljes mértékben megsemmisíteni, azonban jelentős mértékben meggyengült. Mégsem állíthatjuk, hogy a Gázai övezet pacifikálása megtörtént volna. Ehhez nem elég a harcokat megnyerni, hanem a békét is meg kell politikai eszközökkel, ahogy a második intifádát is Izrael az elhúzódó katonai offenzívát követően a Palesztin Hatóság biztonsági kooperációjának biztosításával nyerte meg valójában. A túszoknak csupán körülbelül a felét sikerült kiszabadítani a Hamász fogságából, a kilencvenhét megmaradt, életben lévő vagy halott izraeli túsz kiszabadítására jelenleg egy tűzszünet adhat esélyt. A háború során később fogalmazódott meg a Hezbollahhal szemben az északi polgárok visszatérésének biztosítása,

mint háborús cél, ez a kutatás lezárásáig szintén nem valósult meg, azonban a 2024. november 27-én életbe lépett tűzszünet erre esélyt ad. Ugyanakkor a harmadik háborús cél indok volt arra, hogy Izrael átfogó kampányt indíthasson a Hezbollahhal szemben, ezzel a biztonsági környezetét összességében javítsa. Bár ez utóbbi nem hivatalos háborús cél, talán ebben a tekintetben ért el Izrael a legtöbbet az elmúlt egy évben. Arra pedig, hogy miért tartanak a harcok ilyen sokáig két válasz adható. Az egyik, hogy rendkívül összetett és nehéz feladat egy terrorszervezet legyőzése városias területen, nem létezik egyetlen döntő csata, amelynek megnyerésével az ellenfél kapitulációra kényszeríthető. A másik ok, hogy Izraelt mind a hazai, mind a külső szereplők hagyták ennyi ideig harcolni és elérni katonai céljait, minden humanitárius következmény ellenére, ezt pedig nem vehetjük magától értetődőnek.

3.4 Milyen mértékben sikerült Izraelnek elválasztani a lokális ellenséggel szembeni harcot a regionális támogatójával szembeni küzdelemtől?

A gázai invázió Közel-Keleten átívelő hatása nyomán kijelenthető, hogy Izraelnek nem sikerült leválasztani a Hamászt annak partnereiről, ugyanakkor azok teljes képességeiket tekintve csupán korlátozott mértékben avatkoztak be a Hamász oldalán. Ennek nyomán igazolható, hogy a terrorfenyegetés jelenléte, elhárítása és felszámolása elválaszthatatlan a regionális hatalmi egyensúlytól és vákuumtól. Ugyanakkor ki kell emelni, hogy az elmúlt egy év tapasztalatainak tükrében Izrael képes volt a Hamász és az ellenállás tengelye közötti koordinációt korlátozni a tengely többi tagjának elrettentése által. Emellett az ellenségei közötti korlátozott együttműködést a hasznára is tudta fordítani olyan tekintetben, hogy a kezdeti terrorelhárítási céllal indított gázai offenzívát Izraeli kiterjesztette egy, a teljes biztonsági környezetét kedvező irányba módosító átfogó hadjárattá.

3.5. Vannak-e hasonló területek, ahonnan az október 7-i terrortámadáshoz hasonló műveletek indulhatnak ki?

Arra a kérdésre, hogy vannak-e területek a Közel-Keleten és a világban, ahonnan a Hamász október 7-i támadásához hasonló terrorista akciók indulhatnak a válasz egyértelműen igen. Tekintettel a Hamász fegyvereseinek nemzetközi összehasonlításban limitált számára, az elméleti lehetősége fennáll a hasonló támadásoknak. Több szempontot azonban ki kell emelni, amelyek szerint ezek a potenciális támadási frontok azonosíthatóak, illetve, legalább részlegesen kizárhatóak. Az első, hogy a Gázai övezetet és Izraelt nem választja el természetes határ, ezért is lett volna nagy jelentősége az izraeli biztonsági kerítésnek. A

terrortámadás újra bebizonyította a védhető határok jelentőségét és a földrajzi adottságok kiemelt szerepét a védelemben. A második tényező a Hamász megkérdőjelezhetetlen uralma a Gázai övezet felett, ami lehetővé tette, hogy a terrorista szervezkedés megtörténhessen és ne érje belső kihívás a hosszú éveken át tartó előkészítést, amelynek a *status quo* megágyazott. A Gázai övezet adottságai nem csupán a természetes határok hiánya miatt vizsgálandóak, hanem az a sűrűn beépített környezet, amely megint csak lehetővé tette az erők koncentrációját, a támadás előkészületeinek legalább részleges elfedését, majd a terrorakciót követően a visszavonulást a megerősített területre, elméletben felkészülten és a Hamász számára elméletileg a legkedvezőbb körülmények között várva az izraeli ellentámadást. Hangsúlyozni szükséges továbbá, hogy a Hamász számíthatott az ellenállás tengelyének támogatására, a támadást megelőző fegyverszállítmányokra és kiképzésre, mivel még ha Irán és partnerei nem is tudtak a Hamász pontos szándékairól, az kétségtelen, hogy a felfegyverzésében kulcsszerepet játszottak az elmúlt években.

Végezetül tehát Izraelből koncentrikus körökben kiindulva a határain, a Közel-Keleten és a világ távolabbi pontjain vizsgálom meg az esetleges hasonló támadások kiindulópontjait. Az első Ciszjordánia, amelyet a jelenlegi helyzetben elvethetünk, mivel eddig sem sikerült a Hamásznak megfelelő erőket felépítenie, uralma nem átfogó, mint a Gázai övezetben, hanem a Fatah és Izrael erői is jelen vannak. Emellett a földrajzi adottságok miatt arányaiban kevesebb a beépített terület és a ciszjordániai izraeli telepek jobban védettek, magaslati pontokon helyezkednek el, ellentétben a Gázai övezet melletti kibucokkal. Hasonló támadásra jóval esélyesebb Dél-Libanon és Szíria, ahol Irán síita partnerei évek óta fejlesztenek hasonló inváziókra kész erőket. Kiemelt a Hezbollahhoz tartozó Radwan Erők és a Galilea meghódítására irányuló tervek.[92] Éppen ezért volt fontos Izrael számára egy északi támadás megelőzése október 7-én és a kutatás befejezése idején a Hezbollah hátra kényszerítése határaitól a korábbi katonai offenzíva és a tűzszüneti megállapodás révén. A szíriai irány sem lebecsülendő, azonban ott fontos magaslati pontokat kellene megrohamozni a Golán-fennsíkon, megint csak a Gáza melletti sík tereptől eltérően. Mindez nem jelenti azonban, hogy Izraelnek, az október 7-i precedenst követően ne lenne elsődleges prioritás minden hasonló támadási kísérlet előkészítését felderíteni és megakadályozni, mivel a viszonyok bármelyik fronton rövid idő alatt megváltozhatnak, ideértve további államok, mint Jordánia vagy Egyiptom válsága vagy akár bukásának esetét.

[92] IZRAELI VÉDELMI ERŐK (2024a)

A tágabb Közel-Keletet tekintve több potenciális konfliktuszónában is elképzelhető hasonló támadás. A síita terrorszervezetek és milíciák több ponton jelentenek fenyegetést. Egyik kiemelt terep, amelyre érdemes lesz figyelni a jövőben is a húszik által uralt Észak-Jemen és Szaúd-Arábia határa, ahol további radikalizáció eredményeként hasonló támadás elképzelhető. Emellett az Iszlám Állam által korábban uralt szíriai-iraki határvidék és Líbia jelent olyan veszélyforrást, ahol radikális szervezetek, kihasználva az esetlegesen felerősödő hatalmi vákuumot hasonló támadást követhetnek el, a mindhárom országban egymással a központi hatalomért vetélkedő erőkkel szemben, valamint az amerikai bázisokat is érintve a kurd területeken. Nagyobb bizonytalanságot jelent a kurd nemzeti ambíciók jövője és egy esetleges radikalizációs folyamat, amely leginkább Törökországra jelent fenyegetést a Kurd Munkapárt és annak iraki és szíriai partnerei részéről, így Ankara számára is aggasztó fejleményt jelent a tömeges terrorinváziók precedense által jelentett új korszak. Végezetül talán a legnagyobb kockázatot az Irán, Afganisztán és Pakisztán hármasának határzónái jelentik, ahol a szunnita radikális erők, a beludzs felkelők, valamint az Iszlám Állam és a Talibán, az iráni és pakisztáni kormányerők közötti permanens, civileket rendszeresen érő fegyveres konfliktus könnyen az október hetedikei támadás mintáját adaptálhatja.

A Közel-Kelettől eltávolodva számos terület van, ahol hasonló terrortámadás, illetve abból elemeket eltanuló műveletek létrejöhetnek. Ki kell emelni Afrika konfliktusgócait, ahol a gyors városiasodás, a hatalmi vákuum és a radikális ideológiák mind robbanékony elegyet teremtenek és minden naposak a felkelők, milíciák és terroristák kegyetlenkedései, különösen a Száhel-övezet államaiban, Nigériában és a Kongói Demokratikus Köztársaságban. Tekintettel a világ számos konfliktusára, ezeket nem sorolom fel, azonban két tényezőt kiemelek a további gondolkodás megalapozása érdekében. Az első, hogy hiba lenne azt gondolni, hogy kizárólag terrorszervezetek adaptálhatják a módszert, ellenkezőleg, egy állami aktor, mint Észak-Korea is megkísérelhet hasonló betörést Dél-Koreába,[93] de bűnözői szervezetek, mint latin-amerikai drogkartellek is átvehetnek elemeket a Hamász támadásból és megfélemlíthetik így a lakosságot és nyomást gyakorolhatnak a központi kormányzatokra. A második tényező, hogy a világ konfliktusgócai dinamikusan alakulnak és az, hogy ma nem reális rövidtávon hasonló terrortámadástól tartani például a Balkánon, Magyarország szomszédságában, ez nem jelenti azt, hogy néhány éves távlatban ez ne jelentene veszélyforrást. Összességében tehát a Hamász terrorista „innovációja” a legkevésbé sem csak Izraelt érinti, hanem a világ összes államát, így a háború kimenetele és a Hamász

[93] MACKENZIE (2023)

elpusztításában elért siker nemzetközi jelentőséggel bír. Ugyanakkor, tekintettel arra, hogy Izrael a világ egyik legnagyobb és legfejlettebb konvencionális fegyveres erejével is bír, a többi, kisebb és kevésbé felkészült ország esetében aláhúzza a nemzetközi együttműködés, különös tekintettel a szövetségi rendszerekben való közös fellépés jelentőségét a terrorszervezetekkel szembeni globális fellépésben.

Végezetül három további kutatási irány megjelölésével zárom az anyagot. Az első, hogy a fenti kérdéseket természetszerűleg újra meg kell vizsgálni amint a háború lezárul és amint a hivatalos izraeli vizsgálóbizottság jelentését megismerhetjük. A második, hogy az anyagban nem érintettem az Izrael-Hamász háború nyomán felerősödött antiszemitizmust és Izrael-ellenességet, amely különösen a nyugati világ országaiban egyrészt politikailag destabilizáló hatással járt, másrészt pro-Hamász terrorfenyegetést jelent. Emellett az őshonos társadalom dzsihádista és szélsőbaloldali radikalizációra adott válasza is több helyen felerősíti a szélsőjobboldal társadalmi támogatottságát, hozzájárulva a növekvő társadalmi feszültségekhez. Végezetül érdemesnek tartom a támadás regionális és globális mintaadó szerepének további vizsgálatát és monitorozását, megfigyelhető-e a módszerek adaptálása, Hamász militánsok kiképző szerepének esetleges elterjedését, vagy, hogy ellenkezőleg, az izraeli válasz éppen, hogy elvette ennek az igényét és lehetőségét.

FELHASZNÁLT IRODALOM

BASHI, Sari (2024): North Gaza: Between Death and Displacement. *Human Rights Watch*. 2024.10.18. Online: https://www.hrw.org/news/2024/10/18/north-gaza-between-death-and-displacement

BBC (2024): *Hamas: What has happened to its most prominent leaders?* 2024.10.18. Online: https://www.bbc.com/news/world-middle-east-67103298

BERMAN, Lazar (2024): In first, Netanyahu said to acknowledge Israel carried out pager attacks on Hezbollah. *Times of Israel*. 2024.11.10. Online: https://www.timesofisrael.com/in-first-netanyahu-said-to-admit-israel-carried-out-pager-attacks-on-hezbollah/

BREUER, Eliav (2024): Oct. 7 a result of 'arrogant' groupthink instilled by Netanyahu, civil probe finds. *Jerusalem Post*. 2024.11.26. Online: https://www.jpost.com/israel-news/article-830804

BYMAN, Daniel (2023): Did Hamas Ignite a Third Intifada? *Foreign Affairs*. 2023.10.23. Online: https://www.foreignaffairs.com/israel/did-hamas-ignite-third-intifada *Jerusalem Post*. 2024.11.26. Online: https://www.jpost.com/israel-news/article-830804

COGAT (2024): *Gaza Humanitarian Aid Data*. Online: https://gaza-aid-data.gov.il/main/

COUNCIL ON FOREIGN RELATIONS (2024): *A Conversation With U.S. Special Envoy to Monitor and Combat Antisemitism Deborah Lipstadt*. 2024.01.24. Online: https://www.cfr.org/event/conversation-us-special-envoy-monitor-and-combat-antisemitism-deborah-lipstadt

CSEPREGI, Zsolt (2023): A „hadjárat a háborúk között" eljárás helye az izraeli katonai stratégiában. *Nemzet és Biztonság*. 2023(1), 35–48. Online: https://folyoirat.ludovika.hu/index.php/neb/article/view/6519/5579

CSICSMANN László (2020): *Arab tavasz – arab tél*. Budapest: Nemzeti Közszolgálati Egyetem.

DEKEL, Udi (2024): A Simulation of Military Rule in Gaza: The Advantages and Disadvantages. *Institute for National Security Studies*. INSS Insight No. 1880. 2024.07.21. Online: https://www.inss.org.il/publication/simulation-gaza/

DETTMER, Jamie (2023): Israel could open second front in Lebanon, defense minister hints. *Politico*. 2023.12.06. Online: https://www.politico.eu/article/israel-could-open-second-front-lebanon-defense-minister-hintsgaza-hamas-war-yoav-gallant/

EBRAHIM, Nadeen – TEL, Amir – KREVER, Mick (2023): Israel's judicial overhaul sparks military crisis as number of refusing reservists grows. *CNN*. 2023.07.26. Online: https://edition.cnn.com/2023/07/26/middleeast/israel-judicial-overhaul-military-reservists-intl/index.html

EFRON, Shira – GOTTESMAN, Evan – KOPLOW, Michael (2023): Leveraging the Prospect of Israel-Saudi Normalization to Advance Israeli-Palestinian Progress. *Israel Policy Forum.* Online: https://israelpolicyforum.org/wp-content/uploads/2023/06/Leveraging-the-Prospect-of-Israel-Saudi-Normalization-to-Advance-Israeli-Palestinian-Progress-June-2023.pdf

EGYESÜLT ÁLLAMOK KÜLÜGYMINISZTÉRIUMA (2024): *Anniversary of October 7th Attack.* Online: https://www.state.gov/anniversary-of-october-7th-attack/

FABIAN, Emanuel (2023): Defense minister announces 'complete siege' of Gaza: No power, food or fuel. *Times of Israel.* 2023.10.09. Online: https://www.timesofisrael.com/liveblog_entry/defense-minister-announces-complete-siege-of-gaza-no-power-food-or-fuel/

FABIAN, Emanuel (2024): Authorities name 806 soldiers, 68 police officers killed in Gaza war. *Times of Israel*. 2024.11.26. Online: https://www.timesofisrael.com/authorities-name-44-soldiers-30-police-officers-killed-in-hamas-attack/

FABIAN, Emanuel (2024): IDF spokesman: Majdal Shams death toll risen to 12, Hezbollah used Iranian-made rocket. *Times of Israel*. 2024.07.28. Online: https://www.timesofisrael.com/liveblog_entry/hagari-majdal-shams-death-toll-risen-to-12-hezbollah-used-iranian-made-rocket/

FELDMAN, Shai (2021): The Impact of the May 2021 Hamas-Israel Confrontation. *Crown Center for Middle East Studies*. 2021.10.28. Online: https://www.brandeis.edu/crown/publications/crown-conversations/cc-10.html

FOUNDATION FOR DEFENSE OF DEMOCRACIES (2024): *Elimination of Hezbollah Leader Hassan Nasrallah a Watershed Moment in Israel's War Against Iranian Proxies*. 2024.09.28. Online: https://www.fdd.org/analysis/2024/09/28/elimination-of-hezbollah_-leader-hassan-nasrallah-a-watershed-moment-in-israels-war-against-iranian-proxies/

FRANKEL, Julia– LEE, Matthew – MAGDY, Samy (2024): US says it will not limit Israel arms transfers after some improvements in flow of aid to Gaza. *AP News*. 2024.11.24. Online: https://apnews.com/article/israel-palestinians-hamas-war-aid-us-48cd09c1c007cacd6d7a309589490320

FREILICH, D. Charles (2018): *Israeli National Security: A New Strategy for an Era of Change*. London: Oxford University Press.

GAT, Azar (2024): Expanding Israel's Ground Forces or Prioritizing Technology? *Institute for National Security Studies*. 2024.03.24. Online: https://www.inss.org.il/publication/land-force/

GOL, Jiyar (2024): Iran faces dilemma of restraint or revenge for attacks on ally Hezbollah. BBC. 2024.09.26. Online: https://www.bbc.com/news/articles/clylgv2dk3yo

HAID, Haid (2024): The strike on Iran's consulate in Syria could be the spark that ignites the Middle East. *Chatham House*. 2024.04.22. Online: https://www.chathamhouse.org/2024/04/strike-irans-consulate-syria-could-be-spark-ignites-middle-east

HAZUT, Guy – SHELAH, Ofer (2024): The IDF Ground Operation in Lebanon — Goals, Alternatives and Consequences. *Institute for National Security Studies*. 2024.10.14. Online: https://www.inss.org.il/publication/ground-maneuver/

HECHT, Eado (2024): The Gaza Terror Offensive 28 September – 17 October 2024. *Begin-Sadat Center for Strategic Studies*. 2024.10.18. Online: https://besacenter.org/the-gaza-terror-offensive-october-7-8-2023/

HEIMANN, Ariel (2024): The Reserve Forces in the Gaza War: Challenges for the Continuation of the Fighting. *Institute for National Security Studies*. 2024.01.07. Online: The Reserve Forces in the Gaza War: Challenges for the Continuation of the Fighting. Online: https://www.inss.org.il/publication/reserve-october-7/

HOKAYEM, Emile (2024): Israel's attack leaves Iran with a difficult dilemma. *International Institute for Strategic Studies*. 2024.10.28. Online: https://www.iiss.org/online-analysis/commentary/2024/10/israels-attack-leaves-iran-with-a-difficult-dilemma/

I24NEWS ENGLISH (2023): Female IDF soldiers recount tank battle on October 7. *Youtube*. 2023.11.28. Online: https://www.youtube.com/watch?v=oA9RLwInqn4

IZRAELI MINISZTERELNÖKI HIVATAL (2023): *Security Cabinet Approves War Situation.* 2023.10.08. Online: https://www.gov.il/en/departments/news/spoke-war081023?__cf_chl_tk=.7_SMyTUiosgLbOD2xpdlzxDY6WRX9HF04tmWX76v3c-1732619795-1.0.1.1-stJuWb09gWJT5Dx.o1plODoIXTBTg2Ce_AUMkBmUPAI

IZRAELI VÉDELMI ERŐK (2023a): *Battle of Kibbutz Be'eri.* 2023.11.07. Online: https://www.idf.il/en/mini-sites/7-10-the-inquiries/all-of-the-7-10-inquiries/battle-of-kibbutz-be-eri-the-inquiry/

IZRAELI VÉDELMI ERŐK (2023b): *Hamas Terrorists Continue to Prevent Civilian Evacuation in Gaza.* 2023.10.26. Online: https://www.idf.il/en/mini-sites/idf-press-releases-israel-at-war/october-23-pr/hamas-terrorists-continue-to-prevent-civilian-evacuation/

IZRAELI VÉDELMI ERŐK (2024a): *Exposed Hezbollah's Plan to „Conquer the Galilee".* 2024.10.01. Online: https://www.idf.il/en/mini-sites/exposed-hezbollah-s-plan-to-conquer-the-galilee/

IZRAELI VÉDELMI ERŐK (2024b): *Press Briefing by IDF Spokesperson RAdm. Daniel Hagari- July 27, 2024*. Online: https://www.idf.il/en/mini-sites/israel-at-war/briefings-by-idf-spokesperson-rear-admiral-daniel-hagari/july-24-press-briefings/press-briefing-by-idf-spokesperson-radm-daniel-hagari-july-27-2024/

JEWISH NEWS SYNDICATE (2023): *Netanyahu to keep Gallant as defense minister*. 2023.04.03. Online: https://www.jns.org/netanyahu-to-keep-gallant-as-defense-minister/

JEWISH NEWS SYNDICATE (2024a): *7,000 Gazans took part in Oct. 7 attacks, new IDF data shows*. 2024.09.01. Online: https://www.jns.org/7000-gazans-took-part-in-oct-7-attacks-new-idf-data-shows/

JEWISH NEWS SYNDICATE (2024b): *Gallant: Hezbollah must withdraw north of Litani River*. 2024.08.14. Online: https://www.jns.org/gallant-hezbollah-must-withdraw-north-of-litani-river/

KAHAV, Avi (2023): Cahi Hanegbi: Tévedtünk, két és fél órával a támadás előtt több jelzés érkezett (צחי הנגבי: "טעינו, שעתיים וחצי לפני המתקפה הגיעו אינדיקציות שונות"). *Izrael HaJom*. 2023.10.14. Online: https://www.israelhayom.co.il/news/geopolitics/article/14708908

KAM, Ephraim (2021): Iran's Deterrence Concept. *Institute for National Security Studies*. Online: https://www.inss.org.il/strategic_assessment/irans-deterrence-concept/

KELLER-LYNN, Carrie (2023): Gallant vows to 'wipe Hamas from earth,' after 'the worst terror attack' in history. *Times of Israel*. 2023.10.12. Online: https://www.timesofisrael.com/gallant-vows-to-wipe-hamas-from-earth-after-the-worst-terror-attack-in-history/

KHOURI, Rami G. (2024): Arab States Have Supported and Shunned Hamas in the Gaza War. *Arab Center Washington DC*. 2024.02.21. Online: https://arabcenterdc.org/resource/arab-states-have-supported-and-shunned-hamas-in-the-gaza-war/

KINGSLEY, Patrick – BOXERMAN, Aaron – SOBELMAN, Gabby (2023): „There Were Terrorists Inside": How Hamas's Attack on Israel Unfolded. *New York Times*. 2023.10.08. Online: https://www.nytimes.com/2023/10/08/world/middleeast/israel-hamas-attack.html

KIRCHWEGER, Stefanie (2024): Predicting the Unpredictable: Anticipating Disruptive Terrorist „Innovation". *Begin-Sadat Center for Strategic Studies*. BESA Center Perspectives Paper No. 2,293. Online: https://besacenter.org/predicting-the-unpredictable-anticipating-disruptive-terrorist-innovation/

KONGRESSZUSI KÖNYVTÁR (2023): *Israel: Government Declares War and Special Situation on Home Front Following October 7 Hamas Attacks.* 2023.12.12. Online: https://www.loc.gov/item/global-legal-monitor/2023-12-11/israel-government-declares-war-and-special-situation-on-home-front-following-october-7-hamas-attacks/

KRASNA, Joshua – MELADZE, George (2021): *The "Four Plus One": The Changing Power Politics of the Middle East*. The Moshe Dayan Center. Online: https://dayan.org/content/four-plus-one-changing-power-politics-middle-east

LAISH, Gur (2024): The Long War Phenomenon: Is a New Security Concept Required After October 7? *Begin-Sadat Center for Strategic Studies.* BESA Center Perspectives Paper No. 2,295. Online: https://besacenter.org/the-long-war-phenomenon-is-a-new-security-concept-required-after-october-7/

LAPIN, Yaakov (2023): Radwan Force's plans for Oct. 7-style massacre mostly thwarted. *Jewish News Syndicate*. 2024.09.25. Online: https://www.jns.org/radwan-forces-plans-for-oct-7-style-massacre-mostly-thwarted/

LUKIV, Jaroslav (2024): Israel sets new war goal of returning residents to the north. *BBC*. 2024.09.17. Online: https://www.bbc.com/news/articles/cglkkrj94ldo

LUPOVICI, Amir (2024): Israeli Deterrence and the October 7 Attack. *Institute for National Security*. Online: https://www.inss.org.il/strategic_assessment/deterrence/

MACKENZIE, Jean (2023): South Korea fears Hamas-style attack from the North. *BBC*, 2023.11.14. Online: https://www.bbc.com/news/world-asia-67411657

MAGID, Jacob (2024): UAE signals willingness to join postwar Gaza peacekeeping force. *Times of Israel*. 2024.07.21. Online: https://www.timesofisrael.com/uae-signals-willingness-to-join-post-war-gaza-peacekeeping-force/

MAHMOUDIAN, Arman (2023): Hamas is Only One of Four Iranian Fronts Against Israel. *Stimson Center.* 2023.10.12. Online: https://www.stimson.org/2023/hamas-is-only-one-of-four-iranian-fronts-against-israel/

MAKOVSKY, David (2024): Reminder: The Hostages (or: Why an „All for All" Deal Doesn't Help Them). *Washington Institute.* 2024.09.24. Online: https://www.washingtoninstitute.org/policy-analysis/reminder-hostages-or-why-all-all-deal-doesnt-help-them

MARGOLIN, Devorah – NEUMANN, Neomi (2024): Countering Hamas's Shadow Governance in Gaza. *Washington Institute.* PolicyWatch 3948. 2024.10.25. Online: https://www.washingtoninstitute.org/policy-analysis/countering-hamass-shadow-governance-gaza

MCCABE, Riley (2024): Ismail Haniyeh's Assassination: Escalation or an Off-Ramp? *Center for Strategic and International Studies*. 2024.08.01. Online: https://www.csis.org/analysis/ismail-haniyehs-assassination-escalation-or-ramp

MEIR AMIT INTELLIGENCE AND TERRORISM INFORMATION CENTER (2024): *Muhammad Dahlan and His Possible Involvement in "The Day After" in the Gaza Strip*. 2024.11.25. Online: https://www.terrorism-info.org.il/en/muhammad-dahlan-and-his-possible-involvement-in-the-day-after-in-the-gaza-strip/

MIZRAHI, Orna – DEKEL, Udi – BAZAK, Yuval (2021): The Next War in the North: Scenarios, Strategic Alternatives, and Recommendations for Israel. *Institute for National Security Studies.* Memorandum No. 211. Online: https://www.inss.org.il/publication/next-war-in-the-north/

MIZRAHI, Orna – SCHWEITZER, Yoram (2024): *100 Days of Fighting Against Hezbollah: An Interim Assessment*. Institute for National Security Studies. INSS Insight No. 1815. 2024. január 17. Online: https://www.inss.org.il/publication/hezbollah-swords-of-iron/

N. RÓZSA Erzsébet (2024): Változó regionális rend a Perzsa-öbölben? *Külügyi Szemle,* 2023(1), 54–71.

NETANYAHU, Benjamin (2024): Statement by Prime Minister Benjamin Netanyahu. *Youtube*. 2024.10.17. Online: https://www.youtube.com/watch?v=i9-_nvSbEo8&t=9s

NEW YORK TIMES (2023): *Where Was the Israeli Military?* 2023.12.30. Online: https://www.nytimes.com/2023/12/30/world/middleeast/israeli-military-hamas-failures.html

ORION, Assaf (2024): To Defeat Iran's Resistance Axis, the IDF Needs a New Strategy—and a Unified Country. *Foreign Affairs*. 2024.09.12. Online: https://www.foreignaffairs.com/israel/israel-and-coming-long-war

ORTAL, Eran (2024): A Sustainable Strategy: Principles for Updating Israel's Strategy and Security Concept. *Begin-Sadat Center for Strategic Studies*. Mideast Security and Policy Studies No. 205. Online: https://besacenter.org/wp-content/uploads/2024/07/205ENGweb.pdf

PARAGI Beáta (2024): Hamász és iszlám ellenállás a Gázai övezetben. *Külügyi Szemle,* 23(1), 72–93. Online: https://hiia.hu/wp-content/uploads/2024/05/5-Paragi-Beata.pdf

RADFORD, Antoinette – SANGAL, Aditi – CHOWDHURY, Maureen – POWELL, Tori B. – MAGRAMO, Kathleen (2024): November 26, 2024 – Israel-Hezbollah ceasefire news. *CNN*. 2024.11.26. Online: https://edition.cnn.com/world/live-news/israel-hezbollah-ceasefire-deal-gaza-war-11-26-24-intl-hnk/index.html

ROBINSON, Kali (2024): Who Governs the Palestinians? *Council on Foreign Relations*. Online: https://www.cfr.org/backgrounder/who-governs-palestinians

RUDNITZKY, Arik (2023): On a tightrope: Israel's Arab citizens and the War Between Israel and Hamas. *Israeli Democracy Institute*. 2023.11.13. Online: https://en.idi.org.il/articles/51473

SAID, Summer (2023): Hamas Tells Civilians Not to Evacuate to the South. *Wall Street Journal*. 2023.10.23. Online: https://www.wsj.com/livecoverage/israel-hamas-war-gaza-strip/card/hamas-tells-civilians-not-to-evacuate-to-the-south-T9TX4p5KHl930OHJDyfp

SAID-MOORHOUSE, Lauren – KOTTASOVÁ, Ivana – JOHN, Tara – TANNO, Sophie – TAYLOR, Jerome –CHOI, Annette – ROBERTS, Gillian –O'BRIEN, Kathy Rose – SMITH-SPARK, Laura – KORBER, Hoffman Joshua (2024): Who are the hostages freed during the Israel-

Hamas conflict? *CNN*. 2024.08.27. Online: https://edition.cnn.com/interactive/2023/12/world/hostage-israel-hamas-deal-dg/

SALAMI, Mohammad (2024): Egypt-Iran Normalization: The View from the Gulf. *Gulf International Forum.* Online: https://gulfif.org/egypt-iran-normalization-the-view-from-the-gulf/

SATLOFF, Robert – ROSS, Dennis – MAKOVSKFY, David (2023): Israel's War Aims and the Principles of a Post-Hamas Administration in Gaza. *Washington Institute*. 2023.10.17. Online: https://www.washingtoninstitute.org/policy-analysis/israels-war-aims-and-principles-post-hamas-administration-gaza

SCHMITT, Michael N. (2023): Israel – Hamas 2023 Symposium – What is and is not Human Shielding? Articles of War. *Lieber Institute – West Point*. 2023.11.03. Online: https://lieber.westpoint.edu/what-is-and-is-not-human-shielding/

SHABAN, Mohammad Ali (2024): Iran After October 7. *Center for Strategic and Insternational Studies*. 2024.11.12. Online: https://www.csis.org/analysis/mohammad-ali-shabani-iran-after-october-7

SHABTAI, Shay (2024): What Would „Total Victory" Mean in Gaza? *Begin-Sadat Center for Strategic Studies*. BESA Center Perspectives Paper No. 2,267. Online: https://besacenter.org/what-would-total-victory-mean-in-gaza/

SHAIKH, Shaan (2024): The Iran-Israel Air Conflict, One Week In. *Center for Strategic and International Studies*. 2024.04.19. Online: https://www.csis.org/analysis/iran-israel-air-conflict-one-week

SHAMIR, Eitan (2024): A Not an End State but a Long Game: Israel's Strategic Goals in the Iron Swords War. *Begin-Sadat Center for Strategic Studies*. BESA Center Perspectives Paper No. 2, 314. Online: https://besacenter.org/not-an-end-state-but-a-long-game-israels-strategic-goals-in-the-iron-swords-war/

SOBELMAN, Daniel (2024): Israel and the Axis of Resistance in the wake of the Gaza war. *Middle East Institute.* 2024.08.24. Online: https://www.mei.edu/publications/israel-and-axis-resistance-wake-gaza-war

STEINBERG, Jessica (2024): Sderot memorializes police station that was destroyed on October 7. *Times of Israel*. 2024.11.24. Online: https://www.timesofisrael.com/sderot-memorializes-police-station-that-was-destroyed-on-october-7/

TARNOPOLSKY, Noga – RUBIN, Shira (2023): Israel massed troops in the West Bank. Then Hamas attacked from Gaza. *Washington Post*. 2023.10.09. Online:

https://www.washingtonpost.com/world/2023/10/09/israel-hamas-attack-gaza-intelligence/

TÜRK, Volker (2024): 40,000 Palestinian lives lost in Gaza: UN Human Rights Chief pleads for end to fighting stating that 130 people have been killed every day in Gaza over the past 10 months. *United Nations*. 2024.08.15. Online: https://www.un.org/unispal/document/gaza-40000deaths-turk-ohchr-15aug24/

YAGNA, Yanir (2023): Hat lakos tucatnyi terrorista ellen: a Sofa kibuc hősei felidézik (שישה תושבים מול עשרות מחבלים: גיבורי הקרב בקיבוץ סופה משחזרים). *Walla*. 2023.10.13. Online: https://news.walla.co.il/item/3615926

YOO, John - RABKIN, Jeremy (2024): The Laws of War and Their Application in Israel's Fight Against Hamas. Strategika No. 89. *Hoover Institution*. Online: https://www.hoover.org/sites/default/files/issues/resources/Strategika_89_WebreadyPDF.pdf

ZIMMT, Raz (2024): Toward Possible Changes in Iran's Security Concept. *Institute for National Security Studies*. INSS Insight No. 1915. 2024.11.18. Online: https://www.inss.org.il/publication/iran-changes/

VÁKÁT OLDAL

Viszkocsil László

A terrorfinanszírozás hagyományos és új típusú finanszírozásának vizsgálata

1. BEVEZETÉS

A közelmúltban Európában és a világ többi részén elkövetett terrorcselekményeket vizsgálva megállapítható, hogy a terrorizmus és annak finanszírozása a XXI. század egyik legjelentősebb globális biztonsági kihívása, amely a geopolitikai, társadalmi és technológiai változásokat kihasználva folyamatosan új elkövetési módokat generál, így azok jelentős biztonsági kockázatot jelentenek a társadalom teljes egészére. A konkrét terrorcselekmények megelőzése mellett fokozatosan nő a mögöttük húzódó pénzügyi hálózatok felderítése és felszámolása iránti igény a nemzetközi és nemzeti rendészeti, nemzetbiztonsági szervek részéről.

