

Földes Tibor¹

Védett létesítmények fizikai védelme

Különös tekintettel a katonai kritikus
infrastruktúrákra

Physical Protection of Secured Facilities

With Special Emphasis on Military Critical Infrastructures

Absztrakt

A kritikus infrastruktúrák fizikai védelme olyan összetett, többváltozós rendszertervezési kérdés, ahol a fizikai, információs és humán alrendszerek nem izoláltan, hanem egymás működését folyamatosan befolyásolva határozzák meg a rendszer egészének teljesítményét. Ez a komplexitás különösen a katonai létesítményeknél érzékelhető, ahol a tapasztalatok tartósan magas fenyegetési terhelést és jelentős sokféleséget mutatnak, és ezek a tényezők a tervezési és üzemeltetési döntéseket közvetlenül befolyásolják.

A tanulmány a katonai kritikus infrastruktúrák fizikai védelmét rendszerszintű összefüggések mentén elemzi, külön figyelmet fordítva a többretegű védelmi architektúrákra, a korszerű műszaki megoldások alkalmazhatóságára és a szabályozási környezet tényleges hatásaira. A vizsgálat olyan nemzetközi doktrínákra, mérnöki irányelvekre és hazai-európai szabványokra épül, amelyek a gyakorlatban bizonyítottan stabil és összehasonlítható keretet adnak a fizikai védelmi rendszerek tervezéséhez és értékeléséhez. A vizsgálat rámutat, hogy a fizikai védelem hatékonyságát döntően az alrendszerek közötti információáramlás minősége, a késleltetési képesség és a reagálási lánc integráltsága határozza meg, amelyek együttesen befolyásolják a rendszer műveleti teljesítményét.

Kulcsszavak: fizikai védelem, kritikusinfrastruktúra-védelem, védelmi architektúra, humán tényező, ellenálló képesség

¹ Okleveles kiberbiztonsági szakértő, doktori hallgató, Nemzeti Köszolgálati Egyetem Katonai Műszaki Doktori Iskola, e-mail: foldestibor252@gmail.com

Abstract

The physical protection of critical infrastructures is a complex, multivariable system-design challenge in which the physical, informational, and human subsystems do not operate in isolation, but continuously influence one another's functioning and jointly determine the overall performance of the system. This complexity is particularly evident in military facilities, where operational experience consistently indicates high threat intensity and considerable diversity, factors that directly shape planning and operational decision-making. The study analyses the physical protection of military critical infrastructures through system-level interdependencies, with particular emphasis on multilayered defence architectures, the applicability of modern engineering solutions, and the practical effects of the regulatory environment. The analysis builds on international doctrines, engineering guidelines, and national–European standards that have proven in practice to provide a stable and comparable framework for the design and evaluation of physical protection systems. The findings highlight that the effectiveness of physical protection is fundamentally determined by the quality of information flow between subsystems, the system's ability to delay hostile actions, and the integration of the response chain – factors that collectively shape the operational performance of the entire system.

Keywords: physical security, critical infrastructure protection, protective architecture, human factors, resilience

Bevezetés

A tudományos felfedezések, az innovációban rejlő képességek és lehetőségek szinte folyamatosan változtatták és változtatják a biztonsági környezetet.² A védett létesítmények fizikai védelme a biztonságstudomány, a hadtudomány és a mérnöki tudományok olyan metszéspontján helyezkedik el, ahol a tervezési és műveleti döntések során az interdiszciplinaritás nem elméleti jelenség, hanem a mindennapi gyakorlatot meghatározó működési feltétel.

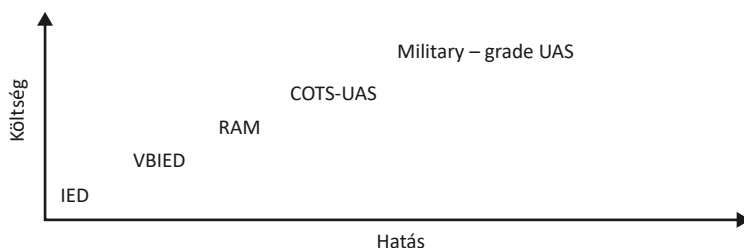
A katonai kritikus infrastruktúrák – a repülőterektől a logisztikai és parancsnoki központokon át a kommunikációs hálózatokig – közvetlen hatást gyakorolnak a haderő műveleti és reagálóképességére, így működésük sérülése azonnal stratégiai következményekkel jár. Ez a közvetlen összefüggés magyarázza, hogy a kritikus infrastruktúrák védelme miért kiemelt stratégiai jelentőségű a katonai tervezésben. Az elmúlt két évtized tapasztalatai szerint a fenyegetési skála jelentősen bővült és differenciálódott, ami a tervezési folyamatok számos elemét – különösen a zónarendszer kialakítását és a reagálási protokollokat – újragondolásra kényszerítette. E fenyegetések közös jellemzője a nehezen előre jelezhető működés és az aránytalan műveleti hatás. Az IED³-k – különösen a járműbe telepített robbanóeszközök (VBIED⁴), a járművel

² FÖLDES 2025: 146.

³ IED: *improvised explosive device* – házilag összeállított, nem ipari gyártású robbanóeszköz.

⁴ VBIED: *vehicle-borne improvised explosive device* – járműbe rejtett rögtönzött robbanóeszköz.

végrehajtott támadások (RAM⁵), valamint a kereskedelmi drónok (COTS UAS⁶) nemcsak fizikai károkat okoznak, hanem a műveleti folytonosságot és a személyi állomány biztonságát is komolyan veszélyeztetik. A fenyegetések heterogén természete miatt a védelmi rendszernek képesnek kell lennie arra, hogy a közvetlen támadásokat, a rejtett behatolást és a robbanóanyag-bejuttatást párhuzamosan vagy gyors egymásutánban kezelje, amit az 1. ábra a fenyegetési skála alakulásán keresztül szemléltet.



