Munk Sándor

Az információs mûveletek típusai és modelljei

Csak információs támadás és védelem?

A katonai mûveletekre alapvetõen jellemzõ konfliktushelyzetekben az információs fölény kikvívása és fenntartása érdekében információs tevékenységeket, mûveleteket kell végrehajtani, amelyek négy alapvetõ csoportját a saját képességek növelésére irányuló támogató mûveletek és az azok megóvására irányuló védelmi mûveletek; a szembenálló felek képességeinek csökkentésére irányuló támadó mûveletek; valamint a környezet saját szempontból kedvezõ befolyásolására irányuló véleményformáló mûveletek képezik. A szerzõ az információs fölénnyel összefüggõ alapelveket és azok fontosabb jellemzõit egy korábban megjelent cikkében (a Hadtudomány 2001. évi 3. szám) vázolta.

A katonai mûveletek eredményességét jelentõs mértékben befolyásoló, az alapvetõ katonai képességeket megalapozó, támogató és erõsítõ információs fölény, illetve az ennek kivívására irányuló információs hadviselés fogalma elõször 1992 decemberében jelent meg az Egyesült Államok Védelmi Minisztériumának egy szigorúan titkos utasításában, majd ezt 1995 szeptemberében követte az információs hadviselés elsõ nyílt minõsítésû meghatározása[1]:

„Az információs fölény kivívása a szemben álló fél információi, információs folyamatai és információs rendszerei befolyásolására, illetve a saját információk, információs folyamatok és információs rendszerek védelmére irányuló tevékenységek összessége."

Bár egy, már 1994-ben megjelent tudományos jelentés is felhívta a figyelmet az információs fölény kivívását szolgáló más jellegû tevékenységek létére és jelentõségére[2], a hazai és nemzetközi tudományos kutatás az eddigiekben elsõsorban a hagyományos és mai felfogású támadó és védelmi jellegû összetevõkre, eljárásokra és eszközökre irányult. Lényegesen kevesebb figyelem összpontosult az információs fölény saját információs képességek növelésével, illetve a meglévõ képességek hatékonyabb kihasználásával történõ biztosításának vizsgálatára. Többek között e szûk értelmezés bõvítése érdekében jelent meg az Egyesült Államok szárazföldi haderejének 1996-ban kiadott szabályzatában[3], majd terjedt el késõbb az információs mûveletek fogalma.

A katonai alkalmazás szempontjából e témakörben megítélésünk szerint – bár a hadtudományi szakirodalomban találkozhatunk a tudásfölény, vezetési fölény kifejezésekkel is – az információs fölény fogalma képezi a súlypontot. Az informatikai alkalmazások, illetve az ezekben megtestesülõ tudásösszetevõk általános rendeltetése a vezetés és mûködés támogatása, amely a 21. századi katonai mûveletek esetében mindenekelõtt az információs fölény kivívásához történõ hozzájárulásuk révén realizálódik.

A fentiekben megfogalmazottaknak megfelelõen jelen publikációban annak a vizsgálatára kerül sor, hogy milyen mûveletek, tevékenységek megvalósításával érhetõ el az információs (tudás-, vezetési) fölény? Mindezekre azért is szükség van, mert ezen kérdéskörök, illetve ezek egyes összetevõi megítélésében a nemzetközi szakirodalom nem egységes és a kapcsolódó magyar hadtudományi publikációk köre is rendkívül szûkös.

Az információs mûveletek típusai

A kitûzött célok elérését elõsegítõ információs fölény[4] kialakítása és fenntartása a dinamikusan változó környezetben aktív tevékenységeket is igényel, ennek megfelelõen az információs fölénnyel párhuzamosan

találkozhatunk az információs mûveletek (information operations) és az információs hadviselés (information warfare) összetartozó kifejezéseivel és azok definícióival:

„ Az információs mûveletek a döntéshozókat befolyásoló, politikai és katonai célkitûzések megvalósítását támogató tevékenységek, amelyek más felek információi, információs folyamatai, vezetési (C2), híradó és informatikai (CIS) rendszerei befolyásolására, ugyanakkor a saját információk és információs rendszerek felhasználására és védelmére irányulnak." [NATO, 2001][5]

„Az információs mûveletek a szemben álló fél információi és információs rendszerei befolyásolására, illetve a saját információk és információs rendszerek védelmére irányuló tevékenységek." [USA Egyesített Vezérkar, 2000][6]

„Az információs mûveletek a katonai információs környezetben végrehajtott folyamatos (had)mûveletek, amelyek a (had)mûveletek bármely fajtájában történõ elõnyszerzés érdekében biztosítják, növelik és védik a *saját erõk képességét az információk gyûjtésére, feldolgozására és felhasználására;* az információs mûveletek magukban foglalják a globális információs környezettel kapcsolatos tevékenységeket, valamint a szemben álló fél *információs és döntési képességei*[7] kihasználását, vagy korlátozását." [USA Szárazföldi Haderõ, 1996][8]

„Az információs mûveletek az információk és információs rendszerek felhasználására, védelmére vagy támadására irányuló tevékenységek, amelyek magukban foglalják a hadmûveleti információfeldolgozást (information–in-warfare) és az információs hadviselést is." [USA Légierõ, 1998][9]

