

Imhof László alezredes:

A MAGYAR HONVÉDSÉG RENDSZERINTEGRÁCIÓS ARCHITEKTÚRÁJA ÉS A KATONAI DIGITALIZÁCIÓS FOLYAMAT KIHÍVÁSAI

DOI: 10.35926/HSZ.2026.4.4

ÖSSZEFOGLALÓ: A tanulmány a Magyar Honvédség rendszerintegrációs architektúráját és a katonai digitalizációval összefüggő kihívásokat vizsgálja, különös tekintettel a vezetés-irányítási (C2¹), valamint a C4ISR²- és infokommunikációs képességek integrált fejlesztésére. Az elemzés a horizontális, vertikális és diagonális rendszerintegráció fogalmi és gyakorlati értelmezésére épül, bemutatva a jelenlegi képességek, infrastruktúrák és szervezeti megoldások korlátait. Az írás az orosz–ukrán háború híradó-informatikai és hálózatalapú hadviseléssel kapcsolatos tapasztalatait, valamint NATO-tagállamok nyílt forrásból elérhető gyakorlatait is felhasználva fogalmaz meg következtetéseket. A szerző célja olyan integratori szemléletű megközelítés bemutatása, amely stratégiai és hadműveleti szinten egyaránt hozzájárulhat a Magyar Honvédség jövőbeni rendszerintegrációs és digitalizációs irányainak megalapozásához.³

KULCSSZAVAK: rendszerintegráció, katonai digitalizáció, hálózatalapú hadviselés, C2, C4ISR, FMN, Magyar Honvédség

A SZERZŐRŐL:

Imhof László alezredes tanársegéd (NKE HHK Katonai Infokommunikációs Intézet, Infokommunikációs és Információbiztonsági Tanszék) (ORCID: 0009-0001-7596-0554; MTMT: 10101600)

BEVEZETÉS

A 21. század fegyveres konfliktusai egyértelműen igazolták, hogy a katonai képességek értéke napjainkra túllépett az egyes fegyverrendszerek önálló technikai paraméterein. A hadműveleti hatékonyságot egyre inkább az határozza meg, hogy az alkalmazott eszközök, érzékelők, vezetés-irányítási elemek és infokommunikációs rendszerek milyen mértékben képesek integrált, hálózatra szervezett rendszerként működni. A vezetés-irányítás (C2) és a C4ISR-képességek így nem csupán támogató funkciót töltenek be, hanem önálló, hadműveleti értelemben kritikus képességgé váltak.

¹ A Command and Control (C2) rendszer olyan integrált informatikai és technikai struktúra, amely adatgyűjtés, elemzés és kommunikáció révén támogatja a döntéshozatalt és a műveletek irányítását.

² A Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) egy integrált katonai informatikai és kommunikációs rendszer (vezetés, irányítás, kommunikáció, számítógépek, hírszerzés, megfigyelés, felderítés), amely valós idejű adatokkal segíti a döntéshozatalt és a helyzet tudatosságot.

³ Imhof 2024, 38–63.

Az orosz–ukrán háború tapasztalatai különösen élesen világítottak rá arra, hogy az információs fölény megszerzése és fenntartása önálló hadművelleti tényezőként jelenik meg. A konfliktus során egyértelműen kimutatható volt, hogy a vezetési pontok közötti összeköttetések sérülékenysége, a szenzor–döntéshozatal–végrehajtás lánc megszakadása, illetve az integrált információs környezet hiánya közvetlenül befolyásolta a műveletek sikerét vagy kudarcát. A tapasztalatok azt mutatják, hogy a korszerű hadviselésben a technológiai eszközök önmagukban nem garantálják a fölényt, amennyiben azok nem egy egységes rendszerintegrációs architektúrába illeszkednek. A gyorsan adaptálható, redundáns és integrált híradó-informatikai rendszerek hiánya közvetlenül vezethet a vezetési pontok elszigetelődéséhez, a döntéshozatali ciklus lassulásához, végső soron pedig a harci képességek csökkenéséhez.

A Magyar Honvédség jelenlegi helyzetét tovább árnyalja, hogy a stacioner és a tábori infokommunikációs rendszerek fejlesztése nem arányosan történik, hanem stacioner fejneház, továbbá azt is látni kell, az örökölt infrastruktúra korlátai fokozott integrációs kockázatokat hordoznak.

A különböző időszakokban, eltérő technológiai szinten és részben eltérő követelményrendszer szerint kialakított rendszerelemek összekapcsolása csak egy következetes integrátori szemlélettel biztosítható, ennek hiányában fennáll a veszélye annak, hogy a fejlesztések eredményeként egy félkomplex és működésében széttagolt rendszer jön létre, amely nem képes teljes mértékben támogatni sem a nemzeti, sem a szövetségi műveleteket.

E kihívások a Magyar Honvédség számára is meghatározó jelentőséggel bírnak. A Honvédelmi és Haderőfejlesztési Program (HHP) keretében megvalósuló, példa nélküli és volumenű képességfejlesztés új fegyverrendszerek, harcjárművek, szenzorok és infokommunikációs megoldások rendszerbe állítását eredményezi. Ugyanakkor a fejlesztések hadművelleti értéke csak akkor realizálható, ha az új képességek következetes, architektúraalapú rendszerintegráció mentén illeszkednek a Magyar Honvédség vezetés-irányítási és C4ISR-környezetébe. Ennek hiányában fennáll annak a veszélye, hogy a fejlesztések eredményeként technológiailag korszerű, ám működésében széttagolt, hadműveletileg korlátozott rendszer jön létre.⁴

A hazai és a nemzetközi szakirodalom széles körben foglalkozik a hálózatalapú hadviselés, a C4ISR-rendszerek és a katonai digitalizáció kérdéseivel. Ugyanakkor megállapítható, hogy viszonylag kevés olyan elemzés áll rendelkezésre, amely a rendszerintegrációt önálló hadművelleti képességként értelmezi, továbbá az integráció különböző dimenzióit (horizontális, vertikális, diagonális) egységes architekturális keretben vizsgálja. Olyan tanulmány sem lelhető fel, amely ebben az integrációs filozófiában kifejezetten a Magyar Honvédség szervezeti, technológiai és szövetségi sajátosságaira adaptálva tenné meg az elemzését.

A magyar nyelvű szakirodalomban különösen hiányzik az a megközelítés, amely a rendszerintegrációt nem kizárólag technikai vagy informatikai kérdésként, hanem vezetés-irányítási és hadművelleti hatékonyságot meghatározó tényezőként elemzi. A jelen tanulmány ezt a tudományos rést kívánja csökkenteni azáltal, hogy a Magyar Honvédség rendszerintegrációs architektúráját stratégiai és hadművelleti szintű összefüggésben vizsgálja.

A tanulmány központi kutatási kérdései a következőkben foglalhatók össze:

⁴ Zrínyi 2026 Honvédelmi és Haderőfejlesztési Program – nyilvános koncepcióelemek.

- Mitől válik a rendszerintegráció hadműveleti értelemben kritikus képességgé a Magyar Honvédség számára?
- Mely rendszerintegrációs dimenziók hiánya okoz mérhető vezetés-irányítási (C2) hatékonyságsökkenést nemzeti és szövetségi műveleti környezetben?

A kutatás alaphipotézise szerint a rendszerintegráció hiánya vagy részleges megvalósulása önmagában képes lerontani a C2 hatékonyságát, függetlenül attól, hogy az egyes fegyverrendszerek és infokommunikációs eszközök technológiai színvonala korszerűnek tekinthető-e. Másképpen megfogalmazva: az integráció hiánya hadműveleti értelemben képességvesztést eredményez.

A tanulmány kvalitatív módszertani megközelítést alkalmaz, amelynek fő elemei a NATO- és a nemzeti doktrínák elemzése, a nyílt forrású nemzetközi tapasztalatok és esettanulmányok feldolgozása, valamint a Magyar Honvédség meglévő és tervezett infokommunikációs és vezetés-irányítási képességeinek rendszerszintű értelmezése.

Az elemzés kizárólag nyílt forrásokra és publikálható adatokra épül, nem érint minősített információkat. Ennek megfelelően a következtetések koncepcionális és architekturális szinten értelmezendők, és céljuk a gondolkodási keretek és fejlesztési irányok megalapozása.

A tanulmány célja, hogy a Magyar Honvédség rendszerintegrációs architektúráját stratégiai és hadműveleti szintű megközelítésben mutassa be, különös tekintettel a horizontális, a vertikális és a diagonális integráció szerepére. A cikk egyrészt a meglévő és a tervezett képességek rendszerbe illesztésének kihívásait elemzi, másrészt – az orosz–ukrán háború, valamint más NATO-tagállamok elérhető tapasztalatai alapján – olyan következtetéseket fogalmaz meg, amelyek hozzájárulhatnak a Magyar Honvédség jövőbeni digitalizációs és rendszerintegrációs irányainak megalapozásához.

ELMÉLETI ÉS FOGALMI KERETEK – A KATONAI RENDSZERINTEGRÁCIÓ ÉRTELMEZÉSE

A katonai rendszerintegráció fogalma a hadtudományi és katonai műszaki szakirodalomban gyakran szűkebb, technikai értelemben jelenik meg, elsősorban informatikai vagy híradórendszerek összekapcsolásaként értelmezve. A korszerű hadviselés tapasztalatai azonban egyértelművé tették, hogy ez a megközelítés nem képes megragadni a rendszerintegráció valódi hadműveleti jelentőségét. Katonai értelemben a rendszerintegráció olyan összetett, többdimenziós tevékenység, amely a különböző fegyverrendszerek, szenzorok, vezetés-irányítási elemek, infokommunikációs infrastruktúrák és szoftverrendszerek egységes, hadműveletileg koherens rendszerbe szervezését célozza.

E megközelítés középpontjában nem az egyes technikai komponensek önálló működése, hanem a döntéshozatali folyamat támogatása áll. A rendszerintegráció hadműveleti értelme abban ragadható meg, hogy képes lerövidíteni az információ keletkezése és a döntés végrehajtása közötti időt, miközben növeli az információ pontosságát, megbízhatóságát és relevanciáját, és ezáltal közvetlen hatást gyakorol a vezetés-irányítás hatékonyságára és a műveletek sikerére.

