NEMZETBIZTONSÁGI SZEMLE

Kiemelt közlemények

Bor Olivér: *Autonóm drón-rendszerek kiberbiztonsága: kockázatok és reziliencia*

Erdélyi Ákos: *A pszichológiai boncolás elméleti alapjai és alkalmazásási lehetőségei*

14. évf. (2026)
1. szám

ISSN 2064-3756 (elektronikus)

LUDOVIKA
EGYETEMI KIADÓ

Impresszum

Nemzetbiztonsági Szemle
A Nemzeti Közszolgálati Egyetem Nemzetbiztonsági Intézetének elektronikus (online) megjelenésű tudományos folyóirata

HU ISSN 2064-3756 (elektronikus)

Szerkesztőség
Nemzeti Közszolgálati Egyetem Nemzetbiztonsági Intézet
Szerkesztő: Dr. Deák József
Szerkesztőségi titkár: Mezei József
Internetes elérhetőség: https://folyoirat.ludovika.hu/index.php/nbsz

Kiadó
Nemzeti Közszolgálati Egyetem | Ludovika Egyetemi Kiadó
Kapcsolat: www.ludovika.hu; kiadvanyok@uni-nke.hu
Székhely: 1083 Budapest, Ludovika tér 2.
A kiadásért felel: Dr. Deli Gergely rektor
Olvasószerkesztők: Bujdosó Hajnalka, Farkas-Nagy Judit, Gergely Zsuzsánna, Resofszki Ágnes
Tördelőszerkesztő: Kőrösi László

Tartalom

Bor Olivér
Autonóm drónrendszerek kiberbiztonsága: kockázatok és reziliencia 3

Solti István
A nemzetbiztonsági szolgálatokról szóló törvény előképei 23

Fórizs Sándor
Külföldre szökés és kémkedés bűntettének vádja 36

Gábor Andrékó
Why Institutional Isolation Fails 46

Erdélyi Ákos
A pszichológiai boncolás elméleti alapjai és alkalmazási lehetőségei 57

NEMZETBIZTONSÁGI SZEMLE
14. évfolyam (2026) 1. szám 3–22. | DOI: 10.32561/nsz.2026.1.1

Bor Olivér[1]

Autonóm drónrendszerek kiberbiztonsága: kockázatok és reziliencia

Szakirodalmi áttekintés

Cybersecurity of Autonomous Drone Systems: Risks and Resilience

Literature Review

Az autonóm és részben autonóm pilóta nélküli légi járművek (unmanned aerial vehicle, UAV), valamint az ezek működését integrált módon biztosító pilóta nélküli légijármű-rendszerek (unmanned aircraft system, UAS) gyors térnyerése alapvetően új kiberbiztonsági kihívásokat hívott életre.[2] *Az autonóm döntéshozatal, a hálózat-alapú kommunikáció és a fizikai működés szoros összekapcsolódása következtében a kibertérben végrehajtott támadások közvetlen és azonnali működési, valamint biztonsági következményekkel járhatnak. A tanulmány szisztematikus szakirodalmi áttekintésre építve elemzi az autonóm UAS-okat érintő kiberbiztonsági kockázatokat, hangsúlyt fektetve a navigációs rendszereket célzó GPS-spoofing-fenyegetésekre. Az elemzés bemutatja továbbá azokat a rétegezett védelmi mechanizmusokat és rezilienciafokozó megközelítéseket, amelyek alkalmasak e komplex fenyegetések hatásainak mérséklésére és az autonóm rendszerek üzembiztonságának növelésére.*

Kulcsszavak: *autonóm drónrendszerek, UAV, UAS, GPS-spoofing, kiberbiztonság, reziliencia*

The rapid proliferation of autonomous and semi-autonomous unmanned aerial vehicles (UAVs), along with the integrated unmanned aircraft systems (UAS) that enable their operation, has introduced fundamentally new cybersecurity challenges. Due to

[1] PhD-hallgató, Nemzeti Közszolgálati Egyetem Hadtudományi Doktori Iskola, e-mail: oliver.bor@protonmail.com

[2] A tanulmány következetesen a pilóta nélküli légijármű-rendszer (UAS) fogalmát használja, mivel a kiberbiztonsági kockázatok nem kizárólag a repülő platformra (UAV) terjednek ki, hanem a földi irányítási, kommunikációs és támogató informatikai komponensekre is.

the tight coupling of autonomous decision-making, network-based communication, and physical operation, cyberattacks conducted in cyberspace may lead to direct and immediate operational and safety consequences. Building on a systematic literature review, this study analyses the cybersecurity risks affecting autonomous UAS, with particular emphasis on GPS spoofing threats targeting navigation systems. The analysis further presents layered defensive mechanisms and resilience-enhancing approaches capable of mitigating the impact of these complex threats and improving the operational reliability of autonomous systems.

Keywords: *autonomous drone systems, UAV, UAS, GPS spoofing, cybersecurity, resilience*

Bevezetés

Az autonóm és részben autonóm pilóta nélküli légi járművek fejlődése szorosan illeszkedik a modern technológiai forradalom tágabb kontextusába, amelyet a különböző tudományterületek fokozódó konvergenciája jellemez. A drónok nem értelmezhetők pusztán repülőeszközként: ezek olyan komplex műszaki rendszerek, amelyekben a mechanikai megoldások, az elektrotechnika, az irányítástechnika, az elektronika és az informatika szoros, integrált egységet alkotnak.[3] E platformok fejlődését különösen a mesterséges intelligencia (*artificial intelligence,* AI) és a robottechnika előretörése, valamint a műholdas és vezeték nélküli kommunikációs technológiák elterjedése gyorsította fel, miközben ezzel párhuzamosan új, korábban kevésbé ismert sérülékenységek is megjelentek.

A szakirodalomban és a szabályozási dokumentumokban a *drón* kifejezés jellemzően a pilóta nélküli légi járművet (UAV) jelöli, amely elsősorban magára a repülő platformra utal. Ezzel szemben a pilóta nélküli légijármű-rendszer (UAS) ennél lényegesen átfogóbb fogalom: az UAV mellett magában foglalja a fedélzeti érzékelőket és vezérlőegységeket, a földi irányító és kommunikációs infrastruktúrát, valamint az üzemeltetést és adatfeldolgozást támogató háttérrendszereket is. A NATO által alkalmazott definíció hangsúlyozza, hogy a pilóta nélküli légi járművek távirányítással, előre programozott autonóm működéssel vagy e megoldások kombinációjával üzemelhetnek, és adott esetben halálos vagy nem halálos hatás kiváltására alkalmas hasznos teher *(payload)* hordozására is képesek lehetnek. E meghatározásból következően a biztonsági kérdések nem szűkíthetők le kizárólag az UAV szintjére, hanem szükségszerűen az egész UAS-architektúra átfogó vizsgálatát igénylik.[4]

A pilóta nélküli repülőeszközök történeti fejlődése a 20. század elejéig vezethető vissza, azonban szélesebb körű és rendszeres katonai alkalmazásuk a második világháborúban jelent meg, amikor elsősorban célrepülőgépként használták őket. A valódi technológiai áttörést azonban az információs és kommunikációs rendszerek fejlődése hozta el. Az 1970-es évektől kezdve megjelent a valós idejű adatátvitel lehetősége, amely jelentősen lerövidítette az információszerzés ciklusait, és egyúttal új védelmi

[3] Kiss–Palik 2023.
[4] Krasznay–Ináncsi 2021.

megoldások – például radarbesugárzás-jelzők és elektronikai zavaró rendszerek – kifejlesztését is ösztönözte. Az öbölháború ebből a szempontból fordulópontnak tekinthető, mivel ez volt az első olyan fegyveres konfliktus, amelyben az informatikai eszközök meghatározó szerepet játszottak a felderítésben, a vezetésben és a döntéstámogatásban. A különböző dróntípusok alkalmazása nemcsak a célmegjelölés és a tűzvezetés pontosságát növelte, hanem jelentős pszichológiai hatást is gyakorolt az ellenséges erőkre.[5] A későbbi fejlesztések során a GPS-alapú navigáció integrálása, majd a 2000-es évek elején a fegyverzettel ellátott UAV-ok megjelenése tovább fokozta e rendszerek technológiai összetettségét és stratégiai jelentőségét.[6]

Napjainkra a drónok mind a civil, mind a katonai alkalmazási területeken a mindennapi gyakorlat részévé váltak, miközben a róluk folytatott szakmai és társadalmi diskurzus jellemzően továbbra is a repülésbiztonsági aspektusokra összpontosít. Ezzel szemben az UAV-ok és az UAS-ok működésük lényegét tekintve hálózatba kapcsolt, vezeték nélküli kommunikációt alkalmazó informatikai rendszerek,[7] amelyek sok esetben közvetett módon az internethez is kapcsolódnak. Ez a működési környezet szükségszerűen kiteszi őket a kibertérben megjelenő fenyegetéseknek. Az UAS-ok vonatkozásában a kockázatok három fő csoportba sorolhatók: a kommunikációs csatornákat érintő támadások, a kiberbiztonságot befolyásoló fizikai beavatkozások, valamint a támogató informatikai infrastruktúra elleni támadások. E fenyegetések nem csupán adatvédelmi és adatbiztonsági incidensekhez vezethetnek, hanem szélsőséges esetben a rendszer feletti irányítás elvesztését is eredményezhetik, ami a kibertéri eseményeket közvetlen fizikai károkozássá alakítja.[8]

Jelen tanulmány célja annak bemutatása, hogy az autonóm drónrendszerek kiberbiztonsági kockázatai miként értelmezhetők rendszerszinten, valamint milyen védelmi lehetőségek állnak rendelkezésre e sérülékenységek mérséklésére. A vizsgálat abból az alapfeltevésből indul ki, hogy az autonóm működés fokozódásával párhuzamosan a kiberbiztonság az UAS-ok egyik meghatározó biztonsági dimenziójává vált, amely szorosan összefonódik a biztonságos üzemeltetés követelményeivel és a technológia társadalmi elfogadottságával.

Módszertan

A tanulmány módszertani keretét szisztematikus szakirodalmi áttekintés képezi, amelynek célja az autonóm, illetve részben autonóm pilóta nélküli légijármű-rendszerekhez kapcsolódó kiberbiztonsági kockázatok és az ezekre adott védelmi válaszok strukturált, visszakövethető feltárása. A választott megközelítés lehetővé teszi, hogy a releváns tudományos eredmények ne esetleges vagy illusztratív módon jelenjenek meg, hanem előre rögzített keresési és kiválasztási kritériumok mentén, egységes elemzési logika szerint legyenek feldolgozva.

---

5 Kiss–Palik 2023.

6 Connor 2018.

7 Noha az autonóm drónrendszerek működése bizonyos pontokon hasonlóságot mutat az ipari irányítórendszerekkel (*operational technology,* OT), mobilitásuk, autonóm döntéshozataluk és nyílt, dinamikus környezetben történő üzemeltetésük miatt kiberbiztonsági szempontból eltérő fenyegetési és védelmi logikát igényelnek.

8 Krasznay–Ináncsi 2021; Ináncsi 2022.

Ennek megfelelően a kutatás elkerüli a szelektív irodalomhasználatot, és a szakirodalom szintetizálását nem egyedi példákra, hanem azonosítható mintázatokra és összefüggésekre alapozza. A kutatási folyamat egyes szakaszaiban – különösen a szakirodalom előszűrése, strukturálása és a koncepcionális keretek reflexív vizsgálata során – a mesterségesintelligencia-alapú eszközöket támogató jelleggel alkalmazta a szerző, azonban minden esetben az általa végzett szakmai értékelés és döntéshozatal mellett.

A szakirodalmi feltárás elsődleges adatforrását a Scopus adatbázis jelentette, amelyet kiegészítő jelleggel olyan mesterségesintelligencia-alapú kutatástámogató platformok (Scopus AI, Elicit) alkalmazása támogatott, amelyek a releváns publikációk, hivatkozási hálózatok és tematikus kapcsolódások előzetes feltérképezését segítették. A beválogatás és a relevancia megítélése, valamint a végső irodalomjegyzék összeállítása minden esetben önálló szakmai döntés alapján történt. A keresési stratégia tudatosan kialakított, többdimenziós kulcsszó-kombinációkra épült, amelyek együttesen fedték le a kiberbiztonság általános fogalmi kereteit, a sérülékenységek és fenyegetések típusait, valamint az autonóm drónrendszerek technológiai és üzemeltetési sajátosságait. Ennek megfelelően a keresések a *(cybersecurity OR cyber threat OR information security OR data protection) AND (vulnerability OR weakness OR flaw OR risk) AND (autonomous drone OR unmanned aerial vehicle OR UAV OR drone) AND (threat OR vulnerability OR attack OR risk) AND (malware OR hacking OR breach OR intrusion) AND (defense OR protection OR mitigation OR security measures)* kulcsszó-kombinációkra épültek. Ez a logika biztosította, hogy a találati halmaz kizárólag olyan publikációkat tartalmazzon, amelyek a vizsgált technológiai környezetben értelmezhető kockázatokkal és azok kezelésével foglalkoznak.

A válogatási kritériumok értelmében kizárólag 2019 után megjelent, lektorált folyóiratcikkeket és könyvfejezeteket elemeztem, amelyek közvetlen módon tárgyalták az autonóm UAS-ok kiberbiztonsági aspektusait. A kiválasztott művek teljes szövegű feldolgozása kvalitatív, tematikus tartalomelemzés keretében valósult meg.

Az elemzés során a publikációkat egységes kódolási séma alapján dolgoztam fel. Ennek során az egyes tanulmányokban azonosítottam a meghatározó kiberfenyegetési kategóriákat, valamint az ezekhez kapcsolódó védelmi és mitigációs megoldásokat. A kódok összevetése lehetővé tette annak vizsgálatát, hogy a különböző forrásokban megjelennek-e visszatérő mintázatok, illetve kirajzolódnak-e koherens tematikus csoportok. A módszertani megközelítés sajátossága, hogy a tematikus szintézis nem a részletek mechanikus felsorolására törekedett, hanem a feltárt kódok alapján értelmezési keretbe rendezte a szakirodalmi állításokat.

Ez a megközelítés különösen indokoltnak tekinthető az autonóm drónrendszerek esetében, ahol a kockázatok nem izolált technikai problémák formájában jelennek meg. A kommunikációs csatornákat érintő támadások, a fizikai beavatkozások, valamint a támogató informatikai infrastruktúra elleni műveletek egymással szoros kölcsönhatásban álló, rendszerhatásokat kiváltó fenyegetési környezetet alkotnak. Szélsőséges esetben ezek a folyamatok az irányítás elvesztéséhez vezethetnek, és a kibertérben bekövetkező események közvetlen fizikai károkozásban materializálódhatnak.

A kódolás és a tematikus csoportképzés ennek megfelelően nem öncélú elemzési technikaként jelent meg, hanem olyan módszertani eszközként, amely lehetővé tette a különböző szinteken – szoftveres, hardveres, kommunikációs és navigációs rétegben – azonosítható sérülékenységek és az ezekre adott válaszok rendszerszintű értelmezését. Ez az elemzési

keret megalapozza a kiberkockázatok és a védelmi lehetőségek strukturált bemutatását az autonóm UAS-architektúra összefüggésében, összhangban a modern, kockázatalapú kiberbiztonsági megközelítések elméleti és gyakorlati követelményeivel.

Szakirodalmi szintézis az autonóm UAS-ok kiberbiztonsági kockázatairól és védelméről

A kiberbiztonsági kockázatok és sérülékenységek rendszerezése

Az autonóm drónok alkalmazása az elmúlt években jelentősen kiterjedt a katonai felhasználástól kezdve a környezetmegfigyelésen át egészen a logisztikai megoldásokig. Ezzel párhuzamosan azonban olyan kiberbiztonsági sérülékenységek kerültek felszínre, amelyek komoly kockázatot jelentenek a drónok biztonságos és megbízható működésére nézve.[9] A szoftveres sérülékenységek közül kiemelendő az illetéktelen hozzáférés problémája, amely lehetővé teszi a vezérlési csatornák manipulálását és érzékeny adatok megszerzését, ezáltal veszélyeztetve a drón irányítását és az általa gyűjtött információk védelmét.[10] Szintén komoly fenyegetést jelentenek a rosszindulatú programok és a szoftveres kihasználások, amelyek az autonóm drónrendszerek működését és biztonságát veszélyeztethetik.[11] A szoftveres támadási felület mellett a drónok biztonságát a fizikai komponensek és az érzékelési lánc sérülékenységei is érdemben befolyásolják.

A hardveres sebezhetőségek körében fontos szerepet kap az érzékelők manipulálása, megtévesztése, más néven *sensor spoofing,* amely során a támadó hamis adatokat juttat a drón érzékelőibe, így félrevezeti annak navigációs rendszerét és működési döntéseit.[12] Ezzel összefüggésben megjelennek az úgynevezett trójai támadások is, amelyek különösen a mélytanulási modelleket alkalmazó UAV-ok esetében veszélyesek: ezek során a mesterséges intelligencián alapuló rendszerek tanítási adatait mérgezik meg, ami hibás objektumfelismeréshez és téves navigációs döntésekhez vezethet.[13] A drón működése ugyanakkor nemcsak a fedélzeti döntéshozatalon múlik, hanem azon is, hogy a navigációs és vezérlési csatornák mennyire védettek. Emiatt a kommunikációs réteg kompromittálása gyakran azonnali, látványos működési következményekhez vezet.

A kommunikációs sérülékenységek talán a leglátványosabb kockázati tényezők közé tartoznak. A GPS-jelek megtévesztése vagy zavarása – *GPS-spoofing* és *-jamming*[14] – révén a támadó eltérítheti a drónt a tervezett útvonalától, vagy akár működésképtelenné is teheti azt.[15] Hasonlóan súlyos fenyegetést jelent a távoli irányítás jogosulatlan átvétele, amely

[9] Renu–Sarveshwaran 2025.
[10] Sissodia et al. 2025.
[11] Oracevic–Salman 2024.
[12] Oracevic–Salman 2024.
[13] Mynuddin–Khan–Mahmoud 2023; Mynuddin et al. 2024.
[14] A *GPS-spoofing* a navigációs jelek megtévesztésén alapul, míg a *GPS-jamming* a jelek zavarásával vagy blokkolásával teszi lehetetlenné a helymeghatározást; a két támadási forma eltérő detektálási és mitigációs stratégiákat igényel.
[15] Renu–Sarveshwaran 2025.

során illetéktelen szereplők szereznek hozzáférést a drón vezérléséhez.[16] E kockázatok csökkentése tipikusan több rétegből álló védekezést igényel, amely a kommunikáció, a hozzáférések és a detektálás oldalán egyszerre erősít.

A sérülékenységek csökkentésére számos védelmi stratégia alakult ki. Az adatátvitel védelmét fejlett titkosítási technikák biztosíthatják, amelyek megakadályozzák, hogy illetéktelenek hozzáférjenek a drón és az irányítórendszer között cserélt információkhoz.[17] Ezt egészíti ki a többtényezős hitelesítés alkalmazása, amely nem csupán egyetlen azonosítási elemre – például jelszóra – támaszkodik, hanem több egymást kiegészítő ellenőrzési lépcsőt alkalmaz annak érdekében, hogy kizárólag jogosult felhasználók irányíthassák a drónokat.[18]

A behatolásészlelő rendszerek (*intrusion detection systems,* IDS) egyre inkább gépi tanuláson alapulnak, ami lehetővé teszi a rendellenes működési minták és a potenciális támadások valós idejű felismerését, ezáltal növelve az autonóm drónműveletek biztonságát.[19] A blokklánc-technológia alkalmazása hozzájárulhat az adatok integritásának és nyomonkövethetőségének biztosításához az autonóm drónrendszerek adatcseréje során.[20] A nulla bizalom elvén alapuló architektúra – amely abból indul ki, hogy sem belső, sem külső szereplők nem tekinthetők automatikusan megbízhatónak – folyamatos ellenőrzést és hitelesítést valósít meg, ezáltal csökkentve az adatszivárgás és a jogosulatlan hozzáférés kockázatát.[21]

A mesterséges intelligenciát érintő védekezési stratégiák között megjelenik az ellenséges környezetre felkészített, úgynevezett önjavító AI-modellek alkalmazása, amelyek képesek önállóan felismerni és tanulni az újonnan megjelenő kiberfenyegetésekből, ezáltal növelve a UAV-rendszerek ellenálló képességét. A feltörekvő technológiák közül a posztkvantum-kriptográfia olyan titkosítási megoldásokat kínál, amelyek a jövőben várható kvantumszámítógépes támadásokkal szemben is ellenállónak tekinthetők. Az élperemszintű mesterséges intelligencia *(edge AI)* lehetővé teszi a fenyegetések valós idejű, fedélzeti észlelését anélkül, hogy a drón felhőalapú szolgáltatásokra támaszkodna, ezáltal csökkentve a késleltetést és gyorsítva a reakcióidőt. Végül a 6G-alapú kommunikációs hálózatok rendkívül gyors és erősen titkosított adatátvitelt ígérnek, ami hosszú távon jelentősen hozzájárulhat az autonóm drónrendszerek átfogó kiberbiztonságának megerősítéséhez.[22]

A fenti megoldások az általános védelmi eszköztárat rajzolják fel. A következőkben a fenyegetéseket részletesebben, működési hatásuk szerint bontjuk ki, majd kiemelten a navigációt érintő *GPS-spoofing* kérdésére szűkítjük a fókuszt.

Az autonóm drónrendszerek esetében a navigációs képességek megbízhatósága kritikus, mivel a helymeghatározási adatok sérülése közvetlen hatással van a repülési útvonalak betartására és az autonóm döntéshozatal pontosságára. A leggyakrabban azonosított kockázatok közé tartoznak a globális helymeghatározó rendszert érintő támadások. A *GPS-spoofing* esetében a támadó hamis helymeghatározó jeleket sugároz, amelyek következtében a drón téves pozícióadatokat érzékel, ami az előre tervezett útvonaltól való eltéréshez, az irányítás

16 Oracevic–Salman 2024; Nascimento Aquilar Pey et al. 2022.
17 Damis et al. 2026.
18 Alsadie 2025.
19 Bhargavi et al. 2025; Renu–Sarveshwaran 2025.
20 Alsadie 2025; Damis et al. 2026.
21 Alquwayzani–Albuali 2024.
22 Alsadie 2025.

elvesztéséhez, vagy akár a légi jármű lezuhanásához is vezethet. E fenyegetéssel szoros összefüggésben áll a *GPS-jamming,* amely nem hamis jelek továbbításával operál, hanem a műholdas navigáció ellehetetlenítésével, a jelek blokkolásával vagy zavarásával fosztja meg a drónt a megbízható tájékozódás lehetőségétől.[23]

A korábban jelzett vezérlésátvételi kockázat különösen súlyos működési következményekkel jár, mivel a támadók a drón és az operátor közötti kommunikációs csatornák sérülékenységeit kihasználva átvehetik az irányítást a légi eszköz felett.[24] További fenyegetési kategóriát alkotnak a rosszindulatú szoftverek és egyéb szoftveres kihasználások, amelyek révén a drón fertőzhetővé válhat, működési anomáliák léphetnek fel, illetve lehetőség nyílhat érzékeny adatok jogosulatlan megszerzésére vagy módosítására.[25] A *sensor spoofing* során a fedélzeti érzékelők manipulált vagy hamis adatokat kapnak, ami hibás döntéshozatalt eredményezhet, és autonóm üzemmód esetén különösen súlyos, akár veszélyes helyzetek kialakulásához is vezethet.[26]

Az adatok jogosulatlan módosítása és megszerzése – adatmanipuláció vagy adatvédelmi incidensek formájában – szintén jelentős fenyegetést hordoz. Ilyen esetekben a támadók hozzáférhetnek a drón által gyűjtött információkhoz, ezáltal veszélyeztetve azok bizalmasságát és integritását.[27] A szolgáltatásmegtagadásos (*denial of service,* DoS) támadások célja a vezérlő- vagy kommunikációs rendszerek túlterhelése, amelynek következtében a drón részlegesen vagy teljes mértékben működésképtelenné válhat.[28] Az autonóm rendszerek elterjedésével párhuzamosan egyre nagyobb jelentőséget kapnak a mesterséges intelligenciát célzó ellenséges támadások is, amelyek során az AI-modellek manipulálásával a drón nem a tervezett módon reagál a környezeti hatásokra, és hibás döntéseket hoz.[29]

A fenyegetések köre nem korlátozódik kizárólag a digitális térre, mivel a közvetlen fizikai támadások – például az alkatrészek szándékos megrongálása – szintén komoly működési zavarokat és szolgáltatáskiesést idézhetnek elő.[30] A kommunikációs csatornák lehallgatása vagy módosítása lehetőséget biztosíthat az adatok jogosulatlan megszerzésére, illetve a vezérlési parancsok manipulálására, ami közvetlen irányítási és adatbiztonsági kockázatot jelent. Emellett egyre hangsúlyosabbá válnak az ellátási láncot érintő támadások is, mivel a gyártási vagy logisztikai folyamat során kompromittált komponensek rejtett sérülékenységeket hordozhatnak, amelyek később a rendszerrel szemben kihasználhatók.[31] A felsorolt kockázatok kezelése ezért nem egyetlen kontrollal oldható meg, hanem egymást kiegészítő technikai és szervezeti védelmi rétegek kombinációjával.

---

23 Oracevic–Salman 2024; Singh et al. 2023.
24 Lee–Kim 2019.
25 Laraib–Sial–Ujjan 2025.
26 Oracevic–Salman 2024.
27 Laraib–Sial–Ujjan 2025; Lee–Kim 2019; Shafik – Mojtaba Matinkhah – Shokoor 2023.
28 Aldossary–Alzamil–Almutairi 2025; Sree Lakshmi et al. 2025.
29 Javed et al. 2025; Sissodia et al. 2025.
30 Singh et al. 2023.
31 Damis et al. 2026.

Védelmi stratégiák és rétegezett kiberbiztonsági megközelítések

Az alábbiakban a bemutatott fenyegetésekhez rendelhető, operatív védelmi intézkedéseket foglaljuk össze. Az adatok titkosítása és a biztonságos kommunikációs protokollok alkalmazása alapvető eszközt jelent az adatforgalom lehallgatásának és manipulációjának megelőzésében.[32] A behatolásészlelő rendszerek bevezetése operatív eszközt biztosít a támadások azonosítására és kezelésére az autonóm drónrendszerekben.[33] A redundáns megoldások alkalmazása – például több GPS-vevő és inerciális navigációs rendszer párhuzamos használata – hozzájárulhat a helymeghatározást érintő támadások felismeréséhez és hatásuk mérsékléséhez.[34] A nulla bizalom elvén alapuló biztonsági modell alkalmazása elősegíti a jogosulatlan hozzáférések és az adatszivárgás kockázatának csökkentését az autonóm drónrendszerek esetében.[35] Végül a blokkláncalapú megoldások alkalmazása szavatolhatja a biztonságos és megváltoztathatatlan adatcserét, ami különösen alkalmas az adatintegritás és a nyomonkövethetőség garantálására.[36] E védelmi intézkedések integrált alkalmazása, valamint a kutatók, fejlesztők és üzemeltetők közötti folyamatos együttműködés elengedhetetlen feltétele az autonóm drónrendszerek kiberbiztonsága megerősítésének és hosszú távon megbízható működésük biztosításának.

A felsorolt intézkedések közül több általánosan alkalmazható, ugyanakkor vannak olyan támadási formák, amelyek különösen kritikusak autonóm repülés esetén. Ezek közé tartozik a *GPS-spoofing,* amely a navigáció megbízhatóságát közvetlenül érinti, ezért önálló áttekintést indokol.