„Az információs hadviselés a válsághelyzetben és konfliktusok során végrehajtott, szemben álló fél vagy felek elleni konkrét célok elérését biztosító vagy támogató információs mûveletek összessége." [USA Egyesített Vezérkar, 2000][10]

„Az információs hadviselés az információs fölény elérése érdekében végrehajtott, a szemben álló fél információi, információalapú folyamatai, információs rendszerei és számítógépes hálózatai befolyásolására, illetve a saját információk, információalapú folyamatok, információs rendszerek és számítógépes hálózatok védelmére irányuló tevékenységek összessége." [USA Szárazföldi Haderõ, 1996][11]

„Az információs hadviselés a saját információs rendszer integritásának, jogtalan felhasználás, rongálás és megsemmisítés elleni védelmére, ugyanakkor a szemben álló fél információs rendszere felhasználására, rongálására és megsemmisítésére, valamint az erõk alkalmazása során információs elõnyök elérésére irányuló tevékenységek összessége." [USA Szárazföldi Haderõ, 1995][12]

„Az információs hadviselés a saját információk és információs rendszerek védelmére, illetve a szemben álló fél információi és információs rendszerei támadására és befolyásolására végrehajtott információs mûveletek összessége." [USA Légierõ, 1998][13]

Bár az itt ismertetett egyes definíciókban még elõfordul eltérés az információs mûveletek és az információs hadviselés fogalmai közötti viszony értelmezésében, mára már viszonylag egységesen elfogadott az a nézet, hogy *az információs mûvelet a tágabb és az információs hadviselés a szûkebb fogalom.* Ezzel egyetértve jelen kutatás is arra az értelmezésre épít, hogy – a késõbbiekben részletesebben tárgyalt – információs mûveletek a (had)mûveletek minden fajtájában és minden idõszakban (békében, válság, illetve konfliktus idején) folynak, míg az információs hadviselés mûveletei tulajdonképpen csak a két utóbbiban (válság illetve konfliktus esetén).

Az információs fölény elérését biztosító tevékenységek, mûveletek rendszerezésével a szakirodalomban számos helyen és eltérõ tartalommal találkozhatunk. Ezek közé tartoznak többek között az alábbiak:

„Az információs fölény három forrása:

- a vezetés, amely lehetõvé teszi, hogy tudjuk: hol vagyunk a harci térben és képessé tesz a (had)mûveletek szükséges idõben és gyorsasággal történõ végrehajtására;
- a felderítés, amely az ellenség elhelyezkedésének ismeretétõl az ellenséges erõforrások helyének ismeretéig terjed – valósidõben és az „egy lövéssel történõ megsemmisítéshez" szükséges pontossággal;

- az információs hadviselés, amely különbözõ pontokon (szenzorok, kommunikáció, feldolgozás és vezetés) pusztítja az ellenséges információs rendszereket, ugyanakkor védi a saját hasonló rendszereket." [USA Nemzetvédelmi Egyetem, 1997][14]

„Az információs fölény a felderítésben, a vezetésben, a híradásban és az informatikában (C4) elért fölény, amely az információs mûveletek segítségével érhetõ el." [USA Egyesített Vezérkar, 2000][15]

„A vezetési hadviselés definíciójában megtalálható két alapvetõ összetevõ (C2–támadás és C2–védelem) mellett egy harmadik kategóriát alkot az információs technológia integrálása a fegyverrendszerekbe, azok »okossá«[16] tétele. Így a három összetevõ megnevezése információs támadás, információs védelem és információs fejlesztés (information-attack, protect és enhance)." … „Az információs fejlesztés célja, hogy pontos és átfogó képet biztosítson a parancsnok számára a harci térrõl, elõsegítse a környezet értelmezését." [Gortler, 1995][17]

„Az információs hadviselésnek ki kell terjednie egy adott félnek az aktuális, vagy potenciális ellenfelekkel szembeni »versengése« három, egymással nagymértékben összefüggõ szférájára:

- a szemben álló fél (felek) döntéshozatali struktúrái és folyamatai elleni támadó tevékenységekre;
- a saját döntések meghozatalát és hatását biztosító képességek védelmére;
- az információk saját célok érdekében történõ létrehozásának és felhasználásának a szemben álló félnél (feleknél) nagyobb hatékonyságára." [RAND Corporation, 1997][18]

Az ismertetett definíciókkal és megállapításokkal részben megegyezõen, részben egyesekkel ellentétben az információs fölény kialakításának és növelésének négy alapvetõ, formális logikai úton is levezethetõ lehetõsége megítélésünk szerint a következõ:

- a saját információs képesség növelése, optimális kihasználása;
- a saját információs képesség káros külsõ hatások elleni védelme;
- a szemben álló fél információs képességének csökkentése, korlátozása;
- illetve a további szereplõk saját fél számára kedvezõ befolyásolása.

Ezt a felosztást szemlélteti az *információs mûveletek modellje*[19], amelyet a alábbi ábra tartalmaz.