A terrorfinanszírozás elleni hatékony fellépés aktualitását tovább növeli a digitális technológiák szignifikáns térhódítása, amely új lehetőségeket teremt a terrorszervezetek számára mind a vagyonszerzés, mind annak felhalmozása és felhasználása terén, miközben a hatóságok számára fokozódó kihívásokat jelent a tranzakciók nyomon követése és a finanszírozási csatornák detektálása, felszámolása.

A terrorizmus finanszírozásának hagyományos és modern módszerei közötti átalakulás megismerése elengedhetetlen a hatékony terrorelhárítási stratégiák kidolgozásához, mivel a globalizáció és a digitális forradalom nemcsak a terrorszervezetek működését változtatta meg, hanem a finanszírozási mechanizmusaikat is. Magyarország szempontjából a téma különösen releváns, mivel hazánk földrajzi helyzete és nemzetközi szerepvállalásai miatt potenciális – de jellemzően tranzit – célpontja lehet terrorizmusfinanszírozással kapcsolatba hozható hálózatoknak.

Kutatásom elsősorban kvalitatív módszereket használ és a releváns hazai és nemzetközi jogszabályokat, ajánlásokat, illetve terrorizmus elhárításban érintett szervek publikációit veszi alapul. Esettanulmányok és konkrét példák segítségével mutatom be a terrorszervezetek által alkalmazott finanszírozási módszereket, különös tekintettel a hagyományos és a modern elkövetési technikákra. A kutatásomban az előzőeken túl bemutatom továbbá a globális pénzügyi rendszerek változásait is, valamint ezzel párhuzamosan a technológiai fejlődés hatását a terrorizmus finanszírozására.

A tanulmányom célja, hogy átfogó képet nyújtson a terrorizmusról és annak finanszírozásáról, különös tekintettel a múltbeli, jelenlegi és jövőbeli kihívásokra, amelyeket a technológiai fejlődés idéz elő.

2. SZÜKSÉGLETEK, GAZDASÁGI RACIONALITÁS

A létezésünkhöz és cselekvésünkhöz elengedhetetlen szükségleteink alapvetően két fő csoportra, a termékek (anyagi szükségletek) és szolgáltatások (nem anyagi szükségletek) piacára osztható, melyeket - a jelen társadalmában jellemzően - pénzzel tudunk megvásárolni. Valamennyi gazdasági szereplő, legyen az természetes vagy jogi személy, legális vagy illegális entitás a szükségletei maximális kielégítésére törekszik, amelyhez úgynevezett javakat vagy jószágokat használ fel. Az anyagi javak felosztható szabad és gazdasági javakra.

A szabad javak körébe tartozik valamennyi olyan termelési tényező, amely a természetben „végtelen" mennyiségben megtalálható, úgynevezett természeti tényező. Ide tartozik többek között a víz és a föld. A gazdasági javak fő forrása a termelés, melyhez különféle termelési tényezők szükségesek, így hozzáférésük térben és időben korlátozott, létrehozásukhoz a legtöbb esetben más javakat kell felhasználni, transzformálni.

A terrorszervezetek esetében a szabadon hozzáférhető eszközök köre lehet egy, a hatóságok előtt ismeretlen helyen létesített kiképzőközpont. Ezzel szemben gazdasági jószágként definiálhatjuk a céljaik eléréséhez szükséges fegyverek, robbanóanyagok, járművek beszerzését, amiket gyártókapacitás hiányában előállítani nem tudnak, így azok beszerzéséhez pénzre van szükségük.[1] Közgazdasági szempontból a különféle terror- és radikális szervezetek nagyfokú átfedést mutatnak a klasszikus értelemben vett vállalkozásokkal, mivel azok:[2]

- meghatározott cél érdekében jöttek létre;
- különböző időtávokon politikai, gazdasági, katonai céllal, úgynevezett vízióval rendelkeznek;
- működésük és céljaik elérése érdekében gazdálkodási, termelő vagy egyéb (pl.: adománygyűjtő) tevékenységet folytatnak;

[1] LUTZ – LUTZ (2006)
[2] PEDAHZUR – PERLIGER (2006)

– és mindezek megvalósíthatósága érdekében toborzó, humánigazgatási tevékenységet folytatnak.[3]

A fenti gazdasági logika feltérképezése és megértése segítheti az erőforrás-áramlás, így például a terrorizmus finanszírozás detektálását és nyomon követhetőségének ténybeli megismerését.

3. TERRORSZERVEZETEK BEVÉTELI FORRÁSAI

Bevételi forrásaik alapvetően két nagy csoportba sorolhatóak, mint legális és illegális bevételi források. Ezek azonban sok esetben nehezen vagy egyáltalán nem különíthetőek el egymástól, ami megnehezíti a terrorizmus finanszírozásának felderítését.

Legális bevételi források:

– Adományok, adók gyűjtése,
– olaj és ásványkincsek kiaknázása, kereskedelme,
– gazdasági társaságok, fedővállalkozások működtetése,
– állami támogatások.

Illegális források, különféle bűncselekmények elkövetése, mint:

– Embercsempészet és emberkereskedelem (beleértve a kényszermunkát is);
– kábítószer előállítás és kereskedelem;
– zsarolás, emberrablás, védelmi pénzek gyűjtése;
– fegyverkereskedelem;
– kibertérben elkövetett cselekmények.

Az iráni kormány nyíltan támogatja pénzzel, logisztikai segítséggel, illetve fegyverrel is a Hezbollahot, valamint a húszi lázadókat. Évente százmillió dolláros nagyságrendű összegekkel, fegyverekkel és logisztikai segítséggel, akiket az „ellenállás tengelyének” tart kommunikációjában is. Az így juttatott támogatások az iráni jogrendszerben legálisnak tekinthetőek.[4]

A Hezbollah[5] jelentős összegeket gyűjtött és vélhetően jelenleg is gyűjt adományokat a libanoni síita közösségektől, valamint a diaszpórához tartozó külföldön élő személyektől

[3] Ide sorolhatóak többek között az általuk végzett képzések, de az olyan tevékenységek is, mint fizetés, „zsold” vagy özvegyi járadékok fizetése.
[4] LANE (2023)
[5] A Hezbollah („Isten Pártja”) egy libanoni síita iszlamista politikai és katonai szervezet, amelyet 1982-ben alapítottak, Irán támogatásával, az izraeli megszállás elleni harcra válaszul. Katonai, politikai és szociális „szárnnyal” rendelkezik. Politikai szárnya libanoni parlamentben jelentős szerepet játszik, szociális hálózata kórházat, klinikákat, iskolákat és mezőgazdasági központokat működtet, olcsó vagy ingyenes szolgáltatásokat nyújtva, elsődlegesen a síita közösségnek. Katonai szárnya, a Dzsihád Tanács, a libanoni hadseregnél erősebb

például Nyugat-Afrikában és Dél-Amerikában élő libanoniaktól. Az általuk korábban felügyelt területeken adót szedtek az ott élőktől, amit vallási vagy közösségi hozzájárulásként tüntettek fel.[6]

Az Iszlám Állam (továbbiakban: ISIS) 2014-2017 között az általuk elfoglalt szíriai és iraki területeken olajmezőket üzemeltetett, például a Deir ez-Zor régióban. Az olajat helyi kereskedőkön, fedővállalkozásokon keresztül értékesítették Törökországba, amiből akár napi 1-2 millió dollár bevételhez jutottak.[7]

Az ISIS Líbiában és Szíriában az ott kezdődő polgárháborús időszak kezdetén fegyvereket szerzett, majd azokat értékesítette más fegyveres csoportoknak a feketepiacon[8]. A szervezet, amelyik – gyengülését követően – alkalmazkodott a megváltozott környezethez. Dokumentáltan alkalmaztak kibertámadásokat, adathalász kampányokat és zsarolóvírusokat annak érdekében, hogy pénzügyi forrásokhoz jussanak.[9]

A Boko Haram Nigériában és a környező országokban emberrablásokat hajt és hajtott végre, ilyen volt például a 2014-es chiboki iskoláslányok elrablása is, akiket később váltságdíj ellenében engedtek szabadon.[10]

A tálib csoportok Afganisztánban az ópium és heroinkereskedelem kulcsszereplőinek tekinthetőek. Az ENSZ becslései szerint 2020-ban a bevételeik jelentős része, akár 400 millió dollár ezen tevékenységükből származott.[11]

A sri lankai Tamil Ílam Felszabadító Tigrisei nevű terrorszervezet a tamil diaszpóra által lakott területeken működtetett különféle vállalkozásokat (pl. éttermeket, szállítmányozási cégeket), amelyek fedőtevékenységként szolgáltak, hogy azokon keresztül a törvényesség látszatát keltve pénzmosási és terrorizmus finanszírozási tevékenységet végezzenek szervezetük számára.[12]

---

fegyveres erővel rendelkezik, és számos ország, például Izrael, vagy az Európai Unió terrorista szervezetként tartja számon.

[6] LEVITT (2013)
[7] FINANCIAL ACTION TASK FORCE (2015b)
[8] CONFLICT ARMAMENT RESEARCH (2017)
[9] EUROPOL (2020)
[10] THURSTON (2017)
[11] UNITED NATIONS OFFICE ON DRUGS AND CRIME (2021)
[12] HUMAN RIGHTS WATCH (2006)

4. A GLOBÁLIS PÉNZÜGYI VILÁG ÉS FIZETÉSI TRENDEK VÁLTOZÁSA

A fizetési és tranzakciós szokások, illetve esetszámok jelentős változáson mentek keresztül a 2000-es évektől napjainkig. A bázis időszakban jellemzően a hagyományos papíralapú tranzakciók domináltak, a készpénzforgalom mellett. A banki online jelenlét kezdetleges volt, a díjak viszont magasnak mondhatóak.

A 2010-es évek elején a digitális pénzforgalom robbanásszerű növekedésnek indult, amely megfelelő környezetet teremtett a terrorszervezetek forrásai eredetének, tranzaktálásának leplezéséhez. Akkoriban jelentek meg az első szélesebb körben hozzáférhető internetes banki alkalmazások, amelyek rövid időn belül a fő tranzakciós eszközzé váltak, a díjak pedig csökkenésnek indultak. A bankkártya, mint fizetési eszköz általánosan is elfogadottá vált és elkezdődött az NFC[13] alapú fizetési megoldások bevezetése.

A 2020-as évek elejére a fizetési és átutalási szokások tovább változtak, amit jelentősen befolyásolt a 2019-es COVID–19 világjárvány. Az új technológiák, mint a kriptovaluták és a blokklánc-alapú rendszerek egyre inkább elérhetőek lettek és nagyobb szerepet kaptak az érintésmentes, online, illetve mobilfizetési megoldások, mivel a személyes tranzakciók elkerülése érdekében sokan az elektronikus fizetési lehetőségeket választották. Annak ellenére, hogy a klasszikus értelemben vett fintech[14] cégek, mint a Revolut vagy Wise már a 2010-es évek közepén megjelentek, globális térhódításuk erre az időpontra datálható.

A globális fizetési rendszer bővülésére vonatkozó adatok[15] szerint 2014. év elején napi szinten 21,58 millió tranzakció ment végbe a SWIFT[16] rendszeren keresztül. 2019. év végére ez 36,07 millióra, majd 2022. decemberére 45,2 millió tranzakcióra emelkedett, és a keresztülhaladó pénzösszeg átlagosan napi 5-6 ezermilliárd dollárt tett ki globálisan.

A SWIFT tekinthető a legnagyobb fizetési hálózatnak, de globálisan azzal párhuzamosan több másik is üzemel, mint például:

- az Amerikai Egyesült Államokban működő CHIPS[17];
- az Európai Unió (továbbiakban: EU) által működtetett SEPA[18];

[13] Near Field Communication: rövid hatótávú kommunikációs szabványgyűjtemény okostelefonok és hasonló eszközök között, egymáshoz érintéssel vagy egymáshoz nagyon közel helyezéssel (maximum pár centiméter) létrejövő rádiós kommunikációra.

[14] Financial Technology: pénzügyi technológia rövidítése, amely magában foglalja az okoseszközökön internethasználat mellett végrehajtott banki és pénzügyi ügyintézést.

[15] STATISTA (2023)

[16] A bankszektor szereplőinek tulajdonában lévő kommunikációs hálózat, amely standardizált és biztonságos üzenetforgalmat kínál, saját hálózati kapcsolódási megoldásokon keresztül a világ legtöbb országban közel 10 ezer pénzügyi intézménynek.

[17] Clearing House Interbank Payments System: elsősorban az amerikai pénzügyi intézmények közötti tranzakciók gyorsaságát segíti elő.

– a kínai CIPS[19];
– vagy az Oroszországi Föderáció által felügyelt SPFS[20] és RUB[21].

2000. és 2010. között a globálisan[22] a gyanús tranzakcióval érintett bejelentések száma hozzávetőleg 300.000-ről 3–4 millióra nőtt a pénzügyi szektor fejlődése mellett, majd 2020-ra ez a szám elérte az 5–6 milliós darabszámot.[23] Ezen tranzakciók közül 1–5 % volt érintett közvetlenül terrorizmus finanszírozásában.

A párhuzamosan működő, bankok közötti fizetési rendszerek jelentősen befolyásolhatják – akár negatív irányba is – a terrorszervezetek által tranzaktált pénzeszközök valós időben történő felderítésének lehetőségét az illetékes hatóságok számára. Példaként említhető a Kongói Demokratikus Köztársaságban működtetett Banque Congolaise nevű pénzügyi intézmény, amelyen keresztül a libanoni Hezbollah tevékenysége finanszírozásához szükséges forrásokhoz jutott.[24]

A jövőben a trendek figyelembevétele alapján folytatódik az online és mobilfizetések számának emelkedése, valamint új típusú digitális pénzügyi megoldások (pl.: CBDC[25]) is elterjedhetnek, amelyek a fizetési szokások megváltozásához vezetnek, ilyen módon hatással lehetnek az ez idáig ismert terrorizmus finanszírozási metódusokra.

5. A TERRORIZMUS ÉS FINANSZÍROZÁSÁNAK EVOLÚCIÓJA

A modernkori terrorizmus az elmúlt negyed évszázadban jelentős átalakuláson ment keresztül és ebben trendválasztóként értelmezhető a 2001. szeptember 11. napján, az al-Kaida terrorszervezet tagjai által a World Trade Center tornyai ellen elkövetett támadások, majd az azt követő globális terrorszervezetek elleni küzdelem.

Az Amerikai Egyesült Államok területén végrehajtott támadásokkal bezárólag a szervezetek fő célja a lehető legnagyobb támadás végrehajtása volt, aminek a kivitelezéséhez kis túlzással „korlátlan” mennyiségű pénz állt rendelkezésükre.

---

[18] Single Euro Payments Area: az Európai Unió tagállamaiban és néhány más európai országban egységesített átutalásokat tesz lehetővé.
[19] Cross-Border Interbank Payment System: a jüanban végzett nemzetközi tranzakciók egyszerűsítését segíti elő.
[20] System for Transfer of Financial Messages: Az orosz központi bank, a **Bank of Russia** által üzemeltetett rendszer, amely a SWIFT alternatívájaként működik.
[21] Russian Ruble Payments System: Az orosz rubelben történő belföldi és nemzetközi átutalások kezelésére szolgál.
[22] Az értékek centralizáltan nem állnak rendelkezésre, amelynek részben oka, hogy a gyanús tranzakciók bejelentésére országonként eltérő szabályozás vonatkozik, illetve az ezeket kezelő hatóságok, a pénzügyi hírszerző egységek eljárásrendje, publikációs szemlélete is eltérő. A közölt értékek egyfajta szakmai konszenzusnak tekinthetőek.
[23] *Financial Crimes Enforcement Network*. www.fincen.gov
[24] LEVY (2013)
[25] Központi banki digitális valuta.

Az említett támadás „sikerét” követő globális fellépés eredményeként a radikális szervezetekhez köthető vagyonelemek, így az akkoriban legjellemzőbb készpénz és jelentősen kisebb mennyiségű - bankszámlákon elhelyezett - bankbetét lefoglalásra kerültek a különböző országok rendőri- és nemzetbiztonsági hatóságai által. Ez átmeneti nehézséget okozott a terrorszervezetek számára.

Globális szinten a terrorszervezetek csoportdinamikája megváltozott a felderítésükre tett hatékony erőfeszítésekre válaszul. Vertikális struktúrából átváltottak horizontális, sejt-szerű tagolódásra, ahol a kisebb csoportok közötti utasítási és kommunikációs kapocs enyhült.

Az elkövetett cselekmények is jelentős átalakuláson mentek keresztül: A 2010-es évekre elkezdték előnyben részesíteni az úgynevezett magányos elkövetők által végrehajtott terrorcselekményeket, amelyek célja nem a pusztítás mértékének maximalizálása, hanem az áldozatok számának növelése és a költségek minimalizálása volt. Ezeknek a támadásoknak az elkövetői még jellemzően a terrorszervezet tagjai közül kerültek ki, vagy a terrorszervezet tagjaitól kaptak kiképzést. A 2010-es években az ISIS térhódításának meghatározó újítása volt a digitális technológia felhasználása, mint egészen addig kihasználatlan technológia, amelyet a radikális tartalmak terjesztésére, toborzásra és működésük érdekében pénzeszközök gyűjtésére használtak.

Napjainkra a terrorszervezetek kiterjedt toborzó és pénzgyűjtő tevékenységüket az interneten folytatják és az Európában elkövetett cselekményekre másod- és harmadgenerációs muszlim gyökerekkel rendelkező, vagy áttért személyeket toboroznak, finanszírozásukat pedig a korábbiakkal ellentétben jelentős mértékben interneten elérhető szolgáltatókon keresztül bonyolítják le.

A klasszikus vallási indíttatású terrorizmus mellett ismét megjelent a politikai polarizáció mentén jelentkező szélsőbal- és jobboldali belföldi terrorizmus, illetve a globális felmelegedéssel kapcsolatos ökoterrorizmus is.

A terrorszervezetek mellett a pénzügyi világ is jelentős változásokon ment keresztül a globalizáció és digitalizáció hatására. A csoportok finanszírozása az évtizedek során jelentős változásokon ment keresztül, így a finanszírozási források és mechanizmusok az idő múlásával egyre kifinomultabbá váltak, figyelembe véve a változó politikai, gazdasági és technológiai környezetet.

Az első modern terrorista csoportok jellemzően állami szereplőktől vagy nemzetközi politikai szövetségektől kapták a működésükhöz szükséges forrásokat támogatások formájában, amelyek megtestesülhettek pénzügyi segítségben, fegyverek átadásában,

képzések biztosításában. Az iszlamista szervezeteknél már ebben az időszakban megjelentek a vallási adományok (pl. zakát[26]), mint jelentős bevételi források.

Az al-Kaida által elkövetett, már fentebb említett cselekmény idején a terrorszervezetek számára az egyre terjeszkedő nemzetközi pénzügyi rendszerek, banki átutalások és a készpénzmozgások koordinálása kellően kooperatív, gyorsan elérhető és hatékony finanszírozási formát biztosítottak. Ebben az időben a terrorszervezetek céljaik elérése és tényleges tevékenységük leplezése érdekében elkezdtek létrehozni szervezeteket, amelyek jótékonysági szervezetként gyűjtöttek forrásokat.

A modernkori terrorfinanszírozás megjelenése és robbanásszerű fejlődése a már említett ISIS-hez köthető. Vezetőik az illegális bevételek és adományok mellett különböző „legális" tevékenységeket is bevételi forrásként használtak. Ilyenek voltak a Szíriában és Irakban ellenőrzés alá vont területeken kinyert természeti erőforrások, mint például az olaj értékesítése.

Kereskedelmi, vagyonfelhalmozási és felhasználási tevékenységük során különféle interneten elérhető pénzügyi szolgáltatást, illetve kripto- és digitális pénzkereskedelmi platformot kezdtek el használni, kombinálva olyan anonimitást biztosító technológiákkal, amelyek segítették a pénzeszközök kevésbé ellenőrzött vagy nem is detektálható áramlását az érintett szereplők között.

Napjainkban a terrorszervezetek az ISIS által alkalmazni kezdett eszközök és lehetőségek repertoárját alkalmazzák, finanszírozási oldalon pedig megjelentek a különböző kiberbűnözéssel összefüggő bevételi források, úgymint a zsarolóvírusok és adatlopások elkövetésével szerzett pénzeszközök.

Magyarországon ez idáig vallási indíttatású terrorcselekmény elkövetésére nem került sor, azonban a környező államokban több ilyen jellegű támadás is történt. Hazánk az EU, az Észak-atlanti Szerződés Szervezete (NATO) tagállamaként, valamint a nemzetközi terrorellenes küzdelem aktív résztvevőjeként tevékenyen lép fel a területén esetlegesen detektálható radikális személyek és cselekmények felderítése érdekében.[27]

A jelenlegi napi geopolitikai történések, illetve társadalmi struktúra ismeretében kijelenthetjük, hogy hazánk terrorizmusfinanszírozás szempontjából tranzit országnak számít, azonban fontos láncszeme az országokat átívelő terrorizmussal érintett hálózatoknak.[28]

[26] A zakát, elérheti egy teljes muszlim család vagyonának 2,5%-át is, amelyet „rászorulók" rendelkezésére bocsát.
[27] EUROPOL (2022)
[28] MAGYAR NEMZETI BANK (d.n.)

Napjainkban Magyarország és az EU terrorfenyegetettsége ugyan nem emelkedett jelentősen,[29] azonban az itt élő palesztin lakosság vagy a társadalomban jelenlévő egyéb csoportok tevőleges kiállása konkrét cselekményekben is megnyilvánulhat a HAMASZ, az Iráni Iszlám Köztársaság, illetve „húszi lázadók" iránt. Ez a támogatás akár konkrét cselekményekben is megnyilvánulhat, miközben anyagi eszközökkel is hozzájárulhatnak e szervezetek Izrael Állam, az EU intézményei vagy tagállamai elleni harcaihoz.

5.1. A TERRORIZMUS FINANSZÍROZÁS HAZAI ÉS SZŰKEBB MIKROGAZDASÁGI SZABÁLYOZÁSA

Az érintett jogszabályi keretrendszer a 2001. szeptember 11-i terrortámadásokat követően született meg. Maguk a támadások egyfajta nemzetközi indikátornak tekinthetők és paradigmaváltást hoztak a globális biztonságpolitikában, kiemelve a terrorista hálózatok pénzügyi támogatásának felszámolásának szükségességét.

Az ENSZ Biztonsági Tanácsának 1373. (2001) számú határozata kötelezte a tagállamokat a terrorizmus finanszírozásának kriminalizálására és a kapcsolódó vagyonbefagyasztási intézkedések bevezetésére, ezzel megalapozta a nemzetközi és regionális szintű jogalkotást.

Az EU a hivatkozott támadásokra válaszul gyors és átfogó intézkedéseket vezetett be az Európai Tanács 2001. szeptember 21-i rendkívüli ülésén, így a terrorizmus elleni hatékony fellépést az EU kiemelt feladatai közé emelte.

A folyamat részeként született meg a Tanács 2580/2001/EK (2001. december 27.) rendelete, amely a terrorizmus leküzdése érdekében egyes személyekkel és szervezetekkel szemben hozott különleges korlátozó intézkedésekről szólt. A rendelet célja a terrorcselekményekben érintett személyek, csoportok és szervezetek pénzeszközeinek és vagyoni értékű jogainak befagyasztása, valamint a banki és pénzügyi szektor által nyújtott szolgáltatások hozzáférésének korlátozása volt.

A rendelet pontosan meghatározza a pénzeszközök és a befagyasztás fogalmát, továbbá előírja a terroristák jegyzékének rendszeres felülvizsgálatát, amely az uniós és unión kívüli szervezetekre egyaránt vonatkozik. A 2580/2001/EK rendelet az ENSZ-határozatok implementációján túlmutatva egységes uniós megközelítést is biztosít.

[29] Hazánk terrorfenyegetettségi szintjének besorolását a *1824/2015. (XI. 19.) Kormány határoza*t szabályozza, amely meghatározza, hogy a Belügyminiszter a Terrorellenes Koordinációs Bizottság javaslatára vagy saját hatáskörében, a Védelmi Tanács egyetértésével dönt a fokozat elrendeléséről, módosításáról vagy megszüntetéséről. A terrorfenyegetettségi szint emelésére akkor kerül sor, ha konkrét, ellenőrzött vagy részben ellenőrzött információk alapján terrorcselekmény elkövetésének veszélye áll fenn az EU vagy a NATO tagállamaiban, és Magyarországon reális egy terrorcselekmény végrehajtásának lehetősége.

Az Európa Tanács 2005. évi, a terrorizmus megelőzéséről szóló egyezménye (CETS 196) a finanszírozás büntethetőségét hangsúlyozta, míg a varsói egyezmény (CETS 198) a pénzmosás és a terrorizmus finanszírozása elleni küzdelem integrált megközelítését szorgalmazta. Ezek az egyezmények a tagállamokat a nemzeti jogszabályok harmonizációjára ösztönözték.

Hazánkban a terrorizmus finanszírozása elleni fellépés jogi evolúciója megfelelt a nemzetközi és uniós előírásoknak. A terrorizmus finanszírozás a Büntető Törvénykönyvről szóló 2012. évi C. törvényben (továbbiakban: Btk.) önállóan került definiálásra, összhangban a 2580/2001/EK rendelettel, illetve a Btk. 2013-as módosítása a pénzeszköz fogalmát az uniós rendelet definíciójával összhangba hozta.

A pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról szóló 2017. évi LIII. törvény (továbbiakban: Pmt.), illetve annak hatályon kívül helyezett változatai további adminisztratív eszközöket vezettek be, például az ügyfél-azonosítási és szűrési kötelezettségeket, amelyek a pénzügyi szektor szereplőire vonatkoznak.

A jelenleg hatályos Pmt. nem tartalmaz explicit definíciót a vagyonelem fogalmára. A jogszabály kontextusában vagyonelemnek tekint minden olyan materiális vagy immateriális jószágot, amely pénzben kifejezhető értékkel bír és alkalmas lehet pénzmosás, illetve esetünkben a terrorizmussal kapcsolatba hozható szervezetek finanszírozására.

Az előzőek alapján az alábbiak lehetnek a terrorizmus finanszírozás elkövetésének eszközei:

- **Pénzeszközök**: készpénz, bankszámlán lévő egyenleg, elektronikus pénz.
- **Pénzügyi eszközök**: értékpapírok, kötvények, részvények, derivatívák.
- **Ingatlanok**: lakóingatlanok, kereskedelmi ingatlanok, földterületek.
- **Ingóságok**: nagy értékű tárgyak, drágakövek, műkincsek, nemesfémek, járművek.
- **Jogok és követelések**: vagyoni jogosultságot megtestesítő okiratok, dematerializált értékpapírok, szellemi tulajdonjogok.
- **Virtuális fizetőeszközök**: kriptovaluták, amelyek elektronikusan tárolhatók, csereértékként elfogadottak.

A Pmt. 1. § (1) bekezdése alapján a törvény hatálya kiterjed a Magyarországon székhellyel, fiókteleppel vagy telephellyel rendelkező következő szolgáltatókra, akik bejelentési kötelezettséggel bírnak, ha pénzmosásra vagy terrorizmus finanszírozására utaló adat, tény vagy körülmény merül fel:

- **Hitelintézetek**: bankok, takarékszövetkezetek.
- **Pénzügyi szolgáltatók**: befektetési vállalkozások, biztosítók, pénzváltók, lízingcégek.

- **Könyvvizsgálók**: kamarai tag könyvvizsgálók, könyvvizsgáló cégek.
- **Könyvelők**: számviteli, könyvviteli szolgáltatást nyújtók.
- **Adótanácsadók**: adószakértők, okleveles adóellenőrök.
- **Ügyvédek**: meghatározott tevékenységek esetén (például vagyonkezelés, cég alapítása, ingatlanügyletek).
- **Közjegyzők**: különösen vagyonátruházással kapcsolatos ügyletekben.
- **Ingatlanügylettel foglalkozók**: ingatlanok adásvételének vagy bérbeadásának közvetítői (havi 500 000 Ft feletti bérleti díj esetén).
- **Nemesfém-kereskedők**: nemesfémekkel vagy ezekből készült tárgyakkal kereskedők.
- **Árukereskedők**: nagy értékű áruk (például műkincsek, régiségek) kereskedői, ha az ügylet értéke eléri a 2,5 millió forintot.
- **Kulturális javak kereskedői**: műalkotások, régiségek kereskedelmével vagy közvetítésével foglalkozók.
- **Szerencsejáték-szolgáltatók**: kaszinók, online szerencsejáték-szervezők.
- **Bizalmi vagyonkezelők**: bizalmi vagyonkezelési szerződések kezelői.
- **Virtuális fizetőeszköz szolgáltatók**: kriptovaluta-váltással, letétkezeléssel foglalkozók.
- **Székhelyszolgáltatók**: székhelyszolgáltatást nyújtó vállalkozások.
- **Postai szolgáltatók**: pénzügyi tranzakciókat bonyolító postai szereplők.
- **Egyéb szolgáltatók**: a törvény által meghatározott, pénzmosási kockázattal érintett tevékenységet végzők (például pénzküldési szolgáltatók).

A Pmt. 30. § alapján a fenti szolgáltatók a Nemzeti Adó- és Vámhivatal Pénzmosás Elleni Információs Iroda (továbbiakban: NAV PEII) irányába kötelesek jelenteni a pénzmosásra vagy terrorizmus finanszírozására utaló tényeket, adatokat, körülményeket. A szolgáltatóknak a törvény rendelkezései alapján kockázatalapú megközelítést kell alkalmaznia és belső szabályzatot kell készíteniük a gyanús ügyletek azonosítására és kezelésére vonatkozó eljárási protokolljaikról.

5.2. A TERRORIZMUS FINANSZÍROZÁS ÉS PÉNZMOSÁS MEGAKADÁLYOZÁSÁT SZOLGÁLÓ INTÉZMÉNYI INTÉZKEDÉSEK

A terrorizmus finanszírozásának megakadályozása érdekében az érintett szolgáltatók és intézmények úgynevezett AML (anti money laundering - pénzmosás elleni)[30] és KYC (know your customer – ügyfél azonosítási) intézkedéseket alkalmaznak, amelyek rájuk nézve kötelezettségeket fogalmaznak meg az EU-s és nemzeti jogszabályokon keresztül.

Az AML tevékenység a tranzakciók monitorozására, érintettjeire és a gyanús tevékenységek jelentésére fókuszál, míg a KYC az ügyfelek azonosítását és kockázati besorolását segíti. Ezeknek a komplex rendszereknek a működtetése fejlett technológiai és magasan képzett humán erőforrásokat igényel. Amennyiben az érintett szolgáltatók a jogszabályokban foglaltakat nem, vagy csak részben teljesítik, az szankciókat vonhat maga után. Végső esetben pedig engedélyeinek bevonását is eredményezheti összhangban a nemzetközi Pénzügyi Akciócsoport (Financial Action Task Force; továbbiakban: FATF) ajánlásaival[31], illetve hazánkban a Magyar Nemzeti Bank rendeleteivel.

5.2.1. AML intézkedések

Célja a bűncselekményből származó pénzeszközök tisztára mosásának és a terrorista tevékenységek finanszírozásának megakadályozása, aminek szűkebb mikrogazdasági megközelítésben az Európai Parlament és Tanács 2015/849 és 2018/843 irányelvek képezik az alapját, amelyek előírják a kockázatalapú megközelítést, az ügyfél-átvilágítást és a gyanús tranzakciók jelentését.

Magyarországon a Pmt. szabályozza a meghatározott szolgáltatók részére az AML-kötelezettségeket, részletezve a tranzakciófigyelési rendszerek és a szankciós szűrések követelményeit. Az intézményeknek olyan belső szabályzatokat kell kidolgozniuk, amelyek megfelelnek a Pmt., továbbá a 30/2024. (VI. 24.) MNB rendelet előírásainak. Ez utóbbi a szűrőrendszerek minimumkövetelményeit határozza meg.

Az előírások kulcsfontosságú eleme a tranzakciók valós idejű monitorozása és a terrorizmus finanszírozására utaló gyanús tevékenységek azonosítása, amelyeket a szolgáltatóknak hazánkban a NAV PEII felé kell továbbítaniuk. Az FATF ajánlásai kiemelik a nemzetközi együttműködés szükségességét a vizsgálatok, ellenőrzések lefolytatása során és a magas kockázatú országokkal kapcsolatos tranzakciók fokozott ellenőrzését.