GPS-spoofing mint kritikus navigációs fenyegetés

A GPS-spoofing *támadások működési hatásai és fenyegetési modellje*

Az autonóm drónrendszerek esetében a navigációs képességek megbízhatósága rendkívül fontos, mivel a helymeghatározási adatok sérülése közvetlen hatással van a repülési útvonalak betartására és az autonóm döntéshozatal pontosságára. Az autonóm drónrendszerek *GPS-spoofing* támadásokkal szembeni védelem érdekében az elmúlt években több, eltérő technológiai alapokon nyugvó megoldás kidolgozása és kísérleti validálása történt meg. E módszerek közös célja annak azonosítása, hogy a drón által vett helymeghatározási jelek mennyiben térnek el a tényleges környezeti állapottól, valamint annak biztosítása, hogy a rendszer az eltérések észlelése esetén gyors és megbízható válaszlépéseket legyen képes végrehajtani. A detektálási és mitigációs technikák egyik meghatározó csoportját a gépi tanuláson alapuló anomáliaészlelési eljárások alkotják. E megközelítésben a hardveres és szoftveres komponensek integrált alkalmazása – így például a GPS-vevők, a szoftveresen definiált rádiók (*software-defined radio*, SDR) és a gépi tanulási algoritmusok együttes

[32] Damis et al. 2026.
[33] Aldossary–Alzamil–Almutairi 2025; Maqbool et al. 2024.
[34] Singh et al. 2023.
[35] Alquwayzani–Albuali 2024.
[36] Damis et al. 2026; Orye et al. 2024.

használata – hatékony eszközt biztosít a hamisított jelek felismerésére. Egy ilyen rendszer esetében 97%-os észlelési arány volt elérhető, miközben a biztonsági reakcióként alkalmazott „visszatérés az indulási pontra" (*return-to-home,* RTH) funkció mindössze 2,3 másodperces késleltetéssel lépett működésbe.[37] A mélytanuláson alapuló modellek tovább növelik e megközelítés hatékonyságát: az összetett architektúrák, mint például a BiLSTM-Attention-CNN modell, képesek az időbeli mintázatok megragadására és a releváns jelszekvenciák kiemelésére, ami különösen alkalmassá teszi őket a *GPS-spoofing* jellegzetes mintáinak azonosítására.[38]

A szenzorfúzión alapuló módszerek szintén kulcsszerepet töltenek be a védekezési stratégiákban. Az inerciális mérőegységek (*inertial measurement unit,* IMU) – beleértve a gyorsulásmérőket, a giroszkópokat és a magnetométereket –, valamint a GPS-adatok együttes elemzése lehetőséget teremt az elvárt és a tényleges mozgásminták összevetésére. Az ilyen jellegű eltérések megjelenése erős indikátorként szolgálhat egy folyamatban lévő *spoofing* támadás azonosításához.[39] A több, egymástól független érzékelőrendszer alkalmazása tovább fokozza az észlelés megbízhatóságát, drónrajok esetében például a GPS-alapú távolságszámítások összevethetők az *ultra-wideband* (UWB) technológiával mért értékekkel, ami lehetővé teszi a helymeghatározási adatok hatékony keresztellenőrzését.[40]

A vizuális információk feldolgozása egy további, ígéretes irányt képvisel a *GPS-spoofing* detektálásában. Az előre betanított képfeldolgozó modellek – például a ResNet36 – alkalmasak arra, hogy a drón által rögzített képeket műholdfelvételekkel hasonlítsák össze, és az észlelt eltérések alapján következtessenek a helymeghatározási adatok megbízhatatlanságára.[41] E megközelítést egészíti ki a videófolyamok valós idejű elemzése, amely során a kamera által rögzített képkockák térbeli összefüggéseit vetik össze a GPS-koordinátákkal, ezáltal lehetővé téve a *spoofing* támadások gyors felismerését.[42]

A jelszintű elemzési módszerek elsősorban a rádiófrekvenciás (RF) jelek feldolgozására építenek. E megoldások statisztikai és gépi tanulási technikákat – így például főkomponens-analízist (*principal component analysis,* PCA), valamint hosszú rövid távú memóriával rendelkező neurális hálózatokat (*long short-term memory,* LSTM) – alkalmaznak annak érdekében, hogy a hamisított jeleket nagy pontossággal elkülönítsék a hiteles GPS-jelektől. Egy másik irányt képviselnek az alaptér-projekción és az érkezési irány becslésén *(direction of arrival)* alapuló algoritmusok kombinációi, amelyek lehetővé teszik az eredeti és a megtévesztő jelek térbeli elkülönítését, ezáltal mérsékelve a *spoofing* támadások hatását.[43]

Az önellenőrző, más néven öndiagnosztikai megközelítések a drón belső működési paramétereinek elemzésére támaszkodnak. A repülési dinamikában, az energiafelhasználásban vagy a vezérlési válaszokban megjelenő rendellenességek vizsgálata révén a pilóta nélküli légi jármű képes lehet önállóan azonosítani azokat az anomáliákat, amelyek *GPS-spoofing*-támadás jelenlétére utalnak.[44]

---

37 Tucker–Nadeem–Pervez 2025.
38 Yang–Oracevic–Dilek 2025.
39 Liang et al. 2019, 2022; Prasanna Srinivasan – Sathyadevan 2023.
40 Mykytyn et al. 2023.
41 Jain–Jain–Sahoo 2024.
42 Davidovich–Nassi–Elovici 2022.
43 Tiwari et al. 2023.
44 Basan et al. 2021.

A gyakorlati alkalmazás során rendkívül fontos a valós idejű működés biztosítása, mivel a túlzott késleltetés érdemben csökkentheti a védekezési mechanizmusok hatékonyságát. Egyes információfúzión alapuló eljárások képesek a *spoofing* támadások észlelésére akár nyolc másodpercen belül, ami már lehetőséget teremt az időben történő beavatkozásra. Emellett figyelembe kell venni a kisebb méretű vagy erőforrás-korlátozott drónplatformok sajátosságait is, amelyek esetében előnyt élveznek azok a megoldások, amelyek nem igényelnek kiegészítő hardverelemeket. Az alacsony erőforrás-igényű mélytanulási architektúrák alkalmasak arra, hogy alacsony számítási és energiaigény mellett is hatékony védelmet biztosítsanak *GPS-spoofing* támadásokkal szemben.[45]

Míg az előző technikák elsősorban a *spoofing* észlelésének módszercsaládjait mutatták be, a következő megközelítések már a reakciót és a működésfenntartást helyezik előtérbe. Ezek célja, hogy a drón a detektálás után is biztonságos állapotba kerüljön, illetve navigációja helyettesíthető legyen.

Detektálási, mitigációs és rezilienciafokozó megoldások GPS-spoofing *ellen*

Az autonóm drónrendszerek *GPS-spoofing* támadásokkal szembeni védelme érdekében több, egymást kiegészítő ellenintézkedés alkalmazható, amelyek a fenyegetések felismerésére, azok hatásainak mérséklésére, valamint alternatív navigációs képességek biztosítására egyaránt irányulnak. E megközelítések célja, hogy a drónműveletek megbízhatósága és biztonsága még kompromittált vagy erősen zavaró környezetben is fenntartható maradjon. A detektálási és hitelesítési technikák egyik alapvető pillére a biztonságos GPS-jelhitelesítés alkalmazása, amely lehetőséget ad a navigációs jelek eredetének ellenőrzésére, jelentősen csökkentve annak kockázatát, hogy a drón navigációs rendszere hamisított jeleket fogadjon el.[46] Ezt a megoldást tovább erősítik a kriptográfiai eljárások, különösen a *timed efficient loss-tolerant authentication* (TESLA) protokoll, amely a Galileo nyílt szolgáltatásához kapcsolódó navigációs üzenethitelesítés (*open service navigation message authentication,* OSNMA) részeként olyan védelmi réteget biztosít, amely hatékonyan támogatja a *spoofing* támadások felismerését és kezelését.[47] A gépi tanuláson alapuló megoldások ebben az összefüggésben szintén nagyon fontosak. Az olyan mélytanulási architektúrák, mint a CTDNN-Spoof modell, valós időben képesek a *GPS-spoofing* támadások azonosítására és osztályozására, ezáltal növelve a drónok reakcióképességét és adaptív működését.[48]

A GPS-alapú helymeghatározás kiegészítésére, illetve átmeneti kiváltására alternatív navigációs megoldások is rendelkezésre állnak. A nem GPS-alapú RTH-eljárások például légi felvételekre és konvolúciós neurális hálózatokra (CNN) épülnek, és lehetővé teszik, hogy a drón akkor is biztonságosan visszatérjen kiindulási pozíciójába, amikor a GPS-jelek megbízhatatlanná válnak vagy teljes mértékben kiesnek.[49] Ezt egészítik ki az inerciális navigációs rendszerek (INS), amelyek a GPS-szel kombinálva redundáns navigációs

[45] Hakeem et al. 2025.
[46] Almadhor et al. 2025.
[47] Shariat et al. 2025.
[48] Almadhor et al. 2025.
[49] Fadheli–Khalid–Fadzil 2025.

képességet biztosítanak, és hozzájárulnak a pozícióbecslés pontosságának fenntartásához GPS-zavarás vagy *spoofing* támadás esetén.[50]

A jelszintű elemzés és a redundancia elvének alkalmazása további fontos védelmi réteget képez. Több GPS-vevő párhuzamos használata és az általuk szolgáltatott adatok összehasonlítása lehetőséget teremt az inkonzisztenciák azonosítására, amelyek gyakran *GPS-spoofing* támadások jelenlétére utalnak.[51] Hasonló célt szolgál a GPS-jelek statisztikai jellemzőinek vizsgálata, amely során az anomális mintázatok felismerése elősegíti a hamis jelek kiszűrését. A vett jelerősség (*received signal strength,* RSS) ellenőrzésére épülő módszerek tovább növelik a detektálás megbízhatóságát: az olyan algoritmusok, mint a k-legközelebbi szomszéd (*k-nearest neighbors,* KNN), több bázisállomás RSS-adatai alapján képesek ellenőrizni a drón által jelentett pozíció hitelességét.[52]

A kooperatív és együttműködésen alapuló megközelítések új lehetőségeket nyitnak a *spoofing* elleni védekezésben. A kooperatív lokalizáció során a drón nem kizárólag saját, potenciálisan kompromittált GPS-adataira támaszkodik, hanem a közelben működő más UAV-ok információinak bevonásával határozza meg pozícióját, ezáltal csökkentve a megtévesztés hatását. A játékelméleti alapú modellek, így például a dinamikus Stackelberg-játék alkalmazása, lehetőséget biztosítanak a GPS-*spoofer* és a drónüzemeltető közötti kölcsönhatások formális leírására, ami elősegíti a támadásokkal szemben alkalmazható optimális védekezési stratégiák kidolgozását.[53]

A fejlettebb *spoofing* detektálási technikák közé sorolható az úgynevezett segédcsúcskövetés *(auxiliary peak tracking)* alkalmazása a GPS-vevőkben, amely még nagy teljesítményű, erős *spoofing* támadások esetén is képes a hamis jelek azonosítására, megakadályozva a drón szándékos eltérítését a támadó által meghatározott irányba.[54] A terepi környezetben is validált megoldások közül kiemelhetők azok az intelligens ellenintézkedések, amelyek az optikai azonosítást és a pozíciómérést integrálják a *GPS-spoofing* felismerésével, és szükség esetén a drónt biztonságos repülési pályára irányítják át, ezáltal megelőzve, hogy védett vagy érzékeny területeket veszélyeztessen.[55] E különböző ellenintézkedések összehangolt és integrált alkalmazása jelentősen hozzájárulhat ahhoz, hogy az autonóm drónrendszerek *GPS-spoofing* támadásokkal szemben ellenállóbbá váljanak, és megbízható működést biztosítsanak még ellenséges környezetben is. Az ellenintézkedéseknek fontos része a támadások felismerése és az azonnali mitigáció. A legújabb kutatási irányok ugyanakkor egyre inkább arra koncentrálnak, hogyan tartható fenn a működés folytonossága akkor is, ha a navigációs környezet tartósan kompromittált.

Az autonóm drónrendszerek *GPS-spoofing* támadásokkal szembeni ellenálló képességének növelésére irányuló kutatások egyre hangsúlyosabban olyan megoldásokra összpontosítanak, amelyek nem csupán a támadások detektálását célozzák, hanem a működés folytonosságának biztosítását is lehetővé teszik részben vagy teljes mértékben kompromittált navigációs környezetben. Ebben az összefüggésben a mesterséges intelligencián alapuló technológiák kiemelt szerepet töltenek be. A konvolúciós neurális hálózatokra

50 Singh et al. 2023.
51 Singh et al. 2023.
52 Sarkar et al. 2024.
53 Eldosouky–Ferdowsi–Saad 2020; Meng et al. 2021.
54 Ranganathan–Ólafsdóttir–Capkun 2016.
55 Buske et al. 2022.

épülő, transzfertanulást használó MobileNet modell például kifejezetten alkalmas erőforrás-korlátozott drónplatformokon történő alkalmazásra, miközben 98,49%-os felismerési pontosságot ért el *GPS-spoofing* támadások esetén. Ez az eredmény jól szemlélteti, hogy a magas detektálási teljesítmény nem szükségszerűen jár együtt a számítási vagy az energiaigény jelentős növekedésével.[56] A generatív ellenséges hálózatok (*generative adversarial networks,* GAN) egy további ígéretes irányt képviselnek, mivel képesek szintetikus támadási minták előállítására, amelyek révén a behatolásészlelő rendszerek felkészíthetők a korábban nem tapasztalt, adaptív támadási formákra, ezáltal növelve a rendszer általános ellenálló képességét.[57]

A szenzorfúzión alapuló megközelítések szintén nélkülözhetetlen szerepet játszanak a reziliencia erősítésében.[58] A *sensor-health aware resilient fusion* (SHARF) algoritmus olyan integrált módszert valósít meg, amely a GPS, az inerciális mérőegységek (IMU) és egyéb fedélzeti szenzorok adatait együttesen értékeli, miközben figyelembe veszi az egyes érzékelők aktuális állapotát és megbízhatóságát. Ennek eredményeként a drón képes fenntartani a pozícióbecslés elfogadható pontosságát akkor is, ha a GPS-adatok részben vagy teljes egészében kompromittálódtak.[59] Az IMU-k és a GPS kombinált alkalmazása önmagában is lényeges védelmi mechanizmust jelent, mivel lehetőséget biztosít a helymeghatározási információk kölcsönös ellenőrzésére, és támogatja a stabil navigáció fenntartását *spoofing* támadások fennállása esetén.[60]

A blokkláncalapú megoldások a *spoofing* gyanús események és szenzoradatok megmásíthatatlan naplózásával támogathatják az utólagos verifikációt és incidenskezelést. A decentralizált és megváltoztathatatlan adatstruktúrák elősegítik az adatintegritás megőrzését, valamint jelentősen megnehezítik az illetéktelen hozzáférést és az adatok manipulálását, ami közvetett módon hozzájárulhat a *GPS-spoofing* támadások hatásainak mérsékléséhez. A fejlett kriptográfiai megoldások szintén kulcsszerepet töltenek be a kommunikációs és navigációs csatornák védelmében. A kvantumkriptográfia olyan elméleti és gyakorlati alapokon nyugvó megoldásokat kínál, amelyek rendkívül magas biztonsági szintet szavatolnak, és jelentősen megnehezítik a navigációs jelek hamisítását vagy manipulálását.[61] Ezt egészítik ki a posztkvantum-kriptográfiai megközelítések közé tartozó Kyber-algoritmuson alapuló megoldások, amelyek lehetővé teszik az autentikus GPS-adatok helyreállítását *spoofing* támadások során, miközben kedvező számítási hatékonyságot és megnövelt biztonsági szintet nyújtanak.[62]

Az alternatív navigációs eljárások alkalmazása tovább növeli az autonóm drónrendszerek alkalmazkodóképességét. A légi képelemzésen alapuló módszerek konvolúciós neurális hálózatok segítségével dolgozzák fel a környezeti vizuális információkat, és támogatják a GPS-től független RTH-navigációt, ami különösen előnyös erősen zavart vagy ellenséges környezetben.[63] A jármű-jármű (*vehicle-to-vehicle,* V2V) kommunikációra épülő

[56] Hakeem et al. 2025.
[57] Alhoraibi–Alghazzawi–Alhebshi 2024; Asif et al. 2023.
[58] A tanulmányban a reziliencia a rendszer azon képességét jelenti, hogy részleges vagy teljes kompromittálódás esetén is képes biztonságos állapotba kerülni, illetve alapvető funkcióit fenntartani.
[59] Moosavi–Moore–Gopalswamy 2024.
[60] Poornima–Kumari 2025.
[61] Baba–Alothman–Khattab 2023; Sathiyanathn et al. 2024.
[62] Nair–Thampi–P. 2025.
[63] Fadheli–Khalid–Fadzil 2025.

kooperatív lokalizáció lehetőséget biztosít arra, hogy a drónok egymással együttműködve, megosztott információk alapján határozzák meg saját pozíciójukat, ezáltal pontosabb helyzetbecslést érjenek el *GPS-spoofing* támadások fennállása esetén is.[64]

Végül az adaptív antennarendszerek alkalmazása fizikai szinten is érdemben hozzájárul a reziliencia növeléséhez. A kétsávos, adaptív GPS-antennák – például egy 11 × 11 elemű egyenletes téglalap rácsú antennatömb (*uniform rectangular array,* URA) és a minimum varianciájú torzításmentes válasz (*minimum variance distortionless response,* MVDR) sugárformálási algoritmus kombinációja – lehetővé teszik az interferencia dinamikus elnyomását, valamint a hiteles és hamisított jelek elkülönítését, ezáltal hatékony védelmet biztosítanak a *GPS-spoofing* támadásokkal szemben.[65] A reziliencia növelése mellett kulcskérdés, hogy a rendszer milyen pontossággal és milyen késleltetéssel képes a *spoofing* események azonosítására. Ennek megfelelően a következőkben a *GPS-spoofing* detektálására alkalmazott gépi tanulási modelleket részletesebben tekintjük át.

Gépi tanuláson alapuló GPS-spoofing *detektálási módszerek*

A *GPS-spoofing* támadások detektálásában a gépi tanulási módszerek kiemelkedően hatékony eszközt jelentenek az autonóm drónrendszerek számára, mivel alkalmasak a navigációs jelek és a fedélzeti szenzoradatok finom szerkezeti mintázatainak feltárására, valamint a valós idejű döntéstámogatás biztosítására. A klasszikus megközelítések közé tartozik a támogatóvektor-gépek (*support vector machine,* SVM) alkalmazása, amelyek különböző jellemzők – így például a jel időbeli ingadozása *(jitter),* amplitúdóváltozása *(shimmer),* illetve frekvenciamodulációja – alapján végzik el a GPS-jelek osztályozását.[66] Az ilyen módszerek kiemelkedő pontosságot, precizitást, visszahívási arányt és F1-mutatót – vagyis a precizitás és a visszahívási arány harmonikus átlagát – tükröztek, ami alkalmassá teszi őket a hamisított GPS-jelek megbízható azonosítására. Az SVM-alapú eljárások hatékonysága különösen zajos vagy torzított adatkörnyezetben érvényesül, ahol a hiteles és a manipulált jelek elkülönítése fokozott kihívást jelent. A klasszikus osztályozók mellett a reprezentációtanulásra építő módszerek is elterjedtek, amelyeknél az eredmények gyakran *baseline*-ként vagy összehasonlításként jelennek meg más modellekkel szemben. Ilyen környezetben az SVM-alapú megoldások 99,8% feletti észlelési arányt értek el, ami jól alátámasztja a módszer robusztusságát és gyakorlati alkalmazhatóságát.[67]

Az autoenkódereken és logisztikus regresszión alapuló módszerek egy további jelentős irányt képviselnek. Ebben a megközelítésben az autoenkóderek a dimenziócsökkentés feladatát látják el, vagyis az adatok lényegi információtartalmának tömör reprezentációját állítják elő, amelyet ezt követően logisztikus regresszió segítségével osztályoznak. A módszert különböző adathalmazokon validálták, beleértve a Gauss-zajjal terhelt, valamint az osztályeloszlás szempontjából kiegyensúlyozatlan adatokat is. E megközelítések jellemzően automatikus tanulására építenek, csökkentve a kézi jellemzőválasztás szükségességét. Az időbeli összefüggések kezelésére alkalmas hosszú rövid távú memóriával

[64] Wang–Li–Wang 2025.
[65] Hossain–Islam 2025.
[66] Shafique–Mehmood–Elhadef 2021.
[67] Burns et al. 2023.

rendelkező (LSTM) autoenkóderek tovább bővítik ezt a megközelítést, mivel képesek a GPS-jelek és a kapcsolódó szenzoradatok időbeli mintázatainak elemzésére. Az LSTM-autoenkódereken alapuló rendszerek szintén magas pontosságot mutattak a *spoofolt* jelek felismerésében, különösen fokozatosan vagy dinamikusan kibontakozó támadások esetén.[68]

A több szenzor adatain alapuló észlelési megoldások közül kiemelkedik az észlelési adatokra épülő detektálás (*perception-data-based detection,* PerDet), amely különböző fedélzeti érzékelők – többek között gyorsulásmérők, giroszkópok, magnetométerek, GPS és barométerek – adatait integrálja. Ez a megközelítés képes ellensúlyozni az egyes szenzorok egyedi korlátait, és átfogóbb képet nyújt a drón tényleges állapotáról és mozgásáról. A PerDet módszer 99,69%-os észlelési arányt ért el, amely meghaladta számos korábbi megoldás teljesítményét, különösen összetett és változatos repülési környezetekben.[69]

A mélytanulási modellek további jelentős előrelépést hoznak a *GPS-spoofing* felismerésében. Az olyan komplex architektúrák, mint a BiLSTM-Attention-CNN modell, egyesítik a kétirányú LSTM-rétegeket, a figyelmi *(attention)* mechanizmusokat és a konvolúciós rétegeket annak érdekében, hogy egyszerre ragadják meg az adatok globális időbeli összefüggéseit és a lokális mintázatokat. Ez az integrált megközelítés a szakirodalomban jelenleg az egyik legjobb teljesítményt eredményezte a *GPS-spoofing* támadások detektálásában.[70]

A faalapú modellek *(tree-based model)* és a magyarázható mesterséges intelligencia (*explainable AI,* XAI) alkalmazása különösen fontos a gyakorlati bevezetés szempontjából. Az olyan algoritmusok, mint a Random Forest, az XGBoost, a CatBoost és a LightGBM, hatékonyan alkalmazhatók a *GPS-spoofing* felismerésére, amelyek közül az XGBoost bizonyult a legeredményesebbnek. Ez a modell 99,89%-os pontosságot ért el, miközben a SHAP-*(shapley additive explanations)* módszer lehetővé tette az egyes jellemzők hozzájárulásának értelmezését, ezáltal növelve a rendszer átláthatóságát és a felhasználói bizalmat.[71]

A teljesítménymutatók átfogó elemzése alapján megállapítható, hogy a bemutatott modellek többsége rendkívül magas pontosságot ért el, gyakran meghaladva a 99%-os szintet.[72] A precizitás, a visszahívási arány és az F1-mutató szintén következetesen magas értékeket hoztak, ami a detektálási képességek megbízhatóságát jelzi különböző támadási forgatókönyvek esetén is.[73] A valós idejű alkalmazhatóság szempontjából rendkívül kritikus a detektálási késleltetés kérdése. Egyes megoldások – például a *drone flight path controller* interfészt alkalmazó modellek – alacsony késleltetést demonstráltak, ami elengedhetetlen a gyors reakciót igénylő repülési környezetekben.[74]

A gyakorlati megvalósítás során fontos, hogy a modellek valós környezetből származó adatokon is igazolják hatékonyságukat. Az olyan rendszerek, mint a PerDet és a ConstDet, valós repülések során gyűjtött adatok felhasználásával történő tanítással és teszteléssel növelték gyakorlati relevanciájukat és megbízhatóságukat.[75] Emellett szimulációs környezetek – például a JMAVSim és a QGroundControl – alkalmazása lehetővé tette valósághű

68 Burns et al. 2023.
69 Wei–Wang–Sun 2022.
70 Yang–Oracevic–Dilek 2025.
71 Devkota–Devkota–Kandel 2025.
72 Burns et al. 2023; Devkota–Devkota–Kandel 2025; Shafique–Mehmood–Elhadef 2021; Yang–Oracevic–Dilek 2025.
73 Shafique–Mehmood–Elhadef 2021; Shafique et al. 2026.
74 Tucker–Nadeem–Pervez 2025.
75 Wei et al. 2022; Wei–Wang–Sun 2022.

GPS-spoofing forgatókönyvek előállítását a modellek fejlesztése és értékelése során.[76] Összességében megállapítható, hogy a különböző gépi tanulási megközelítések – az SVM-alapú módszerektől az autoenkódereken és LSTM-modelleken át a faalapú és mélytanulási architektúrákig – hatékony és megbízható eszköztárat biztosítanak a *GPS-spoofing* támadások felismerésére az autonóm drónrendszerek esetében, és megfelelő alapot teremtenek a valós idejű, biztonságkritikus alkalmazások számára.

Összegzés

Az autonóm és részben autonóm pilóta nélküli légi járművek fejlődése a technológiai konvergencia következményeként olyan összetett, kiber- és fizikai elemeket integráló autonóm rendszereket hozott létre, amelyekben a légi platform, a fedélzeti érzékelő- és vezérlőrendszerek, a földi irányítás, a kommunikációs kapcsolatok és a háttér-informatikai infrastruktúra szoros egységet alkotnak. E rendszerszintű összekapcsoltság következtében a drónok biztonsága nem értelmezhető kizárólag repülésbiztonsági kérdésként: az autonóm működés és a hálózati integráció miatt a kiberbiztonság a megbízható üzemeltetés alapvető tényezőjévé vált. A digitális térben végrehajtott támadások közvetlen működési zavarokat idézhetnek elő, amelyek szélsőséges esetben fizikai következményekben is megjelenhetnek, például az irányítás elvesztése, a navigációs döntések torzulása vagy a küldetés megszakadása révén.

A tanulmány szisztematikus szakirodalmi áttekintésre támaszkodva, rendszerszinten vizsgálta az autonóm drónrendszerek fenyegetési környezetét és a lehetséges védekezési megoldásokat. Az elemzés rámutatott arra, hogy a sérülékenységek több, egymással kölcsönhatásban álló rétegben jelentkeznek. A szoftveres komponensek esetében a jogosulatlan hozzáférés, a rosszindulatú kódok és a kihasználható hibák veszélyeztetik a vezérlési funkciókat és az adatkezelést. A hardveres és érzékelési láncban az érzékelők manipulálása, valamint a mesterséges intelligenciát célzó támadások torzíthatják a helyzetértékelést és az autonóm döntéshozatalt. Különösen kritikus a kommunikációs és navigációs réteg, mivel ezek kompromittálása gyorsan vezethet eltérítéshez, működésképtelenséghez vagy az autonóm funkciók hibás működéséhez. A kockázatokat tovább növelik a támogató informatikai infrastruktúra elleni műveletek, az adatok illetéktelen megszerzése vagy módosítása, illetve az ellátási lánc rejtett sérülékenységei.

A védekezés ebből következően nem redukálható egyetlen technikai megoldásra, hanem rétegezett, egymást kiegészítő technikai és szervezeti intézkedések integrált alkalmazását igényli. Alapvető szerepet kap a biztonságos kommunikáció és a hozzáférések szigorú kezelése, valamint a folyamatos monitorozás és anomáliaészlelés, amely lehetővé teszi a rendellenes működési minták korai felismerését. A bizalom minimalizálására és folyamatos hitelesítésre épülő biztonsági modellek, továbbá az adatintegritást és a nyomonkövethetőséget biztosító megoldások szintén meghatározó elemei a védelmi eszköztárnak. Az autonóm rendszerek sajátosságai miatt jelentősége van a redundanciának és a degradált üzemmódokra való felkészülésnek: a rendszernek támadás vagy zavar

[76] Yang–Oracevic–Dilek 2025.

esetén is képesnek kell lennie arra, hogy biztonságos állapotba kerüljön, illetve a kritikus funkciók fenntartására.