A felsorolt összetevõk közül az elsõ és utolsó tevékenységcsoport önálló létezése, szerepének megítélése és megnevezése a szakirodalomban korántsem egyértelmû, a két középsõ tartalmában és megnevezésében azonban a szakirodalom gyakorlatilag egységes álláspontot képvisel:

„A támadó információs mûveletek (offensive information operations) alárendelt és támogató képességek és tevékenységek integrált, a felderítéssel egymást kölcsönösen támogató alkalmazása a szemben álló fél döntéshozói befolyásolására meghatározott célok elérése vagy elõsegítése érdekében. Összetevõi közé tartoznak többek között a hadmûveleti biztonság, a megtévesztés, a lélektani mûveletek, az elektronikus hadviselés, a fizikai megsemmisítés, a speciális információs mûveletek és magában foglalhatja a számítógép-hálózati támadásokat." [USA Egyesített Vezérkar, 2000][20]

„A védelmi információs mûveletek (defensive information operations), eljárások, mûveletek, a személyzet és technológia integrációja és koordinációja az információk és információs rendszerek védelmére. E mûveletek az információs védelem (information assurance), a fizikai védelem, a hadmûveleti biztonság, a megtévesztés és a lélektani mûveletek elleni tevékenység, az ellenfelderítés, továbbá az elektronikai hadviselés és a speciális információs mûveletek megvalósításával kerülnek végrehajtásra." [USA Egyesített Vezérkar, 2000][21]

A két további összetevõ közül az információs színtér szereplõinek a saját fél számára kedvezõ irányban történõ befolyásolásához általában a (tömeg)tájékoztatási, illetve civil–katonai kapcsolatokhoz tartozó tevékenységeket sorolják, míg a saját információs képességek növeléséhez kapcsolódó tevékenységcsoport meghatározását önálló megnevezéssel a szakirodalom csak a következõ formákban tartalmazza:

- „A »hadmûveleti információfeldolgozás« (information-in-warfare) a légierõnek a katonai mûveletek minden fajtájában biztosítandó globális helyzetismeretére irányuló – integrált felderítõ, megfigyelõ (ISR) erõforrásaira; információgyûjtõ és elosztó tevékenységeire; valamint globális navigációs és

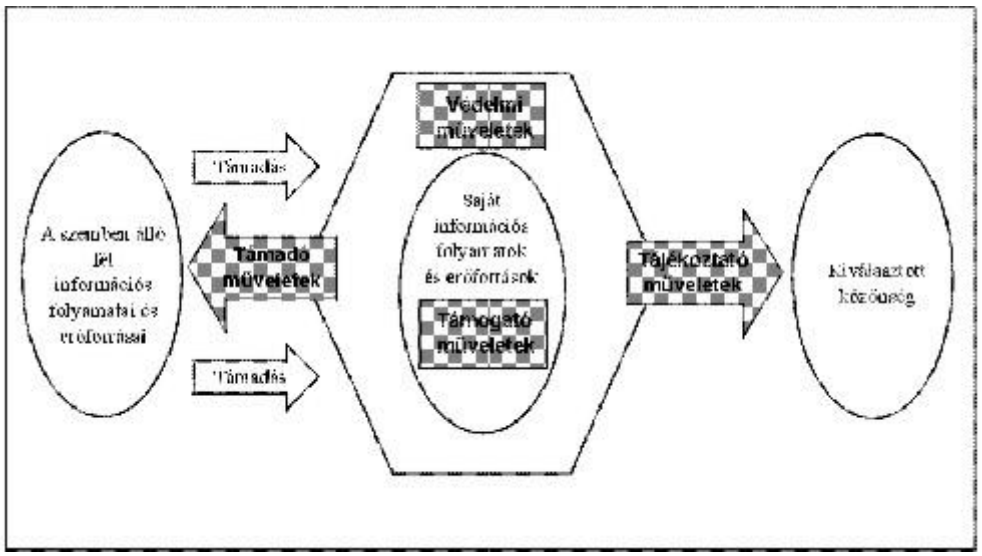
helymeghatározó, idõjárási helyzetnyilvántartó és kommunikációs lehetõségeire alapozott – kiterjedt képességeit foglalja magában.” [USA Légierõ, 1998][22]

- „Az információalapú hadviselés (information-based warfare) rendeltetése a katonai célkitûzések elérésének támogatása az információs erõforrások leghatékonyabb alkalmazásával.” [USA Nemzetvédelmi Egyetem, 1998][23]

A fenti megállapításokat elemezve látható, hogy az információs fölény elérését biztosító tevékenység alapvetõ összetevõi közé az információgyûjtõ, feldolgozó és elosztó tevékenységek tartoznak, amelyeket más – a korábbiakban már bemutatott – megfogalmazások a felderítés és a vezetés (vezetéstámogatás) vagy a „releváns információk és információs rendszerek” formájában próbáltak meghatározni. E tevékenységrendszer megnevezésére – a jellegzetesen válság- és konfliktushelyzetekben alkalmazott „hadviselés” utótagú kifejezés helyett – megítélésünk szerint a támogató információs mûveletek kifejezés bevezetése célszerû.