[30] A jogszabályok mind nemzeti szinten, mind globális szinten jellemzően nem tesznek különbséget a pénzmosás megelőzését szolgáló intézkedések és a terrorizmus finanszírozás visszaszorítását célzó intézkedések között, mivel ezen tevékenységek egymást kiegészíthetik és elhatárolásuk sok esetben nem lehetséges.
[31] FINANCIAL ACTION TASK FORCE.

Az AML rendszerek működtetése jelentős technológiai beruházásokat és szakértői képzést igényel, ebben azonban nagyfokú előrelépés mutatkozhat a közeljövőben a mesterségesintelligencia-alapú szűrőrendszerek bevezetésével, amelyek alkalmasak lehetnek majd a komplex tranzakciós mintázatok elemzésére is.

5.2.2. KYC intézkedések

Ezek az intézkedések az ügyfelek azonosítására, kockázati profiljuk értékelésére és tranzakcióik céljának megértésére szolgálnak a terrorizmus finanszírozásának megakadályozása érdekében. Alapvető eleme az ügyfél-átvilágítás, amelyet az AML előírásokhoz hasonlóan a Pmt. szabályoz, és amely magában foglalja az ügyfél személyazonosságának ellenőrzését, a tényleges tulajdonosok azonosítását, valamint a politikai közszereplők azonosítását is. Az EU 2018/843 irányelve szigorúbb szabályokat vezetett be a magas kockázatú harmadik országokból származó ügyfelekre, előírva a fokozott átvilágítást.

Az intézményeknek itt is kockázatalapú megközelítést kell alkalmazniuk, amely figyelembe veszi az ügyfél földrajzi helyzetét, tevékenységi körét és tranzakciós szokásait is. A KYC folyamat során az intézményeknek dokumentálniuk kell az ügyfél által szolgáltatott információkat, illetve rendszeresen frissíteniük kell azokat. Hazánkban a 30/2024. (VI. 24.) MNB rendelet előírja az automatizált szűrőrendszerek használatát a politikai közszereplők és a nemzetközi szankciós listán szereplő entitások ellenőrzésére.

A KYC rendszerek működtetése jelentős adminisztratív és technológiai terhet jelent a szolgáltatók számára – az AML-hez hasonlóan – azonban elengedhetetlen a jogszabályi megfelelés és a terrorizmus finanszírozásának megelőzése szempontjából.

A stróman[32] olyan természetes személy, aki jogi személyiséggel rendelkező fedővállalkozás mögött áll, és annak nevében jár el. Olyan személyek tartoznak ebbe a körbe, akiket bűncselekmény elkövetésére, – jelen esetben terrorizmus finanszírozása céljából – használnak fel, akár tudtukon kívül is, annak érdekében, hogy a tényleges elkövető kiléte a hatóságok előtt titokban maradjon. A stróman ebből kifolyólag látszólag legális tranzakciókat hajt végre, miközben a háttérben az ügyletek tényleges haszonélvezői, kedvezményezettjei rejtve maradnak. Ezáltal megkerülik a szolgáltatók által alkalmazott, kötelező AML- és KYC-intézkedésket.

2019-ben az Amerikai Egyesült Államok Törökországgal közösen szankciókat vezetett be az ISIS finanszírozási struktúrájának részét képező Rawi-hálózat ellen, amely fő működési

[32] A kifejezés a német strohmann, azaz szalmabáb kifejezésből származik.

területe ugyan Irak volt. A szervezet irányítói strómanokat, fedővállalkozásokat használtak arra, hogy több millió dollárt juttassanak a konfliktusövezetbe. A hálózat Európán, Törökországon és Szírián keresztül bonyolította tranzakcióit, amelynek részét képezte a készpénzfutárok és a hawala rendszer alkalmazása is a pénz eredetének, valamint felhasználási helyének leplezése érdekében. A strómanok által alapított fedővállalkozások és jótékonysági szervezetek segítették az ISIS-t abban, hogy erőforrásait és támadásait finanszírozzák.[33]

6. A TERRORIZMUS FINANSZÍROZÁS KLASSZIKUS MÓDSZEREI

A terrorizmus finanszírozásának vizsgálata és a hatékony fellépés szempontjából ki kell emelni azon folyamatokat, amelyek során a legális vagy illegális bevételekből származó pénzeszközök továbbításra, tranzaktálásra kerülnek az érintett terrorszervezetek vagy személyek részére. Az alábbiakban a készpénzcsempészet, a bankszámlák használata és a Hawala rendszer kerül részletes elemzésre, mint a terrorizmus finanszírozásának hagyományos, ám továbbra is releváns eszközei.

6.1. KÉSZPÉNZ CSEMPÉSZET

A terrorizmus finanszírozásának egyik legrégebbi és legelterjedtebb formája, amely során a fizikailag rendelkezésre álló pénz határokon átnyúlóan, illegálisan kerül elszállításra a felhasználási helyre. Az elkövetésnek ez a módszere igényli a legalapvetőbb infrastrukturális hozzáférést és nehezen nyomon követhető, ezért a terrorizmussal kapcsolatba hozható szervezetek és személyek egyik preferált elkövetési módszere.

A csempészet során a pénzeszközöket gyakran rejtett módon poggyászban, ruházatban vagy járművekben szállítják, hogy elkerüljék a vám- és pénzügyi hatóságok ellenőrzését.[34]

A módszer hatékonyságát példázza az is, hogy az amerikai hatóságok a 2001. szeptember 11-i támadások finanszírozását csak utólag, a cselekmény bekövetkezése után tudták rekonstruálni. Megállapították, hogy egyéb módszerek mellett az elkövetéshez szükséges vagyon jelentős része készpénzben került „beutaztatásra” az Egyesült Államokba a Közel-Keletről Európán keresztül.[35] A készpénzmozgás detektálását ezen konkrét esetben

[33] U.S. DEPARTMENT OF THE TREASURY (2024)
[34] Ismertek olyan esetek, amelyek során az elkövetők különböző strómanokon keresztül fuvarozó vállalkozásokat alapítottak, így legális tevékenység álcája alatt szállíthatták nagy mennyiségű, nehezen ellenőrizhető árú közé rejtve a bűnös tevékenységgel összefüggésbe hozható pénzeszközöket.
[35] NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES (2004)

is – és napjainkban is – nehezíti, amennyiben a készpénz kisebb összegekben kerül szállításra. Ennek hatályos jogszabályban rögzített összege jelenleg 10.000 euró.

Az ISIS a 2010-es években a szíriai és iraki területeken folytatott műveleteit finanszírozta készpénzfutárokon keresztül. Ennek elsődleges oka az instabil gazdasági környezet és a formális bankrendszer hiánya volt. A FATF 2015. évi jelentése szerint az ISIS nagy mennyiségű készpénzt – gyakran dollárt vagy eurót – szállított át a határon, hogy finanszírozza a fegyverbeszerzést és a toborzási kampányokat.

A jelentés szerint az ISIS évente akár több tízmillió dollárt is mozgathatott ilyen módon, kihasználva a térség instabilitását és a határőrizetben, vámellenőrzésben illetékes hatóságok korlátozott kapacitását.[36]

6.2. BANKSZÁMLÁK HASZNÁLATA

A bankszámlák terrorizmus finanszírozási célú felhasználása alatt első sorban azt a tevékenységet értjük, amely során a legális pénzügyi rendszereket az érintettek illegális tevékenységre használják fel, így a terrorszervezetek vagy támogatóik a banki infrastruktúrán keresztül pénzeszközöket gyűjtenek, tárolnak, átutalnak vagy azok eredetének leplezésére használják fel azt. A módszer lehetővé teszi a nagy összegű tranzakciók gyors és globális lebonyolítását úgy, hogy a pénzmozgások a legitim gazdasági tevékenységek és átutalások álcája mögé, közé rejthetők csökkentve ezáltal a hatóságok előtti dekonspiráció esélyét.

A 2005. július 7-i londoni metró- és buszrobbantások 52 ember halálát és több száz sérülését okozták. A támadást végrehajtó négy brit állampolgár a szigetország bankrendszerén keresztül gyűjtött és utalt pénzeszközöket a művelet előkészítésére, amelynek költségei hozzávetőleg 8.000 fontot tettek ki. Tevékenységük során szándékosan csak alacsony összegű tranzakciókat végeztek, ezen összegek a brit pénzügyi felügyelet akkori szabályozási határértékét nem érték el. A londoni esetet követően az Egyesült Királyságban szigorították a pénzmosás elleni szabályozást, így a gyanús tranzakciók összegére, jelentésére vonatkozó követelményeket.[37]

A kis, lokális hálózattal szemben a Hezbollah korábban egy dél-amerikai hálózatot működtetett a Paraguay, Argentína és Brazília hármas határvidékén, finanszírozási célból. A szervezet támogatói helyi bankokat használtak fel arra, hogy a drogkereskedelemből és hamisított áruk értékesítéséből származó pénzeket átutalják libanoni számlákra.[38]

[36] FINANCIAL ACTION TASK FORCE (2015b): l.
[37] HOUSE OF COMMONS (2006)
[38] LEVITT (2013)

Az Egyesült Államok Pénzügyminisztériuma 2011-ben szankciókat vezetett be a Lebanese Canadian Bank ellen, miután megállapította, hogy a bank több mint 300 millió dollár Hezbollah részére történő átutalásában segített, amely során a pénz Dél-Amerikából az Amerikai Egyesült Államokba, majd onnan Libanonba került tranzaktálásra.

A hazánkban 2020. március 2. napjától elérhető azonnali fizetési rendszer rendészeti, nemzetbiztonsági szempontból kockázatokat rejthet magában. A schengeni zónán belüli ellenőrzés – és így gyakorlatilag nyom nélküli határátlépés – lehetőségét kihasználva európai állampolgárok vagy Európába már beléptetett harmadik országbeli állampolgárok tudnak számlát nyitni hazai pénzintézeteknél, amelyet végső esetben terrorizmus finanszírozására vagy más bűncselekmények elkövetéséhez is használhatnak.

6.3. HAWALA RENDSZER

A hawala[39] egy hagyományokon és bizalmon alapuló pénzküldési rendszer, amelyet főként a Közel-Keleten, Dél-Ázsiában és Afrikában használnak. A rendszer globálisan is működő képes, fő szervezőjének és egyben központjának pedig Szaúd-Arábia tekinthető. A tranzakciók hivatalos papíralapú nyilvántartás, illetve a legális banki csatornák nélkül zajlanak, így nehezen nyomon követhetők.

A hawala-ügynökök hálózata valós készpénzmozgás nélkül teszi lehetővé a fizikailag egymástól távol lévő vagy akár konfliktus zónában elhelyezkedő földrajzi helyek közötti tranzaktálást, minimalizálva a fizikai pénzmozgást, amely csak adott időközönként, régiónként kerül balanszírozásra.

A készpénz feladója a tartózkodási helyén fellelhető hawala-ügynöknek jelzi szándékát, aki intézkedik a célhelyen a hálózat egy kifizetőpontjával történő kapcsolatfelvételre, melyet követően a tranzakcióval érintett összeget és a jutalékát átveszi. A kifizető helyen meghatározott kód közlése után intézkednek a címzett részére történő kifizetésről.

A hawala rendszer központjának ugyan a fentiek alapján Szaúd-Arábiát tekinthetjük, valójában az decentralizált, egymással laza kapcsolatban álló hálózatokból épül fel.

A terrorizmus finanszírozásának komplexitását jól példázza, hogy a 2015-ös párizsi terrortámadások vizsgálata során megállapítást nyert, hogy annak költségeit az ISIS belső

[39] A dél-ázsiai eredetű, ősi, alternatív pénzátutalási rendszer, a „hawala” az arab „hawal” szóból eredeztethető, ami váltást és átutalást is jelent. A „hawala” szó váltópénzt, vagy ígérvényt egyaránt jelent, és „hawala safar” összetételben utazási csekket is jelöl. A szó farszi és urdu nyelvű változata az eredeti jelentés megtartása mellett kiegészült a bizalom és a hivatkozás jelentésekkel is, ami nyilván a rendszer működési módjára utal. Indiában és Pakisztánban a „hawala” szinonímájaként a szanszkrit „hundi” szó is használatos, ami gyűjtés-t jelent. A „hawala” rendszer működtetője a „hawaladar”, vagy (Indiában és Pakisztánban) a „hundiwala”. JOST – SANDHU (2013)

forrásokból (például: zsarolásból és olajkereskedelem) finanszírozta. A francia és belga hatóságok később azonban megállapították, hogy kisebb összegek mozgatása, amelyek fegyvervásárlásra vagy logisztikai költségek fedezésére kerültek felhasználásra informális csatornákon, köztük hawala hálózatokon keresztül kerültek tranzaktálásra Európán belül.[40]

6.4. PÉNZKÜLDÉSI SZOLGÁLTATÓK

A hawala rendszerhez hasonlóan működnek az olyan pénzátutalási szolgáltatók, mint a Western Union vagy a MoneyGram. Ezek a rendszerek földrajzilag távoli entitások között is lehetővé teszik a tranzakciók lebonyolítását, azonban állami, rendészeti és nemzetbiztonsági kontroll alatt működnek.

Engedéllyel rendelkező vállalkozásokként meg kell felelniük a törvényi előírásoknak, így a klasszikus ügyfélazonosítási, adatszolgáltatási kötelezettségüknek is, azonban ennek ellenére is a bűn- és terrorszervezetek előszeretettel használják ezeket céljaik megvalósítására. Az Európai Unióban tapasztalt 2015-ös migrációs válság során az embercsempész csoportok „munkadíjukat" gyakran ezt a lehetőséget kihasználva kapták meg, illetve fizették ki a csoport tagjainak a szolgáltatási díjakat. Megfigyelhető trend volt az is, hogy az európai országokba illegálisan bejutott személyek hazájukban maradt családtagjaiknak vagy általuk támogatott – akár illegális – szervezeteknek strómanokon keresztül ilyen csatornákon keresztül küldtek pénzeszközöket.

A vállalkozások interneten elérhető adatai szerint jelenleg is irodákat tartanak fent konfliktuszónának tekinthető helyszíneken (pl.: Jemen, Szíria, Palesztína, Irak), illetve azok közvetlen közelében (pl.: Libanon, Jordánia), így legális hálózaton keresztül kerülhet sor adott esetben terrorszervezetek vagy azok tagjainak finanszírozására, mind a Közel-Kelet, mind az Európai Unió tagországainak vonatkozásában olyan személyek által, akik ez idáig még nem kerültek az érintett rendvédelmi, nemzetbiztonsági szervezetek látókörébe.

A 2015. január 7-i Charlie Hebdo ellen elkövetett terrortámadást elkövető Kouachi testvérek kisebb összegeket mozgattak Western Unionon keresztül oly módon, hogy azt a szolgáltató, illetve a hatóságok előtt valós pénzügyi tevékenységnek (pl.: cipő és más áruk értékesítése) álcázták, csökkentve a dekonspirációs veszélyt a cselekményük véghezvitelét megelőzően.[41]

[40] FINANCIAL ACTION TASK FORCE (2015b)
[41] CRONE (2016); A French National Police és a Direction Générale de la Sécurité Intérieure (DGSI) jelentései.

7. A TERRORIZMUS FINANSZÍROZÁS MODERN KORI ELKÖVETÉSI MÓDSZEREI

A napjainkban oly sokszor említett fintech vállalkozások olyan cégek, amelyek adott országban érvényes pénzügyi engedélyeket szereznek, amik sok esetben több országra vagy egész Európára érvényeseket. A gazdasági társaságok ezen engedélyek birtokában végzik pénzügyi szolgáltató tevékenységüket. Jellemzően direkt módon bankbetétet nem gyűjthetnek, az ügyfeleik pénzét más bankoknál helyezik el, így kevert ügyfélvagyon-kezelés valósul meg. Az egyes ügyfelek vagyonát ebből kifolyólag virtuális számlákon tartják nyilván.

Költséghatékonyságuk abban rejlik, hogy nem tartanak fenn bankfiókokat, a bankokhoz képest lényegesen kevesebb alkalmazottat foglalkoztatnak, míg rentabilitásuk amiatt nagyobb, mert több országból rendelkeznek ügyfelekkel. Fiatalokat és a középkorosztályt célozzák meg azzal, hogy telefonos applikáción keresztül lehet náluk számlát nyitni, bankkártyát igényelni, a banki ügyfél azonosításnál lényegesen egyszerűbben, gyorsabban és földrajzi helyhez való kötöttségek nélkül. A bűnszervezetek ezeket az ügyfélélményt nyújtó lehetőségeket használják ki. A továbbiakban a legjellemzőbb ilyen típusú szolgáltatási köröket mutatom be, a terrorizmus finanszírozás szempontjából aggályosnak tekinthető és biztonsági kockázatként értékelhető szempontok figyelembevételével.

Ki kell emelni, hogy ezen cégek a hagyományos szolgáltatókkal megegyező szolgáltatásokat nyújtanak, de digitalizált formában. Ezáltal egy újfajta eszköztárat biztosítva a potenciális elkövetőknek, kiemelten az alacsony költségráfordítást igénylő magányos vagy fiatalabb korosztályba tartozó elkövetők számára.

Megjelenésük nemzetbiztonsági szempontból amiatt is kockázatot hordoz magában, mivel ezek használata a hagyományos szolgáltatók tevékenysége mellett, illetve azokkal kombinálva is megvalósulhat, amely a felderítés hatékonyságát nagymértékben nehezíti.

Konkrét terrorizmus finanszírozással kapcsolatos eset ez idáig csak csekély számban került publikálásra az illetékes szervek által. Azonban kijelenthető, hogy a KYC és AML tevékenység által napi szinten került információ átadás a felderítésben és elhárításban illetékes szervek irányába a kialakított intézményrendszeren keresztül.

Az ilyen típusú vállalkozások tekintetében az alábbi általános kockázat definiálhatóak:

- Pénzeszközök gyors, valós idejű tranzaktálása távoleső földrajzi helyek, ügyfelek között.
- A KYC folyamatok gyakran nem olyan szigorúak, mint a hagyományos szolgáltatóknál.

– A tranzakciók nyomon követése nemzetbiztonsági, rendvédelmi szempontból bonyolultabb lehet, különösen, ha kriptovalutákat vagy anonim fizetési szolgáltatókat is igénybe vesznek az elkövetők.

7.1. NEOBANKOK

Az olyan vállalatok, mint a Revolut, N26 és Monzo innovatív, felhasználóbarát felületekkel és alacsony díjakkal célozzák az ügyfeleket és az „open banking”[42] technológiára épülve integrálják a pénzügyi szolgáltatásokat, javítva az ügyfélélményt a „legális” felhasználóik számára.

A terrorizmus finanszírozással kapcsolatos kockázatok esetükben a gyors számlanyitási folyamatok és a globális elérhetőség miatt tekinthetők magasnak, amit az alacsony hatásfokú digitális azonosítás, hamis vagy hamisított dokumentumok felhasználása, strómanok bevonása tovább növelhet. A Financial Crimes Enforcement Network ajánlásainak megfelelően a nemzetközi szankciós listák ellenőrzése és a tranzakciók folyamatos, akár valós idejű monitorozása elengedhetetlen, mivel a neobankok szolgáltatása anonimitást biztosíthat a terrorszervezetek és azok tagjai számára.[43]

A Revolutnál az elmúlt 10 évben több terrorizmusfinanszírozással és pénzmosással kapcsolatos szabályozói elmarasztalás is történt. Ezek jellemzően abból fakadtak, hogy a vállalat nem megfelelő algoritmusokat alkalmazott a tranzakciók monitorozására és szűrésére.

Legutóbb 2025 elején a litván központi bank 3,5 millió eurós bírságot szabott ki a vállalatra emiatt, annak ellenére, hogy konkrét pénzmosással vagy terrorizmus finanszírozással kapcsolatos cselekményt a vizsgálatok sem tártak fel, ennek ellenére rámutattak a működtetett rendszerek gyengeségeire.[44]

7.2. FIZETÉSI SZOLGÁLTATÓK

A fizetési szolgáltatók, mint a PayPal, a Skrill vagy a Square a hagyományos fizetési szolgáltatók által nyújtott lehetőségeket digitálisan biztosítják, lehetőséget biztosítva ezáltal a pénzügyi tranzakciók gyors, biztonságos és relatíve olcsó lebonyolítására mobiltelefonos vagy számítógépen futtatott alkalmazásokon.

[42] Az „open banking” azt a folyamatot jelenti, amely során a pénzügyi intézmények az ügyfeleik beleegyezésével biztonságos, szabványosított hozzáférést biztosítanak azok pénzügyi adatokhoz harmadik szereplő, például fintech vállalkozások számára.
[43] CUVÉE (2019)
[44] REUTERS (2025)

A terrorizmusfinanszírozással kapcsolatos kockázatok abban az esetben növekedhetnek ezek használata során, ha gyenge a vállalatok KYC eljárása, mivel így a globális pénzpiacon anonim szereplők által tranzaktált pénzeszközök jelenhetnek meg.

A vállalatok a magas kockázatú országokba (konfliktus zónákba) történő, nagyösszegű vagy ismétlődő kisösszegű tranzakciókat gyanús tevékenységként értékelhetik és az ilyenek teljesítését a nemzeti vagy nemzetközi jogszabályban foglaltak szerint megtagadhatják, valamint az illetékes hatóságok értesítéséről rendelkezhetnek.[45]

7.3. KÖZÖSSÉGI FINANSZÍROZÁSI PLATFORMOK

A közösségi finanszírozási platformok, mint a Kickstarter, Indiegogo vagy a GoFundMe online formában biztosítják projektek vagy konkrét vállalkozások finanszírozását kis összegű egyéni hozzájárulásokkal. A terrorizmus finanszírozási kockázatok a nagy tranzakciószámú és kis összegű átutalások miatt nőnek meg az ilyen vállalkozások tekintetében potenciálisan, megnehezítve a gyanús tevékenységek kiszűrését. A nonprofit szervezetekhez hasonló projektek esetében fennállhat a kockázata, hogy a terrorszervezetek vagy magányos elkövetők szimpátiát ébresztő kampányokkal gyűjtenek pénzt.[46]

A FATF 2023-as jelentése[47] szerint az ISIS, az al-Kaida és a HAMASZ is gyűjtött pénzeszközöket online tevékenységeik finanszírozására, olyan kampányokon keresztül, amelyek a felajánlók érzelmeire hatottak. A gyűjtés céljaként például vízhiányos területeken történő kútépítést vagy árva gyermekek megsegítését tüntették fel. Az így összegyűjtött pénzeket a harcosaik és az általuk elkövetett támadások finanszírozására használták fel.

A támogatók között több alkalommal olyan személyek is szerepeltek, akik az iszlám radikális tanaival nem azonosultak vagy elítélték azt, ennek ellenére tudatukon kívül kerültek egy-egy terrorszervezet aktív finanszírozói közé.

A vallási indíttatású támadások mellett a magányos szélsőjobboldali vagy nőgyűlölő, incel[48] körhöz tartozó magányos elkövetők is alkalmazhatják ezt a pénzgyűjtési módot, amely során a zárt csoportjaikban szerezhetnek anonim támogatókat céljaik megvalósításához, amely az elkövetések számában és érintettjeiben is radikális emelkedéshez vezethet.

[45] FINANCIAL ACTION TASK FORCE (2015a)
[46] FINANCIAL ACTION TASK FORCE (2023b)
[47] FINANCIAL ACTION TASK FORCE (2023a)
[48] EUROPOL (2024)

7.4. KRIPTOVALUTA PLATFORMOK

A különböző kriptovaluta kereskedési platformok, mint például Binance vagy Coinbase az online szerveződő csoportok által értékközvetítőként elfogadott kriptovaluták tárolását, kereskedelmét és átutalását teszik lehetővé. Ezek az értékközvetítők blokklánc technológiára épülnek, ami decentralizált és transzparens tranzakciókat biztosít gyors, határokon átnyúló, anonim tranzakciókat biztosítva. A kriptovaluták egy részének blokkllánca a Bitcoinéval ellentétben nem nyilvános, azok kereskedése visszakövethetetlenül történik.

A nyilvános blokklánccal rendelkező kriptovaluták kereskedelme online nyomon követhető és a küldő, valamint feladó tárcák címe is nyilvános, azonban ennek ellenére is a rendészeti és nemzetbiztonsági fellépés a legtöbb esetben csak utólag lehetséges a bűncselekmény elkövetése után, a teljes tranzakciós lánc felderítésekor.

A terrorizmus finanszírozási kockázatok a fentiekben ismertetett módszerekhez képest is magasnak tekinthetők a kriptovaluták anonimitása és a tranzakciók visszafordíthatóságának hiánya miatt.

2020-ban az Amerikai Igazságügyi Minisztérium által végzett vizsgálat feltárta, hogy a HAMASZ-hoz köthető al-Kasszám Brigád, az ISIS és az al-Kaida is kriptovalutákat használt tevékenysége finanszírozására. Az ellenőrzés eredményeképpen a finanszírozási kampányt sikeresen felszámolták és annak eredményeképpen több, mint 2 millió dollárnyi kripto pénztárcát foglaltak le a hatóságok.

A HAMASZ[49] az interneten olyan weboldalt működtetett, amelyen tevékenységüket és céljaikat ismertették és a dzsihád eredményes lefolytatása érdekében gyűjtöttek Bitcoin adományokat. Az al-Kaida[50] Szíriában Telegram csatornákon keresztül gyűjtött különböző kriptovalutákat, jótékonysági kampánynak álcázva, amely során a befolyt összegeket fegyverek vásárlására fordították. A tranzakciókat virtuális valutaváltók bevonásával és egyéb pénzmosási technikával tranzaktálták azt a látszatot keltve, hogy azok legális vagyonelemek. A nyomozás során a többek között a Bitcoinhoz köthető blokklánc nyomon követhetősége segítette a hatóságokat a tranzakciók visszakövethetőségében, demonstrálva a kriptovaluták kettős természetét, amelyek egyrészt lehetőséget teremtenek a terrorizmus finanszírozásához, de egyben nyomozati, felderítési potenciált is biztosítanak a hatóságoknak.

Megfigyelhető trend az is, hogy a különféle szélsőséges propagandaanyagokban a terrorszervezetek vagy ahhoz köthető személyek gyakran a feltüntetik a saját kriptovaluta pénztárcáinak nyilvános címét, vagy az ahhoz tartozó közvetlen átutalást biztosító QR kódot.

[49] U.S. DEPARTMENT OF JUSTICE (2020)
[50] HOMELAND DEFENSE & SECURITY INFORMATION ANALYSIS CENTER (2025)

Megteremtve ezzel a lehetőséget az arra fogékony személyeknek az azonnali támogatás elküldésére. Ez a metódus szintén lehetőséget biztosíthat magányos elkövetőknek kis számú, nehezen detektálható fórumokon cselekményük végrehajtásához szükséges „adományok”, vagyonelemek gyűjtésére.

8. ÖSSZEFOGLALÓ

Tanulmányomban átfogóan vizsgáltam a terrorszervezetek működését, ahol közgazdasági szempontból tekintettem át a rajtuk keresztül áramló vagyonelemeket azok keletkezésétől egészen a felhasználásukig, illetve bemutattam azt a jogszabályi környezetet is, amely a velük szembeni hatékony fellépést szabályozza.

A terrorszervezetek fejlődésével párhuzamosan bemutattam a globalizáció hatására változó pénzpiacokat és rámutattam azok összetettségére. A klasszikus mellett a modern kori terrorizmus finanszírozási módszereket is demonstráltam, amelyhez a terrorista szervezeteket, önálló gazdasági entitásokként definiáltam, amelyek mind legális, mind pedig illegális forrásból származó vagyonelemekkel gazdálkodnak.

Hazánkban – mint tranzitországban – a terrorizmus finanszírozása elleni küzdelem a nemzetközi és uniós jogszabályokkal összhangban zajlik, különös hangsúlyt fektetve az AML és KYC intézkedésekre. A trendek ismerete alapján a terrorszervezetek gazdálkodása és pénzügyi „hatékonysága” a digitális technológiák térhódításának hatására feltehetően exponenciálisan javulni fog.

Kijelenthető, hogy a terrorizmus finanszírozása napjainkban a globális biztonsági kockázatok egyik kulcsfontosságú eleme, amelyre az aktuális geopolitikai, társadalmi és technológiai változások indikátorként hatnak.

A kutatás rámutat arra, hogy a hatékony terrorelhárítás, illetve felderítés érdekében elengedhetetlen a globális pénzügyi rendszerek és a technológiai fejlődés aktuális állapotának megismerése, valamint az érintett szervek közötti együttműködés megerősítése.

A fejlődő technológia új lehetőséget nyújt a terroristák számára, ugyanakkor korszerű eszközöket biztosít a rendvédelmi és nemzetbiztonsági szervek számára is. Napjainkban a legnagyobb figyelem a mesterséges intelligenciára irányul, amely hasonlóan a bemutatott pénzügyi szolgáltatásokhoz legális és illegális felhasználási lehetőséget is magában hordoz.

A terrorszervezetek a mesterséges intelligencia használatával deepfake[51] tartalmakat gyárthatnak, amelyek segítségével eredményesebb adománygyűjtő kampányokat folytathatnak, hamis identitások felhasználásával fiktív személyekhez köthető, de ténylegesen általuk kezelt szolgáltatásokat vehetnek igénybe.

Terrorelhárítási szempontból a mesterséges intelligencia ugyanakkor elősegítheti a hatóságok és a vagyonelemeket kezelő szolgáltatók munkáját a hatékony felderítésben, mivel annak felhasználásával a gyanús pénzügyi tranzakciók gyorsabban és pontosabban azonosíthatóak.

Tanulmányomban átfogó képet kívántam nyújtani a terrorizmus finanszírozásának múltjáról, jelenéről és lehetséges jövőjéről, hangsúlyozva a gazdasági, a rendvédelmi és a jogalkotási folyamatban résztvevők proaktív intézkedéseinek szükségességét a terrorizmus visszaszorítása érdekében.

FELHASZNÁLT IRODALOM

1824/2015. (XI. 19.) Kormány határozat a terrorizmus elleni küzdelem feladatainak egységes végrehajtási rendjéről a terrorizmus leküzdése érdekében egyes személyekkel és szervezetekkel szemben hozott különleges korlátozó intézkedésekről.

2012. évi C. törvény a Büntető Törvénykönyvről.

2017. évi LIII. törvény a pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról.

30/2024. (VI. 24.) MNB rendelet a Magyar Nemzeti Bank által felügyelt szolgáltatóknak a pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról szóló törvényben foglalt egyes kötelezettségei végrehajtásának részletszabályairól, valamint e szolgáltatóknak az Európai Unió és az ENSZ Biztonsági Tanácsa által elrendelt pénzügyi és vagyoni korlátozó intézkedések végrehajtásáról szóló törvény szerinti szűrőrendszere kidolgozásának és működtetésének minimumkövetelményeiről.

Az Európai Parlament és a Tanács (EU) 2018/843 irányelve (2018. május 30.) a pénzügyi rendszerek pénzmosás vagy terrorizmusfinanszírozás céljára való felhasználásának megelőzéséről szóló (EU) 2015/849 irányelv, valamint a 2009/138/EK és a 2013/36/EU irányelv módosításáról.

CONFLICT ARMAMENT RESEARCH (2017): *Weapons of the Islamic State*. Online: https://www.conflictarm.com/reports/weapons-of-the-islamic-state/

[51] Olyan digitális hamisítási technológia, amellyel a valódihoz a megtévesztésig hasonlító multimédiás tartalmakat lehet előállítani.

CRONE, Manni (2016): Radicalization Revisited: Violence and the Financing of Terrorism. *Studies in Conflict & Terrorism*, 39(7-8), 579-593.

CUVÉE, Koos (2019): Fintechs Fuel Surge in UK Defense Against Money Laundering Requests. Online: https://www.moneylaundering.com/news/fintechs-fuel-surge-in-uk-defense-against-money-laundering-requests/

ENSZ Biztonsági Tanácsának 1373. (2001. szeptember 28.) számú határozata.

Európa Tanács 2580/2001/EK rendelete (2001. December 27.) a terrorizmus leküzdése érdekében egyes személyekkel és szervezetekkel szemben hozott különleges korlátozó intézkedésekről.

Európa Tanács határozata az Európai Bizottságnak az Európa Tanács pénzmosásról, a bűncselekményből származó jövedelmek felkutatásáról, lefoglalásáról és elkobzásáról, valamint a terrorizmus finanszírozásáról szóló egyezményéhez (CETS 198. sz.) csatolt kiegészítő jegyzőkönyvről folytatandó tárgyalásokon az Európai Unió nevében való részvételre történő felhatalmazásáról.

Európa Tanács terrorizmus megelőzéséről szóló Egyezménynek (CETS 196) az Európai Unió nevében történő megkötéséről.