1. ábra: A fenyegetési skála alakulása

Forrás: a szerző szerkesztése

Kovács Zoltán rámutat, hogy az IED-knek az egyszerű előállíthatóság, az alacsony költség és a médiában kiváltott pszichológiai hatás miatt nemcsak harcászati, hanem stratégiai jelentősége is van. A közelmúlt műveleti tapasztalatai jól szemléltetik a fentiek gyakorlati jelentőségét.⁷ Az ukrajnai hadszíntéren 2022 óta több esetben is megfigyelhető volt, hogy viszonylag alacsony költségű, kereskedelmi forgalomban elérhető pilóta nélküli eszközök képesek voltak jelentős hatást gyakorolni katonai infrastruktúrára. Ezek az esetek rávilágítanak arra, hogy a fenyegetések hatékonysága nem feltétlenül a technológiai komplexitásból, hanem a védelmi rendszer hiányosságainak kihasználásából ered.

A NATO doktrínái – különösen az AJP-3.14 (2024) – a fizikai védelmet a force protection olyan integrált elemének tekintik, amely a fenyegetések észlelésétől a késleltetésen át a végrehajtott elhárításig a teljes műveleti ciklus minden szakaszában meghatározó szerepet tölt be. Az AJP-3.14 (2024) a fizikai védelem négy funkcióját – megelőzés, észlelés, késleltetés, elhárítás – egymásra épülő folyamatként értelmezi, hangsúlyozva, hogy az idő és az információáramlás minősége döntően befolyásolja a rendszer valós műveleti hatékonyságát. A doktrína kiemelten kezeli a rendszerszemléletű megközelítést, és a többrétegű védelem következetes alkalmazását tekinti alapelvnek, mivel ez biztosítja a fenyegetések gyengítését több ponton. A 2024. évi LXXXIV. törvény a hazai ellenállóképesség-szabályozást a szolgáltatásalapú ellenálló képességi modell irányába mozdította el, amely a korábbi létesítmény-központú megközelítést kiegészítve a működésfolytonosság, az éves gyakorlatok és a bizonyítható kockázatértékelés követelményeit erősítette meg. A normatív átalakulás következtében a hangsúly mindinkább a működésfolytonosság bizonyítható biztosítására, az éves gyakorlatok

⁵ RAM: *rocket-assisted munition* – rakétahajtással indított lőszer.

⁶ COTS: *commercial-off-the-shelf* – kereskedelmi forgalomban beszerezhető (polgári célú).

⁷ Kovács 2013: 78.

szabályozott végrehajtására és az intézményközi együttműködés mérhető fejlesztésére került, amelyek együtt az ellenálló képesség tényleges erősödését szolgálják. A fizikai védelem ebben a megközelítésben már nem csupán műszaki vagy építészeti feladat, hanem olyan alkalmazkodó biztonsági rendszer, amelynek működése folyamatos alkalmazkodást igényel a változó fenyegetési mintázatokhoz és a műveleti környezet dinamikus sajátosságaihoz.

A fizikai védelem rendszerszintű értelmezése

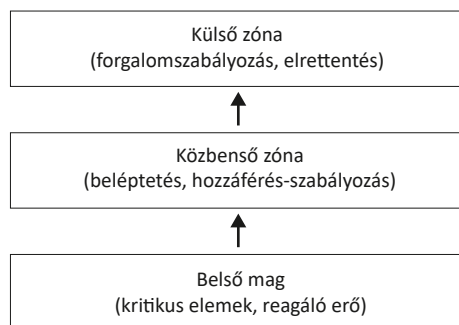
A fizikai védelem a katonai és kritikus infrastruktúrák biztonsági architektúrájának azon eleme, ahol a műszaki megoldások, a működési eljárások és az emberi tényezők nem elkülönülten, hanem valós időben, egymásra ható, folyamatos visszacsatolásban működő rendszerként jelennek meg.

A katonai infrastruktúrák sajátossága miatt a fizikai védelemnek nemcsak a közvetlen támadások elhárítására kell fókuszálnia, hanem a túlélőképesség és a műveleti folytonosság fenntartására is. Ez magában foglalja a kritikus képességek megfelelő redundanciáját, a parancsnoki struktúrák rezilienciáját és a támadás utáni helyreállítási folyamatok olyan szintű integrációját, amely lehetővé teszi a műveleti képességek gyors visszaállítását. A cél tehát nem csupán a támadás megállítása, hanem annak biztosítása is, hogy a létfontosságú katonai funkciók a támadás közben és azt követően is fenntarthatók legyenek.

A rendszerszemlélet egyik központi eleme a többrétegű védelem, amely térben és funkcionálisan elkülönülő, egymást kiegészítő védelmi zónákból áll. A külső zónák elsődleges feladata az elrettentés, a korai észlelés támogatása és a forgalom kontrollálása; a közbenső zónák a hozzáférés korlátozására és a támadó késleltetésére szolgálnak; míg a belső zónák a kritikus elemek közvetlen védelmét és a gyors reagálást biztosítják. A belső mag a kritikus rendszerek közvetlen védelmét és a gyors reagálás feltételeit teremti meg. A kockázatalapú megközelítés jelentőségét a NATO-szintű értékelések és a gyakorlati tapasztalatok is alátámasztják, különösen azokban az esetekben, amikor a fenyegetések gyors változása miatt a statikus védelmi modellek már nem alkalmazhatók. A kockázatelemzés gyakorlati alkalmazása ugyan nem minden esetben követi a formális módszertani előírásokat, mégis a fenyegetés–sebezhetőség–következmény hármásának elemzése nélkülözhetetlen a megalapozott védelmi döntésekhez. A CARVER⁸- és RAMCAP⁹-alapú rangsorolási módszerek alkalmazása tovább növeli a döntéshozatal átláthatóságát és objektivitását, különösen akkor, amikor a rendelkezésre álló erőforrások szűkösek, ami jól látható a többrétegű fizikai védelmi architektúra egymásra épülését bemutató 2. ábrán is.

⁸ CARVER: *criticality, accessibility, recuperability, vulnerability, effect, recognizability* – célpontértékelési módszer.

⁹ RAMCAP: *risk analysis and management for critical asset protection* – kockázatalapú értékelési módszer.



