

A Magyar Honvédség informatikai interoperabilitási politikája

Jelen publikáció célja a honvédelem informatikai interoperabilitási politikája alapjainak lefektetése. A szerző ennek érdekében összegzi az interoperabilitási kérdések szerepét és jelentőségét; bemutatja az informatikai interoperabilitási politika fogalmát, meghatározza annak legfontosabb jellemzőit; ismerteti a magyar honvédelmi informatikai interoperabilitási politikát befolyásoló alapvető dokumentumokat; végül javaslatot tesz az informatikai interoperabilitási politika tartalmi felépítésére és megfogalmazza legfontosabbnak ítélt elemeit.

A globalizáció és az információ korában az együttműködés minden (politikai, védelmi, gazdasági, kulturális stb.) szférában egyre nagyobb jelentőségre tesz szert. Ezzel egyenes arányban növekszik az interoperabilitás szerepe is, amelynek megjelenése és előtérbe kerülése a technikai és ezen belül elsősorban az informatikai rendszerek és eszközök hálózatba kapcsolódásához köthető. Az interoperabilitás és ezen belül az informatikai rendszerek, eszközök közötti interoperabilitás szerepe napjainkban különösen jelentős szerepre tett szert a katonai alkalmazásban.

A megváltozott biztonságpolitikai környezetben, a katonai műveletek jellegében és azokat végrehajtó erők felépítésében bekövetkezett változások eredményeként az interoperabilitást a NATO új stratégiai koncepciója a Szövetség hatékony működése egyik alapvetően meghatározó tényezőjének minősítette. A NATO prágai csúcscrtekezletét megelőzően, a prágai képességfejlesztési elkötelezettség előkészítéseként a védelmi miniszterek az interoperabilitást már a négy kiemelt jelentőségű műveleti képesség-terület egyikeként azonosították.

A Magyar Honvédség, mint egy NATO-tagállam hadereje számára az interoperabilitás kialakítása és fenntartása a szövetséges, a koalíciós és más együttműködő partnerekkel küldetései és feladatai eredményes és hatékony végrehajtásának mindinkább alapvető feltételévé válik. Bár a Magyar Honvédség jelenlegi helyzetét nagyjából egymástól független rendszerek, szigetszerű megoldások jellemzik és átfogó, integrált informatikai rendszer még nem alakult ki, a kibontakozó és várhatóan felgyorsuló informatikai fejlesztési folyamat megkerülhetlenné teszi az interoperabilitási célok és alapelvek megfogalmazását.

Az informatikai interoperabilitás alapjai

Az informatikai interoperabilitás kérdései, problémái alapvetően olyan tartós, vagy ideiglenes együttműködési helyzetekben merülnek fel, amelyben az egyes szereplők közötti információcsere egy része informatikai (vagy információs képességekkel rendelkező más technikai – továbbiakban együtt röviden informatikai) rendszereik, eszközeik közötti, emberi közreműködés nélküli adatcsere révén valósul meg. Az interoperabilitási kérdések felmerülésének további feltétele az adatcserében érintett informatikai rendszerek, eszközök közötti különbözőségek, heterogenitás megléte.

Megoldásra váró informatikai interoperabilitási probléma akkor jelentkezik, amikor különböző informatikai rendszerek nem képesek tulajdonosaik, felhasználóik igényeinek

megfelelő, vagyis szervezeti működési folyamataik által megkövetelt módon, mértékben és minőségben információt cserélni, a másik rendszer információit felhasználni. Az informatikai interoperabilitás tehát nem egy öncélú, önmagáért kialakítandó, hanem magasabbszintű szervezeti szükségletek, képességek megvalósulását biztosító képesség. Az informatikai interoperabilitás a szereplők közötti információs interoperabilitás egyik összetevője, ez utóbbi pedig a szereplők közötti műveleti (szervezeti) interoperabilitás alapvető feltétele.

Az interoperabilitási problémák, hiányosságok megoldatlanul hagyása, vagy nem megfelelő szintű megoldása befolyásolja az érintett rendszerek által támogatott működési folyamatok eredményességét, hatékonyságát, vagy gazdaságosságát, illetve az érintett szereplők együttműködésének hatékonyságát. Informatikai interoperabilitás hiányában egyes tevékenységek egyáltalán nem hajthatóak végre, vagy csak hosszabb idő alatt, több erőforrás felhasználásával, rosszabb eredménnyel, illetve nem, vagy csak alacsonyabb szinten biztosítható a különböző tevékenységek összehangoltsága, egymást erősítő (szinergikus) hatása.

Az információs és ezen belül az informatikai rendszerek közötti interoperabilitás előtérbe kerülésének, növekvő jelentőségének okai az információtechnológia fejlődésében, az informatikai szolgáltatások egyre bővülő mértékű igénybevételében, a világméretű, egyes emberekre és eszközökre is kiterjedő hálózatok elterjedésében, ezzel az emberek, rendszerek és eszközök közötti kapcsolatrendszer volumenének ugrásszerű bővülésében és ehhez kapcsolódóan az információcserében érintett felek, rendszerek heterogenitásának megnövekedésében rejlenek. A heterogén szereplők és rendszerek közötti információcsere ugyanis értelemszerűen növekvő mértékben igényli az interoperabilitási megoldások alkalmazását.