EUROPOL (2020): *Internet Organised Crime Threat Assessment*. Online: https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2020

EUROPOL (2022): *European Union Terrorism Situation and Trend Report*. Online: https://www.europol.europa.eu/publication-events/main-reports/european-union-terrorism-situation-and-trend-report-2022-te-sat

EUROPOL (2024): *Incel online communities, violence, and the construction of collective victimhood*. Online: https://www.europol.europa.eu/publications-events/publications/incel-online-communities-violence-and-construction-of-collective-victimhood

FINANCIAL ACTION TASK FORCE (2015a): *Emerging Terrorist Financing Risks*. Online: https://www.fatf-gafi.org/en/publications/Methodsandtrends/Emerging-terrorist-financing-risks.html

FINANCIAL ACTION TASK FORCE (2015b): *Financing of the Terrorist Organisation Islamic State in Iraq and the Levant*. Online: https://www.fatf-gafi.org/en/publications/Methodsandtrends/Financing-of-terrorist-organisation-isil.html

FINANCIAL ACTION TASK FORCE (2023a): *Crowdfunding for Terrorism Financing*. Online: https://www.fatf-gafi.org/en/publications/Methodsandtrends/crowdfunding-for-terrorism-financing.html

FINANCIAL ACTION TASK FORCE (2023b): *Understanding the Abuse of Crowdfunding for Terrorism Financing*. Online: https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Crowdfunding-Terrorism-Financing.pdf.coredownload.inline.pdf

Financial Action Task Force. Online: www.fatf-gafi.org

Financial Crimes Enforcement Network. Online: https://www.fincen.gov/

HOMELAND DEFENSE & SECURITY INFORMATION ANALYSIS CENTER (2025): *Financing Terrorism Through Cryptocurrencies*. Online: https://hdiac.dtic.mil/articles/financing-terrorism-through-cryptocurrencies/

HOUSE OF COMMONS (2006): *Report of the Official Account of the Bombings in London on 7th July 2005*. London: The Stationery Office.

HUMAN RIGHTS WATCH (2006): *Funding the "Final War": LTTE Intimidation and Extortion in the Tamil Diaspora*. Online: https://www.hrw.org/report/2006/03/14/funding-final-war/ltte-intimidation-and-extortion-tamil-diaspora

JOST, Patrick M. – SANDHU, Harjit Singh (2013): *The Hawala Alternative Remittance System and its Role in Money Laundering*. Online: https://www.assetsearchblog.com/wp-content/uploads/sites/197/2013/06/FinCEN-Hawala.pdf

LANE, Ashley (2023): *Iran's Proxy Network in the Middle East*. Online: https://www.wilsoncenter.org/article/irans-islamist-proxies

LEVITT, Matthew (2013): *Hezbollah: The Global Footprint of Lebanon's Party of God*. Washington: Georgetown University Press.

LEVY, Dan (2013): *Hezbollah's Fundraising Activity in Africa Focus on the Democratic Republic of Congo*. Online: https://www.ict.org.il/UserFiles/ICTWPS%20-%20Dan%20Levy%20-%2012.pdf

LUTZ, James M. – LUTZ, Brenda J. (2006): *Terrorism as Economic Warfare*. Global Economy Journal, 6(2), 1-21.

MAGYAR NEMZETI BANK (d.n.): *Összefoglaló a pénzmosás és terrorizmus finanszírozása kockázatairól szóló nemzeti kockázatértékelés felülvizsgálatáról*. Online: https://www.mnb.hu/letoltes/osszefoglalo-nra21.pdf

NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES (2004): *The 9/11 Commission Report*. Washington: U.S. Government Printing Office.

PEDAHZUR, Ami – PERLIGER, Arie (2006): *The Organizational Dynamics of Terrorist Groups: A Network Approach*. Security Studies.

REUTERS (2025): *Lithuania fines Revolut 3.5 million euros for money-laundering prevention failures*. Online: https://www.reuters.com/technology/lithuania-fines-revolut-35-million-euros-money-laundering-prevention-failures-2025-04-08/

STATISTA (2023): *Average number of SWIFT messages per day from January 2014 to December 2022*. Online: https://www.statista.com/statistics/1398256/swift-transaction-volume/

THURSTON, Alexander (2017): *Boko Haram: The History of an African Jihadist Movement*. New Jersey: Princeton University Press.

U.S. DEPARTMENT OF JUSTICE (2020): *Global Disruption of Three Terror Finance Cyber-Enabled Campaigns*. Online: https://www.justice.gov/archives/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns

U.S. DEPARTMENT OF THE TREASURY (2024): *Terrorism and Illicit Finance*. Online: https://home.treasury.gov/news/press-releases/jy2346

UNITED NATIONS OFFICE ON DRUGS AND CRIME (2021): *Afghanistan Opium Survey*. Online: https://www.unodc.org/documents/crop-monitoring/Afghanistan/Afghanistan_Opium_Survey_2021.pdf

Kiss Nikoletta

Radikalizáció napjainkban

1. BEVEZETÉS

Minél nagyobb egy populáció, és minél eltérőbb az erőforrásokhoz, különböző javakhoz való hozzáférés az egyének között, annál nagyobb a társadalmi feszültségek kialakulásának valószínűsége. Ugyanakkor a radikalizáció nem pusztán ezeknek a strukturális tényezőknek a következménye; egyéni pszichológiai, kulturális és csoportdinamikai hatások egyaránt szerepet játszhatnak benne. A jelenség megértése nemcsak társadalmi késztetésből fakad, hanem a bűnüldözés és a nemzetbiztonság szempontjából is gyakorlati jelentőséggel bír. Az egyik alapvető kérdés az, hogy a folyamat mely pontján lehet beavatkozni annak érdekében, hogy megelőzhető legyen az erőszakos cselekmények bekövetkezése. Ez az igény érthető, hiszen a rendvédelmi szervek kapacitásai korlátozottak, ugyanakkor a radikalizáció megelőzése nem csupán jogérvényesítési kérdés: társadalmi, oktatási és pszichológiai eszközök egyaránt fontos szerepet játszanak a beavatkozási stratégiák kialakításában.

A radikalizáció folyamata nem egyértelműen azonosítható, nem beszélhetünk minden esetre alkalmazható fordulópontok soráról. Az erőszakos cselekményekhez vezető út egyik gyakran említett előzménye a kognitív radikalizáció, amely azonban nem minden esetben vezet tényleges akcióhoz. Az, hogy végül ki válik aktorrá, mindig egyéni tényezők mentén dől el.[1] A jelenség hasonlítható a pszichoterápiához: ahogyan nem létezik egyetlen univerzális pirula, amely minden pszichés problémát megoldana, úgy a radikalizáció folyamata sem írható le egyetlen egységes mintázat mentén. A személyiségbéli sajátosságok, a társadalmi környezet és a csoportdinamikai tényezők egyedi konfigurációja minden esetben eltérő, noha természetesen léteznek ismétlődő mintázatok.

Amikor mélyebben vizsgáljuk a radikalizáció kérdését, elkerülhetetlenül felvetődik az is, hogy a történelem során megjelenő radikális aktorok nélkül vajon hallhatóvá váltak volna-e az általuk képviselt társadalmi csoportok hangjai. A radikalizációt általában negatív jelenségként értékeljük – és kétségtelen, hogy a legtöbb esetben nemkívánatos folyamat –, azonban érdemes megvizsgálni, hogy bizonyos történelmi kontextusokban volt-e reális esély

[1] Ugyanakkor olyan esetek is ismertek, amikor a terrorcselekmények elkövetői nem ezen a folyamaton mentek keresztül, hanem bűnözői környezetből érkeztek, és elsődlegesen az anyagi haszonszerzés motiválta őket. Emellett előfordul az is, hogy az elkövető nem önálló döntés eredményeként válik aktorrá, hanem manipuláció, fenyegetés vagy pszichológiai kényszer hatására sodródik bele az erőszakos cselekményekbe.

demokratikus eszközökkel elérni a kívánt társadalmi változásokat. Az ilyen kérdések ugyanakkor nem relativizálják az erőszakot, hanem arra mutatnak rá, hogy a radikalizáció jelensége komplex és történelmi-társadalmi kontextus függvénye.

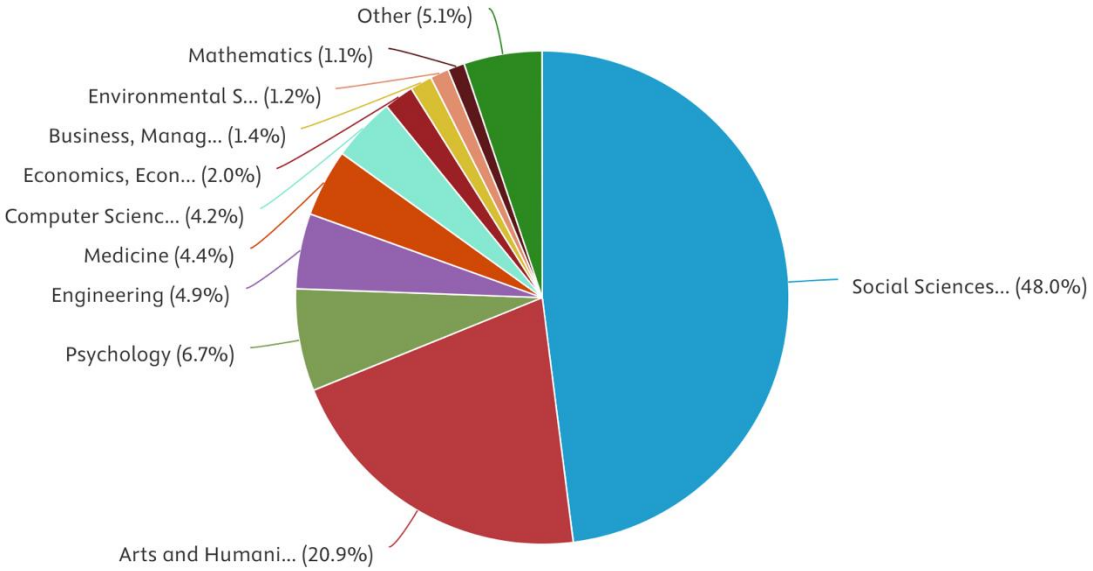
Kutatások igazolják, hogy az egyén radikalizációjához nem feltétlenül objektív sérelem vezet; gyakran egy szubjektíven megélt, vélt sérelem is elegendő lehet ahhoz, hogy elindítsa az egyént ezen az úton. Az érzelmi intenzitás növekedése és a sérelmek szubjektív értelmezése tehát kulcsszerepet játszik a radikalizáció dinamikájában, amely folyamat végső soron erőszakos cselekményekhez is vezethet. Tehát egy dinamikus folyamatról beszélhetünk, ami nem értelmezhető kizárólagosan ideológiai vagy vallási keretben. Ennek fényében különösen fontos elkerülni a leegyszerűsítő modelleket, hiszen a főleg decentralizált közösségi médiás platformokon megjelenő, kevert ideológiás szélsőséges csoportok számának folyamatos növekedése is azt bizonyítja, hogy számos formája létezik.

Jelen tanulmány fókusza a morálisan megkérdőjelezhetetlen esetekre összpontosít, és nem tér ki a fentebb is feszegetett történelmi kérdésekre. Célja, hogy szakítson azzal a tudományos beidegződéssel, amely gyakran egyenlőségjelet tesz a vallási radikalizáció és a terrorizmus között, illetve amely a radikalizációt kizárólag vallási kontextusban értelmezi. A kutatás célja annak bemutatása, hogy a radikalizáció jelensége ennél jóval szerteágazóbb. Bár az iszlamista terrorizmus vizsgálata jelentős mértékben hozzájárult a témával kapcsolatos ismeretek bővítéséhez, éppen ezeknek a kutatásoknak a tanulságait felhasználva szélesíthető a radikalizációs spektrum értelmezési kerete.

2. LÉTEZIK E A RADIKALIZÁCIÓ FOGALMA?

A radikalizáció fogalma azon terminusok közé tartozik, amelyek meghatározása során visszatérő elemként jelenik meg a megállapítás, miszerint nincs egységesen elfogadott definíció. A fogalom értelmezését tovább bonyolítja, hogy meghatározásához először annak kontextusát kell rögzíteni, mivel önmagában még a tudományági besorolásra sem feltétlenül alkalmas. Ez éles kontrasztban áll például a metafora fogalmával, amelynek értelmezése során fejben automatikusan az irodalomtudományi ismereteinkhez fordulunk. A radikalizáció multidiszciplináris jellegét empirikusan is igazolhatjuk: a Scopus adatbázisban a „radicalisation” kifejezésre keresve 1969 és 2025 között 6669 találatot kapunk, amelyek 53 különböző tudományterülethez kapcsolódnak.[2]

[2] A keresés 2025. február 1-jén, keresőszó „radicalisation”, https://www.scopus.com/results/results.uri?st1=radicalization&st2=&s=TITLE-ABS-



1. ábra: *A „radicalisation" kifejezésre adott találatok a Scopus adatbázisban*.

A társadalomtudományok dominanciája a radikalizációval kapcsolatos kutatásokban nem meglepő, hiszen számos tanulmány foglalkozik ennek okaival. A jelenség megértését meghatározzák a 20. század történelmi sajátosságai és napjaink biztonsági kihívásai, amelyek a hadtudományi és nemzetbiztonsági diskurzusban is központi szerepet kapnak. A biztonság percepciója, valamint az emberi társadalmak ősi igénye a rend és kiszámíthatóság fenntartására hozzájárulnak ahhoz, hogy a radikalizáció vizsgálata kiemelt figyelmet élvezzen.

A 2001. szeptember 11-i terrortámadások jelentős hatást gyakoroltak az EU terrorizmusellenes stratégiájára, de a radikalizáció kérdése kezdetben háttérbe szorult. A 2004-es madridi és a 2005-ös londoni támadások azonban rámutattak arra, hogy a terrorizmus belső fenyegetésként is értelmezhető, ami paradigmaváltást eredményezett. Az EU ekkortól kezdve egyre inkább arra összpontosított, hogy miért válnak egyes európai állampolgárok radikálissá, és hogyan előzhető meg ez a folyamat. A radikalizáció fogalma eredetileg a nemzeti rendészeti és hírszerzési szervek diskurzusában jelent meg, majd az EU szakpolitikai keretének kulcsfontosságú elemévé vált.[3]

2004 októberében az Európai Bizottság első ízben hivatkozott a radikalizációra egy hivatalos dokumentumban. Azóta az EU jelentős erőforrásokat fordított a radikalizáció kutatására és megelőzésére, amely idővel az unió terrorizmusellenes stratégiájának alapvető pillérévé vált. A radikalizáció fogalmát egyre szélesebb körben alkalmazzák a szakpolitikák

KEY%28radicalization%29&limit=10&origin=searchbasic&sort=plf-f&src=s&sot=b&sdt=b&sessionSearchId=d4db14e2aa075f846194e536a1c5354d

[3] BAKOWSKI (2022)

különböző területein, és kormányzati szinten is integrált megközelítés alakult ki a jelenség kezelésére.

Noha a radikalizáció fogalma elterjedt mind a politikai, mind az akadémiai diskurzusban, egységes meghatározása továbbra sem létezik. Az Európai Bizottság 2005-ben úgy definiálta, mint azt a jelenséget, amelynek során egyének olyan nézeteket sajátítanak el, amelyek terrorcselekményekhez vezethetnek. A Radikalizációtudatossági Hálózat (RAN) pedig ennél részletesebb definíciót alkalmaz, amely a szélsőséges eszmék és a jogállamiság elutasításának folyamatára helyezi a hangsúlyt. A radikalizáció kutatása során a szakértők eltérő nézőpontokat képviselnek. Míg egyes megközelítések a terrorizmus felé vezető útra összpontosítanak, mások az erőszakos szélsőségesség vagy az ideológiai radikalizmus felé vezető folyamatokat vizsgálják. Az akadémiai definíciók általában részletesebbek, figyelembe véve a radikalizáció társadalmi, politikai és pszichológiai vonatkozásait. Az egységes meghatározás hiánya azonban továbbra is kihívást jelent a szakpolitikai és tudományos közösség számára.[4]

Az ENSZ Kábítószer-ellenőrzési és Bűnmegelőzési Hivatala (UNODC) terrorelhárítással kapcsolatos oktatási anyagaiban a radikalizációt az erőszakos szélsőségességgel összefüggésben tárgyalja, és utóbbi fogalom meghatározására több értelmezési kísérletet is tesz. A fogalmi megközelítések sokfélesége arra utal, hogy az „erőszakos szélsőségesség” egy átfogóbb jelenségként értelmezhető, amely meghaladja a terrorizmus kereteit.

A megelőzési és visszaszorítási (PVE/CVE) stratégiák során felmerülő lehetséges buktatók közé tartozik a jelenség leegyszerűsítő értelmezése, különösen annak vallási, nemzetiségi, civilizációs vagy etnikai csoportokhoz való kapcsolása. Ez a reduktív megközelítés nem csupán hatástalan a szélsőségesség terjedésének megakadályozásában, hanem akár elő is segítheti annak elmélyülését és legitimációját.[5]

A terrorizmuskutatás területén végzett kutatások erősen kétségbe vonják az ideológia és az erőszak közötti állítólagos kapcsolatot. Például azt mutatják, hogy az ideológiai elköteleződés gyakran a kollektív cselekvésben való részvételből ered, nem pedig annak előzménye, és hogy az egyének különféle okok miatt csatlakoznak vagy hagyják el a radikális mozgalmakat, amelyek gyakran Nem kapcsolódnak ideológiai meggyőződésükhöz.[6]

Összességében az EU radikalizáció elleni politikája az elmúlt két évtizedben folyamatosan fejlődött, reflektálva a biztonsági kihívásokra és a terrorizmus változó természetére. Mivel a

[4] BAKOWSKI (2022)
[5] KKIENERM (2018)
[6] FORD –JACKSON (2024)

radikalizáció egy dinamikusan változó jelenség, annak megértése és kezelése folyamatos újragondolást igényel az aktuális biztonsági kihívások tükrében.

3. ONLINE VAGY OFFLINE?

Tradicionális megközelítés szerint a radikalizáció folyamatát megérteni szándékozók offline és online formára bontják azt. Bár talán volt egy nagyon rövid időszak, amikor ez helytálló megközelítés lehetett - amikor még az internethez való hozzáférés kiváltság volt - napjainkra erősen megkérdőjelezhető ennek a felosztásnak a létjogosultsága.

Az elmúlt két évtizedben a radikalizáció jelensége, valamint az internet szerepének vizsgálata egyre nagyobb hangsúlyt kapott a tudományos diskurzusban. Már az „online radikalizáció" koncepciójának elterjedését megelőzően is felmerült az a feltételezés, hogy a digitális tér sajátos szerkezeti jellemzői elősegíthetik a szélsőséges nézetek kialakulását és terjedését. Bár ez a megközelítés széles körű figyelmet kapott, kritikusai arra hívják fel a figyelmet, hogy a kapcsolódó kutatások sok esetben nem empirikus vizsgálatokon alapulnak, hanem más tudományterületekről átvett elméleti modellekre és anekdotikus beszámolókra építenek. A radikalizáció folyamatának értelmezése során a szakirodalomban gyakran központi szerepet kap az online propaganda fogyasztása, azonban ez a tényező önmagában nem feltétlenül elegendő a radikalizáció mechanizmusainak megértéséhez. A jelenség rendkívül komplex, és az empirikus kutatások eddigi eredményei nem mindig támasztják alá egyértelműen azt a feltételezést, miszerint a digitális tér önálló, az offline világtól élesen elkülönülő radikalizációs közeget alkot.[7]

Bár a terrorista cselekmények előkészítése egyre inkább digitális lábnyomot hagy maga után, a kutatási eredmények azt mutatják, hogy az elkövetők jellemzően nem kizárólag az online térben, hanem a fizikai világban is aktívan tevékenykednek. Gill és munkatársai egy brit tanulmány keretében 223 elítélt terrorista radikalizációs folyamatát elemezve arra a következtetésre jutottak, hogy az online és offline radikalizáció éles szétválasztása nem tartható fenn, mivel az elkövetők rendszerint mindkét közegben párhuzamosan mozognak.[8]

Whittaker egy hasonló vizsgálat során 231 olyan személy esetét elemezte, akik az Egyesült Államokban az Iszlám Állam nevében hajtottak végre cselekményeket. Kutatásának eredményei alapján a digitális és fizikai dimenziók szorosan összefonódnak, így az online és offline tér közötti merev elhatárolás nem tükrözi a valóságot.[9]

[7] WHITTAKER (2023)
[8] GILL et al. (2017): 114.
[9] WHITTAKER (2021): 195.

Herath és Whittaker a meglévő adatok bővítése érdekében klaszterelemzést alkalmaztak, amelynek eredményeként négy különböző radikalizációs útvonalat azonosítottak. Elemzésük rámutatott arra, hogy ezek az útvonalak nem egymástól élesen elkülönülő kategóriák, hanem egy folytonos spektrum mentén helyezkednek el, amely az online és offline tevékenységek összefonódását tükrözi. Ennek fényében az „online" és „offline" radikalizáció merev megkülönböztetése túlságosan leegyszerűsítő, és nem ad pontos képet a radikalizáció dinamikájáról.[10]

A terrorista tevékenység online és offline dimenzióinak elkülönítése hosszú ideje a biztonságpolitikai és társadalomtudományi kutatások egyik központi kérdése. Felmerül azonban a dilemma, hogy ez a megkülönböztetés mennyire tükrözi a valóságot, illetve mennyiben járul hozzá a jelenség pontosabb megértéséhez. Az elmúlt évek során egyre több filozófiai és társadalomelméleti megközelítés vonta kétségbe ezt a dichotómiát, arra hivatkozva, hogy a digitális és fizikai világ közötti határvonal fokozatosan elmosódott, és a két tér már nem tekinthető egymástól független jelenségként. Ezt az újfajta társadalmi és technológiai környezetet 'Onlife' néven határozták meg, amely arra utal, hogy az internet – különösen a közösségi média és a mobiltechnológia térnyerésével – immár nem csupán egy különálló szféra, hanem az offline létezést kiegészítő és alakító tényezővé vált. Az online térben zajló folyamatok nem függetlenek a meglévő társadalmi struktúráktól, hanem azokkal kölcsönhatásban formálódnak, egy kiterjesztett, folyamatosan változó valóság részeként.

A digitális kapcsolódás mindennapossá vált, az emberek már nem különálló cselekvésként „lépnek be" az online világba, hanem folyamatos kapcsolatban állnak vele, amely akár passzív módon is – például adatgyűjtés révén – hatással van tapasztalataikra és döntéseikre. Ennek következtében a valóság és a virtuális tér közötti éles határvonal eltűnőben van, az ember és technológia, valamint a természet és a mesterséges környezet közötti megkülönböztetés egyre inkább relativizálódik. Az információszerzés logikája is átalakult: a korábbi hiányalapú modell helyett az információs túltelítettség vált dominánssá, amelyben az egyértelmű, bináris kategóriák helyét hálózatok, folyamatos interakciók és dinamikusan változó összefüggések vették át.

Amennyiben az online és offline dimenziók közötti határvonal elmosódik, úgy az online radikalizáció fogalmának érvényessége is megkérdőjelezhetővé válik. Valentini, Lorusso és Stephan kutatásai arra világítanak rá, hogy a radikalizáció napjainkban 'onlife' terekben zajlik, vagyis olyan közegben, ahol a digitális és fizikai interakciók szétválaszthatatlanul

[10] HERATH – WHITTAKER (2021): 1027–1048.

összefonódnak. Ahogy fogalmaznak, „a radikalizációs folyamatok úgy fejlődnek és alakulnak, hogy mindkét dimenzió elemeit integrálják”, vagyis a radikalizáció nem kizárólag az egyik vagy másik térben zajlik, hanem ezek kölcsönhatásában nyer értelmet.

Ezt a dinamikát jól illusztrálják a közösségi média ajánlórendszerei, amelyek bizonyos körülmények között felerősíthetik a szélsőséges tartalmak terjedését, hozzájárulva a szűrőbuborékok kialakulásához. Bár az algoritmusok által vezérelt tartalomajánlás elsődlegesen digitális jelenségnek tűnik, valójában számos offline tényezőt is figyelembe vesz. A felhasználók fizikai tartózkodási helye, demográfiai jellemzői és társadalmi környezete egyaránt befolyásolhatja, hogy milyen tartalmakkal találkoznak az online térben.

Whittaker kutatásai szintén rávilágítanak arra, hogy a terroristák propagandával való érintkezése nem kizárólag online folyamat. Bár a szélsőséges tartalmak terjedése és fogyasztása jellemzően digitális platformokon történik, azok hatása gyakran az offline kapcsolati hálókon keresztül erősödik fel. Az egyének nem pusztán passzív fogyasztói a szélsőséges ideológiáknak, hanem aktívan megvitatják és tovább ajánlják azokat személyes környezetükben, ezzel is hozzájárulva a radikalizáció terjedéséhez. Ennek fényében az online és offline radikalizáció közötti merev elkülönítés nemcsak mesterséges, hanem akadályozhatja is a jelenség teljes körű megértését.[11]

4. RADIKALIZÁCIÓ ÉS ÖSSZEESKÜVÉSELMÉLETEK

Bár a radikalizáció fogalma és értelmezése folyamatosan bővül, egyre világosabbá válik, hogy a szélsőséges gondolkodásmód kialakulása nem csupán ideológiai vagy vallási narratívák mentén történik. Az információs tér átalakulásával a radikalizáció egyre gyakrabban olyan alternatív világmagyarázatokra épül, amelyek az összeesküvés-elméletek logikáját követik.

Az összeesküvés-elméletek és a radikalizáció közötti kapcsolat többdimenziós és szinergikus jellegű. E jelenségek gyakran kölcsönösen erősítik egymást, és elősegíthetik a szélsőséges meggyőződések kialakulását, valamint az ezekből fakadó deviáns vagy erőszakos cselekedeteket. Az összeesküvés-elméletek narratívái gyakran legitimálják a radikális ideológiákat, míg a radikalizáció folyamata fokozhatja a konspirációs gondolkodás elfogadását és belsővé tételét. A két jelenség közötti összefüggés komplex és többrétegű,

[11] WHITTAKER (2023)

amely pszichológiai, társadalmi és technológiai tényezők kölcsönhatásán keresztül válik értelmezhetővé.[12]

A radikalizáció jelenségének átfogóbb értelmezése során fontos figyelembe venni az új, nem hagyományos formákat is. Az összeesküvés-elméletek terjedése és az ezekre való fogékonyság növekedése egy ilyen új dimenzióját jelenti a radikalizációnak.[13]

Az összeesküvés-elméletek nem csupán ártalmatlan hiedelemrendszerek, hanem gyakran a radikalizáció melegágyául is szolgálnak. Ezek a narratívák egy közös ellenségképre épülő alternatív valóságértelmezést kínálnak, amely éles „mi" és „ők" dichotómiát konstruálva fokozza a társadalmi polarizációt. E hatás különösen szembetűnő az online terekben, ahol az összeesküvés-elméletek terjedése és a radikalizáció egymást erősítő folyamatként jelenik meg.

A dezinformáció hatékonysága részben pszichológiai tényezőkre vezethető vissza: az emberek nem csupán a megtévesztés következtében hisznek az ilyen tartalmakban, hanem azért is, mert ezek megerősítik előzetes világképüket és kognitív sémáikat. Az emberi megismerés társas és szimbolikus kontextusban formálódik, és a kollektíven osztott meggyőződések jelentős mértékben befolyásolják a valóságról alkotott felfogást. Ebben az értelemben az, amit egy adott közösség igaznak tart, pszichoszociológiai szempontból valóságteremtő erővel bírhat, és hatással lehet történelmi-társadalmi folyamatokra is.[14]

A populáris kultúra – különösen a nagy közönséget elérő könyvek és filmek – szintén közvetítő közegévé válhat a konspirációs narratívák terjedésének. Empirikus vizsgálatok igazolták, hogy bizonyos kulturális termékek – például Dan Brown *A Da Vinci-kód* című regénye vagy Oliver Stone *JFK* című filmje – hozzájárulhatnak az összeesküvés-elméletekbe vetett hit erősödéséhez, miközben gyengíthetik a társadalmi intézményekbe vetett bizalmat.

Fontos azonban megkülönböztetni a valós összeesküvéseket a spekulatív, empirikus alapot nélkülöző elméletektől. A történelem során számos tényleges konspiráció – például politikai puccsok, gazdasági kartellek vagy sportbotrányok – került napvilágra. E precedensek nyomán egyes társadalmi csoportok körében a gyanakvás és a bizalmatlanság adaptív túlélési stratégiává válhatott, különösen marginalizált vagy üldözött közösségek esetében. Az összeesküvéses gondolkodás tehát pszichológiai értelemben részben a fenyegetésészlelésre adott válaszként is értelmezhető.[15] Ezzel szemben az összeesküvés-elméletek túlnyomó többsége nem rendelkezik valóságos empirikus megalapozottsággal. Ezek a narratívák hosszú

[12] MSALL – LARY (2022)
[13] MCCURDY (2021)
[14] PROOIJEN – DOUGLAS (2022): 1–23.
[15] KREKÓ (2023)

távon aláássák a tudományos tények, valamint az intézményes szakértelem legitimációját, és hozzájárulnak az akadémiai tudás társadalmi elfogadottságának csökkenéséhez.

A konspirációs gondolkodás nem újkeletű jelenség. Bár gyökerei a mágikus világértelmezésig vezethetők vissza, strukturáltabb formái a kora modern kor idején jelentek meg, amikor a vallási dichotómiák helyét egyre inkább a társadalmi-politikai ellentétek vették át. A francia forradalmat követően az összeesküvés-elméletek szekuláris jellege vált dominánssá: hangsúlyuk a hatalom és a társadalmi többség-kisebbség viszonyaiban artikulálódott.[16]

A 20. század történelmi eseményei – többek között a tömegpusztító fegyverek alkalmazása, az állami propaganda rendszerei és a polgári szabadságjogokat korlátozó megfigyelési gyakorlatok – tovább erősítették a társadalmi érzékenységet a konspirációs narratívák iránt. A modern technológia, a tömegmédia, valamint az autoriter rendszerek működési logikája hozzájárultak annak a kollektív percepciónak a kialakulásához, miszerint a hatalom képes lehet a valóság tudatos manipulálására.

Ebben az értelemben a modern összeesküvés-elméletek maguk is a modernitás termékei: egyszerre reflektálnak a komplex társadalmi rendszerek által keltett bizonytalanságra, és egyúttal igényt formálnak a koherens magyarázatokra. Az ilyen elméletek leegyszerűsítik a társadalmi valóságot, és lineáris, oksági viszonyokra épülő narratívák formájában kínálnak pszichológiai megnyugvást a befogadó számára.

Napjainkban az összeesküvés-elméletek és a dezinformáció elterjedése nem csupán az egyéni kognitív torzítások következményeként értelmezhető, hanem mélyebb társadalmi változások indikátoraként is. Több kutató szerint az „igazság utáni” korszakban az objektív tények igazolhatósága helyett az számít, hogy ki tudja hatékonyabban artikulálni és terjeszteni a saját narratíváját. Az igazság társadalmi konstrukcióként való értelmezése egyfajta „igazságpiacot” eredményezett, ahol versengő valóságértelmezések kerülnek szembe egymással, és a tudomány korábbi közvetítő szerepe marginalizálódhat. E folyamat velejárója, hogy az összeesküvés-elméletek hívei gyakran úgy érzik: ők képviselik az „alternatív igazságot”, és ellenállóként lépnek fel a domináns hatalmi struktúrákkal szemben. Ez a pozíció egyfajta demokratikus kontrollt imitál, ám gyakran együtt jár a tudományos, intézményes tudásformák elutasításával. A kritikus gondolkodás ilyenkor torzulhat öncélú szkepszissé, amelyben a kétely nem a megismerés kezdete, hanem annak lezárása lesz.

[16] CHRISTOPH (2022): 135–145.

Az összeesküvés-elméletek pszichológiai vonzereje részben abból ered, hogy egyszerű, narratív keretbe ágyazva kínálnak értelmezést komplex, gyakran traumatikus eseményekre. Ezek az elbeszélések világos erkölcsi felosztásokat hoznak létre, egyértelmű felelősöket neveznek meg, és érzelmi megnyugvást kínálnak a bizonytalansággal szemben. A feltételezett szándékosság révén a világot koherensnek és morálisan rendezettnek mutatják be, ami fokozhatja a befogadó kontrollérzetét.

Mindezek alapján az összeesküvéses gondolkodás nem csupán egyéni pszichológiai vagy szociális jellemzőkkel magyarázható. Létrejötte és fennmaradása a tágabb társadalmi-kulturális kontextus, valamint a csoportidentitások, kognitív torzítások és érzelmi szükségletek kölcsönhatásaként értelmezendő. Az ilyen típusú narratívák különösen vonzóvá válhatnak olyan helyzetekben, amelyek bizonytalansággal, fenyegetettség-érzettel vagy információs túlterheltséggel járnak.[17]

5. NEMZETBIZTONSÁGI ASPEKTUSOK

A demokratikus rendszerek stabilitása szempontjából kulcsfontosságú a bizalom és a kritikai attitűd egyensúlya. Az olyan intézmények, mint a független média, a civil társadalmi szervezetek, a bíróságok és a hatalomellenőrző mechanizmusok képesek strukturált módon kezelni a társadalmi visszaéléseket, ezzel csökkentve a tényleges összeesküvések kialakulásának esélyét. Ezért is alapvető fontosságú, hogy a közvélemény differenciálni tudja a megalapozott aggodalmakat a spekulatív, bizonyítatlan elméletektől.[18]

Az összeesküvés-elmélet olyan meggyőződés, amely szerint egy vagy több, jelentős hatalommal rendelkező szereplő titokban együttműködik egy olyan terv végrehajtásán, amely hátrányosan érinti egy adott társadalmi csoport érdekeit. Az ilyen hiedelmek központi eleme, hogy a feltételezett összeesküvők célja valamilyen politikai, gazdasági vagy társadalmi befolyás megszerzése, illetve megtartása – gyakran rejtett, átláthatatlan eszközökkel.

Dezinformáció alatt azokat a szándékosan félrevezető kommunikációs stratégiákat értjük, amelyek célja a közvélemény manipulálása. Ezek a technikák nem csupán teljesen kitalált tartalmak révén működnek, hanem meglévő információk torzított értelmezésén, kiragadásán vagy szelektív kombinálásán keresztül is. A manipuláció tehát sokszor nem az információ abszolút hiányán, hanem annak torz tálalásán alapul.