2. ábra: Többrétegű fizikai védelmi architektúra

Forrás: a szerző szerkesztése

Kovács repülőtéri példái is megerősítik, hogy a külső és belső védelmi zónák csak integrált működésükben hatékonyak: a járművek előszűrése, az ellenőrző-átesztelő pontok működtetése és az optikai-elektronikai érzékelőrendszerek együttese teremti meg a többvonalas védelmi architektúra tényleges hatékonyságát.¹⁰ A szerző repülőtéri esettanulmánya alapján a VBIED-ek elleni védelem kulcsa a megközelítési útvonalak kontrollja: a forgalomlassító berendezések, tüskés útzárak, kiemelkedő oszlopok és sorompók alkalmazása hatékonyan csökkenti annak esélyét, hogy a jármű a kritikus létesítmények közvetlen közelébe jusson.¹¹

A fizikai védelmi rendszerek tervezése a helyzetértékeléstől a követelmények meghatározásán át a megvalósításig és a visszamérésig tartó, PDCA¹²-logikára épülő iteratív folyamat, amely minden ciklusban új finomhangolási lehetőségeket tár fel. E folyamat a dokumentált működés rendjét – biztonsági terveket, üzemeltetési eljárásokat, karbantartási protokollokat – is integrálja, amelyek a rendszer stabilitásának alapfeltételei. A műszaki követelményrendszer – beleértve a DoD UFC-szabványokat, a FEMA 42613 ajánlásait és az EN 1354114 vizsgálati kereteit – meghatározza a robbanás elleni védelem fő paramétereit, különös tekintettel a védőtávolságok megállapítására és a szerkezeti megerősítési követelményekre. Ugyanakkor e dokumentumok alkalmazása mindig telephely-specifikus értelmezést igényel. E szabványok közös pontja, hogy a védelmet rendszerszinten értelmezik: az üvegezés, a keret, a rögzítés és a csatlakozó szerkezet egységét tekintik a teljesítmény mércéjének.

A fizikai védelem ugyanakkor nem választható el a C2/C4ISR15-rendszerek által biztosított információs és vezetésirányítási környezettől. Az érzékelőrendszerekből, beléptetési pontokból és megfigyelő alrendszerekből származó adatok csak akkor képeznek valódi védelmi értéket, ha integrált módon, döntéstámogató logikába

¹⁰ Kovács 2013: 81–82.

¹¹ Kovács 2014: 108.

¹² PDCA: *plan-do-check-act* – tervezés, végrehajtás, ellenőrzés, beavatkozás.

¹³ FEMA 426: kézikönyv, amely az épületek terrorcselekményekkel szembeni védelmének alapelveit, a robbanás hatás csökkentésére szolgáló tervezési megoldásokat és a telephelyi védelmi beavatkozások módszereit foglalja össze.

¹⁴ EN 13541: európai szabvány biztonsági üvegek robbanásálló vizsgálatára és osztályozására.

¹⁵ C2: *command and control*; C4ISR: *command, control, communications, computers, intelligence, surveillance and reconnaissance*.

rendezve jelennek meg. A hatékonyság kulcsa ezért a detektálás, az értékelés és a reagálás folyamatainak összehangoltsága.

A rendszer működésének mérhetősége pedig a visszacsatolási ciklus alapját képezi. Az olyan teljesítménymutatók, mint az észlelési idő, a reagálási idő, a téves riasztások aránya vagy a kritikus alrendszerek rendelkezésre állása, lehetővé teszik a rendszer objektív értékelését és célzott fejlesztését. A folyamatos monitorozás és elemzés biztosítja, hogy a védelem képes legyen alkalmazkodni a változó fenyegetésekhez, és a rendszer rezilienciája a gyakorlatban is fenntartható legyen.

A fenyegetések és a többrétegű védelem gyakorlata

Az elmúlt évtizedben a katonai kritikus infrastruktúrák elleni fenyegetések olyan mértékben változtak meg szerkezetükben és dinamikájukban, hogy a korábban alkalmazott védelmi modellek több ponton már nem bizonyultak megfelelőnek, ezért részbeni újraértelmezésük vagy akár teljes felülvizsgálatuk vált szükségessé. A hagyományos fegyveres fenyegetések mellett az elmúlt években egyre nagyobb hangsúlyt kaptak az aszimmetrikus és hibrid módszerek, ideértve az IED- és VBIED-támadásokat, a RAM-típusú fenyegetéseket, valamint a pilóta nélküli rendszerek sokszínű alkalmazását. E fenyegetéstípusok közös sajátossága, hogy a támadó fél viszonylag alacsony erőforrás-ráfordítással is olyan hatást érhet el, amely jelentős műveleti következményekkel járhat a védett infrastruktúra működésére nézve. A támadási formák közös pontja a nehezen előre jelezhető támadási mintázat, a minimális előkészítési igény és az a jellegzetes *low-cost/high-impact dinamika, amely kis ráfordítással is aránytalan műveleti hatást tesz lehetővé*. A NATO AJP-3.14¹⁶ doktrína a fenyegetések változó mintázataira válaszul továbbra is a force protection rendszerébe illesztve határozza meg a fizikai védelem szerepét, és a védelmi intézkedéseket konkrét fenyegetéstípusokhoz rendelt funkciók szerint strukturálja. Ezzel összhangban a FEMA 426 és a DoD UFC 4-010-01¹⁷ szabványai is a fizikai védelmet konkrét, mérhető kockázati kategóriákhoz kapcsolják, nem pedig általános, nehezen operacionalizálható elvekhez. Ez a keretrendszer lehetővé teszi, hogy a tervezés és az üzemeltetés ne elvont biztonsági elvekre, hanem tényleges támadási profilokra és azok mérhető kockázati paramétereire épüljön.