Ezen belül a navigációs megtévesztés súlyos fenyegetést jelent, mivel a helymeghatározási adatok sérülése közvetlen hatással van az útvonalkövetésre és az autonóm döntéshozatalra. A szakirodalom több, egymást erősítő megközelítést azonosít, így a jelés működésmintákon alapuló anomáliaészlelést, a szenzorfúziót és keresztellenőrzést, a vizuális információk bevonását, valamint a rádiófrekvenciás jellemzők elemzését. A hangsúly egyre inkább nem csupán a támadások felismerésén, hanem a reziliencia növelésén van, vagyis azon, hogy miként tartható fenn a biztonságos működés akkor is, ha a navigációs környezet tartósan kompromittált. Összességében a tanulmány azt támasztja alá, hogy az autonóm drónrendszerek kiberbiztonsági szintje akkor növelhető érdemben, ha a fenyegetéseket architektúraszinten kezeljük, és a megelőző, detektáló, valamint működésfenntartó mechanizmusokat integrált módon, a valós idejű működés és az erőforrás-korlátok figyelembevételével alkalmazzuk.

Felhasznált irodalom

Aldossary, Mohammad – Alzamil, Ibrahim – Almutairi, Jaber (2025): Enhanced Intrusion Detection in Drone Networks: A Cross-Layer Convolutional Attention Approach for Drone-to-Drone and Drone-to-Base Station Communications. *Drones,* 9(1), 46. Online: https://doi.org/10.3390/drones9010046

Alhoraibi, Lamia – Alghazzawi, Daniyal – Alhebshi Reemah (2024): Detection of GPS Spoofing Attacks in UAVs Based on Adversarial Machine Learning Model. *Sensors,* 24(18), 6156. Online: https://doi.org/10.3390/s24186156

Almadhor, Ahmad et al. (2025): CTDNN-Spoof: Compact Tiny Deep Learning Architecture for Detection and Multi-Label Classification of GPS Spoofing Attacks in Small UAVs. *Scientific Reports,* 15, 6656. Online: https://doi.org/10.1038/s41598-025-90809-3

Alquwayzani, Alanoud A. – Albuali, Abdullah A. (2024): A Systematic Literature Review of Zero Trust Architecture for Military UAV Security Systems. *IEEE Access,* 12, 176033–176056. Online: https://doi.org/10.1109/ACCESS.2024.3503587

Alsadie, Deafallah (2025): Cybersecurity and Artificial Intelligence in Unmanned Aerial Vehicles: Emerging Challenges and Advanced Countermeasures. *IET Information Security,* (1), 2046868. Online: https://doi.org/10.1049/ise2/2046868

Asif, Muneeba et al. (2023): Adversarial Data-Augmented Resilient Intrusion Detection System for Unmanned Aerial Vehicles. In *2023 IEEE International Conference on Big Data (BigData).* Sorrento, Italy, 5428–5437. Online: https://doi.org/10.1109/BigData59044.2023.10386140

Baba, Abdullatif – Alothman, Basil – Khattab, Omar (2023): Blockchain-Based Heuristic Study to Secure UAVs from GPS Spoofing Signals and External Attacks. In *2023 Fifth International Conference on Blockchain Computing and Applications (BCCA).* Kuwait, Kuwait, 377–379. Online: https://doi.org/10.1109/BCCA58897.2023.10338915

Basan, Elena et al. (2021): A Self-Diagnosis Method for Detecting UAV Cyber Attacks Based on Analysis of Parameter Changes. *Sensors,* 21(2), 509. Online: https://doi.org/10.3390/s21020509

Bhargavi, M. S. et al. (2025): Unlocking the Potential of Machine Learning for Enhanced Security in Drone-Enabled IoT Networks. In Hassan, Jahan – Khalifa, Sara – Misra, Prasant (szerk.): *Machine Learning for Drone-Enabled IoT Networks.* Cham: Springer, 107–120. Online: https://doi.org/10.1007/978-3-031-80961-3_6

Burns, Jaron et al. (2023): On Effectiveness of Machine and Deep Learning Algorithms for Detection of GPS Spoofing Attacks on Unmanned Aerial Vehicles. In *2023 Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE).* Las Vegas, NV, USA, 2405–2410. Online: https://doi.org/10.1109/CSCE60160.2023.00389

Buske, Ivo et al. (2022): Smart GPS Spoofing to Countermeasure Autonomously Approaching Agile Micro UAVs. In *High-Power Lasers and Technologies for Optical Countermeasures*. 62–67. Online: https://doi.org/10.1117/12.2636236

Connor, Roger (2018): The Predator, a Drone That Transformed Military Combat. *National Air and Space Museum,* 2018. március 9. Online: https://airandspace.si.edu/stories/editorial/predator-drone-transformed-military-combat

Damis, Haitham Abu et al. (2026): Emerging Cyber-Security Techniques for Unmanned Aerial Vehicles. In Fachkha, Claude – Fung, Benjamin C. M. – Tchakounté, Franklin (szerk.): *Safe, Secure, Ethical, Responsible Technologies and Emerging Applications.* Cham: Springer, 22–40. Online: https://doi.org/10.1007/978-3-032-05832-4_2

Davidovich, Barak – Nassi, Ben – Elovici, Yuval (2022): Towards the Detection of GPS Spoofing Attacks Against Drones by Analyzing Camera's Video Stream. *Sensors,* 22(7), 2608. Online: https://doi.org/10.3390/s22072608

Devkota, Bhawana Poudel – Devkota, Bidur – Kandel, Laxima Niure (2025): Leveraging Tree-Based Machine Learning and Explainable AI for UAV GPS Spoofing Detection. In *SoutheastCon 2025.* Concord, NC, USA, 340–345. Online: https://doi.org/10.1109/SoutheastCon56624.2025.10971719

Eldosouky, AbdelRahman – Ferdowsi, Aidin – Saad, Walid (2020): Drones in Distress: A Game-Theoretic Countermeasure for Protecting UAVs Against GPS Spoofing. *IEEE Internet of Things Journal,* 7(4), 2840–2854. Online: https://doi.org/10.1109/JIOT.2019.2963337

Fadheli, Hadjer – Khalid, Shamsul Kamal Ahmad – Fadzil, Lokman Mohd (2025): A Non-GPS Return to Home Algorithm for Drones Using Convolutional Neural Network. *Journal of Advanced Research in Applied Sciences and Engineering Technology,* 51(1), 15–27. Online: https://doi.org/10.37934/araset.51.1.1527

Hakeem, Abeer et al. (2025): Integrating Artificial Intelligence for Improved Security of IoT-Drones Through Cyber-Physical Attack Detection. *Frontiers in Computer Science,* 7, 1545282. Online: https://doi.org/10.3389/fcomp.2025.1545282

Hossain, Shaikat – Islam, Aminul (2025): Dual-Band Adaptive GPS Antennas for Real-Time Spoofing Mitigation. In *2025 International Conference on Electrical, Computer and Communication Engineering (ECCE).* Chittagong, Bangladesh, 1–5. Online: https://doi.org/10.1109/ECCE64574.2025.11013036

Ináncsi, Mátyás (2022): Cybersecurity Challenges of the Civilian Unmanned Aircraft Systems. *Hadmérnök,* 17(2), 205–216. Online: https://doi.org/10.32567/hm.2022.2.14

Jain, Meenal – Jain, Akshat – Sahoo, Anita (2024): Protective System for Drones Against GPS Spoofing Using Image and Signal Analysis. In *Proceedings of the 2024 Sixteenth*

International Conference on Contemporary Computing (IC3-2024). New York: Association for Computing Machinery, 384–389. Online: https://doi.org/10.1145/3675888.3676075

Javed, Muhammad Danyal et al. (2025): Cyber Security Framework for AI-Enabled Robotics and Drone Systems. In *Advancing Cybersecurity in Smart Factories Through Autonomous Robotic Defenses.* Hershey: IGI Global Scientific Publishing, 231–262. Online: https://doi.org/10.4018/979-8-3373-0583-7.ch009

Kiss Beatrix – Palik Mátyás (2023): A drónok katonai alkalmazása modern katonai műveletek során. *Repüléstudományi Közlemények,* 35(1), 115–130. Online: https://doi.org/10.32560/rk.2023.1.9

Krasznay Csaba – Ináncsi Mátyás (2021): Az UAV-ok kiberbiztonsági elemzésének és tanúsításának lehetőségei. *Felderítő Szemle,* 20(3), 63–79.

Laraib, Areeba – Sial, Areesha – Ujjan, Raja Majid Ali (2024): Addresses the Security Issues and Safety in Cyber-Physical Systems of Drones. In Shah, Imdad Ali – Jhanjhi, Noor Zaman (szerk.): *Cybersecurity Issues and Challenges in the Drone Industry.* Hershey: IGI Global Scientific Publishing, 381–404. Online: https://doi.org/10.4018/979-8-3693-0774-8.ch016

Lee, Ho-Sung – Kim, Jong-Bae (2019): Analysis of Cyber Attack Using Drones and Its Countermeasure Strategy. *Journal of Advanced Research in Dynamical and Control Systems,* 11(5), 281–289.

Liang, Chen et al. (2019): Detection of GPS Spoofing Attack on Unmanned Aerial Vehicle System. In Chen, Xiaofeng – Huang, Xinyi – Zhang, Jun (szerk.): *Machine Learning for Cyber Security.* Cham: Springer, 123–139. Online: https://doi.org/10.1007/978-3-030-30619-9_10

Liang, Chen et al. (2022): Detection of Global Positioning System Spoofing Attack on Unmanned Aerial Vehicle System. *Concurrency and Computation: Practice and Experience,* 34(7), e5925. Online: https://doi.org/10.1002/cpe.5925

Maqbool, Albia et al. (2024): Proactive Cyber Defense and Forensic Investigation Techniques for Drone Operation: A Holistic Approach. *Journal of Theoretical and Applied Information Technology,* 102(18), 6697–6709.

Meng, Lianxiao et al. (2021): An Approach of Linear Regression-Based UAV GPS Spoofing Detection. *Wireless Communications and Mobile Computing,* (1), 5517500. Online: https://doi.org/10.1155/2021/5517500

Moosavi, Samin – Moore, Isabel – Gopalswamy, Swaminathan (2024): Using a Sensor-Health-Aware Resilient Fusion for Localization in the Presence of GPS Spoofing Attacks. In *2024 IEEE International Conference on Cyber Security and Resilience (CSR).* London, United Kingdom, 498–505. Online: https://doi.org/10.1109/CSR61664.2024.10679455

Mykytyn, Pavlo et al. (2023): GPS-Spoofing Attack Detection Mechanism for UAV Swarms. In *2023 12th Mediterranean Conference on Embedded Computing (MECO).* Budva, Montenegro, 1–8. Online: https://doi.org/10.1109/MECO58584.2023.10154998

Mynuddin, Mohammed – Khan, Sultan Uddin – Mahmoud, Mahmoud Nabil (2023): Trojan Triggers for Poisoning Unmanned Aerial Vehicles Navigation: A Deep Learning Approach. *2023 IEEE International Conference on Cyber Security Resilience (CSR).* Venice, Italy, 432–439. Online: https://doi.org/10.1109/CSR57506.2023.10224932

Mynuddin, Mohammed et al. (2024): Trojan Attack and Defense for Deep Learning-Based Navigation Systems of Unmanned Aerial Vehicles. *IEEE Access,* 12, 89887–89907. Online: https://doi.org/10.1109/ACCESS.2024.3419800

Nair, Aiswarya S. – Thampi, Sabu M. – P., Jithu Vijay V. (2025): SoCoMNNet: A SocioCognitive and Memristive Neural Network-Based Context-Aware GPS Spoofing Detection and Mitigation in the Internet of Drones. *Vehicular Communications,* 56, 100980. Online: https://doi.org/10.1016/j.vehcom.2025.100980

Nascimento Aquilar Pey, Jeferson – Daniel Amvame Nze, Georges – Oliveira Albuquerque, Robson de (2022): Analysis of Jamming and Spoofing Cyber-Attacks on Drones. In *2022 17th Iberian Conference on Information Systems and Technologies (CISTI).* Madrid, Spain, 1–4. Online: https://doi.org/10.23919/CISTI54924.2022.9820201

Oracevic, Alma – Salman, Ahmad (2024): Unmanned Aerial Vehicles in Peril: Investigating and Addressing Cyber Threats to UAVs. In *2024 International Conference on Smart Applications, Communications and Networking, SmartNets*. Harrisonburg, VA, USA, 1–7. Online: https://doi.org/10.1109/SmartNets61466.2024.10577710

Orye, Erwin et al. (2024): Enhancing the Cyber Resilience of Sea Drones. In *2024 16th International Conference on Cyber Conflict: Over the Horizon (CyCon).* Tallinn, Estonia, 83–102. Online: https://doi.org/10.23919/CyCon62501.2024.10685581

Poornima, B. – Kumari, Lalitha Surya (2025): Mitigating GPS Spoofing in AVS: SHA and RSA Algorithms With Proteus Simulation for Real-Time Detection. *International Journal of System Assurance Engineering and Management,* 16(10), 3375–3389. Online: https://doi.org/10.1007/s13198-025-02864-8

Prasanna Srinivasan, S. – Sathyadevan, Shiju (2023): GPS Spoofing Detection in UAV Using Motion Processing Unit. In *2023 11th International Symposium on Digital Forensics and Security (ISDFS).* Chattanooga, TN, USA, 1–4. Online: https://doi.org/10.1109/ISDFS58141.2023.10131729

Ranganathan, Aanjhan – Ólafsdóttir, Hildur – Capkun, Srdjan (2016): SPREE: A Spoofing Resistant GPS Receiver. In *Proceedings of the 22nd Annual International Conference on Mobile Computing and Networking.* New York: Association for Computing Machinery, 348–360. Online: https://doi.org/10.1145/2973750.2973753

Renu, Yuvaraj – Sarveshwaran, Velliangiri (2025): A Review of Cyber Security Challenges and Solutions in Unmanned Aerial Vehicles (UAVs). *Inteligencia Artificial,* 28(75), 199–219. Online: https://doi.org/10.4114/intartif.vol28iss75pp199-219

Sarkar, Arupa et al. (2024): Smart Verification of Unmanned Aerial Vehicle GPS Geolocation via Received Signal Strength Indicators. In *2024 IEEE 100th Vehicular Technology Conference (VTC2024-Fall).* Washington, DC, USA, 1–6. Online: https://doi.org/10.1109/VTC2024-Fall63153.2024.10757631

Sathiyanathn, S. et al. (2024): Blockchain Integrated Framework to Detect and Prevent CAV Location Spoofing Attack Using GPS Time Series Data Learning and Quantum Cryptography. In *2024 2nd International Conference on Artificial Intelligence and Machine Learning Applications Theme: Healthcare and Internet of Things (AIMLA).* Namakkal, India, 1–7. Online: https://doi.org/10.1109/AIMLA59606.2024.10531539

Shafik, Wasswa – Mojtaba Matinkhah, S. – Shokoor, Fawad (2023): Cybersecurity in Unmanned Aerial Vehicles: A Review. *International Journal on Smart Sensing and Intelligent Systems,* 16(1), 1–16. Online: https://doi.org/10.2478/ijssis-2023-0012

Shafique, Arslan – Mehmood, Abid – Elhadef, Mourad (2021): Detecting Signal Spoofing Attack in UAVs Using Machine Learning Models. *IEEE Access,* 9, 93803–93815. Online: https://doi.org/10.1109/ACCESS.2021.3089847

Shafique, Arslan et al. (2026): Protecting Autonomous Systems From GPS Spoofing With a Machine Learning-Driven Approach. *Ad Hoc Networks,* 183, 104101. Online: https://doi.org/10.1016/j.adhoc.2025.104101

Shariat, Mahyar et al. (2025): UWB-Based Positioning Is Not Invulnerable From Spoofing Attacks: A Case Study of Crazyswarm. *Engineering Proceedings,* 88(1), 43. Online: https://doi.org/10.3390/engproc2025088043

Singh, Ratan – Chandra Mohan, B. – Golda Jeyasheeli, P. (2023): Recent Research and Implementation on Various GPS Spoofing Attacks and Prevention. In *2023 6th International Conference on Recent Trends in Advance Computing (ICRTAC).* Chennai, India, 509–515. Online: https://doi.org/10.1109/ICRTAC59277.2023.10480748

Sissodia, Rajeshwari et al. (2025): Introduction to Artificial Intelligence (AI) and Cybersecurity in Robotics and Drone Systems. In Kumar, Rajeev et al. (szerk.): *Advancing Cybersecurity in Smart Factories Through Autonomous Robotic Defenses*. Hershey: IGI Global Scientific Publishing, 345–374. Online: https://doi.org/10.4018/979-8-3373-0583-7.ch013

Sree Lakshmi, P. et al. (2025): Securing the Future of Transportation: A Deep Dive Into Cybersecurity for Autonomous Vehicles. In Bhateja, Vikrant – Dey, Maitreyee – Simic, Milan (szerk.): *Intelligent Computing and Automation.* Singapore: Springer, 275–285. Online: https://doi.org/10.1007/978-981-96-0143-1_22

Tiwari, Vinita et al. (2023): Mitigation of Jamming and Spoofing Attack on GNSS Signals Using Subspace Projection. In *2023 3rd International Conference on Emerging Frontiers in Electrical and Electronic Technologies (ICEFEET).* Patna, India, 1–6. Online: https://doi.org/10.1109/ICEFEET59656.2023.10452226

Tucker, Rajanbir Singh – Nadeem, Muhammad – Pervez, Shahbaz (2025): Real-Time Detection and Mitigation of GPS Spoofing in UAV Systems. In *2025 12th International Conference on Information Technology (ICIT).* Amman, Jordan, 154–160. Online: https://doi.org/10.1109/ICIT64950.2025.11049153

Wang, Zhuang – Li, Guoqiang – Wang, Zhenpo (2025): GPS Attack Detection and Defense for Secure Localization of Automated Vehicles Based on Vehicle-to-Vehicle Technology. *IEEE Internet of Things Journal,* 12(7), 7723–7735. Online: https://doi.org/10.1109/JIOT.2024.3424518

Wei, Xiaomin et al. (2022): ConstDet: Control Semantics-Based Detection for GPS Spoofing Attacks on UAVs. *Remote Sensing,* 14(21), 5587. Online: https://doi.org/10.3390/rs14215587

Wei, Xiaomin – Wang, Yao – Sun, Cong (2022): PerDet: Machine-Learning-Based UAV GPS Spoofing Detection Using Perception Data. *Remote Sensing,* 14(19), 4925. Online: https://doi.org/10.3390/rs14194925

Yang, Ming – Oracevic, Alma – Dilek, Selma (2025): Deep Learning-Based Defense Against GPS Spoofing Attacks in Unmanned Aerial Vehicles. In *2025 International Conference on Smart Applications, Communications and Networking, (SmartNets).* Istanbul, Turkiye, 1–8. Online: https://doi.org/10.1109/SmartNets65254.2025.11106869

NEMZETBIZTONSÁGI SZEMLE
14. évfolyam (2026) 1. szám 23–35. | DOI: 10.32561/nsz.2026.1.2

Solti István[1]

A nemzetbiztonsági szolgálatokról szóló törvény előképei

Precursors to the National Security Services Act

A tanulmányban a szerző a 30 évvel ezelőtt, 1995-ben elfogadott, majd 1996-ban hatályba lépett, a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvényt (Nbtv.) megelőző jogszabályok fontosabb jellemzőit vizsgálja. A szerző a hazai nemzetbiztonsági szolgálatokat és tevékenységeiket 1990-től 1996-ig szabályozó két ideiglenes jogszabály, az 1990. évi X. törvény és a 26/1990. (II. 14.) MT rendelet keletkezésének körülményeit, szabályozásának tárgyait és az egyes jogintézmények jogállami kereteknek való megfelelését vizsgálja.

Ennek során bemutatja a rendszerváltáskor meglévő politikai elvárások jogszabályi megoldásait, az átfogó szabályozást nyújtó állandó törvény megalkotására vonatkozó terveket, majd a kiadott jogszabályok életútját. Tekintettel arra, hogy a napjainkban is hatályos Nbtv. megalkotása és elfogadása 30 éve történt, amelynek tartalmára és szellemiségére az általa felváltott jogszabályok alkalmazhatósága is hatással volt, a szerző fontosnak tartja kimutatni a folytonosságot meghatározó jogszabályi elemeket.

Kulcsszavak: *állambiztonság, nemzetbiztonság, titkosszolgálat, hírszerzés, elhárítás, titkos információgyűjtés*

In this study, the author examines the most important features of the legislation that preceded Act CXXV of 1995 on National Security Services (Nbtv.), which was adopted 30 years ago in 1995 and entered into force in 1996. The author examines the circumstances surrounding the creation of two provisional laws regulating domestic national security services and their activities from 1990 to 1996, Act X of 1990 and Council of Ministers Decree 26/1990 (II.14.), and the subjects of their regulation, as well as the compliance of individual legal institutions with the rule of law.

In doing so, he presents the legislative solutions to the political expectations that existed at the time of the regime change, the plans for the creation of a permanent

[1] PhD, adjunktus, Nemzeti Közszolgálati Egyetem Rendészettudományi Kar, e-mail: solti.istvan@uni-nke.hu

law providing comprehensive regulation, and then the life cycle of the legislation that was enacted.

Given that the Nbtv., which is still in force today, was created and adopted 30 years ago, and that its content and spirit were also influenced by the applicability of the legislation it replaced, the author considers it important to highlight the legislative elements that determine continuity.

Keywords: *state security, national security, secret service, intelligence, counterintelligence, secret information gathering*

A rendszerváltás kora

Magyarországon a nemzetbiztonsági szolgálatok és a rendészeti szervek titkos információgyűjtő tevékenységének első, a jogállami követelményeknek megfeleltethető jogi szabályozására 1990-ben került sor. Az Országgyűlés rövid előkészítés és vita után 1990. január 25-én fogadta el a különleges titkosszolgálati eszközök és módszerek engedélyezésének átmeneti szabályozásáról szóló 1990. évi X. törvényt. A törvény 1990. február 14-én lépett hatályba.

Terjedelmét tekintve az 1990. évi X. törvény rendkívül rövid volt, mindösszesen kilenc szakaszt tartalmazott. A jogszabályt – ahogy a címében is szerepelt – ideiglenesnek, néhány hónapi szabályozásra szánták. Az ideiglenességnek politikai okai voltak: a karácsonyi és újévi ünnepek ideje alatt kirobbant a Dunagate-botrány,[2] aminek következtében az akkori országgyűlés szükségesnek látta, hogy a lehető leghamarabb szülessen meg egy, a nemzetbiztonsági szolgálatokat szabályozó törvény, még annak árán is, hogy egy minimalista jogszabály jön létre. Azzal együtt is indokoltnak látta ezt a törvényhozás, hogy az 1989. október 23-án kihirdetett módosított Alkotmány előírta a Minisztertanács számára, hogy 1990. április 30-ig készítse elő és nyújtsa be a Parlamentnek azokat a sarkalatos törvényeket, amelyek alapjogi rendezettsége nem felelt meg a jogállami követelményeknek.

A nemzetbiztonsági tevékenységre 1990–1991 fordulóján nem volt nyilvános jogszabályi hierarchiában megtalálható norma. Ugyan a kormányzati álláspont szerint az állambiztonság és a rendőrség tevékenységét egyaránt egy 1974-es törvényerejű rendelet határozta meg,[3] azonban – ahogy azt a Belügyminisztérium államtitkára is elismerte – a jogszabály az általánosítás olyan magas szintjén mozgott, ami csak a szocializmus idején volt elfogadott. Ez egy olyan keretjogszabály volt, amelyet alsóbb szintű normák, az állambiztonság esetében államtitoknak minősített 6000-es kormányhatározatok és az erre épülő miniszterelnök-helyettesi utasítások töltöttek ki.[4]

Az államtitkár megállapítását két észrevétellel szükséges kiegészíteni. Egyfelől a felhívott 1974. évi 17. törvényerejű rendelet nem is keretjogszabály volt, hiszen általánosságban hatalmazta fel a Belügyminisztériumot, hogy derítsen fel minden, az állam belső

[2] Nyilvánosságra került 1990 első napjaiban, hogy a magyar állambiztonsági szolgálat az alkotmányos rendelkezésekkel ellentétesen, titkos eszközökkel és módszerekkel megfigyeli az ellenzéki pártokat és szervezeteket. Révész 2004.

[3] 1974. évi 17. törvényerejű rendelet az állam- és közbiztonságról.

[4] Az Országgyűlés 74. ülése 1990: 6134.

rendjét veszélyeztető magatartást, legyen az köztörvényes bűncselekmény vagy az állam ellen irányuló bármilyen leplezett tevékenység. Ehhez a Belügyminisztérium keretében három szervet határozott meg: a Rendőrséget, a Határőrséget és a Tűzoltóság Országos Parancsnokságát. Mindezt úgy, hogy 1962-től, a belügyminisztériumi főcsoportfőnöki struktúra felállításától kezdve az állambiztonsági szolgálat nem a rendőrség részeként, hanem külön főcsoportfőnökségként működött a Belügyminisztérium szerveként. A jogszabály erről a tényről mégis hallgatott. Másfelől azt is hozzátehetjük, hogy a rendelet rendelkezésével ellentétben a szolgálat szervezeti és feladatrendszerét, valamint az alkalmazható eszközöket és módszereket nem miniszterelnöki utasításokban, hanem belügyminiszteri és belügyminiszter-helyettesi titkos minősítéssel ellátott utasításokban és parancsokban szabályozták.

Az átmeneti jogszabály elfogadását a kormány képviselői is támogatták a parlamenti vita alatt, abban a tudatban, hogy a végleges törvényi megoldás belátható időn belül megérkezik. Horváth István belügyminiszter lemondásának bejelentésekor arról beszélt,[5] hogy a Minisztertanács kabinetje már jóváhagyta az állambiztonsági munka részletes szabályozására vonatkozó koncepciót 1989. július 3-án. Ebben megfogalmazták, hogy a végleges jogszabályban a törvényesség követelményének megfelelően az alkalmazható módszereket, eszközöket törvényi szinten szabályozzák, az ellenőrzésük pedig később a Parlament hatáskörébe kerül. A koncepciót a rendszerváltás politikai egyeztető tárgyalásain bemutatták, és beszámoltak a törvény előkészítésének megindulásáról.[6]

Azonban a tervezet az 1990 fordulóján bekövetkezett események idején nem lehetett megfelelően kiérlelt állapotban, minthogy csak egy ideiglenesnek szánt, rövid törvény megalkotására kerülhetett sor. A beterjesztő az ideiglenes törvény elfogadhatóságát azzal is alátámasztotta a parlamenti vitában, hogy hangsúlyozta: a Kormány elkészítette a végleges törvénytervezetet, amiről napokon belül konzultációt kezdeményez a pártokkal, majd pedig benyújtja az Országgyűlés februári ülésszakára.[7]

Azonban az események nem a parlamenti vitában elhangzottak szerint alakultak. Ugyan az ideiglenes törvényt sarkalatos jogszabályként a Parlament elfogadta, az ezt felváltó részletes törvény benyújtására és elfogadására nemhogy a meghatározott határidőig, hanem még évekig nem került sor. Az 1990. évi X. törvény több mint hat évig biztosította a nemzetbiztonsági szolgálatok működésének törvényi alapjait.