A rendszerintegráció és az információs fölény összefüggései

A modern hadviselésben az információs fölény elérése és fenntartása a hadműveleti siker egyik alapvető feltétele. Az információs fölény nem pusztán az információ mennyiségét jelenti, hanem azt a képességet, hogy a rendelkezésre álló információk gyorsabban, pontosabban

és relevánsabb formában álljanak a döntéshozók rendelkezésére, mint az ellenfél esetében. A rendszerintegráció ebben az összefüggésben nem önálló technikai cél, hanem az információs fölény megteremtésének egyik legfontosabb eszköze.

A NATO-doktrínák és a hálózatalapú hadviselés (Network Enabled Warfare – NEW) koncepciója egyaránt hangsúlyozzák, hogy a hálózatba kapcsolt erők összehatása nagyobb, mint az egyes elemek önálló alkalmazásának eredője. E megközelítésben a híradó-informatikai rendszer nem támogató háttérfunkcióként jelenik meg, hanem a harci képességek egyik meghatározó összetevőjévé válik. A felderítés, a vezetés-irányítás, a tűzvezetés és a logisztikai támogatás közös információs környezetben történő működése a korszerű hadműveletek végrehajtásának alapfeltétele.

A rendszerintegráció közvetlen kapcsolatban áll az OODA-ciklus (Observe–Orient–Decide–Act, OODA loop) hatékonyságával. Az OODA loop egy döntéshozatali modell, amely négy lépésből áll: megfigyelés, tájékozódás, döntés és cselekvés. Az integrált rendszerek képesek csökkenteni az „Observe” és „Orient” fázisok időigényét, miközben növelik az információ minőségét a „Decide” és az „Act” szakaszokban. Ennek hiányában a döntéshozatal lassul, fragmentálttá válik, és növekszik a hibás döntések kockázata.⁵

A katonai rendszerintegráció szintjei és összetevői

A katonai rendszerintegráció több, egymással szorosan összefüggő szinten értelmezhető. A szakirodalom és a doktrinális megközelítések alapján megkülönböztethető:

- technikai integráció, amely az eszközök és a rendszerek fizikai és logikai összekapcsolását jelenti;
- funkcionális integráció, amely az egyes képességek – például felderítés, vezetés-irányítás, tűzvezetés – együttműködését biztosítja;
- szervezeti és eljárásrendi integráció, amely a különböző parancsnoki szintek, szervezetek és nemzeti hozzájárulások összehangolt működését teszi lehetővé.

Katonai környezetben az előbbieken említett szintek bármelyikének hiánya a teljes rendszer hatékonyságának csökkenéséhez vezet, így egy technikailag jól integrált rendszer sem képes hadművelleti előnyt biztosítani, ha a szervezeti és az eljárásrendi összhang hiányzik, ugyanakkor a szervezeti integráció sem érvényesülhet megfelelő technikai háttér nélkül.

A Magyar Honvédség esetében ezek a szintek különös jelentőséggel bírnak, mivel a stacioner és a tábori infokommunikációs rendszerek eltérő technológiai alapokon, eltérő biztonsági és minősítési követelmények szerint működnek. A nemzeti vezetési infrastruktúra és a NATO FMN elvei mentén kialakított tábori hálózatok közötti átjárhatóság megteremtése nem csupán technikai, hanem szabályozási és szervezeti kihívás is.

Horizontális, vertikális és diagonális integráció mint elemzési keret

A tanulmány a katonai rendszerintegrációt három, egymást kiegészítő dimenzió mentén értelmezi – horizontális, vertikális és diagonális integrációként –, elénk vetítve a harcmező dimenzióit, illetve a mélytechnikai integrációs feladatcsomagot. Ez a felosztás

⁵ Alberts et al. 2002, 152–154.

lehetővé teszi a Magyar Honvédség komplex infokommunikációs és vezetés-irányítási rendszerének strukturált elemzését, miközben megőrzi a hadművelleti összefüggések átláthatóságát.

A horizontális integráció az információ áramlását vizsgálja a harcmezőn alkalmazott szenzoroktól és végrehajtó elemektől egészen a stratégiai szintű vezetési pontokig. Ennek középpontjában az információ életútja áll, beleértve annak keletkezését, elsődleges feldolgozását, aggregálását és megjelenítését a különböző vezetési szinteken.

A vertikális integráció az alkalmazott híradási és adatátviteli technológiák egymáshoz illesztésére fókuszál. Ide tartozik a műholdas, a mikrohullámú, a rádiós és a vezetékes megoldások rétegzett, redundáns alkalmazása, amely biztosítja a rendszer túlélőképességét és hadművelleti megbízhatóságát.

A diagonális integráció a horizontális és vertikális dimenziók metszéspontjában jelenik meg, és a konkrét rendszerintegrátori feladatokat, interfészeket és együttműködési pontokat azonosítja. Ez a dimenzió teremti meg a kapcsolatot az elméleti architektúra és a gyakorlati megvalósítás között.

E három dimenzió együttes alkalmazása biztosítja azt az elemzési keretet, amely alkalmas a Magyar Honvédség rendszerintegrációs architektúrájának átfogó vizsgálatára, és megalapozza a következő fejezetek gyakorlati elemzéseit.⁶

A MAGYAR HONVÉDSÉG RENDSZERINTEGRÁCIÓS HELYZETE ÉS FŐBB KIHÍVÁSAI

A Magyar Honvédség rendszerintegrációs helyzetét alapvetően az elmúlt évtizedek eltérő fejlesztési ciklusai, az örökölt infrastruktúra sajátosságai, valamint a jelenleg zajló, nagy léptékű haderőfejlesztési programok együttes hatása határozza meg. E tényezők következtében a vezetés-irányítási és infokommunikációs képességek fejlődése nem lineáris, hanem több, egymással párhuzamos technológiai és szervezeti pályán zajlik, ami önmagában is fokozott rendszerintegrációs kockázatot hordoz.

A rendszerintegrációs kihívások nem elsősorban az egyes technikai megoldások korszerűtlenségéből fakadnak, hanem abból, hogy a különböző időszakokban eltérő követelményrendszerek szerint kialakított rendszerelemek egységes architektúrába történő illesztése nem minden esetben történt meg következetesen. Ez a helyzet különösen élesen jelenik meg a stacioner és a tábori infokommunikációs és vezetés-irányítási rendszerek viszonylatában.

A stacioner és a tábori rendszerek kettőssége

A Magyar Honvédség vezetés-irányítási rendszerének egyik alapvető sajátossága a stacioner és a tábori (telepíthető) rendszerek párhuzamos fennállása. A stacioner környezetben működő infokommunikációs rendszerek elsődlegesen a nemzeti szintű vezetési, irányítási és igazgatási feladatokat támogatják. Ezek a rendszerek magas rendelkezésre állásra, hosszú távú üzembiztonságra, valamint szigorú információbiztonsági és minősítési követelmények teljesítésére optimalizáltak. Ezzel szemben a tábori (telepíthető) rendszerek alapvető követelménye a gyors telepíthetőség, a mobilitás, a rugalmasság és a szövetségi interoperabilitás.

⁶ Federated Mission Networking (FMN)... 2021.

A tábori vezetési pontoknak rövid idő alatt kell képesnek lenniük csatlakozni nemzeti vagy szövetségi hálózatokhoz, miközben ellenállónak kell maradniuk a fizikai, elektronikai és kibertérből érkező fenyegetésekkel szemben.

Önmagában e kettősség nem tekinthető problémának, de a rendszerintegráció szempontjából komoly kihívásokat jelent, hogy a stacioner és a tábori (telepíthető) rendszerek eltérő technológiai alapokon, részben eltérő szabványok mentén és eltérő biztonsági megközelítéssel kerültek kialakításra. Ennek következménye, hogy az egységes információs környezet megteremtése – különösen válsághelyzetben vagy műveleti átmenet során – csak jelentős technikai és szervezeti ráfordítással biztosítható.⁷

A Honvédelmi és Haderőfejlesztési Program integrációs kockázatai

A HHP keretében rendszerbe álló új fegyverrendszerek, harcjárművek és szenzorok minőségi ugrást jelentenek a Magyar Honvédség harcértékében. Ugyanakkor e rendszerek túlnyomó többsége saját, gyártóspecifikus infokommunikációs és vezetés-irányítási alrendszerekkel érkezik, amelyek nem automatikusan illeszkednek a meglévő nemzeti C2- és C4ISR-környezetbe.

Az ebből a helyzetből fakadó részprojektek mentén történő fejlesztések egyik legnagyobb veszélye, hogy az egyes rendszerek önmagukban korszerűek, viszont rendszerszinten nem képesek együttműködni. Ezért a rendszerintegráció egyik legjelentősebb kockázata a részprojektek mentén történő fejlesztés, amennyiben az egyes képességelemek – például harcjárműfedélzeti rendszerek, harcászati rádiócsaládok, szoftveralapú vezetés-irányítási megoldások vagy tábori hálózati elemek – önállóan, egységes architektúra nélkül kerülnek kialakításra, úgy a teljes rendszer működése széttagolttá válhat. Ez a jelenség nemcsak technikai kompatibilitási problémákat eredményezhet, hanem jelentős terhelést ró a személyi állományra is a kiképzés, az üzemeltetés és a fenntartás területén. A rendszerintegráció hiánya ily módon nem csupán hadműveleti, hanem humán és gazdasági kockázatot is jelent.

Örökölt infrastruktúra és technológiai adósság

A Magyar Honvédség rendszerintegrációs helyzetét tovább árnyalja az örökölt infrastruktúra állapota, a stacioner rendszerek egyes elemei technológiailag elavultak, fenntartásuk erőforrás-igényes, pótalkatrész-ellátásuk korlátozott. A tábori infokommunikációs rendszerek modernizációja és fejlesztése az előző haderőfejlesztési ciklusban (2006–2016) – a PK-kódú rádiós vezetési pontok kivételével – csak prototípusszintig jutott el, a HHP keretében is még csak a prototípusok legyártásánál és csapatpróba előtti fázisban járunk.

Ebben a környezetben különösen fontos, hogy az új fejlesztések ne párhuzamos, egymással nehezen összeegyeztethető megoldásokat hozzanak létre, hanem fokozatosan, tervezetten váltsák fel vagy egészítsék ki a meglévő rendszereket.

A technológiai adósság így nemcsak műszaki problémát, hanem hosszú távon hadműveleti kockázatot is jelent.

⁷ Rendszerintegráció feladatrendszere (belső koncepcióanyag).