A robbantásos támadások elemzésekor a támadás módja, a töltet nagysága és az elhelyezés környezeti sajátosságai különösen meghatározó tényezők, mivel ezek döntik el a robbanás terjedésének és károkozásának fő paramétereit. A VBIED-ok elsősorban a külső védelmi zónák nagy energiájú áttörését célozzák, míg az IED-k többnyire a belső mozgási útvonalak mentén okoznak kritikus károkat, megzavarva a személyi és logisztikai folyamatokat. A két támadástípus eltérő detektálási és késleltetési stratégiákat követel meg, mivel a fenyegetés időbelisége, észlelhetősége és a károkozás várható módja jelentősen különbözik. Ezt jól illusztrálják az afganisztáni

¹⁶ NATO AJP-3.14: doktrína, amely meghatározza a haderők védelmének alapelveit, a megelőzés–észlelés–késleltetés–elhárítás folyamatát, valamint a többrétegű fizikai védelem és a vezetésirányítás integrált követelményeit.

¹⁷ DoD UFC 4-010-01: amerikai katonai építészmérnöki szabvány.

műveletek során tapasztalt esetek, ahol a VBIED-támadások elsősorban a külső ellenőrzési pontok ellen irányultak, míg az IED-k a belső mozgási útvonalak mentén okoztak veszteségeket. A tapasztalatok szerint azok a létesítmények bizonyultak ellenállóbbnak, ahol a védelmi zónák közötti információáramlás gyors és strukturált volt, lehetővé téve a reagáló erők időbeni alkalmazását. Ennek megfelelően a védekezés két alapvető pillére a védőtávolság növelése – amely a csúcstúlnyomás és az impulzus csillapításán keresztül csökkenti a terhelést – valamint a szerkezeti ellenálló képesség növelése, amely a láncszerű összeomlással szembeni védelmet biztosítja. A robbanás hatás mérésének két kulcsparamétere, a csúcstúlnyomás (P_{peak} ¹⁸) és az impulzus (I)¹⁹, nemcsak a töltet méretétől, hanem a környezet geometriájától, a visszaverődési felületektől és a csatornázódási hatásoktól is jelentősen függ.

A nyílászárók és az üvegezett felületek különösen sérülékenyek robbanás esetén, mivel az üvegtörmelék által képzett repeszek a másodlagos sérülések leggyakoribb forrásai. A sérülési kockázatot nemcsak az üveg típusa, hanem a keret, a rögzítés és a csatlakozó felület együttes viselkedése határozza meg. Az EN 13541 szabvány a védelem értékelését nem az üveg önálló tulajdonságaira, hanem az üveg–keret–rögzítés–falcsatlakozás egészének viselkedésére alapozza. Ez a rendszerszintű szemlélet tükrözi, hogy a robbanásállóság tényleges mértékét mindig a teljes szerkezeti kombináció határozza meg. Ez a szemlélet egyre inkább megjelenik a nemzetközi gyakorlatban is, ahol a robbanásbiztosítás már nem tekinthető pusztán anyagminőségi kérdésnek.

A RAM-fenyegetések legnagyobb kihívása a kiszámíthatatlanság és a minimális előkészületi idő. A RAM-fenyegetések kezeléséhez a védelem passzív és aktív elemek kombinációjára van szükség. Ide tartozik a kritikus elemek térbeli szétválasztása, a védett útvonalak kijelölése és a menedékhelyek kialakítása, ugyanakkor mindez csak akkor működik hatékonyan, ha gyors riasztási és reagálási lánc kapcsolódik hozzá, amelyet megfelelően integrált C2/C4ISR-rendszer támogat.

Az utóbbi években a pilóta nélküli rendszerek elleni védelem önálló, gyorsan fejlődő szakterületté vált, ami egyértelműen tükrözi a fenyegetés stratégiai jelentőségét és a technológiai fejlődés ütemét. Az UAS²⁰-fenyegetések detektálása különösen összetett feladat, mivel a drónok kis radarkeresztmetszete, csökkentett akusztikus és infravörös emissziója, valamint a kommunikációs protokollok sokfélesége jelentősen korlátozza az egyes szenzortípusok önálló hatékonyságát. Ennek következtében az egyszenzoros detektálási rendszerek megbízhatósága korlátozott, és gyakran nem képesek a fenyegetések időbeni felismerésére. A gyakorlatban ezért multisenzoros adatfúziós megközelítéseket alkalmaznak – például RF-felderítést radarral, elektro-optikai és infravörös érzékeléssel kombinálva –, amelyek képesek a detektálási valószínűséget (P_d) növelni a téves riasztási arány szinten tartása mellett.

A többrétegű védelem gyakorlati hatékonysága elsősorban azon múlik, hogy a különböző védelmi zónák között milyen minőségű funkcionális és információáramlási kapcsolatok jönnek létre. A külső zónák elsősorban az elrettentést és a korai észlelést szolgálják, a közbenső zónák feladata a hozzáférés-korlátozás és a támadó

¹⁸ P_{peak} : a robbanáshullám által keltett maximális túlnyomás.

¹⁹ I : a robbanáshullám időben integrált nyomásterhelése.

²⁰ UAS: *unmanned aircraft system* – pilóta nélküli légi rendszer.

késleltetése, míg a belső zóna a kritikus elemek közvetlen védelmét és a gyors reagálás feltételeinek biztosítását látja el. A zónák hatékonysága valójában nem az egyes zónák önálló teljesítményétől, hanem az egymás közötti információ- és cselekvésáramlás minőségétől függ; ha ez sérül, a védelmi rendszer gyorsan fragmentálódik. A védelem működési teljesítményének objektív mérése elengedhetetlen a fejlesztési ciklus során, mivel csak így azonosíthatók a rendszer gyenge pontjai és a késleltetésből vagy információhiányból eredő hibák. A rendszer működési teljesítménye kvantitatív mutatókkal értékelhető, például az észlelési idővel, a reaklási idővel, a téves riasztási aránnyal és a rendelkezésre állással. Ezek együtt adják a védelmi architektúra működési profilját. Az adatok objektív visszajelzést adnak arról, hogy a rendszer mennyire képes megfelelni a műveleti követelményeknek. A folyamatos monitorozás és az értékelési mechanizmusok lehetővé teszik a rendszer gyenge pontjainak gyors azonosítását, és olyan beavatkozások meghatározását, amelyek javítják a teljes védelmi architektúra adaptivitását.