Az informatikai interoperabilitás problémája először a katonai alkalmazásban merült fel. Az angol nyelvű egy értelmező szótára az interoperábilis kifejezés megjelenését 1965–70 közöttre teszi és példaként az 'interoperábilis fegyverrendszerek' kifejezést adja meg.¹ A katonai gyakorlatban a haderőnemek közötti interoperabilitási problémák a kommunikációs rendszerek esetében már a koreai háborúban megjelentek, az informatikai (C4I) rendszerek között elsőként a vietnami háború idején jelentkeztek. Az alapvető ok abban rejlett, hogy az egyes haderőnemek rendszereiket egymástól függetlenül, az összhaderőnemi követelmények figyelmen kívül hagyásával fejlesztették.² Az Egyesült Államok védelmi minisztériuma az informatikai rendszerek interoperabilitása témakörben 1967-ben adta ki az első szabályozót³.

Az informatikai interoperabilitásnak az iraki konfliktus során változatlanul fennálló, sőt a biztonságpolitikai változások és az információtechnológiai fejlődés következtében bővülő problémái jelentős mértékben növelték e kérdéskör jelentőségét. Ennek eredményeként fogalmazta meg az Egyesült Államok hadereje 1992-ben az interoperábilis informatikai rendszerek összekapcsolt rendszerére és az ezt támogató informatikai infrastruktúrára épülő informatika-alkalmazási jövőképét, „*Informatika a harcos számára*” (C4I for the Warrior) címmel.

Az informatikai interoperabilitás a katonai alkalmazásban mindmáig a más alkalmazási területekhez képest kiemelt, sőt egyre fokozódó jelentőséggel bír. Ennek alapvető oka a katonai műveleteket végrehajtó és abban érintett erők különböző területeken és különböző mértékben fennálló, sok szempontból növekvő mértékű heterogenitásában, másrészt az informatikai rendszerek egyre kiterjedtebb alkalmazásában rejlik. A 21. század kezdetét a biztonságpolitikai környezetben, a katonai műveletek jellegében, az ezeket végrehajtó erők

feladataiban és összetételében, illetve a doktrínális elvekben bekövetkező jelentős változások jellemzik.

A NATO hadászati parancsnokok közös jövőképében ⁴ megfogalmazottak szerint korunk katonai műveleteit holisztikus megközelítés, körük (jellegük) kibővülése, összetettségük, más – információs, gazdasági, társadalmi, jogi, diplomáciai stb. – tevékenységekkel fennálló kapcsolatrendszerük megnövekedése, a műveleteket végrehajtó erők összetételének megváltozása és az együttműködési kör kibővülése, a multilaterális jelleg uralkodóvá válása jellemzi. A műveletek összhaderőnemi, többnemzetiségű – szövetségi, vagy az adott feladatra létrehozott, a résztvevő nemzetek eseti felajánlásaira épülő koalíciós – keretekben kerülnek végrehajtásra. Emellett a műveletet végrehajtó csoportosításoknak küldetésük eredményes megvalósítása érdekében egyre szorosabb együttműködést kell kialakítaniuk más – nemzetközi, kormányzati és nem-kormányzati és civil – szervezetekkel is.

A jövőkép alapvető tényezőként hangsúlyozza az információs fölény szerepét és ezen belül a szervezeti eredményességnek az információk, információs folyamatok és információs rendszerek, illetve a korszerű technológia, köztük az informatika által biztosított lehetőségek kiterjedt és hatékony felhasználásától való függőségét. A dokumentumban külön kiemelésre kerül az információk, mindenekelőtt a felderítési információk megsztásának és a közös helyzetismeret kialakításának szerepe, jelentősége. Kiemelt fontosságú összetevő a hálózatközpontú megközelítés és ennek NATO-értelmezés szerinti alapfogalma, a hálózatalapú képesség is, amelynek lényege szervezeti, képesség- és rendszerszinten egyaránt a más összetevőkkel feladatorientált módon történő, egymás képességeit kiegészítő, szinergikus módon felerősítő összekapcsolódás.

Összességében tehát a NATO hadászati jövőképében foglalt megállapítások egy olyan interoperabilitási környezetet körvonalaznak, prognosztizálnak, amelyben a biztonságpolitikai szintér szereplőinek feladatorientált módon változó, összességében dinamikusan bővülő köre számára kell megteremteni az információs és ezen belül az informatikai interoperabilitás feltételeit; az egyes szereplők által kezelt, illetve a köztük kicserélt információk köre folyamatosan bővül, tartalma dinamikusan változik; végül az információk egyre bővülő köre jelenik meg az informatikai rendszerekben és kerül köztük továbbításra.