Az információs fölényt biztosító mûveleteknek ki kell terjedniük a teljes kognitív folyamatra, amelynek során a rendelkezésre álló információk és információs képességek hozzájárulnak a hatékony döntések meghozatalához. Ennek során el kell különíteni e folyamat korábban már említett szintjeit: az információkat, az ismeretet és a megértést. Valaki ugyanis rendelkezhet információkkal valamirõl anélkül, hogy azt összességében vagy részleteiben ismerné és ismerhet valamit (akár nagyon jól is) anélkül, hogy értené annak lényegét vagy következményeit: különösen annak a konkrét körülményekkel kapcsolatos kölcsönhatásait. Nem ugyanaz sokat tudni valamirõl és (meg)érteni azt.

Az információs mûveletek bonyolultságát fokozza az a – korunkat jellemzõ aszimmetrikus veszélyeztetésekbõl következõ – tény, hogy egy fejlett hadseregnek képesnek kell lennie a szemben álló felek esetleg sokkal fejletlenebb információs (döntéshozatali) struktúráinak és képességeinek támadására, ugyanakkor a saját fejlett képességeinek és infrastruktúrájának védelmére a viszonylag egyszerû, de jelentõs károkat okozni képes fenyegetésekkel szemben.[24]



A támadó és a védelmi információs mûveletek bonyolultságát számos ellentmondás is növeli, amelyek feloldása nem egyszerû feladat. A támadó mûveletek esetében például dönteni kell aközött, hogy egyes ellenséges vagy semleges információforrásokat kihasználni érdemes, vagy megsemmisíteni, akadályozni. A védelmi tevékenységek esetében talán még nagyobb ellentmondás: itt kényelmes és hatékony használat áll szemben a sebezhetõséggel és a védelem magasabb „költségével”.

Nem kevésbé bonyolult a saját információfeldolgozási és döntéshozatali struktúrák és folyamatok relatíve nagyobb hatékonyságának biztosítása. Még ha el is tekintünk az egymás információs képességei elleni közvetlen támadásoktól, e képességeknek az idõbeni, eredményes döntések meghozatalához történõ hatékony felhasználása akkor is nagyon bonyolult probléma.[25] E feladat megoldása elsõdlegesen tudományos kihívás és csak másodsorban technikai probléma. A katonai mûveletek vezetése (de általában a vezetés) olyan (szak)tudásigényes folyamat, amelynek hatékony támogatását, az e téren elérhetõ fölény kivívását elsõsorban

tudásalapú – bár természetesen a rendelkezésre álló technikai lehetõségeket optimális mértékben kihasználó – megoldásokkal, módszerekkel lehet biztosítani.

Az elmondottak alapján az információs fölény elérését biztosító alapvetõ tevékenységi formákat a következõkben az alábbi tartalommal definiáljuk és használjuk:

Az információs mûveletek a katonai információs környezetben végrehajtott, az információs fölény kialakítására és fenntartására irányuló mûveletek, amelyek a saját információs képességek optimális kihasználására és védelmére; a szemben álló felek információs képességeinek korlátozására, valamint az információs környezet saját fél számára kedvezõ befolyásolására irányuló tevékenységeket foglalnak magukban.

A támogató információs mûveletek olyan információs mûveletek, amelyek a saját fél információszükségletei kielégítésére irányulnak.

A védelmi információs mûveletek olyan információs mûveletek, amelyek a saját fél információi, információs folyamatai és erõforrásai káros külsõ behatások elleni védelmére irányulnak.

A támadó információs mûveletek olyan információs mûveletek, amelyek a szemben álló fél (felek) információi, információs folyamatai és erõforrásai megsemmisítésére, akadályozására vagy befolyásolására irányulnak.

A véleményformáló információs mûveletek olyan információs mûveletek, amelyek az információs környezet (had)mûveletben közvetlenül nem érintett szereplõinek a saját fél számára kedvezõ befolyásolására irányulnak.

Támogató információs mûveletek és informatikai alkalmazások

A szakirodalomban a saját információs képességek növelésére irányuló tevékenységekkel kapcsolatban eddig gyakorlatilag nem merült fel a „mûvelet" kifejezés alkalmazása. Az ide sorolható felderítõ feladatok esetében már elfogadott ugyan a „felderítõ mûveletek" kifejezés használata[26], ezek hatóköre azonban csak az „idegen nemzetekre, ellenséges vagy potenciálisan ellenséges erõkre és elemekre, valamint az aktuális, vagy lehetséges mûveletek területeire vonatkozó információk"-ra[27] terjed ki, amelyek csak egy részét alkotják a katonai vezetés, a katonai mûveletek információszükségleteinek. Ezzel szemben eddig nem tekintették „mûveleteknek" a saját és együttmûködõ felekre vonatkozó információk összegyûjtésére, illetve a szükséges információk elõállítására és továbbítására irányuló vezetéstámogató – informatikai és híradó – tevékenységek rendszerét.

A katonai mûveleteket napjainkban még sok tekintetben az információs – ezen belül mindenekelõtt a vezetési és vezetéstámogatási – tevékenységek, folyamatok elõre meghatározott és szabályozott, lényegében a hierarchikus vezetési struktúrához illeszkedõ, alapvetõen az adott tartalmú harci okmányok továbbítására épülõ rendje jellemzi. Ezt a rendszert csak kisebb mértékben egészítik ki, illesztik az aktuális helyzethez, szervezethez és feladathoz például az összekötõ csoportok (személyek) tevékenységei és a rajtuk keresztül áramló információk.