Az 1990. évi X. törvény szabályozási területei

A törvény ideiglenesnek szánt jellegét az is jól mutatja, hogy egy olyan alaki jogszabály volt, amelynek tárgyát a szolgálatok különleges eszköztárának a szabályozása adta, amit a parlament úgy fogadott el, hogy jogszabályi szinten nem ismerhette az új nemzetbiztonsági struktúrát. Ennek kialakítására ugyanis a törvény hatálybalépésének napján kiadott alacsonyabb szintű rendelkezésben, a 26/1990. (II. 14.) MT rendeletben (Rendelet) került sor. Vagyis ez a törvény nem foglalkozott az új nemzetbiztonsági szolgálatok struktúrájával,

[5] Horváth István belügyminiszter 1990. január 23-án jelentette be a lemondását a Dunagate-botrány kirobbanása miatt.
[6] Horváth István lemondásából részlet. Az Országgyűlés 73. ülése 1990: 6049.
[7] Az Országgyűlés 74. ülése 1990: 6136.

szervezet- és feladatrendszerével, irányításával és vezetésével, a szolgálatok és működésük ellenőrzési mechanizmusaival, a személyes adatok kezelésével, csupán a titkos eszközök és módszerek alkalmazására feljogosított nemzetbiztonsági szervek titkos információgyűjtő tevékenységére határozott meg alapvető szabályokat.

Azt azért kijelenthetjük, hogy e jogszabály jelentősége vitathatatlan a tekintetben, hogy a nemzetbiztonsági szféra számára jogállami keretek között első alkalommal állapított meg olyan új jogintézményeket és szabályozási alapelveket, amelyek addig ismeretlenek voltak a hazai jogrendszerben. Így:

- elismerte, hogy a szolgálatok titkos tevékenységei alapvető emberi jogokat érintenek;
- jogintézményként bevezette a különleges titkosszolgálati eszközöket;
- alkotmányos alapelveket ültetett át szabályozási szintre a nemzetbiztonsági tevékenységek korlátjaiként;
- bevezette a titkos információgyűjtés eljárásába a végrehajtó szervtől független, külső engedélyezés intézményét.

Viszont az ideiglenes jellegből és a sietős kidolgozásból adódóan alapvető hiányosságokban szenvedett a norma, amelyek akár annak hatályosulását is negatívan befolyásolhatták volna.

A norma az 1. § (1) bekezdésében felhatalmazta a titkosszolgálatokat, hogy az e törvényben meghatározottak szerint különleges titkosszolgálati eszközöket és módszereket alkalmazhatnak. A szakasz itt titkosszolgálatokat említett, holott a magyar jogrendszer szerint nem léteztek titkosszolgálatok. Maga az 1990. évi X. törvény módosította az 1974-es törvényerejű rendeletet, a módosítás pedig nemzetbiztonsági szolgálatokat említett, mint amelyek a továbbiakban az állam elleni leplezett törekvésekkel szemben voltak hivatottak fellépni. A Rendelet sem hozott létre titkosszolgálatokat február 14-én, hanem nemzetbiztonsági szolgálatot, információs szolgálatot, katonai biztonsági szolgálatot és katonai felderítő szolgálatot. Ugyan a Rendelet a szervek hivatalos megnevezését nem állapította meg, de titkosszolgálatoknak sem minősítette a létrejött nemzetbiztonsági szolgálatokat.

A törvény a (2) bekezdésében határozta meg a különleges eszköz fogalmát, amelynek két fogalmi elemét különböztette meg. Különleges eszköznek minősült minden olyan eszköz és módszer,

- amelyet az érintett személy tudta nélkül alkalmaztak;
- amelynek használata a magánlakás sérthetetlenségéhez, valamint a magántitok, a levéltitok és a személyes adatok védelméhez fűződő jogokat sérthette.

Eszerint a nemzetbiztonsági szolgálatok azon intézkedései és tevékenységei minősültek különleges eszköz alkalmazásának, amelyeket olyan eljárásban folytattak, amelyről sem az eljárással érintett személy, sem pedig annak környezete nem szerezhetett tudomást az eljárás megindításától kezdve egészen annak lezárásáig. A különleges eszköz minősítésének másik szükséges eleme volt, hogy fennálljon a felsorolt alapjogsérelmek valamelyikének legalább a veszélye. A fogalmi elemnek nem képezte részét a lehetséges sérelem mértéke, illetve a jogsérelem megvalósulása. Akár a távoli és csekély jogsérelem is megalapozta a különleges eszköz minősítést. A fogalom meghatározása azt is jelentette, hogy a nemzetbiztonsági szolgálatok minden más formában folytatott információgyűjtést egyébként az általános adatkezelési jogszabályi rendelkezések mentén végezhettek. Vagyis az érintettől közvetlenül vagy az érintett tudomásával történő adatgyűjtés, a nyílt forrásokból

és az érintett által nyilvánosságra hozott személyes adatoknak a gyűjtése, az állami és nem állami nyilvántartásokból és adatbázisokból származó adatok gyűjtése nem esett e törvény hatálya alá.

A norma hiányosságaként említhetjük, hogy a fogalmi meghatározáson túl nem konkretizálta a különleges eszközök körét, amivel a jogalkalmazó számára a törvényesség elvével ellentétesen széles diszkrecionális jogkört biztosított. Eszerint a nemzetbiztonsági szolgálatok tevékenységük során bármely, már korábban is alkalmazott titkos eszközt továbbra is igénybe vehettek azokon kívül, amelyeket egyébként az Alkotmány az emberi élet és méltóság sérthetetlensége miatt nem tiltott. Így például a titkos előállítás, a titkos letartoztatás és a tortúraeszközök tilalma nem az 1990. évi X. törvényből, hanem közvetlenül az Alkotmányból következett. Vagyis azzal, hogy az új szabályozási környezet nem tartalmazta a különleges eszközök taxatív felsorolását, az állampárti időszakban rendszeresített titkos eszközök közül az említetteken kívül valamennyi alkalmazásban maradhatott, csupán az alkalmazásra a felhatalmazást nyilvánosan megismerhető, nem pedig titkos jogszabályban tette meg.

A törvény 1. § (3) bekezdésében és 2. §-ában két alkotmányos alapelv jelent meg, a szükségesség és a célhoz kötöttség elve. A szükségesség értelmében különleges eszközök alkalmazására csak abban az esetben kerülhetett sor, ha a nemzetbiztonsági szolgálatok a feladataik teljesítéséhez szükséges adatokat és információkat nem szerezhették be olyan információszerző eljárásban, amely az érintett tudtával történt, vagy nem járt a felsorolt alapjogok sérelmével. Ezzel az első szabályozás még nem vezette be a szigorú szükségesség alapelvét a gyakorlatba, az egyes alkalmazások során a többszintű szükségesség vizsgálatát még nem várta el.

A célhoz kötöttség körében már konkrétabb megfogalmazások születtek, hiszen hat pontban sorolta fel azokat a célokat, amelyek érvényre juttatása során alkalmazhatók lettek a különleges eszközök. Ezek között megtalálhatók voltak az állam gazdasági és honvédelmi érdekei, az érdekérvényesítés és a felderítés-elhárítás színterei, valamint konkrétabb célként a nemzetbiztonsági védelmi feladatok teljesítése, illetve egyes súlyos társadalmi veszélyt jelentő bűncselekmények felderítése. Fontos hangsúlyozni, hogy e szakaszában a törvény a különleges eszközök alkalmazásának a jogalapjait teremtette meg, nem pedig a nemzetbiztonsági szolgálatok számára határozott meg feladatot. Vagyis e cél meghatározása nem jelentette azt, hogy a nemzetbiztonsági szolgálatoknak a megadott bűncselekmények gyanújának észlelésekor mindenkor eljárási kötelezettsége keletkezett volna. Eljárási kötelezettségük abban az esetben állt fenn, ha az adott szolgálat számára a Rendeletben meghatározott feladatának körében merült fel adott bűncselekménynek akár a legalacsonyabb szintű gyanúja is.

A továbbiakban e rövid törvény egyik fontos, napjainkra sokat vitatott újítását említhetjük, a külső engedélyezés intézményét, hiszen a 3. §-t három különböző okból érdemes kiemelni:

- megnevezett három különleges eszközt, a technikai úton történő adatgyűjtést, a postai küldemény ellenőrzését és a magánlakásba történő titkos behatolást;
- a nyilvános szabályozásba bevezette az arányosság elvét;
- bevezette az ellenőrzési mechanizmus egyik fontos elemét, a külső engedélyezés intézményét.

Mivel az átmeneti törvény a három megnevezett különleges eszköz tartalmi meghatározását nem tette meg, így a napi gyakorlat, a végrehajtó nemzetbiztonsági szolgálatok és az engedélyező igazságügyi miniszter feladatául hagyta a részletek kidolgozását.[8]

Komoly értelmezési problémát vetett fel *a technikai úton történő adatgyűjtés,* hiszen mégis mely információgyűjtő eszközöket kellett technikainak tekinteni?

Ha a jogszabály célja szerinti teleológiai értelmezést végezzük el, akkor minden olyan információgyűjtés beleérthető volt, amit a szolgálatok adatok rögzítésére vagy magatartások megfigyelésére alkalmas technikai eszközök igénybevételével és nem csupán humán erőforrás segítségével hajtottak végre. Eszerint e körbe voltak sorolhatók többek között olyan kevésbé jogkorlátozó eszközök is, mint a rádiófelderítés, illetve a fényképezőgépet, videókamerát, éjjellátót vagy hőkamerát használó konspirált figyelés. Vagy akár idetartozhatott a konspirált környezettanulmány is, amennyiben a művelet során elhangzottakról a végrehajtó állomány hang, álló- vagy mozgókép rejtett rögzítésére alkalmas műszaki berendezéssel a helyszínen felvételt készített.

Ha a jogszabály történeti értelmezését végezzük el, akkor azt az eredményt kapjuk, hogy a korábbi állambiztonsági terminológia szerinti operatív-technikai rendszabályok és operatív-technikai módszerek tartoztak a körbe: a telefonlehallgatás, a szobalehallgatás, a helyiség vizuális megfigyelése, illetve a zártechnika alkalmazása és a dokumentáló képrögzítés.

A rádió-ellenőrzéssel kiegészítve ugyanerre az eredményre jutunk a kifejezés nyelvtani értelmezése alapján, hiszen azok a titkos eszközök tartoztak ide, ahol az információ megszerzése technikai eszköz *útján* történt meg.

A *postai küldemény ellenőrzése* a nemzetbiztonsági szolgálatok egy meghatározott személy által vagy számára postai forgalomban feladott levél- és csomagküldemény roncsolásmentes felnyitását, tartalmának ellenőrzését és dokumentálását jelentette. A továbbiakban a szolgálatoknak nem volt lehetőségük levélküldemények elkobzására, hírigény alapján küldeménycsoportok feldolgozására, konkrét cél nélküli általános levélellenőrzésre és halászó jellegű figyelésre.[9]

Az előző két információgyűjtő módszerrel ellentétben a *magánlakásba történő titkos behatolás* különleges eszköz volt, de nem volt információgyűjtő módszer. Egy helyiségbe bemenetelnek nem volt információs értéke. A helyiségbe történő leplezett vagy titkos bemenetel annak feltétele volt, hogy ott a szolgálatok az információgyűjtő vagy egyéb tevékenységüket előkészítsék, elvégezzék. Ez a különleges eszköz tehát egy olyan eszközcselekmény, amely súlyosan sérti az egyénnek a magánlakás sérthetetlenségéhez való jogát, sértheti vagy veszélyeztetheti más alapjogát, viszont feltétele lehet egyes titkosszolgálati tevékenységek sikerének.

Az arányosság elve mentén a megnevezett különleges eszközök kizárólag a Magyar Köztársaság szuverenitásának és alkotmányos rendjének súlyos veszélyeztetése esetén voltak bevethetők. Fontos kiemelni, hogy az arányosság követelményét e törvény csupán a külső engedélyköteles különleges eszközök esetében fogalmazta meg, az nem vonatkozott a nemzetbiztonsági szolgálatok teljes titkos tevékenységére. Ha ezt összevetjük a célhoz kötöttségnél kiemelt tárgykörökkel, akkor olyan további korlátozott jogköröket látunk, ahol a súlyosság megítélése jogalkalmazói kérdés maradt.

[8] Solti 2020: 44–61.
[9] Hetesy 2011: 70.

A rövid törvény 4. §-a tartalmazta az igazságügyi miniszteri engedélyezés eljárási szabályait, ahol az engedélyező személye komoly politikai vita után lett kijelölve. A Parlament elé benyújtott törvényjavaslat a külső engedélyező személyére két alternatív változatot tartalmazott. Az A változat szerint a legfőbb ügyész, a B változat szerint egy később megválasztandó országgyűlési biztos engedélyezhette volna a különleges eszközök alkalmazását. Az Országgyűlés jogi, igazgatási és igazságügyi, valamint honvédelmi bizottsága a legfőbb ügyészi engedélyezést támogatta, azonban egyik változat sem kapta meg az alkotmányos törvény elfogadásához elegendő többséget, ami a megválasztott képviselők kétharmadának szavazatát jelentette. Az Országgyűlés elnöke így kénytelen volt visszautalni a bizottságoknak a javaslatot és a végszavazást a következő parlamenti ülésnap napirendjébe.[10]

A következő napi ülésen, 1990. január 25-én a jogi, igazgatási és igazságügyi bizottság, valamint a honvédelmi bizottság több újonnan felmerült lehetőség mérlegelése után végül az eredeti álláspontja mellett maradt. Indoklása szerint az engedélyezési jogosultságot olyan személyhez kellett rendelni, aki közvetlen parlamenti irányítás alatt álló személy volt. A Magyar Köztársaság legfőbb ügyészét a Parlament választotta, neki beszámolni tartozott, interpellálható és visszahívható volt, jogosítványait közvetlenül a Parlamenttől kapta. Az Országgyűléshez tartozó hatalmi ág közvetlen irányítása alatt állt, a Magyar Köztársaság alkotmánya szerint egy pártsemleges szervezet élén. A bizottsági javaslat azonban nem nyerte el a képviselők megfelelő szintű támogatását, mert egy részük a legfőbb ügyész Dunagate-ügyben folytatott tevékenységének pártatlanságával és szakmaiságával nem volt elégedett. A kialakult patthelyzet megoldását Németh Miklós miniszterelnöknek a vitában tett javaslata jelentette. Felvetette, hogy az engedélyező személy az átmeneti időre az igazságügyi miniszter legyen. A Németh-kormányban Kulcsár Kálmán széles körben elismert jogászprofesszor töltötte be a miniszteri pozíciót, akinek személye valamennyi fél számára garanciát jelentett az engedélyezés szakmaiságára, amit az Országgyűlés még aznap elfogadott.[11]

Az 1990. évi X. törvény értelmében az engedély iránti kérelmet a szolgálatok vezetői terjeszthették írásban elő, amit részletesen indokolni kellett. Az indoklásnak érintenie kellett, hogy az alkalmazására a nemzetbiztonsági szolgálatok alapvető funkciói mentén, a szükségesség elvének betartásával és a meghatározott szervezeti célok végrehajtása érdekében került sor. A súlyos érdeksérelem írásbeli indoklását a jogszabály nem tette a kérelem kötelező részévé, csak – mint ahogy a 3. §-nál fentebb megjegyeztük – az engedélyező számára határozta meg mérlegelendő körülményként. Az engedélyt írásban, legfeljebb 30 napra lehetett megadni, ami további egy hónapra volt meghosszabbítható.

A különleges eszközök utolsó eljárási elemeként a törvény 5. §-a az alkalmazás megszüntetésének eseteit fogalmazta meg, illetve adatkezelési feladatot és értesítési kötelezettséget írt elő a nemzetbiztonsági szolgálatok számára. Mindösszesen két megszüntetési okot határozott meg. A különleges eszközök alkalmazását meg kellett szüntetni, ha az a célját elérte, vagy nyilvánvalóvá vált, hogy a cél elérésére alkalmatlan lett. Csupán célszerűségi okok megszűnése indokolta az alkalmazások kötelező befejezését; a törvényesség,

[10] Az Országgyűlés 74. ülése 1990: 6161–6162.
[11] Az Országgyűlés 75. ülése 1990: 6191–6195.

a szükségesség vagy az arányosság elveinek megfelelő követelményekben bekövetkezett változások ekkor még nem vezettek megszüntetéshez.

A szakasz második bekezdése egy azóta is rendkívül vitatott rendelkezést emelt be a különleges eszközök eljárási rendszerébe. Kimondta, hogy „[h]a a különleges eszközök alkalmazása nem alapozza meg az ellenőrzött személlyel szemben büntetőeljárás elrendelését, az ellenőrzött személyt az alkalmazott intézkedésről az engedélyt kérő tájékoztatja, és ezt követően az ellenőrzés során szerzett adatokat meg kell semmisíteni”.[12] A rendelkezés rendkívül idegen volt a nemzetbiztonsági szolgálatok feladat- és működési rendszerében. Alapvető probléma, hogy – amint azt maga a rövid törvény adta meg – a szolgálatok elsődleges feladata a szuverenitás és az alkotmányos rend védelme, aminek nem szükséges velejárója az állam büntetőjogi igényének érvényesítése. Sem a hírszerzés, sem az elhárítás, sem az érdekérvényesítés nem feltétlenül eredményezte vagy igényelte büntetőeljárás megindítását, még abban az esetben sem, ha egyébként a 2. § *d)* pontja szerinti bűncselekmények felderítése történt meg. Ráadásul az 5. § pontatlan volt a tekintetben is, hogy nem tette egyértelművé, hogy bármely különleges eszközre vagy csak a külső engedélyköteles eszközökre vonatkozott-e. Tekintettel arra, hogy az 1990. évi X. törvény hatálya a rendőrségre is kiterjedt, a rendőrség is kialakította joggyakorlatát. Így a BM Országos Rendőr-főkapitányság vezetője a különleges titkosszolgálati eszközök és módszerek átmeneti szabályozásáról szóló 1990. évi X. törvényben meghatározott feladatok végrehajtásáról szóló 2/1990. intézkedésének 8. pontjában kikötötte, hogy ha az érintettel szemben nem indult nyomozás, akkor a főkapitány őt az alkalmazás befejezését követő 15 napon belül tájékoztatta.

Anomáliát jelentett, hogy a norma az előző szakasszal ellentétben itt nem jelölte, hogy csak a törvényben nevesített különleges eszközök alkalmazására vonatkozna, hanem általánosan fogalmazott. Ennek értelmében bármely különleges eszköznek, még a legkisebb érdeksérelmet okozónak az alkalmazását követően is értesítési kötelezettség állt fenn az érintettek felé.

Ha a nemzetbiztonsági szolgálatok is szűken értelmezték a rendelkezést – a nemzetbiztonsági szolgálatok erre vonatkozó belső rendelkezéseit a nemzeti minősítés okán nem ismerhetjük meg –, az a nemzetbiztonsági munkát alapjaiban lehetetlenítette volna el. Azt vette volna el a szolgálatoktól, ami az állami funkció teljesítéséhez elengedhetetlen és ezen államigazgatási szervek létét meghatározó körülmény, a konspiráció követelményét. Ezzel kapcsolatban azt is érdemes megjegyezni, hogy a tájékoztatási kötelezettség a külső engedélyhez kötött különleges eszközök alkalmazására bénítólag is hathatott, mert a tájékoztatás számos nemzetbiztonsági feladat ellátásának utólagos dekonspirációjához vezethetett volna.

Végezetül kiemelhetünk még egy kisebb jelentőségű kérdést, ami a nemzetbiztonsági szolgálatok munkatársaira vonatkozott, akik addig rendőri jogállásúak voltak. Ez megszűnt, és a törvény kiterjesztette a nemzetbiztonsági szolgálat hivatásos állományára a fegyveres erők és fegyveres testületek állományának szolgálati viszonyáról szóló jogszabály hatályát.

[12] 1990. évi. X. törvény 5. § (2) bek.

A 26/1990. (II. 14.) MT rendelet szabályozási területei

Már az ideiglenes törvény parlamenti vitájában hangsúlyozta a kormány képviselője, hogy „a jogszabály az egész állambiztonsági szolgálat átszervezése, időbeli helye, szerepe, feladatköre és az államszervezetben elfoglalt helye szempontjából tartalmazott előremutató rendelkezéseket".[13] Mindez igaznak is volt tekinthető, hiszen az meghatározta a szolgálatok állami funkcióit, valamint kivette azokat az 1974. évi 17. törvényerejű rendelet módosításával a belügyminiszter hatásköréből, és az akkori kormányfőhöz, a Minisztertanács elnökéhez rendelte, azonfelül állambiztonsági helyett nemzetbiztonsági szolgálatoknak titulálta. A szolgálatoknak ez a fajta átpozicionálása lényeges minőségi különbséget fejezett ki, a titkosszolgálatok már nem az államhatalom birtokosainak védelmét szolgálták, „hanem az egész nemzet, az alkotmányos rend biztonságát, védelmét tekintik elsődleges feladatuknak".[14]

Az 1990. évi X. törvény a kihirdetése napján lépett hatályba, 1990. február 14-én,[15] mégpedig szinte abban az időben, amikor a végleges törvénytervezet benyújtása a belügyminiszteri ígéret szerint időszerűvé vált. Új törvény benyújtása azonban nem történt meg, hanem a Minisztertanács élt a törvény által a számára nyújtott felhatalmazással, és ugyanazon a napon kiadta a nemzetbiztonsági szolgálatok átmeneti szabályozásáról szóló 26/1990. (II. 14.) MT rendeletet,[16] amely a szféra anyagi jogi részeit volt hivatott átmenetileg rendezni. Az átmenet a Rendelet esetében is több mint hat évig tartott.

A Rendelet a kiadásának napján hatályba lépett, ezzel 1990. február 14-én demokratikus jogállami keretek mentén létrehozta a modern magyar nemzetbiztonsági szolgálatokat, ami azonban szintén magán viselte az átmenet jegyeit. Rövid, mindössze nyolc szakaszt tartalmazó jogszabály volt, még a szolgálatok hivatalos megnevezését sem adta meg.

Első szakasza szerint Magyarországon négy szolgálat látta el a nemzetbiztonsági feladatokat:

- a nemzetbiztonsági szolgálat,
- az információs szolgálat,
- a katonai biztonsági szolgálat,
- a katonai felderítő szolgálat.

Megállapította a szolgálatok jogállását. A polgári elhárító és hírszerző szolgálatok országos hatáskörű és önálló költségvetésű szervek voltak, míg a katonai szolgálatok a Magyar Néphadsereg szervezeti és költségvetési keretében működtek. A katonai szolgálatok esetében a jogállás az irányítás kérdését is rendezte, hiszen mindenben követte a Magyar Néphadsereg, később a Magyar Honvédség sorsát.

A Rendelet a 2. §-ban meghatározta valamennyi titkosszolgálat feladatát. A nemzetbiztonsági szolgálat feladatát állapította meg a legszélesebb körben, mégis viszonylag szűk hatásköröket adott számára is. Pusztán kémelhárító szervként definiálta, nem pedig

[13] Az Országgyűlés 74. ülése 1990: 6137.
[14] Az Országgyűlés 74. ülése 1990: 6138.
[15] 1990. évi X. törvény a különleges titkosszolgálati eszközök és módszerek engedélyezésének átmeneti szabályozásáról (közlöny állapot).
[16] 26/1990. (II. 14.) MT rendelet a nemzetbiztonsági feladatok ellátásának átmeneti szabályozásáról (közlöny állapot).

széles körű elhárító szolgálatként, valamint a kiemelten fontos személyek és objektumok esetében általános nemzetbiztonsági védelmi feladatokkal ruházta fel. Egyes, pontosan meghatározott bűncselekmények esetében felderítési jogkört kapott a szolgálat, függetlenül attól, hogy egyéb bűnüldöző szervek az adott ügyben a büntetőeljárást már megindították, vagy sem. A nemzetbiztonsági szolgálat – a korábbi állambiztonsággal szemben – nyomozó hatósági jogkörrel nem rendelkezett, így a büntetőeljárás egyik szakaszában sem rendelkezett aktív intézkedési lehetőséggel, viszont feljelentési kötelezettséget sem írtak számára elő. Ezen túlmenően végezte a bevándorlói vagy menekültstátuszért folyamodó személyek biztonsági ellenőrzését.

Az információs szolgálat klasszikus, a kormányzati tevékenységet támogató hírszerző szervként jött létre, hasonlóan a katonai felderítő szolgálathoz, amely ugyanezen feladatot a honvédelmi érdekek érvényesítése mentén volt hivatott végezni. A katonai biztonsági szolgálat a kémelhárítási feladatait a külföldi katonai hírszerző szervekkel szemben látta el, és biztosította a fontos katonai objektumok nemzetbiztonsági védelmét. A Rendelet személyek esetében nem tett különbséget a katonai és a polgári nemzetbiztonsági védelmi feladatok között, ugyanazt a rendelkezést helyezte el a polgári és a katonai elhárításnál is, ami hatásköri összeütközéshez vezethetett például a köztársasági elnök esetében. Az ő nemzetbiztonsági védelmét – mint a legfőbb közjogi méltóságét – a nemzetbiztonsági szolgálat volt hivatott ellátni, ellenben mint a Magyar Honvédség főparancsnokáét a katonai biztonsági szolgálat.

Ezenkívül a Rendelet kinyilvánította, hogy a szolgálatok hatósági jogkört nem gyakorolhatnak, habár a migráció területén szakhatósági jellegű feladattal rendelkeztek. A Rendelet a korábbi időszak negatív tapasztalataira válaszul kikötötte, hogy a szolgálatok személyes szabadságot korlátozó kényszerintézkedést nem alkalmazhattak, vagyis olyan rendelkezést hozott rendeleti szinten, amit – mivel alapvető emberi jogot érintett – törvényi szinten lett volna szükséges bevezetni. Ezt követően külön szakasz szólt az állampolgárok, a fegyveres erők és a rendőrség együttműködési kötelezettségéről, egy újabb pedig a kormányzati irányítás formájáról.

A 4. § határozta meg a szolgálatok kormányzati irányítási rendszerét. Az első időszakban az irányítást a kormány látta el az összes nemzetbiztonsági szerv esetében az általa a kormány egyes minisztereinek részvételével felállított Biztonsági Kollégium útján. A Kollégium az irányítás mellett az ellenőrzés feladatait is ellátta.

Az ötödik szakasz adta meg a szolgálatok vezetőinek négy alapfeladatát, viszont nem határozta meg a vezetők jogállását és titulusát. A 6. §-ban titoktartási kötelezettséget írt elő a szolgálatok munkatársai számára, valamint fegyverviselési jogot biztosított a polgári szolgálatok hivatásos állományú tagjainak. Végül kikötötte, hogy a hivatásos munkatársak a Rendeletben meghatározott szöveggel voltak kötelesek esküt tenni.

A jogszabályok dinamikája és szerepe az átmenetben

Az 1990. évi X. törvény és a Rendelet a hatályukat egyszerre, 1996. március 26-án, a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény hatálybalépésével vesztették el, viszont hatályuk alatt eltérő utat futottak be dinamikájukat tekintve. Az 1990. évi X. törvény szövegében egyetlen változás történt 1994. október 1-jén, amikor hatályba lépett

a Rendőrségről szóló 1994. évi XXXIV. törvény, amelybe átkerült a törvényből a rendőrség különleges eszközök alkalmazására felhatalmazó rész.