Az informatikai interoperabilitási politika alapjai

Az információs szintér szereplőinek működését, együttműködését befolyásoló interoperabilitási problémák, kérdések növekvő jelentősége szükségessé teszi, hogy ezek a szereplők megfogalmazzák interoperabilitási céljaikat és követelményeiket; folyamatosan elemezzék, értékeljék az interoperabilitás helyzetét, hatását és következményeit; meghatározzák a megvalósításban érintett személyek és szervezeti elemek körét és felelősségüket; végül megtervezzék és végrehajtsák az interoperabilitás kialakítására, fenntartására, továbbfejlesztésére irányuló feladatokat. Az interoperabilitási kérdésekhez kapcsolódó teendők jelentősége, mennyisége, összetettsége – sok más feladatrendszerhez hasonlóan – egy meghatározott szervezeti szint felett már elengedhetlenné teszi a tevékenységek egységes rendszerben, hosszabb távra szóló, stratégiai szemléletmódban történő kezelését, megvalósítását.

A hosszú távú (stratégiai) tervezés terminológiájának a szakirodalomban több, széles körben elterjedt változata is létezik. Ezek közül jelen tanulmányban a Miniszterelnöki Hivatal által kiadott módszertani útmutató ⁵ fogalomrendszerét alkalmazzuk. Ennek alapfogalma a

stratégia, a célállapot (jövőkép) elérésének átfogó terve, amely helyzetelemzésen alapul, jól definiált célokat tűz ki, ezek eléréséhez eszközöket rendel (beleértve a pénzügyi eszközöket is), valamint rendelkezik a megvalósítás fő intézményeiről, folyamatairól. A stratégia alapjait az adott szakterület politikája (szakpolitika, részpolitika) határozza meg, amely a szakterületre vonatkozó elvek, értékek, trendek és az ezek alapján kialakított átfogó célok, alkalmazható és alkalmazandó eszközök, valamint a szakterületi intézményrendszer összessége. Végül a stratégia megvalósítására programok, akciótervek és intézkedések formájában kerül sor. Míg a különböző stratégiák, rendeltetésükből és terjedelmükből következően általában önálló dokumentumban jelennek meg, addig a szakterületi politikák nem mindig fogalmazódnak meg ilyen formában.

Az informatikai interoperabilitási politika ebben az értelemben egy adott szereplő (szervezet) legfontosabb hosszú távú interoperabilitási céljainak és az elérésükhöz szükséges tevékenységek alapvető irányainak egységes rendszere. Az informatikai interoperabilitási politika rendeltetése, hogy az adott szereplő teljes egészére, egységes szemlélettel fogalmazza meg azt a felsőszintű akaratot és elkötelezettséget, amely hosszabb távra (5–10 évre) meghatározza az interoperabilitáshoz kapcsolódó tevékenységrendszer alapjait. Ez a politika általánosan, a szereplő minden összetevője, személye számára érhető módon rögzíti az interoperabilitás megteremtésével és fenntartásával kapcsolatos, követendő alapelveket. Mindezek képezik az alapját a későbbiekben megfogalmazandó részletes informatikai interoperabilitási célkitűzéseknek és informatikai interoperabilitási stratégiának.

Egy informatikai interoperabilitási politika alapvető összetevői közé tartozhatnak: az informatikai interoperabilitás fogalmi alapjai az adott szereplő értelmezésében; az interoperabilitás szerepének, az alapvető interoperabilitási célkitűzések, szintek és fokozatok meghatározása; az informatikai interoperabilitási tevékenységrendszer alapjainak, szabályozórendszerének általános leírása; az interoperabilitási tevékenységrendszer alapelveinek, valamint az interoperabilitási politika megvalósításában érintett alapvető szerep- és felelősségi körök meghatározása.

Az informatikai interoperabilitási politika egy szakterületi részpolitika, amely jellegéből következően más magasabb szintű, vagy azonos szintű politikákhoz kapcsolódik. Ezek közül kiemelésre méltó az átfogó (szervezeti) interoperabilitási politika, az informatika-alkalmazási politika, az informatikai fejlesztési (és beszerzési) politika, valamint az informatikai biztonsági politika. *Mindezt röviden a következő tények és körülmények indokolják:*

- az informatikai interoperabilitás csak egyik összetevője a szervezeti interoperabilitásnak, követelményeit alapvetően meghatározzák a szervezeti szintű interoperabilitási, együttműködési követelmények;
- az informatikai interoperabilitás követelményeit jelentős mértékben meghatározzák az informatika-alkalmazás jellemzői és sajátosságai, az informatikai rendszerek, eszközök és alkalmazások közötti információcserével kapcsolatos szervezeti igények;
- az interoperabilitási követelményeket alapvetően az új informatikai rendszerek fejlesztése és beszerzése, illetve a meglévő rendszerek továbbfejlesztése során lehet és kell érvényesíteni, összehangolva az alkalmazói és gazdaságossági követelményekkel;
- az informatikai interoperabilitás és az informatikai biztonság követelményei és megvalósítási lehetőségei bizonyos szempontból egymással ellentétesek, de az információcseréhez kapcsolódván egymással szoros kölcsönhatásban is állnak.