A katonai mûveletek e hagyományos információs rendszerében csak a kiemelt jelentõséggel bíró információk áramlanak térben és idõben viszonylag szabadon; jutnak el rövid idõ alatt mindazon helyekre, ahol felhasználásuk szükséges és lényeges mértékben hozzájárul a mûvelet sikeréhez. Az úgynevezett rutininformációk ezzel szemben csak az információáramlás elõre szabályozott rendjében mozognak, és általában akkor is csak azokra a helyekre, amelyeket a harci okmányok tervezett elosztási rendje elõre meghatároz. Emellett az egyes információk kiemelt jelentõségének azonosítása sincs minden esetben biztosítva, hiszen ezt a jelenlegi rendszerben elõzetesen a különbözõ szabályozók, egy adott aktuális helyzetben pedig – a vezetési folyamat egy adott fázisában – a parancsnok által meghatározott információs követelmények determinálják. Ez a rendszer tehát nem biztosítja kellõ rugalmassággal a hozzáférés lehetõségét a helyzettõl függõen fontossá váló és a szervezeten belül valahol már rendelkezésre álló információkhoz.

Az információs képességek optimális kihasználására irányuló tevékenységrendszer formálisan nem illeszkedik ugyan a (had)mûvelet kifejezés jelenleg elfogadott értelmezéséhez[28], de a közeljövõ, illetve a késõbbi idõszak katonai mûveletei esetében már lényegében alig fog különbözni a definícióban konkrétan említett más tevékenységi területektõl. Az információs korszak hadseregei esetében ugyanis a mûveleteket végrehajtó – jellemzõen többnemzetiségû, különbözõ haderõnemekhez tartozó és nem katonai – együttmûködõ szervezetek (szervezeti elemek) rendelkezésére álló információk, információs erõforrások és képességek már oly mértékben

lesznek heterogének, hogy ezek összehangolása, összehangolt felhasználása sokrétû és nagyszámú, elõzetesen megtervezhetõ és helyzetfüggõ információs tevékenység végrehajtását fogja igényli.

Ma – amikor valójában kevés haderõ rendelkezik kiterjedt információs képességekkel – e tevékenység szerepe viszonylag még csekély, de már korunk mûveleteiben is érzékelhetõ a terület jelentõségének növekedése és egyre jobban kirajzolódnak jövõbeni szerepének körvonalai. A katonai mûveletet végrehajtó csoportosítások, valamint az azokat létrehozó szereplõk rendelkezésére álló információk és információs képességek a 21. századi hadviselésben, illetve mûveletekben már olyan döntõ jelentõségû erõforrást képviselnek, amelynek optimális hasznosítása csak szervezeti szintû információkezelés – információmenedzsment, információgazdálkodás – esetén lehetséges.

A támogató információs mûveletek rendeltetésének, alapvetõ feladatainak és sajátosságainak meghatározása, végrehajtási rendjének és eljárásainak kialakítása a hadtudományi, ezen belül a katonai informatikai kutatás elõtt álló olyan bonyolult és nagy volumenû feladat, amelynek megvalósítása kívül esik e konkrét kutatómunka céljain és értelemszerûen meghaladja ennek lehetõségeit. Ennek megfelelõen a következõkben kizárólag a támogató információs mûveletek alapvetõ céljaira támaszkodva elemezzük az informatikai alkalmazások és azok tudásösszetevõinek ehhez kapcsolódó szerepét.

Az informatikai alkalmazások az információs mûveletek minden fajtájában lényeges – természetesen típustól függõ – szerepet játszanak, de mindenekelõtt a saját információs képességek növelésének alapvetõ, egyre növekvõ jelentõségû eszközei. Az emberi tényezõk, a mûveletekben részt vevõ katonai vezetõk és szakemberek szaktudása és tapasztalatai mellett az informatikai alkalmazások formájában megtestesülõ információk és más tudásösszetevõk alkotják ugyanis a információs képességek egyik legfontosabb összetevõjét. E képességek növelése és ezzel az információs fölény kivívása informatikai alkalmazások nélkül ma már gyakorlatilag elképzelhetetlen.

Az informatikai alkalmazások a katonai mûveleteket végrehajtó csoportosítások, szervezetek vezetését és mûködését az információs folyamatok egyes tevékenységeinek támogatásával vagy automatizált megvalósításával segítik; az információs fölény megteremtését és fenntartását elsõsorban a hozzáférhetõ információk körének és minõségének bõvítésével, valamint az információs tevékenységek hatékonyabb megvalósításával, többek között a jövõre vonatkozó jobb minõségû elõrejelzések és tervek hatékonyabb, gyorsabb kialakításának támogatásával biztosítják.