Ezzel szemben a Rendelet nyolc módosítást élt meg 1994 nyaráig. A lényegesnek mondható változások már az első évben megtörténtek, amikor három érdemi módosítás volt. Ezekkel:

- a nemzetbiztonsági szolgálathoz kerültek a Határőrséghez kapcsolódó nemzetbiztonsági védelmi feladatok, bűncselekmény-felderítési jogkörök[17] és az okmányvédelmi hatáskörök;[18]
- az információs szolgálaté lett az országos rejtjeltevékenység;[19]
- a nemzetbiztonsági szolgálat és az információs szolgálat okmányvédelmi, illetve rejtjeltevékenységi hatósági jogkört kapott;[20]
- a 6. §-ba bekerült május 2-án – a fegyelmi jog kapcsán – a két polgári szolgálat hivatalos megnevezése (Nemzetbiztonsági Hivatal, Információs Hivatal), valamint hogy e szolgálatokat elnök vezeti;[21] majd
- június 11-én, hogy a polgári szolgálatokat főigazgatók vezetik.

Az 1990 májusában Antall József miniszterelnökségével megalakult új kormány a szolgálatok irányítási rendjét is megváltoztatta. A megszűnt biztonsági kabinet helyét a Miniszterelnöki Hivatal e feladatokkal megbízott politikai államtitkára vette át.[22] A 4. § következő érdemi módosítására az 1994-es parlamenti választások után felállt kormány második hónapjában került sor, amikor a polgári nemzetbiztonsági szolgálatok irányítási feladatai Katona Béla tárca nélküli miniszterhez kerültek, a szakasz pedig kikerült a Rendeletből.[23] Innentől kezdve az irányítási feladatok kijelölése nem képezte a Rendelet szabályozási tárgyát.

Az 1990. évi X. törvény és a Rendelet hatályosulása

Azt kijelenthetjük, hogy a két jogszabály által fémjelzett időszakban a nemzetbiztonsági szolgálatok napi operatív tevékenységéből fakadó rendszerszintű probléma nem került napvilágra sem a hatályuk alatt, sem azt követően. Viszont már nem érthetünk egyet azzal a parlamenti vitában elhangzott kinyilatkoztatással, miszerint a rövid törvény az átmenetisége ellenére kellő garanciákat szolgáltatott volna az ellenőrzésére.[24] Hiszen egyik jogszabály sem fogalmazott meg a különleges eszköz alkalmazásának előzetes ellenőrzésén túl sem a végrehajtás, sem a befejezés utáni időszakokra ellenőrzési mechanizmust. Nem jogosította fel egyik állami szervet sem a nemzetbiztonsági szervek nemzetbiztonsági feladatai végrehajtásának eljárási szintű ellenőrzésével.

Azt el kell ismerni, hogy rendszerszintű negatív működéssel kapcsolatos adatok nem merültek fel. Csupán egy vitás eset látott napvilágot, ami a jogszabályok nem kellő

17 38/1990. (IX. 14.) Korm. rendelet.
18 90/1990. (V. 2.) MT rendelet.
19 90/1990. (V. 2.) MT rendelet.
20 90/1990. (V. 2.) MT rendelet.
21 90/1990. (V. 2.) MT rendelet.
22 98/1990. (VI. 11.) MT rendelet.
23 108/1994. (VII. 21.) Korm. rendelet.
24 Az Országgyűlés 74. ülése 1990: 6136.

egyértelműségéből adódott, mint ahogy az a nemzeti és etnikai jogok országgyűlési biztosának 1995. július 1. – 1996. december 31. közötti tevékenységéről szóló jelentésből is kitűnik.[25]

A biztos a Nemzetbiztonsági Hivatal (NBH) Baranya megyei kirendeltségének nemzeti kisebbségekkel szemben végzett tevékenységének jogszerűségi vizsgálata eredményeként állapította meg, hogy ugyan a Rendelet 2. § (1) bekezdés *c)* pontja felsorolja azokat a bűncselekményeket, amelyek megelőzése, felderítése és megakadályozása a nemzetbiztonsági szolgálat feladata, de megítélése szerint a rendkívül rövid jogszabály felületesen, hézagosan és tág értelmezésre teret adó módon szabályozta a nemzetbiztonsági szolgálat feladatait. Ennek következtében dilemmaként értékelte, hogy a Rendelet kifejezett felhatalmazása hiányában történt a szabályozás. A Rendeletre alapozva az NBH folytathatott-e egyáltalán védelmi célú adatgyűjtést, az megalapozhatta-e a szolgálat védelmi célú fellépését a közelben fennálló háborús helyzetben a nemzeti kisebbségek védelmére hivatkozva?

Az 1990. évi X. törvény és a Rendelet fent bemutatott értékelése okán azt állíthatjuk, hogy nem egyedül e két jogszabály létének és minőségének eredménye volt a nemzetbiztonsági szolgálatok 1990 és 1996 tavasza közötti konszolidált működése, hanem egyéb tényezők is befolyásolták azt. Ebben meghatározó szerepet játszhattak továbbá a nemzetbiztonsági szféra irányába kinyilvánított társadalmi elvárások, a rendszerváltást követő politikai viszonyok és az átalakuló geopolitikai környezet is.

Mindehhez azonban azt is érdemes hozzátenni, hogy a két jogszabály elfogadásának idején az 1989. október 23-án kihirdetett Alkotmány, majd az 1990 nyarától hatályos Alkotmány[26] sem tartalmazott a tárgykörre vonatkozóan lényegi rendelkezéseket. Kizárólag annyit mondott ki a Magyar Köztársaság Alkotmánya a 40/A. § (2) bekezdésében, hogy a nemzetbiztonsági tevékenységgel összefüggő részletes szabályokról szóló törvény elfogadásához a jelen lévő országgyűlési képviselők kétharmadának szavazata szükséges.

Mivel tehát az Alkotmány nem határozta meg a nemzetbiztonsági szolgálatok funkcióit, alkotmányos feladatait és az államszervezetben elfoglalt helyét, valamennyi kérdés rendezése az Országgyűlés törvényhozói hatáskörében maradt.

Felhasznált irodalom

Az Országgyűlés 73. ülése (1990). *Országgyűlési Napló,* 1990. január 23. 6047–6110.
Az Országgyűlés 74. ülése (1990). *Országgyűlési Napló,* 1990. január 24. 6115–6186.
Az Országgyűlés 75. ülése (1990). *Országgyűlési Napló,* 1990. január 25. 6191–6278.
Beszámoló a nemzeti és etnikai kisebbségi jogok országgyűlési biztosának tevékenységéről. Online: https://jogkodex.hu/doc/8005142
Hetesy Zsolt (2011): *A titkos felderítés.* PhD-értekezés. Pécs: PTE ÁJK.
Révész Béla (2004): Dunagate I. *Beszélő,* 9(12). Online: http://beszelo.c3.hu/cikkek/dunagate-i
Solti István (2020): Különleges eszközök a rendszerváltást követő időszakban. *Nemzetbiztonsági Szemle,* 8(3), 44–61. Online: https://doi.org/10.32561/nsz.2020.3.4

[25] Beszámoló a nemzeti és etnikai kisebbségi jogok országgyűlési biztosának tevékenységéről.
[26] A Magyar Népköztársaság Alkotmányáról szóló 1949. évi XX. törvény újabb módosítása 1990. június 25-én lépett hatályba.

Jogszabályok

1949. évi XX. törvény a Magyar Népköztársaság Alkotmányáról
1974. évi 17. törvényerejű rendelet az állam- és közbiztonságról
1990. évi X. törvény a különleges titkosszolgálati eszközök és módszerek engedélyezésének átmeneti szabályozásáról (közlöny állapot). *Magyar Közlöny,* (14), 1990. február 14. 285–287.
38/1990. (IX. 14.) Korm. rendelet a nemzetbiztonsági feladatok ellátásának átmeneti szabályozásáról szóló 26/1990. (II. 14.) MT rendelet módosításáról
108/1994. (VII. 21.) Korm. rendelet dr. Katona Béla tárca nélküli miniszter feladatairól
26/1990. (II. 14.) MT rendelet a nemzetbiztonsági feladatok ellátásának átmeneti szabályozásáról (közlöny állapot). *Magyar Közlöny,* (14), 1990. február 14. 291–293.
90/1990. (V. 2.) MT rendelet a nemzetbiztonsági feladatok ellátásának átmeneti szabályozásáról szóló 26/1990. (II. 14.) MT rendelet módosításáról
98/1990. (VI. 11.) MT rendelet a nemzetbiztonsági feladatok ellátásának átmeneti szabályozásáról szóló 26/1990. (II. 14.) MT rendelet módosításáról
BM Országos Rendőr-főkapitányság vezetőjének 2/1990. intézkedése a különleges titkosszolgálati eszközök és módszerek átmeneti szabályozásáról szóló 1990. évi X. törvényben meghatározott feladatok végrehajtásáról

NEMZETBIZTONSÁGI SZEMLE
14. évfolyam (2026) 1. szám 36–45. | DOI: 10.32561/nsz.2026.1.3

Fórizs Sándor[1]

Külföldre szökés és kémkedés bűntettének vádja

Charges of Fleeing Abroad and Espionage

A publikáció olyan határőr sorkatonák ellen indított büntetőeljárásokat ismertet, akik külföldre szökést követtek el, majd kémkedéssel is megvádolták őket. Az információkat két levéltár anyagai képezik, ezek a Magyar Nemzeti Levéltár Országos Levéltára, ahol a határőrségi okmányok találhatók, és a Hadtörténeti Levéltár a büntetőeljárások dokumentumaival. Az olvasó megismerheti az események – külföldre szökés, megindított eljárások – körülményeit, a keletkezett vizsgálati és bírósági okmányokat, az ítéletek mértékét és egyes esetekben az események későbbi utóéletét.

Kulcsszavak: *külföldre szökés, kémkedés, vizsgálati munka, vádirat, bírósági ítélet*

The publication describes the criminal proceedings brought against border guard conscripts who fled the country and were subsequently charged with espionage. The information is based on materials from two archives: the Hungarian National Archives, which holds border guard documents, and the Military History Archives, which houses documents relating to criminal proceedings. The author explores the circumstances of the events (i.e. the escapes abroad and the proceedings initiated), the investigation and court documents produced, the severity of the sentences and, in some cases, the aftermath of the events.

Keywords: *escape abroad, espionage, investigation, indictment, court ruling*

[1] Professor emeritus, egyetemi tanár, ny. rendőr dandártábornok, Nemzeti Közszolgálati Egyetem Rendészettudományi Kar, e-mail: drforizs@gmail.com

Bevezetés

Az 1950 és 1989 közötti kiszökésekről rendelkezünk név szerinti kimutatással egy, a határőrségnél folyamatosan vezetett okmányban.[2] Itt 813 volt határőr szerepel 39 év alatt a legfontosabb adatokkal (név, személyi adatok, a szökés helye és időpontja, iránya, néhány szóban a körülmények). Az elkövetők közül csupán keveset vádoltak meg kémkedéssel. Ennek az az oka, hogy míg a külföldre szökést különösebben nem volt problémás bizonyítani, más kérdés a kémkedés. Itt a tisztelt olvasónak nem a bűnügyi filmek hagyományos kémtevékenységére kell gondolnia, ahol valaki egy rejtett kamerával vagy más módon, ügynökökön keresztül szerzi be az adatokat. A vizsgált esetekben azt minősítették kémkedésnek, ha a kiszökött katona a külföldi kihallgatóknak adatokat szolgáltatott a hazai határőrizeti tevékenységről, állapotokról. Márpedig minden kiszökött személyt aprólékosan kihallgattak. Két-három körülményt mindenképpen szükséges megemlítenünk. A szökött határőrök esetében a bírósági eljárást távollétükben is lefolytatták, de automatikusan nem vádolták őket kémkedéssel. Polgári lakóhelyükön a tanácsoknál hirdetményként függesztették ki a tárgyalás időpontját és az idézést. Őket külföldre szökés bűntettével vádolták meg. Csupán a valamilyen módon hazakerült és bíróság elé állítottak esetében merült fel a kémkedés vádja, amit megbízható módon a vizsgálati munka során bizonyítani is kellett. A forrás erre csak egy másik katona lehetett, aki szintén hazakerült, és „rávallott" a társára, hiszen esetleg éppen a kinti fogdában egy cellában ültek, vagy a traiskircheni menekülttáborból ismerték egymást és egymás dolgait. Egyébként nem kevesen valóban hazajöttek, akiket őrizetbe vettek, és a BM Vizsgálati Osztály állította össze a katonai ügyészség, katonai bíróság számára a további vádeljáráshoz szükséges dokumentumokat.

Különös történések is megestek, például amikor valaki szolgálatból kiszökött, távollétében első és másodfokon is halálra ítélték. Évek múlva, mert kint nem tudott megállapodni, illegálisan hazaszökött, elfogták, újra bíróság elé került.

A megtörtént esetek mind érdekesek, érdemes feldolgozni azokat. Nem csupán azért, mert ezek a magyar katonatörténelem részét képezik, hanem azért is, mert rajtuk keresztül betekinthetünk a katonai jogszolgáltatás módjába és gondolatvilágába is. A levéltári okmányokra hivatkozásnál azonnal szólnunk szükséges arról a nehézségről, hogy az egyes dossziék, különösen a bírósági anyagok igen vastagok, gyakran 80–100 darab különböző anyaggal, amelyek többnyire azonos levéltári nyilvántartási számon találhatók, megnehezítve a hivatkozást.

Államtitoksértéshez kapcsolódó szakértői vélemények

Annak eldöntésére, hogy a büntetőeljárás alatt álló volt határőr követett-e el államtitoksértést, a nyomozást végző szerv – külföldre szökések esetében a Belügyminisztérium Vizsgálati Osztály – minden alkalommal szakértői véleményt szerzett be. A szakértő igenlő állásfoglalása a kémkedés vádjának megfogalmazásához feltétlenül szükséges volt. A Hadtörténeti Levéltárban fellelhető bírósági dossziékhoz kapcsolódik több, a vizsgálati okmányokat tartalmazó, a Vizsgálati Osztály által a bíróság számára összeállított

[2] MNL OL HOP XIX-B-10 1989. év 13. sz. doboz III/1–4 tárgykör 4. folyószám.

és a vizsgálati munka befejezésekor a katonai ügyészségnek és bíróságnak megküldött iratgyűjtemény. Ennek részét képezik a szakértői tevékenységre vonatkozó felkérések és az ennek alapján elkészített szakértői vélemények. A szakértőként felkért személy kizáró ok esetén megtagadhatta a részvételt az eljárásban, de ilyenről nincs tudomásom. A lehetőségre a kirendelő hatóság is felhívta az érintett figyelmét. Esetünkben: „Felhívom figyelmét, hogy a szakértői határozat ok nélküli megtagadása, vagy annak késedelmes teljesítése esetén a Be. 71. §. /1/ bek.-ben foglaltak szerint járunk el."[3] Ugyanebben a határozatban a terhelt figyelmét is felhívták, hogy lehetősége van a szakértő személyével kapcsolatban kizáró okra hivatkozni. A felkért szakértők tapasztalatom szerint minden esetben határőr tisztek voltak az országos parancsnokságról, esetleg a sorkatona eredeti szolgálati helyéről, kerületétől. Ez természetesen az érintettre vonatkozóan nem sok jót jelentett, még akkor sem, ha a tiszt korrektül járt el.

SzD „volt határőr" ügye annyiban érdekes, hogy kiszökött az országból, majd illegálisan hazatért, így vele szemben a bírósági eljárást a jelenlétében tudták lefolytatni. A BM Vizsgálati Osztály szakértői kirendelő határozata a rendelkezésünkre áll.

Ebben az esetben a szakértőtől három kérdésre kértek választ:

„1./ SzD által az osztrák rendőrségi kihallgatásai során elmondottak megfelelnek-e a tényleges valóságnak.

2./ Ha igen, ezek államtitkot vagy szolgálati titkot képeznek-e.

3./ A kiszolgáltatott adatok, tények milyen mértékben veszélyeztetik az MNK., vagy a Határőrség érdekeit."[4]

Több katonára vonatkozóan is rendelkezünk szakértői véleménnyel különböző időpontokból.[5] BL esetében a szakértő megnevezi állásfoglalásának a forrását: „A vádlott által felsorolt katonai jellegű adatok a Magyar Forradalmi Munkás-Paraszt Kormány 31/1963. XI. 17. számú rendeletének 1. §. 1. pontja alapján államtitoknak minősülnek. A vádlott által kiszolgáltatott adatok súlyos mértékben veszélyeztetik az MNK honvédelmi és határőrizeti érdekeit."[6]

Egy másik szakértő időben későbbi hivatkozása: a szakértői vélemény alapja a „Magyar Forradalmi Munkás-Paraszt Kormány 14/1971. április 15.-i sz. rendelete és az ennek alapján kiadásra került BM Határőrség Országos Parancsnoki 00307/3/1972 számú Minősítési Ügykörjegyzék – érvénybe lépett 1972. május 1-én."[7] HS határőr esetében a szakértő három kérdésben „szolgálati használatú", hat kérdésben pedig „titkos" minősítést állapított meg a határőr külföldi kihallgatása során elmondottak alapján.

1972-ben következett be egy olyan eset, amikor MI határőr szolgálatban fegyverrel súlyosan megsebesítette a járőrparancsnokát, majd Ausztriába menekült. A sebesült parancsnok vele szemben fegyvert használt, és a szökevény menekülés közben elszórta a magával vitt, korábban összegyűjtött okmányokat, technikai eszközök leírásait, elöljárói neveket, beosztásokat, politikai foglalkozások tematikáját. Ekkor kétszer kérték fel szakértői vélemény készítésére ugyanazt a személyt, 1972. december 5-i és 18-i dátummal.

---

[3] Belügyminisztérium Vizsgálati Osztály, 34-Bü-503/15/70.

[4] Belügyminisztérium Vizsgálati Osztály, 34-Bü-503/15/70.

[5] SzB hőr. 1966. augusztus; BL hőr. 1968. szeptember; SzD hőr. 1970. február 4.

[6] HU HL XI BKB I. 035/1969. Vizsgálati dosszié, szakértői vélemény, 1968. szeptember 25.

[7] MNL OL HOP XIX-B-10 1972. év 9. sz. doboz III. tárgykör 5. folyószám. Szakértői vélemény HS volt határőr esetében. 1972. december 6.

A duplázásnak az a magyarázata, hogy időközben hazatért egy kiszökött határőr katona, SZ, aki szerint MI az alábbi adatokat mondta el kinti kihallgatóinak:

- „a bevonulással kapcsolatos körülmények,
- a kiképzőzászlóalj szervezése,
- a kiképzés rendszere, módszere /milyen kiképzésben részesült/,
- a szombathelyi határőrlaktanya alaprajza,
- létszámra és fegyverzetre vonatkozó adatok,
- a horvátlövői őrs szervezése, az őrs védelmi rendszere,
- az Sz-100 elektromos jelzőrendszer telepítéséről, működéséről szóló adatok,
- a Szombathelyen ideiglenesen állomásozó szovjet csapatokról tett jelentés."[8]

A szakértőnek a szakvélemény elkészítése mellett a bírósági tárgyaláson is meg kellett jelennie.

Esettanulmányok

SzD és PJ határőr közös szökése

Mindkét katona a soproni kerület fertőrákosi őrséről szökött külföldre 1969. március 24-én, korábban fegyelmi felelősségre vonták és megfenyítették őket. Szabadidejükben kiszöktek az őrsről, italoztak, visszajöttek, veszekedtek, lefeküdtek, az éjszakai járőrszállítást végző gépkocsit jogtalanul átvették, egy fegyvert is vittek magukkal, pedig nem voltak szolgálatban. A gépkocsit üresen leállították a határnál, kiszöktek. A gépkarabélyt az államhatárnál visszadobták magyar területre. Egyébként a bírósági ítéletek a fegyverek vonatkozásában nem voltak egységesek. Gyakran a szolgálati hely fegyveres elhagyásánál hiába hagyták azt a járőrök az államhatárnál, az elkövetést a bíró már fegyveresnek ítélte. Érvelése szerint a fegyver azért kellett a katonának, hogy másokkal találkozva azt esetleg használhassa. SzD határőr esetében mindkét levéltár tartalmaz anyagokat.[9] A Győri Katonai Bíróság ítélete a vádlottakat bűnösnek mondja ki, „mindkét vádlottat: fegyveresen elkövetett külföldre szökésben és ezért külön – külön halálbüntetésre, mint, főbüntetésre és teljes vagyonelkobzásra, mint mellékbüntetésre ítéli."[10] A legsúlyosabb büntetést kapták, de itt még nincs szó kémkedésről, „[a] Katonai Főügyészség mindkét vádlottat a Btk. 313.§. /1/ bek-be ütköző, de a /2/ bek a./ pontja szerint minősülő és büntetendő fegyveresen elkövetett külföldre szökéssel vádolta."[11] Az ügy a katonák távollétében is a Magyar Népköztársaság Legfelsőbb Bíróságához került. 1969. július 30-án zárt, titkos tárgyaláson, a bíróság „meghozta a következő végzést: fegyveresen elkövetett külföldre szökés miatt PJ volt határőr és

[8] MNL OL HOP XIX-B-10 1972. év 9. sz. doboz III. tárgykör 5. folyószám.
[9] MNL OL HOP XIX-B-10 1969. év 12. sz. doboz III/1–4 tárgykör 2. folyószám és HU HL XI. KB.II.05/1969. szám, valamint HU HL XI. Katf. I. 011/1969.
[10] HU HL XI. KB.II.05/1969. szám. Győri KB ítélete.
[11] HU HL XI. KB.II.05/1969. szám. Vádirat.

társa ellen indított bűnügyben a Győri Katonai Bíróság KB.II.05/1969. számú ítélete ellen benyújtott fellebbezéseket elutasítja."[12] Vagyis maradt a halálos ítélet, az jogerőre lépett.

SzD a traiskircheni lágerben politikai menedékjogot és ideiglenes tartózkodási engedélyt kapott (későbbi vallomása szerint ezeket nem kérte). Ausztriában dolgozott, hazai levelezésből megtudta, hogy az anyja beteg, ezért úgy döntött, hazajön. Hegyeshalomnál beszökött az országba 1970. február 2-án, hazament, testvére jelezte a határőrségnek a visszatértét. Őrizetbe vették. Ezzel a jogszolgáltatás ugyancsak nehéz helyzetbe került, hiszen vele szemben hatályban volt egy halálos ítélet. Mivel kihallgatása során beismerte, hogy adatokat szolgáltatott ki külföldi szervezet számára, a Katonai Főügyészség államtitok tekintetében elkövetett kémkedés miatt perújítási nyomozást rendelt el, majd vádiratában ezt írta: „vádolom a Btk. 131. §. /2/ bek-be ütköző, de a /3/ bek. a./ pontja szerint minősülő államtitok tekintetében elkövetett kémkedéssel".[13] A Legfelsőbb Bíróság perújítást rendelt el, és a Budapesti Katonai Bíróságot jelölte ki az eljárás lefolytatására. A két ügyet, a korábbi kiszökést és a mostani kémkedést egyesítették. A „tárgyalási jegyzőkönyv" szerint „[a] bíróság az ügy jellegére való tekintettel zárt tárgyalást és közlési tilalmat rendel el."[14]

A bírósági ítélet, tekintettel arra, hogy nem történt fellebbezés, jogerőre emelkedett: „vádlottat bűnösnek mondja ki 1./ államtitok tekintetében elkövetett kémkedésben, 2./ fegyveresen elkövetett külföldre szökésben és ezért őt halmazati büntetésül 6 /hat/ évi szabadságvesztésre, mint főbüntetésre és 5 /öt/ évi közügyektől eltiltásra és teljes vagyonelkobzásra ítéli".[15]

Ezzel talán azt mondhatjuk, SzD számára szerencsésen zárult a vesszőfutása, hiszen egy halálos ítéletet változtattak az újabb eljárás során hatéves börtönbüntetésre, ami egyébként nem következett volna be, ha külföldön marad, illetve ha ki sem szökik.

VJ határőr: külföldre szökés és kémkedés

Az 1942-ben született sorkatona 1964. július 22-én szökött ki a zalaegerszegi határőrkerület nemesmedvesi őrséről. A Hadtörténeti Levéltárban két dosszié tartalmazza az esetét.[16] A vizsgálati iratgyűjtő egyik okmányából részletes tájékoztatást kapunk az ausztriai eseményekről.[17] Itthon nyolc alkalommal hallgatták ki és vettek fel jegyzőkönyvet. Ezek szerint hat általánost végzett, és civilben traktorvezetőként dolgozott. 1962. november 13-án vonult be, Lentiben a kiképző zászlóaljnál részesült alapkiképzésben, és 1963. februárban került az őrsre. Rendszeresen ivott, megfenyítették, 1964. július 22-én délelőtt szabadidőben szökött ki, bement a szemben található osztrák faluba, jelentkezett. Grazba vitték, 26 napig volt letartóztatásban. Úgy nyilatkozott, hogy Ausztriában kíván letelepedni. Elvitték egy katonai laktanyába, és ott is kihallgatták, mindent elmondott, amit a határőrségről tudott, szervezés, felszerelés, személyek nevei, szolgálati helyek és rendszer, kiképző zászlóalj stb. Lerajzolta a laktanyákat, a vallomását aláíratták vele. 1964.

[12] HU HL XI. KB.II.05/1969. szám. Legfelsőbb Bíróság Katonai Kollégium ítélet.
[13] HU HL XI. KB.II.05/1969. szám. Vádirat, Katonai Főügyészség, SzD ellen, 1970. április 8.
[14] HU HL XI. KB.II.05/1969. szám. MNK Legfelsőbb Bíróság ítélete. 1970. április 21.
[15] HU HL XI. KB.II.05/1969. szám. A Budapesti Katonai Bíróság ítélete, BKK KB. VII.025/1970.
[16] HU HL XI BKB I. 012/1965 és HU HL XI. 1. Katf. 013/1965.
[17] HU HL XI BKB I. 012/1965. Jegyzőkönyv a gyanúsított kihallgatásáról, 1965. február 12., 6.

augusztus 17-én szabadult a rendőrség fogdájából. A Vöröskereszthez vitték, ellátták ruhával és 100 schillinggel, 6 hónapra érvényes tartózkodási engedélyt kapott. Elhelyezték egy grazi építkezésen, ahol szállása is volt, itt 1964. október 14-ig dolgozott. Munkahelyét otthagyta, többfelé csavargott, majd felszállt egy Magyarországon áthaladó vonatra, menet közben leugrott, elfogták 1964. december 7-én. Úgy nyilatkozott, a kémkedés bűntettében, amivel időközben meggyanúsították, bűnösnek érzi magát, viszont önként jött haza, így a tiltott határátlépésben nem.

Még 1964. augusztus 10-én nyomozást rendeltek el vele szemben húsz nappal a kiszökését követően, a Btk. 313. §. /1/ bekezdésébe ütköző külföldre szökés alapos gyanúja miatt, de ekkor a kémkedés kérdése még nem merült fel. Az első eljárás során halálra és teljes vagyonelkobzásra ítélték.