Az informatikai interoperabilitás politikai kereteit szabályozó dokumentumok

A interoperabilitás alapvető kereteit a témára vonatkozó NATO, Európai Unió és magyar kormányzati dokumentumok, valamint a felsőszintű, doktrínális szabályozók képezik.

A NATO interoperabilitással kapcsolatos alapvető dokumentumai közé mindenekelőtt a Szövetség hadászati koncepciója, a védelmi képességek kezdeményezés, a prágai képességfejlesztési elkötelezettség, a hadászati parancsnokok jövőképe, valamint a NATO interoperabilitási politika és a NATO C3 interoperabilitási politika tartozik. Az interoperabilitás fogalmát a dokumentumok közül csak a két interoperabilitási politika, illetve a NATO fogalomjegyzék definiálja. Ez utóbbiban a fogalom meghatározása az elmúlt időszakban többször is változott.

1973-tól 2000-ig a fogalomjegyzékben a következő, egy eredetileg technikai jellegű definícióra épülő meghatározás szerepelt: „*rendszerek, egységek és erők képessége arra, hogy szolgáltatásokat nyújtsanak más rendszereknek, egységeknek és erőknek, illetve szolgáltatásokat vegyenek igénybe azoktól oly módon, hogy a szolgáltatások felhasználása elősegítse hatékony együttműködésüket*”⁶. Ezt 2000-ben egy magasabb szintű meghatározás követte, amely szerint az interoperabilitás „*a szövetséges, illetve adott esetben a partner és más országok fegyveres erőinek képessége a hatékony együttes felkészítésre, gyakorlat végrehajtásra és a meghatározott küldetések és feladatok végrehajtása során történő hatékony együttműködésre*”⁷. Az eddigi utolsó változtatásra 2004 júniusában került sor, amely szerint az interoperabilitás „*a meghatározott feladatok végrehajtása során történő szinergikus működésre való képesség*”.⁸

A nemrég megjelent NATO interoperabilitási politikában⁹ már a legfrissebb meghatározás szerepel, a korábban kiadott NATO C3 interoperabilitási politikában¹⁰ viszont még a 2000-es definíció és a NATO híradó és informatikai fogalomjegyzékének¹¹ az 1973-as fogalomra épülő információcsere-orientált szűkítése („*rendszerek képessége arra, hogy információkat nyújtsanak más rendszereknek, illetve információkat fogadjanak azoktól és az így kicserélt információkat hatékony együttműködésüket elősegítésére használják fel*”) található. A két dokumentumban foglaltak azt bizonyítják, hogy a NATO számára már szükségessé vált az átfogó (szervezeti és működési szintű) és a C3 (informatikai) rendszerekre vonatkozó interoperabilitás fogalmának és feladatainak megkülönböztetése, illetve a már korábban létező informatikai interoperabilitási politika mellett egy átfogó interoperabilitási politika kialakítása is.

A NATO 1999-ben elfogadott stratégiai koncepciójában és az azzal egyidőben kiadott védelmi képességek kezdeményezésben az interoperabilitás már kiemelt szerepet kapott. Ezt követően a prágai képességfejlesztési elkötelezettség előkészítéseként a Szövetség védelmi miniszterei az interoperabilitást a négy kiemelt jelentőségű műveleti képesség-terület egyikeként azonosították.¹² A NATO parancsnokok közös hadászati jövőképében¹³ az interoperabilitás szintén jelentős szerepet játszik, mint a katonai műveletek hatásalapú megközelítésének három alapvető összetevője (döntési fölény, koherens hatások elérése, illetve az összhaderőnemi alkalmazás és fenntartás) közül az első kettő megvalósításához szükséges, lényeges feltétel.

A hivatkozott alapidokumentumokban foglaltakkal összhangban a NATO interoperabilitási politika is megállapítja, hogy „*a NATO-műveletek sikere nagymértékben az összhaderőnemi és többnemzetiségű parancsnokságok és erők zökkenőmentes működésén és együttműködésén múlik. Ebben a környezetben az interoperabilitás kulcsfontosságú feltétel és jelentős erősorsorozó tényezőnek kell tekinteni.*”¹⁴ A NATO C3 interoperabilitási politika

bevezetőjében pedig azt fogalmazza meg, hogy „a NATO finanszírozású C3 rendszereknek teljesen interoperábilisnak kell lenniük és együtt kell tudniuk működni a nemzeti rendszerekkel. A tagállamok és partner államok rendszereinek, erőik hatékony együttes működése érdekében szintén együtt kell működniük. Ebből következően a NATO-nak a politikai konzultációtól a harcászati szintű tevékenységeikig terjedő funkciók támogatására jelentősen megnövelt interoperabilitásra van szüksége a NATO C3 rendszer minden szintjén.”¹⁵