A „hagyományos" katonai informatikai támogatás alapvetõen három pillérre – a funkcionális (szakterületi) informatikai alkalmazásokra; az általános célú, törzsmunkát támogató (irodaautomatizálási) alkalmazásokra; valamint az ezek hátterét és alapját képezõ informatikai infrastruktúrára – *épült és épül még napjainkban is.* Az egyes funkcionális informatikai alkalmazások napjainkban egy adott szakterület alapvetõ információs folyamatainak, tevékenységeinek támogatása érdekében – egy vagy több vezetési szintre kiterjedõ – információs rendszerek részeként, egyre növekvõ mértékben más információs rendszerekkel (szakterületi vagy általános célú), alkalmazásokkal együttmûködve nyújtják szolgáltatásaikat.

A katonai mûveletek hatékony támogatásához, az információs fölény megszerzéséhez és fenntartásához tehát az emberek és informatikai összetevõk között az adott feladathoz és helyzethez illeszkedõ, rugalmas – a nyers alapadatoktól a magas fokon szintetizált tudásösszetevõkig terjedõ – információáramlásra van szükség. A katonai mûveleteket ezzel szemben ma még általában egyedi – többségükben önálló vagy más rendszerekkel statikus módon „összehuzalozott" – informatikai rendszerek és alkalmazások, valamint ilyeneket használó, nagy létszámú törzsek és ennek következtében kötött, rugalmatlan információáramlások jellemzik.

Az egyes funkcionális információs rendszerek (alrendszerek), illetve az ezek részét képezõ, viszonylagos önállósággal rendelkezõ informatikai alkalmazások közötti kapcsolatokat – még egy adott állam haderején, sõt annak egyes haderõnemein belül szintén – ma is nagyrészt a kezelt, felhasznált információkkal kapcsolatos, kisebb-nagyobb fogalmi eltérések és ebbõl következõen a tartalmi interoperabilitás[29] hiánya, vagy alacsony szintje jellemzi. Az informatikai rendszerek, alkalmazások közötti interoperabilitás biztosításának napjainkban alapvetõnek tartott feltételei közé tartozik az alkalmazott fogalomrendszerek (ontológiák) összehangolására alapozott egységes adatmodellek, szabványos adatok, valamint az ilyen adatokat hordozó szabványos üzenetformátumok használata.

Az informatikai alkallmazások közötti tartalmi interoperabilitás a NATO C3 interoperabilitási elvei szerint[30] funkcionálisan négy formában, négy szinten valósulhat meg:

- *strukturálatlan adatok* (csak ember által értelmezhetõ) *cseréje* (pl. kötetlen szöveg);
- *strukturált adatok cseréje* manuális és/vagy manuális elemeket (pl. összeállítás, fogadás vagy elosztás) is tartalmazó automatizált adatkezelés segítségével;
- *automatizált adatmegosztás* (pl. adatreplikáció);
- *valódi információmegosztás,* az információ univerzális értelmezésének megteremtése kooperatív alkalmazások segítségével.

A legmagasabb szintû interoperabilitás feltétele tehát a közös, illetve az együttmûködés érdekében kialakított és egyeztetett fogalomrendszer megléte.

A katonai mûveletek során felhasznált informatikai alkalmazások (alkalmazáskomponensek) közötti tartalmi interoperabilitási adatok és üzenetformátumok elõzetes szabványosításával történõ biztosításának jelenlegi módszere a tapasztalatok szerint több szempontból sem alkalmas e cél megfelelõ szintû elérésére. Megítélésem szerint – két legfontosabb ok egyike magában a szabványosítás lehetséges módszerében, a másik az információs színtéren bekövetkezõ változásban rejlik.

A szabványosítási folyamat – jellegébõl következõen – idõben viszonylag hoszszadalmas, a szabványok egyes összetevõinek kialakításához és elfogadásához szükséges idõ az alkalmazási terület kiterjedésétõl, illetve az alkalmazásban érintett szereplõk számától jelentõs mértékben függ, ezek növekedésével együtt a lineárist meghaladó mértékben nõ. A szabványosítás eredményei a hagyományos informatikai alkalmazások esetében megfelelõ hatékonysággal és maradéktalanul csak az új fejlesztések esetében érvényesíthetõk. Ennek megfelelõen a katonai informatikai területen folyó szabványosítási törekvések eredményei is jellemzõen több lépcsõben, többéves idõszak után válnak széleskörûen alkalmazottá. Ebben az idõszakban tehát fokozatosan csökkenõ részaránnyal, de léteznek még az adott szabványokat nem vagy csak részben érvényesítõ alkalmazások, amelyek tudásösszetevõi így nem vagy csak részben hozzáférhetõk más alkalmazások számára.

Az elõzetes szabványosítás jelenlegi formájában csak egy adott nemzeti haderõn, illetve egy szövetségi rendszeren belül valósítható meg és értelemszerûen nem vagy csak jelentõs korlátozásokkal érvényesülhet eltérõ nemzetek haderõi, illetve katonai szervezetek és más kormányzati vagy nem kormányzati szervezetek által használt informatikai alkalmazások esetében. A 21. század elején a katonai vezetésnek viszont növekvõ mértékben dinamikus és bizonytalan környezetben egyre bonyolultabb szituációkkal és egyre változatosabb feladatokkal, például nem háborús mûveletek végrehajtásával kell megbirkóznia. Ezen feladatok legtöbbjének végrehajtására ma már jellemzõen különbözõ koalíciós partnerektõl származó és különbözõ haderõnemekhez tartozó integrált erõk (Combined Joint Task Forces) kerülnek felállításra.