Szövetségi interoperabilitás és nemzeti korlátok

A Magyar Honvédség NATO-tagságából fakadó kötelezettségei tovább növelik a rendszerintegráció komplexitását. A NATO FMN elvei szerint egy nemzeti rendszernek képesnek kell lennie gyorsan és biztonságosan csatlakozni a szövetségi hálózatokhoz, valamint támogatni a többnemzeti törzsek működését. Ezek a követelmények különösen érzékenyen jelennek meg olyan szervezetek esetében, mint a Közép-európai Többnemzeti Hadosztályparancsnokság (HQ MND-C⁸), ahol a nemzeti és a szövetségi elvárások egyidejű teljesítése szükséges. A rendszerintegráció hiányosságai ilyen környezetben nemcsak nemzeti, hanem szövetségi szinten is hatékonyságcsökkenést okozhatnak.⁹

Hadműveleti következmények és tanulságok

Az orosz–ukrán háború tapasztalatai alátámasztják, hogy a vezetés-irányítási rendszerek integráltságának hiánya közvetlen hadműveleti kockázatot jelent. Tény, a Magyar Honvédség rendszerintegrációs kihívásai egyszerre technológiai, szervezeti és koncepcióális természetűek, e kihívások kezelése csak egy egységes, hosszú távú architektúrára épülő integrátori megközelítéssel lehetséges, amely képes összehangolni a stacioner és a tábori (telepíthető) infokommunikációs rendszerek fejlesztését, biztosítani a szövetségi interoperabilitást, valamint támogatni a modern, hálózatalapú hadviselés követelményeit. Jelentős hátrányba kerültek azok a felek, amelyek nem voltak képesek biztosítani a szenzorok, a döntéshozatal és a végrehajtás közötti folyamatos információáramlást. A konfliktus tanulságai egyértelműen azt mutatják, hogy a rendszerintegráció nem halasztható háttérfeladat, hanem a képességfejlesztések előfeltétele.

A Magyar Honvédség esetében megállapítható, hogy amennyiben az integráció nem jelenik meg a tervezési fázisban, már architektúraszinten, úgy a későbbi megoldások szükségesszerűen kompromisszumosak lesznek, növelve a műveleti kockázatot és a fenntartási terheket.

Mindez alapján a Magyar Honvédség előtt álló rendszerintegrációs (digitalizációs) feladatrendszer nem csupán az új technológiák rendszerbe állítása, hanem azok következetes, hadműveleti logika mentén történő összeillesztése. Ez a megközelítés indokolja, hogy a következő fejezetek a rendszerintegráció architektúráját már nem elméleti, hanem gyakorlati oldalról vizsgálják.

A RENDSZERINTEGRÁCIÓ ARCHITEKTÚRÁJA – A HORIZONTÁLIS INTEGRÁCIÓ

A horizontális integráció a katonai rendszerintegráció egyik alapvető dimenziója, amely a peremvonalon – adott esetben a peremvonalon túl – keletkező információk folyamatos, biztonságos és hadműveletileg releváns továbbítását biztosítja a stratégiai szintű döntéshozatalig. E filozófia középpontjában nem egy-egy technikai alrendszer működése áll, hanem az információ teljes életútja, annak keletkezésétől kezdve a feldolgozáson és aggregáláson át egészen a döntéshozók számára történő megjelenítésig.

⁸ The Headquarters Multinational Division Centre (HQ MND-C).

⁹ Federated Mission Networking (FMN)... 2021: i. m.

Hadműveleti értelemben a horizontális integráció biztosítja azt az információs folytonosságot, amely nélkül a modern vezetés-irányítás elképzelhetetlen. A rendszer akkor tekinthető horizontálisan integráltnak, ha a peremvonalon keletkező információk torzulás és indokolatlan késedelem nélkül képesek eljutni a megfelelő vezetési szintekre, miközben megőrzik relevanciájukat és megbízhatóságukat. A Magyar Honvédség esetében a horizontális integráció a felderítőszenzoroktól és a digitális katona által alkalmazott szenzoroktól indul, majd a harcászati szinten alkalmazott digitális átviteli megoldásokon és harcjármű-fedélzeti rendszereken keresztül jut el a zászlóalj-, dandár-, hadműveleti és végső soron a stratégiai szintű vezetési pontokig. A folyamat sikeressége azon múlik, hogy e lánc minden eleme kompatibilis legyen egymással, és az információ torzulás, késedelem vagy biztonsági kockázat nélkül haladjon végig a rendszeren.

Az információ keletkezése a peremvonalon

A horizontális integráció kiindulópontja a harcmezőn, illetve a peremvonalon alkalmazott szenzorok és végrehajtó elemek szintje. Idetartoznak a felderítőegységek érzékelői, a pilóta nélküli rendszerek, a különleges műveleti elemek adatforrásai, valamint a harcos szintjén megjelenő digitális eszközök. A modern hadviselés egyik meghatározó jellemzője, hogy ezek az eszközök nagyságrendekkel több adatot állítanak elő, mint amennyit a hagyományos vezetési struktúrák képesek hatékonyan kezelni. Ebben az értelemben a harcászatba is betörni látszik a „big data”,¹⁰ mely technológiailag a hatalmas adatmennyiségek gyors és hatékony kezelését, feldolgozását jelenti, még akkor is, ha azok különböző forrásokból származnak, és eltérő struktúrával rendelkeznek. Kiemelten fontos a valós vagy közel valós idejű kiértékelésük biztosítása, ami lehetővé teszi a szükség szerinti azonnali vagy rendkívül gyors reagálást az eseményekre. Az orosz–ukrán háború bebizonyította, hogy egység felderítő-elemzői szinten már nemcsak harcászati adatokat, hanem adott esetben a közösségi médián keresztül érkező nyers információkat is szükséges feldolgozni.

A horizontális integráció hadműveleti értelme ezért nem pusztán az adatok továbbításában, hanem azok elsődleges feldolgozásában és szűrésében ragadható meg. A peremvonalhoz közel végrehajtott előfeldolgozás – az úgynevezett „edge computing”¹¹ jellegű megoldások – lehetővé teszi, hogy a vezetési szintek felé már csak a hadműveletileg releváns információk kerüljenek továbbításra. Ennek hiányában az információs túlterhelés a döntéshozatal lassulásához, végső soron pedig hatékonyságcsökkenéshez vezet.

¹⁰ A big data fogalma alatt azt a rendkívül komplex technológiai környezetet – beleértve a szoftvereket, hardvereket és hálózati modelleket – értjük, amely lehetővé teszi olyan hatalmas és bonyolult adatállományok begyűjtését, tárolását, feldolgozását és elemzését, amelyek méretük és komplexitásuk miatt a hagyományos adatbázis-menedzsment eszközökkel már csak jelentős nehézségek árán, vagy egyáltalán nem kezelhetők hatékonyan. A big data koncepciója alapvetően a nagy mennyiségű (volume), nagy sebességgel keletkező vagy változó (velocity) és rendkívül változatos formátumú (variety) adatok kezelésének és elemzésének kihívásairól és az ezekre adott technológiai válaszokról szól, célja pedig az adatokban rejlő érték kinyerése.

¹¹ Az „edge computing” (peremhálózati számítástechnika) egy olyan informatikai modell, amely az adatfeldolgozást és -tárolást a forráshoz – például szenzorokhoz, okoseszközökhöz vagy helyi szerverekhez – közel, a hálózat „szélén” végzi, nem pedig távoli felhőközpontokban. Ez csökkenti a késleltetést, növeli a sebességet, és csökkenti a sávszélességigényt.

A digitális katona szerepe a horizontális integrációban

A digitális katona koncepciója a horizontális integráció egyik kulcseleme. A harcos szintjén megjelenő digitális eszközök – hordozható informatikai platformok, harcászati kézi és személyi rádiók („soldier”¹² rádiók), valamint különböző szenzorok – lehetővé teszik a harctéri információk valós idejű rögzítését és továbbítását. Hadműveleti szempontból azonban e képességek csak akkor járulnak hozzá a harcérték növekedéséhez, ha nem önálló, elszigetelt információs szigeteket hoznak létre.

A horizontális integráció megköveteli, hogy a digitális katona által generált információk szervesen illeszkedjenek a raj-, a szakasz- és a századszintű vezetési rendszerekbe, ennek hiányában a harcos szintjén keletkező adatok nem hasznosulnak, vagy éppen ellenkezőleg, aránytalan terhelést jelentenek az alsóbb vezetési szintek számára. A rendszerintegráció feladata ebben az összefüggésben az, hogy a digitális katona képességeit a teljes vezetési lánc részévé tegye, nem pedig önálló technológiai fejlesztésként kezelje.

Harcjárművek mint információs csomópontok

A korszerű harcjárművek horizontális integrációs szerepe kiemelt jelentőségű. A lövész harcjárművek, harckocsik és egyéb harceszközök fedélzeti rendszerei egyre inkább információs csomópontként, vagy más néven fedélzeti intelligenciaként működnek, ahol különböző híradási formák, szenzoradatok és vezetési információk találkoznak. A fedélzeti intercom és a kapcsolódó informatikai alrendszerek nem csupán a személyzet belső kommunikációját szolgálják, hanem lehetőséget biztosítanak a szenzoradatok, a vezetési információk és a fegyverrendszerek vezérlésének integrált kezelésére, ezért a horizontális integráció sikeressége nagymértékben függ attól, hogy a fedélzeti rendszerek milyen mértékben képesek együttműködni a felsőbb vezetési szintek informatikai környezetével.

Hadműveleti szempontból a harcjárművek fedélzeti rendszerei jelentik azt a szintet, ahol a harcos és a magasabb vezetési szintek közötti információáramlás ténylegesen összekapcsolódik. Amennyiben e rendszerek nem képesek együttműködni a felsőbb vezetési szintek informatikai környezetével, úgy a horizontális integráció megszakad, és az információ nem jut el a döntéshozókhoz időben vagy megfelelő formában.

A vezetési pontok szerepe az információ aggregálásában

A zászlóalj- és dandárszintű vezetési pontok a horizontális integráció kritikus elemei, ezeken a szinteken történik az alsóbb vezetési szintekről érkező információk összesítése, értékelése és továbbítása a hadműveleti szint felé. A tábori (telepíthető) vezetési pontok infokommunikációs kiszolgálása csak akkor képes megfelelni a hadműveleti követelményeknek, ha a vezetékek nélküli és a vezetékes átviteli megoldások egységes architektúra mentén kerülnek redundáns módon alkalmazásra.