Az átfogó, szervezeti szintű interoperabilitással kapcsolatban a NATO interoperabilitási politika alapvetően a különböző vezető szervek (parancsnokságok) és a műveleteket végrehajtó erők közötti interoperabilitás kérdéseire összpontosít, de megfogalmazza a különböző rendszerek és eszközök interoperabilitásának szerepét is.¹⁶ Az informatikai rendszerek közötti interoperabilitásban érintett összetevőket részletesebben a NATO informatikai interoperabilitási direktíva¹⁷ tartalmazza. A dokumentum szerint ezek közé a következők tartoznak: NATO állandó telepítésű parancsnokságok; a NATO parancsnokságokkal együttműködő állandó telepítésű nemzeti parancsnokságok; telepített NATO parancsnokságok és erők; NATO vezetésű műveletekben résztvevő nemzeti erők (egységek); valamint a Szövetséggel együttműködő nem-kormányzati szervezetek.

Az *Európai Unió* interoperabilitással kapcsolatos legfontosabb dokumentuma a pán-európai e-közigazgatási szolgáltatások európai interoperabilitási keretrendszere¹⁸, amelynek alapját a 2005-ben Sevillában elfogadott eEurope akcióterv képezte. A dokumentum szerint az interoperabilitás „*az infokommunikációs (ICT) rendszerek és az általuk támogatott szervezeti (üzleti) folyamatok képessége az adatcserére, valamint az információk és tudás megosztásának támogatására*”¹⁹. Emellett azt is megfogalmazza²⁰, hogy az interoperabilitás kérdéseit három dimenzióban is vizsgálni kell. Ezek közül a szervezeti interoperabilitás tárgya a szervezeti célok és folyamatok összehangolás és a közigazgatási szervek együttműködése. A szemantikai interoperabilitás az egymás között cserélt (nem feltétlenül erre a célra tervezett) információk más alkalmazások általi pontos értelmezésének kérdéseivel kapcsolódik. Végül a technikai interoperabilitás a számítógépes rendszerek és szolgáltatások összekapcsolásának technikai kérdéseivel foglalkozik.

Az európai interoperabilitási keretrendszer a szervezeti szintű interoperabilitás alanyainak alapvető típusait rögzíti. Ezek közé – elsősorban a határokon átnyúló interakció-típusokat azonosítva – a következőket sorolja²¹: az Európai Unió intézményei és hivatalai; a tagállamok közigazgatási intézményei; valamint az állampolgárok, illetve a gazdálkodó szervezetek. A dokumentum az ezen összetevők közötti interoperabilitási kapcsolatokat az A2A (Administration to Administration), A2B (Administration to Business) és A2C (Administration to Citizen) típusokba kategorizálja.²²

A *Magyar Köztársaság* közigazgatást érintő informatikai interoperabilitással kapcsolatos elgondolásai, tervei a Magyar Információs Társadalom Stratégiára²³ és az európai e-közigazgatási folyamatokra épülnek. Az Informatikai és Hírközlési Minisztérium, illetve a Miniszterelnöki Hivatal Elektronikus Kormányzat Központja más minisztériumokkal együttműködve ezen keretek között indított projektet a Magyar E-Közigazgatási Interoperabilitási Keretrendszer (MEKIK) alapjainak lerakására. A projekt keretében elkészült alapvető résztanulmány az interoperabilitás fogalmát egyszerűen együttes (együtt-) működési képességként definiálja, ami önállóan működő hatóságok, szervezetek együttműködését jelenti.²⁴ Az interoperabilitásban érintett összetevők közé ez a dokumentum is a közigazgatási intézményeket, az állampolgárokat (ügyfeleket) és a gazdálkodó szervezeteket sorolja. Az

interoperabilitás szempontjából a projekt a közigazgatáson belüli együttműködésre koncentrált és későbbi kiterjesztés tárgyának tekinti az ügyfelekkel és gazdálkodó szervezetekkel fennálló, valamint a nemzetközi interoperabilitási kapcsolatokat.

A védelmi szférát érintő szabályozók közül a Magyar Köztársaság kül-, biztonság- és védelempolitikai céljaiban ²⁵ nem szerepel az interoperabilitás fogalma, azonban a magyar haderővel kapcsolatban leszögezi, hogy „erősítenie kell együttműködési képességét a környező országokkal, az euro-atlanti integrációs rendszeren belül, illetve azon kívül” és a NATO műveletekben történő részvétel mellett „megfelelő képességekkel kell rendelkeznie az Európai Unió által vezetett ... alkalmi koalíciókban végrehajtott katonai műveletekben való részvételre”. Végül azt is meghatározza, hogy „a magyar haderőnek képesnek kell lennie a polgári hatóságokkal és a lakossággal való együttműködésre az ország határain belül és kívül egyaránt”.