Az elterjedtebb és szélesebb társadalmi ismertséggel bíró összeesküvés-elméletek hatása jóval túlmutat az egyéni vélekedéseken. Ezek a narratívák érdemben befolyásolhatják a

[17] KREKÓ (2023)
[18] KREKÓ (2023)

politikai döntéshozatalt, felerősíthetik a társadalmi csoportok közötti feszültségeket, és alakíthatják az egyének viselkedését, attitűdjeit is.[19]

Egyes elméleti megközelítések szerint az összeesküvés-elméletek nem csupán alulról jövő társadalmi reflexiók, hanem a hatalmi egyensúlytalanságokra adott kommunikációs válaszreakciók, különösen olyan csoportok esetében, amelyek marginalizált helyzetükből fakadóan bizalmatlanok az intézményi struktúrákkal szemben. E nézőpont szerint az ilyen narratívák az identitáspolitikai önérvényesítés és a társadalmi frusztráció artikulálásának eszközeiként jelennek meg. Ugyanakkor egyre nyilvánvalóbbá válik, hogy az összeesküvés-elméletek nem csak spontán alakulhatnak ki, hanem tudatos információs műveletek eredményeként is keletkezhetnek, ezzel stratégiai célokat szolgálva. Különböző politikai aktorok, vagy akár üzleti érdekcsoportok alkalmazzák ezeket a narratívákat a társadalmi bizalom megingatására, a politikai ellenfelek delegitimálására, valamint az információs tér kontrollálására. Ebben a kontextusban az összeesküvés-elméletek a kognitív befolyásolás eszköztárába illeszkednek, mivel képesek manipulálni a kollektív észleléseket, gyengíteni a valóság iránti konszenzust, és polarizálni a közvéleményt. A digitális médiakörnyezetben ezek a tartalmak gyorsan és hatékonyan terjednek, kihasználva a társadalmi kohézió megbomlását és a közösségi média algoritmikus erősítő hatásait.

A „posztigazság" korszakában ez a jelenség kétszintű dinamikát ölt: egyrészt a komplex társadalmi problémák leegyszerűsítésére irányuló kereslet, másrészt az ezekre épülő szándékos dezinformációs kínálat párhuzamos növekedése jellemzi. Ez a kereslet–kínálat viszony erősíti meg azokat az információs környezeteket, ahol a valóság interpretációja nem empirikus alapokon, hanem narratív versengésen és pszichológiai hatékonyságon nyugszik.[20]

Egy állam érdekérvényesítő képessége, funkcionális működése és szuverenitásának fenntarthatósága jelentős mértékben összefügg az intézményi bizalom szintjével, különösen demokratikus berendezkedésű rendszerekben. Válsághelyzetek – mint amilyen a COVID–19 pandémia volt – rávilágítottak arra is, hogy a társadalmi együttműködés és mozgósíthatóság, valamint a legitim, tudományosan megalapozott központi narratíva megléte kulcsszerepet játszhat a hatékony kríziskezelésben. Noha az uralkodó narratívák önmagukban nem garantálják a társadalmi rezilienciát, egy világosan kommunikált, transzparens és hiteles információs keretrendszer képes elősegíteni a kollektív cselekvést, és ezzel közvetett módon hozzájárulhat emberéletek megóvásához. Ugyanakkor e tényezők hatása nem kizárólag a

[19] KREKÓ (2023): 22–23.
[20] KREKÓ (2023): 15.

tartalmukon, hanem azok politikai kontextusán, alkalmazási módján és társadalmi befogadottságán is múlik.[21]

A fentiek fényében világossá válik, hogy az összeesküvés-elméletek nem csupán kognitív vagy társadalomlélektani szempontból érdemelnek figyelmet, hanem biztonságpolitikai és stratégiai kontextusban is. A modern információs műveletek során e narratívák nem passzív melléktermékei a társadalmi frusztrációknak, hanem gyakran aktív eszközei célzott destabilizációs folyamatoknak. Az úgynevezett „cognitive warfare" – kognitív hadviselés – keretében a dezinformáció és a konspiratív narratívák használata képes megbontani a társadalmi kohéziót, gyengíteni a döntéshozatali mechanizmusokat, és aláásni az állampolgárok és intézmények közötti bizalmat.

A kollektív információfeldolgozás manipulálása különösen hatékonynak bizonyul olyan kontextusokban, ahol a társadalmi polarizáció, a gazdasági bizonytalanság vagy az intézményi inkompetencia tapasztalata már eleve jelen van. Az összeesküvés-elméletek ebben az értelemben nem pusztán következményei, hanem előidézői is lehetnek a radikalizációs folyamatoknak. A narratív keret, amelyben az egyén értelmezi a valóságot, könnyen átcsúszhat egy „mi és ők" típusú világképre, amely nemcsak a politikai diskurzust mérgezi, hanem a társadalmi együttműködés alapjait is alááshatja.[22]

Mindez különös súlyt ad a nemzetbiztonsági szempontoknak. A társadalmi kohézió és információs önrendelkezés sérülése – például ha az állampolgárok jelentős része a hivatalos tájékoztatást szisztematikusan hiteltelennek tartja – közvetlenül befolyásolja az állam kríziskezelő képességét, sőt, hosszabb távon a demokratikus intézményrendszer fenntarthatóságát is. Az információs térben zajló befolyásolási kísérletek – legyenek azok külső vagy belső eredetűek – így nem pusztán kommunikációs kihívások, hanem stratégiai fenyegetések is.

Az ilyen jelenségek kezelésére irányuló politikai és társadalmi válaszoknak ezért nem szabad kizárólag represszív vagy technikai megoldásokra korlátozódniuk. A hosszú távú reziliencia alapja a közbizalom tudatos építése, a médiatudatosság fejlesztése, valamint a nyílt és transzparens állami kommunikáció megerősítése. Ugyanakkor elengedhetetlen egy olyan nemzetbiztonsági gondolkodásmód kialakítása is, amely felismeri az információs térben zajló hatásgyakorlás sokszintűségét, és képes arra adaptív, demokratikus, mégis hatékony választ adni.[23]

[21] ELCHEROTH – DRURY (2020)
[22] MARIE – PETERSEN (2022)
[23] GOEL (2020)

6. ÚJ IRÁNYOK

A vegyes ideológiákhoz kapcsolódó radikalizáció és az összeesküvés-elméletek szerepe olyan komplex folyamat, amelyet egyaránt formálnak pszichológiai hajtóerők, társadalmi környezet és technológiai közvetítőrendszerek. A vegyes, tisztázatlan és instabil (Mixed, Unclear, Unstable – MUU) ideológiák egyre gyakoribbá válnak azok körében, akik szélsőséges cselekedetek elkövetésére hajlanak. Ezek az ideológiai mintázatok sokszor nem rendelkeznek koherens elméleti struktúrával, mégis közös jellemzőjük, hogy alapvető elemként tartalmaznak összeesküvéses narratívákat. A konstrukció nem csupán egyéni értelmezési folyamat eredménye, hanem erőteljes hatással van rá a digitális ökoszisztéma, valamint a társadalmi struktúrák által kiváltott bizonytalanságélmény is. Az ilyen narratívák képesek értelmet és közösségi kapaszkodót nyújtani az egyének számára, miközben fokozzák az elkülönülés és az erőszakra való hajlam kockázatát.

Az összeesküvés-elméletek sajátos pszichológiai szerepet töltenek be a radikalizálódás során, mivel képesek kielégíteni az egyének jelentőségtudat iránti szükségletét, egyben világos és személyesíthető felelőst rendelnek a tapasztalt sérelmekhez. E folyamat különösen jól magyarázható a radikalizáció úgynevezett 3N modellje alapján, amely szerint az összeesküvéses hiedelmek egyrészt motiválják az erőszakos viselkedést az észlelt ellenséggel szemben, másrészt megerősítik az identitást azáltal, hogy éles határvonalat húznak a „tudók” és a „kívülállók” között, valamint egy támogató, azonos értékeket valló közösségbe integrálnak.[24] Ezek a funkciók együttesen elősegítik az egyén leválását a mainstream társadalmi normákról, és megteremtik a radikális magatartás legitimitását.

A jobboldali szélsőséges ideológiák jelentős részében kiemelkedő szerepet játszanak az antiszemita összeesküvés-elméletek. Ezek nem csupán történeti alapon szivárogtak be az eszmerendszerekbe, hanem napjainkban is aktívan strukturálják a radikális csoportok világképét, különösen olyan mozgalmakban, mint a fehér felsőbbrendűséget hirdető vagy keresztény identitásalapú szerveződések. Ezekben a közösségekben az antiszemitizmus nem perifériális, hanem központi szervező elvként működik, amely erősíti az ideológiai kohéziót és igazolja az erőszakos fellépést.[25]

A MUU ideológiák kialakulásának hátterében többek között az olyan technológiai eszközök tudatos alkalmazása áll, mint az ún. „outlinking” stratégia, amely lehetővé teszi, hogy az egyének különféle ideológiai elemeket gyűjtsenek össze és illesszenek be saját világképükbe. Ez a folyamat nem lineáris, hanem folyamatos újrastrukturálódás jellemzi,

[24] KRUGLANSKI et al. (2022)
[25] BYINGTON (2019): 1–18.

különösen azokban a szubkultúrákban, ahol az identitáskeresés intenzív formában zajlik. Jó példa erre az „inceloszféra”, ahol a COVID–19 járvány okozta társadalmi elszigeteltség és intézményi szigorítások hatására a már meglévő ideológiai tartalmak hibrid formákban kezdtek tovább élni és radikalizálódni.[26]

A közösségi média platformok meghatározó szerepet töltenek be a vegyes ideológiák terjedésében, mivel lehetőséget biztosítanak az alternatív narratívák gyors és célzott terjesztésére. E folyamat egyik látványos példája a QAnon-mozgalom, amely demonstrálja, hogy a digitális közeg miként járulhat hozzá az összeesküvés-elméleteken alapuló radikalizálódáshoz. Az online interakciók és a közösség által generált tartalmak az ilyen mozgalmakban nem csupán tájékoztatnak, hanem normatív mintákat is közvetítenek, amelyek fokozatosan átalakítják a résztvevők világlátását. Bár a platformok próbálkoztak moderációs eszközök alkalmazásával, ezek korlátozott sikerrel jártak, mivel a radikális tartalmak újraformálódva vagy alternatív csatornákon keresztül továbbra is elérhetőek maradtak.[27]

A COVID–19 világjárvány különösen kedvezett az új típusú radikalizációs mintázatok kialakulásának, főként olyan mozgalmak esetében, amelyek alapvetően kormányellenes vagy rendszerkritikus álláspontokat képviseltek. A kanadai Freedom Convoy mozgalom jól példázza, hogyan fonódhatnak össze az oltásellenes és a szélsőjobboldali diskurzusok egy közös platformon. Az algoritmus vezérelt tartalomterjesztés fokozta az ilyen nézetek megerősítését, miközben marginalizálta az eltérő véleményeket, így megerősítve a buborékhatást és az ideológiai homogenizációt.[28]

Egy további, gyakran alábecsült tényező a platformcenzúra következményrendszere. A közösségi média felületeken alkalmazott központosított vagy decentralizált moderációs gyakorlatok – bár céljuk a félretájékoztatás visszaszorítása – olykor éppen az ellenkező hatást válthatják ki. Az eltérő vélemények kiszorítása vagy láthatatlanná tétele a már eleve radikalizálódás felé sodródó egyéneket tovább erősítheti meggyőződéseikben, mivel az információk elfojtása csak megerősíti a hatalmi struktúrákba vetett bizalmatlanságot és a cenzúra élményét.[29] Ez a paradoxon rávilágít arra, hogy a digitális térben történő beavatkozások nem lehetnek egydimenziósak, hanem érzékenyen kell illeszkedniük a felhasználók érzelmi és értelmezési kereteihez.

Bár az összeesküvés-elméletek integrálása a radikális ideológiákba ma már széles körben ismert és vizsgált jelenség, nem hagyható figyelmen kívül az a társadalmi és egyéni

[26] COOLSAET (2019): 29-51.
[27] WANG et al. (2022)
[28] HOECHSMANN – MCKEE (2023)
[29] LANE et al. (2021)

kontextus, amelyben ezek a hiedelmek kialakulnak és megerősödnek. A radikalizálódás nem egyetlen lineáris úton halad végbe, hanem különböző utak és motivációk mentén zajlik, amelyeket egyszerre formál az identitáskeresés, az információs tér dinamikája, valamint a kollektív frusztrációk strukturális jelenléte. Ezért a megelőzési és beavatkozási stratégiák nem épülhetnek kizárólag az ideológiai tartalom semlegesítésére, hanem figyelembe kell venniük azokat az érzelmi, pszichológiai és társadalmi mechanizmusokat is, amelyek az egyént egyáltalán fogékonnyá teszik az ilyen narratívák iránt. A hatékony válaszhoz szükség van olyan komplex megközelítésekre, amelyek árnyaltan értelmezik a radikalizálódás hátterét, és képesek érzékenyen reagálni a kontextus-specifikus mozgatórugókra. Enélkül a beavatkozások nem csupán hatástalanok maradhatnak, hanem akár kontraproduktív következményeket is kiválthatnak.

7. ESETTANULMÁNY

7.1. TARTALOMELEMZÉS, MINT MÓDSZER

A szövegelemzés napjainkra egyre fontosabb szerepet tölt be a radikalizálódási folyamatok felismerésében és megelőzésében, különösen az online közösségimédia-platformokon aktív személyek esetében. A közösségi média, mint kommunikációs tér kiemelten releváns, mivel ezek a platformok nemcsak az információterjesztés, hanem a társadalmi identitásépítés, a véleményformálás és az ideológiai befolyásolás színterei is. A radikalizálódási folyamatok feltérképezése érdekében a szövegelemzés technikai és tudományos módszertani eszköztárát használják a kutatók annak érdekében, hogy azonosítsák azokat a nyelvi, pszichológiai és viselkedési jellemzőket, amelyek korai indikátorai lehetnek a szélsőséges gondolkodásmód kialakulásának. Ennek során a természetes nyelvfeldolgozás és a gépi tanulási algoritmusok segítségével nagyméretű szöveges adatállományokból képesek kinyerni olyan mintázatokat, amelyek figyelmeztető jelekként szolgáltathatnak a radikalizációs folyamatok elindulásáról, előrehaladásáról vagy konszolidálódásáról.

A kutatások rámutattak, hogy a különböző közösségi terekben eltérő szöveges és viselkedési mintázatokat mutat a radikalizáció, és ezek a különbségek jól nyomon követhetők szövegelemzési módszerekkel. Egy, az Alt-Right mozgalom Reddit-fórumait vizsgáló tanulmány kimutatta, hogy a szélsőséges diskurzusokat folytató közösségek sajátos nyelvi struktúrákat, szókészletet és érzelmi töltetet használnak, amelyek egyértelműen elhatárolják őket más, politikailag orientált csoportoktól.[30] A radikalizációs folyamat során megjelenő

[30] GROVER – MARK (2019): 193–204.

pszichológiai és érzelmi jellemzők szintén leképezhetők szövegelemzéssel. Különösen ígéretesnek bizonyultak azok a modellek, amelyek a pszichológiai profilalkotást ötvözik a szöveges jellemzők – például szentimentanalízis vagy szóvektoralapúbeágyazások – vizsgálatával. Az ilyen multimodális megközelítések jelentős pontosságjavulást eredményeztek a radikális tartalmak detektálásában például a Twitter platformon, ahol a radikalizmus különösen gyorsan terjedhet a nyilvános viták és a rövid formátumú üzenetküldés miatt.[31]

A radikális ideológiák online terjedésének megértéséhez nem elegendő kizárólag a szóhasználat és a szintaktikai szerkezet vizsgálata; elengedhetetlen a narratívák és a retorikai struktúrák elemzése is. A társadalomtudományi megközelítések lehetővé teszik, hogy a kutatók feltárják azokat a narratív mintázatokat – például a mártíromság, a kirekesztettség, az igazságtalanság vagy a bosszú motívumait –, amelyek visszatérően jelen vannak ezekben a diskurzusokban. Az így feltérképezhető struktúrák lehetőséget biztosíthatnak taxonómiák kialakítására, amelyek mentén a különböző ideológiai alapú szélsőségek felismerhetők és elkülöníthetők egymástól.[32]

Mindamellett meg kell említeni azt is, hogy a szövegelemzés műfaja komoly kihívásokkal áll szemben. Az egyik legjelentősebb technikai akadály a szélsőséges tartalmak komplexitásában és kontextusfüggőségében rejlik. A radikális diskurzus nem mindig explicit; gyakran rejtett, eufemisztikus, ironikus vagy mémformában jelenik meg, amely nehezen azonosítható automatikus elemző eszközökkel. Emellett a hamis pozitív és negatív eredmények arányának csökkentése kulcsfontosságú, hiszen ezek közvetlenül befolyásolják a beavatkozások hatékonyságát és társadalmi elfogadottságát.[33] A radikális csoportok továbbá rendkívül gyorsan alkalmazkodnak, és gyakran módosítják nyelvhasználatukat vagy új platformokra helyezik át kommunikációjukat, amint az észlelési mechanizmusok nyomukba erednek. Ez folyamatos modellfrissítést és fejlesztést tesz szükségessé, különösen olyan időszakokban, amikor politikai vagy társadalmi események fokozzák az ideológiai polarizációt.[34]

Az adatvédelem és az etikai keretek betartása is kulcsfontosságú. A szövegelemzési eljárások, különösen, amikor azokat megelőző célzattal alkalmazzák, olyan adatvédelmi dilemmákat vetnek fel, amelyek a magánélet védelme, a megfigyelés legitimációja és az állami beavatkozás határai körül kristályosodnak ki. Egyes szakértők attól tartanak, hogy a

[31] NOUH – NURSE – GOLDSMITH (2019)
[32] DENAUX – GÓMEZ-PÉREZ (2019): 39–45.
[33] ALDERA et al. (2021): 42384–42396.
[34] WOLBERS – DOWLING – CUBITT (2023)

szövegelemzésre alapozott megelőzési gyakorlatok indokolatlan megfigyeléshez, sőt esetenként célzott diszkriminációhoz vezethetnek, különösen, ha az algoritmusokat nem megfelelően kalibrálják kulturális, társadalmi és nyelvi kontextusok szerint.[35]

A szövegelemzés jelentőségét az is alátámasztja, hogy alkalmazásával lehetőség nyílik a proaktív monitoringra, amely nem csupán reagál a már kialakult radikális attitűdökre, hanem előzetesen azonosítja azokat a kommunikációs jegyeket, amelyek a radikalizálódás folyamatára utalnak. Ez különösen értékes lehet a megelőzési stratégiák időzítésének szempontjából, mivel az időben történő beavatkozás csökkentheti annak valószínűségét, hogy az érintett egyének erőszakos cselekmények elkövetéséig jussanak.[36] A módszer hatékonyságát tovább növeli, ha azt közösségi hálózatelemzéssel kombinálják. Ez a kettős megközelítés lehetővé teszi annak feltérképezését, hogy a radikális ideológiák miként terjednek a közösségi struktúrákon belül, illetve hogy mely csomópontok – például véleményvezérek vagy befolyásos csoportok – játszanak kulcsszerepet a radikalizmus közvetítésében. A közösségi kapcsolati hálók és a szöveges tartalmak együttes elemzése hozzájárulhat a célzottabb és hatékonyabb beavatkozások kidolgozásához.[37]

Mindazonáltal a tartalomelemzés alkalmazása nem tekinthető mindenható megoldásnak. A módszertani korlátok, az adaptív ellenstratégiák, valamint az etikai és jogi keretek feszegetése egyaránt arra utalnak, hogy a szövegelemzést átfogóbb társadalomtudományi és biztonságpolitikai keretbe kell ágyazni. A digitális kommunikáció természeténél fogva állandóan változik, és ennek megfelelően a radikális diskurzus is gyorsan alkalmazkodik a platformokhoz, algoritmusokhoz és aktuális társadalmi környezethez.

7.2. VIZSGÁLT DOKUMENTUMOK

Jelen tanulmány vizsgálatának középpontjában Solomon Henderson naplója és manifesztója áll. Henderson 2025. január 22-én hajtott végre halálos iskolai támadást a Tennessee állambeli Nashville egyik középiskolájában, amely során megölte egyik diáktársát, majd önmagával is végzett. Ezt megelőzően hosszabb időn át online felületeken publikált szövegeken keresztül részletesen megfogalmazta világképét, sérelmeit és indokait. Az általa közzétett dokumentumokban – egy 51 oldalas manifesztóban és egy 288 oldalnyi naplóban – szélsőséges, náci ideológiákra alapozott gondolatrendszert fogalmazott meg, miközben mély önutálattól és faji önazonosság-krízistől jellemzett belső konfliktusát is tükrözte. Az elemzés szempontjából különösen figyelemre méltó, hogy Henderson fekete

[35] SUSENO – GULTOM – HIDAYAT (2023)
[36] GROVER – MARK (2019): 193–204.
[37] WOODHAMS (2016)

tinédzserként azonosult a fehér felsőbbrendűséget hirdető, antiszemita nézetekkel, miközben saját etnikai hovatartozását „alfajként” minősítette és gyűlölet tárgyává tette. Ez a belső ellentmondás nem csupán tartalmilag, hanem nyelvileg is megjelenik az írásaiban, és kiemelt jelentőséggel bír a radikalizációs diskurzus önromboló aspektusainak megértésében. A vizsgált dokumentumok tematikus rétegzettségük, érzelmi töltetük és fokozatosan eltolódó retorikai szerkezetük révén különösen értékes forrásként szolgálnak annak nyomon követéséhez, hogyan alakul át az egyéni frusztráció és önértelmezés nyelvezete fokozatosan egy erőszakos cselekedet nyelvi előkészítésévé.

A dokumentumok szisztematikus vizsgálata különösen fontos a kevert ideológiai alapú radikalizáció jelenségének mélyebb vizsgálatában – annál is inkább, mert ezekben az írásokban a náci eszmerendszer motívumai saját faji identitásának válságával fonódnak össze. Ez a paradox viszonyrendszer új távlatokat nyithat a radikalizáció pszichológiai és társadalmi hátterének feltérképezésében. A szöveg ezen dimenziói lehetőséget kínálnak például pszicholingvisztikai megközelítésű vizsgálatokra is, amelyek nyelvi szinten tárhatják fel a személyiség fragmentáltságát, az agresszió artikulációját és a kognitív torzulásokat. Jelen tanulmány – szakmai jártasság híján – nem vállalkozik e mélyrétegek feltárására, hanem két, különböző időpontban készült szöveges dokumentum szóhasználatát hasonlítja össze szófelhők segítségével. A vizsgálat egyik központi kérdése az volt, hogy a kiemelkedően gyakori nyelvi elemek (főnevek, igék, melléknevek) alapján lehetséges-e egy olyan elméleti szólista körvonalazása, amely később a monitoring tevékenységben – megelőző célú szűrőkutatás részeként – releváns szűrési keretet nyújthat. Bár az ilyen típusú szólisták nem helyettesíthetik a kontextuális elemzést, a gyakorisági mintázatok és tematikus hangsúlyok alapján kirajzolódhatnak olyan figyelmeztető jelek, amelyek a radikalizálódás korai stádiumaira utalhatnak. A másik vizsgálati kérdés, hogy a kiválasztott szavak előfordulási gyakorisága miként változik a szöveg előrehaladtával.

Az elemzéshez a *MAXQDA Pro* kvalitatív adatelemző szoftver 14 napos próbaverzióját használtam, amely lehetővé tette a szövegek strukturált vizsgálatát, valamint a kulcsszavak előfordulási gyakoriságának nyomon követését időrendben. A szoftver segítségével azonosítani tudtam a releváns tematikus kategóriákat és a kapcsolódó szóhasználati mintázatokat. A MAXQDA vizualizációs és statisztikai funkciói hozzájárultak ahhoz, hogy a kvalitatív tartalomelemzés kiegészüljön kvantitatív szemlélettel, és így megbízhatóbb képet kapjak a napló és manifesztó belső dinamikájáról.

A vizsgálat során a Henderson által írt két dokumentum szövegéből származó szóelőfordulásokat vettem elemzés alá, kvantitatív szemléletet alkalmazva. Az elemzésbe

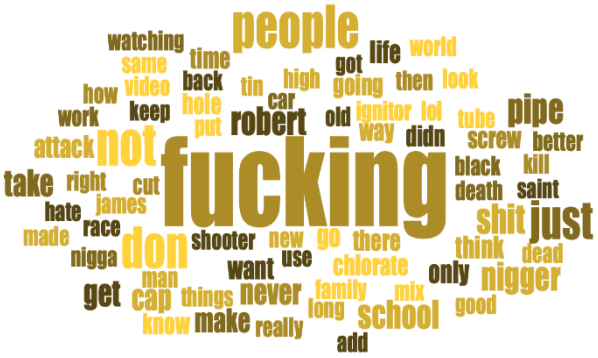
csak azon lexikai elemek kerültek be, amelyek legalább nyolc alkalommal szerepeltek az adott dokumentumban. Ez a küszöbérték igazodott a két forrás terjedelmi különbségeihez, és lehetővé tette a tartalmilag releváns, de statisztikailag is kellően reprezentált szóelemek kiemelését, kizárva a véletlenszerű vagy marginális előfordulásokat.

Mindkét dokumentum esetében egy összesített szófelhő készült, amelyből eltávolításra kerültek az irreleváns elemek: számok, e-mail címek, valamint – különösen a napló esetében – a dátumok, mivel ezek nagyszámú, de tartalmilag semleges előfordulása torzította volna az interpretációs lehetőségeket. Az automatizált szövegelemző program – amely szófaji kategóriák szerinti bontást is lehetővé tett – lehetőséget adott arra, hogy az általános szófelhőn túl célzottan is vizsgáljam három kiemelt szófaj (főnevek, melléknevek és igék) gyakoriságát és tematikus eloszlását. Bár manuális kódolásra nem került sor, így is kizárhatóak voltak a szófaji szűrés során azok a szavak, amelyek funkcionális jellemzőik (pl. kötőszavak, névmások, helyhatározók) révén nem hordoznak érdemi tartalmi információt, illetve kevésbé alkalmasak az ideológiai és érzelmi mintázatok feltárására.

A főnevek vizsgálata különösen fontos volt, mivel ezek hordozzák a diskurzus tárgyait, ideológiai referenciapontjait és a szövegben megjelenő társadalmi szereplők, csoportok, entitások reprezentációját. A melléknevek segítséget nyújtanak a beszélő attitűdjeinek, érzelmi viszonyulásának, értékítéleteinek feltérképezésében, míg az igék a cselekvésre, szándékokra, állapotokra és folyamatokra irányuló nyelvi struktúrák révén fontos indikátorai lehetnek a radikalizáció dinamikájának. E három szófaji kategória különálló vizsgálata tehát lehetővé tette a tartalmi, értékelő és cselekvésorientált nyelvi elemek differenciált feltérképezését, ezáltal megalapozva az elméleti szólistaképzés lehetőségét a későbbi monitoringcélú kutatásokban.

7.2.1. Összesített szófelhők

2. ábra: *Manifesztó összesített szófelhője*. (Maxqda24)



3. ábra: *Napló összesített szófelhője*. (Maxqda24)

A manifesztóból és a naplóból készült szófelhők összehasonlítása alapján megállapítható, hogy míg a napló szókészlete elsősorban a cselekvésre, erőszakos kivitelezésre és konkrét technikai részletekre koncentrál, addig a manifesztó nyelvezete ideologikusabb, elvontabb, és társadalmi kontextusban értelmezi a gyűlöletet. Mindkét szöveg erőteljesen átitatott gyűlöletbeszéddel, rasszista kifejezésekkel és erőszakos tematikával, ugyanakkor ezek eltérő módon jelennek meg. A napló impulzív, indulatos és trágár hangnemet üt meg, közvetlenül utal a potenciális cselekvésre (pl. iskolai támadás), míg a manifesztó inkább világmagyarázati narratívát épít, társadalmi és etnikai kategóriák mentén strukturálva az elutasítás és erőszak ideológiai megalapozását. A két szövegtípus egymást kiegészítve rajzolja ki a radikalizáció diskurzusának különböző szintjeit.

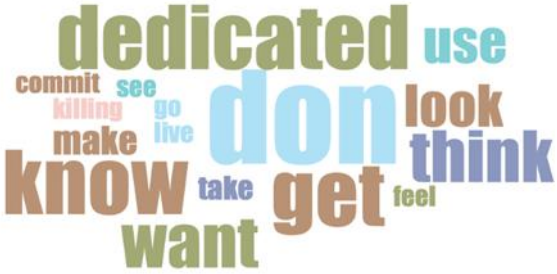
7.2.2. Főnevek szófelhői

4. ábra: *Manifesztó főneveinek szófelhője*. (Maxqda24)

5. ábra*: Napló főneveinek szófelhője*. (Maxqda24)

A főneveket külön vizsgáló szófelhők alapján a manifesztó és a napló jelentésvilága egyaránt erőteljesen tematizálja az erőszakot és a társadalmi konfliktusokat, ám különböző módon strukturálva azokat. A naplóban előforduló főnevek jelentős része konkrét tárgyakra és anyagokra utal – például *pipe, cap, tube, chlorate* –, amelyek egy erőszakos cselekmény technikai előkészítésére engednek következtetni. Ezzel szemben a manifesztó főnevei – mint *culture, laws, society, individuals* – inkább elvont, rendszerkritikai vagy ideológiai töltetű fogalmak, amelyek a szerző világértelmezésének részei. Mindkét szófelhőben dominánsan jelenik meg a „*people*" és a „*school*" kifejezés, amelyek az emberi közösség és az intézményes tér célpontként való azonosítását tükrözhetik. Míg a napló szókészlete a végrehajtás logikáját követi, a manifesztóé inkább az ellenségképzés és társadalmi polarizáció gondolati megalapozására szolgál.

7.2.3. Melléknevek szófelhői

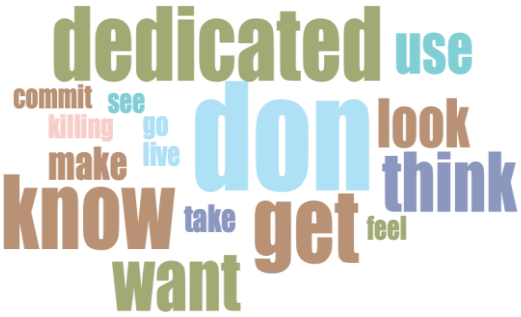


6. ábra: *Manifesztó mellékneveinek szófelhője*. (Maxqda24)

7. ábra: *Napló mellékneveinek szófelhője*. (Maxqda24)

A napló melléknévi szófelhője rendkívül szűk és indulatos nyelvezetet tükröz: a *fucking* dominánsan jelenik meg, ami az érzelmi túlfűtöttség és a nyelvi agresszió jele. A *same* és *black* melléknevek kontextusukban valószínűsíthetően homogenizáló, kirekesztő jelentést hordoznak. Ezzel szemben a manifesztó szófelhője tartalmaz pozitív töltetű melléknevet is (*good*), ugyanakkor ezt ambivalens, sőt nyíltan dehumanizáló kifejezések keretezik (*unworthy*, *nigger*), amelyek a szerző értékrendjének torzulását jelzik. A *black* mindkét szövegben megjelenik, ami a rassz alapú megkülönböztetés központi szerepére utal. A melléknevek alapján tehát jól látható, hogy a napló inkább nyers indulatot, míg a manifesztó értékalapú megítélést és kategorizálást közvetít, ezzel a gyűlöletbeszéd eltérő stilisztikai rétegeit aktiválva.

7.2.4. Igei szófelhők



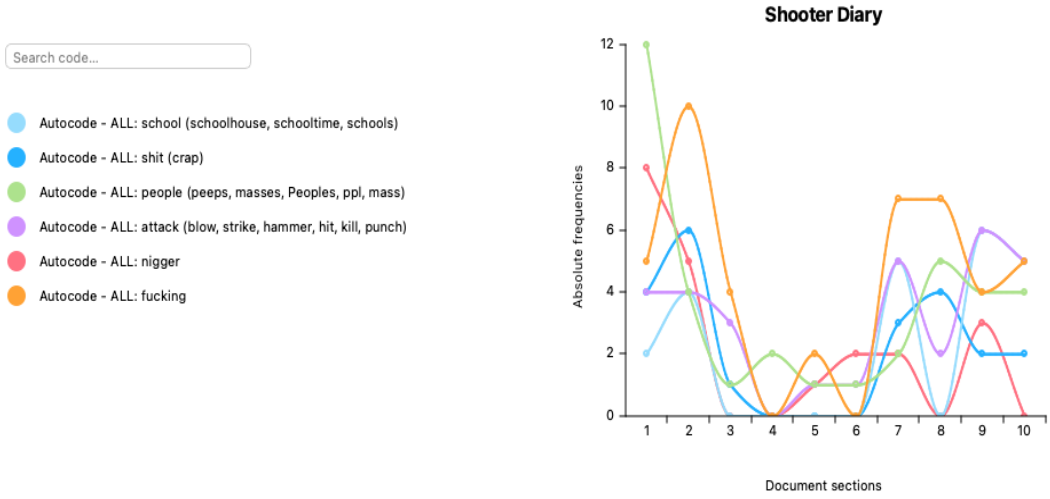
8. ábra: *Manifesztó igéinek szófelhője*. (Maxqda24)

93. ábra: *Napló igéinek szófelhője*. (Maxqda24)

Az igéket tartalmazó szófelhők elemzése alapján jól kirajzolódik a manifesztó és a napló nyelvi dinamizmusának eltérése. A naplóban szereplő igék – mint *take, make, put, cut, kill* – a végrehajtás logikáját követik, közvetlen, fizikai cselekvésre utalnak, és gyakran imperatív vagy célelvű jelentésmezőben helyezkednek el. Ezzel szemben a manifesztó szófelhője –

think, *know*, *feel*, *dedicated*, *want* – belső folyamatokra, szándékokra és elköteleződésre utal, ami a szöveg introspektívabb és ideologikusan motivált jellegét erősíti. Bár néhány közös ige – például *don*, *get*, *go*, *look* – mindkét szövegben megtalálható, ezek kontextuális jelentése eltérhet: míg a naplóban az igék a konkrét végrehajtáshoz kapcsolódnak, a manifesztó esetében inkább a gondolati előkészítést, vágyat vagy értelmezést fejezik ki. Az igék elemzése így jól érzékelteti a radikalizáció eltérő szakaszait: az egyik a megfontolás és motiváció nyelve, a másik a tetté formált szándék nyelvi lenyomata.

