PRO PATRIA AD MORTEM

Információs műveletek a kibertérben

HAIG ZSOLT

dialóg Campus

Haig Zsolt

Információs műveletek a kibertérben

Vákát oldal

Haig Zsolt

INFORMÁCIÓS MŰVELETEK A KIBERTÉRBEN

Dialóg Campus Kiadó ❖ Budapest

A mű a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosítószámú,
„A jó kormányzást megalapozó közszolgálat-fejlesztés” elnevezésű
kiemelt projekt keretében működtetett Ludovika Kiemelt Kutatóműhely
keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült.

Szakmai lektor
Ványa László

© Haig Zsolt, 2018
© Dialóg Campus Kiadó, 2018

A mű szerzői jogilag védett. Minden jog, így különösen a sokszorosítás, terjesztés
és fordítás joga fenntartva. A mű a kiadó írásbeli hozzájárulása nélkül részeiben
sem reprodukálható, elektronikus rendszerek felhasználásával nem dolgozható fel,
azokban nem tárolható, azokkal nem sokszorosítható és nem terjeszthető.

Tartalom

Előszó 9

Bevezetés 11

A könyvben használt fontosabb alapfogalmak 15

1. A távírótól az internetig: rövid történeti áttekintés 17

1.1. A távközlés hőskora 17
1.1.1. A vezetékes távközlés kialakulása 17
1.1.2. A vezeték nélküli távközlés kezdete 20
1.1.3. A rádió megjelenése a katonai vezetésben 24

1.2. Elektronikai technológiák fejlődése a második világháborúban 25
1.2.1. A radarháború 25
1.2.2. A rádiónavigáció kialakulása 31

1.3. A földi mobiltávközlés fejlődése 34

1.4. A műholdas rendszerek kibontakozása 44
1.4.1. A műholdas távközlés fejlődése 44
1.4.2. A műholdas navigáció kialakulása 50

1.5. A számítógép fejlődéstörténete 54
1.5.1. A nagyszámítógépek kora 54
1.5.2. A személyi számítógépek megjelenése 61

1.6. A számítógép-hálózatok evolúciója 64
1.6.1. A számítógép-hálózatok kialakulása 64
1.6.2. Az internet fejlődése 69
1.6.3. A hálózati kommunikáció fejlődése 73
1.6.4. A fejlődés iránya: az emberek és gépek hálózata 75

2. Napjaink meghatározó hálózatos infokommunikációs technológiái 77

2.1. Az infokommunikációs technológiai fejlődés fő irányai 77

2.1.1. A Big Data problémája 77
2.1.2. Infokommunikációs technológiai konvergencia 81
2.1.3. Feltörekvő infokommunikációs technológiák 84

2.2. Civil és katonai hálózat-alapú infokommunikációs technológiák 88
2.2.1. Felhőalapú számítástechnika 88
2.2.1.1. A felhőalapú számítástechnika kialakulása 88
2.2.1.2. A felhőalapú számítástechnika fajtái, típusai 91
2.2.1.3. A felhőalapú számítástechnika katonai alkalmazhatósága 94
2.2.2. Tárgyak internete – IoT 96
2.2.2.1. Az IoT értelmezése 96
2.2.2.2. Az IoT működése 99
2.2.2.3. Az IoT kommunikációs megoldásai 102
2.2.2.4. Az IoT katonai alkalmazhatósága 110
2.2.3. Szenzorhálózatok 113
2.2.3.1. A szenzorok és szenzorhálózatok fogalma, jellemzői 113
2.2.3.2. A szenzorhálózatok architektúrája 117
2.2.3.3. Katonai szenzorok és szenzorhálózatok 122
2.2.3.4. A szenzorhálózatok biztonsági kérdései 132
2.2.4. Katonai műveleti hálózatkoncepciók 135
2.2.4.1. Hálózatközpontú hadviselés 135
2.2.4.2. NATO-hálózatalapú képesség 139
2.2.4.3. NATO szövetséges műveleti hálózatépítés 143

3. Információs műveletek 149

3.1. A műveletek információs környezete 149

3.2. Az információs műveletek kialakulása 153

3.3. Az információs műveletek elméleti alapjai 158
3.3.1. Információelméleti megközelítés 158
3.3.2. Az információs fölény és a befolyásolás elmélete 160
3.3.2.1. Az információs fölény klasszikus értelmezése 160
3.3.2.2. Az információs fölény adaptív megközelítése – a befolyásolás elmélete 164

3.4. Az információs műveletek fejlődése 167
3.4.1. A fejlődés korai szakasza 167
3.4.2. A hadviselés és a műveleti környezet változása 172

3.5. Az információs műveletek kiteljesedése 176
3.5.1. Az Egyesült Államok információs műveletek koncepciójának változása 176
3.5.2. Az információs műveletek NATO-értelmezése 181
3.5.3. Oroszország információs hadviselésének fejlődése 189
3.5.4. Kína információs hadviselési felfogása 199
3.5.5. Az információs műveletek hazai megközelítése 205

3.6. Az információs műveleti koncepciók szintézise és átfogó értelmezése 209
3.6.1. Az információs műveletek fogalma 209
3.6.2. Az információs műveletek műveleti tartománya 211
3.6.3. Az információs műveletek célpontjai 211
3.6.4. Az információs műveletek célja 212
3.6.5. Az információs műveletek képességei 214

4. Információs műveleti képességek a kibertérben 219

4.1. A kibertér 219
4.1.1. A kibertér meghatározása 219
4.1.2. A kibertér struktúrája 229

4.2. Kibertéri műveletek 234
4.2.1. A kiberfölény és a kibertéri befolyásoló hatások 234
4.2.2. A kibertéri műveletek értelmezése 236
4.2.3. A kibertéri műveletek információs képességei 242
4.2.3.1. Elektronikai felderítés 242
4.2.3.2. Számítógép-hálózati műveletek 245
4.2.3.3. Elektronikai hadviselés 250
4.2.3.4. Műveleti biztonság 254
4.2.3.5. Megtévesztés 257
4.2.3.6. Pszichológiai műveletek 262
4.2.3.7. Civil-katonai együttműködés 265
4.2.3.8. Tömegtájékoztatás 267

4.3. A kibertéri információs tevékenységek kölcsönhatása 269
4.3.1. Kibertéri technikai információs képességek 271
4.3.1.1. Kibertéri technikai információs képességek egymásra hatása 271
4.3.1.2. Kína integrált hálózatos elektronikai hadviselési stratégiája 277
4.3.1.3. Az USA kibertéri és elektronikai hadviselési műveletek koncepciója 278
4.3.1.4. Kiberparancsnokságok kialakítása 281
4.3.2. Kibertéri kognitív befolyásolás 285
4.3.2.1. Kibertéri kognitív információs tevékenységek egymásra hatása 285
4.3.2.2. Álhírek a kibertérben 289
4.3.2.3. Kibertér és terrorizmus 297

Összegzés, következtetések 305

Irodalomjegyzék 311

Rövidítések jegyzéke 331

Képek jegyzéke 337

Ábrák jegyzéke 339

Táblázatok jegyzéke 341

Grafikonok jegyzéke 343

Előszó

A *kibertér* talán a 21. század egyik legtöbbet használt kifejezése, amely az információtechnológiának köszönhetően a mindennapjaink szerves részévé vált. A társadalom számos funkciója a fizikai dimenzióból a kibertérre költözött az elmúlt néhány évtizedben, és ennek a folyamatnak még nincs vége.

A társadalom az elmúlt időben már egyre inkább a *hálózatos* kifejezéssel jellemezhető, hiszen számtalan olyan technikai eszközt használunk minden nap, amelyek alapjaiban változtatták meg a kommunikációnkat, az információhoz való viszonyunkat, legyen szó gazdaságról, kultúráról, politikáról vagy éppen biztonságról. Ezek a változások pedig éppen a hálózatba kötött információtechnológiai eszközöknek köszönhetők.

A katonai tevékenységekre, magukra a hadseregekre és azok műveleteire – legyen szó háborús konfliktusról vagy éppen békefenntartásról – az információtechnológia szintén komoly hatással volt. Az információ ebben a fejlődésben kulcsszerepet kapott, hiszen a technikai fejlődés magával hozta azokat a műveleteket, amelyekben az információra alapozott tevékenységek erősokszorozó tényezőként jelentkeznek.

Jelen könyv ezeket a tényezőket vizsgálja tudományos igényességgel. A szerző, aki több mint három évtizede vizsgálja és kutatja az információs műveleteket, tudományos alapossággal mutatja be a technikai fejlődés minden egyes olyan szakaszát, amelyek hatással voltak napjaink információtechnológiai forradalmára és így a katonai műveletekre is.

A könyv egyedi történeti áttekintést ad a távírótól az internetig, majd bemutatja azokat a hálózatos technológiákat, amelyek nemcsak előnyökkel, de számos – elsősorban biztonsági – kihívással is járnak.

Mindezek mellett a szerző bepillantást enged az információs műveletekbe, amelyek az elmúlt néhány évtized katonai tevékenységeinek egész sorát alakították át. A történeti áttekintésen túl a könyv részletesen bemutatja az olyan nagyhatalmak, mint az Egyesült Államok, Oroszország, Kína, illetve a NATO mint katonai-politikai szövetség információs műveletekről alkotott elképzeléseit, doktrínáit. Különösen érdekes lehet az olvasó számára annak tanulmányozása, hogy ezek a műveletek a kibertérben hogyan érvényesülnek, illetve azok a kibertérre milyen hatással is vannak, hiszen ezek nemcsak a katonai, hanem a társadalom legtöbb funkciójára is hatással lesznek a jövőben.

Budapest, 2018. április 28.

Kovács László

Bevezetés

Az elmúlt évszázadban a vezeték nélküli távközlés és az elektronikai technológiák fejlődése, valamint a 40-es évek elején megindult informatikai forradalom az információ kezelése terén valódi paradigmaváltást hozott. A számítástechnika és a kommunikációs technológia fejlődése, illetve konvergenciája lehetővé tette a számítógépek összekapcsolását és a hálózatok kiépítését. Az első funkcionális hálózatokat követő nagykiterjedésű hálózatok és az internet alapjaiban változtatták meg az emberek információs igényeit. Napjainkban már ezeken a hálózatos technológiákon alapuló információs infrastruktúrák biztosítják a társadalom információs funkcióinak kielégítését.

Az infokommunikációs technológiák nagy ütemű fejlődése mára már meghaladta a megszokott hálózatszervezési elveket, és az elmúlt években paradigmaváltozást hoztak a hálózatok értelmezésében. A konvencionális számítógép-hálózatok mellett egyre nagyobb hányadban jelennek meg az interneten keresztül egymással összekapcsolt fizikai eszközök, emellett pedig a felhasználók is részesévé váltak a hálózatnak.

Ez a tendencia megfigyelhető a katonai rendszerekben is. A védelmi célú hálózatokban a civil technológiák fokozatos begyűrűzését tapasztalhatjuk. A katonai műveletekben az összadatforrású felderítés elvei szerint gyakran szenzorhálózatokat alkalmaznak a szemben álló félre és a harctéri környezetre vonatkozó adatok gyűjtése céljából, az így megszerzett adatok kezelésére pedig a polgári szférában már elterjedt hálózatos megoldásokat alkalmazzák.

A hálózatok kiépítése és működése szempontjából az egyik fontos kérdés a kommunikáció megvalósítása. A mobilitás követelményéből fakadóan ma már a hálózatok jellemző kommunikációs módja az elektromágneses tartományban létesített vezeték nélküli kapcsolat. Ennek

köszönhetően a hálózathoz való külső, illetéktelen hozzáférés is könnyebben megvalósítható, ami a rendszerek fenyegetettségének növekedését is magában hordozza.

E fenyegetések az információs környezetben egyre változatosabb formában valósulnak meg, és ezek egymásra hatása az eredményességet is jelentősen növelheti. A 90-es években kialakult információs műveletek mint az egymás hatásait kihasználó információs tevékenységek integrált alkalmazásai mára jelentős átalakuláson mentek keresztül. Ezt az átalakulást a katonai műveletek megváltozott környezete, az új technológiák megjelenése, valamint a kibertér átalakulása generálja.

Mindezek indokolják, hogy az új típusú hálózatos környezetben összegezzük napjaink meghatározó polgári és katonai infokommunikációs technológiáit, bemutassuk kialakulásuk és fejlődésük fő irányait, újszerű megközelítésben elemezzük, majd meghatározzuk a hálózatok elleni kibertéri fenyegetések és a lehetséges védelem formáit, módjait. A tanulmány e fő célkitűzésnek megfelelően az alábbi részcélokat tűzte ki maga elé:

1. A távközlés, az informatika, az elektronikai technológiák és az elektronikus média fejlődési tendenciáinak elemzése alapján igazolni a hálózatosítás általánossá válását, valamint hogy a hálózatok az egyének életében és a társadalmi funkciók minden területén, így a katonai műveletekben is meghatározó jelentőségűvé válnak.
2. Feltárni az információs műveletek kialakulásának és fejlődésének főbb sarokpontjait és ezek alapján bizonyítani az átalakuló műveleti környezetben az információs műveletek funkcióinak és képességeinek megváltozását, valamint a változó műveleti környezethez való igazodását.
3. A kibertéri definíciók és interpretációk elemzése alapján bizonyítani a kibertér értelmezésének és tartományainak kibővülését és ez alapján igazolni a kibertéri műveletekben alkalmazható sokrétű információs tevékenységek létjogosultságát.

4. Az információs környezet dimenzióinak és az információs műveleti képességeknek, valamint a kibertér tartományainak összevetése alapján bizonytani, hogy az egyes képességek mind a tevékenység jellegét, mind pedig hatását illetően értelmezhetők a kibertérben is, és azok egymásra hatása egyre jelentősebbé válik mind a katonai, mind pedig a polgári környezetben.

A fenti céloknak megfelelően e kötet bemutatja a kommunikáció, az elektronikai technológia és az informatika fejlődésének főbb mérföldköveit és a hálózatosítás irányába tett egyértelmű fejlesztéseket. Ismerteti napjaink legújabb hálózatos infokommunikációs technológiai fejlődési irányait, illetve a polgári technológiák katonai megjelenését. Elemzi az információs műveletek kialakulásának és fejlődésének tendenciáit, rámutat a változás jellegére és hatásaira. Végül pedig, a kibertér újszerű megközelítése révén meghatározza az egyes információs műveleti képességek kibertéri megjelenési formáit és alkalmazási lehetőségeit.

Vákát oldal

A könyvben használt fontosabb alapfogalmak

Katonai információs környezet: Katonai információs környezet alatt a globális információs környezet azon szereplőinek, eszközeinek és erőforrásainak, valamint információinak összességét értjük, amelyek lényeges hatással vannak egy adott katonai művelet végrehajtására. (MUNK 2002, 140.)

Információs műveletek: Az információs környezetben érvényesülő információs képességek integrált, összehangolt és koordinált alkalmazására irányuló tevékenységek összessége, amelyek a műveletek célkitűzéseinek elérése érdekében, kognitív képességekkel közvetlenül, illetve technikai képességekkel közvetetten hatásokat gyakorolnak a műveletekben részt vevő célközönség szándékára, helyzetértelmezésére és képességeire.

Kibertér: Az ember által mesterségesen létrehozott, dinamikusan változó tartomány, amelyben az információ gyűjtését, tárolását, feldolgozását, továbbítását és felhasználását végző, egymással hálózatba kapcsolt és az elektromágneses spektrumot is felhasználó infokommunikációs eszközök és rendszerek működnek, lehetővé téve ezzel az emberek és a különféle eszközök közötti folyamatos és globális kapcsolatot.

Kibertéri műveletek: A kibertéri műveletek a kibertérben érvényesülő információs képességek integrált, összehangolt és koordinált alkalmazására irányuló tevékenységek összessége, amelyek a műveletek célkitűzéseinek elérése érdekében, a kibertéri hálózatos infokommunikációs rendszereket felhasználva, a kognitív képességekkel közvetlenül, illetve a technikai képességekkel közvetetten hatásokat gyakorolnak a műveletekben részt vevő célközönség szándékára, helyzetértelmezésére és képességeire.

Elektronikai felderítés: „Az elektronikai felderítés fogalma alatt az elektronikai eszközökkel, különböző hullámtartományokban végzett adatszerzést

és ezen adatok feldolgozását értjük, amely megjelenhet több adatforrástípus esetében is." (HAIG et al. 2013, 96.)

Elektronikai hadviselés: „Az elektronikai hadviselés olyan hatásalapú katonai tevékenységek/műveletek összessége, amelyek elektromágneses környezetben, az elektromágneses energia tudatos használatával biztosítják az elektromágneses műveletek részeként végrehajtott támadó és védelmi jellegű hatások/célok elérését." [MD 3.6 (2) 2014, 12.]

Megtévesztés: Mindazon tevékenységek összessége, amelyekkel a másik fél döntéshozói szándékosan félrevezethetők a saját képességeinket, szándékunkat, elhelyezkedésünket és műveleteinket illetően, és ezáltal a másik felet olyan helyzetbe hozzuk, hogy tetteivel vagy tétlenségével a saját céljaink eléréséhez járul hozzá. (HAIG–VÁRHEGYI 2005)

Műveleti biztonság: Olyan folyamatok, tevékenységek és rendszabályok összessége, amely meghatározza és folyamatosan kontrollálja a saját kritikus információkat, valamint aktív és passzív eszközök és módszerek alkalmazásával csökkenti annak kockázatát, hogy a másik fél kihasználja a sebezhetőségeket. (AAP-06 2014, 2-P-10)

Pszichológiai műveletek: Olyan tervezett tevékenységek, amelyek a célközönség felé irányított kommunikációs módszereket és egyéb eszközöket alkalmaznak annak érdekében, hogy befolyásolják a politikai és katonai célok elérésére hatással lévő észlelési, megértési folyamatot, az attitűdöt és magatartást.

Számítógép-hálózati műveletek: Egyrészt a másik fél hálózatos számítógépes rendszerei felderítésére, adatok megszerzésére, működésük korlátozására, akadályozására, befolyásolására irányul a számítógép-hálózati felderítés és támadás módszereivel, másrészt pedig a saját hasonló hálózatok működését biztosítja a számítógép-hálózati védelem eszközeivel és technikáival.

Tömegtájékoztatás: Rendszerint egy olyan egyirányú kommunikációs tevékenység, amely során az előre megszerkesztett üzenetek, hírek a média segítségével jutnak el a hallgatóság nagy tömegeihez.

1. A távírótól az internetig: rövid történeti áttekintés

1.1. A távközlés hőskora

1.1.1. A vezetékes távközlés kialakulása

Az emberiség történelmében az információ mind ez idáig az emberi lét egyik alapvető alkotóeleme volt, és vélhetően ez a jövőben sem fog változni. Az információ gyűjtése, tárolása, feldolgozása és továbbítása mint az információ kezelésének alapvető formái folyamatosan fejlődtek, megvalósításukra az ember új és újabb eljárásokat, technológiákat talál fel és alkalmaz.

Az információ nagy távolságra történő továbbításának az idők során két nagy csoportja alakult ki. Egyrészt a közlekedéshez kapcsolódott, hiszen a személyszállítás során futárokkal vitték tovább az információt. A másik információtovábbítási módszer a személyszállítástól elkülönülten fejlődött, a távközlés kialakulását jelentette. A kezdetleges távközlési módszerek közé tartozott például a füstjelekkel való kommunikáció vagy a jelzőtüzek alkalmazása. Később, mint például a heliográf esetében a bonyolultabb jelek átvitelére a Nap fényének tükrözését használták fel. A 90-es években már olyan jelzőrendszereket alkalmaztak, mint az őrházak sorából álló Chappe távjelző rendszer vagy az Edelcrantz-féle redőnyös távjelző.

A valódi távíró-berendezések megszületésére azonban a 19. századig kellett várni. Ekkor ismerték fel az elektrosztatikus jelenségeket, illetve az elektromosság alapjait. A kezdeti lépéseket e téren Georges-Louis Le Sage, illetve Samuel Thomas von Sömmering elektromozó gépei jelentették, továbbfejlesztett változataik pedig az elektromágnesesség elvét kihasználó távírók voltak, amelyek már a valódi vezetékes

távközlés eszközei lettek. Ennek legismertebb és legelterjedtebb megoldása a sokak által is jól ismert Samuel Morse festőművész nevéhez köthető Morse távíró volt. Morse 1836-ban készítette el az első kezdetleges távíróját, majd néhány évvel később, 1844-ben Baltimore és Washington között kezdte meg működését az első Morse távírókapcsolat.

Ezt követően 1854-ben Davis Edvin Hughes zenetanár megalkotta a betűnyomó távírót, amely a későbbi géptávíró ősének tekinthető. A berendezés adóoldalán az adott betűkhöz tartozó billentyűket kellett lenyomni, a vevő oldalon pedig a gép azokat rögtön egy papírszalagra nyomtatta (1. kép). Mind a Morse távíró, mind pedig a Hughes-féle betűnyomó távíró hosszú ideig meghatározó szerepet kapott a polgári és a katonai távközlésben egyaránt. (Bartolits 2000)

1. kép

Hughes-féle betűnyomó távíró

Forrás: Hughes Telegraph 2009

A jelek átvitele mellett a beszédhang átvitelének igénye is hamarosan felmerült. E téren a legjelentősebb kezdeti eredmény Alexander Graham Bell nevéhez fűződik, akinek kísérletei nyomán 1876. március 10-én szólalt meg először a „meseszóló", amelyet ma *telefonnak* nevezünk. A kezdeti igen gyenge hangminőség problémájára Thomas Alva Edison 1877-ben találta meg a megoldást. A szénmikrofonnal és a különválasztott beszélő és hallgató készülékkel jelentős hangminőség-javulást ért el. (Bartolits 2000) Az egyre terjedő vezetékes távközlésnek köszönhetően a városokon belüli épületek között, majd a városok közötti telefon és távíróvezetékek ezrei keszekusza vezetékerdőt hoztak létre, mint ahogy azt az alábbi korabeli képeslap is szemlélteti (2. kép).

2. kép

Telefon- és távíróvonalak Broadway utcáin 1885–87-ben, egy korabeli képeslapon

Forrás: Broadway (é. n.)

Hamarosan szükségszerűvé vált, hogy az egyre növekvő számú készülék összekapcsolását egy központon keresztül oldják meg. A telefonközpont feltalálása Puskás Tivadar nevéhez köthető, aki egy kézi kapcsolótábla segítségével kapcsolta össze az egyes előfizetőket. Az első ilyen telefonközpont 1878. január 28-án kezdte meg működését New Havenben. Mindeközben a jelentősen megnövekedett előfizetői szám azt eredményezte, hogy a kezelőknek jelentősen megnövekedett a munkájuk. Ezt egy olyan automata központtal lehetett kiváltani, ahol a hívó maga tudta vezérelni a hívását. Az első automata telefonközpont 1892-ben kezdte meg működését, újabb lökést adva a távközlés fejlődésének és elterjedésének. Ez volt a hálózatok megszületésének pillanata, mivel a központba befutó vonalakkal megkezdődött a távbeszélő hálózatok kiépülése. (Bartolits 2000)

A vezetékes távközlés – köszönhetően az egyre újabb megoldásoknak – rohamos léptekben fejlődött. A földrészek közötti kommunikáció megvalósítására tenger alatti kábeleket fektettek le, amelyekkel összekapcsolták egymással a kontinenseket. Ugyanakkor már korán jelentkeztek a vezetékes távközlés hátrányai is, mégpedig hogy helyhez kötöttek, és a vezetékek is sérülékenyek voltak.