A Magyar Köztársaság nemzeti biztonsági stratégiája szintén nem tartalmazza az interoperabilitás kifejezést, azonban a megvalósítás eszközeinek meghatározása során az interoperabilitást érintő alapvető megállapításokat tartalmaz. ²⁶ Ezek szerint a NATO és az Európai Unió keretében folyó kollektív védelmi, válságkezelő, békefenntartó műveletekben és katasztrófaelhárításban való részvétel érdekében „a honvédségnek rendelkeznie kell ... a szövetséges erőkkel együttműködni képes ... erőkkel”. A dokumentum szerint továbbá „a nemzetbiztonsági szolgálatok és a rendvédelmi szervek – és szükség szerint a fegyveres erők – együttműködése ... nemzeti biztonságunk erősítésének jelentős tartaléka” és „a katasztrófavédelem (polgári védelem, tűzoltóság) erői ... szükség esetén a fegyveres erők kijelölt alakulataival együttműködve védik a lakosság életét és az anyagi javakat”.

A *Magyar Honvédség* doktrinális szabályozói közül az összhaderőnemi doktrína az interoperabilitást csak a híradással és informatikával szemben támasztott követelményként tartalmazza a NATO híradó és informatikai fogalomjegyzékben szereplő meghatározással. ²⁷ Az összhaderőnemi vezetési doktrína az interoperabilitást a vezetéssel szemben támasztott hét követelmény egyikeként kezeli, ami „azt jelenti, hogy a magyar katonai vezetési és irányítási rendszer, illetve főbb elemei, eszközei biztosítják a szövetséges erők vezetési és irányítási rendszeréhez történő illeszkedést, az optimális vezetést” ²⁸. A fogalom jelentését, „együttműködési képesség” megnevezés alatt a *Fogalmak és meghatározások* részben definiálja a NATO fogalomjegyzék 1973-as meghatározásával megegyező tartalommal ²⁹.

Az informatikai interoperabilitás egyes elemei

Az előzőekben megfogalmazottakból következően megállapítható, hogy a Magyar Honvédség rendeltetészerű működéséhez, küldetései és feladatai eredményes és hatékony megvalósításához szükség van az informatikai interoperabilitással kapcsolatos alapelvek, alapvető célok és tevékenységi irányok meghatározására. A magyar honvédelmi informatikai interoperabilitási politika megfogalmazása, bár a katonai informatika-alkalmazás jelenlegi helyzetében nem feltétlenül tűnik aktuálisnak, rendkívüli jelentőséggel bír.

Egy stratégiai szemléletű informatikai interoperabilitási politika elmaradása ahhoz vezethet, hogy a Magyar Honvédség – szükségtelenül – végigjárja ugyanazt az utat, amelyet az informatika-alkalmazásban élenjáró haderők bejártak (és amelynek következményeit viselik): vagyis olyan informatikai rendszereket, eszközöket, szerez be, vagy alakít ki, amelyek egymással és más együttműködő biztonságpolitikai szereplők rendszereivel nem, vagy nem kellő mértékben interoperábilisak.

A Magyar Honvédség informatikai interoperabilitási politikájának minimálisan tartalmaznia kell az interoperabilitással kapcsolatos alapfogalmakat, az alapvető célkitűzéseket és követelményeket, valamint az interoperabilitási tevékenységrendszer alapjait és a kapcsolódó szerepköröket. A továbbiakban ezek közül a jelen tanulmány csak az alapvető megállapításokra vonatkozó javaslatokat fogalmaz meg. A politika lényeges összetevőire vonatkozó, részletesebb elképzelések, javaslatok további kutatások tárgyát kell képezzék.

A Magyar Honvédség informatikai interoperabilitási politikája bevezetőjében célszerűen az alapvető fogalmakat és megállapításokat kell rögzíteni. Ennek során az informatikai interoperabilitás alapjait az átfogó (szervezeti) interoperabilitás keretei között, az együttműködési követelményekre épülve kell megfogalmazni. Ezen megállapítások jelentős részének egy megfogalmazott, kidolgozott, vagy csak részben létező általános interoperabilitási politikából kell származnia, amely kiterjed az interoperabilitás minden formájára és területére (szellemi interoperabilitás, nyelvi interoperabilitás, logisztikai interoperabilitás stb.). Az informatikai interoperabilitási politikában a Magyar Honvédség rendeltetéséből és feladataiból kiindulva elsőként *az együttműködési követelményeket kell meghatározni például a következő formában:*