Műszaki és szabványosított védelmi megoldások

A fizikai védelem műszaki alapját azok a szabványok és követelményrendszerek adják, amelyek egyfelől meghatározzák a létesítmények robbanásállóságának és szerkezeti ellenálló képességének minimumát, másfelől pedig biztosítják a védelmi intézkedések mérhetőségét, ellenőrizhetőségét és dokumentálható igazolhatóságát. Katonai infrastruktúrák esetében ezek a követelmények nem egyszerű ajánlások, hanem kötelező érvényű tervezési alapelvek, amelyek be nem tartása közvetlenül csökkentené a létesítmények túlélőképességét.

A DoD egységes létesítményi szabályozása, az UFC 4-010-01, a minimális antiterro rizmus-követelményeket úgy rögzíti, hogy a tervezők számára egy jól értelmezhető és mérnöki le következetes referenciakeretet adjon a fizikai terhelések, robbanás-védelmi paraméterek és biztonsági funkciók meghatározásához. A követelmények nemcsak új létesítményekre, hanem meghatározott esetekben a meglévő épületekre is vonatkoznak, különösen akkor, ha felújítás, bővítés vagy funkcióváltás történik. A szabvány részletesen rögzíti a robbanás elleni védelem paramétereit, a szükséges védőtávolságokat, valamint azokat a szerkezeti és építészeti kialakítási szempontokat, amelyek a láncszerű összeomlás megelőzését szolgálják.

A robbanás elleni védelem egyik legfontosabb alapelve a védőtávolság, amely lehetővé teszi, hogy a robbanáshullám csúcstúlnyomása és impulzusa már a célobjektum előtt számottevően lecsökkenjen. A robbanáshullám túlnyomása a távolság köbével fordított arányban csökken ($\sim 1/R^3$), ezért a védőtávolság növelése a leghatékonyabb passzív védelmi eszközök közé tartozik: már néhány méteres növelés is jelentős tehersökkenést eredményez. Az UFC 4-010-02²¹ ezt az alapelvet konkrét, számítható tervezési követelményekre bontja le, amelyek egyértelmű iránymutatást adnak a minimális védőtávolság meghatározásához.

²¹ DoD UFC 4-010-02: amerikai katonai építésztechnikai szabvány.

A szerkezeti védelem célja nem pusztán a robbanás elsődleges terhelésének elviselése, hanem annak biztosítása is, hogy egyes teherhordó elemek károsodása ne indítson el láncszerű összeomlást. Ennek érdekében alternatív teherutakat, duktilitást biztosító csomópont-kialakítást és energiaelnyelő szerkezeti megoldásokat szükséges alkalmazni. Ez azt jelenti, hogy egyetlen teherhordó elem kiesése nem indít el olyan láncreakciót, amely az egész épület részleges vagy teljes összeomlásához vezetne. A szabványok ezért redundáns teherhordási megoldásokat és olyan szerkezeti kialakítási elveket követelnek meg, amelyek biztosítják a terhek átvitelét alternatív útvonalakon.

A nyílászárók és az üvegezett felületek különösen érzékenyek, mivel robbanás esetén az üvegtörmelékből származó repeszek adják a másodlagos sérülések legnagyobb részét. A nyílászárók teljesítményét azonban nem önmagában az üveg minősége határozza meg, hanem a keret, a rögzítési rendszer és a csatlakozó felületek együttes, rendszerszintű viselkedése. Az EN 13541 szabvány részletesen meghatározza az üvegezések vizsgálati módszereit és teljesítményosztályait, rendszerszintű megközelítést alkalmazva az üveg–keret–rögzítés–falcsatlakozás egészére. A teljesítményt az üveg–keret–rögzítés rendszere határozza meg (3. ábra).



3. ábra: Üvegezési rendszerek teljesítménye rendszerszinten (EN 13541 logika szerint)

Forrás: a szerző szerkesztése

Kovács Zoltán vizsgálatai szerint a robbanásállóság növelésének leghatékonyabb módszerei közé tartoznak a falszerkezetek hossz- és keresztirányú merevítései, a szénszálas megerősítések alkalmazása, valamint a gyantás, többretegű biztonsági üvegezés, amelyek a repeszhatás és a túlnyomás jelentős részét képesek elnyelni.²² Balogh Zsuzsanna rámutat, hogy a robbanáskor keletkező üvegszilánkok akár 40 m/s sebességgel is kirepülhetnek, ezért a biztonsági fólia önmagában nem elég; a hatásosság jelentősen növelhető, ha az üvegréteget a kerethez rugalmas szilikonragasztással rögzítik, amely a repeszek szétszóródását érdemben csökkenti.²³

A meglévő épületek védelmi fejlesztése gyakran komoly műszaki korlátokba ütközik, ezért a FEMA 426 külön hangsúlyt helyez azokra a fokozatos, kisebb beavatkozást igénylő megoldásokra, amelyekkel a védettség jelentősen növelhető. Ide tartozik például az üvegezések megerősítése, a belső terek átszervezése vagy a forgalom szabályozása.

A fizikai védelem ma már messze túlmutat a statikus szerkezeti elemek alkalmazásán: a modern rendszerek egyre inkább valós idejű érzékelési láncokra, multiszenzoros adatfúzióra és gyors reagálási képességet támogató informatikai infrastruktúrára épülnek. Különösen igaz ez a pilóta nélküli eszközök elleni védelemben, ahol többféle szenzor együttes alkalmazása szükséges.

²² KOVÁCS 2013: 77–78.

²³ BALOGH 2010: 267.

A korszerű C-UAS-rendszerek többféle érzékelési módot kombinálnak, köztük a rádiófrekvenciás skála figyelmet, a radarérzékelést és az optikai rendszereket, hogy növeljék a detektálási valószínűséget és csökkentsék a téves riasztások arányát. Ezek célja elsősorban a korai észlelés és a helyzetkép pontosítása.