1.1.2. A vezeték nélküli távközlés kezdete

A helyhez kötöttség megszüntetése, vagyis a vezeték nélküli kommunikáció lehetőségét egy sor újabb fizikai felfedezés teremtette meg. 1862-ben James Clerk Maxwell egyenletei és Heinrich Rudolf Hertz 1887-es kísérletei igazolták az elektromágnesesség létét. Az elektromágneses energia felhasználásával, szabad térben és vezeték nélkül való jeltovábbítás felismerése tette lehetővé a drót nélküli távírózás és később a telefonálás megvalósítását.

Az erre alkalmas eszköz volt a rádió, amelynek feltalálása és a feltaláló személye körül megoszlanak a vélemények. Három neves tudós személye hozható kapcsolatba a rádió feltalálásával: Nikola Tesla, Alekszandr

Popov és Guglielmo Marconi. A három feltaláló közel egy időben, de külön-külön zajló kísérleteinek eredményeként Marconi 1896-ban szabadalmaztatta elsőként a rádiót (3. kép) Nagy-Britanniában. Érdekesség, hogy vázlata csaknem azonos volt Tesla korábban publikált tervrajzával. Tesla emiatt be is perelte Marconit, aminek következtében az USA Legfelsőbb Bírósága 1943-ban Teslának ítélte oda a rádió feltalálásának jogát. Vélhetően azonban Nikola Tesla, Alekszandr Popov és Guglielmo Marconi egymástól függetlenül érték el eredményeiket. (Haig et al. 2013)

3. kép

Marconi a szikratávíróval (jobbra) és a kohérer detektoros vevővel (balra) 1901-ben

Forrás: Marconi (1901)

Ezek az első készülékek azonban még kezdetleges szikratávírók voltak, és csak néhány kilométer távolságot voltak képesek áthidalni. A nagy távolságú hírközlés megteremtése is Marconi nevéhez köthető, mivel 1899-ben a La Manche csatornán keresztül létesített kommunikációs kapcsolatot, majd két évvel később, 1901. december 12-én megvalósította az európai és észak-amerikai kontinens közötti szikratávíró összeköt-

tetést: a skóciai Cornwallból sugárzott három rövid jelet (a morzeábécé „S” betűjét) a 3500 kilométerrel távolabbi Új-Fundlandon lévő antennával vették. Marconi élete folyamán tovább tökéletesítette rádiótechnikai találmányait, amit 1909-ben Nobel-díjjal ismertek el.

A szikratávíró kifejlesztése óriási hatással volt a távközlés fejlődésére, illetve a polgári és katonai alkalmazásra egyaránt. Bár ezek a berendezések még nagy méretűek és nehezek voltak, de például a hajók egymás közötti és a parti állomásokkal folytatott kommunikációjára már megfeleltek. Katonai alkalmazás terén a haditengerészet kiválóan tudta alkalmazni ezeket az eszközöket, mivel a vezetékes távírók használata a tengeren lehetetlen volt, de a mozgó szárazföldi csapatok esetében is nehézséget jelentettek a vezetékek.

A rádiótávközlés rohamos fejlődésének olyan találmányok adtak további lökést, mint például a katódsugárcső, a trióda, a kristálydetektoros vevőkészülék vagy a Meissner-oszcillátor. Többek között a felsorolt találmányok révén már lehetővé vált, hogy ne csak morzekódokat lehessen továbbítani és venni a rádióhullámok segítségével, hanem az emberi beszédhangot is. Kezdetben a Telefunken cég folytatott eredményes kísérleteket, és tartottak zenei műsoros rádió bemutatót. Majd ezen felbuzdulva az AT&T amerikai telefontársaság 1915. október 12-én, 20-án és 22-én éjjel megvalósította az első rádió-távbeszélő összeköttetését az Eiffel-torony és az egyesült államokbeli Arlington rádióállomásai között. (Balás 2009) A vett frekvenciát közvetlenül erősítő egyenes vevők problémáinak kiküszöbölésére pedig Edwin Armstrong 1918-ban megalkotta a szuperheterodin vevőt, amely aztán hosszú időkig a legelterjedtebb vételtechnikai megoldássá vált.

A beszédátvitel mellett már a rádió megalkotása előtt foglalkoztatta a tudósokat a képátvitel lehetősége is. 1875-ben George Carey már egy vezetékes átvitelt használó mozgókép-továbbítás lehetőségét írta le. A rádió feltalálása és a vákuumcsöves technika elterjedése pedig további lökést adott a mozgóképtovábbítás fejlődésének is. A kezdeti kísérleteket követően Tihanyi Kálmán töltéstárolás elvén működő ikonoszkópja, illetve Vladimir Zworykin elve nyomán megszületett a katódsugár-

csöves televízió (4. kép). Az új technológia lehetővé tette a képfelbontás jelentős növekedését, és 1941-ben az USA-ban megindult az 525 soros, 60 félképes NTSC-szabvány[1] szerinti fekete-fehér adás. A második világháború kitörése azonban megtörte a fejlődés ütemét, amely csak az 50-es években vett újabb lendületet a színes televíziózás fejlesztésével. (Hazay 2005)

4. a) kép

Telefunken FE III katódsugárcsöves televízió 1936-ból

Forrás: Telefunken 1936 (é. n.)

4. b) kép

RCA Viktor TRK 12, a világ első teljes egészében elektronikus letapogatású, 343 soros és 30 kép/másodperc jelmegjelenítésű televíziója 1939-ből

Forrás: RCA Victor 1939 (2014)

Mindezekkel tehát megindult, és hatalmas léptekben fejlődött az információ továbbításának egy új módja, aminek köszönhetően helyhez kötöttség nélkül, a rádióhullámok útján lehetett üzenetet, híreket és egyéb szórakoztató tartalmakat továbbítani. Mindezek a technológiai vívmányok voltak az alapjai annak a mai korban használatos infokommunikációs technológiának, amely az információ kezelésének teljesen újszerű, minden korábbinál hatékonyabb lehetőségeit teremti meg.

[1] National Television System Committee.

1.1.3. A rádió megjelenése a katonai vezetésben

A rádió előnyeit a katonák is hamarosan felismerték, és az első világháborúban megkezdődött széles körű alkalmazása is. A rádiónak köszönhetően a csapatok megnövekedett mobilitási képessége még jobban kihasználhatóvá vált. A harcálláspontokon vezeték nélküli rádiókat telepítettek, és megkezdték a rádióeszközök harcjárművekbe való beépítését, illetve hordozható eszközök is megjelentek, amelyeket rádiótávírászok üzemeltettek. Ennek köszönhetően jelentősen nőtt a csapatok vezetési és irányítási[2] képessége.

A híradás hatékonysága még szembetűnőbben javult a repülőgépek megjelenésével, mivel a fedélzetre telepített rádiókon keresztül gyorsabban lehetett akár légi felderítési adatokat is eljuttatni a vezetési pontokra vagy akár tüzérségi tűzhelyesbítési információkat továbbítani a tüzelőállásokhoz. Ezek a rádiók még rövid hatótávolságú, kezdetleges, nagy méretű és nehéz eszközök voltak, emiatt a szállításuk sokszor csak nagy nehézségek árán, öszvérek és lovak vontatta szerkezeteken volt lehetséges. Ebben az időszakban ezért elsősorban a haditengerészeti alkalmazásuk volt sikeres és széles körű.

A rádióhullámok útján történő kommunikációnak azonban megvolt a hátránya is, miszerint a kódolatlan adások könnyen lehallgathatók, sőt egy hasonló készülékkel zavarhatók is voltak. Erre szolgált első példaként az 1904–1905-ös orosz–japán háború, amikor is a csuzimai ütközetben az orosz rádiósok szikratávíróikat felhasználva zavarták a japán hajók híradását. Mindez azt is jelentette, hogy a híradó katonák tevékenységével szinte egy időben a harctéren megjelentek azok a módszerek is, amelyek a híradás lehallgatását, zavarását voltak képesek megvalósítani. Megjelentek a harctéren a rádió-iránymérő eszközök is, amelyekkel a sugárzó eszközök adásait lehetett bemérni. Az így megszerzett adatok birtokában a tüzérség tűzcsapást tudott mérni a rádiók működési helyéül szolgáló harcálláspontokra. Ez a katonákból úgynevezett rádió-

[2] Command and Control – C2.

iszonyt váltott ki, mivel féltek a működő rádiók közelségétől, ezért a parancsnokok azokat mind távolabb telepíttették.

A rádiózás megjelenésével egy új háborús színtér is megjelent, amely az elektromágneses térben való harc, a rádióháború kialakulását eredményezte, és amely napjainkban egyre nagyobb szerepet és létjogosultságot kap. A feladat ma is ugyanaz, mint száz évvel ezelőtt, felfedni, lehallgatni az ellenség kommunikációját, hozzáférni fontos információihoz, bemérni működő elektronikai berendezéseit, megzavarni azok működését. A technika és a technológia azonban időközben gyökeresen megváltozott.

A rádiók elterjedésének és számuk növekedésének köszönhetően a korábban kizárólagosan használt hosszú és középhullámú sávok telítődtek, így magasabb frekvenciasávok igénybevételére volt szükség. Megjelentek a magasabb frekvenciákat használó, nagyobb teljesítményű és érzékenyebb berendezések, amelyeknek köszönhetően nőtt a hatótávolság. A nagyobb távolságú rádiózás lehetőségét tovább növelte, hogy az irányított antennák alkalmazásával egy adott irányba jobban lehetett koncentrálni a kisugárzott teljesítményt. Az elektroncsövek terén elért eredményeknek köszönhetően a rádiók egyre kisebbekké váltak, ami a felhasználhatóságot jelentősen megkönnyítette úgy a szárazföldön, mint a repülőgépek fedélzetén.

1.2. Elektronikai technológiák fejlődése a második világháborúban

1.2.1. A radarháború

A második világháborúban – köszönhetően a technikai fejlődésnek – a rádióhíradás általánosan elterjedtté vált. A gépesített haderő kialakulásából és elterjedéséből fakadóan a szárazföldi, légi és tengeri hadviselés új követelményeket támasztott a híradással szemben is. A hordozható eszközök megjelenésének köszönhetően már kisalegységi szinten is

megjelentek a rádiók, és a beszédalapú kommunikáció vált a leginkább alkalmazott távközlési móddá. A vezetés biztosítása érdekében a harckocsikban elengedhetetlenné váltak a beépített rádiók. Hadosztály és ezred szinten nagyteljesítményű mobil rádiókészülékeket alkalmaztak, amelyekkel akár 160 km távolságú összeköttetést is meg lehetett valósítani. Az URH-tartományban megjelentek a frekvenciamodulációs eljárások, illetve a mobilitás követelményeit kielégítve rádióreléket alkalmaztak a hatótávolság növelése és a domborzati akadályok kiküszöbölése érdekében. (THOMPSON–BACK é. n.)

A távközlés fejlődése mellett egy másik nagy felfedezés is jelentős szerepet játszott a második világháborúban. Ez volt a rádiólokátor vagy más néven a radar,[3] amely alapvetően a rádióhullámokkal való irány és távolság meghatározására szolgál. A rádióhullámok kutatása és a rádióeszközök fejlesztése során a tudósok – többek között már Hertz is – azt tapasztalták, hogy a rádióhullámok bizonyos tereptárgyakról, objektumokról visszaverődnek. Ez a visszaverődés a távközlésben zavarként jelentkezett, később azonban felismerték, hogy a visszaverődő jelek detektálása alkalmas lehet tárgyak, objektumok észlelésére.

Christian Hülsmeyer 1904-ben szabadalmaztatott *telemobiloscope* elnevezésű készüléke a rádióhullámok kibocsátása és a visszaverődő jelek vétele elvén már 3 km-ről képes volt érzékelni a nagyobb testű hajókat. Ez volt tulajdonképpen az első radarelven működő szerkezet, amelynek azonban annak idején nem tulajdonítottak nagy jelentőséget. (HOLPP 2004) Az elektroncsövek fejlesztésének és az irányított antennáknak köszönhetően a 30-as évekre azonban már minden tudományos felfedezés és technikai feltétel rendelkezésre állt a radar kifejlesztéséhez.

A kezdetleges radarok folyamatosan sugároztak, ami csak kis teljesítményt és ezáltal kis hatótávolságot eredményezett. A nagyteljesítményű rádióhullámok előállításhoz egy új berendezésre volt szükség,

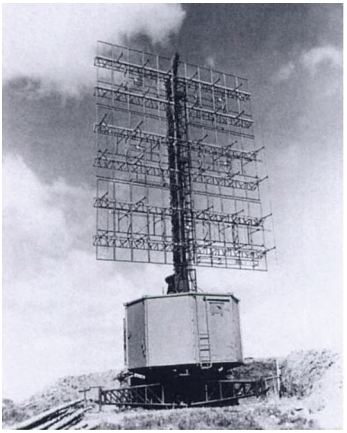
[3] Radio Detection and Ranging – RADAR.

egy olyan elektroncsőre, amely hatékonyan képes nagyteljesítményű, nagyfrekvenciás jeleket előállítani. Ez volt a magnetron, amelyet Albert Hull talált fel 1920-ban, majd John Randall és Harry Boot fejlesztett tovább 1940-ben. Az átütő változást az impulzusüzemű radar megalkotása hozta meg, amelyet egymástól függetlenül 1935-ben alkotott meg Rudolf Kühnhold irányításával a német GEMA vállalat, illetve a brit légügyi minisztérium kutatócsoportja, Robert A. Watson-Watt vezetésével.

A német GEMA vállalat 1936-ban fejlesztett ki egy forgatható antennás légvédelmi radart Freya néven, amelyet 1938-ban a haditengerészet, majd a légierő is rendszeresített [5. a) kép]. A 125 MHz-en működő 8 kW-os teljesítményű radarral a németek 1939-ben már képesek voltak a brit bombázókat 120 kilométerről észlelni a Helgolandi-öböl felett. Ugyanebben az évben a Telefunken cég kifejlesztette a Würzburg nevű rádiólokátort, amely akkor újdonságnak számító parabolaantennájával képes volt bármilyen gyorsan mozgó tárgyat, repülőgépet követni [5. b) kép]. Hatótávolsága ugyan elmaradt a Freya radarétól, pontossága azonban felülmúlta azt. A két radar jól kiegészítette egymást, mivel hatótávolsága miatt a Freya alkalmas volt nagy távolságból észlelni a légi célokat és riasztani a légvédelmet, a Würzburg viszont a nagyobb pontossága révén a Bofors légvédelmi lövegek számára célkövető és tűzvezető funkciót töltött be. (Millar 1983)

A brit radarrendszer fejlesztése Watson-Watt koncepciója alapján kezdődött el. 1936-ban a Temze torkolatában lévő Bawdsey kastélyában telepítették az első kísérleti radarállomást, amely az 1939-ben kiépített, több mint 20 radarból álló „Chain Home" radarrendszer első állomása volt [6. a) kép]. A 80 m magas tornyon lévő adóberendezések 22 és 30 MHz között működtek 200 kW-os teljesítménnyel, amellyel akár 200 km-es hatótávolságot is el lehetett érni. Röviddel ezután, ezt a 200 MHz-en működő „Chain Home Low" rendszerrel egészítették ki, amellyel lehetővé vált a kis magasságon repülő légi célok észlelése is. Az így kiépített radarhálózat képes volt elegendő

pontossággal a megfelelő időben jelezni a közeledő repülőgépek irányát, meghatározni helyzetüket és riasztani a veszélyeztetett városokat, iparvidékeket.



5. a) kép

A német Freya felderítőradar

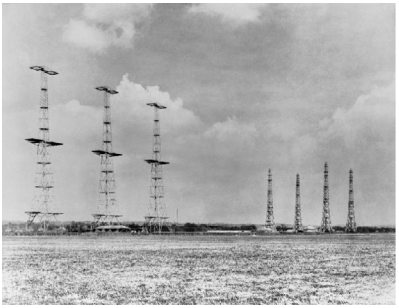
Forrás: Freya (é. n.)

5. b) kép

Würzburg D célkövető radar

Forrás: Wurzburg D (1945)

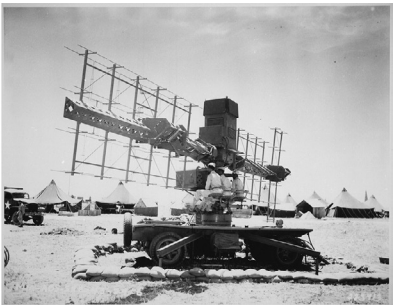
Az Egyesült Államokban nem volt annyira sürgető a radarok fejlesztése, mint Németországban és Nagy-Britanniában. Az USA hadba lépésének idejére azonban már rendelkeztek a 106 MHz frekvencián működő mobil SCR-270 és a fix telepítésű SCR-271 légtérellenőrző radarokkal, valamint a 205 MHz-en működő SCR-268 célkövető radarral. Az SCR-270 radarok 100 kW-os csúcsteljesítménnyel képesek voltak már 80 km-ről észlelni a repülőgépeket. Az SCR-268 célkövető radarban pedig a célkövetést a katódsugárcsöves kijelző alapján a kezelő végezte kézi vezérléssel [6. b) kép]. A magnetronok fejlődésének köszönhetően az USA-ban, 1943-ban elsőként készítették el a 3 GHz-es mikrohullámú tartományban működő SCR-584 tűzvezető radart, amelynek megnövelt iránymérési pontossága már 0,1 fok volt. (Holpp 2004)



6. a) kép

Az egyesült királyságbeli „Chain Home" radarhálózat antennatornyai

Forrás: CHAIN HOME (1945)



6. b) kép

Amerikai SCR-268 célkövető radar

Forrás: SCR-268 (1943)

Mindeközben a földi telepítésű rádiólokátorok mellett megkezdődött a repülőgép- és hajófedélzeti radarok kifejlesztése is. A Telefunken 490 MHz-en, 1,5 kW impulzus teljesítménnyel működő FUG 202 Lichtenstein BC radarja 4 km-es hatótávolságon belül ± 100 m-es és 2,5 fokos mérési pontossággal rendelkezett. A hatótávolság növelésére a 100 MHz alatti tartományban működő FUG 220 Lichtenstein SN2 radart fejlesztették ki. A két radar dipólantennáit a Messerschmitt Me 110G-4 repülőgép orrára szerelték, jellegzetes formát adva ezzel neki [7. a) kép]. Két évvel később, 1943-ban megépítették a Berlin N1A típusjelű radart, amely már rendelkezett a modern fedélzeti radarok legfőbb jellemvonásaival. A 3,3 GHz-es mikrohullámú tartományban működő radarnak 70 cm-es parabolaantennája volt, amelyet a JU 88 repülőgép orr-részében helyeztek el. A radar 15 kW-os impulzusteljesítménye pedig lehetővé tette a légi célok 9 km-es távolságból való észlelését. (HOLPP 2004)

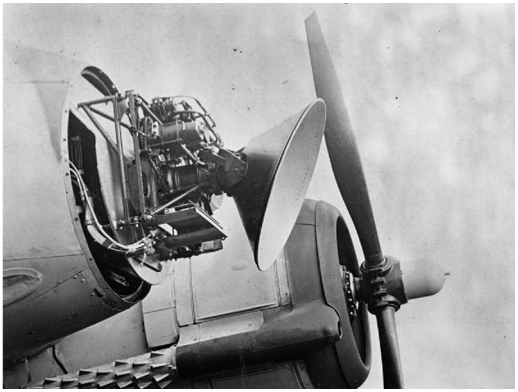
A britek a vadászrepülőgépekbe 1940 őszén építették be az első radarokat, aminek köszönhetően 1941-re már 110 repülőgépük volt felszerelve 200 MHz-es tartományban működő rádiólokátorral. Emellett a mikrohullámú tartományban is fejlesztettek fedélzeti elfogó radarokat. Ennek egyik jellegzetes képviselője volt az AI Mk. VIII radar, amely 1941

végétől lett rendszeresítve a Brit Királyi Légierőben. A 3 GHz-es tartományban, 25 kW-os impulzus teljesítménnyel működő radart és a mozgatható parabolaantennáját a Bristol Beaufighter Mk VIF éjszakai vadászrepülőgép orrában helyezték el [7. b) kép]. A repülőgép a radar képességeit kihasználva 9 km távolságból képes volt befogni a Luftwaffe repülőgépeit és hatékonyan támadni azokat. (Beckh 2005)

7. a) kép

Messerschmitt Me 110G-4 repülőgép orrán a FUG 202 (középen) és FUG 220 radarok antennái

Forrás: FUG 202 – FUG 220 (1945)



7. b) kép

Bristol Beaufighter Mk VIF orrában az AI Mk. VIII radarral

Forrás: AI MK. VIII (é. n.)

Az Egyesült Államokban az MIT[4] mikrohullámú technológiai fejlesztései a háború végére igen fejlett fedélzeti radarokat eredményeztek. Ennek egyik jó példája volt a Sperry cég által kifejlesztett AN/APS-6, amely 9375 MHz-en működött 40 kW-os impulzusteljesítménnyel. Ezt építették be a Vought F4U-4N Corsair vadászgép jobb oldalán lévő fegyver helyére. Ennek köszönhetően a pilóta már az ellenséges géppuska

[4] Massachusetts Institute of Technology.

hatótávolságán kívülről képes volt észlelni a repülőgépek közeledését, ami kedvező lehetőségeket kínált a sikeres légi harchoz. (Holpp 2004)

A radarok fejlesztése és széles körű elterjedése alapvető változást eredményezett a légi hadviselésben. Az Egyesült Királyság partjai körüli radarhálózatnak köszönhetően a Luftwaffe bombázói nem voltak könnyű helyzetben. A radarrendszer által biztosított korai riasztás eredményeként a fenyegetett körzetek lakosait időben lehetett értesíteni, akik így az óvóhelyekre tudtak jutni. Emellett a brit vadászok időben fel tudták venni a légi harcot a nehézkesen manőverező német bombázókkal.

A radarok jelentette előnyöket felismerve már a kezdet kezdetén mindkét oldalon azon gondolkodtak, hogy hogyan lehetne semlegesíteni, megzavarni azokat. E téren a britek kerültek előnybe, mivel Reginald V. Jones fizikus és felderítőtiszt már 1937-ben felvetette, hogy a Bawdsey-kastélybeli radar képes lenne 30 km-ről észlelni egy magasba emelt félhullám-hosszúságú dipólt. E felismerés alapján megkezdődtek a Window (ablak) fedőnevű kísérletek, amelyek során rájöttek, hogy a leghatékonyabb visszaverő felületet sztaniolból kivágott csíkok adják. Mindeközben 1942-ben már a németek is sikeres Düppel-(dipól-) kísérleteket folytattak. A dipólfelhők első háborús próbája 1943 nyarán, Hamburg bombázásakor volt. A repülőgépek egy-egy csomag dipólt vittek magukkal, amiket kiszórva egy-egy nehézbombázót imitáltak a radar indikátorán, amivel eredményesen meg tudták téveszteni a földi radarokat. (Millar 1983)

1.2.2. A rádiónavigáció kialakulása

A radarok kifejlesztésével párhuzamosan a navigáció terén is jelentős eredmények születtek a második világháborúban. Az elektronikus navigáció a repüléssel egy időben elengedhetetlen feladattá vált. Az 1910-es években a Marconi Társaság és a Telefunken is ért el eredményeket e téren, amelyeket aztán a 20-as években a Telefunken a léghajók navi-

gációs megoldásaiban tökéletesített. A 30-as években a Lorenz A.G. fejlesztett ki egy morzejelek adásán alapuló repülőtéri leszállást segítő megoldást, amelyet később minden német repülőtéren használtak.