1. A Magyar Honvédségnek Magyarország és az Észak-atlanti Szövetség fegyveres védelme, a nemzetközi válságkezelésben történő részvétel, a humanitárius segítségnyújtás és a polgári hatóságok támogatása során együtt kell működnie a Magyar Köztársaság és más államok fegyveres erőivel, rendvédelmi és katasztrófavédelmi szerveivel, más kormányzati, nem-kormányzati és civil szervezeteivel.
2. A háborús, béketámogató, válságreakáló, polgári veszélyhelyzet kezelő és humanitárius segítségnyújtó műveletek eredményessége és hatékonysága nagymértékben függ a végrehajtásban érintett erők zökkenőmentes együttműködésének minőségétől.
3. A szervezeti interoperabilitás különböző szervezetek, erők kölcsönös képessége az egymás tevékenységét erősítő, hatékony együttműködésre a meghatározott feladatok végrehajtása során.
4. Napjaink biztonságpolitikai környezetében, amelyet az adott feladatra létrehozott, különböző típusú szervezetek együttműködése, többnemzetiségű erők alkalmazása jellemez, a szervezeti interoperabilitás a kitűzött célok elérésének alapvető feltétele, jelentős erősítő tényezője.
5. Az együttműködő szervezetek interoperabilitásának alapvető összetevője a jelentésmegőrző információcseréi képessége, az információs interoperabilitás, illetve az ennek feltételét képező informatikai interoperabilitás, az informatikai rendszerek és eszközök közötti, a szándékolt jelentést megőrző információ- (adat-) csere képessége.
6. A kibontakozó információs korszakban, amelyben a szervezetek által kezelt információk egyre nagyobb köre kerül informatikai rendszerek, eszközök segítségével tárolásra, feldolgozásra és továbbításra, az informatikai interoperabilitás jelentősége folyamatosan nő.
7. A Magyar Honvédség eredményes és hatékony működése érdekében az informatikai interoperabilitást a honvédség egyes informatikai rendszerei között, és a vele együttműködő szervezetek – a Magyar Köztársaság kormányzati, rendvédelmi, katasztrófavédelmi, védelmi igazgatási szervezetei, a NATO parancsnokságai és erői, a Szövetség és a tagállamok

honvédelmi vezető szervei és erői, a nemzetközi biztonságpolitikai szervezetek, valamint a különböző műveletek végrehajtásában érintett nem-kormányzati és civil szervezetek – informatikai rendszerei között kell biztosítani.

A honvédelmi informatikai interoperabilitási politikának jellegéből következően a Magyar Honvédség vezetésének elképzeléseit kell tükröznie. Ennek megfelelően megvitatására, véleményezésére és az integrált szakmai álláspont kialakítására a jelenlegi szervezeti rendben a HM Informatikai és Hírközlési Alkalmazási Bizottság jogosult. Az informatikai interoperabilitási politika – mint a tárcaszintű (honvédelmi) informatikai stratégia egyik összetevőjének, háttéranyagának – kidolgozását a HM Tervező és Koordinációs Főosztály Informatikai Osztály által vezetett, létrehozott kidolgozó-csoportnak kell megvalósítania. Végül a honvédelmi informatikai interoperabilitási politika kellő hatékonysággal csak akkor érvényesül, amennyiben megfelelő szintű és hatályú szabályozóban kerül megfogalmazásra. Ennek megválasztása az illetékes HM szervek feladata.

Összegzésképpen még egyszer szükséges megfogalmazni, hogy a honvédelmi informatikai interoperabilitási politika kialakítása, elfogadása és érvényesülésének biztosítása az információs korszak kibontakozása, az informatika-alkalmazás szerepének és jelentőségének folyamatos bővülése, a biztonságpolitikai környezet változásai, a NATO transzformációs elképzelései, valamint az Európai Unió és kormányzati célkitűzések által megkövetelt, időszerű feladat, amelynek elmaradása, vagy késedelme a honvédelem küldetési és feladatai megvalósulásának eredményességét, hatékonyságát csökkenti.

FELHASZNÁLT IRODALOM

AAP-6(V), NATO Glossary of Terms and Definitions. – NATO Military Agency for Standardization, 1998.

AAP-6(V) mod 2, NATO Glossary of Terms and Definitions. – NATO Military Agency for Standardization, 2000.

AAP-6(2005), NATO Glossary of Terms and Definitions. – NATO Standardization Agency, 2005.

AAP-31(A), NATO Glossary of Communication and Information Systems Terms and Definitions. – NATO Standardization Agency, 2001. november.

DoD Directive 4630.5. Compatibility and Interoperability of Tactical Command, Control, Communications and Intelligence (C3I) Systems. – US Department of Defense, 1967.

European Interoperability Framework for Pan-European eGovernment Services. Version 1.0 – European Communities, 2004.

Interoperability, DoD Efforts to Achieve Interoperability among C3 Systems. (Report to the House of Representatives) – US General Accounting Office, 1987.

Közigazgatási informatikai rendszerek együttműködéséhez szükséges adatmodellek és adatkommunikációs sémák specifikációja és az ehhez szükséges módszertan (Tervezet, 4.2 verzió). – IDOM 2000 Konzulens Rt., 2004. október.

A Magyar Honvédség Összhaderőnemi Doktrínája. – HM HVK Hadművelési csoportfőnökség, 2002.