Az ilyen többnemzetiségû összhaderõnemi mûveletek támogatása érdekében a különbözõ szövetséges erõk számos informatikai alkalmazását és az ezek által biztosított adatforrásokat kell napok vagy órák alatt (elõzetes szabványosítás hiányában is) interoperábilis módon összekapcsolni. Az egyes – esetleg elsõ alkalommal „találkozó” – alkalmazásokból, alkalmazáskomponensekbõl adott esetben anélkül kell felépülnie egy összehangolt informatikai rendszernek, hogy ehhez informatikai fejlesztéssel foglalkozó szakemberek (programozók) hetekre vagy hónapokra kiterjedõ munkája lenne szükséges (lehetne mód).

Az adott mûveletet támogató informatikai rendszer szolgáltatásainak (alkalmazásainak) a hatékonyság érdekében a konkrét területre (hadmûveleti területre, harcmezõre, harctérre) és feladatra szabottaknak kell lenniük, ugyanakkor kellõen rugalmasan kell tudniuk támogatni a helyzet alakulásában, a mûveletben részt vevõ erõk összetételében, a hozzáférhetõ informatikai rendszerek és adatforrások körében vagy a rendelkezésre álló számítási kapacitásban és kommunikációs sávszélességben bekövetkezõ változásokhoz, valamint a parancsnoki célkitûzésekhez és elgondolásokhoz igazodó – ideális esetben automatikus – alkalmazkodást (újrakonfigurálódást). Az egyes alkalmazáskomponenseknek egymás mellett, a számítási, kommunikációs és adaterõforrásokat megosztva – sokuknak folyamatosan, nagy megbízhatósággal és védetten – kell mûködniük a különbözõ informatikai környezetekben.

Az egyes alkalmazások (alkalmazáskomponensek) közötti hatékony együttmûködés feltételeit hosszú távon csak ezen alkalmazások információs képességeinek (lényegében tehát tudásösszetevõinek), illetve az ezek alapját képezõ fogalomrendszereinek autonóm és dinamikus egyeztetése biztosítja, ami várhatóan mindenekelõtt az intelligens ágensek együttmûködõ rendszerének formájában megvalósított alkalmazások, illetve a korábbi alkalmazások ilyen jellegû képességekkel kiegészítése esetén lesz lehetséges.

Az informatikai alkalmazások az információs fölény saját képességek növelésével történõ kivívásának alapvetõ eszközei. A 21. század információs színterét a hagyományos „monolit” alkalmazások helyett már a magas fokú autonómiával rendelkezõ (közöttük is egyre bõvülõ mértékben az intelligens) tudásösszetevõik alapján elkülönített alkalmazáskomponensekre, illetve ezek együttmûködésére épülõ alkalmazások jellemzik majd. Az ezen alkalmazáskomponensek közötti rugalmas és hatékony együttmûködés – információ- és információs szolgáltatás-csere – feltételét alapvetõen az általuk megtestesített tudásösszetevõk elõzetes (lehetséges mértékû) egységesítése, szabványosítása mellett mindenekelõtt ezek helyzetfüggõ, autonóm összehangolásának képessége fogja biztosítani.

Mindezekbõl levonható az a következtetés, hogy a katonai vezetésben, a katonai mûveletek során felhasznált tudásösszetevõk tartalmi vizsgálata lényeges feltétele ezek informatikai alkalmazások formájában történõ hatékony megjelenítésének; ezen alkalmazások autonóm, együttmûködõ komponensekre (intelligens ágensekre) célszerû tagolásának; és lényeges hozzájárulás az információs fölény kivívása feltételeinek megteremtéséhez, célszerû eszközei és módszerei meghatározásához.

FELHASZNÁLT IRODALOM

C4I for the Warrior, „The Joint Vision for C4I Interoperability” – Joint Chiefs of Staff, 1998. jan.

Brian FREDERICKS: *Information Warfare: The Organizational Dimension.* – Institute for National Strategic Studies, 1996.

FM 100–6, Information Operation. – Headquarters Department of the Army, Washington, 1996. augusztus 20.

AJP–01(B) Allied Joint Doctrine. Ratification Draft 1. – NATO Standardization Agency, 2000. szept.

Joint Pub 1–02, DoD Dictionary of Military and Associated Terms – Joint Chiefs of Staff, 2000. június 14.

Joint Pub 3–13, Joint Doctrine for Information Operations – Joint Chiefs of Staff, 1998. október 9.

TRADOC Pamphlet 525–69, Concept for Information Operations – US Army Training and Doctrine Command, Fort Monroe, 1995. augusztus 1.

Air Force Doctrine Document 2–5, Information Operations. – United State Air Force, 1998. augusztus 5.

Martin C. LIBICKI: *Information Dominance* (In. Strategic Forum, Number 32, November 1997) – National Defense University, Institute for Strategic Studies.

Information Assurance Through Defense in Depth – Joint Chiefs of Staff, 2000. február.