Az ellenség területe feletti navigációhoz és az éjszakai célzott bombázáshoz fejlesztették ki a Knickbein rendszert. Az egymástól távol lévő adók 42,1–47,9 MHz-es frekvenciatartományban olyan két keskeny sugárnyalábon sugározták ki a rövid és hosszú jeleket, amelyek a célpont fölött keresztezték egymást. A bombázók akkor kezdték meg a bombázást, amikor mindkét adó jelét egy folyamatos sípolásként hallották. Ez persze messze elmaradt a ma ismert precíziós bombavetéstől, de arra mindenképpen jó volt, hogy az adott célterületet bombázzák. Ennek ellenszereként a britek a Chain Home radarhálózat tornyain elhelyezett vevőkkel képesek voltak venni a Knickbein rávezető rádiójeleit, amelyek alapján Robert Cockburn dolgozta ki az „Aspirin" fedőnevű Knickbein zavaróberendezést. A zavaróadó folyamatos, nagy teljesítményű, hosszú morzejelek kisugárzásával képes volt elnyomni a rávezető jeleket.

A Knickbein zavarása ellen és a bombavetés pontosságának növelése érdekében a németek egy új rendszert fejlesztettek ki „X-Gerät" néven, amely a 66,5–75 MHz-es tartományban működött. A rendszer egy bármilyen célpontra irányítható fősugárnyalábot és három azt keresztező sugárnyalábot alkalmazva működött. A bombázó repülőgépek 30 km-rel a cél előtt keresztezték a „Rhein" nevű sugárnyalábot, amely azt jelezte, hogy a továbbiakban a „Weser" nevű keskeny fősugárnyaláb mentén kell haladniuk. A cél előtt 10 km-rel keresztezték az „Oder" nevű sugárnyalábot, amikor a navigátorok elindították egy óra kettős mutatóját. A cél előtt 5 km-rel a bombázók keresztezték az „Elbe" nevű nyalábot, amikor a kezelők egy gomb megnyomásával megállították az óramutatókat, majd az egyik mutató elindult az ellentétes irányba, és amikor visszaért a nullához, akkor a bombák automatikusan kioldódtak. Az óra tulajdonképpen egy egyszerű számítóműszer volt, amely figyelembe vette a gép sebességét és a célponttól való távolságát, majd ez alapján számolta ki a ledobás helyét. A rádió-sugárnyalábok

irányítottságát jól mutatja, hogy több mint 300 km távolságban a fősugárnyaláb csak 100 m széles volt, amivel néhány száz méteres pontosságot lehetett elérni. A briteknek csak hosszas fáradozások után, 1940 végére sikerült egy hamis „Elbe" sugárnyalábbal megtéveszteni a rendszert, aminek következtében a bombázás helye távolabbra került a tervezettől.

Ezt követően az X-Gerät helyébe az „Y-Gerät" rendszer lépett, amely már csak egyetlen, a célterület felé sugárzott, 42–45 MHz-es sávban működő rádió-sugárnyalábbal működött. A kisugárzott modulált jelet a repülőgép fedélzetén elhelyezett készülék vette, majd visszasugározta. A visszasugárzott jelet a földi állomáson egyeztették az eredeti jellel, és a fáziskülönbség alapján megállapították a repülőgép és az adó közti távolságot. A rendszer nagy előnye volt, hogy csak egyetlen adóállomásra volt szükség a pontos navigációhoz. Amikor a bombázó a célterület fölé ért, akkor rádión utasították a bombázótisztet a bombák ledobására. A problémát a megválasztott frekvencia okozta, ugyanis az 1936-tól az Alexandra Palace-ban működő BBC televízióadója 45 MHz-en sugárzott, ami zavarta az Y-Gerät rendszert. Ezt felismerve a britek 1941-ben üzembe helyezték az első Cockburn által kifejlesztett, Domino nevű, folytonos jelet sugárzó zavaróberendezést, amellyel eredményesen tudták zavarni az Y-Gerät rendszert. (Millar 1983)

A nagy-britanniai csatában a kor akkori legkorszerűbb elektronikai fejlesztéseit vetették be mindkét oldalon. A felhasznált elektronikai rendszerek és az ellenük alkalmazott felderítő- és ellentevékenységi megoldások újszerűsége, illetve azok hatékonysága miatt a hadtörténelemben sokszor „sugárcsatának"[5] is nevezik a nagy-britanniai légi csatát. A britek a radar- és navigációs rendszerek elleni tevékenység mellett nagy hangsúlyt fektettek a rádiófelderítésre is, a lehallgató csoportok mellett speciális rejtjelfejtő csoportokat működtettek. Emellett számos esetben alkalmazták a dezinformálást és a rádiózavarást is.

[5] Battle of Beams.

Bár mindkét oldalon folytak erőfeszítések a másik fél elektronikai rendszerei működésének korlátozására, azonban a németek kevésbé voltak következetesek ezen a téren. A britek már korán felismerték az elektromágneses tartományban folyó harc fontosságát, előnyeit, emiatt pedig intenzíven fejlesztették és szélesítették a rádióelektronikai felderítés, megtévesztés, zavarás fegyvertárát. A felderítő- és a zavaróeszközök fejlesztése terén elért eredményeik miatt R. V. Jonest és R. Cockburnt az akkoriban születő és kiteljesedő elektronikai hadviselés kiemelkedő alakjaként tartják számon.

A második világháború végére a ma is használt rádiófrekvenciás elven működő elektronikai eszközök és rendszerek szinte teljesen kialakultak, és minden harctéren széleskörűen alkalmazták az egymással szemben álló felek. A harcászati rádióhálókon való csapatvezetés teljesen általánossá vált. A földi telepítésű radarokból radarláncot (Chain Home), összefüggő hálózatot építettek ki, ami elengedhetetlen volt a légi helyzetről szóló információk összegyűjtéséhez, kezeléséhez és a korai előrejelzéshez, riasztáshoz. Tulajdonképpen a mai értelemben vett légvédelmi rendszer egyik alapvető képességét, az összefüggő rádiólokációs mező alapjait ekkor teremtették meg.

Összességében tehát kijelenthető, hogy az elektronika, a rádióhíradás, a radartechnológia, a rádiónavigáció és az ellenük folyó harc a második világháborúban tömeges és általános alkalmazást nyert. A rádió- és radarhálózatok kialakításával és széles körű alkalmazásával pedig mind a vezetés, mind pedig a légi felderítés hatékonysága jelentősen növekedett.

1.3. A földi mobiltávközlés fejlődése

A második világháború után a telekommunikáció terén folyó kutatások az egyre szélesebb körben használható rádiós távközlő rendszerek kifejlesztésére irányultak. A beszédalapú kommunikáció lehetősége már realitás volt, azonban a hangminőség javítása és a többcsatornás átviteli meg-

oldások az alkalmazott frekvenciatartomány növelését irányozták elő. Az antennák és a mikrohullámú rezgéskeltők terén elért fejlesztések már a háború alatt lehetővé tették, hogy kísérleteket folytassanak a néhány száz MHz-es tartományban, aminek eredményeként megszülettek a mikrohullámú rádiórelék. Kezdetben ezek még csak néhány csatornás eszközök voltak, de az 50-es évekre már a GHz-es tartományban is sokcsatornás mikrohullámú eszközöket fejlesztettek ki. Az 50-es években Európában és Amerikában nagy méretű, transzkontinentális mikrohullámú reléhálózatok épültek ki, amelyeken keresztül a városok közötti távolsági távbeszélő-forgalmat és televíziós műsorok közvetítését valósították meg.

A háborút követően a nagy csatornakapacitású rendszerek mellett a távközlés fejlődését alapvetően a mobilitásra való törekvés határozta meg. Egyre nagyobb igényként jelentkezett ugyanis, hogy az emberek vezeték nélküli kommunikáció útján elérhetők legyenek, és másokat is elérjenek. Az amerikai Bell Labs kutatóintézetnek már a 40-es években megszületett egy koncepciója a cellás rendszerű mobiltávközlés megvalósítására. Az akkori csöves technológia és a háborús prioritások azonban nem tették lehetővé a kutatások folytatását. Ennek ellenére 1946-ban az Egyesült Államokban a 150 MHz-es sávban, 1956-ban pedig a 450 MHz-es sávban kereskedelmi célú nyilvános mobil rádiórendszerek kezdték meg működésüket. 1964-ben az AT&T egy IMTS[6] továbbfejlesztett mobiltelefon-rendszert kezdett el működtetni szintén a 150 és 450 MHz-es sávokban (8. kép). Ezeket további rendszerek követték főleg Észak-Amerikában és Európában, amelyek a 40, 80 és 160 MHz-es sávokban, de korlátozott számú csatornán működtek. E korai rendszereknél még szükség volt egy operátorra, aki a hívó felek közötti kapcsolatot felépítette. (Huurdeman 2003) A korábbi elektroncsöves készülékek méretüknél és jelentős energiaigényüknél fogva nem voltak alkalmasak a mindennapi életben használható hordozható rádiók, rádiótelefonok megépítésére. Ennek megvalósulásához egy teljesen új technológiára, a félvezetők kifejlesztésére volt szükség.

[6] Improved Mobile Telephone System – IMTS.

8. kép

Motorola TLD-1100 gépjárműbe szerelhető IMTS rendszerű mobiltelefon 1964-ből

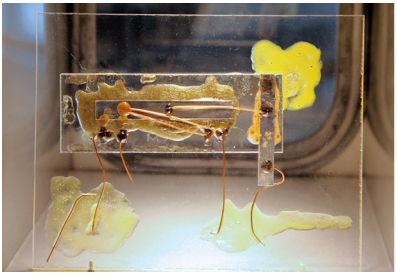
Forrás: MOTOROLA (2014)

A félvezetők kutatása a 30-as években kezdődött az amerikai Bell laboratóriumban, de a világháború miatt a kísérletek félbeszakadtak. Röviddel a háború befejezése után John Bardeen, Walter Brattain és William Shockley germániummal folytatott kísérletei eredményesnek bizonyultak, és 1947 decemberében bemutattak egy olyan alkatrészt, amelylyel egy elektroncsövet eredményesen helyettesítettek egy erősítőben. Ez volt az első tranzisztor, amely ugyanazokat a feladatokat képes volt elvégezni, mint egy elektroncső, de annál jóval kisebb és megbízhatóbb volt, és ami a legfontosabb, hogy sokkal kevesebb energiát igényelt.

A tranzisztor feltalálása alapjaiban változtatta meg az elektronikai ipart, sorra jelentek meg az egyszerű számológépekben, rádiókban, radarokban, navigációs eszközökben, majd később a számítógépekben is. Az alkatrészek miniatürizálásának további lépéseként 1958-ban Jack Kilby a Texas Instruments kutatója egy olyan gyártástechnológiát fejlesztett ki, amelynek köszönhetően tranzisztorok sokaságát lehetett beépíteni egy áramkörbe. Ezzel megszületett az integrált áramkör, amely

a ma is használatos elektronikai berendezéseink egyik alapvető alkotóeleme [9. a) kép].

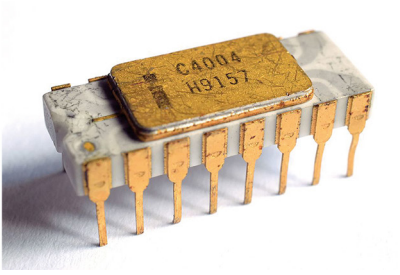
A félvezető-technológia következő nagy eredménye 1971-re tehető, amikor a Gordon Moore által alapított Intel Corporation kifejlesztette az Intel 4004-es integrált áramkört, amelyet *mikroprocesszornak* neveztek [9. b) kép]. Ez a 12 mm-es chip egy aritmetikai és logikai egységet, valamint egy vezérlőegységet egyesített egy nagy integráltságú áramkörben. Ezzel lehetővé vált, hogy a specifikus változóktól függően egy berendezés (például számítógép) logikai műveleteket hajtson végre az operátor folyamatos beavatkozása nélkül is. (Huurdeman 2003) Az Intel 4004 egy 4 bites mikroprocesszor volt, amelyet két évvel később követett a 8 bites Intel 8008, amely aztán a későbbi sikeres 8086 és x86-os, valamint a 8088-as processzorok alapjául szolgált. Erre alapozva 1981-ben megépítették az IBM PC-t. Ezzel nemcsak a különböző elektronikai berendezések, de a mai személyi számítógépek gyártástechnológiai alapjai is megszülettek.



9. a) kép

A Jack Kilby által kifejlesztett első integrált áramkör másolata

Forrás: IC Replica (2015)



9. b) kép

Az első mikroprocesszor, az Intel 4004-es 1971-ből

Forrás: Intel C4004 (2016)

A 70-es években a tranzisztoros technológia jelentős fejlődést hozott a mobiltávközlésben, de a hálózati kapacitást a használható rádiócsatornák alacsony száma jelentősen korlátozta. A hálózati torlódás orvosolására a 70-es évek végén kidolgoztak egy új csatorna-hozzáférési

technikát, a trönkölést. Ezzel a nagyszámú professzionális felhasználó számára (például taxisofőrök, közlekedési vállalatok, segélyszolgálatok stb.) javult a csatorna-hozzáférés, de a nyilvános mobil rádióhálózatokon nem sikerült megoldani a torlódás problémáját. Az AT&T ezért a Bell Labs 40-es évekbeli cellás rendszerű ötletét továbbfejlesztve kidolgozta az áttörést jelentő AMPS[7] fejlett mobiltelefon-rendszert, amelynek lényege, hogy egy frekvenciatartomány újra felhasználható a cellás rendszerben. (Huurdeman 2003)

A cellás elv lényege, hogy a sík terepen elméletileg kör alakú cellák – amelyek a nyilvános célú hálózathoz[8] csatlakoznak – saját adó-vevő állomással rendelkeznek, és egy olyan frekvenciakészletet használnak, amelynek egyik elemét sem alkalmazzák a szomszédos cellákban. A cellákon áthaladó mobiltelefon-használók automatikusan arra a frekvenciára váltanak, amelyikben éppen tartózkodnak. A cellás elvet az 1. ábra szemlélteti, ahol a modellezés és az ábrázolástechnikailag jobban kezelhető hatszög alakú cellák közel azonos méretűek, és amelyekben az eltérő frekvenciakészletet az eltérő betűk jelölik. Ez volt az analóg mobiltávközlés első generációjának (1G) alapelve. A cellás elv olyannyira működőképesnek és hatékonynak bizonyult, hogy a szolgáltatók a mai napig eszerint valósítják meg a földfelszíni mobiltávközlést.

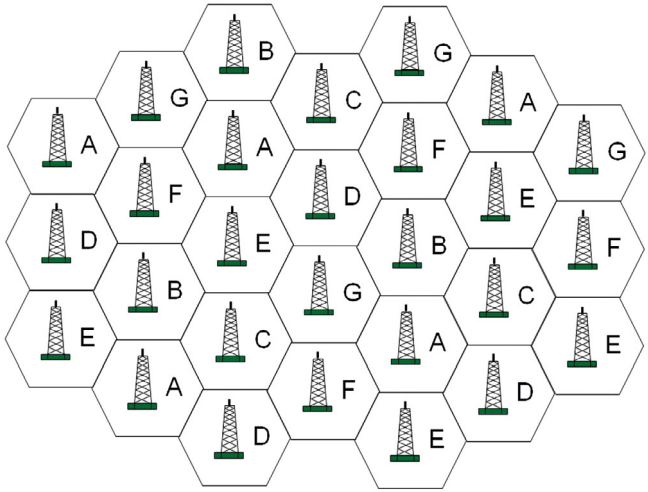
Az első AMPS rendszert 1978-ban Chicagóban mutatták be, és 1982-től használták az Egyesült Államokban. Látva a rendszer használhatóságát, a hasonló elven felépített mobiltávközlési hálózatokat sorra kezdték el rendszerbe állítani a világ fejlett országaiban. A teljesség igénye nélkül néhány példa ezek közül:

- Nagy-Britanniában a TACS;[9]
- Skandináviában az NMT;[10]
- Németországban a C 450;

---

7 Advanced Mobile Phone System – AMPS.
8 Public Switched Telephone Network – PSTN.
9 Total Access Communication System – TACS.
10 Nordic Mobile Telephone – NMT.

- Franciaországban a RadioCom 2000;
- Olaszországban az RTMS;[11]
- Japánban pedig MCS.[12] (Huurdeman 2003)



1. ábra

Cellás elv

Forrás: a szerző szerkeszt**ése**

Magyarországon 1989-ben alakult meg a Westel Rádiótelefon Kft., amely 1990 októberében Közép-Európában elsőként NMT 450 rendszerű, analóg rádiótelefon-szolgáltatást indított a 450 MHz-es frekvenciatartományban. A jelentős előfizetői költségek ellenére 1993-ig folyamatos volt a fejlődés, és óriási érdeklődést mutattak a hordozható készülékek iránt. (Koi 2010) Ugyanakkor mindegyik mobiltelefon-

[11] Radio Telephone Mobile System – RTMS.
[12] Mobile Control Station – MCS.

rendszernek nagy hátránya volt, hogy analóg üzemmódban működtek, és egymással nem voltak kompatibilisek. A 10. kép egy ebből az időszakból származó készüléket mutat.

10. kép

NMT 450 rendszerű Ericson HotLine mobiltelefon

Forrás: Ericson HotLine (é. n.)

Az analóg cellás rendszerek elterjedésének és sikerének köszönhetően a 80-as évek végére világszerte jelentős számú előfizetője volt e rendszereknek, ami ismét jelentős forgalmi torlódást okozott. Ennek kezelésére, illetve az analóg rendszerek előbb említett hátrányainak kiküszöbölésére gyökeresen új megoldásra, a digitális technológiára volt szükség. E technológia amellett, hogy javítja az átvitel minőségét, lehetővé teszi az adatátvitelt és a beszéd titkosítását, valamint a különféle többszörös hozzáférési módok alkalmazásával lényegesen növelhető a mobilhálózat kapacitása is.

A 90-es évek elejére a világon több második generációs (2G) digitális mobiltávközlő rendszert fejlesztettek ki, mint például:

- a GSM[13] mobilkommunikációs rendszert Európában;
- két digitális AMPS rendszert, a D-AMPS-t TDMA[14] és CDMA[15] hozzáférési technikával, valamint
- két személyi digitális cellás rendszert, a PDC 800-at és PDC 1500-at Japánban. (Huurdeman 2003)

Ezek közül a GSM-rendszer vált a legelterjedtebbé, amely ugyanúgy cellás elven működik, mint a korábbi AMPS rendszerek, csak a rendszer struktúrája és a működési módja különböző. A GSM-rendszerben idő- és frekvenciaosztásos többszörös csatorna-hozzáférést alkalmaznak (TDMA, FDMA[16]) a beszéd kódolt, digitális jel formájában történő átvitelére. A dekódolás, vagyis az üzenet megfejtése a vevő oldali készüléken történik, ezáltal a légköri zajok kevésbé befolyásolják a hangminőséget. Az analóg rendszerekkel ellentétben a digitális hálózatokban a beszélgetés és az adatok továbbítása védett és biztonságos.

A rendszer legfontosabb alkotóelemei: a mobil készülék, a bázisállomás és a kapcsolóközpont. A mobil készülék egy olyan rádiós adó-vevő berendezés, amelyben egy cserélhető chip, a SIM-kártya[17] tartalmazza az előfizetői és számlainformációkat. A mobil készülék rádiófrekvenciás kapcsolaton keresztül kommunikál a bázisállomással. A bázisállomás egy felügyelet nélküli, állandó helyű rádió adó-vevő berendezés, amely interfészként működik a mobil készülék és a kapcsolóközpont között. A kapcsolóközpont a hálózat legbonyolultabb része, amelynek feladata a hagyományos telefonközpontoknál megszokott hívási és kapcsolási feladatok ellátása mellett többek között az előfizetői adatok tárolása, kezelése, a készülék pillanatnyi helyének folyamatos

[13] Global System for Mobile Communications, eredetileg Groupe Spécial Mobile – GSM.
[14] Time Division Multiple Access – TDMA.
[15] Code Division Multiple Access – CDMA.
[16] Frequency Division Multiple Access – FDMA.
[17] Subscriber Identity Module – SIM.

nyilvántartása, a számlázási rendszer üzemeltetése és az egész rendszer felügyelete. A mobilhálózat a központon keresztül tartja a kapcsolatot az egyéb telefonrendszerekkel.

A GSM-rendszer 1991-ben kezdte meg működését a 900 MHz-es frekvenciasávban. A 2G-rendszert alapvetően beszédhang átvitelére tervezték, és csak nagyon kicsi, 9,6 kbit/s átviteli sebességgel rendelkezett, amely a beszéden kívül csak rövid szöveges üzenetek (SMS)[18] továbbítására volt alkalmas. Az adatsebesség növelése céljából még ebben az évben elkezdték kidolgozni, és az évtized közepétől bevezetni az 1800 MHz-es sávban működő DCS rendszert[19] (2,5G), amelyben a GPRS-technológiát[20] alkalmazva már akár 115 kbit/s sebességű adatkommunikációra is lehetőség volt. A következő lépcső az EDGE[21] modulációs technológia volt, amely már 384 kbit/s sebességű hozzáférést tett lehetővé a hálózati infrastruktúra megváltoztatása nélkül. Ugyanakkor az adatátvitel rohamos növekedése egyre nagyobb átviteli sebességet igényelt, ami szükségessé tette egy új, más technológiai alapon nyugvó 3G mobil rádiótelefon-rendszer bevezetését.

Európában a 3G-hálózatok az UMTS-technológiát[22] használják. A technológia a WCDMA[23] szélessávú kódosztásos hozzáférési módra épül, amely ugyanakkor visszafelé kompatibilis a GSM-rendszerben alkalmazott technológiával. A WCDMA a CDMA-n alapuló technológia, amely a nagyobb sávszélességet azzal biztosítja, hogy az adatátvitel nem egy szűk frekvenciasávban, hanem a rendelkezésre álló frekvenciatartományban szétterítve történik. Ezt kiterjesztett spektrumú technikának is nevezik, amelyet a katonai hírközlésben is előszeretettel alkalmaznak a rádiófelderítéssel szemben. Kezdetben a 3G-rendszerekben elérhető 2 Mbit/s adatátviteli sebesség a HSPA-technológi-

[18] Short Message Service – SMS.
[19] Digital Cellular System – DCS.
[20] General Packet Radio Service – GPRS.
[21] Enhanced Data Rates for Global Evolution – EDGE.
[22] Universal Mobile Telecommunication System – UMTS.
[23] Wideband Code Division Multiple Access – WCDMA.