A műszaki rendszerek hatékonysága nagyrészt azon múlik, hogy mennyire képesek együttműködni és milyen minőségben integrálódnak a döntéstámogató rendszerekbe. A gyakorlati tapasztalatok szerint sok esetben az integráció hiánya nagyobb működési problémát okoz, mint az egyes eszközökön belüli műszaki korlátok. A szenzorok és védelmi eszközök működése csak akkor tekinthető hatékonynak, ha szorosan kapcsolódik a döntéstámogató és irányítási rendszerekhez, biztosítva az információ gyors és torzításmentes továbbítását. A detektálás, az értékelés és a reagálás így egy koherens folyamatláncot alkot, ahol minden késedelem vagy információs veszteség közvetlenül rontja a védelmi képességet.

A szabványok is ezt a rendszerszemléletet követik: a fizikai védelmi elemeket nem önálló megoldásként, hanem egy összekapcsolt, integrált rendszer komponenseiként kezelik. A műszaki védelem ezért nem csupán szerkezeti, hanem információs és működtetési kérdés is, amelyben az adatáramlás minősége és a reagálási lánc hatékonysága legalább olyan fontos, mint az alkalmazott szerkezeti megoldások.

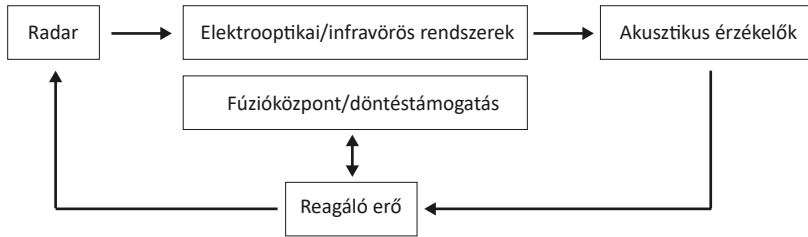
Integrált védelem és jövőbeli irányok

A robbantásos támadások elemzésekor kiemelt jelentősége van a támadás módjának, a töltet nagyságának és az elhelyezés környezeti geometriájának, mivel ezek döntik el a csúcstűlnyomás alakulását és a szerkezet várható válaszát. Emiatt e tényezők tervezési szinten való kezelése alapvető követelmény.

A nyílászárók és üvegezett felületek különösen érzékenyek a robbanás hatására, mivel a másodlagos repeszkarok döntő része ezekből a szerkezetekből ered. Az EN 13541 szabvány rendszerszintű megközelítést alkalmaz: az üvegezés ellenálló képességét nem az üveg tulajdonságai, hanem az üveg–keret–rögzítés–falcsatlakozás teljes szerkezeti együttese határozza meg. Ez a szemlélet mára széles körben elfogadott követelménnyé vált a nemzetközi mérnöki gyakorlatban. A RAM-fenyegetések sajátossága a kiszámíthatatlanság és a rendkívül rövid előkészületi idő, amely a védelem számára kifejezetten szűk reakcióablakot eredményez. E kihívás kezelése érdekében a védelem passzív és aktív elemek kombinációjára épít, amelyek együtt biztosítják a reakcióidő csökkentését és a támadási hatás mérséklését.

Az UAS-fenyegetések az elmúlt években olyan gyors technológiai és taktikai fejlődésen mentek keresztül, hogy mára önálló, specializált védelmi szakterületet alkotnak. Ez nemcsak a fenyegetés súlyát mutatja, hanem azt is, hogy a hagyományos védelmi architektúrák számos elemét újra kellett értékelni. A gyakorlatban több katonai repülőtér esetében is azonosították, hogy az egyszenzoros rendszerek nem biztosítanak megfelelő megbízhatóságot, különösen összetett környezeti háttér esetén. Az ilyen tapasztalatok vezettek a multisenzoros rendszerek szélesebb körű alkalmazásához. A drónok alacsony radarkeresztmetszete, változatos kommunikációs

csatornái és gyors konfigurálhatósága miatt a hatékony detektálás multiszenzoros megközelítést igényel, amelynek felépítését a 4. ábra szemlélteti.



4. ábra: A multiszenzoros C-UAS²⁴ detektálási architektúra

Forrás: a szerző szerkesztése

Napjainkban a radar-, az elektro-optikai és infravörös rendszerek, valamint az akusztikus érzékelők együttes alkalmazása biztosítja a megfelelő észlelési megbízhatóságot. A C-UAS-védelem ugyanakkor nem kizárólag technikai feladat. Legalább ilyen fontos az eljárási és döntési folyamatok megfelelő szabályozása: a felderítés, az azonosítás és a reagálás eljárási integritása, valamint a felelősségi körök pontos kijelölése legalább olyan meghatározó, mint a használt technológia minősége.

A többretegű védelem gyakorlati hatékonyságát elsősorban a védelmi zónák közötti funkcionális kapcsolatok és az információáramlás minősége határozza meg. A késleltetésből nyerhető időablak csak akkor érvényesíthető, ha az érzékelési információk gyorsan, torzításmentesen és a döntéshozatal szempontjából értelmezhető formában jutnak el a megfelelő szereplőkhöz. A védelmi rendszer teljesítményének mérése a fejlesztési ciklus elengedhetetlen eleme. Az olyan mérőszámok, mint az észlelési idő, a reagálási idő, a téves riasztások aránya vagy az alrendszerek rendelkezésre állása objektív visszajelzést adnak a rendszer működési hatékonyságáról és gyenge pontjairól. A folyamatos monitorozás és visszacsatolás nemcsak az aktuális működés optimalizálását segíti elő, hanem a hosszú távú adaptivitás feltételeit is megteremti.

A jövőbeli fejlesztések kulcsterülete az automatizált döntéstámogatás, a mesterségesintelligencia-alapú fenyegetésazonosítás, valamint a fizikai és kiberbiztonsági rendszerek konvergenciája, amelyek új típusú integrációs kihívásokat és egyben lehetőségeket is teremtenek. Összességében a fizikai védelem jövője nem egyetlen technológiai újítástól függ, hanem a különböző műszaki, informatikai és szervezeti megoldások olyan integrációjától, amely képes egységes, alkalmazkodó és közösen fejlődő rendszert alkotni. A tapasztalatok a multiszenzoros rendszerek elsődlegességét igazolják az UAS-fenyegetések kezelésében.