A redundancia, az alternatív átviteli utak és a gyors újrakonfigurálhatóság alapvető követelményként jelennek meg. Egy vezetési pontnak képesnek kell lennie gyorsan alkalmazkodni a megváltozott körülményekhez, legyen szó ellenséges elektronikai tevékenységről, fizikai károsodásról vagy kibertérből érkező fenyegetésekről.

¹² Egyszerűsített kezelőszervű kiszálló katonarádió (elsősorban a lövészkomponens részére).

Horizontális integráció stratégiai és szövetségi szinten

Hadművelleti és stratégiai szinten a horizontális integráció biztosítja azt az információs kontinuitást, amely nélkül a nemzeti és a szövetségi műveletek irányítása elképzelhetetlen. Az összhaderőnemi (*joint*) vagy szárazföldi (*ground*) típusú hadtest- és hadosztály-parancsnokságok (mint például a Többnemzeti Hadosztály-parancsnokság) és a stratégiai vezetési pontok működése megköveteli, hogy a harcászati szinten keletkező információk strukturált, szabványosított formában jelenjenek meg, támogatva a közös művelleti helyzetkép kialakítását. Ezen a szinten különösen fontossá válik a nemzeti rendszerek és a NATO által alkalmazott megoldások közötti interoperabilitás biztosítása.

Hadművelleti tanulságok

Az orosz–ukrán háború tapasztalatai rávilágítottak arra, hogy a nagy mennyiségű adat önmagában nem jelent előnyt, sőt, megfelelő szűrés és priorizálás hiányában a döntéshozatalt lassíthatja. A Magyar Honvédség számára ezért alapvető követelmény, hogy a horizontális integráció ne pusztán technikai összekapcsolást jelentsen, hanem támogassa az információk relevanciaalapú kezelését és a döntéshozók tehermentesítését.¹³

Megállapítható, hogy a horizontális integráció a Magyar Honvédség rendszerintegrációs architektúrájának gerincét képezi. A peremvonalon keletkező, majd feldolgozott információk stratégiai szintig történő eljuttatása csak akkor lehet hatékony, ha az integráció már a szenzor és a harcos szintjén megkezdődik, és a rendszerintegrációs folyamat következetesen érvényesül a teljes vezetési láncon, harctéri adatfolyamon. E megközelítés teremti meg az alapot a következő fejezetben tárgyalt vertikális integráció értelmezéséhez.

A RENDSZERINTEGRÁCIÓ ARCHITEKTÚRÁJA – A VERTIKÁLIS INTEGRÁCIÓ

A vertikális integráció a katonai rendszerintegrációnak az a dimenziója, amely az alkalmazott híradási és adatátviteli technológiák egymáshoz illesztését, valamint azok egységes, hadműveletileg koherens rendszerbe szervezését biztosítja, a stratégiai besorolású technológiáktól egészen a harcmezőn alkalmazott eszközökig. Amíg a horizontális integráció elsődlegesen az információ áramlásának irányára és folyamatára koncentrál, addig a vertikális integráció az információ továbbítását lehetővé tevő technológiai rétegek közötti koherenciát és átjárhatóságot helyezi a középpontba.

A Magyar Honvédség esetében a vertikális integráció jelentősége különösen nagy, mivel a vezetés-irányítási rendszer működése egyszerre támaszkodik stratégiai szintű stacioner infrastruktúrára, illetve a hadművelleti és harcászati szinten működő tábori (telepíthető) rendszerekre, valamint bérelt vagy szövetségi biztosítású átviteli képességekre. A sokrétű technológiai környezet csak akkor képes hadműveletileg megbízható módon működni, ha az egyes átviteli megoldások nem párhuzamos, elszigetelt rendszerekként, hanem egymást kiegészítő, redundáns rétegekként kerülnek alkalmazásra.

¹³ Watling–Reynolds 2023, 13–15.

Hadműveleti értelemben a vertikális integráció hiánya akkor válik kritikussá, amikor az információ ugyan rendelkezésre állna, de a technológiai háttér nem képes azt megfelelő időben, megfelelő minőségben és biztonságosan továbbítani. A vertikális integráció ezért nem pusztán technológiai kérdés, hanem közvetlen hatással van a vezetés-irányítás folyamatosságára és a döntéshozatal megbízhatóságára.

A vertikális integráció szerepe a hadműveleti túlélőképességben

A modern hadviselés egyik meghatározó jellemzője a híradó- és információs rendszerek elleni célzott fellépés. Elektronikai hadviselés, kibertámadások, kinetikus csapások és információs műveletek egyaránt veszélyeztetik a vezetés-irányítás technológiai alapjait. Ebben a környezetben a vertikális integráció egyik elsődleges feladata a túlélőképesség növelése, amely csak több, egymást átfedő és egymást kiegészítő átviteli réteg alkalmazásával érhető el.

A hadműveleti oldalról megközelítve nem az egyes technológiák abszolút teljesítménye a döntő, hanem az, hogy a rendszer egésze képes-e gyorsan váltani a különböző átviteli megoldások között, és fenntartani a vezetési folyamat folytonosságát kedvezőtlen körülmények között is. A vertikális integráció ennek a képességnek az architektúráis alapját teremti meg.

Felső rétegek: műholdas és nagy hatótávolságú átviteli megoldások

A vertikális integráció felső rétegét a műholdas távközlési képességek alkotják. A stratégiai és a hadműveleti szintű vezetési pontok számára a műholdas kommunikáció biztosítja a nagy távolságú, földi infrastruktúrától független adat- és hangátvitelt, valamint a szövetségi rendszerekhez való csatlakozás egyik alapfeltételét. A műholdas képesség többféle rendszerek egyidejű használatát is jelentheti, így az alacsony pályás, a közepes magasságú és a geostacionárius pályán keringő műholdrendszerek alkalmazását is. A nemzeti műholdképesség¹⁴ kialakítása, illetve a katonai célú bérelt kapacitások rendszerben tartása egyidejűleg a bérelt polgári műholdas kapacitásokkal egyaránt hozzájárul a vertikális integráció stabilitásához, különösen válsághelyzetekben vagy nagy intenzitású műveletek során.

A műholdas réteg különösen fontos válsághelyzetekben és nagy intenzitású műveletek során, amikor a földi infrastruktúra sérülékenysége megnő.

A műholdas képességek azonban önmagukban nem tekinthetők elegendőnek. A műholdas réteg alatt helyezkednek el a nagy hatótávolságú vezeték nélküli átviteli megoldások, mint a troposzféra átvitel és a digitális mikrohullámú rendszerek. Ezek a technológiák hídakat képeznek a stacioner és a tábori hálózatok között, lehetővé téve a hadműveleti területen telepített vezetési pontok nagy sávzélességű kiszolgálását.

A vertikális integráció szempontjából a rendszerek szerepe kettős, egyrészt alternatívát biztosítanak a műholdas összeköttetések mellett, másrészt növelik a rendszer egészének túlélőképességét és redundanciáját. A vertikális integráció megköveteli, hogy a műholdas

¹⁴ A magyar nemzeti műholdképesség fejlesztése stratégiai cél, amely magában foglalja az űripari ökoszisztéma kiépítését, a távközlési piac erősítését és védelmi ipari fejlesztéseket. A 4iG Space & Defense és a Remred közreműködésével zajló programok célja a hazai űrtevékenység növelése, beleértve a műholdgyártást és a kapcsolódó infrastruktúra kiépítését, valamint független távközlési képesség kialakítását.

megoldások szervesen illeszkedjenek más, nagy hatótávolságú vezeték nélküli technológiákhoz, mint például a mikrohullámú vagy a troposzféra átvitel. Ezek a rendszerek hidat képeznek a stacioner és a tábori (telepíthető) hálózatok között, és alternatívát biztosítanak a műholdas összeköttetések kiesése esetén.

Középső rétegek: többszintű drónképesség, hadműveleti és harcászati vezeték nélküli rendszerek, telepíthető hírközpontelem-képességek

A vertikális integráció középső rétegét a hadműveleti és harcászati szinten alkalmazott drónalapú átjátszóképeség, a vezeték nélküli adat- és hangátviteli megoldások alkotják, de idetartoznak a közepes és a rövid hatótávolságú vezeték nélküli adat- és hangátviteli megoldások is – beleértve a harcászati rádiórendszereket, a MIMO-Mesh rádióhálózatokat,¹⁵ a speciális katonai célú Wi-Fi- és LTE-megoldásokat –, amelyek a vertikális integráció következő rétegét alkotják.

Ebbe a rétegbe értjük azokat a katonai telepíthető hírközpontelemeket (híradó-informatikai komplexumok és hordozható infokommunikációs rendszerelemek) is, melyek az egység (és alegység) telepíthető infokommunikációs technikai képességét biztosítják.

Ezek a technológiák közvetlenül támogatják a zászlóalj- és a dandárszintű vezetést, valamint biztosítják a kapcsolatot a harcjárművek, az alegységek és a vezetési pontok között. A vertikális integráció szempontjából kritikus követelmény, hogy a rendszerek egységes adatstruktúrák és szabványos interfészek mentén legyenek képesek csatlakozni a felsőbb szintek hálózataihoz, mert az integráció csak ekkor lesz sikeres, ennek hiányában a harcászati szinten keletkező információk nem, vagy csak jelentős késedelemmel jutnak el a hadműveleti döntéshozatal szintjére.

Alsó rétegek: rövid hatótávolságú és vezetékes megoldások

A vertikális integráció alsó rétegeit a rövid hatótávolságú vezeték nélküli rendszerek, valamint a vezetékes átviteli megoldások alkotják. A vezetékes átviteli megoldások – ideértve a tábori optikai és hagyományos vezetékes hálózatokat, valamint a stacioner optikai gerinchálózatot –, továbbá a harcjárművek fedélzeti hálózatai, a vezetési pontok belső kommunikációs rendszerei és a tábori optikai hálózatok biztosítják azt a stabil technológiai alapot, amelyre a magasabb szintű vezetési és döntéstámogató rendszerek épülnek.

Vannak olyan harcászati helyzetek és feladatok, amikor a vezetési pontok belső hálózatai, az adatközponti elemek és a kiszolgáló rendszerek megbízható működése csak megfelelő vezetékes infrastruktúra (optika, réz) mellett biztosítható.

Hadműveleti szempontból a vezetékes megoldások gyakran háttérbe szorulnak a mobilitás iránti igény miatt, ugyanakkor a vezetési pontok belső működése és az adatfeldolgozás megbízhatósága csak megfelelő vezetékes infrastruktúra mellett biztosítható. A vertikális integráció egyik alapvető követelménye, hogy a vezetékes és a vezeték nélküli megoldások egymást kiegészítve, nem pedig egymással versengve kerüljenek alkalmazásra, azaz a vezetékes és a vezeték nélküli technológiák nem egymás alternatívái, hanem egymást kiegészítő elemek.