ának[24] köszönhetően maximálisan 14,4 Mbit/s lett, ami jelentős előrelépés a GPRS és az EDGE pár száz kbit/s adatsebességéhez képest. (Forstner–Ekler–Kelényi 2008)

Mint látjuk, napjainkra a mobiltávközlési hálózatokban a legfőbb fejlesztési irány az adatátviteli sebesség növelése. Az interneten keresztüli nagy felbontású videókhoz és egyéb, nagy sávszélességet igénylő szolgáltatásokhoz való hozzáférés igénye alapvetővé vált. Az ezt lehetővé tevő legnagyobb adatátviteli sebességet ma a 4G-s LTE-rendszerek[25] biztosítják. Az LTE egy IP-alapú,[26] csomagkapcsolt adatátvitelt megvalósító, széles sávú, nagy sebességű mobiltávközlési rendszer. Az LTE-hálózatban elérhető elméleti adatátviteli sebesség kezdetben több 10 Mbit/s volt, mára pedig a technológiai fejlesztéseknek köszönhetően akár a néhányszor 100 Mbit/s-ot is elérheti.

Hazánkban 1994-ben a Westel 900 és a Pannon GSM kezdte meg digitális mobiltelefon-szolgáltatását, aminek köszönhetően a 2000-es évek elejére az analóg szolgáltatás teljesen kiszorult. A Vodafone létrejöttével megjelent a harmadik piaci szereplő is, amely 2003 tavaszán elsőként indította el MMS-szolgáltatását.[27] A korábban Westel 900 néven működő T-Mobil 2005-ben kezdte meg elsőként 3G-s szolgáltatását a 2,1 GHz-es sávban, amelyhez néhány hónap múlva a másik két szolgáltató is csatlakozott. 2010 után mindhárman megkezdték a 4G-s LTE-infrastruktúra kiépítését, aminek köszönhetően a Telekom 2012. január 1-jén elsőként indította el új széles sávú mobilhálózati szolgáltatását. (Koi 2010)

Mindeközben a nyilvános mobilrendszerek mellett megjelentek a diszpécsercélú földi mobilhálózatok is, amelyek egymástól függetlenül egy-egy szervezet, intézmény vagy vállalat mobilkommunikációs igényeit elégítik ki. Ilyen rendszer a TETRA,[28] amely a GSM-hez

[24] High-Speed Packet Access – HSPA.
[25] Long Term Evolution – LTE.
[26] Internet Protocol – IP.
[27] Multimedia Messaging Service – MMS.
[28] Terrestrial Trunked Radio – TETRA.

hasonlóan szintén a második generációs európai mobilszabványcsalád része. Egy olyan cellás elven működő földfelszíni, nyalábolt rádiórendszer, amely egyaránt képes kiszolgálni a védelmi szféra (honvédség, rendőrség, mentők, katasztrófavédelem, határőrség stb.), valamint a polgári felhasználók diszpécserrendszerű, speciális kommunikációs igényeit. A rendszer a beszédkapcsolat mellett adatátvitelt is biztosít, bár alacsony átviteli sebességgel. Az egymáshoz meghatározott közelségben levő készülékek egymással a központi hálózat használata nélkül is képesek kommunikálni, tehát a TETRA-rendszerű készülékek a központi hálózat által le nem fedett (árnyékolt) területeken is használhatók. (Haig–Várhegyi 2005)

A TETRA-rendszer kifejlesztését az Európai Távközlési Szabványügyi Intézet (ETSI)[29] kezdte meg 1989-ben mobil digitális trönkölt rádiórendszer[30] néven, majd 1997-től kezdődően több száz TETRA-rendszer kezdte meg működését szerte a világon. Hazánkban a 380–400 MHz-es frekvenciasávban működő TETRA-rendszerű EDR-hálózat[31] kialakítása 2005-ben kezdődött. A hálózatban – amelynek kiépítése 2006 végére befejeződött – 270 bázisállomás működik, amelyek 42 ezer készülék használatának technikai háttérbázisát biztosítják. (T-System 2012)

1.4. A műholdas rendszerek kibontakozása

1.4.1. A műholdas távközlés fejlődése

A földfelszíni mobiltávközlés mellett egy másik vezeték nélküli kommunikációs technológia is hatalmas ütemű fejlődésen ment keresztül az elmúlt hatvan évben. Ez a műholdas távközlés, amelynek ötlete

[29] European Telecommunications Standards Institute – ETSI.
[30] Mobile Digital TRunked Radio System – MDTRS.
[31] Egységes Digitális Rádiórendszer – EDR.

Arthur Charles Clarke sci-fi-írónak egy 1945-ben a *Wireless World* tudományos szaklapban megjelent írásából származik. Clark javaslata szerint a második világháborúban kifejlesztett német rakétatechnológiát békés célra felhasználva a világűrbe lehet juttatni olyan geostacionárius pályán[32] keringő műholdakra szerelt rádiórelé-berendezéseket, amelyekkel a Föld bármely pontja kommunikációs szempontból elérhető.

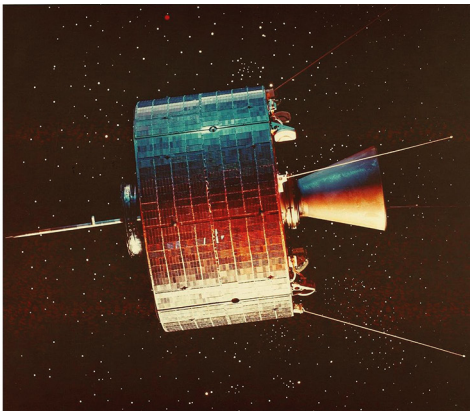
A műholdak pályára állításához szükséges rakétatechnológia kifejlesztése Wernher von Braun német tudós nevéhez fűződik, aki a V-2 rakéta megalkotója volt. A háborút követően Braun az Egyesült Államokban folytatta kutatásait, aminek eredményeként az általa irányított kutatócsoport egy folyékony hajtóanyaggal működő rakétát fejlesztett ki. Az amerikai kutatások ellenére mégis a Szovjetunió volt az, amely először képes volt műholdat a világűrbe juttatni. Ez volt az 1957. október 4-én alacsony Föld körüli pályára állított Szputnyik-1 műhold, amely 20 és 40 MHz-es frekvencián, 1 W-os teljesítménnyel sugárzott jellegzetes „bip-bip” csipogó jeleket, amelyeket a rádióamatőrök képesek voltak venni.

Az első kommunikációs célú kísérleti műholdat a Score-t az Egyesült Államok légiereje juttatta fel a világűrbe 1958. december 18-án. A Score által továbbított első értelmes üzenet Eisenhower amerikai elnök 1958-as karácsonyi üdvözlete volt a világnak. Röviddel ezután, 1962. július 10-én az első kontinensek közötti műholdas műsorszórást biztosító Telstar I. műholdat is útjára indították, amely július 23-án sugározta az első nyilvánosan is fogható adását [11. a) kép]. Mivel azonban a Telstar nem geostacionárius pályán keringett, ezért a kommunikációra csak két és fél óránként, húsz percig volt lehetőség. A Clark által javasolt első működő geostacionárius pályán keringő műhold a Syncom II volt, amelyet 1964. július 26-án indítottak el, és állítottak a közel 36 000 km-es magas-

[32] Az Egyenlítő síkjában lévő Föld körüli pálya, amelyen a műholdnak a keringési ideje megegyezik a Föld forgási periódusával, és így a műhold a Föld bármely pontjáról mindig azonos helyen, látszólag mozdulatlannak látszik.

ságban lévő pályára. [11. b) kép] Ez a műhold Amerika, Európa és Afrika között biztosított folyamatos lefedettséggel telefon- és telefaxkapcsolatot. (Huurdeman 2003)

11. a) kép
Telstar műhold
Forrás: Telstar II. (1964)



11. b) kép
Syncom II. GEO-műhold
Forrás: Syncom II. (2012)

Az első ténylegesen működő kereskedelmi célú, globális műholdas távközlési szolgáltatás megindítása az Intelsat rendszerhez köthető. Az Intelsat egy nemzetközi műholdas távközlési szervezet a globális műholdas szolgáltatási igények kielégítésére, amely 1964. augusztus 20-án jött létre 11 ország kezdeményezésére. A szervezet 1965. április 6-án állította pályára az Intelsat-1 (Early Bird) műholdat, amelyet röviddel ezután több is követett. Ezzel elindult a világ első, valóban működő kereskedelmi célú műholdas távközlési rendszere, amely mára 52 aktív műholddal és több száz földi állomással biztosít az előfizetők számára távközlési szolgáltatást. (Intelsat é. n.)

A távközlési műholdak hosszú távú működtetéséhez az elektroncsöveket felváltó, hosszú élettartamú és megbízható működésű félvezető technológia megjelenésére volt szükség. A félvezető és integrált

áramköri technológia fejlődésének köszönhetően a kezdeti néhány hónaptól a 2000-es években 15 évre emelkedett a műholdak működési élettartama. A 70-es évektől kezdődően a távközlési műholdak pályára állításának üteme is felgyorsult. A globális lefedettséget biztosító műholdas rendszerek mellett a Föld különböző országai, régiói saját műholdakat bocsátottak fel (például Eutelsat, Arabsat, PanAmSat, AsiaSat stb.), biztosítva ezzel a kommunikációs igényük regionális kielégítését. Ma már a földfelszíni mobil cellás távközlő rendszerek mellett a műholdas távközlő rendszerek is jelentős szerepet játszanak a kommunikációs feladatok megoldásában. Napjainkra különböző műholdas távközlési szolgáltatások állnak a felhasználók rendelkezésére, amelyek a Föld olyan területein is képesek kommunikációs szolgáltatást nyújtani, ahol a földfelszíni rendszerek nem.

A műholdas rendszerek a felhasznált pályától függően lehetnek:

- alacsony pályán mozgó (LEO);[33]
- közepes pályán mozgó (MEO);[34]
- geostacionárius pályán mozgó (GEO);[35]
- Molnyija-pályán mozgó rendszerek.

A GEO-műholdak, mint ahogy korábban írtuk, mintegy 36 ezer km magasságban helyezkednek el, és a keringésük szögsebessége pontosan megegyezik a Földével, így a Földről állni látszanak. A GEO-műholdakat főleg rádió- és televízióműsor-szórásra lehet előnyösen használni, de általános célú beszéd- és adatátvitelre, nagy sávszélességű internet-hozzáférésre, valamint VSAT-rendszerek megvalósítására is használják. Ilyen műholdakat alkalmaznak például az Eutelsat, Intelsat, Inmarsat, Thuraya rendszerek. A rendszer hátránya, hogy az Északi- és Déli-sark nem látszik, előnye pedig, hogy nincs szükség mozgó műholdkövető berendezésekre.

---

[33] Low Earth Orbit – LEO.
[34] Medium Earth Orbit – MEO.
[35] Geostationary Earth Orbit – GEO.

A MEO-műholdak mintegy 7–20 ezer km magasságban találhatók, és általában navigációra használják, mint például a Navstar GPS, a Glonass vagy a Galileo.

A LEO-műholdak mintegy 700–1600 km magasságban keringenek, és a GEO-rendszerekkel ellentétben a műholdak egymással is képesek kommunikálni. A LEO-rendszerek, mint például az Iridium, Globalstar, Inmarsat és Odyssey, nagyszámú műhold segítségével folytonos és valós idejű, keskeny sávú adatátvitelre alkalmasak (adat és hang), de az igény szerinti sávszélesség biztosítása nem lehetséges. A LEO-műholdak katonai jelentősége egyre növekszik, mivel válság vagy háború esetén az ilyen típusú műholdakat gyorsan az adott hadszíntér fölé lehet juttatni. (Haig–Várhegyi 2005)

A 80-as években – az atomfegyverek jelentette fenyegetésnek és az elektronikai hadviselésnek köszönhetően – a katonai híradással szemben is fokozottabb követelmények jelentkeztek. Az akkori harctéri rádiórendszerek védtelenek voltak az atomrobbanás keltette elektromágneses impulzusok, valamint az elektronikai zavarok ellen, az elektromágneses kompatibilitási képességük is gyenge volt. 1982-ben a felsorolt hiányosságok megszüntetésére és a hírrendszer tökéletesítésére az USA védelmi minisztériuma új programot indított el Milstar[36] néven, amelynek feladata az összes haderőnem és fegyvernem centralizált vezetésének kommunikációs biztosítása, különös tekintettel a hadászati rendeltetésű erőkre. A Milstar a repülőgépeket, a tengeralattjárókat, a kontinensek közötti ballisztikus rakéták indítóhelyeit, a stratégiai és harcászati vezetési pontokat kapcsolja össze GEO-rendszerű műholdas csatornákon keresztül. Az első műholdat 1994. február 7-én állították GEO-pályára, a rendszer teljes kiépítése pedig 2003-ban fejeződött be.

A rendszer a milliméteres hullámtartományban működik, a Földműhold közötti összeköttetésre a 43,5–45,5 GHz sávot, a műholdműhold viszonylatra pedig a 60 GHz-es tartományt használják. A GEO-

[36] Military Strategic and Tactical Relay – MILSTAR.

pályán keringő két Milstar Block I műhold alacsony sebességű (LDR)[37] adatátvitelre alkalmas, amely egy időben 192 csatornán biztosít hang- és adatkapcsolatot 75–2400 bit/s sebességgel. Ezzel szemben a három Milstar Block II műhold egyidejűleg 32 csatornán egyaránt alkalmas alacsony és közepes sebességű adatátvitelre (MDR)[38] 4,8 kbit/s és 1,544 Mbit/s között. A Föld-műhold irányban az információ továbbítására FDMA, a műhold-Föld irányban pedig TDMA többszörös hozzáférést alkalmaznak. A földi szegmensben a SMART-T[39] és a SCAMP[40] hordozható, milliméteres hullámsávú terminálok biztosítják a kommunikációt. (Haig–Várhegyi 2005; Milstar 2015) A 2. ábra a Milstar rendszer struktúráját szemlélteti.

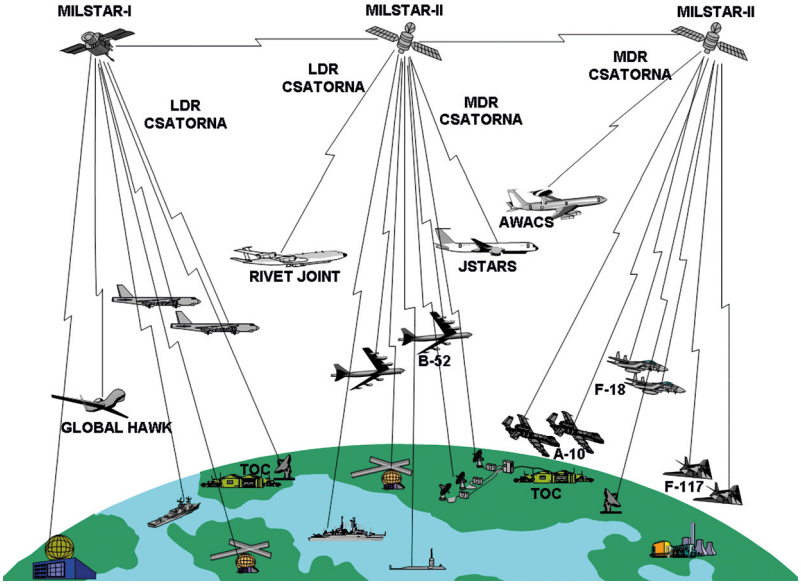
A rendszer kialakításakor nagy figyelmet fordítottak a zavarvédettségre, amelynek érdekében:

- milliméteres hullámsávot alkalmaznak, amely jó felderítés és zavarás elleni védelemmel rendelkezik;
- az üzemi frekvencia álvéletlen áthangolásával zajszerű jelek adásvételét alkalmazzák;
- adaptív vevőantennát használnak, valamint
- különféle iránykarakterisztikák alkalmazásával az antenna manőverezőképességét növelik. (Haig–Várhegyi 2005)

2010-ben az USA hadereje megkezdte a Milstar rendszer korszerűsítését a vele kompatibilis AEHF-rendszerrel,[41] és 2013-ig már három műholdat állítottak rendszerbe. Az AEHF-műholdak a meglévő Milstar-funkciók mellett 8,192 Mbit/s-os, megnövelt adatátviteli sebességet (XDR)[42] és több csatornát is biztosítanak, mindezzel pedig jelentősen javítják a rendszer kapacitását. A több sugárnyalábbal rendelkező, fej-

[37] Low Data Rate – LDR.
[38] Medium Data Rate – MDR.
[39] Secure Mobile Anti-Jam Reliable Tactical Terminal – SMAR-T.
[40] Single Channel Anti-Jam Man-Portable – SCAMP.
[41] Advanced Extremely High Frequency – AEHF.
[42] Extended Data Rate – XDR.

lett antennatechnika jelentősen növeli a rendszer világméretű lefedettségét, javítja a kis méretű antennákkal rendelkező földi terminálokkal való kapcsolatot, aminek köszönhetően gyorsabbá válik az összeköttetés létrehozása. (AEHF é. n.)



2. ábra

A Milstar rendszer

Forrás: Haig–Várhegyi 2005

1.4.2. A műholdas navigáció kialakulása

A távközlés mellett a műholdas rendszerek egy másik, mára teljesen elterjedt alkalmazási módja a helymeghatározás. A helymeghatározás igénye egyidős a hajózással, fejlődése az elmúlt évszázadokban hatalmas utat járt be. Jelenleg többféle navigációs eljárás ismert, amelyek

az autonóm vagy nem autonóm navigációs rendszerek közé sorolhatók. Az autonóm navigációs eljárásnál a helymeghatározáshoz az adott hordozó fedélzetén elhelyezett berendezéseken kívül más külső eszköz nem szükséges. Ezzel szemben a nem autonóm rendszereknek a fedélzeti egységeiken kívül földi vagy műholdas segédberendezései is vannak, amelyek nélkül a működtetésük nem lehetséges. Az elmúlt évszázadokban alkalmazott különböző hagyományos, autonóm navigációs megoldások mellett a 20. században – az elektronika fejlődésének köszönhetően – az elektronikus navigációs módszerek jelentős fejlődésen mentek keresztül. A második világháborúban többféle nem autonóm eljárást is kifejlesztettek, amelyek közül néhányat korábban ismertettünk. A háborút követően továbbfejlődött a navigáció, és újabb földi navigációs megoldások születtek, mint például:

- a VHF-sávban működő rádióiránytűs rendszerek, például a VOR/DME;[43]
- a LORAN, a DECCA vagy az OMEGA globális hiperbolikus navigációs rendszerek, valamint
- a földi, kódolt jeleket sugárzó rendszerek, mint például a harcászati légi navigációs rendszer, a TACAN.[44] (Haig–Várhegyi 2005)

Az első műholdas navigációs rendszert az USA haditengerészete kezdte el fejleszteni 1958-ban. A hadihajók és tengeralattjárók pozíciójának meghatározására kialakított NSSS[45] vagy más néven Tranzit-rendszer – az első műhold 1961. április 13-ai pályára állítását követően – 1964-ben kezdte meg működését. A rendszerben négy műholdat alkalmaztak egy kb. 1000 km-es magasságú, kör alakú, poláris pályán. A helymeghatározás a Doppler-elv alapján történt, miszerint a vevőberendezés egy adott időtartományban a hajó és a műhold távolságának változása alapján határozta meg a saját helyzetét. A 90-es évek elejéig

[43] VHF Omnidirectional Range/Distance Measurement Equipment – VOR/DME.
[44] Tactical Air Navigation – TACAN.
[45] Navy Navigation Satellite System – NSSS.

alkalmazott rendszer pontossága 100 m-es volt, ami a hajók navigációjához még elegendőnek bizonyult. (DANCHIK– PRYOR 1990)

1973-ban az amerikai védelmi minisztérium megkezdte egy megbízhatóbb, pontosabb és stabilabb műholdas navigációs rendszer kifejlesztését, amely a Navstar GPS[46] nevet kapta. A rendszer kiépítésének első üteme 1978-tól 1985-ig tartott, amelynek során 10 db Block I műhold MEO-pályára állítására került sor. A második ütemben, 1989–1997 között pedig 28 db Block II műholdat indítottak el. A Navstar GPS rendszere nem teljes kiépítésben 1990 decemberében kezdte meg működését.

A GPS rendszer polgári célú felhasználását – annak teljes körű kifejlesztése után – Ronald Reagan amerikai elnök rendelte el, miután 1983-ban a koreai légitársaság KAL-007-es járata letért útvonaláról, és a Szahalin-sziget fölött a szovjet légvédelem lelőtte. Kezdetben a polgári felhasználás korlátozott volt, csak szelektív elérhetőséget tett lehetővé, mivel a teljes pontosság kizárólag a katonai célra volt fenntartva. Ennek megszüntetését Clinton amerikai elnök 2000. május 1-jével rendelte el. (Radio-Electronics.com é. n.)

A GPS rendszer három alapvető alrendszerből épül fel:

- a műholdas alrendszerből;
- a felhasználói rendszerből (vevőkészülékek és szolgáltatások), és
- a vezérlőrendszerből (földi vezérlő- és monitorállomások).

A műholdas alrendszer teljes kiépítésében 24 műholdat tartalmaz. A műholdak hat, az egyenlítő síkjával 55°-os,[47] egymástól pedig 60°-os szöget bezáró, közel kör alakú MEO-pályán keringenek a Föld körül 20 200 km magasságban. A műholdak számát és elrendezését az határozza meg, hogy a Föld felszínén, egy adott pontról legalább négy műhold sugárzását lehessen venni a vevőkészülék antennájával.

[46] Navstar Global Positioning System – Navstar GPS.

[47] Inklináció (pályahajlás): egy műhold pályájának a koordinátarendszer alapsíkjával bezárt szöge.

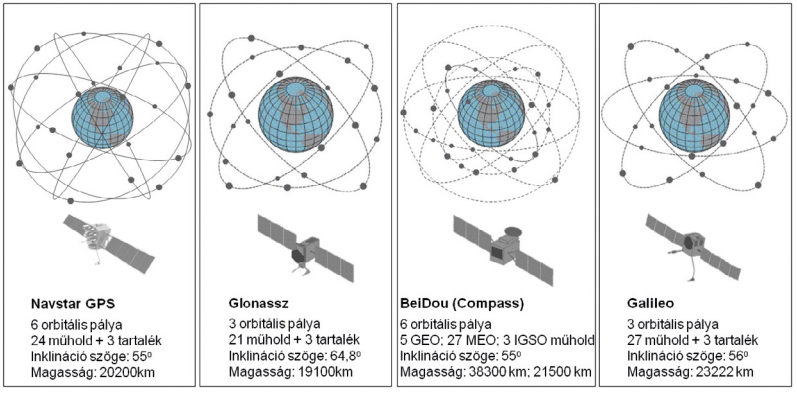
A földi vezérlőrendszer a Colorado Springsben lévő központi vezérlőállomásból és négy monitorállomásból áll. A földi vezérlőrendszer folyamatosan figyeli és ellenőrzi a műholdak működését, pályaadatait, szükség esetén pályakorrekciós jeleket sugároz a műholdak felé, illetve elvégzi a műhold fedélzeti óráinak szinkronizálását, a pontos idő beállítását.