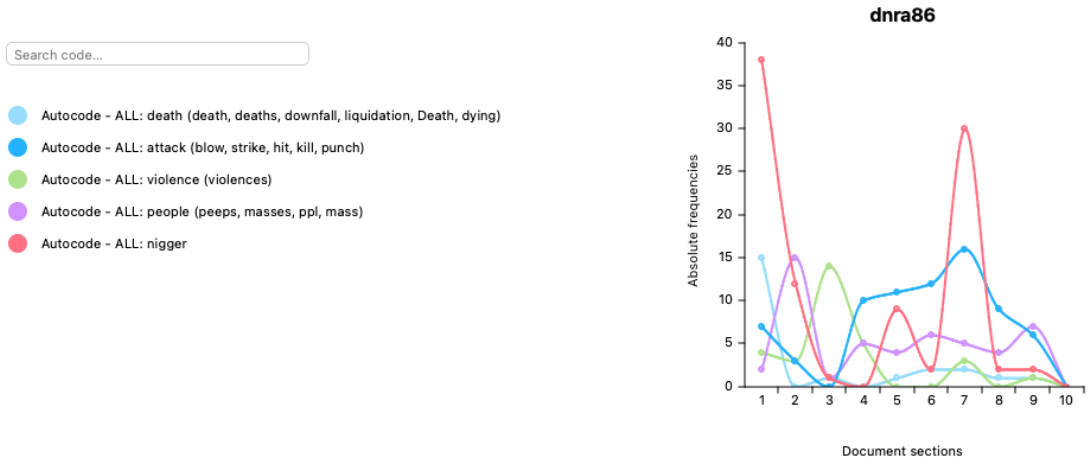
7.2.5. Napló kiválasztott szavainak előfordulási gyakorisága



10. ábra: *A napló kiválasztott szavainak előfordulási gyakorisága*. (Maxqda24)

A szógyakoriság szakaszoláson alapuló vizualizációja jól illusztrálja a radikalizáció belső narratív dinamikáját. A dokumentum elején az „emberekre" (pl. people) vonatkozó hivatkozások dominálnak, valamint a rasszista gyűlöletbeszéd (nigger) és az érzelmi túlfűtöttséget tükröző vulgaritás (fucking) sűrűsödése figyelhető meg. Ezt követően a szövegben megjelenő kulcskifejezések gyakorisága átmenetileg csökken, majd a dokumentum második felében az erőszakos cselekvésre utaló kifejezések (attack, shit, school) frekvenciája újra emelkedni kezd. E mintázat arra utal, hogy a napló nem pusztán érzelemkifejező vagy világmagyarázó szövegként funkcionál, hanem egy fokozatos tematikai eltolódást mutat: az ellenségképzés és frusztráció kezdeti artikulációja fokozatosan átadja helyét a tett-előkészítés retorikájának. Az automatikus kódoláson alapuló tartalomelemzés ilyen típusú vizualizációval történő kiegészítése nemcsak a dokumentum szerkezeti logikáját teszi feltárhatóvá, hanem a radikalizáció nyelvi előrehaladását is jól követhetővé teszi.

7.2.6. Manifesztó kiválasztott szavainak előfordulási gyakorisága



11. ábra: *A manifesztó kiválasztott szavainak előfordulási gyakorisága*. (Maxqda24)

A manifesztó szövegéhez készült vizualizáció a szélsőséges diskurzus szókészletének eloszlását mutatja tíz szakaszra bontva. A grafikon jól érzékelteti a dokumentum nyelvi intenzitásának kezdeti túlfűtöttségét**,** különösen a rasszista gyűlöletkifejezések (*nigger*) drasztikus előfordulási arányával az első szakaszban (több mint 35 előfordulás). Ez a kezdeti csúcspont arra utal, hogy a szöveg nyitó részeiben a szerző erőteljes ellenségképet konstruál, főként etnikai alapon. A további szakaszokban ez a gyűlöletretorika átmenetileg visszaszorul, de a hetedik szakaszban egy újabb jelentős kiugrás figyelhető meg, ami azt jelezheti, hogy a rasszista érvrendszer ismételten előtérbe kerül valamilyen tematikus váltás vagy érzelmi tetőpont hatására. Ezzel párhuzamosan az *attack* (kék) és *violence* (zöld) tematikájú szavak frekvenciája már a dokumentum első harmadában felerősödik, és különösen a középső szakaszokban (*4–7*) mutatnak intenzív előfordulást, majd fokozatos csökkenés figyelhető meg. Az *attack* szóhalmaz azonban a szöveg nagy részében konzisztensen jelen van, ami arra utal, hogy a manifesztó retorikája folyamatosan erőszakos keretben mozog.

Az *emberekre* (lila – *people*) való hivatkozás valamivel egyenletesebben oszlik el, de a dokumentum első felében ennek is magasabb a gyakorisága, különösen akkor, amikor a rasszista vagy erőszakos szókészlettel együtt jelenik meg. A *death*(világoskék) kategória már az első szakaszban is számottevő, de fokozatosan háttérbe szorul, és nem válik domináns tematikává a szöveg későbbi szakaszaiban.

Összességében az ábra azt mutatja, hogy a dokumentum elején nagyon magas intenzitású gyűlölet- és erőszakretorika jelenik meg, amit később a tematika váltakozása ellenére újabb kiugrások, különösen rasszista szóhasználat formájában, időről időre felerősítenek. Ez a

nyelvi dinamika jól tükrözi a radikalizált gondolkodás periodikus újra fokuszálását, ahol az érzelmi töltet és a cselekvésorientált nyelv egymást váltogatva strukturálják a manifesztó érvelését.

7.3. Összegzés

A napló és a manifesztó szóhasználatának összehasonlítása alapján jól látható, hogy bár mindkét szöveg tartalmaz gyűlöletkeltő, erőszakos és polarizáló nyelvi elemeket, ezek eltérő módon és eltérő szerkezetben jelennek meg. A naplóban a gyűlöletbeszéd, különösen a rasszista kifejezések, főként a dokumentum elején jelennek meg erőteljesen, majd idővel visszaszorulnak, és helyüket más témák – például a cselekvés, indulat, vagy a világmagyarázat – veszik át. Ezzel szemben a manifesztóban ugyanilyen kifejezések már az első soroktól dominálnak, és a szöveg előrehaladtával vissza-visszatérnek, gyakran együtt más erőszakra utaló szavakkal.

Ez a különbség arra utal, hogy a napló inkább egy gondolatmenet fokozatos építkezését követi, amelyben a düh és a frusztráció idővel más nyelvi mintázatba fordul át – például az erőszak szándékának megfogalmazásába vagy az „önigazolásba". A manifesztó ezzel szemben már egy kész, kiérlelt, végrehajtásra hangolt szöveg, amelyben a szerző nem érvel, hanem közöl, és az indulati töltet már nem csak jelen van, hanem egyértelműen cselekvéshez kapcsolódik. A két szöveg közötti különbség tehát nemcsak a tartalomban, hanem a szerkezetben és a célban is megmutatkozik: míg a napló inkább egy út, addig a manifesztó a végpont.

8. Következtetések és jövőbeli irányok

A tanulmány áttekintése megerősíti, hogy a radikalizáció napjainkban összetett, többdimenziós jelenség, amely nem írható le kizárólag ideológiai, vallási vagy társadalmi változók mentén. Az elméleti áttekintés, az online–offline dichotómia kritikája, valamint az összeesküvés-elméletek szerepének részletes vizsgálata világossá teszi, hogy a kortárs radikalizációs folyamatokat az ún. onlife tér dinamikája, a digitális ökoszisztéma sajátosságai és a kollektív identitáskeresés szükségletei együttesen alakítják.

Az elemzésben szereplő esettanulmány – Solomon Henderson naplója és manifesztója – új perspektívákat nyit a vegyes ideológiai radikalizáció megértésében. A szófelhőalapú szövegelemzés módszertana jól illusztrálja, hogyan lehet kvantitatív eszközökkel feltérképezni a szélsőséges diskurzus tematikus és érzelmi hangsúlyait, és

hogyan rajzolódnak ki ezekből a cselekvésre utaló, ideológiai vagy értékelő nyelvi mintázatok.

A jövőbeni kutatásokban célszerű lenne az automatizált szövegelemzési eljárásokat pszicholingvisztikai vagy gépi tanulási módszerekkel kombinálni, különös tekintettel az irónia, eufemizmus és mémkultúra detektálására. Emellett szükséges olyan normatív keretek kidolgozása is, amelyek biztosítják, hogy a megelőző célú szűrés nem válik öncélú megfigyeléssé, és nem sérti a polgári szabadságjogokat.

A szófelhők elemzése értékes betekintést nyújtott a Henderson által írt két dokumentum – a manifesztó és a napló – nyelvi és tematikus különbségeibe, melyek egymást kiegészítve rajzolják ki a radikalizáció komplex folyamatát. A főnevek vizsgálata egyértelműen rávilágított arra, hogy míg a napló szókészlete technikai, végrehajtás-orientált, és az erőszakos cselekmény materiális előkészítésére fókuszál, addig a manifesztó inkább az elméleti, világmagyarázó diskurzust jeleníti meg, rendszerkritikai és ideológiai fogalmak mentén. Ez a dichotómia jól leképezi a radikalizáció két dimenzióját: az ideológiai alapozást és a fizikai kivitelezést.

A melléknevek vizsgálata szintén árnyalt különbségeket tárt fel a két szöveg retorikai szerkezetében. A naplóban domináló obszcén és erősen érzelmi töltetű melléknevek az elfojtás nélküli agresszió nyelvét közvetítik, míg a manifesztóban megjelenő értékelő – gyakran dehumanizáló – melléknevek a szerző értékrendjének torzulását és az ellenségkép formálásának folyamatát mutatják be. A nyelvhasználat ezáltal nemcsak az erőszakra való hajlamot, hanem annak érzelmi és kognitív alapozását is tükrözi.

Az igék elemzése különösen jól érzékelteti a radikalizáció időbeli és pszichológiai ívét: míg a manifesztó nyelvezete a szándék, gondolat és belső érlelődés jegyeit hordozza, addig a naplóé a kivitelezés, cselekvés és fizikai beavatkozás fázisát ragadja meg.

A vizsgálat módszertani egyszerűsége ellenére (pl. automatizált szófelhő-generálás, manuális kódolás mellőzése) a kutatás fontos megállapításokat tett lehetővé a radikális szövegek tematikus és stilisztikai fejlődéséről. A szófaji bontás külön-külön történő elemzése hozzájárult a szövegek mélyebb megértéséhez, különösen a gondolat- és cselekvésvilág elkülönítésében. Bár a vizsgálat nem törekedett pszicholingvisztikai mélységű elemzésre, a szóhasználat és szófaji arányok alapján kirajzolódó tendenciák megalapozhatják egy olyan elméleti szólista kidolgozását, amely később prediktív eszközként szolgálhat a megelőző monitoring munkában. Mindez rámutat arra, hogy az ilyen típusú kvantitatív-nyelvi vizsgálatok nemcsak leíró, hanem alkalmazott relevanciával is bírnak a korai radikalizációs mintázatok felismerésében és szűrésében.

A jövőbeni kutatások szempontjából ígéretes irányt jelenthet annak vizsgálata, hogy hasonló szófelhő- és szófaji elemzések miként alkalmazhatók más, az internetre feltöltött manifesztók és naplók esetében. Számos elkövető publikált online olyan dokumentumokat, amelyek – bár eltérő ideológiai és kulturális háttérrel rendelkeznek – közös nyelvi és tematikus mintázatokat hordozhatnak. E szövegek egységes módszertannal történő feldolgozása lehetővé tenné egy olyan összehasonlító szókészleti adatbázis létrehozását, amely a radikalizáció különböző típusait nyelvhasználatuk alapján klaszterekbe rendezheti. Az így nyert szólisták egymás mellé helyezése nemcsak a szélsőséges diskurzusok közös nevezőinek feltárását szolgálhatja, hanem segítheti azokat a kutatásokat is, amelyek a radikalizálódás nyelvi előzményeinek beazonosítását célozzák. Egy ilyen longitudinális, több dokumentumon és elkövetőn átívelő összevetés hozzájárulhat ahhoz, hogy ne csupán egyéni, hanem rendszerszintű nyelvi mintázatok ismerhetők fel, amelyek a jövőben a prediktív monitoring eszközeivé válhatnak.

Fontos, és egyben sürgető kutatási kérdés marad továbbra is a multimodális tartalomelemzés fejlesztése, amely nem csupán a nyelvi, hanem a vizuális elemeket is integrálja az értelmezési folyamatba. A jelen tanulmányban vizsgált napló – hasonlóan más radikalizálódási narratívákhoz – jelentős mennyiségű képi anyagot is tartalmazott (pl. mémek, képernyőfotók, ábrák, szerkesztett képek), amelyek jelentéshordozó szerepe messze túlmutat az illusztratív funkción. Ezek gyakran a nyelvi elemeket kiegészítve vagy éppen azokkal ellentmondásban tovább árnyalják a szerző belső világát és ideológiai pozícióját, ugyanakkor még nem áll rendelkezésre olyan értékelési rendszer, amely képes lenne a képek, szimbólumok és nyelvi elemek együttes értelmezésére, így a kutatások többsége szükségszerűen redukcionista módon, kizárólag szövegalapú adatokkal dolgozik.

A radikalizációs folyamatok mélyebb megértése, valamint az ezekre épülő megelőzési és szűrőmechanizmusok hatékonyságának növelése érdekében elengedhetetlen egy multidiszciplináris kutatási megközelítés, amely egyesíti a nyelvészet, pszichológia, képelemzés, mesterséges intelligencia és biztonságpolitika eszköztárait. Az ilyen komplex szemléletmód nemcsak a tartalomelemzés pontosságát növelheti, hanem hozzájárulhat a radikalizáció korai szakaszainak felismeréséhez, ezáltal lehetőséget teremtve célzott és időben történő intervenciókra.

Ugyanakkor nem elegendő kizárólag a tudományágak közötti együttműködésben gondolkodni – a technológiai fejlődés üteme és a társadalmi adaptáció késése olyan kihívásokat eredményez, amelyek önmagukban is új értelmezési és beavatkozási kereteket követelnek. Hiszen minél fejlettebb technológiai megoldásokkal rukkolunk elő, annál több

adattal rendelkezünk, melyek másodlagos felhasználásának – elemzésének etikus, hatékony módjai nem egyszerre születnek meg az adott fejlesztéssel, melyek jellemzően elsőkörben a fogyasztói társadalomban megjelenő – vagy akár még meg sem fogalmazott – igényeket igyekeznek kihasználni. Jó példa erre a Big Data kérdése, mely az internet fejlődését tekintve jóval később lett a kutatási kérdések középpontjában, mint ahogy valójában elkezdtük legenerálni ezeket az adatokat. Ez a fajta versenyfutás az idővel ugyanakkor azt a megközelítést erősíti, melyben a társadalomtudomány oldaláról közelítve szükséges a folyamatok olyan mértékű átlátása, mely a problémát enyhítő gyakorlatokhoz vezethet. Ebben épp úgy része van az oktatásnak – mely küzd sok esetben a generációs szakadékokkal, és a neveléstudományi eszköztelenséggel, mint az egészségügynek, melyben nem csak a látható problémák kezelését kell tudnia megoldani, de a mentálhigiénés kezelést is.

FELHASZNÁLT IRODALOM

ALDERA, Saja –EMAM, Ahmad – AL-QURISHI, Muhammad – ALRUBAIAN, Majed – ALOTHAIM, Abdulrahman (2021): Online Extremism Detection in Textual Content: A Systematic Literature Review. *IEEE Access*, 9(20), 42384–96. Online: https://doi.org/10.1109/ACCESS.2021.3064178

BAKOWSKI, Piotr (2022): *Preventing radicalisation in the European Union. How EU policy has evolved*, European Parliamentary Research Service. Online: https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/739213/EPRS_IDA(2022)739213_EN.pdf

BYINGTON, Bradley (2019): Antisemitic Conspiracy Theories and Violent Extremism on the Far Right: a Public Health Approach to Counter-Radicalization, *Journal of Contemporary Antisemitism,* 2(1), 1–18.

CHRISTOPH, Stephan (2022): On Conspiracy Thinking: Conspiracist Ideology as a Modern Phenomenon. *Politics and Governance,* 10(4), 135–145.

COOLSAET, Rick (2019): *Radicalization: the origins and limits of a contested concept*. In FADIL, Nadia – KONING, de Martjin – RAGAZZI, Francesco (szerk.): *Radicalisation in Belgium and the Netherlands : critical perspectives on violence and security.* London: I.B. Tauris, 29–51.

DENAUX, Ronald – GÓMEZ-PÉREZ, Jose Manuel (2019): *Textual Analysis for Radicalisation Narratives aligned with Social Sciences Perspectives*. In: JORGE, Alípio Mário – CAMPOS, Ricardo – JATOWT, Adam – BAHTIA, Sumit (szerk.): *Proceedings of the*

Text2StoryIR'19 Workshop, Cologne, Germany. Online: http://ceur-ws.org/Vol-2342/paper5.pdf

ELCHEROTH, Guy – DRURY, John (2020): Collective Resilience in Times of Crisis: Lessons from the Literature for Socially Effective Responses to the Pandemic. *British Journal of Social Psychology,* 59(3), 703–13. Online: https://doi.org/10.1111/bjso.12403

FORD, Kieran – JACKSON, Richard (2024): *Problematising radicalisation*. In LEWIS, James R. – AWAN, Akil N. (szerk.): *Radicalisation: A Global and Comparative Perspective*. Oxford Academic.

GILL, Paul – CORNER, Emily – CONWAY, Maura – THORNTON, Amy – BLOOM, Mia – HORGAN, John (2017): Terrorist Use of the Internet by the Numbers. *Criminology & Public Policy*,16(1), 99–117. Online: https://doi.org/10.1111/1745-9133.12249

GOEL, Sanjay (2020): National Cyber Security Strategy and the Emergence of Strong Digital Borders. *Connections: The Quarterly Journal*, 19(1), 73–86.

GROVER, Ted – MARK, Gloria (2019): Detecting Potential Warning Behaviors of Ideological Radicalization in an Alt-Right Subreddit. *Thirteenth International AAAI Conference on Web and Social Media*. 193–204. Online: https://ojs.aaai.org/index.php/ICWSM/article/download/3221/3089

HADINGRAT, Wahyu – SUSENO, Sigid – GULTOM, Elisatris – HIDAYAT, Dadang Rahmat (2023): Radicalism Assessment as a Concept of Countering Radicalism through Social Media in Indonesia. *Journal of Hunan University Natural Sciences*, 50(4). https://doi.org/10.55463/issn.1674-2974.50.4.20

HERATH, Chamin – WHITTAKER, Joe (2021): Online Radicalisation: Moving Beyond a Simple Dichotomy, *Terrorism and Political Violence*, 35(5), 1027–1048. Online: https://doi.org/10.1080/09546553.2021.1998008

HOECHSMANN, Michael. – MCKEE, Miranda (2023): Truck Fudeau: Algorithms, Conspiracy and Radicalization. *Norteamérica, Revista Académica Del CISAN-UNAM*, 18(1), 355–376. Online: https://doi.org/10.22201/cisan.24487228e.2023.1.622

KKIENERM (2018): *Counter-Terrorism Module 2 Key Issues: Radicalization & Violent Extremism*. Online: https://www.unodc.org/e4j/en/terrorism/module-2/key-issues/radicalization-violent-extremism.html

KREKÓ Péter (2023*): Tömegparanoia 2.0 Összeesküvéselméletek, álhírek és dezinformáció*. Budapest: Athenaeum Kiadó.

KRUGLANSKI, Arie W. – MOLINARIO, Erica – ELLENBERG, Molly – CICCO, Di Gabriele (2022): Terrorism and Conspiracy Theories: A View from the 3N Model of

Radicalization. *Current Opinion in Psychology*, 47(101396). Online https://doi.org/10.1016/j.copsyc.2022.101396

LANE, Justin E. – MCCAFFREE, Kevin. – SHULTS, F. Leron (2021): Is radicalization reinforced by social media censorship, *arXiv: Social and Information Networks*. Online: https://dblp.uni-trier.de/rec/journals/corr/abs-2103-12842.html

MARIE, Antoine – PETERSEN, Michael Bang (2022): Political conspiracy theories as tools for mobilization and signaling. *Current Opinion in Psychology*, 48(101440). Online: https://doi.org/10.1016/j.copsyc.2022.101440

MCCURDY, Emmett (2021): Radicalizing Online: An overview of the role the internet plays in radicalization into extremism. *MacEwan University Student EJournal*, 5(1). Online: https://doi.org/10.31542/muse.v5i1.2008

MSALL, Kyle – LARY, Noor (2022): A link between radicalisation models and extremist propaganda, *Global Security Health Science and Policy*, *7*(1), 44–50. Online: https://doi.org/10.1080/23779497.2022.2103446

NOUH, Mariam – NURSE, Jason R. C. – GOLDSMITH, Michael (2019): Understanding the Radical Mind: Identifying Signals to Detect Extremist Content on Twitter, *arXiv: Social and Information Networks*. Online: https://arxiv.org/abs/1905.08067

PROOIJEN, Jan-Willem van – DOUGLAS, Karen M. (2022): Conspiracy theories as part of history: The role of societal crisis situations and group-based motivations. *British Journal of Psychology*, 113(1), 323–333. Online: https://journals.sagepub.com/doi/10.1177/1750698017701615

WANG, Emily – LUCERI, Luca – PIERRI, Francesco – FERRARA, Emilio (2022): Identifying and Characterizing Behavioral Classes of Radicalization within the QAnon Conspiracy on Twitter. Online: https://doi.org/10.48550/arXiv.2209.09339

WHITTAKER, Joe (2021): The Online Behaviors of Islamic State Terrorists in the United States. *Criminology and Public Policy*, 20(4), 177–203. Online: https://doi.org/10.1111/1745-9133.12537

WHITTAKER, Joe (2024): *Onlife Radicalisation: Understanding the Online/Offline Nexus*. Europol ECTC 4th Conference of the European Counter Terrorism Centre (ECTC) Advisory Network On Terrorism and Propaganda, 14–15 March 2023. Online: https://cronfa.swan.ac.uk/Record/cronfa66068

WOLBERS, Heather – DOWLING, Christopher – CUBITT, Timothy (2023): Understanding and preventing internet-facilitated radicalisation. *Trends & issues in crime and criminal justice*, no.673, Online: https://doi.org/10.52922/ti77024no

WOODHAMS, Katrina Marie (2016): *Connections Among Communities: Preventing Radicalization and Violent Extremism Through Social Network Analysis in the Threat and Hazard Identification and Risk Assessment (THIRA) Framework.* Online:https://www.hsdl.org/?view&did=798821

Jasenszky Nándor ny. r. ezredes

A nagy kockázatú akciók komplex végrehajtása[1]

1. ELŐSZÓ

1981-ben 25 éves koromban kezdtem meg a hivatásos szolgálatomat a BRFK Betörési Csoportjánál, rendőr alhadnagyként. Egy olyan szakterületre és szakmai közösségbe érkeztem, amely az egész további életemre meghatározó volt. A csapat legfiatalabbjaként minden típusú feladatvégrehajtásban szerencsém volt részt venni. A mostani jegyzet szakmai témája kapcsán az elfogásokkal, a fedett akciókkal és ezek „törzsfejlődésével" kapcsolatban szeretnék bevezetőül pár gondolatot megosztani.

Rendőri pályafutásom során sikerült megélni a „Rendőrség! Mindenki velem jön" korszakát – és valóban megtörtént a csoda: mindenki jött. Innen jutottunk el a tervezett, részben koreografált, többszereplős nyomozói elfogásokig, amelyben már bevetési egységekkel – bárhogy is nevezeték őket az adott időszakban – közösen terveztük meg és hajtottuk végre az akciókat. Ez utóbbi szemlélet napjainkban is meghatározó. Ezt az idővonalat nyugodtan nevezhetjük a ma használatos szakmai kifejezéssel a taktikai műveleti munka evolúciós folyamatának. A fejlődés nem áll meg: a körülmények, a kihívások változnak, ezért a rendvédelemnek és a műveleti egységeknek új eljárásokkal és válaszokkal kell reagálniuk az eredményes és biztonságos végrehajtás érdekében. Ehhez kívánok hozzájárulni azzal, hogy a nagy kockázatú akciók komplex végrehajtásával kapcsolatos tapasztalataimat a legjobb tudásom szerint rendszerezem és összefoglalom. Célom, hogy egy összegző, ellenőrzőlista-formátumú módszertani segédletet nyújtsak a taktikai és műveleti tervezéshez, valamint a végrehajtási munkához.

2. KIS EREDET- ÉS FEJLŐDÉSTÖRTÉNET

Ebben a fejezetben egy olyan területtel foglalkozunk, amely speciális tartalma, kiemelt rendvédelmi fontossága, valamint a végrehajtó állománnyal szembeni különleges elvárásokat övező „misztikuma" miatt is a szakmai és a laikus közvélemény érdeklődésének középpontjában áll.

[1] Azonos című egyetemi tantárgyi előadások támogató, módszertani jegyzete Nemzeti Közszolgálati Egyetem hallgatói számára

A szakma eredettörténetében számos példát találhatunk, hiszen már Mózes könyveiben, a középkori krónikákban, valamint az újkori hadtörténeti és hadtudományi leírásokban is megjelennek speciális műveletek. Ezek közül most a közelmúltból emelünk ki egy olyan konkrét eseményt, amely mérföldkőnek számít a szakterület fejlődésében.

Az 1970-es évek elején a nyugati demokráciák hirtelen számos terrorista szervezet támadásainak kereszttüzébe kerültek. Ezek a csoportok drasztikus módon igyekeztek érvényre juttatni szélsőséges nézeteiket, politikai céljaikat. Egyre több szervezet „helyben", Nyugat-Európában támadta a demokratikus társadalmi értékeket. A gyakran a Közel-Keletről és a kommunista Kelet-Európából szponzorált csoportok mindent megtettek annak érdekében, hogy aláaknázzák a Nyugat biztonságát. 1972 szeptemberében megmutatták a világnak, mire képesek.

A terroristák a lehető legnagyobb nyilvánosság elérése érdekében választották akciójuk színhelyéül az 1972-es müncheni olimpiát. Szeptember 5-én a Fekete Szeptember nevű palesztin terrorista csoport nyolc felfegyverzett tagja, kihasználva az olimpiai falu alacsony hatékonyságú biztonsági rendszerét, foglyul ejtett 11 izraeli sportolót. 234 terrorista társuk szabadon bocsátását követelték és a szabad eltávozást Egyiptomba. Azzal fenyegetőztek, hogy ha nem teljesítik követeléseiket, azonnal megkezdik a túszok kivégzését. A német rendőrség korábban sohasem került szembe ilyen problémával, ezért úgy döntöttek, hogy látszólag engednek a terroristák követeléseinek, és helikopterrel a repülőtérre szállítják őket. Amikor azonban megérkeztek a repülőtérre, az ott elrejtőzött mesterlövészek tüzet nyitottak, két embert megöltek, többet megsebesítettek, beleértve a helikopter pilótáját is. Az életben maradt terroristák a helikopterekben kerestek menedéket, a német csapatok pedig páncélozott járművekkel támadást intéztek ellenük. A terroristák és a csapatok között heves tűzpárbaj zajlott le, és az egyik helikopter, amelyben túszok is voltak, felrobbant. A másik helikopterben a terroristák kivégeztek még öt túszt, majd magukkal együtt azt is felrobbantották. A kimenekítési művelet teljes kudarccal végződött: tizenegy izraeli sportoló és öt terrorista vesztette életét.

A balul sikerült túszmentő akció tanulságait levonva Németország létrehozta a professzionális, antiterrorista rendőri szervezetet, a Grenzschutzgruppe–9-et, közismertebb nevén a GSG–9-et.

A müncheni incidens hatására több országban is felülvizsgálták a terrorelhárító rendőri és katonai képességeket. Bár Európa sok országában már léteztek különleges alakulatok, egyik sem volt kiképezve terrorelhárító műveletekre. München fájdalmas ébredés volt a világ több kormánya számára: a terrorizmust létező és egyre növekvő problémaként kellett kezelni.

Várható volt, hogy a következő célpontok valószínűleg olyan országokban lesznek, amelyek kevésbé készültek fel egy ilyen támadás elhárítására.

Ennek hatására világszerte sorra alakultak meg a speciális terrorelhárító egységek.

Az ad hoc reagálások ideje lejárt – egyetlen modern állam sem engedhette meg magának, hogy valamilyen formában ne gondoskodjon saját terrorizmus elleni védelméről egy erre elhivatott elhárító, beavatkozó szervezet létrehozásával.

Még számos történelmi példát hozhatnánk fel sikeres – vagy éppen kudarcba fulladt – kommandós akcióra, de jelen tanulmány célja nem egy teljes történeti áttekintés, hanem annak bemutatása, hogy a kezdetekben – a „kommandókról" szólva – elsősorban katonai egységekről beszélhettünk. Ennek oka, hogy e területen jelentek meg először azok a stratégiai (hadászati) feladatok, amelyek végrehajtásához kifejezetten egy **kisebb létszámú, speciálisan felkészített és felszerelt, gyorsan bevethető taktikai (harcászati) egységre** volt szükség. Ugyanakkor napjainkban, az új típusú fenyegetettségek korában – amelyek közül több korábban is jelen volt a társadalomban, azonban csak a globalizáció és kísérőjelenségei hatására aktivizálódtak, vagy váltak jelentős problémává – a tisztán katonai mellett megjelennek a terrorelhárítási és egyéb, rendvédelemmel kapcsolatos feladatok is. A katonai alakulatok – legyenek ezek bármennyire speciálisak – belföldi bevethetőségét általában szigorú szabályokhoz, rendkívüli körülményekhez kötik a törvényalkotók. Ezért a rendvédelem területén bekövetkező változások, a szervezett bűnözés elleni küzdelem, valamint a terrorizmus elleni fellépés előtérbe kerülése szükségesség tették a különleges rendőri alakulatok létrehozását, amelyek a rendvédelmi feladatokra jellemző taktikai és végrehajtási sajátosságokat képesek kezelni.

Hazánkban az első elhíresült túszhelyzet 1973 januárjában volt. Egy balassagyarmati határőrtiszt két tizenéves fia ellopta apja fegyvereit, és túszul ejtette a helyi leánykollégium 22 diákját. Helikoptert követeltek, hogy külföldre juthassanak. A rendőrség – mivel ekkor még saját túsztárgyalója nem volt – a balassagyarmati kórház pszichiátriai és neurológiai osztályának vezető főorvosát kérte fel, hogy közvetítsen a két túszejtő és a hatóságok között. A tárgyalások ugyan nem vezettek eredményre, de javították a túszok helyzetén, késleltették a túszejtők fenyegetéseinek beváltását, és hozzájárultak a „kifárasztásukhoz", sőt még operatív lehallgató technika rejtett bejuttatását is lehetővé tették. Végül a rendőrök – a kellő pillanatban beavatkozva – az egyik túszejtőt lelőtték, a másikat elfogták, a túszok közül senkinek sem esett bántódása.

A magyarországi rendvédelem vezetői számára is egyértelművé vált, hogy „Az ad hoc reagálások ideje lejárt", szervezeti, műveleti válaszokra van szükség.

- 1973-ban a Forradalmi Rendőri Ezred egységeként létrehozták az *„akciószakaszokat”.*
- 1987-ben létrejött a Komondor Terrorelhárító Szolgálat, amelynek feladata már kifejezetten a terrorcselekmények elleni fellépés volt.
- 1990-ben létrejött a Terrorelhárítási Önálló Osztály, közvetlenül az ORFK közbiztonsági főigazgatójának alárendeltségben. 1991-ben a Terrorelhárítási Önálló Osztályból és a Komondor Szolgálatból a Rendőrség Különleges Szolgálatának (RKSZ) létrehozásával egy hatékonyabban működő, önálló, különleges és továbbra is terrorelhárítási alapfeladatokkal felruházott egység alakult meg, amellyel egy kézbe került a rendőrség terrorelhárítási tevékenysége. 1998-ban az addig önállóan működő szolgálatot Terrorelhárító Szolgálat (TESZ) néven a Készenléti Rendőrség szervezetébe integrálták.
- A komplex műveleti munka szervezeti és tartalmi evolúciójának jelenlegi állomása a 2010-ben megalakult Terrorelhárítási Központ.