Fred W. GORTLER: *Understanding Information Power and Organizing for Victory in Joint Warfighting* – Marine Corps Command and Staff College, 1995. május 31.

John ROTHROCK: *Information Warfare: Time for Some Constructive Skepticism?* – (Chapter 9, In Athena’s Camp) – John Arquilla – David Ronfeldt (szerk.): In Athena’s Camp: Preparing for the Conflict in the Information Age – RAND Corporation, 1997.

Concept for Future Joint Operations. Expanding Joint Vision 2010 – Joint Chiefs of Staff, 1997. máj.

Edward WALTZ: *Information Warfare Principles and Operations* – Artech House, Boston–London, 1998.

AAP–6(V), NATO Glossary of Terms and Definitions (English and French). Modified Version 02. – NATO Military Agency for Standardization, Brussels, 2000. augusztus 7.

NATO C3 Technical Architecture, Volume 5, NC3 Common Operating Environment (NCOE). Version 1.0. – ISSC NATO Open Systems Working Group, 1999. július 30.

1

DoD Directive S–3600.1 „Information Warfare”, majd ezt követõen egy C3I helyettes államtitkári, ASD(C3I) kiadvány – ismerteti [Fredericks].

2

Az „information in warfare” rendeltetése, hogy az információkat idõben és megbízhatóan eljuttassa arra a helyre, ahol szükség van rá. Magában foglalja az információk gyûjtését, feldolgozását, valamint elosztását és az Egyesített Vezérkar 1992-ben kibocsátott „C4I for the Warrior” jövõképében foglaltak szinonímájának tekinthetõ (Defense Science Board jelentése, amelyet ismertet [Fredericks]).

3

FM 100–6, Information Operations.

4

A szerzõnek az információs fölénnyel kapcsolatos véleményét egy korábbi publikáció – Információs fölény, tudásfölény, vezetési fölény – tartalmazza.

5

AJP–01(B) Allied Joint Doctrine. Ratification Draft 1. – 14–1. o.

6

Joint Pub 1–02, DoD Dictionary of Military and Associated Terms, 221.o.; Joint Pub 3–13, Joint Doctrine for Information Operations (Glossary), GL–7. o.

7

Egy korábbi dokumentumban (TRADOC Pam 525–69, Concept for Information Operations, 1995) a kiemelt részek helyett még „a parancsnoki vezetési ciklust és a feladat-végrehajtást”, illetve az „információs és döntési rendszerei” megfogalmazások szerepelnek.

8

FM 100–6, Information Operations (Glossary) – GL–7 .o.

9

AFDD 2–5, Information Operations (Glossary) – 41. o.

10

Joint Pub 1–02, DoD Dictionary of Military and Associated Terms, 221.o.; Joint Pub 3–13, Joint Doctrine for Information Operations (Glossary), GL–7. o.

11

FM 100–6, Information Operations – Glossary, GL–8. o.

12

TRADOC Pamphlet 525–69, Concept for Information Operations.

13

AFDD 2–5, Information Operations (Glossary) – 42. o.

14

Libicki: Information Dominance.

15

Information Assurance Through Defense in Depth, 2000 – 4. o.

16

Smart weapons, „okos” fegyverek.

17

Gortler: Understanding Information Power and Organizing for Victory in Joint Warfighting.

18

Rothrock: Information warfare. Time for some constructive scepticism?

19

Készült a Concept for Future Joint Operations hasonló tartalmú ábrája részeinek felhasználásával.

20

Joint Pub 1–02, DoD Dictionary of Military and Associated Terms – 329. o.

21

Joint Pub 1–02, DoD Dictionary of Military and Associated Terms – 128. o.

22

AFDD 2–5, Information Operations – 2. o.

23

Waltz: Information Warfare Operations and Principles – 107. o.

24

Részletesebben lásd Rothrock: Information warfare. Time for some constructive scepticism?

25

Mindezt jelzi a korábban már említett információalapú hadviselés (information-based warfare) fogalmának bevezetése és elterjedése az USA Nemzetvédelmi Egyetemén folyó oktatásban.

26

Joint Pub 1–02, DoD Dictionary of Military and Associated Terms – 228. o.

27

AAP–6, NATO Glossary of Terms and Definitions – 2–I–5.o.

28

(Had)mûvelet (operation): Katonai tevékenység, illetve hadászati, harcászati-hadmûveleti, kiszolgáló, kiképzési vagy katonai igazgatási feladat végrehajtása; a harc megvívásának folyamata, beleértve a kitûzött célok eléréséhez szükséges erõ-eszközmozgatást, utánpótlást, támadást, védekezést és manõvereket. [AAP–6, NATO Glossary of Terms and Abbreviations – 2–O–2. o.]

29

(Mûveleti) interoperabilitás: rendszerek, egységek és csoportosítások képessége arra, hogy szolgáltatásokat nyújtsanak más rendszereknek, egységeknek és csoportosításoknak vagy fogadjanak azoktól, illetve e szolgáltatások cseréjével képesek legyenek hatékonyan együttmûködni. [Joint Pub 1–02, DoD Dictionary of Military and Associated Terms – 233. o.]

30

NATO C3 Technical Architecture, NC3 COE – 40. o.