A GPS rendszer a felhasználó helyzetét távolságmérés elve alapján határozza meg. Ehhez a műhold által kisugárzott jel terjedési idejének nagypontosságú mérése és a Föld körüli MEO-pályán keringő műholdak helyzetének pontos ismerete szükséges. A nagypontosságú időméréshez minden műholdon igen pontos cézium és rubídium atomórák találhatók, amelyek abszolút pontossága eléri a 10^{-13}–10^{-14} értéket. A GPS-műholdak két jelet sugároznak. Az első jel vivőfrekvenciája L1=1575,42 MHz, a másodiké L2=1227,60 MHz. Mindkét vivőfrekvenciát modulálják a 10,23 MHz-es P(Y)[48] kóddal. Az L1 vivőfrekvenciát ezenkívül modulálják még az 1,023 MHz-es C/A kóddal.[49] A P(Y) kód nagyobb, a C/A kód kisebb pontosságot biztosít. (Papp 2003) Az ismert pozíciójú GEO-műholdak által sugárzott jeleket a vevőkészülék veszi, majd a mérési adatokból és a jelfeldolgozás eredményéből határozza meg a saját helyzetét.

Mára a Navstar GPS-en kívül más műholdas helymeghatározó rendszerek is léteznek, amelyeket a felhasználók egy egységes globális műholdas navigációs rendszerként (GNSS)[50] használhatnak. Ezek az orosz Glonassz, a kínai BeiDou vagy más néven Compass, illetve az európai Galileo, amelyek jelenleg még különböző kiépítettségben vannak (lásd 3. ábra). A rendszerek működési módja, az alkalmazott frekvenciák, illetve a jelstruktúráik különböznek egymástól. Ennek ellenére több mai felhasználói készülék már alkalmas a GPS- és a Glonassz-műholdak vételére. A GNSS alkalmazásának előnye,

[48] Precision Code.
[49] Coarse/Acquisition Code.
[50] Global Navigation Satellite System – GNSS.

hogy több független rendszert, így több műholdat észlelve nő a helymeghatározás biztonsága, integritása és pontossága.



3. ábra

A GNSS rendszer várható teljes kiépítettségben

Forrás: GEOG 862 (é. n.) alapján a szerző szerkesztése

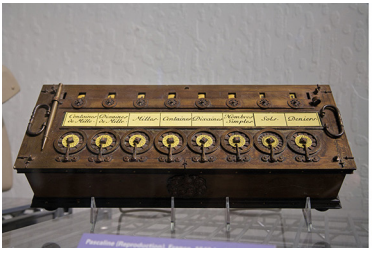
1.5. A számítógép fejlődéstörténete

1.5.1. A nagyszámítógépek kora

Mint azt korábban láttuk, a 20. században az információ gyűjtése, feldolgozása és továbbítása a társadalom működésének kulcsfontosságú elemévé vált. Az információs igények kielégítésére a kutatások eredményeként sorra jelentek meg olyan elektronikai információs eszközök, rendszerek és hálózatok, amelyek többek között olyan berendezéseket foglaltak magukban, mint például az előzőekben bemutatott telefon, rádió, televízió, rádiólokátor, navigációs berendezés, műholdas eszközök stb. Mindezek mellett az évszázad egyik leginnovatívabb technológiája is megszületett, amelyik máig meghatározója, alakítója a társadalmi-gazdasági folyamatoknak, ezáltal pedig a fejlődés legfőbb motorjává

vált. Ez pedig nem volt más, mint a számítógép és később azok összekapcsolt hálózata. Amíg azonban a napjaink technológiájának megfelelő számítógépet és a számítógép-hálózatokat megalkották, addig több, a számítástudományhoz kapcsolódó eredmény is született az elmúlt évszázadokban is.

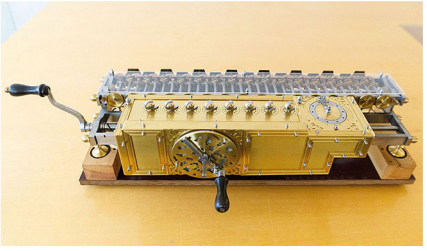
A számítás tudománya a hajózás és a kereskedelem fejlődésének köszönhetően már az ókorban is foglalkoztatta az embert. Az első kezdetleges számoló szerkezet az *abacus* volt, amelyet a Wilhelm Schickard matematikus és csillagász által 1623-ban megépített, golyókkal (kavicsokkal) működő számológép követett. 1645-ben pedig Blaise Pascal francia matematikus készített egy összeadásra és kivonásra alkalmas szerkezetet, amelyet Pascaline-nak nevezett el [12. a) kép]. Pascalt követően Gottfried Wilhelm von Leibniz német matematikus 1672-ben épített egy léptetőhengerrel, más néven „Leibniz kerékkel" működő számológépet, amely már mind a négy alapműveletet automatikusan oldotta meg. [12. b) kép] Fontos mérföldkő volt a Joseph Marie Jacquard nevéhez fűződő lyukkártya feltalálása is, amely a szövés folyamatát automatizálta 1805-ben. Jacquard a szövőmintának megfelelő helyen kilyukasztott kártyasorozatot alkalmazott, amely a későbbi programvezérlés elvét alapozta meg. (O'Regan 2012)



12. a) kép

Blaise Pascal Pascaline nevű számológépe

Forrás: Pascalin (2008)

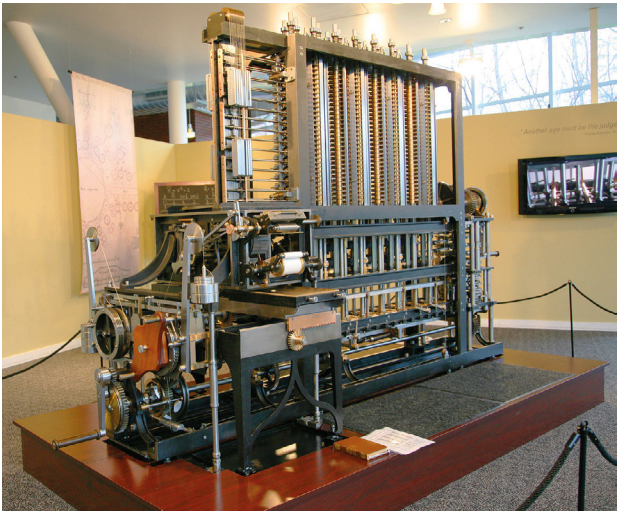


12. b) kép

Leibniz léptetőhengeres számológépének rekonstrukciója

Forrás: Leibniz (2016)

Az 1830-as évek közepén Charles Babbage analitikus gépe már tartalmazott egy memóriaegységet, egy lyukkártyás soros vezérlőegységet, valamint más, a mai számítógépekben is használatos alkotóelemeket. Babbage gépe a kor technikai színvonala miatt nem épülhetett meg, de az 1937-ben megtalált feljegyzései alapján brit tudósok 1991-ben megépítették az úgynevezett „Difference Engine No. 2-t" (13. kép). A lyukkártyás adattárolást Herman Hollerith fejlesztette tovább, akinek gépét az 1889-es amerikai és az 1910-es német népszámlálásban is alkalmazták. (Baló–Lipovecz 1988)



13. kép

A Babbage elképzelése szerint megépített Difference Engine No. 2

Forrás: Difference Engine (2010)

A mai értelemben vett számítógépek megalkotása felé vezető úton jelentős mérföldkő volt a német Konrad Zuse találmánya. Zuse, miután sikereket ért el a Z1 és Z2 nevű mechanikus eszközeivel, 1941-ben világelsőként megalkotta a Z3 elnevezésű, szalagos tárolású, programozható gépét (14. kép). A Z3 2600 db relével, bináris számrendszerben, 5 Hz-es

órajellel már képes volt lebegőpontos aritmetikai műveleteket végrehajtani. A beviteli egysége egy decimális billentyűzet, kimenete pedig egy lámpasor volt, amely a számolás eredményeit jelenítette meg. Ez volt a világon az elsőként megalkotott digitális számítógép.

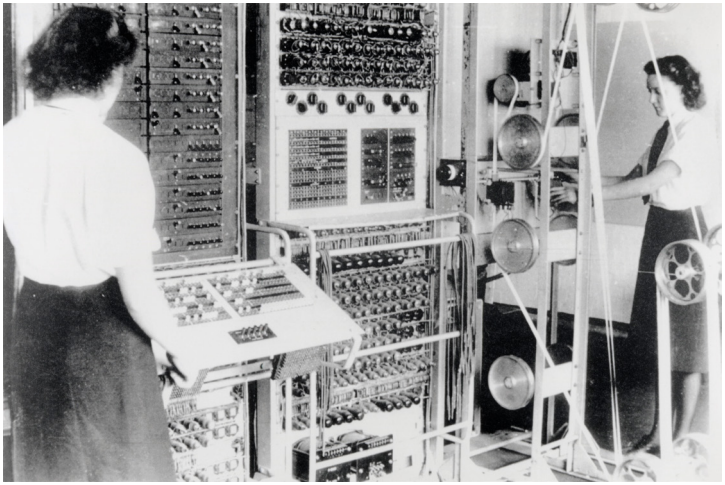
14. kép

Konrad Zuse Z3 mechanikus relés számítógépének másolata

Forrás: ZUSE Z3 (é. n.)

A mai értelemben vett korszerű, elektronikai áramkörökre épülő számítógépek megalkotása azután valósulhatott meg, miután a már korábban ismertetett vákuumcsövek és később a félvezetők megszülettek. Az elektroncsövek fejlődésének köszönhetően a Z3 számítógép után egy évvel, 1942-ben John Atanasoff egy diákjával, Clifford Berryvel megépítette az első elektronikára épülő digitális számítógépet, a 270 db elektroncsövet tartalmazó ABC-t. Az ABC egy lineáris egyenletek megoldására tervezett célszámítógép volt, amelynek nem volt még központi egysége, és programozni sem lehetett. Ugyanakkor úttörőnek számított, mivel a számításokat elektronikával vezérelve végezte, illetve külön-külön számítási egységet és memóriaegységet tartalmazott.

A második világháborúban a hatékony légvédelmi, tüzérségi ballisztikai számítások és a titkosított információk megfejtése is rendkívül számításigényes feladatnak mutatkozott. Közülük is kiemelkedett a német Enigma által kódolt üzenetek megfejtése, mivel azt kézi úton lehetetlen volt feltörni. A Bletchley Parkban a brit Alan Turing vezette kódfejtő csoport először a lengyelek által épített szerkezet továbbfejlesztett változatát, egy elektromechanikus számítógépet, a tárcsás „Turing-bombát" alkalmazta. Később az Enigma bonyolultabb kódolása, illetve a Lorenz SZ40/42 kódoló alkalmazása miatt 1944 elején megalkották a Colossust, amelyben 1500 db 15 kW teljesítményszükségletű vákuumcső volt, ami a számítási kapacitást jelentősen megnövelte (15. kép). A gép szintén a „nyers erő" módszerével fejtette meg a kódolt üzeneteket, de a korábbi több órán át tartó desifrírozás helyett ez néhány perc alatt megtörtént. (O'Regan 2012)



15. kép

A Colossus

Forrás: Colossus (1943)

Szintén a háborús években kezdődött el a világ egyik első nagy méretű, általános célú elektronikus digitális számítógépének az ENIAC-nak[51] a fejlesztése is a Pennsylvania Egyetemen, amelyet azonban csak 1946-ban fejeztek be. A hatalmas méretű számítógép 18 ezer elektroncsövet, 70 ezer ellenállást, 10 ezer kondenzátort és 6 ezer kapcsolót tartalmazott, hossza 30 m, magassága 3 m, szélessége 1 m, energiafelhasználása pedig 150 kWh volt. A számítógép a működése során több problémával is küzdött: a programozását lyukkártyákkal és kapcsolókkal kellett megoldani, a tízes számrendszerben dolgozott, emellett pedig a nagyszámú elektroncsőnek köszönhetően igen gyakran meghibásodott.

A mai napig használatos számítógép-architektúra kialakításában elévülhetetlen szerepet játszott Neumann János, aki az EDVAC[52] 1949-es tervezése és megépítése során fektette le a máig érvényes teóriáját. Ennek lényege, hogy a számítógép egy olyan tárolt programú, belső programvezérlésű, kettes számrendszert használó berendezés, amelynek főbb alkotóelemei a központi vezérlőegység, az aritmetikai egység, a memória, valamint a be- és kiviteli egység. Két évvel később, 1951-ben pedig megszületett az első általános célú kereskedelmi forgalomba került számítógép, az UNIVAC,[53] amelyet Presper Eckert és John Mauchly tervezett. Az Egyesült Államokban megépített számítógépek mellett Európában is intenzív számítástechnikai fejlesztések folytak a háború után. Ennek egyik első eredménye volt az EDSA,[54] amely az egyesült királyságbeli Cambridge-ben készült 1946-ban. Az első hazai számítógép pedig a még relés rendszerű MESZ-1 volt, amelyet Kozma László tervezett és épített meg 1955-ben. (Baló–Lipovecz 1988)

Az 50-es években a nagyobb teljesítményű számítógépek tervezésének és fejlesztésének egyik fontos hajtóereje volt a kétpólusú

[51] Electronic Numerical Integrator and Computer – ENIAC.
[52] Electronic Discrete Variable Automatic Computer – EDVAC.
[53] Universal Automatic Computer – UNIVAC.
[54] Electronic Delay Storage Automatic Calculator – EDSA.

világrend kialakulása. Mind a Szovjetunió, mind pedig az Egyesült Államok intenzív fegyverkezési versenybe kezdett, és nyilvánvalóvá vált, hogy a számítástechnika fontos szerepet játszik majd a kifinomult haditechnikai rendszerek fejlesztésében. Ennek első példánya volt az USA és Kanada légterének védelmét ellátó félautomatizált, számítógéppel támogatott SAGE[55] légvédelmi vezetési rendszer, amely a NORAD[56] rendszerében az 50-es évek végétől a 80-as évekig teljesített szolgálatot (16. kép). Feladata volt a radaroktól érkező légi célokra vonatkozó adatok elemzése és a légi helyzet információinak automatizált továbbítása az elfogó vadászgépek felé.

16. kép

SAGE félautomata légvédelmi vezetési rendszer

Forrás: SAGE (2005)

[55] Semi-Automated Ground Environment – SAGE.

[56] North American Aerospace Defense Command – NORAD.

1.5.2. A személyi számítógépek megjelenése

Az 50-es, 60-as években kifejlesztett számítógépek a méretük és az áruk miatt otthoni felhasználásra alkalmatlanok voltak. Ez vezette az olyan nagy gyártókat, mint például az IBM-t vagy a DEC-et arra, hogy már a 60-as években olcsóbb és kisebb méretű számítógépeket fejlesszenek. A tranzisztorok megalkotása, majd később Kirby integrált áramkörének köszönhetően lehetővé vált, hogy nagyszámú tranzisztort helyezzenek el egyetlen szilíciumlapkán. A mikroprocesszor megjelenése a 70-es évek közepétől hatalmas lökést adott a személyi számítógépek fejlesztéséhez. Az IBM volt az első, amely az IBM S/360 számítógépcsalád kifejlesztésével már az egyéni felhasználók és a vállalkozások számára is megfizethető, az igényeiknek is megfelelő számítógépeket hoztak forgalomba. (O'Regan 2012)

A miniatürizálásnak köszönhetően 1980-ra már olyan számológépek és kis méretű számítógépek jelentek meg, amelyek bár kisebb kapacitásúak voltak, de akár kézben is elfértek. Megjelentek azok a memóriaegységek (ROM,[57] RAM[58]), amelyekben az adat elérésének ideje független a tárban való elhelyezkedés helyétől. A mágnesszalagos adatrögzítés mellett a programok, adatok tárolására kezdetben 8"-os, majd 5,25"-os papírtokos, később 3,5"-os 1,41 MB kapacitású, műanyagházas, hajlékony mágneslemezeket (floppy) fejlesztettek ki. A beépített merevlemezes adattárolók (winchesterek) a kezdeti időben 10–100 MB kapacitásúak voltak, 1980-ra pedig megszületett a nagy sebességű lézeres adatrögzítés és adatkiolvasás technológiája. (Haig et al. 2013)

A 80-as évektől a személyi számítógépek megkezdték hódító útjukat. A kezdeti otthoni hobbiszámítógépek (Commodore 64, 128, Atari) után az IBM 1981-ben mutatta be az IBM PC-t,[59] amely

[57] Read Only Memory – ROM.
[58] Random Access Memory – RAM.
[59] Personal Computer – PC.

olcsóságánál fogva a kis méretű vállalkozások számára vagy otthoni személyes használatra egyaránt alkalmas volt. Az IBM által alkalmazott nyílt architektúra eredményeként sorra jelentek meg az olcsóbb, de IBM-kompatibilis PC-k, amelyekben már a Microsoft Corporation MS-DOS operációs rendszerét alkalmazták. Az áttörést az 1983-ban piacra dobott IBM PC XT, majd rá egy évre pedig az IBM PC AT hozta meg, amely már nagyobb memóriával, kétoldalas hajlékonylemezes meghajtóval, valamint nagy kapacitású merevlemezes meghajtóval is rendelkezett. Eközben az Apple is piacra dobta az IBM PC-től jelentősen különböző Macintosh gépét. A Macintoshnak sokkal felhasználóbarátabb grafikus interfésze volt, így sokkal egyszerűbb volt kezelni, mint a parancsvezérelt operációs rendszerrel rendelkező PC-ket. Ugyanakkor ez drágább is volt, mint az IBM PC, ami döntő fontosságúnak bizonyult a kétféle rendszer piaci elterjedésében. (O'Regan 2012)

A 90-es évektől a számítástechnika még intenzívebb fejlődési szakaszba lépett. A gyártástechnológiának köszönhetően a processzorok egyre fejlettebbek, nagyobb számítási kapacitásúak lettek. A PC-k az évek során az Intel 286, 386, 486, majd a Pentium sorozatú processzoraival kerültek piacra, napjainkra pedig már többmagos processzorok köré épülnek a számítógépek és a hordozható infokommunikációs eszközök. Az 1981-ben napvilágot látott, varrógéptáska méretű Osborne 1 hordozható gépet (17. kép), illetve az 1982-es GRiD Compass 1101 felhajtható kijelzővel rendelkező „noteszgépet" követően az asztali számítógépek mellett sorra jelentek meg az újabb, kisebb méretű, de nagyobb teljesítményű laptopok, notebookok. Mára a mobilitás követelményének eleget téve, akár egy tenyérben is elférnek azok a tabletek, okostelefonok és más okoseszközök, amelyek teljesítményben és szolgáltatásban akár nagyságrendekkel is felülmúlják a korábbi nagy méretű és nagy súlyú őseiket.

17. kép

Osborne 1, az első hordozható számítógép

Forrás: Osborne 1 (2010)

Mindeközben már a 70-es években megjelentek az első rosszindulatú programok is, amelyeket kezdetben azért írtak, hogy részben felhívják a figyelmet a rendszer sérülékenységeire, másrészt pedig, hogy készítőik elsőként legyenek képesek egy-egy rendszer feletti ellenőrzés megszerzésére. Az első feljegyzett vírust, a Creepert 1971-ben fedezték fel, amely az akkorra már kiépített ARPANET-hálózaton terjedt, és a TENEX operációs rendszert futtató számítógépeket fertőzte meg. Hatástalanítására alkották meg a Reaper nevű programot, amely így a világ első antivírusszoftverének tekinthető.

Az első személyi számítógépes vírust, az Elk Clonert 1982-ben írta Rich Skrenta, akkor 15 éves középiskolás, amely floppy lemezen keresztül terjedt, és az Apple DOS 3.3 operációs rendszerét fertőzte meg. (Judge 2014) A számítógépek megjelenésével és fejlődésével szinte egy időben tehát megjelentek a működésének korlátozását és a tárolt adatok törlését, kompromittálását végző kártékony programok is, amelyek napjainkra rendkívüli mértékben terjednek, és évről évre hatalmas károkat okoznak.

1.6. A számítógép-hálózatok evolúciója

1.6.1. A számítógép-hálózatok kialakulása

A távközlési hálózatok kialakulásával és nagy ütemű fejlődésével párhuzamosan a számítógépek egy adott fejlettségi szintjén felmerült a gépek összekapcsolásának igénye. A számítógépen tárolt adatok megosztása, a több helyről való hozzáférés lehetősége, az erőforrások elosztása, a párhuzamos munkavégzés lehetősége mind-mind olyan előny, amelyet a hálózatok biztosítanak a felhasználóknak.

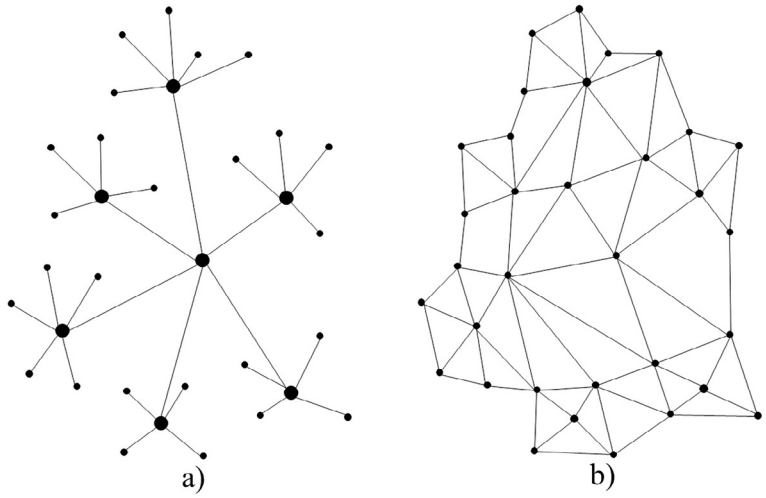
Tulajdonképpen az első számítógép-hálózatnak a már korábban említett SAGE félautomata légvédelmi vezetési rendszer tekinthető, amely a radaroktól érkező adatok feldolgozását követően a légvédelem elemei számára biztosította az aktuális légi helyzet információit. A SAGE 24 db irányítóközpontból és 3 harci irányítóközpontból állt, amelyeket nagy távolságú telefonvonalakon keresztül kapcsoltak össze.

A katonai alkalmazhatóság mellett a polgári életben is rövid időn belül felmerült a hálózatok kialakításának igénye, amely elsőként a légi közlekedésben vált valóra az IBM által 1960-ban létrehozott SABRE[60] félautomata repülőjegy-foglaló hálózatával. (O'Regan 2012) Ezzel megkezdődött a számítástechnika és a távközlés konvergenciája. Ugyanakkor ezek a rendszerek még vonalkapcsolt hálózatok voltak, amelyekben a telefonhálózat felügyeleti központjának kiesése esetén a kapcsolat megszakadt.

Mindeközben a 60-as évek hidegháborús időszakában felmerült az igény, hogy a decentralizált telefonhálózatra alapozott katonai kommunikációs rendszer és hálózat (mint például a SAGE) helyett egy biztonságosabb, akár több központ kiesését is elviselő rendszer épüljön ki. Erre Paul Baran találta meg elsőként a megoldást, amikor egy olyan hibatűrő hálózati topológiát gondolt ki, amely elosztott módon kapcsolta össze az egyes hálózati elemeket. Eszerint a hálózatban két adott

[60] Semi-Automated Business Research Environment – SABRE.

pont között az üzenet számos útvonalon haladhat, aminek következtében a hálózat kevésbé sérülékeny (4. ábra). Emellett az üzeneteket az adóoldalon csomagokra bontva kell továbbítani a hálózatban, amelyeket a vételi oldalon kell újra összeilleszteni. Baran ötlete volt tulajdonképpen a mai csomagkapcsolás alapja, amelyet azonban a megvalósítására felkért akkori vezető amerikai távközlési cég, az AT&T nem tartott megvalósíthatónak.