¹⁵ Ez egy olyan technológia, amely dinamikusan hoz létre új kapcsolatokat, és csatlakozik más csomópontokhoz. Előnyei az önszerveződő hálózat, az önjavítás, a többugrásos kaszkádolás és a csomópont-önkezelés, amelyek nagymértékben csökkenthetik a hálózati telepítés költségeit és bonyolultságát.

Szoftverrendszerek és hálózati rétegek összhangja, valamint információvédelem és információbiztonság

A vertikális integráció nem korlátozódik csak a fizikai átviteli megoldásokra. A vezetés-irányítási, a felderítő- és a tűzvezetőszoftver-rendszerek működőképessége közvetlenül függ attól, hogy az alkalmazott hálózati rétegek biztosítják-e a szükséges sávszélességet, késleltetési paramétereket és információbiztonsági feltételeket. A technológiai rétegek közötti összhang hiánya közvetlenül rontja a szoftverrendszerek hatékonyságát és ezáltal a döntéshozatal minőségét.

A képességsomagból nem szabad kihagyni azokat az információvédelmi képességeket és eljárásrendet, melyek megvalósítják azt a védelmet, amely a saját információnkat elrejti a szemben álló fél vagy az azonosíthatatlan identitású offenzív kibertervekenységet végző identitás elől. A hálózatalapú hadviselés egyik kulcseleme a saját információnk védelme és a megfelelő egyéni kibertudatosság megléte (OPSEC¹⁶).

Hadműveleti tanulságok

Az orosz–ukrán háború tapasztalatai egyértelműen alátámasztják a vertikális integráció jelentőségét. Azok a rendszerek bizonyultak ellenállóbbnak, amelyek több, egymást átfedő átviteli rétegre támaszkodtak, valamint képesek voltak gyorsan váltani a különböző technológiai megoldások között. A konfliktus tanulságai a Magyar Honvédség számára is világossá teszik, hogy a vertikális integráció nem opcionális technikai fejlesztés, hanem a rendszer túlélőképességének és hadműveleti megbízhatóságának alapfeltétele.

Alaptézis, hogy a vertikális integráció a Magyar Honvédség rendszerintegrációs architektúrájának meghatározó pillére. A különböző híradási és adatátviteli technológiák egységes rendszerbe szervezése teremti meg annak lehetőségét, hogy a horizontális integráció során keletkező információk megbízható módon jussanak el a megfelelő vezetési szintekre. Ez a rétegzett megközelítés képezi az alapját a következő fejezetben tárgyalt diagonális integrációnak, amely a konkrét rendszerintegrátori feladatok és interfészek szintjén vizsgálja a Magyar Honvédség infokommunikációs rendszerének működését.

A RENDSZERINTEGRÁCIÓ ARCHITEKTÚRÁJA – A DIAGONÁLIS INTEGRÁCIÓ

A diagonális integráció a katonai rendszerintegrációnak az a dimenziója, amely a horizontális és a vertikális integráció metszéspontjában jelenik meg, és a rendszer tényleges működőképességét meghatározó konkrét együttműködési pontokra fókuszál. Amíg a horizontális integráció az információ áramlási útját, a vertikális integráció pedig az alkalmazott

¹⁶ Az OPSEC (Operations Security, azaz műveleti biztonság) egy folyamat, amelynek célja a kritikus információk védelme a potenciális ellenfelek elől, megakadályozva, hogy azokat felhasználhassák a célok (legyenek azok katonai, üzleti vagy személyes) kárára; ez magában foglalja az információk azonosítását, a fenyegetések elemzését, a sebezhetőségek feltárását és a kockázatok csökkentését, gyakran az egyéni online viselkedés (digitális lábnyom) ellenőrzésével is.

technológiai rétegek összhangját írja le, addig a diagonális integráció arra ad választ, hogy az egyes rendszerek és alrendszerek miként képesek ténylegesen együttműködni a hadműveletek során.¹⁷

A Magyar Honvédség esetében a diagonális integráció különös jelentőséggel bír, mivel a vezetés-irányítási és infokommunikációs környezetben számos eltérő időben, eltérő gyártói és technológiai háttérrel kialakított informatikai és szoftverrendszer működik párhuzamosan. A rendszerek együttműködése nem biztosítható pusztán szabványok vagy technikai interfészek meglétével, hanem célzott rendszerintegrátori tevékenységet, mérnöki támogatást és folyamatos együttműködést igényel az érintett gyártók és üzemeltetők között.

Hadművelleti értelemben a diagonális integráció hiánya akkor válik kritikussá, amikor az információ ugyan rendelkezésre állna, a technológiai infrastruktúra is működőképes, de a különböző rendszerek közötti együttműködés hiánya miatt a döntéshozatal mégsem válik gyorsabbá vagy pontosabbá. A diagonális integráció ezért tekinthető a rendszerintegráció „kritikus láncszemének”, amely közvetlen hatással van a vezetés-irányítás hatékonyságára.

A rendszerintegrátor szerepe és jelentősége

A diagonális integráció egyik alapfeltétele a rendszerintegrátori képesség megléte. A korszerű hadseregek tapasztalatai azt mutatják, hogy a különböző gyártók által szállított eszközök és szoftverrendszerek összehangolása nem hagyható kizárólag a beszállítókra, szükség van egy olyan kompetens, hadművelleti szemléletű rendszerintegrátori szerepkörre, amely képes az architektúrák következtességbiztosítására, a katonamérnöki szemlélet és a hosszú távú fenntarthatóság kritériumainak szem előtt tartására.

A Magyar Honvédség esetében ez a szerep különösen felértékelődik, mivel a jelenlegi és a tervezett rendszerek jelentős része eltérő technológiai háttérrel, eltérő adatstruktúrákkal és eltérő biztonsági megoldásokkal rendelkezik. A rendszerintegrátor feladata nem pusztán az interfészek kialakítása, hanem annak biztosítása, hogy a rendszer egésze hadműveletileg értelmezhető és kezelhető maradjon. A kutatások és a nemzetközi tapasztalatok alapján a rendszerintegrátori mérnöki munka és a programmenedzsment-szemléletű ciklikus rendszerű tervezés csakis egy közös katonai-polgári együttműködésben létrehozott szervezettel valósítható meg. A katonai rész adja a haderő igényeihez és a szövetségi elkötelezettségekhez igazított tervezési és hadművelleti szakértői képességet, míg a polgári rész adja a mérnöki és a fejlesztői tudásbázist, valamint a szaktudást, illetve azt a programmenedzsmenti tapasztalatot a sikeres integráció érdekében, mely képes a megfelelő szerződésekkel a zökkenőmentes rendszerintegrációhoz az összes érintett felet (gyártót) és képességet összefogni.

Szenzorok és adatforrások integrációja

A diagonális integráció egyik legfontosabb területe a szenzorok és az egyéb adatforrások integrálása a vezetés-irányítási rendszerbe. A felderítőszenzorok, pilóta nélküli rendszerek és egyéb érzékelők által szolgáltatott adatok csak akkor járulnak hozzá a hadművelleti hatékonysághoz, ha strukturált, feldolgozható formában jelennek meg a vezetési és a döntéstámogató rendszerekben.

¹⁷ Rendszerintegráció feladatrendszere (belső koncepcióanyag): i. m.

Ennek hiányában a szenzorok által generált adatok elszigetelt információhalmazként jelennek meg, ami nem támogatja érdemben a döntéshozatalt. A diagonális integráció feladata ebben az összefüggésben az adatkonverziók, a szűrési mechanizmusok és a priorizálási eljárások kialakítása, valamint a különböző szoftverrendszerek közötti kompatibilitás biztosítása.¹⁸

Digitális katona és harcjármű-fedélzeti rendszerek összekapcsolása

A digitális katona és a harcjármű-fedélzeti rendszerek integrációja a diagonális integráció egyik legösszetettebb, ugyanakkor hadműveletileg legkritikusabb területe. A harcosszintjén keletkező információk csak akkor hasznosíthatók hatékonyan, ha zökkenőmentesen illeszkednek a raj-, a szakasz- és a századszintű vezetési rendszerekhez, valamint a harcjárművek fedélzeti informatikai környezetéhez.

A fedélzeti belső beszélgetőrendszer és az ahhoz kapcsolódó „központi intelligencia” szerepe itt abban áll, hogy összekapcsolja a különböző kommunikációs és informatikai alrendszereket, valamint biztosítsa azok egységes működését. Amennyiben ez az integráció nem valósul meg, úgy a digitáliskatona-koncepció hadműveleti előnyei nem realizálódnak, sőt akár növelhetik is a vezetési terhelést.

Szoftverintegráció és adat-interoperabilitás

A diagonális integráció egyik legösszetettebb eleme a szoftverrendszerek közötti együttműködés biztosítása. A vezetés-irányítási, a felderítő- és a tűzvezető rendszerek csak akkor képesek hatékonyan támogatni a műveleteket, ha az alkalmazott szoftverek képesek szabványosított adatstruktúrák kezelésére és egymással történő adatcserére.

A Magyar Honvédség esetében különös hangsúlyt kap a nemzeti fejlesztésű vezetés-irányítási megoldások (a HUNTACCIS¹⁹ vezetés-irányítási szoftverrendszer) és a NATO által alkalmazott automatizált vezetés-irányítási szoftverek közötti interoperabilitás biztosítása, ami folyamatos tesztelést és validációt igényel.

Ez a feladat érintheti az összes fegyverrendszerhez és vezetés-irányítási alrendszerhez beszerzett szoftvert és alkalmazást, amelyeknek egymáshoz történő integrálása folyamatos tesztelést, validációt és visszacsatolást igényel, ami a rendszerintegráció egyik legfontosabb, ugyanakkor legnagyobb erőforrás-igényű területe. A katonai oldal a szövetségi rendszerben az évenként megrendezett NATO CWIX²⁰ interoperabilitási gyakorlatsorozaton tudja a rendszereinek az interoperabilitási képességét mérni, az új fejlesztéseit tesztelni, vagy éppen az elkészült terméket validálni.

Minősített és nem minősített tartományok kezelése

A diagonális integráció további kritikus területe az informatikai tartományok és minősítési szintek kezelése. A nyílt és a minősített hálózatok közötti átjárhatóság megteremtése csak megfelelő szűrő- és átjárómegoldások alkalmazásával lehetséges, amelyek biztosítják az

¹⁸ (AJP-6) 2024, 10–25.