Ezen alakulatokat a rendvédelmi területen nevezik kommandónak, bevetési egységnek, gyors reagálású egységnek, különleges fegyverzetű és harceljárású csapatnak (Special Weapons and Tactics, S.W.A.T), mobil különleges osztagnak (Mobiles Einsatzkommando, MEK), taktikai egységnek, műveleti csoportnak és hasonlóknak. Az elnevezések nemzetenként változhatnak, de adott esetben egy országon belül is feltűnik több, párhuzamosan alkalmazott megnevezés. Szinte mindegyikben találhatunk külön magyarázatot érdemlő fogalmakat (bevetési, gyors reagálású, mobil, taktikai, műveleti), amelyek részletes kibontásával a későbbiek során fogunk foglalkozni. A közös jellemzőjük: **kis létszámú (15-20 fő/ csoport), gyorsan mobilizálható (állandó készültségben lévő), speciálisan kiképzett és felkészített személyi állományú, sokrétű speciális fegyverzettel és technikával ellátott taktikai egységekről van szó, amelyek rendeltetése a nagy horderejű, különleges műveleti (harci) feladatok megoldása.**

Magyarországon az 1990-es évek elején és közepén jelentősen megváltozott a bűnügyi operatív helyzet. Előtérbe kerültek az egyre erőszakosabb bűnelkövetések, a leszámolásos jellegű emberölések. Teret nyertek az idegen, főleg az orosz ajkú bűnözői csoportok. A szervezett bűnözéssel foglalkozó felderítőknél egyre több adat mutatott arra, hogy a bűnözők fegyverkeznek, és fegyvereiket használni is tervezik. A külföldi bűnelkövetők bennünket érintő csoportjait tapasztalataink szerint két fő részre lehetett osztani. Az egyik az aktuális bűnügyi konjunktúrának megfelelően választotta ki működési területét. Ezek a csoportok garázdálkodtak korábban az ún. KGST-piacokon, és ez idő tájt a főváros vonatkozásában leginkább az autópiacok környékén fejtették ki „áldásos” tevékenységüket. Elég volt egy

nagyobb értékű gépkocsi vásárlását tervezni valahol Oroszországban, és máris kiraboltak egy szállodában Magyarországon. Ebből is látszik, hogy a hálózat meglehetősen jól működött.

A másik csoport tagjai tehetős üzletemberek voltak, akik pénzek befektetésével és az ezzel kapcsolatos tranzakciók lebonyolításával foglalkoztak. Mivel tevékenységük rejtettebb volt és nagyobb haszonnal járt ezért a köztük folyó harc egyre véresebb lett. A 90-es évek fegyveres konfliktusai mögött sok esetben ilyen „tiszteletreméltó" üzletemberek álltak.

A magyar elkövetői kör meglehetősen polarizálódott. Főleg a két véglet volt megtalálható. A nagyobb csoport a hagyományos, döntően vagyon elleni bűncselekmények sorozat jellegű elkövetésével foglalkozott, egyre szervezettebb formában. A másik garnitúra azoknak a kisebb számú bűnözőknek a csoportja volt, akik döntően a '80-as évek elejétől gazdagodtak meg és pénzüket különböző vállalkozásokba fektették. Addigra jellemzően már csak a háttérből irányítottak, és a feketegazdaságban mosták tisztára a pénzüket. Természetesen itt-ott még tetten érhetőek voltak egy-egy védelmi zsarolás, nagyobb betörés tippadóiként, esetleg szervezőiként. Később aktív szerepet vállaltak a magyarországi olajbűnözésben.

A szervezett bűnözés elleni felderítések során egyre gyakrabban merült fel a fedett, illetve titkos akciók ún. műveleti támogatásának igénye. Ez magában foglalta a hang és képi dokumentálást és a műveletek biztosítását is. Esetenként még egy „egyszerű" informátori találkozót sem lehetett megfelelő előkészítés és biztosítás nélkül végrehajtani, nem beszélve az operatív kombinációk során alkalmazott elővásárlási akciókról, fedett bevetési, időszakos beépülési műveletekről. A számos külföldi, illetve az egyre jobban konspiráló hazai elkövetők felderítése, sok esetben a kilétük megállapítása is egyre több operatív intézkedést, figyelést, dokumentálást, technikai telepítést igényelt. Megváltozott az időtényező szerepe is. Sok esetben gyors, szinte azonnali megjelenésre, beavatkozásra volt szükség. A bűnözők mobilitásából fakadóan az elfogások dinamikája jelentősen átalakult. Egyre több alkalommal rövid, figyeléssel biztosított mozgásból kellett azt végrehajtani.

A felsorolt sokrétű bűnügyi felderítési szempontoknak, a kombinált komplex feladatok által támasztott szakmai igényeknek az akkori RKSZ – majd később a TESZ – nem felelt meg sem szervezetileg, sem felkészültségét tekintve. A kialakítási koncepciónak megfelelően a TESZ egy kiemelt, terror jellegű cselekmények kezelésére rendelt, döntően statikus, a területek között nehezen átmozgatható, taktikailag felszámolás centrikus egység volt. Nem könnyítette a bevethetőséget a más szolgálati (közbiztonsági) ághoz tartozó, nagyon magasra pozícionált, meglehetősen sokszintű és sokszínű parancsnoki, engedélyezési hierarchia sem.

A korszak kiemelkedő jelentőségű bűnügyi felderítő egységeként az ORFK Nemzetközi, Szervezett és Kábítószer-bűnözés Elleni Szolgálatát – a mai NNI jogelőd szervezetét – kell

megemlítenünk. Az 1990-ben alakult egység elsőként igyekezett megvalósítani egy angolszász mintát követő „közösségi”, ha úgy tetszik „szövetségi” felderítési modellt, tényleges nyomozati hatáskörrel, országos illetőséggel, a vidéki kirendeltségek bevonásával. Az „új típusú” bűnözéssel szemben egy új típusú szervezet lépett fel. Természetesen a történeti és szakmai hűséghez hozzátartozik, hogy az „új” kifejezés használata Magyarországra volt értendő, hiszen más országokban hasonló munka már korábban is folyt. Ebben a sokrétű, sok esetben nemzetközi rendőri szervekkel közösen végrehajtott munkában rengeteg új tapasztalat keletkezett a felderítéssel, a határon átnyúló műveletekkel kapcsolatosan. Ennek során fogalmazódnak meg az önálló műveleti, támogatási és biztosítási igények. Figyelemre méltó gyorsasággal, a szolgálat 1993-as átszervezése során – ahol a szervezet neve Szervezett Bűnözés Elleni Szolgálatra (SZBESZ) változott – létrehozták a Bevetési Osztályt. Ez volt az első komplex bevetési, a mai terminológia szerint részben műveleti feladatokat ellátó egység Magyarországon.

A hasonló műveleti igények szélesebb szakmai körökben való akkori megjelenését bizonyítja, hogy 1993–1994-ben, az ORFK SZBESZ Bevetési Osztály megalakulását követően sorra alakultak a részben hasonló feladatra létrehozott egységek:

- BRFK Szervezett Bűnözés Elleni Osztály bevetési egysége;
- Pest MRFK Szervezett Bűnözés Elleni Osztály bevetési egysége;
- Vám- és Pénzügyőrség bevetési egysége;
- Büntetés-végrehajtás bevetési egysége.

A feladatrendszerből kiemelendő volt az elfogások kérdése. Talán ezt volt az a terület, amelyik a legradikálisabb változásokon ment keresztül, és ez a fejlődés napjainkban is tart. A bűnözői csoportok vezetői – részben státuszszimbólumként, részben a valós fenyegetettség miatt – nagy létszámú testőrséget alkalmaztak. Egy esetleges rendőri akció végrehajtása szempontjából ez fontos momentum. Egyre kevésbé lehetett sikeres egy ad hoc, nem kellően előkészített intézkedés. Jellemző lett, hogy az ún. „egymozzanatos akciók”, például a próbavásárlások, az addigi formában szinte teljesen megszűntek. A legegyszerűbb elkövetői körök is biztonsági rendszabályokat, ellenőrzéseket, elővigyázatossági, óvatossági intézkedéseket építettek be manővereikbe.

A végrehajtási környezet „fejlődésének”, folyamatos változásának az okait a következőkben láttuk:

1) A bűnözök (és a terroristák is) fejlődtek, értékelték az ismeretségi köreikben történt lebukásokat, azok okait, és a tapasztalatok tükrében folyamatosan korszerűsítették a modus operandijukat (működésmódjukat).

2) Az eljáró *rendőri szervek* – részben objektív okok miatt – *azonos vissza-vissza térő taktikákat alkalmaztak.* Hiányzott a felkészültség mind taktikailag, mind technikailag, és sok esetben az anyagi-pénzügyi feltételek sem álltak rendelkezésre.
3) Egyes hatékony bűnüldözési módszerek lelepleződtek, mert az eredményesen végrehajtott akciók után nem minden esetben dolgoztak ki és alkalmaztak megfelelő legendát, a nyilvánosságot késedelmesen vagy egyáltalán nem, esetleg nem megfelelően tájékoztatták. A rendőrség „vásárlási akciói" hasonló okok miatt váltak széles körben ismertté. Annak ellenére, hogy a titkos felderítő munka az egyik legveszélyesebb, de ugyanakkor az egyik legeredményesebb és leghatékonyabb módszeréről van szó, a kellő szabályozottság, vagy annak következetes betartása nem érvényesült. A fedett nyomozó alkalmazásának jogszabályi keretekben való rögzítése abban az időben még hiányzott.

Az elkövetők magatartásánál és viselkedésénél a mai napig külön kell vizsgálni az agresszivitás kérdését. A cselekmények brutalitásának megállapításánál nem elégedhetünk meg azzal, hogy ezt egyfajta „külföldi módiként" fogjuk fel, és csak az ő „stílusukként" értékeljük. Tudomásul kellett venni, hogy a felfegyverzett végrehajtás mindennapjaink problémájává vált. Számos ügy tapasztalata bizonyította, hogy sokszor már az „első bűntényesek" is fegyverrel követik el cselekményeiket. Sőt, egyre több az operatív információ arra, hogy a nagyobb tűzerejű, sorozatlövő fegyverek irányába fordult az érdeklődés.

Kijelenthetjük, hogy a műveleti munka az 1990-es évek végére már önálló rendvédelmi szakterületté vált.

3. A MŰVELETI MUNKA FOGALMI ÉS TARTALMI ELEMEI

Anélkül, hogy elvesszünk a fogalmak erdejében nézzünk egy-két meghatározást Rendészettudományi Szaklexikonból:

> **Akció:** (1) A rendvédelmi szervek által szervezett tevékenység, amely különböző célok elérésére irányul, például határrendészeti, közlekedésrendészeti jogsértések megelőzése és felszámolása, valamint személyek elfogása. (2) Titkos információgyűjtés során konspirált műveletek és nyílt intézkedések kombinált végrehajtása meghatározott cél érdekében.
>
> **Bevetés-, műveletirányító:** a feladatsor operatív végrehajtását koordináló személy, aki egyszemélyi felelősséggel és parancskiadási joggal rendelkezik. A műveletirányító a műveleti feladat eredményes végrehajtásáért felelős vezetőként irányítja a

végrehajtók összehangolt tevékenységét, valamint koordinálja a részt vevő műveleti egységek feladatteljesítését és kapcsolatot tart a felkérő szerv összekötőivel.

Nagy kockázatú művelet: Olyan feladat, amelyet jelentős kockázati tényezők – mint az operatív körülmények, a célszemély előélete, várható ellenállás, helyszín adottságai vagy sok jelenlévő személy – nagymértékben nehezítenek és veszélyeztetnek.

Itt behoznék egy másik, a végrehajtók oldaláról megközelítő meghatározási lehetőséget:

Azokat a rendvédelmi vagy katonai műveleteket, beavatkozásokat, amelyek végrehajtásához speciális felkészültségű és kiképzettségű, megfelelő védőfelszereléssel ellátott és sokrétűen felfegyverzett egységre van szükség, méltán nevezhetjük nagy, vagy kiemelt kockázatú akciónak. Az egységeknek rendelkezniük kell kidolgozott és folyamatosan fejlesztett végrehajtási stratégiával és taktikával. Az eredményes és biztonságos végrehajtás érdekében nagyfokú mobilitás kell, hogy jellemeze őket bonyolult körülmények között is.

Láhatjuk az elvi azonossági pontokat, a fogalmak segítik az eligazodást az intézkedés fajták között. A továbbiakban egy kifejezetten gyakorlat specifikus megközelítést, és a komplex akció és művelet irányítás rendszerét kívánjuk bemutatni.

A művelet:

- Célirányos;
- Előre meghatározott helyen és időpontban végrehajtott;
- Nyílt és leplezett intézkedés, illetve azok sorozata.

Térben és időben meghatározott, a titkos információgyűjtés erőinek, eszközeinek és módszereinek, illetve nyílt intézkedések összehangolt alkalmazásával végrehajtott olyan tevékenység, ami a célszemélytől, célszemélyről beszerezhető releváns dolgok (információk) megszerzésére irányul.

A műveleti taktikai munka fogalmi elemei:

Speciális felkészültséget, kiképzettséget és felszereltséget igénylő, rendészeti szaktevékenység. Szervesen illeszkedik a nyílt és titkos felderítések rendszerébe. Képes kiszolgálni a felkérő szervek különleges akciókra irányuló igényeit.

Ennek során végrehajthat:

- Nyílt;
- Titkos, fedett és
- Leplezett

műveleteket.

Az előzőekben leírt fogalom próbálja körvonalazni, hogy mitől válhat egy akció nagy vagy kiemelt kockázatúvá. Ez megint a szakmai életünk olyan része lesz, ahol nem fogunk labortiszta tényállással, helyzettel, a fogalmak minden kritériumának megfelelő körülményekkel találkozni. Egy felderítő munkának szinte soha sincs statikus szakasza, dinamikusan változó, rész mozzanatokból áll össze, ezért rendre előfordulhat, hogy a folyamatban lévő művelet kockázata emelkedni fog, akár a kritikus kiemelt kockázatú magasságokba. Ezért igyekszünk a gyakorlatban értelmezhető és használható megközelítést bemutatni.

Egy művelet kiemelt kockázatú lehet:

Az akcióban résztvevők miatt:

- Védendő személyek;
- Együttműködők;
- Tanúvédelemi programba felvett személyek;
- Felderítő, fedett nyomozók.

A célszemélyek köre miatt:

Ennek meghatározásához részben rendelkezésre kell, hogy álljon a teljes, a személy vagy csoport korábbi tevékenységének felderítésére vonatkozó információ halmaz, továbbá a konkrét akció előkészítése során beszerzett, aktualizált életvezetésére, szokásaira vonatkozó adatok.

Védendő eszköz miatt:

- Operatív technika beépítése és kivonása;
- Később végrehajtandó művelet előkészítéséhez alkalmazott technikai eszközök telepítése, kivonása;

Védendő módszer miatt:

- Mintavásárlás;
- Bizalmi vásárlás;
- Álvásárlás;
- Ellenőrzött szállítás;
- Bűnszervezetbe beépülés
- Sértetti szerepkör átvállalása;

Várhatóan megjelenő anyagok, tárgyak miatt:

Biztonság technikailag veszélyes anyagok:

- Sugárzó, és egyéb veszélyes anyag;
- Robbanóanyag, robbantószer;

– Fegyver, lőszer;

Államilag védett termékek, tiltott szerek:

– Minősített irat, hamis pénz, kábítószer stb.

Kiemelt bűncselekmények – nagy a sikerhez fűzött elvárás

Egyebek (pl. külföldi helyszín stb.)

4. A MŰVELETI MUNKA, HELYE A FELDERÍTÉS RENDSZERÉBEN

4.1. AZ AKCIÓ ELŐKÉSZÍTÉSÉT BEFOLYÁSOLÓ INFORMÁCIÓ MEGSZERZÉSE.

Általánosságban:

- Operatív helyzet megismerése;
- Személyes kapcsolat a felderítést végző tiszttel;
- Értékelés;
- A konkrét feladat megfogalmazása;
- Közös elképzelés kialakítása;
- Vizsgálati szervekkel való egyeztetés;

Minden feladat meghatározásnál a legfontosabb, hogy részletesen, mindenki számára egyértelműen kerüljenek meghatározásra a feladatok, az elérendő célok.

Célok meghatározása és kockázatok elemzése:

- Célok tisztázása: Az akció előtt pontosan meg kell határozni, hogy mi az akció célja (pl. gyanúsított elfogása, túszmentés, fegyverek lefoglalása). A céloknak világosnak és elérhetőnek kell lenniük.
- Kockázatelemzés: Az egyik legfontosabb lépés a kockázatok elemzése, amely az akció lehetséges következményeire és az azokat befolyásoló tényezőkre koncentrál. Ez magában foglalja a fegyveres ellenállás, a civilek veszélyeztetése, az akció környezetében rejlő veszélyek (pl. épületek, terepviszonyok, időjárás), és a lehetséges pszichológiai hatások elemzését is.

Ezt követően a végrehajtás szempontjából dönteni kell az alábbiakról:

Célszerűség

Alkalmazhatóság

Megvalósíthatóság

Biztonság, vállalható, arányos kockázat

Mindenkinek azt javaslom, hogy ezt a betűszót (CAMB – Célszerűség, Alkalmazhatóság, Megvalósíthatóság, Biztonság) nagyon mélyen vésse be a tudatába, és

mindig emlékezzen rá, és mérlegelje bármilyen szintű, nem csak a nagy kockázatú akciók szervezése során.

4.2. AZ AKCIÓ ELŐKÉSZÍTÉSE

(itt az előkészítés általános szabályait tárgyaljuk, a taktikai művelet sajátosságaival később külön foglalkozunk)

Minden akció ügyspecifikus, de vannak közös pontok!

- Minősítés;
- Célszemély(ek) megismerése;
- Helyszín, időpont kiválasztása;
- Együttműködő kivonásához szükséges lépések;
- Fedett nyomozó kiválasztása, legenda kidolgozása;
- Titkos információgyűjtés, erő, eszköz, módszerei alkalmazásának lehetősége, azok engedélyezése;
- Szakértők bevonásához szükséges intézkedések;
- Kapcsolattartás megszervezése;
- Szükséges pénzügyi források biztosítása;
- Intézkedés kidolgozása dekonspiráció és egyéb rendkívüli esemény esetére
- Nyílt intézkedés esetén a nyílt egység vezetőjének nyilatkozata a tervvel való egyetértésről;

A célszemély megismerése:

Nagyon fontos a célszemélyi kör alapos ismerete!

- A célszemély személyisége, életrajza, kapcsolatrendszer;
- Priusz, bűnügyi előélet, korábbi bűntársak;
- Rendszabály értékelése;
- Legendaépítéshez előnyös lehet ismerni pl. a hobbiját, kedvenc focicsapatát. (A fedett nyomozónak nagy segítség lehet a közös pontok megtalálása a közös nevező kialakítása érdekében.);
- Kóros szenvedélyek (ital, kábítószer, gyógyszer);
- Anyagi gondok, erőszakosság, fegyver;
- Helye, szerepe az alvilágban;
- Van-e operatív előzménye:
    - Volt-e együttműködő, vagy célszemély;
- Tovább lehet-e/kell-e rajta lépni? Stb.

Helyszín:

Legyenek előre kidolgozott helyszín javaslatok!

- A helyszín kiválasztásának privilégiumát tartsuk meg (kivel szemben?)
- Az akció célja határozza meg a helyszínnel szemben támasztott
- követelményeket:
    - Más szempontok érvényesülnek egy megismerési találkozón, mint pl. egy realizáláskor.
- Vegyük figyelembe a különböző szempontokat:
    - Biztonsági szempontok (pl. mutatópénz, veszélyes anyag jelenléte);
    - Figyelési szempontok (pl. dokumentálás lehetősége);
    - Külső-belső biztosítást végzők szempontjai;
    - Bevetési egység szempontjai (főként realizálás esetén);
    - Milyen kaliberű a célszemély (Mc'Donalds … ötcsillagos szálloda);
        - Megközelítési és távozási útvonalak, megfelelő forgalom.

AZ ELŐKÉSZÍTÉS SORÁN ISMERJÜK MEG A HELYSZÍNT, LEHETŐLEG AZ AKCIÓ IDŐPONTJÁVAL MEGEGYEZŐ NAPSZAKBAN!

Időpont:

Legyenek előre kidolgozott időpont javaslataink!

- A helyszín kiválasztásának privilégiumát lehetőleg tartsuk meg az ellen érdekelt féllel szemben.
- A helyszínre vonatkozó javaslatunk megtartása érdekében az időpontban alkudhatunk velük.

Az időponttal szemben támasztott alapvető követelmény:

- Megfelelő látási és – esetenként – megfelelő forgalmi viszonyok.
- Megközelítési és távozási útvonalak időszaktól függő forgalma.
- Gondoljunk ismét a helyszínnél tárgyalt összetevőkre: figyelés, biztosítás, bevetés igényei.
- Kerüljük a hivatali munkarend korlátait, a szabadságos időszak miatti halasztást.
    - Bizalmi vagy álvásárlás előtt – mielőtt rábólintunk az újabb akció időpontjára – számoljunk az engedélyeztetési eljárás időigényével! (pl. ügyészi engedély).

Együttműködő kivonása:

Fedett nyomozó bemutatása a bizalmi személynek.

- Ha bizalmi személy a bemutató, tanácsos kapcsolattartójának elhallgatni előtte, hogy fedett nyomozót fog bemutatni. Célszerű a fedett nyomozót informátorként említeni.

- Másként viselkedik egy bizalmi személy egy olyasvalakivel, akiről tudja, hogy hivatásos rendőr: gyanakvóbb, nem olyan őszinte, s az is lehet, hogy jobban is fél.
- Az előzetes négyes találkozó rendszere:
    - Részt vesz a „két tartó” és a „két informátor”.
    - A bemutatást követően a legenda-egyeztetést olykor tanácsos a fedett nyomozóra és a bizalmi személyre hagyni, akik négyszemközt megbeszélik a tudnivalókat.

Legenda

„*A természetesség látszatát fenntartani a legnehezebb szerepek egyike!*”

(Oscar Wilde, 1856-1900)

Alapelvek (később részletesen):

- Biztonság – Hitelesség – Rugalmasság
- Életvezetési legenda
- Akciólegenda

Speciális esetek, figyelemmel a különleges taktikai művelet támogatta akciókra és igényekre:

- Különleges személyi igény pl. vevő fizikai megjelenése, felkészültsége, nyelvismerete, szakképzettsége.
- **Nagyon fontos körülmény tisztázni, hogy a bűnözői kör milyen személyre szóló „bemutató” adatokkal rendelkezik a bevezetendő munkatársról!**
- „Legenda” építés külsőségei, pl. ruházat, testőrség, gépkocsi.
- Különleges helyszín igény.

4.3. A KONKRÉT ELŐKÉSZÍTÉS FÁZISAI

A feladatnak megfelelő személy(ek):

- Kiválasztása;
- Felkészítése;
- Tárgyalási taktika meghatározása;
- Magatartási vonal kidolgozása;
- Felkészülés a lehetséges verziókra;

A műveleti végrehajtás előtti felkészülés:

Információgyűjtés és hírszerzés.

- A taktikai műveleti, bevetési egységek számára elengedhetetlen, hogy pontos és megbízható információval rendelkezzenek az akció előtt. Ez magában foglalja az

akció célpontjának, helyszínének, lehetséges ellenállásának és a célpont személyes szokásainak részletes ismeretét.

- Az előzetes hírszerzés segítségével az egységek képesek lesznek felmérni az akció sikerességét és azokat a váratlan helyzeteket, amelyek adódhatnak. Az információkat folyamatosan frissíteni kell, és titkos megfigyeléseket kell végezni, hogy minél többet tudjunk meg az ellenfél mozgásairól és szándékairól.

Az akció végrehajtásához megfelelő hely:

- Kiválasztása, (kültéri kamerák!);
- Feldolgozása;
- Dokumentálása;
- Elfogási akció esetén az alkalmazandó alap taktika kidolgozása.

A szükséges technikai eszközök felmérése és biztosítása:

- Dokumentálás;
- Mobilitás;
- Hírrendszer;
- Speciális eszközök pl. behatoló készlet, álcázó eszközök, személyvédő technika.

Ennek a szakasznak az egyik fő jellemzője az ún. „ötletbörze”. Lényege, hogy a legjobb megoldás kiválasztása érdekében, lehetőség szerint szélesebb körű állomány véleménye ki legyen kérve.

Az előkészítő munka rögzítése. Az írásosság és dokumentáltság.

„*A tervezett, de hivatalos dokumentumban le nem írt taktikai műveleteket* ***soha nem tervezték***.”

US SWAT alapelv

Írásban rögzíteni kell:

Operatív helyzet bemutatása és értékelése.

Az összefüggések megismerése után a célok kijelölése:

- Milyen akciót kérnek, kikkel szemben, várható magatartás, háttér adatok pl. fotó, priusz, modus stb.
- Elkövetett bűncselekményre, társakra vonatkozó adatok.
- Fegyverre, agresszivitásra, várható magatartásra utaló adatok, (pl. kutya).
- Egyéb, az akció végrehajtását befolyásoló felderítési adat.
- Az akció során együttműködő más szervek felsorolása, konkrét feladataik, a parancsnokok kijelölése:
    - A konkrét feladat meghatározása.

– Az előkészítés során tett konkrét intézkedések felsorolása, a végrehajtó személy megjelölése.

Mellékelni kell a:

– Térképeket;
– Helyszínrajzokat, vázlatokat;
– Fotó- és videofelvételeket.

Az előkészítés adatai alapján a végrehajtásról akció vagy műveleti tervet kell készíteni. A tervben foglaltakat minden esetben a meghatározott, illetve kijelölt parancsnokkal engedélyeztetni kell.

A műveleti terv tartalma:

– Rövid operatív helyzetismertető;
– A konkrét feladat, az elérendő cél;
– Az előkészítés során beszerzett adatok, végrehajtott intézkedések;
– A művelet jellegének, típusának meghatározása;
– A végrehajtás ütemezése, lehetőség szerint rész-felelősi, személy szerinti lebontásban, külön figyelemmel az alkalmazott taktikára és a várható fegyverhasználatra;
– A parancsnok(ok) kijelölése, veszteség esetére a parancsnokolási sorrend meghatározása;
– Az együttműködők és támogatók, szerepük, feladataik.

Technikai tartalom (terven belül):

– Fegyverzet, lőszer;
– Ruházat, felszerelés;
– Akció, fedett jármű, fedett jelzőhely, speciális páncélozott szállító járművek;
– Különleges felszerelések, drónok, fotó és dokumentáló eszközök;
– Egészségügyi támogatás, saját MEDIC egység, ügyeletes kórház, mentők;
– Szükség szerint az akció esetleges elhúzódása esetén, élelmezés, váltás, pihentetés;
– Hírrendszer: -típus, -csatorna, -kódolás, -bejelentkezési sorrend, -hívójelek, -telefon kommunikáció;
– Kivonulás;
– Bevonulás.

Eligazítás:

„*A műveleti terv kidolgozásának és a műveleti tájékoztató megtartásának elmulasztása nem menthető, kivéve, ha a helyzet*

kényszere ezt nem teszi lehetővé. Például ***»fokozatos bevetési« helyzetek*** *(barikád vagy túszhelyzet)*."

US SWAT alapelv

Vezeti az akcióért felelős parancsnok.

Célszerű lehet felbontani:

- Előkészítés;
- Taktikai rész;

Ezeket a részeket az azt végrehajtó vagy azért felelősvezető adhatja elő.

Lehetőség szerint résztvevő:

- Teljes résztvevői állomány;
- Együttműködők vezetői;
- Vizsgálati szerv képviselője;

A lebonyolítás illeszkedik a tervben meghatározottakhoz.

- Bemutatásra kerülnek a rendelkezésre álló fotó és videó anyagok.
- Részletes feladat meghatározás és visszakérdezés történik.
- Ismertetik az operatív helyzetben bekövetkezett esetleges változásokat (pl. szoros lehallgatási anyag alapján).

Meghatározásra kerül a:

- Készenléti idő;
- Megindulási idő;
- Helyszíni készenléti idő;

Fel kell hívnunk a figyelmet arra, hogy a több résztvevős lebonyolítás külön kihívásokat állít a műveletet szervező parancsnok elé. Ez leginkább a tervezésben, előkészítésben továbbá a végrehajtás során pl. a döntési pontok elhatárolásában jelentkezik. Mikor dönthet, illetve kell döntenie a felderítésért felelős jelenlévő vezetőnek, a figyelők vezetőjének, a taktikai parancsnoknak? Ezek nagyon lényeges, előre tisztázandó döntéseket igényelnek a hibátlan döntés láncolat kialakítása érdekében.

4.4. A VÉGREHAJTÁS DOKUMENTÁLÁSA

„A végrehajtott, de nem dokumentált taktikai műveletek ***soha nem történtek meg***.”

US SWAT alapelv

Végrehajtási jelentés tartalmazza:

- Pontosan időrendi sorrendben az összes mozzanatot a végrehajtó személyek pontos megjelölésével.
- Külön ki kell térni a tervtől való eltérésekre és azok okára.
- Rendkívüli helyzetek és események és az azt követő intézkedések.
- Az elfogott személyek adatai, átadás helye, ideje, körülményei, esetleges sérülések, (minden esetben célszerű videófelvételt készíteni az elfogott személy állapotáról).
- A helyszíni intézkedést átvevő neve, rendfokozata és beosztása.

Videó dokumentálás:

- Célszerűsége, szükségessége, (értékelés, fegyverhasználat, elbírálás, panasz elbírálás elfogott személy állapota stb.);
- A rögzítést végző felkészítése;
- Lehetőség szerinti több kamera alkalmazása;
- Videótár kialakítása, hozzárendelése az akció dokumentumokhoz.

Értékelés:

Mottó: „*Ki, hogy élte meg az akciót a saját helyén*.”

- Lehetőleg 3 napon belül;
- Név, rendfokozat, beosztásra való tekintet nélküli megbeszélés az egyenjogúság alapján.

Felhasználandók:

- Írott anyagok;
- Előkészítő anyagok;
- Videofelvételek;
- Végrehajtási jelentés;
- Tapasztalati adatok;

A feltárt hiányosságokkal szembeni azonnali intézkedések kidolgozása és meghozatala, célirányos ráképzések szükség szerinti végrehajtása.

4.5. SPECIÁLIS MŰVELETI FELADAT VÉGREHAJTÁSOK

4.5.1. Találkozók

Befolyásoló körülmények:

- Konkrét cél;
- Kik között zajlik;
- Környezet felmérése, kültéri kamerák!
- Előkészített vagy spontán a hely;
- Hely hangulata, jellege az ennek megfelelő külsőségek;
- Hell-e a védelem, beavatkozó távolság, megindulás lehetőségei;
- Lesz-e belőle figyelés, megismerés;
- Személyvédő technika szükségessége;
- Dokumentálás, képi-, hangrögzítés;
- Felállás, hírrendszer, jelző;

Saját kapcsolattartó és kapcsolata közötti találkozó során, főleg külföldön vagy bűnügyileg erősen ellenséges környezetben célszerű:

- Csak előre szervezett és (speciális biztosítók által) biztosított találkozót lehet tartani.
- Vezető tiszt megfelelő önellenőrzés után érkezik az előkészített és biztosított találkozási helyre.
- A személyes kapcsolatfelvétel előtt jelzést kap a biztosítóktól, hogy a partner tiszta és kontaktálhatnak.
- Az operatív kapcsolat meghatározott útvonalon közelítheti csak meg a találkozási helyet. Az ezen lévő ellenőrzési pontokon a biztosítók megállapítják, hogy nincs-e vele (ellenséges) figyelés.
- A biztosítók jelzik az operatív tisztnek, hogy találkozhat-e vagy sem.
- A találkozás befejeztével szintén meghatározott útvonalakon hagyják el a helyszínt.
- Ezeken az útvonalakon a biztosítást végzők ellenőriznek, illetve szükség szerint bizonyos leplezett beavatkozásokat végezhetnek pl. leszakítás, kizárás stb.

4.5.2. Figyelés

- Céljából fakadó térbeli és időbeli felmérés, tervezés.
- Szükséges erő és eszköz biztosítása.
- Megismerők:
    - Helyszín;
    - Célszemélyek.

- Felkészülés az esetleges kapcsolatokra, szétválás esetén brigád megosztás, rádiókon csatornaváltás.
- Belsőzések, több fővel, forgószínpadszerűen.
- Megállapított címek azonnali pontosítása gépkocsi rendszámok ellenőrzése.

A felmerült személyeket minden esetben (fotó, video) dokumentálni kell.

- Folyamatos dokumentáció a későbbi célszemély azonosításhoz, szükség szerint online.
- Objektum felderítések (helyszínrajzok), fedett jelzőhely, beépülések.
- Figyelni a lehetséges távozási útvonalakat. Nem gépkocsit, célszemélyt figyelni!
- Csomagok és táskák kiemelt szerepe a figyelések során leírásuk, színük, méretük, alakjuk.

4.5.3. „Vevő" bevezetése, tárgyalási felkészülés

- Felderítés felmérése, értékelése, időszerűség.
- Az elérendő cél érdekében megtettünk-e már mindent.
- A megfelelő figura megépítése:
    - Se sok;
    - Se kevés.
- Esetlegesen közbeeső fokozat beépítése pl. „testőr" tárgyal.
- Az arra alkalmas személy kiválasztása és speciális felkészítése.
- Megfelelő tárgyalási taktika kidolgozása a vásárlási magatartás felépítése:
    - Próba;
    - Bizalmi;
        - Álvásárlás.

Meg- illetve berendelések feltételei, tárgyalással történő felkészülés a realizálásra, hely felkínálás, elfogadás sajátosságai. Ún. „pénzvillantás" helye és szerepe.