4. ábra

a) Decentralizált, vonalkapcsolt és b) elosztott, csomagkapcsolt hálózati topológia

Forrás: a szerző szerkesztése

Az ARPA[61] a védelmi célú kutatási eredmények hatékonyabb megosztása és felhasználása érdekében érdeklődött egy teljesen új elven kiépített hálózat kialakítása iránt, amely végül is a Baran által felvázolt elosztott topológiára és a csomagkapcsolás elvére épült. A hálózatban – akkori

[61] Advanced Research Project Agency – ARPA.

mércével mérve – nagyteljesítményű számítógépekből (IMP)[62] álló csomópontokat hoztak létre, amelyeket 56 kb/s-os bérelt vonalak segítségével kapcsoltak össze. Tulajdonképpen ezek töltötték be a mai routerként ismert hálózati eszközök szerepét. A kaliforniai egyetem hálózatfejlesztési munkacsoportja mindeközben megkezdte egy hálózati protokoll (NCP)[63] kidolgozását, amely meghatározta, hogy a hálózatban lévő számítógépek hogyan kommunikáljanak egymással. Mindezek alapján 1969 végére alkották meg azt a négy csomópontból álló kísérleti hálózatot, amelyet ARPANET-nek neveztek el, és amelynek első elemei az UCLA-n,[64] az UCSB-n,[65] az SRI-n[66] és a Utahi Egyetemen voltak. (Tanenbaum–Wetherall 2013)

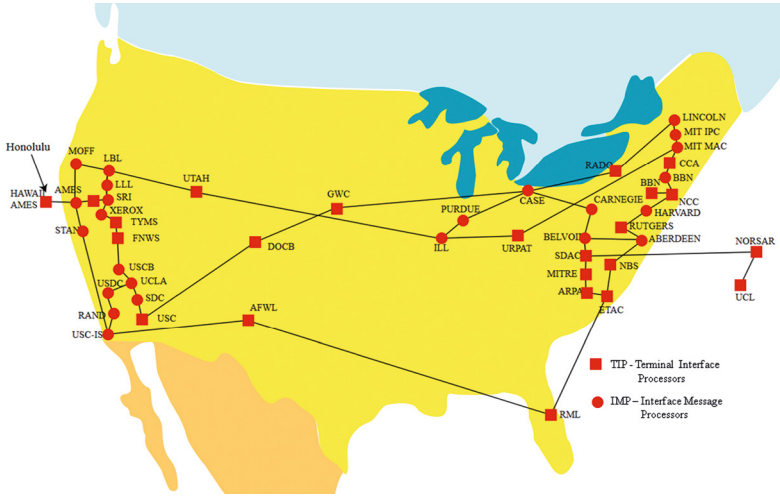
A hálózat fejlődésére mindeközben hatással voltak olyan munkavégzést jelentősen megkönnyítő programok, mint például a Telnet és az FTP.[67] Előbbi lehetővé tette, hogy egy számítógépre távolról is be lehessen jelentkezni, utóbbival pedig egy számítógép felhasználója más számítógépről volt képes fájlokat fogadni vagy arra küldeni. 1971-ben Ryan Tomlinson a @ jel bevezetésével megoldotta az elektronikus levelezés problémáját, és az e-mailezéssel lehetővé vált, hogy a hálózatban mindenki levelezhessen mindenkivel. Mindezeknek köszönhetően 1974-re – egyesült királyságbeli és norvég intézmények bekötésével – már több mint 30 egyetem, intézmény és szervezet csatlakozott az ARPANET-hálózathoz. (O'Regan 2012) (5. ábra)

Az amerikai kontinensen túli csomópontok bekötése az ARPANET-hálózatba azonban rávilágított az NCP hálózati protokolljának problémájára is, amely az eltérő interfészekből, csomagméretekből és az átviteli sebességből adódott. Ezt a korábbi protokoll nem tudta lekezelni, illetve nem rendelkezett vonali hibák elleni védelemmel, így el-

---

62 Interface Message Processors – IMP.
63 Network Control Protocol – NCS.
64 University of California at Los Angeles – UCLA.
65 University of California at Santa Barbara – UCSB.
66 Stanford Research Institute – SRI.
67 File Transfer Protocol – FTP.

veszett csomagok esetén gyakran leállt. Az ilyen problémákat kiküszöbölő TCP/IP-protokollt [68] Bob Kahn és Vinton Cerf mutatta be 1974-ben a Sussexi Egyetemen. A TCP-protokoll képes az eltérő csomagméreteket kezelni, illetve az elveszett csomagokat újra lekérni, így biztosítja a kommunikációt az eltérő paraméterű számítógépek, routerek és hálózatok között. Az IP-protokoll egy egyedi hálózati azonosító, illetve egy olyan kapcsolat nélküli protokoll, amely az egyes csomagok címzéséért és továbbításáért felel. A protokoll számos előnyös tulajdonsága ellenére csak 1983-tól vált szabvánnyá, és kezdték el alkalmazni az ARPANET-hálózatban.



5. ábra

Az ARPNAET 1974-es kiépítettsége

Forrás: ARPANET 1974 (2007)

Az ARPANET jó néhány éves megbízható működése után, 1983-ban a katonai hálózati elemet leválasztották róla, és létrehozták az önálló

[68] Transmission Control Protocol/Internet Protocol – TCP/IP.

MILNET-hálózatot. Ezen a hálózaton keresztül bonyolították a védelmi minisztérium nem minősített adatforgalmát. (NAUGHTON 2000) Ezt követően az ARPANET további helyi hálózatokkal[69] bővült, alapvetően kutatási célokat szolgált, és nyilvános felhasználású hálózattá alakult. A hálózat bővülése miatt a címzés egyre nehezebbé vált, aminek kezelésére megalkották a tartománynévrendszert (DNS),[70] amely az egyes gépeket tartományokba szervezi, és a hosztok neveit leképezi az IP-címükre. A DNS azóta is egy olyan megosztott adatbázist képez, amelyben az egyes hosztokkal kapcsolatos többféle információt is tárolnak.

Az ARPANET sikerét látva az Amerikai Nemzeti Tudományos Alap kezdeményezte egy már jól bevált technológiára alapozott hálózat kiépítését. Az NSFNET-nek[71] nevezett hálózat hat szuperszámítógépből álló és egymással 56 kbit/s-os adatátviteli vonalakkal összekapcsolt gerinchálózaton alapult, amelyhez később számos – egyetemeket, kutatóintézeteket, könyvtárakat stb. magukban foglaló – területi hálózat kapcsolódott. A kezdetekben már jelentkező túlterhelés miatt a 80-as évek végére optikai kábeles átviteli utakon keresztül is lehetőség volt a kapcsolat kialakítására, és így az 1,5 Mbit/s-os sebesség elérésére.

1990-ben egy nonprofit vállalkozás, az ANS[72] vette át a hálózat felügyeletét, aminek köszönhetően nevet is váltott ANSNET-re, és ezzel megindult a kereskedelmi hálózattá alakulása. A fejlesztéseknek köszönhetően a hálózatban az átviteli sebesség 45 Mbit/s-ra növekedett, mindezzel párhuzamosan pedig a mai világméretű hálózat alapját jelentő és számos technológiát bevezető ARPANET-hálózatot leállították. Ezen időszakban a világ számos országában, régiójában épültek ki elsősorban kutatási céllal az ARPANET-hez és az NFSNET-hez hasonló hálózatok, amelyek mind-mind felhasználták az előbbiekben tesztelt hálózati megoldásokat. Ilyen volt például Európában az EuropaNET és az EBONE

---

69 Local Area Network – LAN.

70 Name System – DNS.

71 National Science Foundation Network – NSFNET.

72 Advanced Networks and Services – ANS.

is, amelyek kezdetben 2 Mbit/s-os kapcsolattal működtek, és amelyet később 34 Mbit/s-ra növeltek. (Tanenbaum–Wetherall 2013)

1.6.2. Az internet fejlődése

A világméretű hálózat, az internet fejlődésének egyik fontos állomása volt 1990-ben a világháló, a World Wide Web (a továbbiakban: web) kifejlesztése, amelynek alapjait Tim Berners-Lee, a svájci CERN kutatóközpont munkatársa dolgozta ki. A világháló megalkotása lehetővé tette, hogy az internetet már ne csak az akadémiai, egyetemi szféra használja kutatási célokra, hanem az egyéni felhasználók számára is elérhetővé váljon. A világhálót a korábbi hálózatoktól számos unikális tulajdonsága különbözteti meg, mint például:

- az internetnek nincs egy központi irányító, felügyelő szervezete sem,
- az internetnek nincs egy központi vezérlő számítógépe sem,
- az interneten számítógépek milliárdjai kapcsolódnak egymáshoz,
- az internet nem egy fizikailag jól definiálható helyszínen található,
- az internet nem egy fizikailag megfogható dolog. (O'Regan 2012)

A web egy TCP/IP-protokollon alapuló olyan globális hálózat, amelynek hipermédia-adatbázisában szöveges dokumentumok, képek, grafikák, animációk, audio- és videofájlok találhatók. Ehhez az adatbázishoz az egyes oldalak egyedi URL-címének[73] a megadásával lehet hozzáférni. Az URL-cím tartalmazza:

- az átviteli protokollt, amelyet a célgéppel való kommunikációhoz használunk;
- a hosztgép vagy tartomány nevét;

[73] Uniform Resource Locator – URL.

- a hálózati port számát, amelyen az igényelt fájl vagy szolgáltatás elérhető a szerveren, valamint
- a fájlhoz vezető elérési utat a szerveren belül.

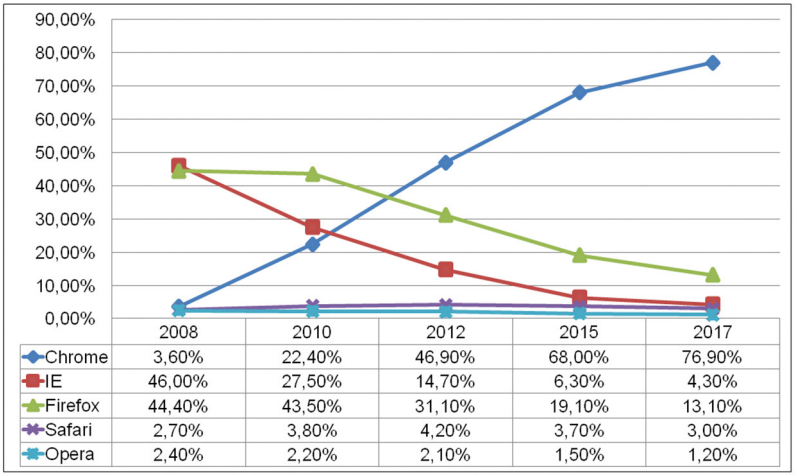
A web átviteli protokollja a HTTP,[74] amely meghatározza, hogy egy oldalról egy másik oldal hogyan érhető el. A HTTP egy kérés-válasz alapú, kliens-szerver modellt használó kommunikációs protokoll, amely a TCP/IP-t alkalmazza a kapcsolat létrehozására. Egy weboldalra való csatlakozáskor egy HTTP-kéréssel jön létre a hálózati kapcsolat, amelyet a kiszolgáló a fájl letöltését követően bont, majd a további fájlok letöltéséhez újabb kapcsolatokat kell létrehozni. A biztonságos webes kommunikációhoz – mint például a fizetési tranzakciókhoz és a felhasználói jelszavas bejelentkezésekhez – ma széles körben a HTTPS-rendszert[75] használják.

A weben az adatállományokat webszervereken tárolják, amelyek feladata az úgynevezett HTML-nyelv[76] segítségével létrehozott dokumentumok kezelése. A HTML egy leíró nyelv, amely megmutatja a böngészőnek, hogy hogyan kell megjeleníteni, illetve feldolgozni az adott állomány tartalmát. A HTML-dokumentumokba olyan hypertextlinkeket lehet beépíteni, amelyek ugyanerre a dokumentumra vagy más gépeken elhelyezett további dokumentumokra mutatnak. Ezek a hypertextkapcsolatok nagymértékben segítik az interneten való navigálást és az információk elérését, visszakeresését.

A weben az egyes tartalmakat a böngészővel érhetjük el. A böngésző egy weboldal eléréséhez a felhasználó által meghatározott kéréseket küld a webszerver felé, amely az adott weboldal megnyitásának engedélyezésével tesz eleget. A korai böngészők közé tartozott a Gopher és a Mosaic, amelyeket a Netscape váltott fel. Később a Microsoft a Windows operációs rendszerbe integrált Internet Explorerrel jelent-

[74] Hypertext Transport Protocol – HTTP.
[75] HTTP Secure – HTTPS.
[76] Hypertext Markup Language – HTML.

kezett, amely hosszú időre az Explorer dominanciájához vezetett. Mára azonban az Explorer mellett már számos grafikus böngésző áll a felhasználók rendelkezésére, mint például a Mozilla Firefox, a Google Chrome, a Safari vagy az Opera, amelyek ingyenesen elérhetők. Közülük is 2012-től meghatározóvá vált a Google Chrome böngészője, amelynek 2008-as kifejlesztése óta tartó folyamatos erősödését és a többi gyengülését jól szemlélteti az 1. grafikon.



	2008	2010	2012	2015	2017
Chrome	3,60%	22,40%	46,90%	68,00%	76,90%
IE	46,00%	27,50%	14,70%	6,30%	4,30%
Firefox	44,40%	43,50%	31,10%	19,10%	13,10%
Safari	2,70%	3,80%	4,20%	3,70%	3,00%
Opera	2,40%	2,20%	2,10%	1,50%	1,20%

1. grafikon

Webböngészők felhasználói részarányának alakulása az elmúlt tíz évben

Forrás: Browser Statistics (2017) alapján a szerző szerkesztése

A Google története 1995-ben kezdődött, amikor Larry Page és Sergey Brin találkozott a kaliforniai Stanford Egyetemen. 1996-ban egy olyan keresőmotort fejlesztettek, amely az adott weboldal relevanciáját a rá beérkező linkek alapján határozta meg. A PageRank szabadalmaztatott böngészőtechnikát kezdetben Backrubnak nevezték el, majd egy évvel később pedig a ma már jól ismert *Google.com* domainnévvel regisztráltatták be. A Google nemcsak a tudományos közösség, hanem a Szilícium-völgy befektetőinek figyelmét is felkeltette, aminek ered-

ményeként majd egy évvel később, 1998 augusztusában megalapították a Google vállalatot.

A Google azóta az internet meghatározó cégévé vált, amely az évek során számos olyan alkalmazást, eszközt fejlesztett, amelyet emberek milliárdjai nap mint nap használnak. Csak néhány a ma leggyakrabban használt alkalmazások közül:

- Gmail levelező rendszer,
- Google Maps és Google Earth digitálistérkép-alkalmazások,
- Android mobil operációs rendszer,
- Chrome böngésző,
- YouTube videomegosztó,
- Google+ közösségi hálózat stb.

Mindeközben az internet fejlődése elindult a közösségi hálózatok kialakításának irányába, amelynek lényege, hogy a technológián keresztül az embereket, a felhasználókat szervezzék hálózatba. A kezdeti cél az volt, hogy az egyének vagy szervezetek között olyan kapcsolatot hozzanak létre, amelyek alapján feltérképezhető, hogy az egyes szereplők között a társadalmi kapcsolatok hogyan és milyen módon léteznek.

Az első közösségi hálónak felfogható weboldal az 1997-ben létrehozott Six Degrees volt, amely lehetővé tette a felhasználók számára, hogy saját profilt hozzanak létre, és egymással ismeretséget kössenek. A 2000-es években egyre több ember a hálózaton keresztül, csevegő szobákban, illetve fórumoldalakon kezdett el kapcsolatba kerülni egymással. Ebben az időben indult a még ma is létező MySpace, amely akkoriban a legnépszerűbb közösségi oldalnak számított, és olyan ma meghatározó közösségi médiaszolgáltatásokat inspirált, mint például a Facebook vagy a Twitter.

2004-ben a Harvard Egyetem hallgatója, Mark Zuckerberg készítette el a kezdetben csak az egyetem hallgatói számára elérhető *Thefacebook.com* oldalt. Ezt később kiterjesztették több egyetemre is, majd 2006-ban Facebook néven, az egyetemi szférán túlra is, amihez már minden regisztrált e-mail-címmel csatlakozni lehetett. (Hale 2015) A Facebook

lehetőségeit egyre többen ismerték fel, és a közösségi oldal mögött lévő cég egyre nagyobb ütemben kezdett fejlődni. Mára a Facebook vezető közösségi médiafelületté vált, amelynek már több mint 2 milliárd aktív felhasználója van a világon. A kezdetekben pusztán kapcsolatépítésre létrehozott közösségi szolgáltatások a mindennapi életünk részévé váltak, és ennek köszönhetően az általánosan ismert felhasználás mellett a politikai döntéshozatal, a befolyásolás és a nyíl forrású hírszerzés fontos elemeit képezik.

1.6.3. A hálózati kommunikáció fejlődése

Az internet terjedésének ütemét jelentősen befolyásolta a hálózati hozzáféréshez használt kommunikációs technológia és az elérhető maximális adatátviteli sebesség. Kezdetben az internetszolgáltatók egy DSL-modemen[77] keresztül, a hagyományos telefonvonalon biztosítottak úgynevezett betárcsázós[78] kapcsolatot, amelynek maximális sebessége 56 kbit/s volt. Ez a korai, alapvetően szöveges és csak kis méretű képeket tartalmazó weboldalak eléréséhez volt elegendő. Az egyre nagyobb méretű fájlok eléréséhez azonban ez a technológia már elégtelennek bizonyult. A nagyobb adatátviteli sebességet az ADSL[79] aszinkron digitális előfizetői vonal tette lehetővé. Az ADSL-technológia azt használja ki, hogy az internetet a felhasználók általában adatletöltésre használják, és feltöltésre kevésbé. Így az ADSL-megoldásnál a letöltési és a feltöltési sávszélesség aránya nem egyenlő (aszimmetrikus), amely letöltési sebesség a feltöltéssel szemben átlagosan 8:1 arányú. Kezdetben az ADSL-kapcsolat sebessége 256 kbit/s volt, ami a különböző technológiai váltásokkal néhányszor 10 Mbit/s-ra nőtt, és mára elérte maximális teljesítőképességét.

---

77 Digital Subscriber Line – DSL.
78 Dial-up.
79 Asymmetric Digital Subscriber Line – ADSL.

A nagyobb átviteli sebességet a hagyományos telefonvonalon már nem lehet megvalósítani, ezért az internetszolgáltatók közé beléptek a kábeltévé-szolgáltatók, akik a meglévő kábelhálózaton, kábelmodem alkalmazásával biztosítanak szélessávúinternet-hozzáférést. Az így elérhető sebesség már több száz Mbit/s is lehet, ami alkalmas napjaink internetezési szokásainak kielégítésére. A még nagyobb sávszélesség pedig optikai kábelekkel valósítható meg, amelyekkel már több internetszolgáltató is biztosít lakásig futó optikai kábeles hozzáférést,[80] amellyel a Gbit/s-os adatsebesség is elérhetővé válik.

Az optikai kapcsolat mellett a vezeték nélküli technológiák jelentik az internetes hozzáférés legdinamikusabban fejlődő területét. Mára a bárhol, bármikor elérhető mobilinternetes hozzáférés alapvető igényként jelentkezik a felhasználók részéről. A mobil cellás távközlési hálózatokon jelenleg a korábban ismertetett 3G- és 4G-technológiák nyújtotta átviteli sebességek érhetők el. A tesztelés alatt lévő 5G-s mobiltechnológia pedig már lehetővé teszi az egyre növekvő adatmennyiség és adatállomány-méretek mellett a több milliárd fizikai eszköz hálózatba kapcsolását is.

A mobil cellás rendszerek mellett a másik vezeték nélküli hozzáférési mód a Wi-Fi-technológia, amelyet 1997-ben mutattak be. A technológia hamar népszerűvé vált a felhasználók körében, mivel kényelmes alternatívát jelentett a hálózati kábelek kiváltására. A számítógépek Wi-Fi-routereket használva, a rádiófrekvenciás hullámok segítségével csatlakozhatnak például egy lakásban, irodában vagy közösségi terekben kialakított helyi hálózathoz és azon keresztül az internethez. A folyamatos fejlesztésnek köszönhetően a Wi-Fi-technológia mind a hatótávolság, mind pedig az elérhető sebesség tekintetében folyamatosan javul. Az elméleti sebesség a kezdetben elérhető néhány Mbit/s-ról mára néhány Gbit/s-ra, a hatótávolság pedig néhány 10 m-ről néhány 100 m-re nőtt, ez pedig jelentős hatással volt az elterjedésére is.

[80] Fiber to the Home – FTTH.

A vezeték nélküli hálózatok létjogosultságát és rohamos terjedését támasztja alá a New Jersey Institute of Technology idevágó tanulmánya is, miszerint míg 2013-ban egy átlagos háztartásban kb. 10 vezeték nélküli eszköz csatlakozott az internethez, addig 2017-re ez a szám 17-re nőtt, 2022-re pedig – köszönhetően a „tárgyak internete" (IoT)[81] rohamos terjedésének – várhatóan kb. 50-re fog emelkedni. (NJIT é. n.)

1.6.4. A fejlődés iránya: az emberek és gépek hálózata

Az internet az elmúlt több mint 25 év alatt rohamos fejlődést mutatott minden téren. Az eredetileg elképzelt világháló mára jóval felülmúlta a kezdeti lehetőségeket, és olyan új távlatokat nyitott meg, amelyek teljesen átalakítják az emberek mindennapi életét. A közösségi média minden képzeletet felülmúló fejlődése és elterjedése következtében a felhasználók maguk is a hálózat részévé, a hatalmas méretű információ előállítójává és az információtartalom alakítójává válnak. Ezáltal a pozitív értelmű tájékoztatás és a negatív tartalmú befolyásolás olyan új távlatai nyíltak meg, amelyek korábban elképzelhetetlenek voltak. Emellett a fizikai eszközök hálózatos összekapcsolása révén kialakulóban van a gépek hálózata is, az IoT. Ez pedig az okosautó, okosotthon, okosváros stb. alkalmazásokon keresztül az emberek életét megkönnyítő lehetőségeken túl további fenyegetettségeket és sebezhetőségeket is magában hordoz, amire nem árt előre felkészülni.

Az infokommunikációs technológia fejlődéstörténetének rövid áttekintése alapján látható, hogy a kezdetek óta hatalmas változás következett be a távközlés, az elektronika és a számítástechnika világában. Az elektronikus kommunikáció megjelenésével a 20. századtól kezdődően jelentősen megnőtt és megváltozott az információ szerepe. Kezdetben a vezetékes kommunikáció, majd a rádiótávközlés volt e téren a fejlődés motorja. A második világháborúban a vezeték nélküli

[81] Internet of Things – IoT.

távközlés további fejlődése mellett megjelent új elektronikai technológiák, mint például a radar és a navigáció megteremtették az információ gyűjtésének, feldolgozásának technikai alapjait, és további kiterjesztését adták az információ kezelésének. Az egyesült királyságbeli radarlánc kiépítésével, a radarinformációk megosztásával pedig megjelent a hálózatos információkezelés kezdeti képessége.