¹⁹ Az MH Tábori vezetési és irányítási (C2) szoftverrendszere (HUNGarian Tactical Command and Control Information System).

²⁰ A CWIX (Coalition Warrior Interoperability eXploration, eXperimentation, eXamination, eXercise) a NATO (és a PfP-országok) katonai híradó-informatikai rendszereinek interoperabilitási rendszergyakorlatát jelenti.

információbiztonsági követelmények betartását, miközben nem akadályozzák a hadműveleti információáramlást. Ezek lehetnek egyirányú adatdiódák²¹ vagy kétirányú IEG-ek.²²

A diagonális integráció szorosan kapcsolódik a kibertérműveletekhez és a kibervédelmi képességekhez is. A hálózatba kapcsolt rendszerek növekvő száma és komplexitása növeli a támadási felületet, ezért a rendszerintegráció során a kibervédelmi szempontoknak már a tervezési fázisban meg kell jelenniük. A kibervédelem nem önálló funkcióként, hanem a teljes infokommunikációs és vezetés-irányítási rendszer szerves részeként értelmezendő.²³

Ez a terület egyszerre technikai, szabályozási, eljárásrendi és szervezeti kérdés. A diagonális integráció feladata ebben az összefüggésben az, hogy az információbiztonság és a hadműveleti szükségletek közötti egyensúlyt fenntartsa, elkerülve mind a túlzott kockázatvállalást, mind a túlzott korlátozást.

Diagonális integráció és C2-hatékonyság

Az orosz–ukrán háború tapasztalatai világosan rámutattak arra, hogy a diagonális integráció hiánya közvetlen hadműveleti következményekkel járhat, az integráció hiányosságai közvetlenül mérhető hatással vannak a vezetés-irányítás hatékonyságára. A nem megfelelően integrált szenzorok, a széttagolt szoftverrendszerek és az információbiztonsági akadályok egyaránt növelik a döntéshozatal idejét és rontják a döntések minőségét. Ezzel szemben a jól megtervezett diagonális integráció képes csökkenteni a vezetési lánc terhelését, valamint támogatni a gyorsabb, megalapozottabb döntéshozatalt.

A Magyar Honvédség számára ez is megerősíti azt, hogy a diagonális integráció nem opcionális kiegészítő tevékenység, hanem a rendszerintegráció egyik központi eleme, ennek a feladatrendszernek a sikeres végrehajtása teremti meg a kapcsolatot az elméleti architektúra és a gyakorlati megvalósítás között. A Magyar Honvédség rendszerintegrációs architektúrája csak akkor válhat valóban működőképpé, ha a horizontális és vertikális integráció mentén kialakított struktúrákat következetes, hadműveleti és egyben mérnöki szemléletű integrátori tevékenység köti össze.

KATONAI DIGITALIZÁCIÓ ÉS A KIBERTÉR KIHÍVÁSAI A RENDSZERINTEGRÁCIÓ TÜKRÉBEN

A katonai digitalizáció napjainkra a haderőfejlesztés egyik meghatározó irányává vált, ugyanakkor a technológiai fejlődés önmagában nem eredményez automatikusan hadműveleti képességnövekedést. A digitalizáció valódi katonai értéke abban ragadható meg, hogy miként képes támogatni a vezetés-irányítási folyamatokat, csökkenteni a döntéshozatali ciklusidőt, valamint növelni a rendszer egészének ellenálló képességét. E célok csak akkor érhetők el, ha a digitalizáció szorosan illeszkedik a rendszerintegráció architektúrájához, és nem önálló, elszigetelt fejlesztési irányként jelenik meg.

²¹ Az adatdióda egy olyan kiberbiztonsági hardvereszköz, amely egyirányú adatáramlást biztosít, ami azt jelenti, hogy az adatok fizikailag csak egy irányba haladhatnak egyik hálózatból a másikba, a visszaáramlás lehetősége nélkül. Ez az egyirányú kommunikáció elengedhetetlen az érzékeny rendszerek védelméhez, mivel teljesen elszigeteli azokat a külső fenyegetésektől.

²² A NATO meghatározta az információcsere-átjáró (IEG – Information Exchange Gateway) koncepcióját, hogy elősegítse a különböző minősítési szintű rendszerek közötti biztonságos kommunikációt.

²³ Cyber Operations and the Military Commander...

A Magyar Honvédség esetében a digitalizációs törekvések elsősorban a vezetés-irányítási rendszerek, a szenzorhálózatok, a harcászati és hadművelleti kommunikáció, valamint a támogató informatikai szolgáltatások területén koncentrálódnak. A digitális megoldások elterjedése lehetővé teszi a közös művelleti helyzetkép (COP²⁴) gyorsabb és pontosabb kialakítását, ugyanakkor jelentősen növeli az infokommunikációs rendszer komplexitását. A komplexitás kezelése a rendszerintegráció egyik kulcskérdésévé válik, mivel a digitális rendszerek közötti kölcsönhatások hibás tervezés esetén nemcsak hatékonysági veszteséget, hanem művelleti kockázatot is hordoznak.

A digitalizáció hatása a vezetés-irányításra

A digitalizáció egyik legfontosabb hatása a vezetés-irányítási folyamatok átalakulásában érhető tetten. A korszerű digitális rendszerek lehetővé teszik a közös művelleti helyzetkép gyorsabb és pontosabb kialakítását, valamint a döntéshozók számára releváns információk célzott megjelenítését. Hadművelleti értelemben azonban a digitalizáció csak akkor jelent előnyt, ha nem növeli aránytalanul a vezetési terhelést.

A „több adat = jobb döntés” logika katonai környezetben nem feltétlenül érvényes. A túlzott mennyiségű, szüretlen információ lassíthatja a döntéshozatalt, növelheti a hibázás kockázatát, és csökkentheti a parancsnoki szintek hatékonyságát. A rendszerintegráció feladata ebben az összefüggésben az, hogy a digitalizáció eredményeként keletkező adatokat relevanciaalapon strukturálja, és támogassa a parancsnokok döntési folyamatát, ne pedig helyettesítse azt.

Adatkezelés, információfeldolgozás és döntéstámogatás

A digitalizáció másik jelentős kihívása az adatkezelés és az információfeldolgozás területén jelentkezik. A modern szenzorok, pilóta nélküli rendszerek és digitáliskatonamegoldások nagyságrendekkel több adatot állítanak elő, mint amennyit a hagyományos vezetési rendszerek kezelni tudnak. Ez a jelenség új megközelítést igényel az adatkezelés és az információfeldolgozás területén. A rendszerintegráció egyik kulcskérdése, hogy az adatok miként alakulnak át hadműveletileg értelmezhető információvá, majd döntéstámogató elemekké, hiszen az adatmennyiség növekedése önmagában nem járul hozzá az információs fölény kivívásához, amennyiben nem társul hozzá megfelelő adatfeldolgozási, szűrési és priorizálási képesség.

A digitalizáció akkor szolgálja a hadművelleti hatékonyságot, ha a rendszer képes az adatok automatikus előszűrésére, a redundáns információk kiszűrésére, valamint a parancsnoki szintekhez igazított információmegjelenítésre. Ennek hiányában a digitalizáció nem gyorsítja, hanem lassítja a vezetés-irányítást.

A kibertér mint hadművelleti környezet

A katonai digitalizáció szorosan összekapcsolódik a kibertérrel, valamint a hadművelleti környezettel. A hálózatba kapcsolt rendszerek növekvő száma és komplexitása jelentősen bővíti a támadási felületet, ami a kibervédelem szerepét stratégiai szintre emeli. A kibertérben végrehajtott műveletek – legyenek azok támadó vagy védelmi jellegűek –, közvetlen

²⁴ Common Operating Picture (COP) – közös művelleti helyzetkép.

hatással lehetnek a vezetés-irányítási rendszer működésére és ezáltal a hadműveletek sikerére. Hadműveleti szempontból a kibertér nem különálló dimenzióként értelmezendő, hanem a fizikai műveleti térrel szorosan összekapcsolódó környezetként.

A rendszerintegráció feladata ebben az összefüggésben az, hogy a kibervédelmi megoldások a teljes infokommunikációs és vezetés-irányítási rendszer szerves részeként jelenjenek meg, nem pedig utólagos kiegészítésként, ugyanis a katonai digitalizáció és a kibertér kihívásai elválaszthatatlanok a rendszerintegráció kérdésétől.²⁵

Információbiztonság és minősítési szintek a digitalizáció korában

A Magyar Honvédség számára külön kihívást jelent a nyílt és a minősített informatikai környezetek párhuzamos kezelése a digitalizáció előrehaladtával. A digitális rendszerek közötti adatsere megköveteli a különböző minősítési szintek közötti szabályozott átjárhatóságot, ami csak megfelelő technikai és eljárásrendi megoldásokkal biztosítható. E területen a rendszerintegráció feladata az információbiztonsági követelmények és a hadműveleti szükségletek közötti egyensúly megteremtése.

A harc megvívása szempontjából a túlzottan merev biztonsági megoldások akadályozhatják az információáramlást, míg a túlzott engedékenység elfogadhatatlan kockázatokat hordoz. A digitalizáció és a rendszerintegráció közös feladata ezért az információbiztonsági követelmények és a hadműveleti szükségletek közötti dinamikus egyensúly megteremtése.

Hadműveleti tanulságok és következtetések

Az elmúlt évek fegyveres konfliktusainak tapasztalatai – különösen az orosz–ukrán háború – világosan rámutattak arra, hogy a digitalizáció önmagában nem jelent hadműveleti fölényt. Azok a felek voltak képesek hatékonyan alkalmazni digitális képességeiket, amelyek a technológiai megoldásokat integrált rendszerként, megfelelő kibervédelmi háttérrel és hadműveleti szemlélettel alkalmazták.

A Magyar Honvédség számára e tanulságok azt erősítik meg, hogy a digitalizáció nem önálló cél, hanem a rendszerintegráció által válik értelmezhető és alkalmazható katonai képességgé, a „nem több adat, hanem jobb döntés” elve ebben az összefüggésben nemcsak technológiai, hanem hadműveleti alapelvként értelmezendő. A digitalizáció pedig csak akkor járul hozzá a vezetés-irányítás hatékonyságának növeléséhez, ha az a horizontális, a vertikális és a diagonális integráció által meghatározott architektúrába illeszkedik, és már a tervezési fázisban figyelembe veszi a kibertérből eredő kockázatokat.

