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