Az iratgyűjtőben található második vádiratban már szerepel a kémkedés kérdése: „vádolom a Btk. 303. § /1/ bek-be ütköző, a /2/ bek. c/pontja szerint büntetendő szolgálati tevékenység felhasználásával elkövetett külföldre szökés, valamint a Btk. 131. § /2/ bek-be ütköző, a /3/ bek a/pontja szerint büntetendő államtitok tekintetében elkövetett kémkedés bűntettében."[18] Ügyét a Budapesti Katonai Bíróság tárgyalta. Az erről készült jegyzőkönyvben olvasható, hogy a katonai ülnököket a határőrség országos parancsnokságáról rendelték ki, a szakértőt, egy határőr őrnagyot, pedig szintén onnan kérték fel. A szokásos módon a katonai bíróság zárt tárgyalást és közlési tilalmat rendelt el. A bíróság bűnösnek mondta ki szolgálati tevékenység felhasználásával elkövetett külföldre szökés és államtitok tekintetében elkövetett kémkedés bűntettével, és halmazati büntetésül 10 év börtönbüntetésre ítélte.[19] A vádlott a döntést elfogadta, de a védő és a katonai ügyész fellebbezést nyújtott be, így az ítélet nem emelkedett jogerőre, az ügy másodfokra került. A Katonai Főügyészség gondolatmenetébe a fellebbezéssel kapcsolatos felterjesztése enged betekintést: „ez az ítélet törvénysértően enyhe, mivel két olyan bűntettet követett el, melyre a törvény a legsúlyosabb büntetés alkalmazását is lehetővé teszi".[20]

A fellebbezési tárgyalási jegyzőkönyv szerint a Legfelsőbb Bíróság Katonai Kollégiuma a külföldre szökést nem látta szolgálati elkövetéssel megtörténtnek, „ezért cselekményét a külföldre szökésnek a Btk. 313. §. /1/ bekezdésében írt alapesetének minősítette."[21] Egyebekben az elsőfokú büntetést érintetlenül hagyta, maradt a 10 év börtönbüntetés.

BL határőr oda-vissza szökése

Nevezett 1967. november 23-án vonult be sorkatonaként, és 1968. április 21-én szolgálatból szökött ki a zsirai őrs területén. Mindkét levéltárban találunk okmányokat az esettel kapcsolatban.[22] A Hadtörténeti Levéltár róla szóló dossziéján a „Külföldre szökés és kémkedés" felirat szerepel. Esete emlékeztet a korábbi történetekre. Kihelyezett járőrcsoportban teljesített szolgálatot, az államhatár átlépésekor fegyverét a honi oldalon a drótkerítéshez

18 HU HL XI BKB I. 012/1965. Vádirat, Katonai Főügyészség B. 050/1964. 1965. február 19., 9.
19 HU HL XI BKB I. 012/1965. Ítélet, BKB KB. I. 012/1965., 23.
20 HU HL XI. 1. Katf. 013/1965.
21 HU HL XI BKB I. 012/1965. Fellebbezési tárgyalási jegyzőkönyv, 1965. április 14., 33.
22 MNL OL HOP XIX-B-10 1968. év 11. sz. doboz III. tárgykör 2. folyószám, valamint HU HL XI BKB I. 035/1969.

támasztotta, két töltött tárat vitt magával. Érdekes, hogy ezt a bíróság később miként értékelte (fegyveres elkövetés másodfokon). Az első éjszakát egy osztrák családnál töltötte, majd azok elvitték az oberpullendorfi csendőrőrsre. Innen a bécsi rendőrségre és a traiskircheni menekülttábor zárt részébe került. 8–10 alkalommal a bécsi rendőrségre szállították kihallgatásra. Egy Schuman nevű, magyarul jól beszélő személy vezette a kikérdezését, amelyen egy alkalommal két katona is részt vett. Fényképeket, vázlatokat, rajzokat mutattak neki fegyverekről és a műszaki zárról. Kérdésükre úgy nyilatkozott, hogy a jobb élet reményében szökött ki, és Ausztriában szeretne maradni. Részletesen beszámolt az általa ismert személyekről, szervezetekről, a zsirai szolgálati rendszerről és az SZ-100-as riasztórendszerről, illetve annak kiszolgálásáról, alkalmazásáról. A kihallgatás befejezésével politikai menedékjogot és ideiglenes tartózkodási, munkavállalási engedélyt kapott. A táborban elhelyezett más magyarok szereztek neki munkahelyet. Mivel nem sikerült megfelelően rendezni a körülményeit, kivándorolni nem tudott, mert időközben jelentős tartozást halmozott fel, ezért 1969. szeptember 12-én visszaszökött Magyarországra, és egy járőr elfogta.

Kiszökését követően először a szokásos eljárás keretében a határőrkerület parancsnoka feljelentette, és a Legfőbb Ügyészség megfogalmazta a vádiratot, amelyben még csak a következő vád szerepelt: „Vádolom a Btk. 313. §. /1/ bek-be ütköző, de a /2/ bek. a/ és c/ pontja szerint minősülő fegyveresen és szolgálati ténykedés felhasználásával elkövetett külföldre szökéssel."[23] Ügyét a katonai bíróság Győrben tárgyalta, és döntésében „bűnösnek mondja ki szolgálati ténykedés felhasználásával elkövetett külföldre szökésben és ezért őt halálra, mint főbüntetésre és teljes vagyonelkobzásra, mint mellékbüntetésre ítéli."[24] Az ítélet ellen az ügyészség fellebbezési óvást nyújtott be, mintha a halálos ítélet nem lett volna elég. Indoklása: „indítványozom, az ítéletet úgy változtassák meg másodfokon, hogy a bíróság fegyveresen elkövetettnek is minősítse."[25] Ezzel az elsőfokú ítélet nem vált jogerőssé, és az ügy a Legfelsőbb Bíróság Katonai Kollégiuma elé került. A másodfok határozata: „A Győri Katonai Bíróság ítéletét annyiban változtatja meg, hogy a vádlott cselekményét fegyveresen és szolgálati ténykedés felhasználásával elkövetett külföldre szökésnek minősíti."[26] A védőnek az ítélet enyhítésére vonatkozó fellebbezését elutasította.

Hazaszökése új helyzetet teremtett, és megszületett ellene a második vádirat: „vádolom a Btk. 131. § /2/ bekezdésébe ütköző, de a /3/ bekezdés a./ pontja szerint minősülő államtitok tekintetében elkövetett kémkedéssel és a Btk. 203. § /1/ bekezdésbe ütköző tiltott határátlépéssel". Ebben már szerepel a kémkedés és a befelé irányuló tiltott határátlépés bűntette. Valamint: „Indítványozom, hogy a katonai bíróság a terhelt ellen fegyveresen és szolgálati ténykedés felhasználásával elkövetett külföldre szökés miatt a Győri Katonai Bíróságon folyamatban volt és perújítás alatt levő ügyet a Be. 56. § /2/ bekezdése alapján egyesítse jelen bűnüggyel és a két ügyet egy eljárásban bírálja el."[27] Vagyis a kiszökést, a kémkedést, a befelé irányuló tiltott határátlépést egy ügyben, egy eljárásban javasolták tárgyalni. Erre a Legfelsőbb Bíróság a Budapesti Katonai Bíróságot jelölte ki.

[23] HU HL XI BKB I. 035/1969. Vádirat, Katonai Főügyészség B.022/1968. szám, 1968. június 10.
[24] HU HL XI BKB I. 035/1969. A Győri Katonai Bíróság ítélete, KB. I. 010/1968. szám, 1968. július 4.
[25] HU HL XI BKB I. 035/1969. Győri Katonai Ügyészség, Fellebbezési óvás B.II. 013/1968. június 7.
[26] HU HL XI BKB I. 035/1969. Ítélet, Magyar Népköztársaság Legfelsőbb Bírósága, Katf. II. 018/1968. szám, 1968. augusztus 07.
[27] HU HL XI BKB I. 035/1969.Vádirat, Katonai Főügyészség Bf.025/1968. 1968. november 08.

Az új ítéletben a bíróság: „Bűnösnek mondja ki

1. fegyveresen és szolgálati ténykedés felhasználásával elkövetett külföldre szökésben,
2. államtitok tekintetében elkövetett kémkedésben,
3. tiltott határátlépésben, és ezért őt halmazati büntetésül 8 év börtönbüntetésre, 10 év közügyektől való eltiltásra és teljes vagyonelkobzásra ítéli. […] A szabadságvesztést szigorított börtönben kell végrehajtani."[28]

A tárgyalásról készült jegyzőkönyv szerint a három érintett, ügyész, védő és vádlott az ítéletet tudomásul vette, az jogerőre emelkedett.

Az iratgyűjtőben található egy kegyelmi eljárással kapcsolatos bejegyzés: „Az ET 1970. október 30-án kelt E.T. 10-10/22/1970. számú elhatározásával […] BL volt határőr elítéltre kiszabott szabadságvesztés hátralévő részének végrehajtását kegyelemből elengedte." Ezzel egy nehezen megmagyarázható folyamat zárult le. A határőrt először a külföldre szökésért halálra ítélték. Hazaszökése után meggyanúsították kémkedéssel, és a két ügy összevonása után végül 8 évre ítélték, azaz enyhébb büntetést kapott, mint előzőleg. A bíróság 1969. februárban hozta meg a végső ítéletet. Ezt követően 1970. október 31-én kegyelemmel szabadult. Lényegében az előzetes letartóztatás idejét is beszámítva, 1968. szeptember 13-tól 26 hónapot töltött őrizetben.

Külön dossziéban az irattartón belül a bíróságnak elkészített nyomozati, vizsgálati munkaokmányok találhatók, összesen 22 darab, közöttük járőrjelentés, elmeszakértői vélemény, határozat szakértő kirendeléséről stb. Az államtitok megsértéséhez kapcsolódó szakértői véleményt egy határőr őrnagy készítette.

MI határőr külföldre szökése fegyverhasználattal

A határőr 1972. október 21-én szökött ki a horvátlövői őrsről szolgálatban, esete más szempontból is különleges. A körülményeket a szombathelyi határőrkerület jelentése tartalmazza. MI határőr mint járőrtárs elöl ment, fegyverét hirtelen csőre töltötte, megfordult, egy papírlapot mutatott a parancsnoknak, és azt mondta: „Nyugati kém vagyok, kezeid emeld fel, hátra arc, és indulj a mélység felé."[29] Amikor megközelítette egy méterre a parancsnokát, az a fegyver csöve után nyúlt, erre egy lövést adott le, amely a bal comb külső felszínét megsértette. A különböző jelentések a sérülést később hol súlyosnak, hol könnyebbnek írják le. A járőrparancsnok összeesett. MI elvette a járőrparancsnok fegyverét, abból a tárat kivette, a fegyvert eldobta, átmászott a műszaki záron. A parancsnok tárat tett a fegyverbe, és két rövid sorozatot lőtt utána. Az odaérkező szomszédos járőr úgy találta, hogy a sérült járőrparancsnok szíjjal elszorította a lábát. A helyszínen éleslőszert is találtak a földön, talán akkor került oda, amikor a fegyver elakadt. A határőr hosszabb ideje készülhetett a kiszökésre. Jegyzetlapok maradtak a helyszínen a földön.

[28] HU HL XI BKB I. 035/1969. Budapesti Katonai Bíróság, Ítélet, KB. VII. 035/1969. szám 1969. szeptember 10.

[29] MNL OL HOP XIX-B-10 1972. év 9. sz. doboz III. tárgykör 5. folyószám. Tárgy: Kivizsgáló jelentés a horvátlövői őrs szakaszán történt külföldre szökésről. 1972. december 6.

Az eset annyira különlegesnek bizonyult, hogy az országos parancsnok levélben fordult a Katonai Főügyészség önálló osztályvezető ügyészéhez:

> „A cselekmény elkövetési módja és egyéb megfontolások miatt szükségesnek tartjuk, hogy nevezett ellen jelenlétében folytassák le a büntető eljárást. […] Ezért kérem intézkedésedet az elfogató parancs kibocsátása, valamint annak a Külügyminisztérium Konzuli Főosztályához történő megküldése iránt, a kiadatással kapcsolatos diplomáciai lépések megtétele céljából."[30]

Arra vonatkozóan nincsenek adataink, hogy ez a kikérés megtörtént-e. Feltételezhetően nem, mert az osztrák szervek nem adtak ki szökött katonákat. A Magyar Nemzeti Levéltárban a katona dossziéjában megtalálható a szakértői kirendelő határozat és a szakértői vélemény. Tudjuk, hogy egy hazajött határőr (SZ) vallomása alapján MI-t meggyanúsították kémkedéssel, de további bírósági anyagok nem állnak a rendelkezésünkre.

Zárógondolatok

Sajátos a kémkedés vádjának felbukkanása a külföldre szökött határőr sorkatonák esetében. Külön kérdés, mennyiben rendelkeztek olyan információkkal, amelyek megalapoztak egy ilyen vádat. A szakértőként kirendelt hivatásos tisztek véleménye a kapcsolódó eljárást alátámasztotta, hivatkozva a hatályos titokjegyzékre. Lényegében másként nem is foglalhattak állást a beosztásuk miatt. Viszont a titokjegyzék összeállítása, annak tartalma a korábbi határőrizeti viszonyokat tükrözte, több vonatkozásban már elavult, de módosítására, pontosítására nem került sor. Ami szerintem külföldön valóban hasznosítható lehetett korábban, az az adott őrs szolgálati rendszere. Erről mindent pontosan megkaphattak a kihallgatók. Különösen értékesek lehettek az információk 1971-ig az aknamezőről, az aknák elhelyezkedéséről, a leküzdés lehetőségéről. 1971 után esetleg az elektromos jelzőrendszeren történő áthatolás lehetőségeiről, illetve a jelzések esetén a zárási szakaszokon belül az egyes zárási szolgálati helyekről. Viszont mit lehetett kezdeni ezekkel az információkkal? Lényegében semmit. Már régen elmúlt az az időszak, amikor ügynökök jártak ki és be a zöldhatáron. Amikor fegyveres biztosítás mellett küldtek be, illetve juttattak ki személyeket, esetenként éjjel átjárót nyitva a műszaki záron. A határforgalom már olyan jelentős lett az 1960-as években, hogy annak sodrában, érvényes úti okmányokkal minden veszély nélkül lehetett utazni. Azaz nem szorultak rá a kinti felderítő szervek az ilyen jellegű információkra, és ezeket az adatokat nehezen lehetett beilleszteni a kémkedés körébe. A bíróságok még reflexszerűen hoztak halálos vagy más súlyos ítéletet külföldre szökés esetén, de az elkövetett bűntett, mármint a kémkedés belső tartalma már nem volt a régi. Az is ellentmondás, hogy éppen a visszatért katonákat gyanúsították meg kémkedéssel, holott a kiszökésért is megfelelő súlyú büntetést lehetett kiszabni jogszabály szerint. Az eljárások összevonásának, a kémkedéssel meggyanúsításnak nem látom különösebb értelmét, a Katonai Főügyészség részéről egyfajta bosszúálló, súlyosbító eljárásnak tekintem. Hogy jelentős mértékben csökkent a zöldhatárra irányuló ellenséges tevékenység,

[30] MNL OL HOP XIX-B-10 1972. év 9. sz. doboz III. tárgykör 5. folyószám. Az országos parancsnok levele. 1972. november 3.

alátámasztja a Határőrség Országos Parancsnokság Felderítő Osztályának értékelése.[31] Ez tartalmazza a befelé történt határsértéseket éves bontásban az osztrák államhatáron:

- 1959: 64 fő,
- 1960: 59 fő,
- 1960/61: 37 fő,[32]
- 1961/62: 22 fő,
- 1962/63: 42 fő.

Ezek közül 1959-től 1963 novemberéig a statisztika szerint csupán 4 büntetlen (azaz eredményes) tiltott határátlépés történt befelé, az ország belsejébe külföldről, a határőrség nyilvántartása szerint. A BM Vizsgálati Osztály ügynökként 1959-ben 1 főt, 1960-ban 1 főt, 1963-ban 2 főt azonosított, az ügynökök beküldése áttevődött a turizmusra. Két bírósági ítéletről szól az anyag, az egyik személy 15, a másik 6 évi szabadságvesztést kapott. Őket amerikai felderítő szervek szervezték be az NSZK-ban. Az osztály megállapítása szerint a határőrségi külső felderítés nem tudott adatokat szolgáltatni az ellenséges ügynöki tevékenységgel kapcsolatban.

A bírósági ítéletekből kiolvasható, hogy a szolgálatból történt külföldre szökést a katonai bíróságok gyakran a legsúlyosabb, halálos ítélettel büntették. Ennek végrehajtása viszont elmaradt, még azok esetében is, akik valamilyen módon hazakerültek. A vizsgált három esetben az újabb egyesített eljárások során az érintett három fő 6, 8 és 10 év büntetést kapott. A kiszököttek további sorsával kapcsolatban a határőrség csupán hézagos információkkal rendelkezett. Ezek legjelentősebb forrásai a hazaküldött levelek és a visszatértek beszámolói voltak. A szervezet ezen volt határőrök ügyében nem folytatott további jelentős felderítést a traiskircheni menekülttábort leszámítva.

Felhasznált irodalom

Belügyminisztérium Vizsgálati Osztály, 34-Bü-503/15/70. Szigorúan titkos. Határozat szakértő kirendeléséről. 1970. február 24. SzD határőr anyagai.
HU HL XI BKB I. 012/1965.
HU HL XI BKB I. 035/1969. BL határőr anyagai.
HU HL XI. 1. Katf. 013/1965. VJ határőr anyagai.
HU HL XI. Katf. I. 011/1969.
MNL OL HOP XIX-B-10 1964. év 12. sz. doboz IV/8–9. tárgykör 23. folyószám. A nyugati viszonylatban befelé irányuló határsértések értékelése. 1963. november 14.
MNL OL HOP XIX-B-10 1968. év 11. sz. doboz III. tárgykör 2. folyószám. BL határőr anyagai.
MNL OL HOP XIX-B-10 1969. év 12. sz. doboz III/1–4 tárgykör 2. folyószám. SzD és PJ határőrök anyagai.
MNL OL HOP XIX-B-10 1972. év 9. sz. doboz III. tárgykör 5. folyószám. MI határőr anyagai.
MNL OL HOP XIX-B-10 1989. év 13. sz. doboz III/1–4 tárgykör 4. folyószám. Hazaárulások nyilvántartása (1950–1989).

[31] MNL OL HOP XIX-B-10 1964. év 12. sz. doboz IV/8–9. tárgykör 23. folyószám.
[32] Az 1960/61-es jelölés úgynevezett határőrizeti évet tartalmaz októbertől októberig. A határőrség néhány évig áttért erre a nyilvántartásra, megnehezítve az egyes évek adatainak összevetését.

NEMZETBIZTONSÁGI SZEMLE
14. évfolyam (2026) 1. szám 46–56. | DOI: 10.32561/nsz.2026.1.4

Gábor Andrékó[1]

Why Institutional Isolation Fails

UN Voting, Legal Sovereignty and Hierarchical Geopolitics in the Russia Case

Despite the overwhelming condemnation of the Russian Federation in the United Nations General Assembly following the outbreak of the Russia–Ukraine war, international efforts aimed at isolating Russia have produced limited tangible geopolitical effects. While formal voting patterns suggest broad institutional isolation, Russia has retained significant political, economic and strategic support from major powers such as China and India, as well as from a substantial proportion of states in Africa and the Global South.

This paper addresses the apparent paradox between institutional isolation and geopolitical resilience by distinguishing between legal sovereignty and effective geopolitical position. The argument advanced is that the UN General Assembly operates on the principle of formal legal equality, where each state possesses one vote, while the geopolitical sphere is structured hierarchically, reflecting asymmetric power relations, network dependencies and resource-based influence.

Building on the analysis of UN voting behaviour and patterns of diplomatic alignment, the paper demonstrates that institutional isolation does not automatically translate into geopolitical insulation. Instead, isolation efforts are constrained by hierarchical support structures in the international system, where major powers and strategically positioned states can mitigate or neutralise the effects of institutional condemnation.

By introducing the conceptual distinction between institutional isolation and geopolitical insulation, the paper contributes to a more nuanced understanding of contemporary sanction regimes and diplomatic pressure mechanisms. The findings have direct implications for security studies, sanctions policy and strategic planning, highlighting the limits of institution-based approaches in a hierarchically structured international order.

Keywords: *legal sovereignty, institutional isolation, geopolitical insulation, institutionalised hierarchy, geopolitical network*

[1] Research Fellow, Institute of National Security, Ludovika University of Public Service, e-mail: andreko.gabor@uni-nke.hu

Introduction

Since the outbreak of the Russia–Ukraine war in 2022, the international community has employed a broad range of diplomatic and economic instruments aimed at isolating the Russian Federation. One of the most visible manifestations of this effort has been the repeated condemnation of Russia in the United Nations General Assembly (UNGA), where an overwhelming majority of member states have supported resolutions criticising Russian actions and reaffirming core principles of international law.[2]

At first glance, these voting outcomes appear to indicate a high degree of international consensus and, by extension, the successful institutional isolation of Russia. However, this interpretation becomes problematic when juxtaposed with the empirical reality of continued diplomatic engagement, sustained economic relations, and strategic cooperation between Russia and a significant number of states, including major powers such as China and India, as well as a large proportion of countries in Africa and the Global South. Collectively, these states represent a substantial share of the world's population, natural resources, and economic potential.

This discrepancy gives rise to a fundamental analytical paradox: how can a state be simultaneously institutionally condemned by a majority of the international community and yet remain geopolitically resilient and connected? The persistence of Russian influence and cooperation networks challenges the assumption – often implicit in policy and academic discourse – that institutional isolation within international organisations necessarily translates into effective geopolitical isolation.[3]

The central argument of this paper is that this paradox can be resolved by distinguishing between two analytically distinct dimensions of isolation: *institutional isolation* and *geopolitical insulation*. While institutional isolation operates within a legal–procedural framework based on formal equality and symbolic delegitimation, geopolitical insulation depends on hierarchical power relations (Figure 1), network-based dependencies, and material capacities that lie largely outside the reach of institutional voting mechanisms.[4]

By examining UN voting behaviour alongside broader patterns of geopolitical alignment, the paper demonstrates that institutional isolation has inherent structural limits. These limits become particularly visible in cases involving major or systemically significant powers, whose hierarchical position within the international system enables them to mitigate or neutralise the effects of institutional pressure. The Russia case thus offers an instructive example for reassessing the relationship between legal sovereignty, institutional legitimacy, and effective geopolitical positioning.[5]

The paper proceeds as follows. The next section outlines the principles of legal sovereignty and institutional equality that underpin the functioning of the United Nations system. This is followed by an examination of the conceptual and empirical limits of institutional isolation as a tool of international pressure. Subsequent sections develop a hierarchical interpretation of geopolitical space to explain why institutional condemnation often

[2] United Nations General Assembly 2022a; United Nations General Assembly 2022b.
[3] Hurrell 2007.
[4] Ikenberry 2011.
[5] Lake 2009.

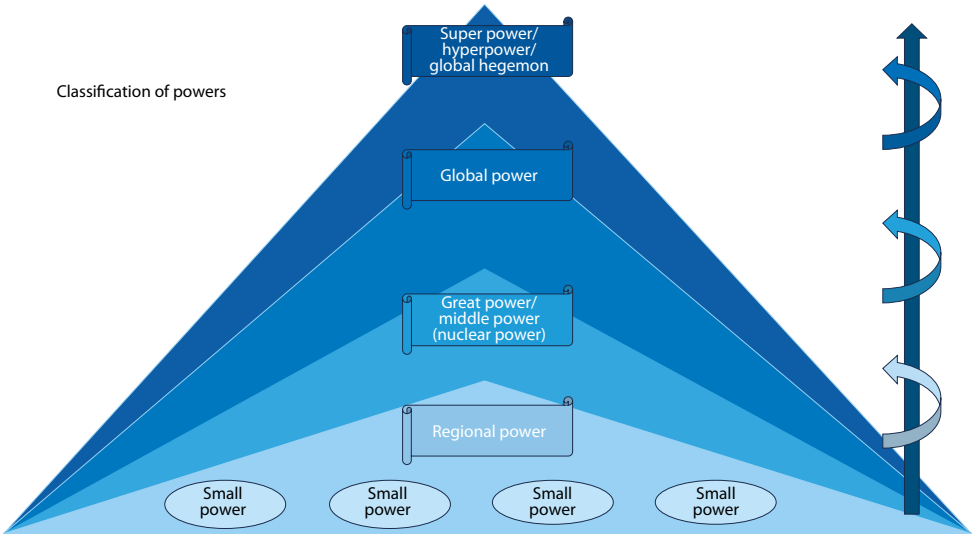


Figure 1: Ranking of powers by their ability to influence
Source: Andrékó 2025: 153

fails to produce the intended strategic outcomes. The concluding section reflects on the implications of this analysis for security studies, sanctions policy, and strategic planning.

Legal sovereignty and institutional equality in the United Nations

The United Nations system is founded on the principle of the sovereign equality of states, as enshrined in Article 2(1) of the UN Charter. This principle constitutes the legal and normative cornerstone of the organisation and is operationalised most visibly in the United Nations General Assembly, where each member state possesses one vote regardless of its size, power, or level of development. From a legal perspective, this arrangement reflects a commitment to formal equality and the universality of international law.[6]

Within this institutional framework, UN General Assembly resolutions function primarily as expressions of collective political judgment and normative positioning. Although such resolutions lack binding force, they carry symbolic weight by signalling the degree of international support or opposition toward a particular state's actions. In this sense, institutional isolation manifests as a form of delegitimation, intended to stigmatise behaviour that is perceived as violating international norms.[7]

However, the legal equality embedded in the UNGA voting system also imposes important analytical constraints. By design, the system abstracts from material power

[6] United Nations 1945.
[7] Hurrell 2007.

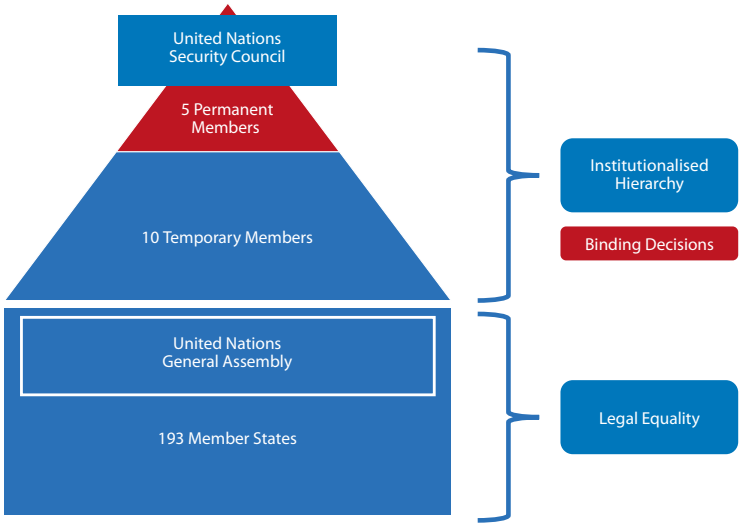


Figure 2: Legal equality vs. institutionalised hierarchy
Source: compiled by the author

differentials and treats all states as formally equivalent actors. This abstraction, while normatively significant, limits the capacity of UN voting outcomes to capture the actual distribution of power and influence in the international system. As a result, institutional isolation measured through voting behaviour may provide an incomplete or even misleading picture of a state's effective geopolitical position.[8]

This limitation becomes particularly evident when considering the distinction between the UN General Assembly and other components of the UN system, most notably the Security Council. Unlike the General Assembly, the Security Council explicitly institutionalises hierarchy through permanent membership and veto power (Figure 2). The coexistence of these two bodies reflects a fundamental tension within the international order: the aspiration toward legal equality on the one hand, and the recognition of hierarchical power relations on the other.[9]

In the context of international isolation strategies, this tension has significant implications. Institutional condemnation in the General Assembly may signal broad normative disapproval, but it does not automatically translate into enforceable constraints or coordinated action. Enforcement mechanisms – such as sanctions regimes, trade restrictions, or diplomatic downgrades – depend on the willingness and capacity of states to implement them. These capacities are unevenly distributed and closely tied to hierarchical positioning within global economic, political, and security networks.