A háború után a földfelszíni mobil- és műholdas távközlő rendszerek, hálózatok tovább növelték és szélesítették az információ továbbításának lehetőségét. A helyhez kötött információtovábbítás korlátja megszűnt, lehetővé vált a „bárhol, bármikor" kommunikációs igény kielégítése, és emellett a távközlés szempontjából korábban elérhetetlen földrajzi területek is lefedhetővé váltak.

Az ARPANET alapjain kialakított internet az elmúlt bő 25 év alatt nélkülözhetetlen információforrássá vált. Napjainkra a folyamatosan és sokszor robbanásszerűen fejlődő infokommunikációs technológia meghatározóvá vált az információ termelésében, közvetítésében és felhasználásában. A digitális információhoz való hozzáférhetőség, a mobilkommunikáció, az online média, az internetes közösségi oldalak soha nem látott módon járulnak hozzá a társadalmi, gazdasági, kulturális fejlődéshez. Mindez azt is jelenti, hogy az internet és a hálózati hozzáférést biztosító infokommunikációs szolgáltatások alapjaiban változtatták meg az emberek életét és szokásait, a munkavégzést, a szórakozást és az ügyek intézését. A mobilkommunikációs technológia adta szabadságnak köszönhetően pedig mindezt bárhol, bármikor megtehetjük.

A következő fejezetben a fentiek alátámasztására, illetve a hálózatoknak az egyének életére és a társadalomra, valamint a haderőre, a katonai műveltekre gyakorolt jelentős hatása miatt megvizsgáljuk napjaink infokommunikációs trendjeit, és bemutatunk néhány jellemző polgári és katonai hálózatos infokommunikációs technológiát.

2. Napjaink meghatározó hálózatos infokommunikációs technológiái

2.1. Az infokommunikációs technológiai fejlődés fő irányai

2.1.1. A Big Data problémája

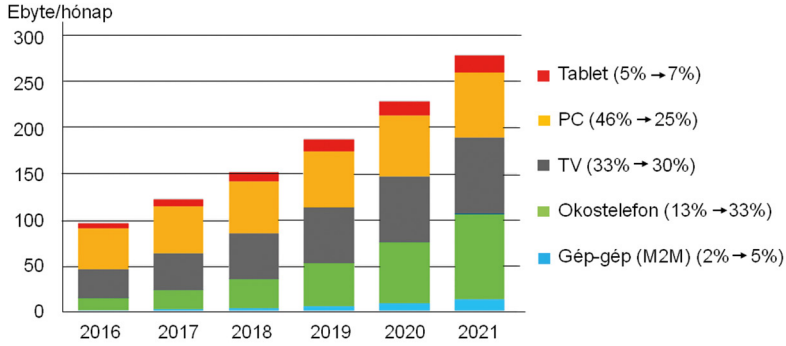
Az infokommunikációs technológiai fejlődés és a hálózatosítás eredményeként az adatok és információk mennyisége folyamatosan és exponenciálisan növekszik. Napjainkban számos tanulmány és előrejelzés foglalkozik a világon előállított adatmennyiség növekedési tendenciáival. Bár a különböző felmérések és előrejelzések az egyes területek megítélésében és a számok tekintetében kismértékben eltérőek, de a trend egyértelműen kimutatható és egy irányba mutat.

A Cisco 2016–2021 közötti időszakra vonatkozó elemzése alapján az éves IP-alapú adatforgalom 2021-re el fogja érni a 3,3 zettabyte-ot (Zbyte),[82] ami közel háromszoros növekedést mutat a 2016-os 1,2 Zbyte adatforgalomhoz képest. Ez havi adatforgalomban 96 exabyte-ról (Ebyte)[83] 278 Ebyte-ra való növekedést jelent (2. grafikon). Mindez az egy főre jutó IP-alapú adatforgalom estében azt jelenti, hogy a 2016-ban mért 13 Gbyte-ról 2021-ben 35 Gbyte-ra fog emelkedni. (Cisco 2017) A fentiek alapján ma is helytálló a Dell EMC 2014-ben közzétett tanulmánya, miszerint a „digitális univerzum" mérete exponenciálisan nő, a tárolt és kezelt adatok mérete 2013 és 2020 között várhatóan megtízszereződik, 4,4 Zbyte-ról 44 Zbyte-ra növekszik. (EMC[2] 2014)

---

[82] 1 zettabyte = 10^{12} gigabyte.

[83] 1 exabyte = 10^{9} gigabyte.



2. grafikon

Eszközspecifikus havi adatforgalom növekedési előrejelzés

Forrás: Cisco (2017) alapján a szerző szerkesztése

Különösen figyelemre méltó, hogy a Cisco trendjelentése szerint az internetes adatforgalom közel kétharmada már vezeték nélküli hálózati hozzáférésen fog alapulni. Míg 2016-ban a teljes adatforgalom 51%-a vezetékes kapcsolaton keresztül zajlott, addig 2021-re ez már csak 37% lesz, a Wi-Fi- és mobil adatforgalom pedig el fogja érni a 63%-ot. Ezen belül is a személyi számítógépes IP-adatforgalom a 2016-os 46%-ról, 2021-ben 25%-ra, az okostelefonokon keresztül zajló pedig 13%-ról 33%-ra fog növekedni. Mindez jól mutatja a vezeték nélküli technológiák jelentős előretörését, a felhasználók mobilitási igényét a hálózati hozzáférés tekintetében. (Cisco 2017)

Az infokommunikációs technológia növekedési ütemének bemutatásakor szót kell ejteni az egyre elterjedtebb hálózaton keresztül megvalósuló gép-gép (M2M)[84] közötti kapcsolatról. Az IoT és az IoE[85] technológiáknak köszönhetően, amikor emberek és tárgyak kapcsolódnak az internetre és azon keresztül egymáshoz, az M2M-kapcso-

[84] Machine to Machine – M2M.
[85] Internet of Everything – IoE.

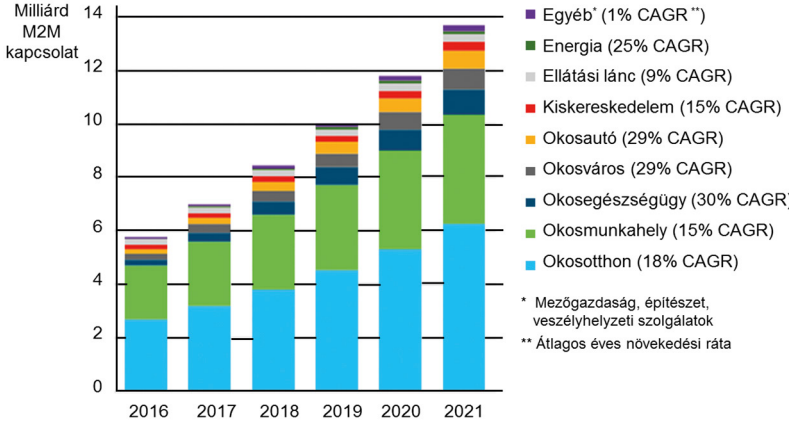
latok szintén szignifikáns növekedést mutatnak az elkövetkezendő négy évben. Globálisan az M2M-kapcsolatok 2016 és 2021 között 2,4 szeresére, 5,8 milliárdról 13,7 milliárdra fognak növekedni. Az otthoni alkalmazások, mint például a lakásautomatizálás, biztonsági és megfigyelő rendszerek, háztartási eszközök stb. a teljes M2M-kapcsolatok 46%-át fogják adni 2021-ben. Ez jól mutatja, hogy az elkövetkezendő években a mindennapi életünket milyen mértékben fogják befolyásolni az interneten keresztül elérhető, vezérelhető okoseszközök. Az e téren legdinamikusabban növekvő ágazat a távorvoslásnak, az egészségügyi monitoring és gyógyszerellátó alkalmazásoknak köszönhetően a hálózatosított okosegészségügy[86] lesz, amelynek 30%-os átlagos éves növekedést[87] prognosztizálnak. A második leggyorsabb növekedést az intelligens, interneten keresztül összekapcsolt technológiákat használó okosautó-[88] és okosváros-alkalmazások[89] fogják produkálni 29%-kal. (Cisco 2017) (3. grafikon)

E hatalmas adatmennyiség kezelése kapcsán néhány éve már megjelent a *Big Data* fogalma. A Big Data a környezetünkből, az emberektől, tárgyaktól strukturálatlan formában származó, óriási mennyiségű adatok tömegét és azoknak a korábbi elterjedt és megszokott módszerektől eltérő feldolgozását jelenti. A Big Data tehát elsősorban az IoT-nek és az M2M-kapcsolatok rohamos növekedésének köszönhetően a különböző szenzorokkal összegyűjtött adatok feldolgozásának újszerű módja.

A Big Data a 3V-vel[90] jellemezhető, amely az adatok mennyiségére, sebességére és változatosságára utal. A különböző hálózatba kötött szenzorok a környezetünkből másodpercenként tömegesen és folyamatosan szállítják az adatokat a feldolgozás helyére. Ezek továbbítása egyre nagyobb adatátviteli sebességet igényel, illetve az egyre növekvő

86 Connected Health.
87 Compound Annual Growth Rate – CAGR.
88 Connected Car.
89 Connected City.
90 Volume, Velocity, Variety.

adatmennyiség feldolgozását egyre gyorsabban és valós időben kell megvalósítani. A Big Data egyik legnagyobb kihívását a strukturálatlan adatok tömege és azok változatossága jelenti.



3. grafikon

M2M-kapcsolatok növekedési trendje szektoronként

Forrás: Cisco (2017) alapján a szerző szerkesztése

A helyzethez illeszkedő optimális döntések meghozatalához szükséges értelmezett információk a változó struktúrájú adatfolyamok elemzésével, formázásával, összehasonlításával, fuzionálásával nyerhetők ki, ez pedig a mai környezetben a leghatékonyabban a felhőalapú számítástechnika[91] alkalmazásával valósítható meg. Az internet és a felhőalapú technológia egyszerre teszik szükségessé és lehetővé a Big Data kezelését. Szükségessé, mivel az adatok a hálózatba kötött szenzoroknak köszönhetően áramlanak, illetve lehetővé, mert a felhő által biztosított hatalmas tárolókapacitás és a nagyteljesítményű szerverek nyújtják az egyetlen jó megoldást, hogy a Big Data infrastruktúra igényeit ki

[91] Cloud Computing.

lehessen elégíteni. A Big Data kezelésének egyik legígéretesebb ilyen technológiai megoldása ma például a hálózat szélén,[92] az adatok keletkezési helyén történő felhőalapú adatfeldolgozás.

Mindez a katonai környezetre is érvényes. A katonai műveletekben ma szenzorok tömegét és azokból kialakított hálózatokat alkalmazunk az összadatforrású felderítés[93] követelményeinek megfelelően. Ezek a sokszor felügyelet nélkül működő, autonóm szenzorok szintén nagy mennyiségű, változatos, strukturálatlan adatok tömegét gyűjtik az ellenségről és a harctéri környezetről, amelyeket ugyanúgy a Big Data követelményei szerint kell feldolgozni..

2.1.2. Infokommunikációs technológiai konvergencia

Az adatok gyűjtését, előállítását, tárolását, feldolgozását, továbbítását biztosító különböző elektronikai, informatikai eszközök és rendszerek közötti legátfogóbb, legmeghatározóbb jelenség ezen területek konvergenciája, amelyet *infokommunikációs technológiai konvergenciának* nevezünk. A konvergencia alapvetően a bevált, magas fejlettségi szintet elért és széles körben elterjedt technológiák egymáshoz való közeledése, integrációja révén alakul ki, és fejti ki hatását. Az infokommunikációs technológiai konvergencia első lépcsőjén is ez történt, amikor a távközlés és a számítástechnika összeolvadása következtében létrejöttek a számítógép-hálózatok.

A konvergencia folyamatát a digitális technológia megjelenése és hatalmas ütemű fejlődése váltotta ki. A digitális technológia elterjedésével megindult a számítógép, a vezetékes és vezeték nélküli távközlési eszközök, majd később az elektronikus média egymáshoz való közeledése, technológiai konvergenciája. Ennek következtében megvalósul az információ mindenfajta formában (zene, beszéd, szöveg,

---

92 Edge Computing.

93 All Source Intelligence – ASI.

rajz, álló- és mozgókép) történő továbbítása ugyanazon a kommunikációs csatornán. Lehetővé vált a kezdetben önálló információkezelési módok összekapcsolása, kombinálása, és ezáltal különböző infokommunikációs alkalmazások jöttek létre. Ilyen infokommunikációs alkalmazások közé sorolhatjuk a különféle multimédia-szolgáltatásokat, internetes alkalmazásokat, elektronikus tartalomszolgáltatásokat és tulajdonképpen általában véve az úgynevezett információs társadalmi szolgáltatásokat. (Sallai–Abos 2007) Az infokommunikációs technológiai konvergencia következő szintje a szenzortechnológia és a már kialakult infokommunikációs eszközök között valósul meg, ami az IoT- és az M2M-kapcsolatoknak köszönhetően rohamosan terjed.

Az infokommunikációs technológiai konvergencián belül megkülönböztethetjük:

- a szolgáltatások konvergenciáját,
- a hálózatok konvergenciáját és
- a készülékek konvergenciáját. (Sallai–Abos 2007)

A szolgáltatások konvergenciájakor egy infokommunikációs rendszer szolgáltatásában különféle információs tartalmak jelennek meg (például a multimédia-termékek). A *hálózatok konvergenciája* azonos technológiai alapokat, szolgáltatások együttes kiszolgálását lehetővé tevő kapacitásokat és hálózati funkciókat jelent, amelyet a széles sávú internet tesz lehetővé. A készülékek konvergenciája pedig a korábban különálló készülékek funkcióinak egybeépülését jelenti. (Sallai–Abos 2007) Ilyenek például az okostelefonokba beépülő mobiltelefonos, vezeték nélküli internet, navigációs és multimédia-alkalmazások (hang- és képrögzítés, valamint visszajátszás), játék- és egyéb más alkalmazások.. A készülékszintű konvergencia jó példája az okostévé is, amely már nemcsak a hagyományos televízió funkcióját látja el, hanem a különböző smartalkalmazásoknak köszönhetően internetkapcsolatra is képes, és azon keresztül pedig különféle médiatartalmak válnak hozzáférhetővé, illetve távközlési lehetőségek nyílnak meg például az IP-alapú kommunikáció alkalmazásával.

A szolgáltatások, hálózatok és készülékek teljes körű konvergenciája az infokommunikációs rendszereken alapuló információs infrastruktúrák egymásba kapcsolódó, komplex rendszerén keresztül valósul meg. A rendszerek komplexitását és a technológiai konvergenciát bizonyítja, hogy a távközlési és informatikai rendszerek, a hozzájuk kapcsolódó adatgyűjtést végző szenzorokkal és más elektronikai rendszerekkel egységes rendszert képeznek. Így a teljes körű konvergenciát jelentő infokommunikációs rendszerekbe beletartoznak mindazon eszközök és technológiák is, amelyek az érzékelés, irányítás, vezérlés funkcióit látják el. Így például idesorolhatók azok a szenzorhálózatok, távérzékelő, távfelügyeleti, navigációs rendszerek, repülőtéri leszállító és irányítórendszerek stb. is, amelyek a számítógép-hálózatokon keresztül csatlakoznak egymáshoz és más rendszerekhez. Ennek megfelelően fejlett információtechnológián alapuló infokommunikációs rendszerekkel látják el a különböző kormányzati, közigazgatási, gazdálkodó, oktatási, egészségügyi és védelmi szervezeteket, intézményeket, illetve a vállalatokat. (Haig 2015; Haig–Várhegyi 2005)

A konvergencia jelensége a katonai infokommunikációs rendszerek vonatkozásában is megfigyelhető. A katonai műveleti környezetben olyan teljes körű konvergenciát felmutató, összefüggő hálózatokat alakítanak ki, amelyek az előbb ismertetett elvnek megfelelően az adatszerzési, adattovábbítási, adattárolási és adatfeldolgozási, majd szétosztási funkciókat kielégítik. Amennyiben egy katonai szervezet e komplex katonai infokommunikációs rendszereket hatékonyan tudja működtetni, ki tudja használni a bennük rejlő lehetőségeket és biztosítani tudja a biztonságos működtetésüket is, akkor az jelentős támogatást nyújt a műveletek céljainak eléréséhez. A későbbiekben az információs műveletek összefüggései és az egyes információs műveleti képességek tárgyalásakor ez a hatásnövelő és képességjavító tényező kiemelt jelentőséggel bír, különösen a kibertérben zajló információs műveletek esetében.

2.1.3. Feltörekvő infokommunikációs technológiák

Az infokommunikációs technológiai trendek kutatása tekintetében meghatározó Gartner kutatóintézet évek óta elemzi az elmúlt évek technológiai változásait, és ezek alapján a jövőre vonatkozóan prognosztizálja a fejlődés főbb tendenciáit. A fejlődési irányokat egy úgynevezett Hype-ciklus görbéjén ábrázolják, amely jól szemlélteti, hogy a legújabb technológiák milyen fázisokban és ütemben haladnak előre, illetve hogy éppen melyik fejlődési szakasznál tartanak. A Hype-ciklus az alábbi öt fázisban mutatja a technológiai fejlődés ütemét:

- Innovation Trigger, vagyis az innováció megindításának szakasza, a kezdeti fázis, amikor egy teljesen új technológia jelenik meg, amely iránt hirtelen megugró érdeklődés mutatkozik elsősorban a média- és a technológiai újdonságok iránt fogékonyak részéről;
- Peak of Inflated Expectations, a nagyfokú elvárások csúcsa, amikor már a még kiforratlan technológia iránti érdeklődés széles körűvé válik, egyre többen alkalmazzák;
- Trough of Disillusionment, vagyis a kiábrándulás mélypontja, amikor az egyes új technológiák iránt a médiafelhajtás elcsitul, a nem megfelelően megalapozott technológiák fejlődése megáll, hanyatlásnak indul, és csak a valóban értéket képviselő és az érdeklődést fenntartó technológiák maradnak talpon;
- Slope of Enlightenment, a megvilágosodás emelkedő szakasza, amikor a kezdeti hirtelen lelkesedés lecsendesedik, és a felhasználók számára valóban értéket és új megoldásokat, szolgáltatást nyújtó technológiák tudatos és átgondolt fejlesztése folyik;
- Plateau of Productivity, vagyis a termelékenység fennsíkja, az utolsó fázis, amikor már a felhasználók a technológiát teljeskörűen elfogadják, egyre többen használják, és mindennapi életünk részévé válik. (Gartner é. n.)

2017-ben a Gartner három fő technológiai megatrendet vizionált, amelyekben számos feltörekvő technológia található, és amelyeknek leírja

a Hype-ciklusát. A három megatrenden belül a Gartner többek között az alábbi kifejezetten infokommunikációs technológiákat nevesíti:[94]

1. Artificial intelligence everywhere (mindenhol jelen lévő mesterséges intelligencia):
   - Autonomous Vehicles (autonóm járművek);
   - Smart Robots (okosrobotok);
   - Smart Workspace (okosmunkaterek);
   - Smart Dust (okosporszemek, azaz okos-mikroelektromechanikai szenzorok);
   - Commercial Drones (kereskedelmi célú drónok);
   - Machine Learning (gépi tanulás);
   - Cognitive Computing (kognitív számítástechnika);
2. Transparently Immersive Experiences (magával ragadó élményeket nyújtó technológiák):
   - 4D printing (4D-s nyomtatás);
   - Augmented reality (kiterjesztett valóság);
   - Virtual Reality (virtuális valóság);
   - Brain-Computer Interface (emberi agy-számítógép interfész);
   - Connected Home (okoshálózatos otthon);
3. Digital Platforms (digitális platformok):
   - 5G (5G mobilhálózati technológia);
   - Digital Twin (digitális iker, vagyis egy fizikai objektum digitális modellezése);
   - Blockchains (blokkláncok);
   - IoT Platforms (IoT-platformok);
   - Edge Computing (a hálózat szélén, az adatok keletkezési helyén történő felhőalapú adatfeldolgozás);
   - Quantum Computing (kvantum számítástechnika);
   - Serverless PaaS (szerver nélküli, felhőalapú platformszolgáltatás). (Panetta 2017)

[94] A trendek sokszor magyarul nem vagy csak nehezen lefordíthatóak, ezért azokat az angol elnevezésükkel soroljuk fel.

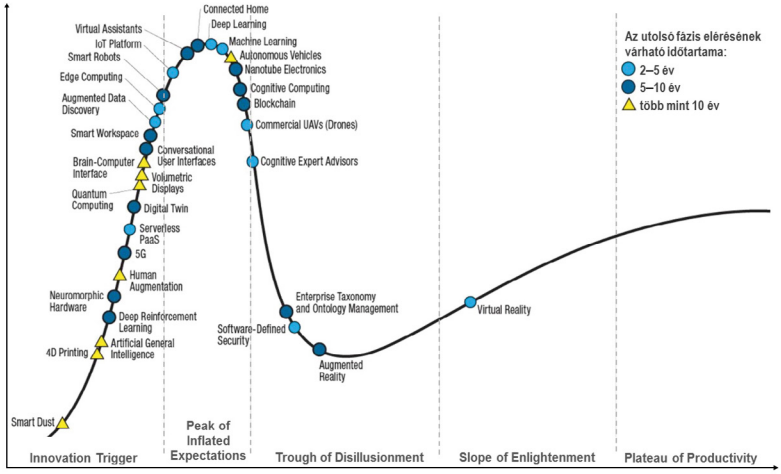
Az egyes technológiák 2017-re prognosztizált Hype-ciklus szerinti előrehaladását a 6. ábra szemlélteti. Ez alapján megfigyelhető, hogy a legtöbb technológiai újdonság, mint például a mesterséges intelligencia, a kvantum-számítástechnika, az emberi agy-számítógép interfész, az okosrobotok vagy az IoT-platformok ma még a kezdeti, felfutó szakaszban vannak, és bár fokozatosan emelkedő, nagyfokú érdeklődés mutatkozik irántuk, de ezek ma még nem kiforrott megoldásokat takarnak. Ugyanakkor az olyan új feltörekvő technológiák, mint a gépi tanulás, a blokkláncok, a kognitív számítástechnika vagy a kereskedelmi célú pilóta nélküli eszközök (UAV-k,[95] drónok) jelentősen elmozdultak a Hype-ciklus mentén 2016 óta.

Ma már szinte az összes fentebb ismertetett technológia közös műveleti környezete a hálózat. A munkavégzéshez, szórakozáshoz és a mindennapi élethez használt legkülönfélébb eszközök hálózatba kacsolva, az interneten keresztül érhetők el, illetve nyújtanak különféle szolgáltatásokat a felhasználóknak. A mobilkommunikációnak köszönhetően a hálózatosodás rendkívüli mértékben növekszik, ezért a hálózatba kapcsolt eszközök és szolgáltatások már szinte bárhonnan elérhetők. A mobiltechnológia tendenciáját jól mutatja, hogy míg 2000 előtt a vezetékes távközlés volt az alapvető kommunikációs technológia, és kb. 1 milliárd helyhez kötött előfizető volt a világon, addig 2010 körül már 6 milliárd mobilfelhasználó tudott kommunikálni egymással, és 12,5 milliárd eszköz volt hálózatba kapcsolva.