²⁴ C-UAS: *counter-unmanned aircraft system* – pilóta nélküli légi rendszerek elleni védelem (drónellenes rendszerek).

Szervezeti és humán tényezők

A fizikai védelem hatékonysága nem kizárólag a telepített műszaki rendszerek teljesítményétől függ, hanem attól is, hogy a működtető szervezet és a személyi állomány mennyire képes ezeket működtetni. A technikai rendszerek valós teljesítménye végső soron az állomány kompetenciáját tükrözi: még a legkorszerűbb szenzor- és döntéstámogató rendszerek sem működnek hatékonyan, ha a kezelők nem értik azok működési logikáját és a potenciális hibamódokat. A NATO AJP-3.14 (2024) szerint a *force protection* hatékonyságának egyik kulctényezője a jól képzett állomány és a világosan meghatározott parancsnoki felelősségi struktúra, amely garantálja, hogy a döntések időben, torzításmentesen és megfelelő prioritási sorrendben szülessenek meg. A védelem akkor tekinthető működőképesnek, ha a szervezet képes a fenyegetések gyors felismerésére, a helyzetek értelmezésére és a szükséges reakciók következetes végrehajtására. Tapasztalatok szerint az incidensek jelentős részében nem a technikai rendszer hibája, hanem az eljárások nem megfelelő alkalmazása vezetett a védelmi hiányosságokhoz. Ez különösen igaz olyan helyzetekben, ahol a kezelőszemélyzet nem rendelkezett kellő gyakorlattal a komplex riasztási helyzetek kezelésében.

Az amerikai ADP 3-37²⁵ doktrína szintén hangsúlyozza, hogy a védelem operatív hatékonysága alapvetően az eljárások ismeretén és következetes alkalmazásán múlik. A tapasztalatok szerint az eljárási fegyelem hiánya sok esetben nagyobb kockázatot jelent, mint a műszaki rendszer hiányosságai, mivel közvetlenül érinti a reakálás időbeliségét és pontosságát. A szabályok pusztá végrehajtása azonban nem elegendő: az állománynak értenie kell az eljárások mögötti célokat, összefüggéseket és várható következményeket, különösen gyorsan változó fenyegetési helyzetben.

A felkészítés három, egymást kiegészítő területet foglal magában: a fenyegetések felismerését és értelmezését; a technikai rendszerek biztonságos, hibatudatos használatát; valamint a jelentési és parancsnoki lánc torzításmentes működtetését. E készségek bármelyikének hiánya – még fejlett technikai infrastruktúra mellett is – gyorsan a védelem gyengüléséhez, súlyosabb esetben pedig működésképtelenséghez vezethet.

A hatékony működés alapját az egyértelműen dokumentált és rendszeresen validált eljárások adják, amelyek biztosítják, hogy a döntések ne improvizáción, hanem előre meghatározott és gyakorlatban is tesztelt folyamatokon alapuljanak. A Standard Operating Procedure dokumentumok intézményesítik azokat a működési folyamatokat, amelyek különböző helyzetekben meghatározzák a szükséges lépéseket és felelősségi köröket, ezzel minimalizálva az improvizációból eredő hibák lehetőségét. A szakirodalom hangsúlyozza, hogy a stabil és konzisztensen alkalmazott eljárásrend közvetlenül hozzájárul a működési ellenálló képesség növeléséhez, mivel csökkenti a bizonytalanságból eredő hibák előfordulását.

A szervezeti felépítés határozza meg, hogy a védelmi funkciók miként oszlanak meg az őrszolgálat, a beléptetés, a műszaki üzemeltetés, a reagáló erők és az irányítás között, és hogy a funkciók összhangja mennyire támogatja a működési rezilienciát.

²⁵ ADP 3-37: doktrína, amely meghatározza a védelem (*protection*) alapelveit, a fizikai védelem, erővédelem és veszteségminimalizálás eljárásrendjeit, valamint a műveletek folytonosságát biztosító szervezeti és technikai követelményeket.

A fizikai védelemben részt vevő alrendszerek – az őrszolgálatról és beléptetéstől kezdve a műszaki üzemeltetésen át a reagáló erőig és az irányítási struktúráig – csak akkor képesek hatékonyan működni, ha a feladat- és felelősségi körök egyértelműek, a kommunikációs utak pedig redundánsak és torzításmentesek. A riasztások, jelentések és parancsok áramlása gyakran a védelem legérzékenyebb pontját jelenti: a késedelem vagy információtorzulás gyorsan rontja a teljes rendszer teljesítményét.

A humán tényező nemcsak a végrehajtásban, hanem a helyzetértékelésben és a döntéshozatalban is fontos, különösen akkor, amikor a beérkező adatok hiányosak vagy ellentmondásosak. Bár a modern rendszerek egyre nagyobb szerepet szánnak az automatizált döntéstámogató megoldásoknak, az emberi ítélőképesség továbbra is nélkülözhetetlen, különösen összetett vagy bizonytalan helyzetekben. A kutatások egybehangzóan jelzik, hogy az automatizált rendszerek hatékonyan képesek támogatni, de nem tudják helyettesíteni az emberi megfontolást, különösen nem magas kockázatú döntési helyzetekben.

A folyamatos képzés és a rendszeres gyakorlatoztatás ezért nem adminisztratív teher, hanem a működési ellenálló képesség alapfeltétele. A gyakorlatok lehetőséget adnak a technikai rendszerek tesztelésére, a szervezet együttműködésének vizsgálatára és a reagálóképesség valós körülmények közötti értékelésére. A jól megtervezett és végrehajtott gyakorlatok rendszerint rávilágítanak a szervezet rejtett gyenge pontjaira, és értékes visszajelzést adnak a folyamatok finomhangolásához.

Mindezek alapján a fizikai védelem akkor tekinthető valóban működőképesnek, ha a műszaki rendszerek és a humán tényezők nem egymástól elkülönülten, hanem szerves módon, egymást erősítve vesznek részt a kritikus infrastruktúrák védelmében. A technológiai fejlődés csak akkor válik valós értékévé, ha a mögötte álló szervezet és állomány képes azt integrálni, értelmezni és a gyakorlatban is hatékonyan működtetni.