Consequently, institutional isolation should not be understood as a binary condition in which a state is either isolated or not isolated. Rather, it constitutes a spectrum of symbolic and procedural exclusion that interacts with, but does not determine, a state's material

[8] Lake 2009.
[9] Ikenberry 2011.

and strategic environment. In cases where a targeted state retains access to alternative markets, strategic partners, or major power backing, institutional isolation may coexist with continued geopolitical engagement.[10]

The Russia case illustrates this dynamic with particular clarity. Despite repeated condemnations in the UN General Assembly, Russia has maintained substantial economic ties, diplomatic channels, and strategic partnerships beyond the Western institutional sphere. This outcome suggests that legal sovereignty and institutional equality, while central to the normative architecture of the international system, do not fully account for the mechanisms through which power, influence, and resilience are exercised in practice.[11]

Empirical evidence: The limits of institutional isolation in the Russia case

From a policy perspective, the effectiveness of international isolation strategies is commonly assessed through institutional indicators, most notably voting behaviour in international organisations and formal participation in sanction regimes. In the case of the Russian Federation, United Nations General Assembly voting records appear to provide strong evidence of widespread international opposition since 2022. A clear majority of UN member states have repeatedly supported resolutions condemning Russian actions and reaffirming principles of territorial integrity and sovereignty.[12]

However, when these institutional indicators are compared with patterns of actual political, economic, and strategic interaction, a significant discrepancy emerges (Figure 3). Despite formal condemnation, Russia has not experienced comprehensive geopolitical isolation. Instead, it has retained – and in some cases expanded – cooperation with a range of strategically significant actors. This divergence highlights the need to distinguish between symbolic institutional alignment and effective geopolitical behaviour.[13]

Several empirical patterns are particularly relevant. First, a number of major and emerging powers have consistently refrained from supporting or enforcing isolation measures beyond the institutional level. China and India, while adopting cautious diplomatic rhetoric, have maintained extensive economic relations with Russia, particularly in the fields of energy, trade, and strategic cooperation. These relationships have provided Russia with alternative markets and revenue streams, mitigating the impact of Western-led sanctions.[14] Second, a substantial proportion of states in Africa, the Middle East, and parts of Asia have avoided full alignment with isolation efforts. Many of these states abstained from UN General Assembly votes or supported resolutions rhetorically while continuing pragmatic engagement with Russia. Collectively, these regions represent a large share of the global population and control significant natural resources, transit routes, and emerging markets.

10 Baldwin 1985.
11 Lake 2009; Hurrell 2007.
12 United Nations General Assembly 2022a; 2022b.
13 Drezner 2011.
14 Farrell–Newman 2019.

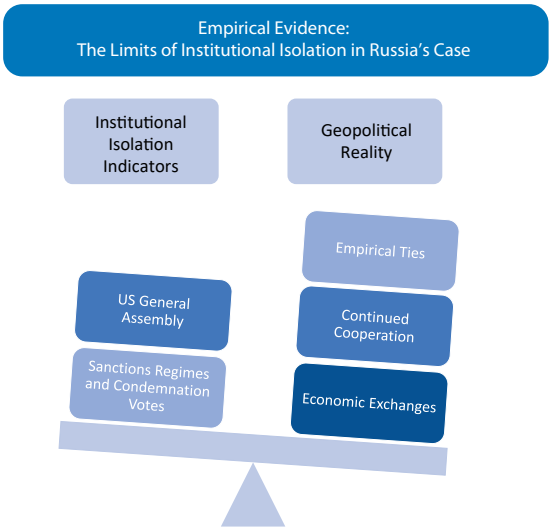


Figure 3: Institutional isolation and geopolitical reality
Source: compiled by the author

From a policy standpoint, this pattern undermines the assumption that numerical majority in institutional voting equates to strategic leverage.[15]

Third, the implementation of isolation measures has varied considerably across regions and policy domains. While certain financial and technological restrictions have imposed real costs, enforcement gaps and selective compliance have limited their overall effectiveness. The persistence of trade flows through third countries, the reorientation of supply chains, and the development of alternative payment mechanisms illustrate how geopolitical connectivity can be reconfigured rather than severed.[16] Taken together, these observations suggest that institutional isolation operates primarily at the level of political signalling and normative positioning. It shapes reputational environments and diplomatic narratives, but it does not automatically disrupt the underlying networks that sustain a state's geopolitical resilience. For policymakers, this implies that institutional condemnation alone is an insufficient indicator of strategic isolation, particularly when dealing with systemically significant actors.

Explaining the paradox: Hierarchical geopolitics and policy constraints

To understand why institutional isolation has failed to produce comprehensive geopolitical isolation in the Russia case, it is necessary to move beyond a purely institutional or legal

[15] Narlikar 2013.
[16] Drezner 2011; Farrell–Newman 2019.

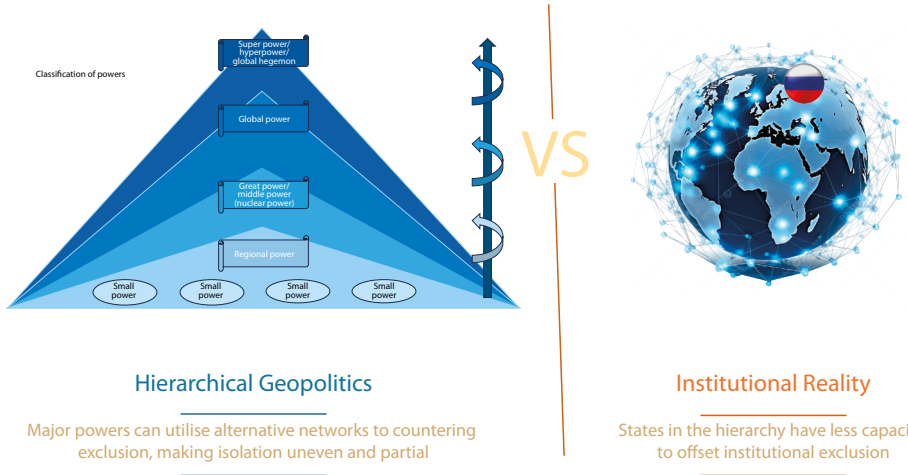


Figure 4: Hierarchical geopolitics and the geopolitical network
Source: compiled by the author

framework and consider the hierarchical structure of the international system. From a policy-analytic perspective, the key limitation of institution-centred approaches lies in their implicit assumption of horizontal state relations, where formal rules and collective decisions are expected to generate uniform effects.[17]

In practice, the international system is characterised by hierarchical differentiation. States occupy unequal positions based on their material capabilities, network centrality, and strategic relevance. These hierarchies shape the range of options available to both those seeking to impose isolation and those attempting to resist it. Major powers and systemically connected states are less vulnerable to institutional pressure because they possess alternative channels for economic exchange, diplomatic engagement, and security cooperation.[18]

Within this hierarchical context, isolation functions differently depending on a state's position. For actors situated lower in the hierarchy, institutional condemnation may coincide with tangible constraints, as they lack the capacity to compensate for lost access to markets, technologies, or security guarantees (Figure 4). By contrast, states occupying higher or more central positions can leverage their network connections to offset institutional exclusion. In such cases, isolation becomes partial, selective, and uneven.[19]

From a policy standpoint, this distinction is crucial. Institutional mechanisms such as UN resolutions are most effective when they align with existing power hierarchies and network structures. When they do not, their impact is largely symbolic. The Russia case demonstrates that even extensive institutional condemnation may fail to generate decisive strategic effects if alternative geopolitical alignments remain available.[20]

17 Lake 2009.
18 Lake 2009; Ikenberry 2011.
19 Farrell–Newman 2019.
20 Hurrell 2007.

This dynamic can be conceptualised as the difference between *institutional isolation* and *geopolitical insulation*. Institutional isolation refers to formal exclusion or condemnation within international organisations and legal–normative frameworks. Geopolitical insulation, by contrast, refers to a state's capacity to shield itself from the practical consequences of isolation through hierarchical support, resource control, and network-based resilience.

For security and foreign policy planners, this distinction carries important implications. Overreliance on institutional indicators may lead to overestimation of isolation effectiveness and underestimation of a target state's adaptive capacity. Effective isolation strategies must therefore account for hierarchical positioning, identify critical network nodes, and assess the availability of alternative partnerships. Without such an assessment, isolation risks becoming a declaratory policy instrument rather than a tool of strategic influence.[21]

Implications for sanctions design, alliance management and risk assessment

The distinction between institutional isolation and geopolitical insulation has direct and practical implications for contemporary security policy. In particular, it challenges prevailing assumptions regarding sanctions effectiveness, alliance cohesion, and strategic risk assessment. Policymakers who rely predominantly on institutional indicators may misjudge both the resilience of targeted states and the durability of international pressure coalitions.

Sanctions design: From declaratory measures to network disruption

Sanctions regimes are often constructed on the implicit assumption that institutional condemnation and coordinated legal restrictions will generate cumulative economic and political pressure. While such measures can impose significant costs, the Russia case demonstrates that the effectiveness of sanctions is highly contingent on the hierarchical position and network embeddedness of the targeted state.

For systemically connected actors, sanctions tend to trigger adaptive behaviour rather than isolation. Alternative trade routes, substitute markets, and parallel financial mechanisms can reduce vulnerability and redistribute costs across the network. From a policy perspective, this suggests that sanctions design should move beyond broad-based restrictions toward more targeted interventions aimed at critical nodes within geopolitical and economic networks.

Effective sanctions strategies require granular mapping of dependencies, including energy flows, technological bottlenecks, logistics corridors, and financial intermediaries. Rather than assuming uniform compliance, policymakers must anticipate selective enforcement and design measures that account for differential incentives among third-party

[21] Lake 2009.

states. In hierarchical systems, sanctions are most effective when they disrupt high-value connections rather than merely signal disapproval.[22]

Alliance management: Managing asymmetry and divergent incentives

Institutional coalitions, particularly those formed around multilateral organisations, often mask underlying divergences in strategic priorities and threat perceptions. The Russia case illustrates how alliance cohesion at the institutional level may coexist with significant variation in actual policy implementation.

From an alliance management perspective, the key challenge lies in reconciling formal unity with asymmetric costs and benefits. States occupying different positions within the geopolitical hierarchy face distinct exposure levels to economic retaliation, energy disruptions, or security risks. As a result, institutional alignment does not necessarily imply uniform commitment to sustained isolation efforts.

Effective alliance management therefore requires proactive coordination mechanisms that address these asymmetries explicitly. This includes burden-sharing arrangements, compensatory measures, and differentiated timelines that reflect partners' structural constraints. Failure to acknowledge hierarchical differences within alliances risks erosion of compliance and gradual fragmentation of collective strategies.[23]

Risk assessment: Rethinking isolation as a strategic variable

Traditional risk assessments often treat isolation as a binary condition: a state is either isolated or not. The findings presented in this paper suggest that such an approach is analytically insufficient and potentially misleading for security planning.

A more robust risk assessment framework should conceptualise isolation as a multidimensional variable influenced by legal status, network connectivity, and hierarchical positioning. Analysts should assess not only the presence of institutional condemnation but also the availability of alternative alignments, the resilience of supply chains, and the capacity for strategic substitution.

In practical terms, this means that policymakers should be cautious in extrapolating long-term outcomes from short-term institutional signals. The persistence of geopolitical insulation may enable targeted states to prolong conflicts, absorb economic shocks, or exploit divisions within pressure coalitions. Incorporating hierarchical analysis into risk assessments can therefore improve strategic foresight and reduce the likelihood of policy overconfidence.[24]

[22] Baldwin 1985; Drezner 2011.
[23] Ikenberry 2011; Narlikar 2013.
[24] Farrell–Newman 2019; Lake 2009.

Conclusion

This paper has examined the apparent paradox between widespread institutional condemnation and limited geopolitical isolation in the case of the Russian Federation. By distinguishing between institutional isolation and geopolitical insulation, the analysis demonstrates that formal legal equality and institutional voting outcomes provide an incomplete picture of power, influence, and resilience in the international system.

The findings suggest that institutional mechanisms, while normatively significant and politically visible, operate primarily at the level of legitimacy signalling. Their strategic impact is constrained by hierarchical structures that shape access to resources, networks, and alternative partnerships. In such a context, isolation strategies that rely predominantly on institutional alignment risk overestimating their effectiveness, particularly when applied to systemically significant actors.

For security studies and policy practice, the implications are clear. Sanctions design must focus on disrupting critical network nodes rather than assuming uniform compliance. Alliance management should explicitly address asymmetries in exposure and incentives among partners. Risk assessment frameworks must move beyond binary conceptions of isolation and incorporate hierarchical positioning as a core analytical variable.

More broadly, the Russia case underscores the need to rethink how sovereignty, isolation, and power are conceptualised in contemporary international relations. Legal sovereignty remains a foundational principle of the international order, but its practical significance is mediated by hierarchical dynamics that determine which actors can absorb pressure and which cannot. Recognising this distinction is essential for developing more realistic and effective security strategies in an increasingly fragmented and stratified global system.

References

Andrékó, Gábor (2025): The Russian Theory of the World's Geopolitical Space and the Classification of Powers. In Dobák, Imre – Farkas, Johanna (eds.): *Law Enforcement, Psychology and Security in Dialogue. Interdisciplinary Perspectives.* Budapest: Magyar Rendészettudományi Társaság, 148–156. Online: https://en.uni-nke.hu/document/en-uni-nke-hu/LEPSY_Conf_2025_Book_ISBN.pdf

Baldwin, David A. (1985): *Economic Statecraft.* Princeton: Princeton University Press.

Drezner, Daniel W. (2011): Sanctions Sometimes Smart: Targeted Sanctions in Theory and Practice. *International Studies Review,* 13(1), 96–108. Online: https://doi.org/10.1111/j.1468-2486.2010.01001.x

Farrell, Henry – Newman, Abraham L. (2019): Weaponized Interdependence: How Global Economic Networks Shape State Coercion. *International Security,* 44(1), 42–79. Online: https://doi.org/10.1162/isec_a_00351

Hurrell, Andrew (2007): *On Global Order. Power, Values, and the Constitution of International Society.* Oxford: Oxford University Press. Online: https://doi.org/10.1093/acprof:oso/9780199233106.001.0001

Ikenberry, G. John (2011): *Liberal Leviathan. The Origins, Crisis, and Transformation of the American World Order.* Princeton: Princeton University Press. Online: https://doi.org/10.2307/j.ctt7rjt2

Lake, David A. (2009): *Hierarchy in International Relations.* Ithaca, New York: Cornell University Press.

Narlikar, Amrita (2013): *New Powers. How to Become One and How to Manage Them.* New York: Columbia University Press.

United Nations (1945): *Charter of the United Nations.* Online: https://www.un.org/en/about-us/un-charter

United Nations General Assembly (2022): *Aggression against Ukraine* (A/RES/ES-11/1). Online: https://docs.un.org/en/A/RES/ES-11/1

United Nations General Assembly (2022): *Territorial Integrity of Ukraine: Defending the Principles of the Charter of the United Nations* (A/RES/ES-11/2). Online: https://digitallibrary.un.org/record/3990673?v=pdf

NEMZETBIZTONSÁGI SZEMLE
14. évfolyam (2026) 1. szám 57–68. | DOI: 10.32561/nsz.2026.1.5

Erdélyi Ákos[1]

A pszichológiai boncolás elméleti alapjai és alkalmazási lehetőségei

A magányos merényletek, különösen az iskolai lövöldözések elemzés-értékelése során

Theoretical Foundations of Psychological Autopsy and Its Potential Applications

Analysis and Evaluation of Lone-Actor Attacks, Particularly School Shootings

A pszichológiai boncolás (psychological autopsy, PA), mint alkalmazott pszichológiai eljárás, a kevésbé validált pszichológiai eljárások közé tartozik. Ennek oka abban keresendő, hogy a PA nem rendelkezik egzakt, szisztematikus módszertannal, sőt, konceptualizálása is kezdetleges. Annyi azonban bizonyos, hogy a módszer eredetileg annak eldöntését segíti, hogy egy halál természetes úton, baleset miatt, öngyilkosság révén vagy gyilkosság eredményeként következett-e be. Ez az alaptézis fejleszthető tovább és egészíthető ki a magányos merénylők radikalizációjának vizsgálatával, legyen szó iskolai lövöldözőkről vagy öngyilkos merénylőkről. Ezen írás célja bemutatni a pszichológiai boncolás elméleti hátterét és gyakorlati alkalmazhatóságát. Mint az megállapítható, annak ellenére, hogy a PA nem rendelkezik jól meghatározott keretekkel és módszertannal, annyi bizonyos, hogy alkalmazása új szintre emeli a felderítés és elhárítás támogatására szolgáló pszichológiai eljárások eszköztárát.

Kulcsszavak: *pszichológiai boncolás, személyiségelemzés, magányos merényletek, terrorizmus*

[1] Krízisintervenciós szakpszichológus-jelölt, kriminológus, PhD-hallgató, egyetemi tanársegéd, Nemzeti Közszolgálati Egyetem Rendészettudományi Kar Rendészeti Magatartástudományi és Kriminálpszichológia Tanszék, e-mail: erdelyi.akos@uni-nke.hu

Psychological Autopsy (PA), as an applied psychological procedure, belongs to the category of less validated psychological methods. This is primarily due to the fact that PA lacks an exact, systematic methodology and, furthermore, its conceptualisation is also defined rather briefly. What is certain, however, is that the original purpose of the method is to help determine whether a death occurred due to natural causes, an accident, suicide, or homicide. This foundational premise can be further developed and expanded to include the examination of radicalisation processes in lone actor terrorists, such as school shooters or suicide bombers. The aim of this paper is twofold: first, to present the theoretical background of Psychological Autopsy, and second, to demonstrate its practical applicability. As can be established, even though PA lacks well-defined frameworks and methodology, its application undoubtedly elevates the toolkit of psychological procedures intended to support investigation and prevention efforts to a new level.

Keywords: *psychological autopsy, personality analysis, lone-actor attacks, terrorism*

Bevezetés

Általánosan megfigyelhető jelenség, hogy a bűncselekményekről szóló tudósításokban sok esetben találkozunk olyan – költői – kérdésekkel, amelyek a bűnelkövetők motivációira igyekeznek reflektálni és azokat feltárni. Kifejezetten igaz ez azokra az esetekre, amelyek valamilyen oknál fogva a társadalom fokozott érdeklődésére tesznek szert, vagy a különösen kegyetlen elkövetési magatartás miatt, vagy azért, mert speciális sértetti vagy elkövetői körrel rendelkeznek. A 2023-as belgrádi iskolai lövöldözés után például azt próbálták megérteni, hogy mi vihetett rá egy akkor mindössze 13 éves fiatal fiút, hogy kilenc emberrel végezzen, vagy hogy mi vezérel egy 12 éves lányt, hogy halállistát készítsen, és az iskolában hátba szúrja egy osztálytársát. A miértek feltárása többféleképpen történhet, amiben számos módszer segíthet – egyik ilyen módszer a pszichológiai boncolás, amely hazánkban még kevésbé alkalmazott eljárás.

A pszichológiai boncolás elméleti alapjai

A pszichológiai boncolás (*psychological autopsy,* PA) megjelenése a múlt század közepére nyúlik vissza, ennek ellenére igazán nagy figyelmet mégis csak napjaink tudományos munkáiban kapott.[2]

A PA-t annak érdekében dolgozták ki a 20. század második felében, hogy segítse a nyomozó hatóság munkáját azokban az esetekben, amikor kétség merül fel, hogy egy halál természetes úton következett be, esetleg baleset, öngyilkosság vagy gyilkosság eredménye-e.[3] Noha az első PA-k több mint 70 éves múltra tekintenek vissza, az azóta

[2] Amritha et al. 2025; Johal–Appleby–Turnbull 2024; Sablone et al. 2024; Posa et al. 2023; Weinberger–Botello–Gross 2018; Saxena–Saini 2017.

[3] Amritha et al. 2025; Sablone et al. 2024; Posa et al. 2023; Weinberger–Botello–Gross 2018; Saxena–Saini 2017; Canter 2000; Shneidman 1994.

eltelt évtizedek ellenére a fentinél pontosabb definíció vagy szisztematikus módszertan nem áll rendelkezésünkre.[4]

Az első PA-elemzéseket két pszichológus, Shneidman és Farberow készítette az 1950-es években, akik akkoriban a Los Angeles-i Öngyilkosság-megelőzési Központ *(Los Angeles Suicide Prevention Centre)* munkatársai voltak, és a halottkémi hivatal felkérésére segédkeztek a nem egyértelmű öngyilkosságok vizsgálatában.[5] Egyszer a központ pincéjében egy dobozt találtak, amely több mint 200 búcsúlevelet tartalmazott, és ezeknek, valamint az öngyilkosság egyéb vonatkozásainak tanulmányozásába kezdtek.[6] Tudományos munkájuk során ők eljárásként definiálták a PA-t, amely az elhunyt személy életét retrospektív módon rekonstruálja, az elhalálozás körülményeire összpontosít, és arra keresi a választ, hogy az elhunytnak milyen szándékai voltak a saját halálával kapcsolatban (azaz saját elhatározásból vetett véget az életének, vagy sem), vagy miért éppen abban az időben következett be a halál.[7]

A PA lényege, hogy rekonstruálják az elhunyt személy utolsó napjait, és sok egyéb tényező mellett elemzik a halál beálltát megelőző mentális állapotát is. A vizsgálat során minden lehetséges információt begyűjtenek az elhunyttal kapcsolatban, amelyek közvetlenül vagy közvetve utalhatnak azokra a releváns tényezőkre, amelyek segíthetnek az elhunyt személy szokásainak feltérképezésében, személyiségének elemzésében, életmódjának és társas kapcsolatainak azonosításában.[8] Az adat- és információgyűjtés elsődleges forrása az elhunyttal kapcsolatban állók köre, így családja, barátai, közvetlen kollégái és ismeretségi köre, például háziorvosa. A tanúk meghallgatása mellett információforrás lehet minden egyéb olyan körülmény, amely az elhunythoz kapcsolódik, úgymint pénzügyi helyzete, orvosi dokumentációi, szocioökonómiai jellemzői, társadalmi helyzete/státusza, mindennapi szokásai. Murthy ezt úgy összegzi, hogy az elhunyttal kapcsolatos információk jellegük alapján három típusba sorolhatók be:[9]

- az *életrajzi adatok* az elhunyt szociodemográfiai információit tartalmazzák;
- a *személyes információk* között találjuk az elhunyt mentális állapotának és személyiségének jellemző karakterisztikáit, társas kapcsolatait, életmódját, az esetleges stresszorokat, valamint a főbb életeseményeket;
- míg a *másodlagos információkhoz* elsősorban a családi anamnézisből, a bűnügyi nyilvántartásból vagy épp a búcsúlevélből juthatunk hozzá.

Amint látjuk, a PA kezdeti alkalmazása azt a célt szolgálta, hogy megállapítsák a kétes halálesetek pontos okát, ma pedig már az egyik leggyakrabban alkalmazott eljárás a szuicidium kockázati tényezőinek vizsgálata.

Az évek alatt két típusát dolgozták ki: a szuicidium pszichológiai boncolása (*suicide psychology autopsy*, SPA) az áldozat közvetlenül az öngyilkosság előtti pszichológiai állapotának felmérésére fókuszál, míg a kétes halálesetek pszichológiai boncolása (*equivocal death*

[4] Sablone et al. 2024; Conner et al. 2021; Menon et al. 2020; Murthy 2010.
[5] Johal–Appleby–Turnbull 2024; Posa et al. 2023; Weinberger–Botello–Gross 2018; Saxena–Saini 2017; Canter 2000.
[6] Murthy 2010.
[7] Shneidman–Farberow 1961.
[8] Amritha et al. 2025; Sablone et al. 2024.
[9] Murthy 2010.

psychology autopsy, EDPA) a halál valódi okának és módjának feltárására irányuló vizsgálat.[10] A kezdeti célok mellett ma már gyakran alkalmazzák a PA-t az öngyilkosságra fókuszáló epidemiológiai vizsgálatokban, a kockázati profilok felmérésére, a gyermek- és serdülőkori öngyilkosságot elkövetők, valamint az idős korosztály karakterisztikáinak feltárására, illetve az öngyilkossági viselkedéssel összefüggő kockázati tényezők vizsgálatára.[11]

Az öngyilkosság mögött számos ok húzódhat meg: alapja lehet mentális zavar, pszichés funkcióvesztés, lehet egy akut krízis vagy trauma, szocioökonómiai veszteség, de az okok között találjuk az iskolai/kortársbántalmazást, sőt, szélsőséges esetben a radikális csoportok közrehatását is (lásd öngyilkos merényletek). A PA mindezek elemzése során támpontot szolgáltathat a nyomozó hatóság számára, és segítséget nyújthat egy jövőbeni cselekmény időben történő elhárításához. De mégis hogyan?

Mivel a PA során az elhunyt (ebben az esetben a támadást végrehajtó, majd öngyilkosságot elkövető) személy teljes életét feltérképezik, elemzik és értékelik, azonosíthatóvá válnak

- egyrészt azok az életesemények, amelyek közrehatása érzékelhető a radikalizáció egyes lépései során, például kortársközösség elutasítása, elmagányosodás, határozatlan jövőkép, a valahova való tartozás iránti vágy, majd a szélsőséges gondolatok internalizálása;
- másrészt a kihallgatások, az explorációk és a viselkedéselemzés eredményeként az elkövető pszichológiai karakterisztikái, személyiségprofilja is elkészíthető, amely jó kiindulás lehet arra vonatkozóan, hogy milyen személyiséget is rejt egy-egy magányos merénylő.

Itt érdemes megjegyezni, hogy a magányos merénylők kategóriája nem homogén, számos kategóriája van, az öngyilkos merénylőtől az ámokfutón és tömeggyilkoson át egészen az iskolai lövöldözőkig. Az egyes kategóriák pedig más és más elkövetői kört reprezentálnak, akik eltérő pszichológiai karakterisztikákkal, eltérő motivációs bázissal és eltérő áldozatpreferenciával rendelkeznek, így a PA-elemzéseket, azok megbízhatósága miatt, célszerű az egyes elkövetői kategóriákhoz illesztve alkalmazni.

Érdemes lehet a PA felhasználhatóságának kereteit kibővíteni, hiszen az eljárás számos más területen lehet jól alkalmazható:[12] a rendkívüli halálesetek mellett a PA a gyanús eltűnések, valamint az olyan kiemelt cselekmények elemzés-értékelésekor segédkezhet, mint a kiterjesztett öngyilkosság (például családirtás) vagy a magányos jellegű terrorizmus témakörébe tartozó cselekmények esetében, úgymint a magányos merénylők, ámokfutók és iskolai lövöldözők által elkövetett cselekmények elemzése során és az elkövetők radikalizációjának vizsgálatakor. Ezen cselekmények PA-elemzése olyan aspektusokat tárhat fel, amelyek segíthetnek megelőzni egy következő, hasonló cselekményt.

[10] Amritha et al. 2025; Saxena–Saini 2017; Canter 2000.
[11] Sablone et al. 2024.
[12] Sablone et al. 2024.

Szuicidium

Weinberger és munkatársai összefoglaló tanulmányukat azzal a kijelentéssel kezdik, hogy az öngyilkosságnak nincs egzakt, konszenzuson alapuló definíciója,[13] ugyanakkor az öngyilkosság komoly népegészségügyi kérdés napjainkban is. Ezt támasztja alá Szabó János és munkatársainak meglátása is:

> „A szuicid cselekmény hátterében álló lélektani folyamatok vonatkozásában továbbra is kevés megbízható információval rendelkezünk, továbbá a szuicidrizikó-becslő skálák is csak korlátozott prediktív értékkel bírnak. A nemrégiben leírt, úgynevezett szuicidspecifikus szindrómák – mint az akut szuicid affektív zavar és a szuicidkrízis-szindróma – azonban új lehetőségeket nyitnak a szuicid viselkedés komplex értelmezéséhez és az öngyilkossági rizikó becsléséhez."[14]

Annyi azonban bizonyos, hogy az utóbbi évek-évtizedek kutatásai igyekeznek egyre inkább újszerű megközelítések alapján, multidiszciplináris szemlélettel megközelíteni a szuicidológiai kutatásokat, és ma már főként komplex bio-pszicho-szociális szemlélettel vizsgálják a szuicidológia témaköreit. E szemlélet alaptézise, hogy vizsgálódásai során „a biológiai-fiziológiai, pszichiátriai és pszichopatológiai jellemzők mellett figyelembe veszik a lélektani tényezőket, a szociális interperszonális és társadalmi-kulturális faktorokat is".[15] Ez a multidiszciplináris megközelítés adja azoknak a gyakorlati módszereknek az alapjait, amelyek a kockázatértékelésre helyezik a hangsúlyt,[16] legyen szó akár violens, akár non-violens szuicid magatartásról.