NEMZETKÖZI TAPASZTALATOK ÉS TANULSÁGOK A RENDSZERINTEGRÁCIÓ TERÜLETÉN

A katonai rendszerintegráció és a hozzá kapcsolódó digitalizációs folyamatok napjainkban nem értelmezhetők kizárólag nemzeti keretek között. A modern hadviselés többnemzeti, szövetségi környezetben zajlik, ahol az egyes nemzeti képességek hadműveleti értéke nagymértékben függ azok interoperabilitásától, valamint attól, hogy mennyire képesek illeszkedni

²⁵ Libicki 2009, 139–144.

a szövetségi vezetés-irányítási és információs rendszerekhez. Ennek megfelelően a NATO-tagállamok és más fejlett hadseregek rendszerintegrációs gyakorlata releváns tanulságokkal szolgál a Magyar Honvédség számára.

A NATO Federated Mission Networking (FMN) tapasztalatai

A NATO elmúlt évtizedének egyik legjelentősebb kezdeményezése a Federated Mission Networking (FMN) koncepció bevezetése és folyamatos fejlesztése. Az FMN célja, hogy a különböző nemzeti rendszerek közötti interoperabilitást már békeidőben megalapozza, és lehetővé tegye a többnemzeti műveletek gyors, szabványosított információs támogatását.

Az FMN tapasztalatai egyértelműen rámutattak arra, hogy az interoperabilitás nem valószínűsíthető meg pusztán technikai csatlakozási megoldásokkal. Azok a nemzetek képesek hatékonyan csatlakozni a szövetségi hálózatokhoz, amelyek a nemzeti rendszerintegrációt eleve FMN-kompatibilis architektúrára építik, és nem utólagos illesztésekkel próbálják kezelni az interoperabilitási követelményeket. Az FMN így nemcsak technikai keretrendszerként, hanem szemléletformáló tényezőként is értelmezhető.

Az FMN-környezet evolúciója 2026. január 1-jétől már az FMN *Spiral 5*²⁶ bevezetésére készül, ami azt jelenti, hogy az FMN-családhoz tartozó országok hadseregei tábori (telepíthető) infokommunikációs képességének az interoperabilitási szintje a Spiral 5-ben meghatározott infokommunikációs technikai és informatika eljárásrendi követelményeknek kell, hogy megfeleljen – beleértve azokat a szakterületi szervezet elemeket is, amelyek ehhez szükségesek.

Amerikai tapasztalatok, hálózatközpontú és többdoménes megközelítés

Az Amerikai Egyesült Államok fegyveres erőinek fejlesztési irányai szintén jelentős tanulságokkal szolgálnak a rendszerintegráció stratégiai jelentőségéről. A hálózatközpontú hadviselés koncepcióját követően az amerikai haderő a multitérműveletek támogatását célzó vezetés-irányítási megoldások felé mozdult el, amelyek központi eleme az érzékelők, a döntéshozatali rendszerek és a végrehajtó elemek szoros, architektúraalapú integrációja.

Az amerikai elveken alapuló interoperabilitási filozófia – amely már meghaladta a klaszszikusnak mondható C4 vagy C5ISR metódust –, a Combined Joint All-Domain Command and Control, azaz CJADC2, ez az igazi megközelítése a modern multi-domén hadviselés interoperabilitásának. Ez a koncepció a magas fokú interoperabilitást az együttműködés lehetőségétől a koalíciós interoperabilitási gyakorlatok végrehajtásán, a modernizáció és a digitalizáció szükségességén keresztül vezeti le az interoperabilitás lényegét.

²⁶ Az FMN-spirálok a NATO által jóváhagyott dokumentumok, amelyek meghatározzák a koalíciós hálózatok interoperabilitásának műszaki, eljárási és biztonsági követelményeit. Gördülő, fokozatos megközelítést követnek, a végleges, Spiral 6 specifikációt 2025 novemberében hagyják jóvá, a bevezetése 2030-ra szól, és kiterjed a szabványokra, a szolgáltatási utasításokra és az architektúrákra. Minden spirál eljárási utasításokat (PI – Procedural Instructions) és szervezési utasításokat (SI – Service Instructions) tartalmaz több mint 400 szabványra hivatkozva az interoperabilitás biztosítása érdekében. Míg a korábbi spirálok az operatív (műveleti) hírközlő és informatikai rendszerekre (Communications and Information Systems – CIS) összpontosítottak, az 5. spiráltól kezdve a fókusz kiterjedt a magasabb mélységű hadműveleti, a peremhálózati, alacsony sávszélességű és instabil környezetek számára.

Az amerikai tapasztalatok rávilágítanak arra, hogy a technológiai fölény önmagában nem elegendő. A különböző haderőnemek és domének (szárazföld, légi, tengeri, kibertér, világűr) közötti hatékony együttműködés csak akkor valósulhat meg, ha a rendszerintegráció központi irányítás és következetes architektúra mentén történik. Ennek a megközelítésnek az egyik legfontosabb tanulsága, hogy a rendszerintegráció nem alárendelt műszaki feladat, hanem stratégiai szintű vezetési kérdés.

Európai NATO-tagállamok gyakorlata

Az európai NATO-tagállamok közül több ország – így például Németország és az Egyesült Királyság – a nemzeti vezetés-irányítási rendszerek megújítása során külön hangsúlyt fektet a rendszerintegráció és az architektúraalapú tervezés kérdéseire. Ezekben az országokban a fejlesztések egyik közös jellemzője a moduláris, skálázható rendszerek alkalmazása, amelyek képesek alkalmazkodni a különböző műveleti környezetekhez.

A tapasztalatok ugyanakkor azt is megmutatják, hogy a modularitás önmagában nem jelent megoldást. Amennyiben a modulok közötti kapcsolatok és interfészek nem kerülnek egyértelműen meghatározásra, úgy a rendszer egészének működése fragmentálttá válhat. Az európai gyakorlat ezért megerősíti azt az elvet, hogy a rendszerintegráció folyamatos tevékenység, amely a teljes életciklust végigkíséri a tervezéstől az üzemeltetésig.^{27, 28, 29}

A rendszerintegrátor szerepének nemzetközi felértékelődése

A nemzetközi tapasztalatok egyik közös eleme a rendszerintegrátor szerepének egyértelmű felértékelődése. A fejlett hadseregek egyre inkább felismerik, hogy a különböző gyártók által szállított rendszerek összehangolása nem bízható kizárólag a beszállítókra. Erős, kompetens megrendelői és integrátori képességre van szükség, amely képes az architektúrakövetkezetesség biztosítására, a hadműveleti követelmények érvényesítésére, valamint a hosszú távú fenntarthatóság garantálására.

Ez a szerep különösen fontos lehet többnemzeti környezetben, ahol a nemzeti és a szövetségi követelmények egyidejű teljesítése szükséges.

Az orosz–ukrán háború tanulságai

Az orosz–ukrán háború tapasztalatai különösen értékes tanulságokkal szolgálnak a rendszerintegráció gyakorlati jelentőségéről. A konfliktus során megfigyelhető volt, hogy az a fél, amely képes volt gyorsan integrálni különböző szenzorait, kommunikációs megoldásait és döntéshozatali folyamatait, jelentős hadműveleti előnyre tett szert.

Ezzel szemben a nem megfelelően integrált, széttagolt rendszerek sérülékenysége gyorsan felszínre került. A konfliktus tanulságai megerősítik, hogy a rendszerintegráció hiánya nem csupán hatékonysági veszteséget, hanem közvetlen hadműveleti kockázatot is jelent. Különösen fontos tanulság, hogy a civil technológiák gyors adaptációja csak akkor vezet sikerre, ha az integráció hadműveleti logika mentén történik, és nem *ad hoc* megoldások sorozataként.

²⁷ Sechster Bericht zur Digitalen Transformation... 2024, 4–8.

²⁸ Land Environment Tactical CIS (LE TacCIS) Concept...

²⁹ Joint All-Domain Command and Control (JADC2) Strategy... 2022, 6–9.

Következtetések a Magyar Honvédség számára

A nemzetközi tapasztalatok összességében egyértelmű irányt mutatnak, hogy a rendszerintegráció nem technikai részfeladat, hanem stratégiai jelentőségű katonai képesség. A Magyar Honvédség számára ezek a tanulságok azt erősítik meg, hogy a nemzeti sajátosságok figyelembevételével, de a szövetségi követelményekhez igazodva kell kialakítani a rendszerintegráció architektúráis kereteit.

A siker kulcsa abban rejlik, hogy a technológiai fejlesztések mögött következetes koncepció, világos felelősségi rend és hosszú távú gondolkodás álljon. A nemzetközi példák azt is világossá teszik, hogy a rendszerintegráció nem egyszeri projekt, hanem folyamatos, tanuló folyamat, amely a Magyar Honvédség számára is alapvető feltétele a jövőbeni hadművelési sikernek.

JÖVŐBENI IRÁNYOK ÉS AJÁNLÁSOK A MAGYAR HONVÉDSÉG RENDSZERINTEGRÁCIÓJA SZÁMÁRA

A tanulmány célja a Magyar Honvédség rendszerintegrációs architektúrájának átfogó vizsgálata volt, különös tekintettel a katonai digitalizáció és rendszerintegráció, a vezetés-irányítás és az infokommunikációs képességek összefüggéseire. Az elemzés a horizontális, a vertikális és a diagonális integráció hármas megközelítésére épült, amely alkalmas keretet biztosított a komplex, több szinten működő katonai rendszerek értelmezéséhez.

A vizsgálat eredményei megerősítik a tanulmány alaphipotézisét: a rendszerintegráció hiánya vagy részleges megvalósulása önmagában képes rontani a vezetés-irányítás (C2) hadművelési hatékonyságát, függetlenül az egyes technikai alrendszerek korszerűségétől. A rendszerintegráció így nem pusztán technikai vagy informatikai kérdésként értelmezendő, hanem önálló, hadművelési értelemben kritikus katonai képességként.

A kutatási kérdésekre adott válaszok összegzése

A tanulmány első kutatási kérdése arra irányult, hogy mitől válik a rendszerintegráció hadművelési értelemben kritikus képességgé. Az elemzés alapján megállapítható, hogy a rendszerintegráció kritikus jellege abból fakad, hogy közvetlenül befolyásolja az információáramlás sebességét és megbízhatóságát, a döntéshozatali ciklus (OODA) időigényét, valamint a parancsnoki szintek terhelhetőségét és hatékonyságát.