A Magyar Honvédség Összhaderőnemi Vezetési Doktrínája (Tervezet). – HM HVK Vezetési csoportfőnökség, 2003. április.

Magyar Információs Társadalom Stratégia. – Informatikai és Hírközlési Minisztérium, 2003. november.

A Magyar Köztársaság kül-, biztonság- és védelempolitikai céljai. – 2002. szeptember 16.

A Magyar Köztársaság nemzeti biztonsági stratégiája. (2073/2004. Korm. határozat) – 2004. április 27.

Módszertani útmutató a kormányzati stratégiai tervezéshez. – Miniszterelnöki Hivatal, Budapest, 2004.

NATO C3 System Interoperability Policy. – NATO C3 Board, 2004.

NATO C3 System Interoperability Directive (Version 2). – NATO C3 Board, 2004.

NATO C3 Technical Architecture. Volume 1–5. Version 1.0, 2.0 – ISSC NATO Open Systems Working Group, 1999. július 30., 2000. december 15.

ADatP–34, NATO C3 Technical Architecture. Volume 1–5. Version 3.0, 4.0, 5.1, 6.0 – ISSC NATO Open Systems Working Group, 2001. december 15., 2002. december 16., 2004. március 3., 2004. szeptember 30.

NATO Policy for Interoperability. – NATO Committee for Standardization, 2004. december 14.

The Prague Summit and NATO's Transformation. A Reader's Guide. – NATO, 2003.

Strategic Vision: The Military Challenge (by NATO Strategic Commanders). – Allied Command Transformation – Allied Command Operations, 2004.

Webster's Encyclopedic Unabridged Dictionary of the English Language. – Gramercy Books, New York, 1996.

1 Webster's Encyclopedic Unabridged Dictionary of the English Language: capable of being used or operated reciprocally. [« vissza](#)

2 Interoperability, DoD Efforts to Achieve Interoperability among C3 Systems. [8–9. o.] [« vissza](#)

3 DoD Directive 4630.5, Compatibility and Interoperability of Tactical Command, Control, Communications and Intelligence (C3I) Systems. [« vissza](#)

4 Strategic Vision: The Military Challenge (By NATO Strategic Commanders). [« vissza](#)

5 Módszertani útmutató a kormányzati stratégiai tervezéshez. – Miniszterelnöki Hivatal, 2004. [« vissza](#)

6 AAP–6(V) mod 1, NATO Glossary of Terms and Definitions [2–I–7. o.]. [« vissza](#)

7 AAP–6(V) mod 2, NATO Glossary of Terms and Definitions [2–I–6. o.]. [« vissza](#)

8 AAP–6(2005), NATO Glossary of Terms and Definitions [2–I–6. o.]. [« vissza](#)

9 NATO Policy for Interoperability [1. pont] [« vissza](#)

10 NATO Policy for C3 Systems Interoperability [2.1 pont] [« vissza](#)

11 AAP–31(A), NATO Glossary of CIS Terms and Definitions [systems interoperability, 2–35. o.] [« vissza](#)

12 The Prague Summit and NATO's Transformation. A Readers Guide. 2003. [27. o.] [« vissza](#)

13 Strategic Vision: The Military Challenge (By NATO Strategic Commanders). – NATO, 2004. [« vissza](#)

14 NATO Policy for Interoperability. [2. pont] [« vissza](#)

15 NATO C3 System Interoperability Policy. [1.1.2 pont] [« vissza](#)

16 NATO Policy for Interoperability [9. pont] [« vissza](#)

17 NATO C3 System Interoperability Directive [7. fejezet] [« vissza](#)

18 European Interoperability Framework for Pan–European eGovernment Services. Version 1.0. – European Communities, 2004. [« vissza](#)

19 i.m. [1.1.2 pont, 3. o.] [« vissza](#)

20 i.m. [2.2.1 pont, 15. o.] [« vissza](#)

21 i.m. [2.1.1 pont] [« vissza](#)

22 Más megnevezéssel G2G, G2B, G2C (ahol a G = Government). [« vissza](#)

23 Magyar Információs Társadalom Stratégia. – Informatikai és Hírközlési Minisztérium, 2003. november. [« vissza](#)

24 Közigazgatási informatikai rendszerek együttműködéséhez szükséges adatmodellek és adatkommunikációs sémák specifikációja és az ehhez szükséges módszertan [11. o., 16. o.]. [« vissza](#)

25 A Magyar Köztársaság kül-, biztonság- és védelempolitikai céljai. [« vissza](#)

26 2073/2004. Korm. határozat, A Magyar Köztársaság nemzeti biztonsági stratégiája [IV. fejezet]. [« vissza](#)

27 A Magyar Honvédség Összhaderőnemi Doktrínája [1103. pont, 87. o.]. [« vissza](#)

28 A Magyar Honvédség Összhaderőnemi Vezetési Doktrínája [1036. pont, 16. o.]. [« vissza](#)

29 i.m. [62. o.] [« vissza](#)

[« 2006/1-2. Tartalom](#)