Összegzés

A katonai kritikus infrastruktúrák fizikai védelme olyan összetett, többszintű rendszerként értelmezhető, amelynek hatékonysága nem egyetlen komponens teljesítményétől, hanem a rendszer egészének összehangolt működésétől függ. A vizsgálatok és a gyakorlati tapasztalatok is azt mutatják, hogy a védelmi rendszer csak akkor működik megbízhatóan, ha a műszaki megoldások, az eljárási folyamatok és a humán tényezők egymást kiegészítve, összehangoltan járulnak hozzá a működéshez. A védelem hatékonysága emergens tulajdonság,²⁶ amelyet elsődlegesen az elemek közötti kapcsolatok minősége – például az illesztések, a reakcióidők vagy a döntéstámogatási folyamatok – határoz meg.

A fenyegetési környezet nemlineáris, nehezen előre jelezhető dinamikája – különösen a robbanóeszköz-alapú támadások, a hibrid módszerek és a pilóta nélküli rendszerek terjedése – elkerülhetetlenné teszi a többrétegű védelem következetes

²⁶ Emergens tulajdonság: olyan rendszerjellemző, amely az elemek kölcsönhatásából, nem pedig az elemek önálló tulajdonságaiból ered.

alkalmazását. A többrétegű védelmi logika mára a nemzetközi szabványok és doktrínák egyik alapvető, univerzálisan alkalmazott elvévé vált.

A szabályozási és doktrinális környezet világos keretet ad a fizikai védelem kialakításához, ugyanakkor a gyakorlati hatékonyság végső soron azon múlik, hogy ezek az elvek hogyan jelennek meg a konkrét rendszerekben, a szervezeti folyamatokban és a működési döntésekben. A védelmi architektúra valódi értékét az mutatja meg, hogy a szabványokban rögzített követelmények mennyire épülnek be a napi működésbe, és mennyire képesek iránymutatást adni egy gyorsan változó fenyegetési környezetben.

A technológiai fejlődés számos új lehetőséget nyit a védelem számára – legyen szó korszerű érzékelőkről, adatfúziós algoritmusokról vagy automatizált elemzőrendszerekről –, a gyakorlat azonban egyértelműen megmutatja, hogy ezek az eszközök önmagukban nem helyettesítik a fizikai védelem alapvető struktúráit. A stabil műszaki kialakítás, a szabályozott és jól dokumentált működési környezet, valamint a felkészült személyi állomány továbbra is a védelmi rendszer hatékonyságának legfontosabb meghatározói.

A fizikai védelem jövője ezért nem egyetlen technológiai megoldáson múlik, hanem azon, hogy a műszaki rendszerek, az informatikai háttér, a vezetésirányítás és a humán tényezők mennyire képesek egységes, alkalmazkodó és folyamatosan fejlődő rendszert alkotni. A hatékony védelem lényegében egy folyamatosan karbantartott és időről időre újragondolt struktúra, amelyben a mérés, az értékelés és az alkalmazkodóképesség együttesen biztosítja az ellenálló képesség fenntartását.

A fizikai védelem napjainkban nem tekinthető statikus vagy lezárt megoldásnak. Sokkal inkább dinamikus, életciklus-alapú biztonsági rendszerként értelmezhető, amely folyamatosan alkalmazkodik a környezeti változásokhoz. Fejlesztése nem csupán a szabványok követésén múlik, hanem azon is, hogy a szervezetek mennyire képesek a tapasztalatokat beépíteni és intézményesített tanulási folyamatokká alakítani.

A tanulmány egyik fő megállapítása, hogy a fizikai védelem hatékonyságát nem elsősorban az egyes technológiák fejlettsége, hanem az integráció minősége és a reagálási lánc időkritikus működése határozza meg.

Felhasznált irodalom

BALOGH Zsuzsanna (2010): Üveg az építészetben, a terrorista robbantások tükrében. *Műszaki Katonai Közlöny*, 20(1–4), 257–271.

EN 13541. *Security Glazing – Testing and Classification of Resistance Against Explosion Pressure* (2012).

FÖLDES Tibor (2025): A biztonság szerepe és fontossága a szövetségi kritikus infrastruktúra szabályozásának kialakításában. *Katonai Nemzetbiztonsági Szolgálat Szakmai Szemle*, 1, 146–163. Online: <https://ojs.knbsz.gov.hu/index.php/szakmai/article/view/234/130>

Joint Forward Operating Base Force Protection Handbook (2005).

- Kovács Zoltán (2012): Repülőterek védelme improvizált robbanóeszközök (IED) ellen. *Repüléstudományi Közlemények*, 24(2), 70–79. Online: www.repulestudomany.hu/kulonszamok/2012_cikkek/05_Kovacs_Zoltan.pdf
- Kovács Zoltán (2013): Repülőterek robbantások elleni védelmének technikai lehetőségei. *Repüléstudományi Közlemények*, 25(2), 78–88. Online: www.repulestudomany.hu/kulonszamok/2013_cikkek/2013-2-06-Kovacs_Zoltan.pdf
- Kovács Zoltán (2014): Repülőtéri létesítmények fizikai védelme IED ellen. *Repüléstudományi Közlemények*, 26(2), 106–113. Online: <https://folyoirat.ludovika.hu/index.php/reptudkoz/article/view/4602/3759>
- NATO Standardization Office (2024): *AJP-3.14. Allied Joint Doctrine for Force Protection. Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings (FEMA 426)* (2011).
- U.S. Army (2009): *FM 3-37 Protection*.
- U.S. Army (2018): *ADP 3-37 Protection*.
- UFC 4-010-01. *DoD Minimum Antiterrorism Standards for Buildings* (2024). Whole Building Design Guide. Online: www.wbdg.org/dod/ufc/ufc-4-010-01
- UFC 4-010-02. *DoD Minimum Antiterrorism Standoff Distances for Buildings* (2020). Online: www.wbdg.org/dod/ufc/ufc-4-010-02

Jogi forrás

2024. évi LXXXIV. törvény a kritikus infrastruktúrák ellenálló képességéről