A második kutatási kérdés azt vizsgálta, hogy mely integrációs dimenziók hiánya okoz mérhető C2-hatékonyságcsökkenést. A tanulmány megállapította, hogy bár mindhárom integrációs dimenzió (horizontális, vertikális, diagonális) hiányosságai kockázatot jelentenek, a diagonális integráció hiánya a legkritikusabb, mivel ez az a szint, ahol az elméleti architektúra gyakorlati működőképességgé alakul át.

Stratégiai szintű irányok

A Magyar Honvédség jövőbeni rendszerintegrációs fejlődése szempontjából elsődleges jelentőségű az architektúraalapú gondolkodás intézményesítése. A nemzetközi tapasztalatok és a hazai sajátosságok egyaránt azt mutatják, hogy a komplex infokommunikációs és vezetés-irányítási rendszerek fejlesztése nem kezelhető eseti vagy kizárólag projektalapú megközelítéssel.

Szükséges egy olyan, szervezetenként és megfelelő jogosultságokkal, továbbá szakmai kompetenciákkal is megerősített rendszerintegrátori szerepkör kialakítása, amely képes a különböző fejlesztési programok architektúráis szintű összehangolására, a hadművelleti követelmények következetes érvényesítésére, valamint a szövetségi interoperabilitás hosszú távú biztosítására.³⁰

Ennek a funkciónak stratégiai jelentősége abban áll, hogy képes hidat képezni a politikai és a katonai célok, illetve a technikai megvalósítás között.

A Magyar Honvédség számára további stratégiai irányt jelent a szövetségi interoperabilitás következetes erősítése. Az FMN és az ahhoz kapcsolódó kezdeményezések nem csupán technikai követelményeket fogalmaznak meg, hanem szemléletváltást is igényelnek a nemzeti rendszerintegrációs gyakorlatban. A jövőbeni fejlesztéseknek ezért már alapértelmezetten figyelembe kell venniük a többnemzeti műveletek információs és vezetési igényeit.

Hadművelleti szintű ajánlások

Hadművelleti szinten a rendszerintegráció jövőbeni irányainak meghatározásakor kiemelt figyelmet kell fordítani arra, hogy a fejlesztések ne önálló képességelemeket, hanem működő vezetési láncokat hozzanak létre. A kibertér és az információbiztonság területén a jövőbeni fejlesztéseknek a „*security by design*”³¹ elvére kell épülniük. A kibervédelmi szempontoknak már a rendszertervezés korai szakaszában meg kell jelenniük, és nem utólagos kiegészítésként kell kezelni őket. Ez különösen fontos a tábori infokommunikációs rendszerek esetében, ahol a mobilitás és a gyors telepíthetőség fokozott sérülékenységet eredményezhet.

A horizontális integráció erősítése érdekében szükséges az információ relevanciaalapú kezelése, különösen a peremvonalon keletkező adatok esetében.

A vertikális integráció területén a túlélőképesség és a redundancia elveinek következetes alkalmazása elengedhetetlen. A különböző átviteli technológiák nem alternatívái, hanem kiegészítői egymásnak, a rendszernek képesnek kell lennie gyors technológiai váltásokra kedvezőtlen hadművelleti környezetben is.

A diagonális integráció tekintetében az egyik legfontosabb ajánlás a szoftver- és az adat-interoperabilitás követelményének következetes érvényesítése. Az újonnan rendszerbe álló eszközök és rendszerek kiválasztásánál nem az önálló teljesítményparamétereknek, hanem az összenszerbe illeszthetőségnek kell elsődleges szempontnak lennie.

A digitalizáció és a humán tényező összefüggései

A tanulmány egyik fontos következtetése, hogy a katonai digitalizáció sikeressége nem kizárólag technológiai kérdés. A humán tényező szerepe a rendszerintegráció jövőjében sem csökkenthető. A komplex, integrált rendszerek üzemeltetése és fejlesztése magasan képzett, rendszerszintű gondolkodásra képes személyi állományt igényel. A képzési és a felkészítési rendszereknek ezért nemcsak az egyes eszközök kezelésére, hanem az integrált működés megértésére is ki kell terjedniük.

³⁰ Zrínyi 2026 Honvédelmi és Haderőfejlesztési Program: i. m.

³¹ A *security by design* (SbD) egy kiberbiztonsági és rendszertervezési koncepció, amely előírja, hogy a biztonságot a kezdetektől fogva be kell építeni a rendszerekbe, nem pedig utólagos gondolatként.

A humán tényező fejlesztése nélkül a legkorszerűbb technológiai megoldások sem képesek hadműveleti előnyt biztosítani. A tudásmegosztás, a gyakorlati tapasztalatok visszacsatolása és a folyamatos továbbképzés a rendszerintegráció fenntarthatóságának alapvető feltétele.

Záró megállapítások

A Magyar Honvédség rendszerintegrációjának jövőbeni irányai egy olyan komplex, több-dimenziós fejlesztési pályát rajzolnak ki, amelyben a technológiai innováció, a szervezeti felkészültség és a hadműveleti gondolkodás szorosan összekapcsolódik. A siker kulcsa abban rejlik, hogy a rendszerintegráció ne kényszerű alkalmazkodásként, hanem tudatosan tervezett, stratégiai képességként jelenjen meg a honvédség fejlesztési gyakorlatában.

A tanulmány rámutatott arra, hogy a Magyar Honvédség előtt álló rendszerintegrációs és digitalizációs kihívások összetettek, és egyszerre érintik a technológiai, a szervezeti és a hadműveleti dimenziókat, illetve a humán jellegű kihívásokat. A modern hadviselés tapasztalatai, valamint a nemzetközi gyakorlatok, továbbá a stacioner és a tábori rendszerek kettőssége, az örökölt infrastruktúra korlátai, valamint a HHP keretében megvalósuló képességfejlesztések integrációs igényei mind azt erősítik, és egyértelműen azt igazolják, hogy a rendszerintegráció nem utólagos korrekciós tevékenység, hanem a képességfejlesztés egyik alapvető előfeltétele.

A nemzetközi tapasztalatok és az orosz–ukrán háború tanulságai egyaránt bebizonyították, hogy az információs fölény, a hálózatalapú hadviselés és a multi-domain műveletek sikerének alapfeltétele az integrált, rugalmas és védett infokommunikációs rendszer. Azok a haderők képesek hatékonyan alkalmazkodni a változó hadműveleti környezethez, amelyek tudatosan építik fel rendszerintegrációs architektúrájukat, valamint megfelelő súlyt helyeznek a kibervédelemre, az interoperabilitásra és a humán erőforrás fejlesztésére. Ez a megközelítés teremti meg annak lehetőségét, hogy a Magyar Honvédség a 21. század hadviselési kihívásaira felkészülten, szövetségi környezetben is hatékonyan tudjon reagálni.³²

A horizontális, a vertikális és a diagonális integráció egységes értelmezése alkalmas arra, hogy a Magyar Honvédség vezetés-irányítási és infokommunikációs rendszerének fejlesztése koherens, hadműveletileg megalapozott irányba haladjon. Ez a megközelítés biztosíthatja azt, hogy a technológiai modernizáció valódi katonai értékke váljon, és a Magyar Honvédség a jövőben is képes legyen hatékonyan reagálni a 21. század hadviselési kihívásaira.

FELHASZNÁLT IRODALOM

- Alberts, David S.: *Information Age Transformation*. CCRP Publication Series, Washington, D.C., 2002. http://www.dodccrp.org/files/Alberts_IAT.pdf (Letöltés időpontja: 2026. 05. 22.)
- Alberts, David S. et al.: *Network Centric Warfare: Developing and Leveraging Information Superiority*. CCRP Publication Series, Washington, D.C., 2002. <https://doi.org/10.21236/ADA406255> (Letöltés időpontja: 2026. 05. 22.)
- *Allied Joint Doctrine for Communication and Information Systems (AJP-6)*. NATO Standardization Office (NSO), 2024. https://www.coemed.org/files/stanags/01_AJP/AJP-6_EDB_V1_E_2525.pdf (Letöltés időpontja: 2026. 05. 26.)

³² Alberts 2002, 21–34.

- *Cyber Operations and the Military Commander*. Tallinn, NATO Cooperative Cyber Defence Centre of Excellence.
- *Federated Mission Networking (FMN) Framework Overview*. NATO Communications and Information Agency, Brussels, 2021.
- Imhof László: *Az orosz–ukrán konfliktus CIS-támogatása és konklúziói*. Ukrán Tapasztalat-feldolgozó Konferencia különkiadás 2024 – Konferencia kiadvány.
- Joint All-Domain Command and Control (JADC2) Strategy. US Department of Defense, Washington, D.C., 2022. <https://media.defense.gov/2022/Mar/17/2002958406/-1/-1/1/SUMMARY-OF-THE-JOINT-ALL-DOMAIN-COMMAND-AND-CONTROL-STRATEGY.PDF> (Letöltés időpontja: 2026. 05. 22.)
- Land Environment Tactical CIS (LE TacCIS) Concept. UK Ministry of Defence, London. <https://www.gov.uk/guidance/le-taccis-programme> (Letöltés időpontja: 2026. 05. 22.)
- Libicki, Martin C.: *Cyberdeterrence and Cyberwar*. RAND Corporation, 2009. <https://doi.org/10.7249/MG87> (Letöltés időpontja: 2026. 05. 22.)
- *Rendszerintegráció feladatrendszere* (belső, saját koncepcióanyag). Magyar Honvédség.
- *Sechster Bericht zur Digitalen Transformation des Geschäftsbereichs des Bundesministeriums der Verteidigung*, Berlin, 2024. <https://www.bmvg.de/resource/blob/5729842/44f9fc60325fb62bf9665cd53d771dc6/download-6-digitalbericht-data.pdf> (Letöltés időpontja: 2026. 05. 22.)
- Watling, Jack – Reynolds, Nick: *Meatgrinder: Russian Tactics in the Second Year of the Ukraine War*. RUSI Special Report, London, 2023. <https://static.rusi.org/403-SR-Russian-Tactics-web-final.pdf> (Letöltés időpontja: 2026. 05. 22.)
- *Zrínyi 2026 Honvédelmi és Haderőfejlesztési Program – nyilvános koncepcióelemek*. https://web.archive.org/web/20180306144605/https://honvedelem.hu/files/files/108409/zrinyi2026_190_190_7.pdf (Letöltés időpontja: 2026. 05. 22.)