4.5.4. Egyéb speciális akció feladatok

- Leplezett meghallgatás.
- Speciális megismerése célszemélyeknek és fedett nyomozóknak.
- Leplezett műszaki szemle, operatív technika telepítés, titkos kutatás biztosítás.

4.5.5. Elfogási akciók

Értékelni kell az elfogás jellegét, típusát, helyét a felderítésben:

- Előzmény;
- Legenda alkalmazás szükségessége;

– Biztonsági rendszabályok, állomány fizikai védelmének, anonimitásának biztosítása abban az esetben, ha rendszeresített speciális védő ruházat és felszerelés nem vehető igénybe (civil ruhás művelet).

Külön figyelmet érdemel a műveleti egység, továbbá a folytatandó nyílt büntetőeljárás szempontjából a kérdéskör előzetes tisztázása:

– Hogyan kerültünk oda?
– Hogyan lesz adminisztrálva az eljárásban? (egyeztetve az ügygazdával és a vizsgálati szervekkel)
– A legenda összeillik-e a speciális felszereléssel?

Tapasztalataink szerint egy nyílt környezetben, speciális bevetési felszerelésben végrehajtott akció „megmagyarázására" gondot kell fordítani főleg akkor, ha csak operatív előzménye van, pl. egy vásárlási akció. A humán együttműködők biztonsága kiemelt prioritást kell, hogy kapjon. Megfelelő legenda kell arra, hogy egy speciális rendvédelmi alakulat, hogy került oda és hajtott végre műveletet a célszemélyekkel.

Konkrét feladatok:

– Megfelelő helyszín választása vagy az adott hely feldolgozása.

4.6. ELŐRE FELDOLGOZOTT AKCIÓHELYEK NYILVÁNTARTÁSA ÉS ENNEK SZÜKSÉGESSÉGE.

A tapasztalataink azt mutatják, hogy vannak típusos helyek, ahol nagyobb számban kerülhet sor műveleti végrehajtásra bármelyik eddig felsorolt feladatkörben. Ilyenek pl. a repülőterek, pályaudvarok és azok kiszolgáló környezetei, bevásárló központok, plázák, kiemelt, magas besorolású szállodák, kiemelt közparkok, ligetek stb. Ezeknek a helyeknek az objektumszerű feldolgozása, kifejezetten egy jövőbeni akció lebonyolítása szempontjából, nagyon ajánlott.

Kellően feldolgozott, dokumentált, megfelelő minősítés után objektum dossziéba rendezett anyag – kellő időszakos frissítéssel – nagy segítséget tud nyújtani, amennyiben gyorsan, rögtönözve kell akció helyszínt ajánlanunk.

– Az ügynek és a körülményeknek megfelelő taktika kidolgozása.
– A jelzés-rendszer kidolgozása.
– A vevőt lehetőleg ebből már ki kell vonni, de esetenként, ha más mód nincs, akkor még meg kell győződni az áru ottlétéről.
– Lehetőség szerint a másik fél figyelésének megszervezése legkésőbb aznaptól, (pl. érkező létszám).

- Külső biztosításba a figyelők bevonása.
- Hírrendszer:
    - Figyelőkkel;
    - Jelző, dokumentáló hellyel;
    - Személyvédő hallgatása;
    - Akció végrehajtókkal;
    - Egyéb támogatókkal;
    - Esetleg bázissal;
    - Dokumentálás, fotó, videó, hang;
- Egyéb támogató erők:
    - Bűnügyi helyszínelést, házkutatást végzők;
    - Tűzszerészek;
    - Külső egészségügyi támogatók (pl. OMSZ);
    - Szakértők, szaktanácsadók. (pl. CBRN);

Az akció befejezése után törekedni kell a helyszín mielőbbi elhagyására. Biztosítani kell a további mobilitást. Az egységnek képesnek kell lenni arra, hogy a helyzetnek megfelelően ismételt szakmai feladatokat hajtson végre.

A műveleti egységet nyílt rendőri intézkedésben - házkutatások előtti biztonsági átvizsgálás kivételével (spec. felszerelésben, maszkban) - lehetőség szerint alkalmazni nem szabad konspirációs okokból.

Többféle vezetői modellt is tárgyal a külföldi és hazai szakirodalom is. A skála elég széles a döntően angolszász fúziós központoktól kezdve az országosan működtetett műveletirányítási központokon (TEK, ORFK) át a klasszikus kis bevetési csoport irányításáig. Egy olyan modellt szeretnénk bemutatni, amely tartalmi elemeit tekintve alkalmas széleskörű, alacsony és magasszintű műveleti integrációra.

4.7. VEZETŐI MUNKA A KOMPLEX AKCIÓ IRÁNYÍTÁSBAN

„Száz emberből tíznek nem is kellene ott lennie, nyolcvan csak célpont, kilencen vannak az igazi harcosok, és szerencsések vagyunk, hogy ők vannak, mert ők vívják a csatát. Ám az Egy, az Egy harcos, és ő majd visszahozza a többieket.”

DiFusco – Chaves – Caristi: Tracers

4.7.1. Az akció parancsnoka – a művelet irányítója

A művelet középpontjában helyezkedik el, ami nem feltétlen azonos a műveletirányítási központtal. Egy nagy léptékű, több helyszínes feladatvégrehajtás során az egész műveletért felelős parancsnok és a helyszíni parancsnok személye elválik. Az alább felsorolt ismérvek a helyszíni parancsnok munkájára fokuszálnak.

- Ismeri a titkos információgyűjtés előzményeit (honnan származik az alapinformáció, mennyire megbízható a forrás stb.).
- Tanulmányozza a dossziét (célszemélyek, árak, kapcsolatok, módszerek, helyszínek, veszélyforrások stb.).
- Tisztában van az általános operatív helyzettel, a szakvonalra jellemző új trendekkel, fejleményekkel.
- Személyesen konzultál a fontosabb résztvevőkkel (figyelés, bevetés, nyílt erő, tartó, vezetőtiszt, ügyész stb.).
- Kidolgozza és elkészíti az akció tervét (az ügygazda véleményét, valamint a többi résztvevő sajátos szempontjait figyelembe véve és mindvégig szem előtt tartva!).
- Engedélyezteti a tervet az arra jogosult(tal)akkal (és válaszol az esetleg felmerülő kérdésekre).
- Részt vesz az akciót közvetlenül megelőző eligazításon, ellenőrzi a feltételek meglétét.
- A helyszínen, vagy annak közelében tartózkodik az akció alatt (műveletirányító kisbusz, bázislakás – vezetési pont).
- MINDIG ELÉRHETŐ!
- Folyamatos kapcsolatban van a résztvevőkkel, illetve azok parancsnokaival, vezetőivel.
- Ő az, aki a helyszínen eldönti, hogy a konkrét operatív helyzet ismeretében mekkora eltérés engedélyezhető a tervhez képest.
- Csak akkor „zaklatja” a főnökét, ha szükséges!

4.7.2. Lehetőleg ki ne legyen a helyszínen parancsnok?

- Nyílt támogató, bűnügyi vagy közrendvédelmi erő képviselője.
- Figyelést koordináló parancsnok.
- A bevetési egységet irányító parancsnok, kivétel a kizárólagos taktikai művelet vagy mozzanat végrehajtásakor.
- A fedett nyomozó vezetőtisztje.
- Az együttműködő tartója.

– Osztályvezetőnél magasabb beosztású vezető.

4.7.3. Milyen a jó akcióparancsnok?

a) Szakmailag felkészült (Btk., Be., Rtv., belső utasítások, stb.).
b) Döntésképes, és mer is dönteni, felelősséget vállalni.
c) Tudja, hol vannak a kompetenciája határai.
d) Tisztában van a résztvevők képességeivel és korlátaival.
e) Rendelkezik a figyelem megosztásának képességével.
f) Felvállal szakmai és emberi konfliktusokat, és azokat kezelni is tudja.
g) Higgadtság, kiegyensúlyozottság, empátia.
h) Átfogóan, stratégiailag látja a történteket, nem ragad le egy-egy momentumnál.
i) Kiváló szakmai és emberi kapcsolatokkal rendelkezik szervezeten belül és kívül!
j) Nem sajnálja az időt ezen kapcsolatok „karbantartására”.
k) Elfogultságtól mentes, valamennyi résztvevő szakterülettel szemben objektív és egyforma távolságot tart. (nagyon-nagyon nehéz…)
l) Jól tudja eladni a csapatot „felfelé és kifelé”, vagyis jó menedzser…

Persze a sor még folytatható, árnyalható. Természetesen érhet az a vád, hogy ez egy szubjektív felsorolás, de ezt én vállalom. Eddigi szakmai életem során, a megszerzett tapasztalatok alapján alakult ki ez a véleményem.

4.8. TENNIVALÓK AZ AKCIÓ BEFEJEZÉSÉT KÖVETŐEN

Értékelés:

– Lehetőleg az érdemi résztvevők társaságában (névre, rangra, beosztásra tekintet nélkül).
– Mennyire sikerült a tervben lefektetett célokat elérnünk?
– Mit csináltunk jól, és mit rosszul? Hol hibáztunk?
– Milyen típusú hibák voltak?
– Miért hibáztunk, hogyan lehetett volna elkerülni?
– Milyen volt a résztvevők közötti kommunikáció?
– Ki (avagy mi) volt a leggyengébb láncszem?
– NEM A FELELŐSÖK KERESÉSÉRŐL VAN SZÓ!
– Tanuljunk az esetleg elkövetett hibákból!

5. AZ AKCIÓK GYAKORLATI KOMPLEX VÉGREHAJTÁSA

Egy nagykockázatú műveleteket végrehajtó egységnek az általa folytatott operatív akciókat az alábbi szempontok alapján célszerű szerveznie:

1./ Operatív helyzet bemutatása és értékelése. Az összefüggések után a célok kijelölése:

a) Milyen akciót kérnek, kikkel szemben, a célszemélyek várható magatartása, (háttér adatok, modus, fotó, priusz).
b) Elkövetett bűncselekmény, társakra vonatkozó adatok.
c) Fegyverre, agresszivitásra utaló adatok.
d) Egyéb, az akciót befolyásolható felderítési adat.
e) Az akció során együttműködő más szervek felsorolása, konkrét feladataik, parancsnokok kijelölése.

2./ Feladat:

A felderítésen belül a konkrét, akciót végrehajtók részére meghatározott feladat megfogalmazása.

3./ Előkészítés:

A műveleti egység által elvégzendő előkészítő feladatok. Részletesen személyre lebontva. Ebben benne foglaltatik a helyszín feldolgozása, fotó, videó dokumentálása, megrajzolása, különböző verziók kidolgozása az alkalmazott taktikai elemek kiválasztása.

4./ Végrehajtás:

a) Átfogó vázlata az egész műveletnek, (részletek nélkül);
b) Több egység esetén a feladatok egységenként, a kivonulás rendje;
c) A feladatok személyre lebontva;
d) Parancsnokolás, veszteség esetén parancsnoki sorrend;
e) Elfogott személyek elszállítása, helyszínbiztosítás, együttműködők, támogatók szerepe;
f) Bevonulás rendje;

5./ Személyi, technikai feltételek, hírrendszer:

1. Fegyverzet, lőszerek;
2. Ruházat, felszerelés;
3. Akció- és szállítójárművek;
4. Különleges felszerelések;

5. Egészségügyi ellátás, ügyeletes kórház;
6. Mentő személyzet biztosítása;
7. Élelmezés, szünetek, váltás;
8. Rádiók
   8.1. Típus;
   8.2. Csatorna;
   8.3. Kódolás;
   8.4. Bejelentkezési sorrend;
   8.5. Hívójelek;
   8.6. Forgalmazási fegyelem;
9. Telefonkommunikáció.

Az eligazításokon kerüljön meghatározásra az akció adminisztrálásáért felelős operatív tiszt. A keletkezett anyagokat akciónként elkülönítve, önálló anyagként kezeljük, minősített iktatású vonaldossziéban.

6. ÉRTÉKELŐ JELENTÉSEK – MŰVELETI STATISZTIKA (LEHET ÉVES VAGY RÉSZIDŐS)

Az eredményesség fontos záloga az írásosság és a statisztika. A tevékenység időszakos értékelése nélkül magunkat fosztanánk meg a fejlődés lehetőségétől. Egy-egy tárgyidőszak értékelése elemzés mutathat rá olyan hibákra, eseményekre, rendszer szintű hiányosságokra, amiket enélkül az elszigetelt végrehajtásokból nem észlelnénk. A plasztikus bemutatás, és az értékelés fontos eleme az objektív és részletes műveleti statisztika!

6.1. AZ ÉRTÉKELŐ JELENTÉS AJÁNLOTT FELÉPÍTÉSE

A bevezetésben a szervezet és azon belül az egység feladat rendszerének rövid ismertetése.

Az operatív helyzet, – feladatellátásunkat befolyásoló – értékelése.

Az operatív helyzet:

- Politikai, társadalmi helyzetkép, amennyiben szükséges.
- A terror- és bűnügyi helyzet változásai.
- Új jelenségek, ezek milyen változásokat jelentenek számunkra.
- A változások értékelése, akár bűncselekmény csoportok szerint.
- Az elkövetési magatartások, a bűnözői aktivitás esetleges változásai, mint az akciókat befolyásoló jelenségek.

Feltételek – személyi:

Létszám:

- Szervezet;
- Fizetés (összevetve országosan);
- Pótlékok rendszere;

Erkölcsi, fegyelmi helyzet:

- Jutalmazások, elismerések;
- Fenyítések, elmarasztalások;

Kiképzés:

- Tervezett, végrehajtott;
- Speciális igények, belföld, külföld;
- Akár személyre, szakterületekre bontva;

Feltételek – tárgyi (technikai ellátottság):

Elhelyezés:

- Gépkocsi ellátottság, több funkciós járműpark;
- Hírrendszer, -bázis, -jármű, -személyi (nyílt, álcázott, rejtett);
- Fotó és videó dokumentálás (nyílt, rejtett);

Titkos operációk speciális feltételrendszere:

- Védelmi és lehallgató technika;
- Követő technika;
- Fedő okmányolás;
- Kiegészítő rejtő és fedő és álcázó eszközök;
- Álruhatár;

Fegyverzet, kiegészítő speciális felszerelések:

- Fegyverzeti ellátottság, funkció és típus ismertetés;
- Lőszerek, mennyiségi igény (művelet + képzés), ellátottság;
- Egyéb kiegészítő speciális felszerelések.

6.2. A KONKRÉT MUNKA ÉRTÉKELÉSE – MŰVELETI STATISZTIKA

1. Műveletek – a megrendelő szervek szerint, hogy lehessen elemezni, és legyen látható trend. Következtetések levonása, ha vannak:
   1.1. Bázis év választás;
   1.2. Több éves adatsorok;
   1.3. Db + kik által;

1.4. Összes végrehajtásra eső kérők, megrendelők aránya % bontásban, (táblázat + grafikus ábrázolás).

2. Műveletek – bűncselekmények szerinti megoszlása.
   2.1. A műveletek jellege szerint:
      2.1.1. Elfogási akció;
      2.1.2. Figyelés;
      2.1.3. Figyelés + elfogás;
      2.1.4. Találkozó biztosítás + figyelés;
      2.1.5. Találkozó biztosítás + testőrrel;
      2.1.6. Találkozó biztosítás + testőr + figyelés;
      2.1.7. Személyvédelem, vezető munkatárs biztosítása;
      2.1.8. Tanúvédelmi biztosítás;
      2.1.9. Vásárlási akció, esetleg testőrrel;
      2.1.10. Objektum felderítés;
      2.1.11. Álvásárlás + elfogás;
      2.1.12. Leplezett meghallgatás biztosítás;
      2.1.13. Operatív technika telepítés, biztosítás;
      2.1.14. Szállítmány, személy biztosítás;
      2.1.15. Titkos kutatás, biztosítás;
      2.1.16. Határon átnyúló vagy külföldön végrehajtott művelet ... stb.;
3. Elfogott személyek száma, nemzetiségi megoszlása;
4. Területi megoszlás: főváros, nagyváros, város, egyéb települések, külföld;
5. Műveletek eredményessége, az esetleges eredménytelenség vizsgálata;
6. Dokumentációk száma.

6.3. MŰVELETEKTŐL „FÜGGETLEN” TEVÉKENYSÉG

- Akció helyek előkészítése, feldolgozása;
- Érdemleges operatív információk pl.: saját humán forrásból, vagy egyéb forrású, hírértékű információ átadása, ha volt ilyen;
- Szakirányítási tevékenység, ha van;

Társszervekkel végzett együttműködés, konzultációk, közös képzések, tárgyidőszaki értékelések, javító intézkedésekre javaslatok.

Összegzés – Javaslatok – Tervek (rövid, közép és hosszú távú).

7. KÉPZÉSEK – KIKÉPZÉSEK – GYAKORLATOK – BELSŐ ÉS NEMZETKÖZI EGYÜTTMŰKÖDÉSEK

Természetesen ennek az anyagnak nem feladata, hogy egy teljesen komplex tematika összeállítására vállalkozzon, ez az ezzel a területtel foglalkozó szakemberek dolga. Fontosnak ítélem azonban, hogy bizonyos szempontokra, rendező elvekre felhívjam a figyelmet. A tárgyalt bevetési, műveleti munkára való alkalmasság, mentális, fizikai, szakma tapasztalati, csapatban dolgozni tudó képességek bázisán nyugszik. Természetesen a képet tovább lehet és kell is árnyalni. A kompetenciák vizsgálatának kiemelt szerepe van.

A hazai és nemzetközi tapasztalatok azt mutatják, hogy a műveleti munka leghasználhatóbb derékhada a 35–45 éves korosztály. A külföldön végzett kutatások egyértelműen támasztják alá ezt a megállapítást. Fizikailag tökéletes állapotban vannak, mentálisan kiegyensúlyozottak, a fiatalabb korosztályokra esetenként jellemző meggondolatlan feladatvégrehajtás már letisztult. Kellő tapasztalat halmozódott már fel, megalapozott döntések születnek. Nagyon fontos ezért, hogy a korosztályok, generációk megfelelő arányban jelenjenek meg az egységekben vagy az eseti jelleggel összeállított bevetési csoportokban. Itt külön felhívom a figyelmet a generációs különbözőségekből fakadó képzési problémákra. Tudomásul kell venni, – ezt parancsnoki és egyetemi oktatói munkám egyértelműen visszaigazolta –, hogy sok esetben a vezetők, a kiképzést összeállítók és az ezt tartók között előfordul, hogy több generációs távolság van. Javaslom, hogy aki ilyen feladatok előtt áll, kicsit mélyedjen el a generációkutatás anyagaiban. Saját gyakorlatból tudom, hogy napjainkban azonos témáról mennyire más felépítésű, tartalmú, dinamikájú előadásra, prezentációra esetleg gyakorlati bemutatóra van szükség, a középiskolai végzősök, az egyetemi nappalis hallgatók, sőt az egyetemi levelezős hallgatók csoportjainál. Erre tudatosan készülni nem csak a képzés, hanem a parancsnoki munka területén is szükséges.

A csapat vezetési, parancsnoki munka kapcsán néhány szakma specifikus gondolatot szeretnék beidézni és megosztani:

- Ismerd a szakmai környezetedet, a szervezetet, amelybe integrálódsz. Ez fogja főleg befolyásolni a végrehajtandó szakmai feladataidat.
- Mélyrehatóan ismerd a munkatársaidat, tudd a képességeiket, mentális és fizikai állapotukat, esetleges szakmai vagy magánéleti problémájukat. Ezek mind meghatározói a napi, aktuális terhelhetőségnek, feladat végrehajtásnak.
- Sport hasonlattal élve, ha edzésen edzősködsz, akkor a meccs napján meg kell adnod a játékszabályokat.

- Vezetőként a Te felelősséged, hogy ismerd a vonatkozó eljárásjogi környezetet, az alkalmazott gyakorlatokat, a műveleti közösség normáit.
- Felelős vagy azért, hogy tudd képviselni a vezetés felé a legjobb tudásod szerint kialakított norma rendszert, legyél meggyőző abban, hogy a csapatodnak ez a követendő út.
- A Te felelősséged, hogy meghatározd csapatod képzési igényeit, és a Te válladon nyugszik, hogy felkészítsd csapatodat azokra a küldetésekre, amelyeket a vezetés elvár, és amire a csapatnak képesnek kell lennie.
- Az nemzetközi egységek iránymutatásai és bevált gyakorlatai szerint egy részmunkaidős csapatnak is legalább havi 16 órát kell edzenie.
- Azok a csapatok, amelyek csak házon belüli képzéseket tartanak, a rossz taktikák beltenyésztését kockáztatják.
- Csak annyira vagy jó, mint az utolsó bevetésed.
- Vedd fel a kapcsolatot más csapatokkal, és derítsd ki, mit és miért csinálnak.
- Ahhoz, hogy meghatározhasd a csapat képzési igényeit, néhány változót kell megvizsgálnod:
    - Működési terhelés, akció sűrűség.
    - A végrehajtandó feladatok típusos, fajta szerinti megoszlása.
    - A rendelkezésedre álló technikai, fegyverzeti eszköz állomány, felszerelések, járművek.
    - Vezetői, felsőbb elvárások. A reálisan megvalósítható műveleti, taktikai eljárási lehetőségeid.

A csapatod sikere és biztonsága szempontjából létkérdés, hogy tudd a megfelelő kiképzési időt és feltételeket, eszközöket, fogyóeszközöket, lőszereket stb. biztosítani! Ennek hiányában a nagy kockázatú akciós igénybevétel, minimum gondatlan veszélyeztetés!

A kapcsolattartás a tapasztalatcsere fontosságát erősíti, hogy bizonyos végrehajtási eljárásokat, taktikai elemeket célszerű lenne egységesíteni, figyelemmel egy jövőbeni esetleges közös feladat teljesítések lehetőségére. Nagyon nem mindegy, hogy egy elfogás végrehajtása során a résztvevők azonos taktikán vannak-e és mindenki tudja, hogy a másik merről, mit fog csinálni. Rossz emlékeim között tartom számon a nyári balatoni vezényléses biztosítások alkalmával a három megyéből vezényelt kollégák menetből háromféle módon tettek kísérletet a bilincselésre.

Ennek a szakmai logikának alátámasztása érdekében szeretném bemutatni az ATLAS Hálózatot – Az Európai Rendvédelmi Különleges Egységek Együttműködését.

Az **ATLAS Network** 2001-ben alakult az Európai Unió tagállamainak különleges rendvédelmi egységei között, azzal a céllal, hogy javítsa a tagországok közötti együttműködést a terrorizmus és a súlyos bűncselekmények elleni fellépésben. 2008-tól az Europol koordinálásával működik. Tagjai az EU tagállamai, valamint több társult ország, például Norvégia, Svájc és Izland.

Fő célkitűzései

- Tapasztalatcsere a különleges műveleti egységek között.
- Közös szakkiképzések és műveleti eljárások egységesítése.
- Reagálási képesség javítása határokon átnyúló helyzetekben.
- Gyors támogatás biztosítása más ország egysége számára szükség esetén.
- Innováció és felszerelés fejlesztésének összehangolása.

Közös szakkiképzések

Az ATLAS rendszeresen szervez szakkiképzéseket különféle tematikákban, például:

- Túszmentés;
- Tömeges terrorcselekmények elhárítása;
- Repülőtéri és légi járművel kapcsolatos műveletek;
- Kritikus infrastruktúra védelme;
- CBRN helyzetek kezelése.

Ezeket gyakran különböző országok különleges egységei vezetik, például a francia RAID vagy a német GSG–9.

Néhány nemzetközi gyakorlat szituációja:

- Tömeges túszejtés: Több helyszínes támadás-szimuláció városi környezetben.
- CBRN fenyegetés: Vegyi vagy biológiai anyaggal történő támadás egy vonaton.
- Repülőgép eltérítés: Közös beavatkozás egy elhagyott repülőtéren.
- Buszeltérítés: Több országon áthaladó, közös reagálást igénylő incidens.

Magyar részvétel és szerep:

A Terrorelhárítási Központ (TEK) aktív tagja az ATLAS-hálózatnak. Magyarország kiemelkedő szerepet játszik:

- Taktikai orvoslás terén: 2019-ben létrehozta Európa első független taktikai orvoslási képzési központját, melyben évente több alkalommal 20-30 fős csoportokban képzik a tagországok munkatársait.

– Városi műveletek oktatása: épületbehatolás, városi harcászat, speciális mesterlövész kurzus tartása.
– Több nemzetközi gyakorlat házigazdája: koordinált kiképzések és tesztgyakorlatok szervezése.

Jövőkép:

A jövőben az ATLAS célja egy egységes **Quick Reaction Force (Gyors Reagálású Erő) létrehozása, amely azonnal bevethető határokon átnyúló incidensek esetén**, valamint a NATO, FRONTEX és más európai biztonsági szervekkel való szorosabb együttműködés.

Az ATLAS doktrina és stratégia egyértelmű és iránymutató, véleményem szerint meghatározónak kell lennie a nemzeti különleges alakulatok, továbbá a többi bevetési egység számára is.

8. ÖSSZEFOGLALÁS

A nagy kockázatú rendészeti akciók előkészítése tehát komplex feladat, amelyben minden részletre figyelni kell a siker és a biztonság érdekében. Az előkészítés során a legnagyobb hangsúlyt a kockázatok csökkentésére, a precíz tervezésre és a csapatok felkészítésére kell fordítani.

Nem szabad elfelejteni, hogy a legegyszerűbb elfogásnál sem lehetünk biztosak abban, hogy a célszemély milyen tudati állapotban van, esetleg milyen tudatmódosító szer hatása alatt lehet és ez mennyiben befolyásolja a „józan" ítélőképességét. Mi adott esetben azokat a ránézve terhelő információkat ismerjük, amiket sikerült felderítenünk, de az igazi tettesi múltját csak ő maga ismeri. E múlt komplex kockázatának megfelelően fog várhatóan reagálni, ellenállni, ami adott esetben nagyságrendekkel térhet el az általunk várttól. Ezért hiszem, hogy egy akciót nem lehet túlbiztosítani, csak a kellő előkészítés, tervezés, a megfelelő erő és eszköz rendelkezésre állása, és meggyőző fölénye lehet a záloga az eredményes és biztonságos végrehajtásnak.

Ebben a közegben át kell értékelni a feladat-végrehajtások rendszerét, és pontosan meg kell húzni azokat a határvonalakat, ahol csak nagyobb erővel, kellő biztosítással és speciális felkészültséggel lehet intézkedéseket végrehajtani.

FELHASZNÁLT IRODALOM

BODA József főszerk. (2019): *Rendészettudományi Szaklexikon*. Budapest: Dialog Campus Kiadó.

BOLZ, Frank Jr. – DUDONIS, Kenneth J. – SCHULZ, David P. (2011): *The Counterterrorism Handbook: Tactics, Procedures, and Techniques*. Boca Raton: CRC Press.

CALIFORNIA COMMISSION ON PEACE OFFICER STANDARDS AND TRAINING (2005): *SWAT Operational Guidelines and Standardized Training Recommendations*. Sacramento. Online: https://post.ca.gov/Publication-List

DIFUSCO, John – CHAVES, Richard – CARISTI, Vincent (1986): *Tracers*. New York: Hill and Wang. 24. Online: https://archive.org/details/tracersplay00difu/page/90/mode/2up?q=one-hundred+

HATTES, Keith A. (1999): *Special Operations Mission Planning and Analysis Support System*. Master's Thesis. Monterey: Naval Postgraduate School. Online: http://hdl.handle.net/10945/8990

HEADQUARTERS, DEPARTMENT OF THE ARMY (2020): *Special Forces Branch – DA PAM 600-3*. U.S. Army. Reserve. Online: https://www.usar.army.mil/Portals/98/Documents/ARCD/DA%20PAM%20600-3s/SF%20DA%20PAM%20600-3.pdf

JASENSZKY Nándor – CSOMÓS István – LÉCZ Róbert – SZÉPLAKI Beatrix – SZINÁK Attila (2016): *Nagy kockázatú akciók, avagy a terrorelhárítók mindennapjai*. In: BEBESI Zoltán dr. (szerk.): *Terrorelhárítási alapismeretek*. Budapest: Dialóg Campus Kiadó – Nordex Kft. 263–296.

JASENSZKY Nándor – CSOMÓS István – LÉCZ Róbert – SZÉPLAKI Beatrix – SZINÁK Attila (2017): *Nagy kockázatú akciók*. In: KASZNÁR Attila (szerk.) *Bevezetés a terrorelhárítás alapjaiba*. Budapest: Dialóg Campus Kiadó – Nordex Kft. 351–399.

JASENSZKY Nándor – SOMOSKÖVI Áron dr. (2016): *A terrorelhárítás információéhsége és a „csillapítás" lehetőségei*. In: Dr. BEBESI Zoltán (szerk.) *Terrorelhárítási alapismeretek*. Budapest: Dialóg Campus Kiadó – Nordex Kft. 193–212.

JASENSZKY Nándor (1987): *Operatív erők, eszközök és módszerek komplex alkalmazása, illegálisan hazánkban tartózkodó, külföldi bűnözők által elkövetett betörési sorozat felderítésében*. Szakdolgozat. Belügyminisztérium Rendészettudományi Főiskola

JASENSZKY Nándor (2015*): Adatszerzés – Információhasznosulás – Biztonságtudatos vállalati kultúra*. In: *SZAMOS Tamás (szerk.) A nyílt információgyűjtés fejlődő területei*: Nemzetközi tudományos-szakmai konferencia Tanulmánykötet. Budapest: Belügyi Tudományos Tanács. 55–65.

KASZNÁR Attila – JASENSZKY Nándor – SOMOSKÖVI Áron (2017): *Az információ szerepe és elemzési lehetőségei a terrorfelderítés aspektusából*. In: KASZNÁR Attila (szerk.) *Bevezetés a terrorelhárítás alapjaiba*. Budapest: Dialóg Campus Kiadó – Nordex Kft. 211–269.

MARAS, Marié-Helen (2016): *A terrorizmus elmélete és gyakorlata*. Budapest: Antall József Tudásközpont.

MIJARES, Tomas C. – MCCARTHY, Ronald M. (2008): *The Management of Police Specialized Tactical Units*. Springfield: Charles C. Thomas. Online: https://archive.org/details/managementofpoli0000mija

NATIONAL TACTICAL OFFICERS ASSOCIATION (2016): *Strategic Leadership Program and SWAT Command Training Modules*. Online: https://www.ntoa.org/academy/strategic-leadership/

REDMAN, Alvin (1959): *The Wit and Humor of Oscar Wilde*. New York: Dover. Online: https://archive.org/details/withumorofoscarw00wild/page/n283/mode/2up

SCHMID, Alex P. ed. (2021): *Handbook of Terrorism Prevention and Preparedness*. The Hauge: ICCT Press Publication. Online: DOI: 10.19165/2020.6.01

VÁKÁT OLDAL

Szerzőink

Csepregi Zsolt: A Nemzeti Közszolgálati Egyetem Hadtudományi Doktori Iskolájának hallgatója és az amerikai Everbridge, válságkezelést és üzletmenetfolytonosságot támogató vállalat közel-keleti térségért felelős elemzője.

Forró Tamás: A Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskolájának doktorandusza. Kutatási területe az információs műveletek, valamint a kiberterrorizmus.

Jasenszky Nándor: Nyugalmazott rendőr ezredes, 20 éven át hivatásos bűnügyi felderítőként tevékenykedett. Ezt követően a magánbiztonságban, az üzleti hírszerzés területén dolgozott. 2016 óta a Terrorelhárítási Központ Társadalmi Kapcsolatok Osztályának vezetője.

Kiss Nikoletta: A Nemzeti Közszolgálati Egyetem, Hadtudományi Doktori Iskolájának doktorandusza.

Petruska Ferenc Dr.: Hivatásos katona, alezredes, egyetemi docens, a Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Karának nemzetközi dékánhelyettese, valamint a Honvédelmi Jogi és Igazgatási Tanszék tanszékvezetője. Kutatási területei közé tartozik a mesterséges intelligencia alapú akadémiai adatszakértelem (academic data science) az autonóm fegyverrrendszerek (AWS), a jogi hadviselés, (lawfare), a veterángondoskodás, valamint a vallásgyakorlás kereteinek jogi szabályozása. Emellett hadijogot. a megszllás jogát, honvédelmi jogot és igazgatást is oktat., valamint a Honvéd Zrínyi Sportegyesület elnökeként széleskörű gyakorlati tapasztalattal rendelkezik a sportjog területén.

Viszkocsil László: A Terrorelhárítási Központ munkatársa, a CTFINET támogató szakértője.

VÁKÁT OLDAL

A XXI. század biztonsági környezetét alapvetően formálja a terrorizmus állandó és sokrétű fenyegetése. Az elmúlt évtizedek tapasztalatai is rávilágítottak arra, hogy a terrorizmus nem statikus jelenség, hiszen folyamatosan alkalmazkodik a politikai, társadalmi és technológiai változásokhoz.

A kötet tanulmányai széles spektrumot ölelnek fel. Kiemelt témaként jelenik meg a mesterséges intelligencia, a hírszerző szolgálatok közötti nemzetközi együttműködés kérdésköre, a kritikus infrastruktúra sebezhetősége, a kiberterrorizmus és a radikalizáció folyamatának elemzése.

A kötet nem csupán a jelen problémáira reflektál, hanem a jövő kihívásaira is tekint. E szemelvények célja, hogy gondolatébresztőként és tájékozódási pontként szolgáljanak mindazok számára, akik a terrorizmus komplex kihívásainak megértésére és kezelésére törekszenek.