A szuicid kockázatértékelés kapcsán dolgozták ki az öngyilkos magatartás kockázatértékelésének háromlépcsős modelljét,[17] amely a szuicid cselekményig vezető út három egymásra épülő lépését határozza meg. Az első lépés az öndestruktív gondolat megjelenése, amelyhez sok esetben társul reménytelenség, kilátástalanság és fájdalom; a második lépcső a valahova való tartozás hiánya, amikor az egyén azt érzi, hogy senkinek a támogatására nem számíthat a gondjai megoldásában; harmadik lépésként az egyénben kialakul az öngyilkosság megvalósításához szükséges állapot, és az egyén elkötelezi magát a szuicid cselekmény végrehajtása mellett.

Az integrált motivációs-akarati modell az úgynevezett akarati moderátorok szerepére helyezi a hangsúlyt. E szerint a modell szerint az akarati moderátorok késztetik igazán cselekvésre az egyént, például az eszközök beszerzésére, a tervezésre, az elszántság megszilárdulására, miközben csökken az egyénben a fájdalomtolerancia, és növekszik az impulzivitás.[18]

A modellek mellett a Szabó és munkatársai által bemutatott két szuicidspecifikus szindróma is újszerű megközelítésbe helyezheti napjaink szuicidkutatásait, és nem utolsósorban mind azok bűnügyi-kriminálpszichológiai, mind műveleti pszichológiai – és

13 Weinberger–Botello–Gross 2018.
14 Szabó et al. 2022: 863.
15 Szabó et al. 2022: 864.
16 Csomós 2023.
17 Szabó et al. 2022; Klonsky–May 2015.
18 O'Connor et al. 2016.

akár nemzetbiztonsági – aspektusainak feltérképezését. Az akut szuicid affektív zavar (*acute suicidal affective disorder,* ASAD) alapja,

> „hogy a szuicid kísérletet megelőző pszichés tünetek nagyon rövid idő alatt alakulnak ki, így ezen felgyorsuló dinamika elemeinek azonosítása révén előre jelezhetővé válik a szuicid cselekmény. Fő összetevői: a szuicid intenciók gyors felerősödése napok vagy órák alatt; a szociális izoláció (súlyos szociális visszahúzódás, társaságkerülés, annak érzése, hogy mások számára terhet jelent); a saját magától való elidegenedés (önutálat, lelki fájdalom); a reménytelenség a helyzet javulásával kapcsolatban; valamint az arousal fokozódása (agitáció, irritabilitás, insomnia, rémálmok)."[19]

A szuicidkrízis-szindróma (*suicide crisis syndrome,* SCS) olyan preszuicidális állapot, amely a vélt vagy valós fenyegetettségre adott, affektív és kognitív diszregulációval járó, váratlanul megjelenő reakciókat foglalja magában. A vezető tünetek közé tartozik az a rögzült és vissza-visszatérő érzés, hogy

> „az egyén az elviselhetetlen helyzet csapdájába esett, mellyel sem megbirkózni, sem belőle kilépni nem képes, és a halál látszik az egyetlen kiútnak, hogy megszabaduljon a gyötrelmektől. Így egyre inkább uralkodóvá válnak a halállal és az öngyilkossággal kapcsolatos gondolatok, és gyakoriak a direkt szuicid ideációk is. További fontos jellemzői a társuló affektív tünetek (depresszió, kétségbeesés, pánikszerű szorongás, lelki fájdalom, akutan kialakuló örömtelenség), a kognitív folyamatok feletti kontroll elvesztése (ruminatio, kognitív rigiditás és beszűkülés, a negatív gondolatok elnyomására tett kísérletek) és a problémamegoldó kapacitás beszűkülése, valamint a hiperarousalhoz társuló változások (agitáció, hipervigilancia, irritabilitás, insomnia). Ezen tünetek gyorsan alakulnak ki és tartósan fennállnak, vagy visszatérően jelentkeznek. Gyakran társul szociális izoláció, mely tovább növeli a szuicid cselekmény rizikóját."[20]

A két szindróma kapcsán már létrejöttek olyan kérdőívek és becslőskálák, amelyek klinikai közegben megbízhatóan tudják előre jelezni a szuicid vulnerabilitást, ugyanakkor ezen szindrómák kriminálpszichológiai vizsgálata még hátravan, amely ugyancsak új szintre emelné az öngyilkossággal kapcsolatos bűnügyi ismereteinket.

Az öngyilkos merényletek

Az öngyilkossággal mint rendkívüli halálesettel leggyakrabban közigazgatási eljárásban találkozunk, legyen szó akár polgári környezetben, akár büntetés-végrehajtási intézetben elkövetett befejezett öngyilkosságról. Ennek megfelelően pedig mind az általános rendőrségi feladatokat ellátó szerv,[21] mind a büntetés-végrehajtás[22] rendelkezik megfelelő

[19] Szabó et al. 2022: 868.
[20] Szabó et al. 2022: 868.
[21] 24/2014. (VII. 11.) ORFK utasítás a rendkívüli halál esetén követendő rendőri eljárásról.
[22] 18/2020. (V. 29.) BVOP utasítás a fogvatartotti krízisek, öngyilkossági kísérletek és önártalmak megelőzéséről; 26/2022. (XII. 21.) BVOP utasítás a büntetés-végrehajtási szervezet műveleti egységeinek működéséről.

szabályzókkal az egészségügyről szóló 1997. évi CLIV. törvény mellett, amely pontosan meghatározza az öngyilkos magatartás keretrendszerét.

Ritkábban esik szó a kiterjesztett öngyilkosságról,[23] ami nem meglepő, tekintve a jelenség alacsony prevalenciáját. Kiterjesztett öngyilkosságról – pszichiátriai megközelítés alapján – akkor beszélünk, ha egy személy más személyt/személyeket a tudta/tudtuk és beleegyezése/beleegyezésük nélkül bevon a szuicid cselekménybe, majd az elkövető a gyilkosságot követő meghatározott időn, rendszerint 24 órán belül öngyilkosságot követ el.[24]

Még ritkábban merülnek fel a szuicid cselekmények nemzetbiztonsági aspektusai, annak ellenére, hogy sok esetben találkozunk öngyilkos magatartással egy-egy terrorcselekmény során, legyen az akár egy terrorszervezethez tartozó öngyilkos merénylő, egy magányos farkas vagy egy iskolai lövöldöző által elkövetett cselekmény – ez utóbbi kriminológiai kategóriában az elkövetők a cselekmény után szignifikánsan magas arányban vetnek véget önkezűleg életüknek.

Az iskolai lövöldözésekről

Az iskolai lövöldözéseket – kriminológiai szempontból – az ámokfutás egyik altípusaként szokás kezelni, habár a terminológia kapcsán nem beszélhetünk konszenzusról: Kulcsár Gabriella kiemeli, hogy a jelenségnek nincs a hazai szakirodalomban rendszeresített terminológiája, így ő a vizsgálódásai során az iskolai ámokfutás terminológiát alkalmazza, tekintettel arra, hogy az iskolai támadás ezen típusa az ámokfutás altémaköreként kezelendő. Mint azt kifejti,

> „az ámokfutás oktatási intézményekben előforduló formája esetében egyetértek a »school shooting« használatával angol és német szövegekben, azonban a magyar nyelv jellemzői nem teszik lehetővé az angol kifejezés egy az egyben történő átemelését. Szó szerinti fordítása (»iskolai lövöldözés«) sajnos – hasonlóan a német változathoz (»Schulschießerei«) – kissé elüt a tudományos nyelvezettől, valamint nem fejezi ki kellőképpen a jelenség specialitását, bár a szóismétlések elkerülése érdekében én is használom elvétve. Az »iskolai ámokfutás« kifejezéssel szemben is felhozható ellenérv, azonban mindenképpen mellette szól, hogy egyértelművé teszi: az ámokfutások egyik formájáról van szó, ezáltal rögtön behatárolja az eset jellemzőit."[25]

Noha az ámokfutásról szóló feljegyzések megjelenése az 1500-as évekre datálható,[26] az első dokumentált iskolai lövöldözés 1974-ben történt a New York állambeli Oleanban, majd 25 évvel később következett be az a tragédia, amely megrázta a világot: 1999. április 20-án két fiatal, Eric Harris és Dylan Klebold tömeggyilkosságot követett el a Colorado állambeli Columbine Középiskolában, megölve 13 embert és megsebesítve további 21 főt, majd saját magukkal is végeztek.[27] Az ezt követő 2 évben további 16 erőszakos iskolai támadás történt az Egyesült Államokban, és a jelenség Európában is megjelent: 1999 és

[23] Bolyky 2015.
[24] Bolyky 2015.
[25] Kulcsár 2016: 19.
[26] Kulcsár 2016.
[27] Pásztor–Angyal 2016.

2006 között Németországban 14 ámokfutást követtek el, amelyek jelentős többsége iskolai lövöldözés volt – 58 ember vesztette életét az ámokfutásokban, és 140-en megsérültek.[28] Magyarországon 2009-ben egy hallgató lövöldözött a Pécsi Tudományegyetem egyik karán, az esetnek halálos áldozatai is voltak.

Az iskolai lövöldözést elkövetőkről keveset tudni – annyit azonban igen, hogy kortársaik rendszerint kiközösítették őket, interperszonális kapcsolataik száma ebből adódóan alacsony volt, és az elkövetők sok esetben, a támadás előtt, halállistát készítettek. A statisztikai adatok alapján azt is tudjuk, hogy az elkövetők rendszerint 14 és 20 év közötti fiúk, akik a cselekményeket általában egyedül követik el – ez alól kivétel például a columbine-i lövöldözés, ahol egy páros hajtotta végre a támadást. Az iskolai ámokfutók nem mutatnak egységes demográfiai profilt, általában nem szenvednek mentális zavarban, és cselekményüket nem az impulzivitás, hanem a nagy fokú megtervezettség jellemzi.[29]

Nemcsak a terminológia kapcsán jutunk kevés információhoz: a jelenség vizsgálata kevésbé volt ez idáig jelentős a hazai tudományos gondolkodásban, lévén, hogy ilyen cselekménnyel ritkán találkozunk a magyar kriminalisztikában. Ám az utóbbi néhány évben hazánkban is megjelentek olyan cselekmények, amelyek könnyen végződhettek volna még nagyobb tragédiával.

Az iskolai lövöldözések pszichológiai-pszichiátriai megközelítése

Az iskolai lövöldözések pszichiátriai megközelítése újszerűnek hangozhat, noha a DSM *(Mentális zavarok diagnosztikai és statisztikai kézikönyve)* a 3. kiadásában leírt egy olyan diagnosztikai kritériumrendszert, amely nagyban hasonlít az ámokfutáshoz.[30] A DSM III-ban[31] közölt izolált explozív zavar diagnosztikai kritériumai az alábbiak voltak:

- Az agresszív impulzussal szembeni ellenállás hiányának egyszeri, erőszakos, külvilág felé irányuló epizódja, amely katasztrofális következményekkel jár másokra nézve.
- Az epizód során kifejtett agresszivitás aránytalanul nagyobb mértékű, mint amit bármilyen kiváltó pszichoszociális stresszor magyarázna.
- Az epizódot megelőzően nem volt jele általános impulzivitásnak vagy agresszivitásnak.
- A zavar nem skizofrénia, antiszociális személyiségzavar vagy alkalmazkodási zavar következménye.

Ezen tünetegyüttesek mentén vélték a kriminológusok azonosítani az átfedést a mentális rendellenesség és az ámokfutás között.

Pásztor Attila és Angyal Miklós tanulmányukban összefoglalják, hogy az iskolai lövöldözők elmeműködése rendszerint nem mutat patológiát, ugyanakkor személyiségműködésükre a nárcisztikus vonások dominanciája jellemző. Inkább introvertáltak, befelé fordulók, sebezhetők, és sok esetben autoagresszív megnyilvánulásaik vannak.[32]

[28] Pásztor–Angyal 2016.
[29] Pásztor–Angyal 2016.
[30] Kulcsár 2016.
[31] American Psychiatric Association 1980.
[32] Pásztor–Angyal 2016.

Az ámokfutások – és így az iskolai lövöldözések – pszichológiai elemzése a patológiás személyiségműködés ellenére mindenképpen hasznos. Ha a korábban tárgyalt szuicidológia oldaláról közelítjük meg a kérdést, akkor látható egyrészt, hogy az elkövetők anamnézisében autoagresszív magatartások dominanciája fedezhető fel, másrészt az is, hogy az iskolai lövöldözések elemzése során szinte valamennyi elkövetőnél azonosíthatók a DSM-III-ban bemutatott modellek egyes aspektusai.

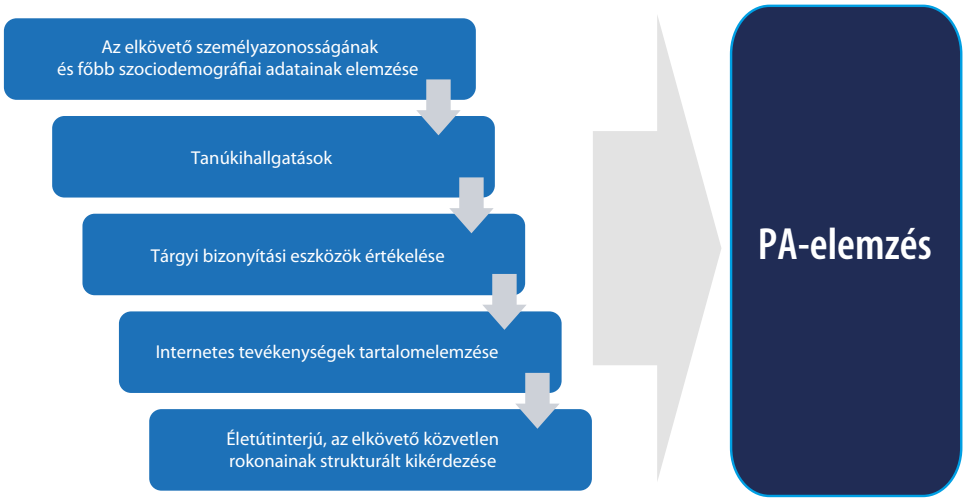
A háromlépcsős modell egyes szintjein olyan tényezők sorakoznak fel, mint a *bullyingból* fakadó csökkent önértékelés, a „semmire sem elég jó" érzése (első lépcső), a kirekesztettség élménye (második lépcső), majd a szélsőséges erőszakos viselkedésformák internalizálása, a stresszor megsemmisítése iránti vágy és az erőszakos fantáziatevékenység, amelyben a fantázia fókusza a bosszúra és a megtorlásra helyeződik (harmadik lépcső). Az akarati moderátorok sorában pedig megtaláljuk többek között a *copycat* jelenséget, amelynek lényege, hogy egy személy más elkövetők által megvalósított cselekményt vesz alapul a saját cselekménye végrehajtásakor, és mintegy leutánozza a korábbit.[33] Ez látható az 1999-es, Columbine Középiskolában elkövetett iskolai lövöldözés után.[34] Szintén fontos jelenség az úgynevezett Werther-effektus:[35] Goethe 1779-ben megjelent, *Az ifjú Werther szenvedései* című műve hatására megugrott az öngyilkosságot elkövető fiatal férfiak száma, akik több hasonlóságot fedeztek fel saját maguk és a regény főhőse között – így, inspirálódva a műtől, ők maguk is öngyilkosságot követtek el. Az 1974-es támadás után az Egyesült Államokban is megugrott az öngyilkosságot elkövetők száma, akiket a médiában látottak ösztökéltek szuicidiumra – a jelenséget David Phillips szociológus nevezte el Werther-effektusnak: „ha valaki vagy valakik irodalmi mű vagy a média hatására követnek el öngyilkosságot vagy gyilkosságot, akkor ezen modellhatás jelenségéről, *Werther effektus*-ról beszélünk".[36]

Hogyan alkalmazható a PA a magányos merényletek, különösen az iskolai lövöldözések elemzés-értékelésében?

Első lépésként azonosítani szükséges az öngyilkos elkövetők kilétét és alapvető személyes és szociodemográfiai adatait, mint a nem, iskolai végzettség, családi állapot stb. Ezután kezdődhet a részletes adat- és információgyűjtés.

Második lépésben kerül sor a tanúk kihallgatására, illetve ha csak közvetett lehetőség van a PA-vizsgálatra, akkor a tanúkihallgatások jegyzőkönyveinek áttekintésére. Ezek alapján megismerjük az öngyilkos elkövető életét – legalábbis azt az életét és énjét, amelyet társas kapcsolataiban mutatott. Körvonalazhatók a mindennapi rutinjai, szokásai és a személyiségének viselkedéses komponense, például a megtévesztésre és manipulációra való hajlam, az erőszakos szélsőségesség mértéke, fantáziaműködésének dinamikája. Ugyancsak azonosíthatók azok a traumatikus események, amelyek az elkövető szélsőséges viselkedésének kialakulásához vezettek. A tanúkihallgatások számos információt adnak

[33] Coleman 2004.
[34] Gladwell 2000; O'Toole 1999.
[35] Pásztor–Angyal 2016.
[36] Pásztor–Angyal 2016: 198.



1. ábra: Az öngyilkos merényletek elemzés-értékelésének lépései a pszichológiai boncolás módszertanával
Forrás: a szerző szerkesztése

nekünk – az összegzésre is komoly figyelmet kell fordítani, hiszen a tanúk által elmondott nagy mennyiségű információ feldolgozása kiemelt szerepet kap a cselekmény megértésében.

A harmadik lépésben a tárgyi bizonyítási eszközként értékelt és begyűjtött adatok kerülnek górcső alá. Ilyenek lehetnek például az elkövető egészségügyi dokumentációi, naplója, rajzai és egyéb személyes dolgai.

Negyedik lépésben az elkövető internetes tevékenységének elemzésére kerülhet sor, különösen, ha információ merül fel arra vonatkozóan, hogy az elkövető az internetes tartalmakat követve tervezhette meg és hajthatta végre a cselekményt. Azt is megtudhatjuk, hogy az elkövető milyen online közösségeknek volt a tagja, kikkel chatelt a legtöbbet, és milyen témák iránt érdeklődött. Ugyancsak itt kerülhet sor az elkövető internetes tevékenységének tartalomelemzésére, például a norvég Anders Behring Breivik az ámokfutás előtt közzétette manifesztumát az interneten, ahogyan korábban az Unabomberként elhíresült Ted Kaczynski is. Az ilyen tartalmak elemzése pszichológiai mélyfúráshoz ad alapot, és segít a motivációk megértésében.

Miután minden objektív adatot elemeztünk, ötödik lépésben nyílhat lehetőség az elkövető közvetlen családtagjaival folytatott mélyinterjúra. Ezzel a lépéssel azért érdemes várni, hogy a lehető legpontosabb képet kapjuk az elkövetőről, és valamennyire megismerjük a viselkedését, a szokásait – az életét –, és így kevésbé lehetünk ítélkezők az interjú során.

A hatodik lépés pedig az elemző-értékelő PA-jelentés elkészítése, az öngyilkos elkövető személyiségvizsgálata, amely a fentieken túl tartalmazhatja azt is, hogy az illető egyedül követte el a cselekményt, vagy tartani kell egy esetleges, *copycat* vagy Werther-effektus által motivált utánzó elkövetőtől.

Az elemzés-értékelés lépéseit a pszichológiai boncolás módszertanával az 1. ábra szemlélteti.

Összegzés

Jelen írás célja végső soron kettős. Egyrészt a pszichológiai boncolás mint alkalmazott lélektani eljárás alapjainak bemutatása, másrészt a magányos merényletek egy speciális esetének, az iskolai lövöldözések PA-elemzésének gyakorlati alkalmazhatóságát bemutató rövid leírás.

A PA-t eredetileg annak érdekében dolgozták ki az 1950-es években, hogy a gyanús halálesetek vizsgálatában nyújtson segítséget. Ez a felhasználási kör bővíthető, hiszen az elemzés-értékelés olyan esetekben is hasznos lehet, mint a gyanús eltűnések felderítésének támogatása vagy a szélsőséges viselkedés kockázatának bejóslása.

Habár a pszichológiai boncolás számos esetben képes segíteni egy-egy haláleset jellegének és módjának vizsgálatát, nem szabad elfeledkeznünk arról, hogy az eljárással kapcsolatban még számos kérdésre kell megbízható választ találnunk. Mint arra Johal és munkatársai is utalnak,[37] a PA reliabilitás- és validitásvizsgálata még hosszú út előtt áll, amelyen végighaladva választ kell találnunk a PA konceptualizálásbeli, etikai, kulturális különbségekből eredő eljárási kérdéseire és szisztematikus módszertani bizonytalanságaira. Annyi azonban bizonyos, hogy az eljárás alkalmazásával készült elemző-értékelő jelentések újszerű, innovatív megközelítésből képesek vizsgálni egy-egy jelenség és az elkövető pszichológiai karakterisztikáit, ami nemcsak a megértésben, hanem a megelőzésben is nagy segítség lehet.

Felhasznált irodalom

24/2014. (VII. 11.) ORFK utasítás a rendkívüli halál esetén követendő rendőri eljárásról

18/2020. (V. 29.) BVOP utasítás a fogvatartotti krízisek, öngyilkossági kísérletek és önártalmak megelőzéséről

26/2022. (XII. 21.) BVOP utasítás a büntetés-végrehajtási szervezet műveleti egységeinek működéséről

American Psychiatric Association (1980): *Diagnostic and Statistical Manual of Mental Disorders*. Third Edition. Washington, D.C.: APA.

Amritha, Roy et al. (2025): Psychological Autopsy: Overview of Equivocal Deaths, Suicides and Homicide-Suicides. *Journal of Forensic and Legal Medicine,* 110, 102813. Online: https://doi.org/10.1016/j.jflm.2025.102813

Bolyky Orsolya (2015): A kiterjesztett öngyilkosságok kriminológiai háttere. *Kriminológiai tanulmányok,* (52), 59–76.

Canter, David V. (2000): Psychological Autopsies. In Siegel, Jay A. – Saukko, Pekka J. – Houck, Max M. (szerk.): *Encyclopedia of Forensic Sciences*. London: Elsevier. Online: https://doi.org/10.1006/rwfs.2000.0782

Coleman, Loren (2004): *The Copycat Effect. How The Media and Popular Culture Trigger the Mayhem in Tomorrow's Headlines*. New York: Praview Pocket Books.

Conner, Kenneth R. et al. (2021): Introducing the Psychological Autopsy Methodology Checklist. *Suicide and Life-Threatening Behavior,* 51(4), 673–683. Online: https://doi.org/10.1111/sltb.12738

[37] Johal–Appleby–Turnbull 2024.

Csomós István (2023): Az erőszak kockázatértékelése – pszichológiai szempontok. *Scientia et Securitas,* 4(1), 31–35. Online: https://doi.org/10.1556/112.2023.00147

Gladwell, Malcolm (2000): *The Tipping Point. How Little Things Can Make a Big Difference*. London: Little, Brown and Company.

Johal, Gursharan – Appleby, Louis – Turnbull, Pauline (2024): Is There Still a Place for Psychological Autopsy in Suicide Research? A Literature Review of Methodological Limitations and Recommendations for Future Development. *International Review of Psychiatry,* 36(4–5), 494–502. Online: https://doi.org/10.1080/09540261.2024.2378075

Klonsky, E. David – May, Alexis M. (2015): The Three-Step Theory (3ST): A New Theory of Suicide Rooted in the „Ideation-to-Action" Framework. *International Journal of Cognitive Therapy,* 8(2), 114–129. Online: https://doi.org/10.1521/ijct.2015.8.2.114

Kulcsár Gabriella (2016): *Az iskolai ámokfutások*. Pécs: Virágmandula Kft.

Menon, Vikas et al. (2020): Psychological Autopsy: Overview of Indian Evidence, Best Practice Elements, and a Semi-Structured Interview Guide. *Indian Journal of Psychiatry,* 62(6), 631–643. Online: https://doi.org/10.4103/psychiatry.IndianJPsychiatry_331_20

Murthy, Vasudeva (2010): Psychological Autopsy – A Review. *Al Ameen Journal of Medical Sciences,* 3(3), 177–181.

O'Connor, Rory C. et al. (2016): The Integrated Motivational-Volitional Model of Suicidal Behaviour. In O'Connor, Rory C. – Pirkis, Jane (szerk.): *The International Handbook of Suicide Prevention*. Hoboken: Wiley-Blackwell, 220–240. Online: http://dx.doi.org/10.1002/9781118903223.ch13

O'Toole, M. E. (1999): *The School Shooter. A Threat Assessment Perspective*. Quantico: FBI Academy.

Pásztor Attila – Angyal Miklós (2016): Iskolai lövöldözők. Kriminálpszichológiai adalékok a megértéshez és a beavatkozási lehetőségekhez. *Psychiatria Hungarica,* 31(2), 193–204.

Posa, Franco et al. (2023): Psychological Autopsy Structured on Individual Cases: Methodological Considerations for a New Protocol. *Medical Research Archives,* 11(4). Online: https://doi.org/10.18103/mra.v11i3.3719

Sablone, Sara et al. 2024: Psychological Autopsy: A Powerful Tool in Forensic Investigations. *Forensic Science,* 4(4), 635–646. Online: https://doi.org/10.3390/forensicsci4040044

Saxena, Geetika – Saini, Vineeta (2017): Psychological Autopsy – A Way to Revealing the Enigma of Equivocal Death. *International Journal of Forensic Sciences,* 2(2), 1–8. Online: http://dx.doi.org/10.23880/IJFSC-16000123

Shneidman, Edwin S. (1994): The Psychological Autopsy. *American Psychologist,* 49(1), 75–76. Online: https://doi.org/10.1037/0003-066X.49.1.75

Shneidman, Edwin S. – Farberow, Norman L. (1961): Sample Investigations of Equivocal Deaths. In Farberow, Norman L. – Shneidman, Edwin S. (szerk.): *The Cry For Help*. New York: McGraw-Hill, 118–129.

Szabó János et al. (2022): Az öngyilkossági rizikó becslése a klinikai gyakorlatban. A jelen kihívásai és a jövő perspektívái. *Orvosi Hetilap,* 163(22), 863–870. Online: https://doi.org/10.1556/650.2022.32464

Weinberger, Linda E. – Botello, Timothy E. – Gross, Bruce H. (2018): Psychological Autopsy: Consultative Tool for Suicide Determination. In Sathyavagiswaran, Lakshmanan – Rogers, Christopher B. (szerk.): *Multidisciplinary Medico-Legal Death Investigation: Role of Consultants*. Los Angeles: Academic Press, 119–137. Online: https://doi.org/10.1016/B978-0-12-813818-2.00007-7

Tartalom

Bor Olivér: *Autonóm drónrendszerek kiberbiztonsága: kockázatok és reziliencia* 3
Solti István: *A nemzetbiztonsági szolgálatokról szóló törvény előképei* 23
Fórizs Sándor: *Külföldre szökés és kémkedés bűntettének vádja* 36
Gábor Andrékó: *Why Institutional Isolation Fails* 46
Erdélyi Ákos: *A pszichológiai boncolás elméleti alapjai és alkalmazásási lehetőségei* 57