A hálózatba kötött fizikai eszközök számának rohamos növekedése azt eredményezi, hogy 2020-ra már 50 milliárd eszköz lesz az interneten keresztül elérhető, ami a populáció növekedését is figyelembe véve több mint 6,5 eszközt jelent fejenként. (Evans 2011) Mindezt a tárgyak internetében (IoT) rejlő lehetőségek felismerése, a különféle vezeték nélküli megoldások, többek között az 5G-mobiltechnológia és a szenzortechnológia fejlődése teszi lehetővé. Emellett rendkívüli mértékben növekszik

[95] Unmanned Aerial Vehicle – UAV.

a hálózaton keresztül elérhető szolgáltatások köre, a felhőalapú számítástechnika alkalmazási lehetőségeinek bővülése.



6. ábra

Feltörekvő technológiák Hype-ciklusa 2017-ben

Forrás: PANETTA (2017) alapján a szerző szerkesztése

Az elmúlt évtizedekben az infokommunikációs technológiákban bekövetkező rohamos ütemű fejlődés megváltoztatta a katonai és polgári technológiák közötti egymásra hatást is. Míg a 70-es, 80-as évekig a katonai technológia területén megjelenő új eredmények alapvetően meghatározták a polgári technológiai fejlődés alakulását, addig ma ennek az ellenkezőjét tapasztaljuk. Különösen a két világháborúhoz kapcsolódóan kifejlesztett legújabb katonai eszközök, mint például a radar, a katonai rádiótávközlés, a rakétatechnika vagy az atombomba feltalálása, illetve a hidegháborús atomfenyegetettség miatt kifejlesztett számítógép-hálózatok, különösen az ARPANET máig ható és meghatározó eredményeket hozott a civil társadalom működésében is.

A 90-es évektől azonban az infokommunikációs technológia terén jelentkező újabb és újabb eredmények, különösen a hálózatos technológiák gyakorolnak meghatározó hatást a katonai rendszerekre. A polgári szférában megjelenő és rendkívüli ütemben fejlődő új, feltörekvő technológiák fokozatosan épülnek be a katonai infokommunikációs rendszerekbe, és teszik hatékonyabbá a felderítést, a döntéshozatalt, a csapatok vezetését és irányítását, valamint a fegyverirányítást. A továbbiakban a teljesség igénye nélkül, röviden áttekintjük e napjainkban legjellemzőbb, már megvalósult, illetve a kiteljesedés előtt álló polgári és katonai hálózatalapú megoldásokat, technológiákat.

2.2. Civil és katonai hálózat-alapú infokommunikációs technológiák

2.2.1. Felhőalapú számítástechnika

2.2.1.1. A felhőalapú számítástechnika kialakulása

Amint láthattuk, a hálózati technológia fejlődése, az adatátviteli sávszélesség folyamatos növekedése következtében gyakorlatilag mára a legtöbb számítógép az interneten keresztül folyamatos kapcsolatban van egymással. A korábban jelzett adatnövekedési tendenciák, az egymással összekapcsolt számítógépek, tabletek, okostelefonok és M2M-kapcsolatok számának drasztikus emelkedése új hálózati hozzáférési megoldásokat is igényelt. A 2020-ra prognosztizált 50 milliárd interneten keresztül elérhető eszköz a már ma is használt IPv6[96] internetprotokoll teljes körű elterjedését jelenti. Ez a címzési protokoll több nagyságrend-

[96] Az IPv6 (Internet Protocol version 6; 6-os verziószámú Internet Protokoll) egy csomagkapcsolt hálózati protokoll, amelyet az IPv4 továbbfejlesztésére dolgoztak ki. Az IPv4 32 bites címzése helyett az IPv6 128 bitet használ címzésre, ami a 2^{32} (kb. 4,3 10^{9}) IP-cím helyett 2^{128} (kb. $3{,}4 \times 10^{38}$) IP-cím kiosztását teszi lehetővé.

del nagyobb címzési lehetőséget és fokozottabb átviteli biztonságot tesz lehetővé, mint elődje, az IPv4.

A teljes körű összekapcsoltság következtében a felhasználók a világon tárolt bármilyen információhoz hozzájuthatnak, és bárkivel kapcsolatba léphetnek, az M2M-kapcsolatoknak köszönhetően pedig lehetővé válik a nagyszámú IoT-platform összekapcsolása. A hálózatba kötött eszközök felhasználhatják egymás erőforrásait, így egy feladat megoldásában több, akár a világ különböző pontjain lévő számítógép vehet részt. Kialakultak az elosztott adatfeldolgozó rendszerek, amelyekben a szenzorok által gyűjtött adatokat, de akár a személyes adatokat is távoli szervereken tárolják. Az infokommunikációs rendszerekben megjelenő újfajta alkalmazásoknak köszönhetően pedig, a nagy adatsebességű kapcsolatokat kihasználva, a távoli tároló- és számítási teljesítmény bármikor elérhető.

A hálózatos hozzáférés természetessé válásával megjelent a felhőalapú számítástechnika, amely különféle informatikai szolgáltatások – mint például az adattárolás, adatbázis-kezelés, hálózatmenedzsment, szoftverek futtatása, adatelemzés stb. – nyújtását jelenti az interneten vagy helyi hálózaton keresztül. A felhőalapú számítástechnikai szolgáltatások igénybevétele során az adatokat részben vagy teljes egészében a „felhőben", a szolgáltató által működtetett és felügyelt távoli elérésű adattárakban, adatközpontokban tárolják, feldolgozásukhoz pedig szintén annak erőforrásait használják fel. Az adattárolás és az adatfeldolgozás többnyire nem egy meghatározott hardvereszközön történik, hanem általában elosztva a szolgáltató erőforrásai között. A felhőszolgáltatást nyújtó cégek a közműszolgáltatókhoz hasonlóan a használat alapján számítják fel a felhőszolgáltatások díjait.

A felhőalapú számítástechnikának számos előnye van, amely a felhasználók számára vonzóvá teszi alkalmazását. Ezek közül néhány:

- költséghatékonyság;
- gyorsaság és azonnali hozzáférhetőség;
- rugalmas skálázhatóság;

- nagyfokú teljesítmény;
- a CIA[97] hármas alapelvének – a bizalmasság, sértetlenség és rendelkezésre állás követelményeinek megfelelő megbízhatóság és magas szintű rendelkezésre állás.

A felhőszolgáltatások jellemző felhasználási területei az alábbiak lehetnek:

- új alkalmazások és szolgáltatások létrehozása;
- adatok tárolása, biztonsági mentése és helyreállítása;
- adatbázis-kezelés;
- weboldalak, portálok és blogok üzemeltetése;
- hang- és videótartalmak tárolása, azonnali hozzáférhetővé tétele;
- igény szerinti, különféle szoftverszolgáltatás stb.

Az emberek a mindennapi tevékenységük során számos alkalommal használnak felhőszolgáltatást, még akkor is, ha ez nem is tudatosul bennük. Amennyiben például valaki online felületen levelezik, zenét hallgat, filmet néz, vagy játszik, akkor azt jó eséllyel valamilyen felhőszolgáltatón keresztül teszi. Mára a felhőalapú szolgáltatásokat a kis- és közepes vállalkozásoktól kezdve a multinacionális nagyvállalatokig, illetve a kormányzati és közigazgatási szervektől a nonprofit szervezetekig szinte mindenki használja. E technológia nagyban segítheti a vállalatokat, különösen a kkv-kat, hogy jelentősen csökkentsék az infokommunikációs technológiai költségeiket, a kormányzat és a közigazgatás számára pedig lehetővé teszi, hogy alacsonyabb költségen nyújtson közszolgáltatásokat az állampolgároknak.

[97] Confidentiality, Integrity, Availability – CIA.

2.2.1.2. A felhőalapú számítástechnika fajtái, típusai

A felhőalapú szolgáltatásokhoz való hozzáférés szempontjából alapvetően háromfajta felhőt különböztethetünk meg:

- nyilvános felhőszolgáltatást;
- magán- vagy zárt célú felhőszolgáltatást, valamint
- hibrid felhőszolgáltatást.

A nyilvános felhő a nevéből adódóan bárki számára hozzáférhető, adattárolási és számítási kapacitásán több felhasználó is osztozik, és üzemeltetését egy külső felhőszolgáltató végzi. A nyilvános felhők számítási erőforrásai, a hardvereszközök (például szerverek és adattárak), szoftverek és egyéb támogató infrastruktúrák a szolgáltató tulajdonát képezik. A szolgáltatásokat és a felhasználói fiókokat a szolgáltatást igénybe vevő valamilyen webböngészővel az interneten keresztül érheti el, illetve kezelheti. A nyilvános felhőalapú szolgáltatások biztonsága napjainkban gyakran felvetődő kérdés, hiszen a felhasználó az adatait egy olyan környezetben kezeli, amelyre nincs rálátása, felügyelete, emiatt a szolgáltatóval szemben nagyfokú bizalom szükséges. A szolgáltató ugyanakkor érdekelt a CIA-elvek betartásában, mivel bármilyen biztonsági incidens következtében jelentősen csökkenhet a fizető felhasználók száma. Ehhez a szolgáltatónak hitelesített biztonsági eszközöket, megoldásokat, behatolást detektáló és megelőző rendszereket[98] kell alkalmaznia.

A magáncélú vagy zárt felhő ezzel szemben kizárólag egyetlen cég vagy szervezet kizárólagos használatában van, és az interneten vagy belső magánhálózaton keresztül elérhető szolgáltatásokat biztosít. A magáncélú felhő fizikailag általában a szervezet telephelyén található, de díjfizetés ellenében külső szolgáltatóknál is üzemeltethető. Az infrastruktúra működtetéséért és a szolgáltatások biztosításáért a szervezet saját informatikai szervezete a felelős. A magáncélú, zárt felhő a belső

[98] Intrusion Detection System – IDS, Intrusion Prevention System – IPS.

üzemeltetés révén jobb biztonságot és adatvédelmet tesz lehetővé, hatékonyabban képes biztosítani, hogy külső felhasználók ne férjenek hozzá bizalmas adatokhoz.

A hibrid felhő a nyilvános és a magánfelhők kombinációjaként jön létre. A hibrid felhő biztosítja az adatok és alkalmazások megosztását a nyilvános és a magánfelhő között, és lehetővé teszi, hogy bizonyos feladatok a nyilvános felhőben legyenek végrehajtva anélkül, hogy a cég teljes adatállománya hozzáférhetővé válna. Így a vállalatok a nem vagy kevésbé bizalmas adatok és számítási feladatok esetében kihasználhatják a nyilvános felhő rugalmasságát és számítási kapacitását, miközben a kiemelt fontosságú adatokat a szervezet saját biztonsági rendszere mögött, saját telephelyükön tárolhatják és kezelhetik. (Microsoft Azure é. n.)

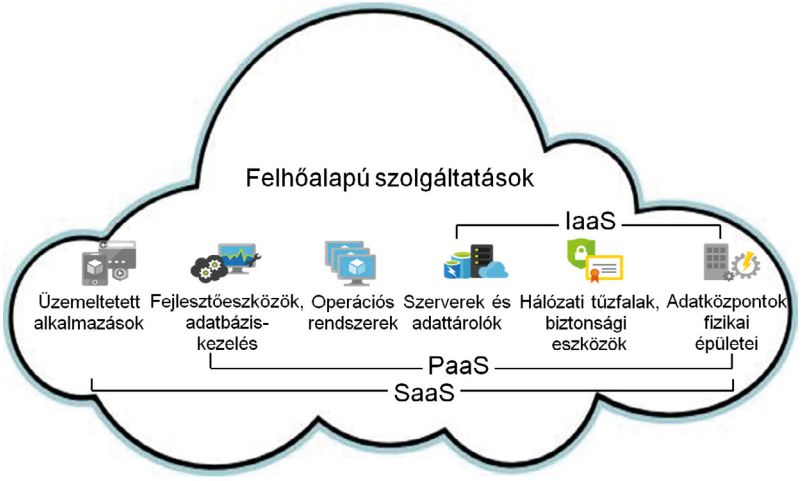
A felhőalapú számítástechnikai szolgáltatásoknak három fő típusa ismeretes (7. ábra):

- szoftverszolgáltatás (SaaS),[99]
- platformszolgáltatás (PaaS),[100] valamint
- infrastruktúra-szolgáltatás (IaaS).[101]

A szoftverszolgáltatás az interneten keresztül többnyire közvetlenül igénybe vehető szoftveralkalmazásokat jelent. Az alkalmazásokat, valamint a hardvereszközöket a felhőszolgáltató üzemelteti és kezeli, emellett a szoftverfrissítéseket, biztonsági javításokat és egyéb karbantartási feladatokat is a szolgáltató végzi. A szoftverszolgáltatás ingyenes vagy használatalapú díjfizetéssel vásárolható meg a felhőszolgáltatótól. Napjainkban számos személyes használatú, ingyenes szoftverszolgáltatás érhető el az interneten, mint például a Google Calendar, Hotmail, Yahoo! Mail, Gmail, Google Drive stb. Szervezeti célú felhasználás során pedig különböző munkahatékonyság-növelő alkalmazásokat (pél-

[99] Software as a Service – SaaS.
[100] Platform as a Service – PaaS.
[101] Infrastructure as a Service – IaaS.

dául levelező- vagy naptárkezelő alkalmazásokat), valamint vállalatirányítási és ügyfélkapcsolati rendszereket lehet használni előfizetés vagy használatalapú díj ellenében.



7. ábra

Felhőalapú számítástechnika

Forrás: MICROSOFT AZURE (é. n.) alapján a szerző szerkesztése

A platformszolgáltatás a szoftveralkalmazások fejlesztéséhez, teszteléséhez, terjesztéséhez és felügyeletéhez szükséges környezetet biztosítják. E szolgáltatással a fejlesztők különböző webes, mobil- vagy nagyvállalati alkalmazásokat készíthetnek el. A fejlesztéshez szükséges hardver- és szoftver-infrastruktúra kialakítását és felügyeletét a szolgáltató végzi, így az a felhasználó költségeit nem terheli. Ilyen szolgáltatást nyújt például a Google App Engine, a Microsoft Azure vagy az OpenShift.

Az infrastruktúra-szolgáltatás az interneten keresztül üzembe helyezhető és felügyelhető hálózati infrastruktúrát (adattárakat, tűzfa-

lakat, terheléselosztási szolgáltatásokat stb.) biztosít alapvetően használatalapú díjfizetéssel. Az infrastruktúra üzemeltetése és felügyelete a szolgáltató feladata. A felhasználó végzi a saját szoftvereinek és alkalmazásainak telepítését, konfigurálását és felügyeletét. A legismertebb példa a Google Compute Engine vagy az Amazon Web Services, amely Elastic Compute Cloud (EC2) számítási felhőt, valamint a Simple Storage Service (S3) tárolókapacitás-szolgáltatást nyújt a felhasználók számára. (Soós–Szabó 2013; Microsoft Azure é. n.)

2.2.1.3. A felhőalapú számítástechnika katonai alkalmazhatósága

A felhőalapú számítástechnika napjainkra megjelent a katonai információs rendszerekben is. A védelmi célú felhő – a katonai infokommunikációs sajátosságokat figyelembe véve – tulajdonképpen ugyanazt a szolgáltatási modellt jelenti, mint a civil felhő, ugyanakkor a katonai célú felhőszolgáltatással szemben komoly biztonsági követelményeket kell támasztani. A megfelelően kialakított kockázatkezelés és az adatvédelem elsőrendű fontosságú a katonai felhőszolgáltatásban.

Mint általában minden felhőalapú számítástechnikai alkalmazás, a katonai célú felhőszolgáltatás alkalmazása is számos előnyt nyújt. Ezek az alábbiak:

- lehetővé teszi az egyidejű hozzáférést az adatokhoz, és javítja az információ megosztását;
- elősegíti a szövetséges műveleti hálózatos koncepció implementálását;
- biztosítja a különböző haderőnemek és fegyvernemek közötti közös műveleti helyzetkép kialakítását;
- a rugalmas hálózati architektúrával és az információhoz való egyidejű hozzáféréssel növeli a vezetés és irányítás hatékonyságát, jelentősen megkönnyíti a parancsnoki döntéshozatali folyamatot;

- a szenzorok adatainak megosztása és az azokhoz való széles körű hozzáférés biztosítása révén növeli a riasztás és a korai előrejelzés képességét;
- csökkenti a hálózati fenyegetések kockázatát a katonai adathálózatokban;
- magas szintű kriptográfiai hitelesítési eljárásokat biztosít;
- szabványosítja a hálózatban kezelt információkhoz való hozzáférési elveket;
- növeli a katonai műveletek tervezése és végrehajtása során az együttműködés, interoperabilitás képességét;
- a skálázhatóság és a modularitás biztosításával optimalizálhatók a hálózat implementálásának költségei. (Ţigănuş 2015)

A katonai célú felhőalapú rendszerek kialakítása és elterjedése a haderőben ma még a kezdet kezdetén jár. Ennek oka lehet többek között a jelenlegi katonai célú infokommunikációs rendszerek viszonylag alacsony adatátviteli kapacitása, a még nem kielégítő biztonsági megoldások, illetve a szenzitív adatok felhőben való kezelésével szembeni fenntartások és az érvényben lévő szabályok. A parancsnok számára alapvető fontosságú a bizalmasság, sértetlenség és rendelkezésre állás követelményeinek teljesülése. A hálózati forgalom megszakadása, az adatokhoz való hozzáférés korlátozottá válása, esetlegesen az adatokhoz való illetéktelen hozzáférés és az adatok kompromittálódása mind-mind olyan tényező, ami a felhőszolgáltatás széles körű elterjedését gátolja a haderőben.

Ennek ellenére a katonai felhőalapú szolgáltatások kialakítására a kezdeti lépések már megkezdődtek. Az amerikai védelmi minisztérium közös információs környezet stratégiájának fő pilléreit a felhőalapú migráció és az adatközpontok konszolidációja képezi. Ennek érdekében a minisztériummal kötött szerződés értelmében az IBM megkezdi egy katonai, zárt célú felhő kiépítését Army Private Cloud II néven, amely 11 már meglévő adatközpontot fog magában foglalni. Ez lesz az első olyan felhőszolgáltatás, amelyben egy cég, nevezetesen az IBM építi ki

a zárt felhőt, és az adatközpontok menedzselését is ő végzi. A kezdeti szakaszban a nem minősített adatok kezelésére 38 alkalmazás kerül a felhőbe. Az elvárt biztonság érdekében a program második évében az IBM az adatok tárolását és kezelését egy titkos IP-alapú hálózatban[102] végzi. (Carberry 2017)

A NATO szintén megkezdte a felhőalapú szolgáltatásokban rejlő lehetőségek feltérképezését. Egy 2014-ben megjelent tanulmány szerint az információtechnológiai modernizációs program átalakítja a NATO infokommunikációs szolgáltatásainak jellegét. (Lenk 2014) A jelenlegi helyi szolgáltatások egyre inkább globális szolgáltatásokká válnak, ami tulajdonképpen a NATO felhőszolgáltatásának kialakítását jelenti. A NATO infokommunikációs infrastruktúra modernizációjának célja, hogy tovább javítsa a NATO-hálózatok rugalmasságát, növelje az adattárolás és -kezelés lehetőségét, és kiterjessze a hálózati hozzáférést. A felhőalapú számítástechnika katonai alkalmazása más technológiákkal együtt minőségi ugrást jelenthet a jövőre nézve, mivel a jelentősen megnövekedett adatmennyiség miatt – a polgári élethez hasonlóan – a döntéshozatali folyamatban egyre nagyobb szerepet kap az adatbányászat, a mesterséges intelligencia és az algoritmizált döntés-előkészítés. A NATO által tervezett Szövetséges Műveleti Hálózat (FMN)[103] koncepciója is alapvetően a felhőalapú hozzáférésen alapul (lásd később).

2.2.2. Tárgyak internete – IoT

2.2.2.1. Az IoT értelmezése

Mára az okos-, mobil eszközök uralkodóvá váltak az infokommunikációs technológiában, és ez a tendencia tovább fog erősödni. A tech-

[102] Secret Internet Protocol Router Network – SIPRNet.
[103] Federated Mission Networking – FMN.

nológia robbanásszerű fejlődése következtében teljesen természetes, hogy különböző szenzorok érzékelik folyamatosan a környezetünket, és az interneten keresztül kommunikálnak egymással, illetve a felhasználókkal. Már nemcsak számítógépek és mobiltelefonok csatlakoznak az internetre, hanem egyre több hétköznapi használati tárgy, eszköz is. Ennek következtében pedig az internetre csatlakozó eszközök száma drasztikusan emelkedik, amit az IoT terjedése pedig egyértelműen erősít.

Zheng és Carter szerint az IoT rohamléptű elterjedését alapvetően a digitális technológiához kötődő alábbi négy fő tényező generálja:

- az első az egyre olcsóbb, kisebb méretű, de nagyobb kapacitású és teljesítményű szenzorok, beavatkozóeszközök (aktuátorok), szabályzók és adók megjelenése;
- a második az internetes penetráció, az adatátviteli sávszélesség, valamit a 4G LTE-, WiFi-, Bluetooth-kapcsolatok bővülése, amelyek lehetővé teszik, hogy a különböző helyeken lévő eszközök a vezeték nélküli kapcsolatokat kihasználva sokféle módon csatlakozhassanak az internetre. A jövőben az 5G-hálózatok megjelenése a sávszélesség még radikálisabb növekedését irányozza elő, ami az IoT szempontjából kiemelt jelentőségű;
- harmadszor az adattárolási és adatfeldolgozó kapacitás növekedése és vele párhuzamosan a költségek csökkenése, ami lehetővé teszi a nagy mennyiségű adat kezelését;
- végül pedig az innovatív szoftveralkalmazások és analitikai eszközök fejlődése, beleértve a gépi tanulási technikákat is. (Zheng–Carter 2015)

Az IoT egyedileg címezhető, saját IP-címmel rendelkező, egymással összekapcsolt tárgyak, eszközök, objektumok világméretű hálózataként értelmezhető, amely a TCP/IP-t használja kommunikációs és címzési protokollként. Az IoT általában különféle szenzorok és aktuátorok hálózata. A szenzorok a környezetben beállt állapotváltozásokat detektálják a fizikai, kémiai, biológiai stb. érzékelési tartományukban, az aktu-

átorok pedig az érzékelt, majd kiértékelt adatok alapján beavatkoznak a működési folyamatokba. A már korábban ismertetett felhőalapú számítástechnika rendkívül fontos része az IoT-nek, hiszen ennek révén lehet igénybe venni a különböző tevékenységekhez szükséges számítási erőforrásokat. A mért adatokat többnyire internetes kapcsolaton keresztül a felhőben kezelik (tárolják, feldolgozzák), illetve a kiértékelt adatok szintén az interneten keresztül válnak hozzáférhetővé.

Az IoT tulajdonképpen az internet fejlődésének a következő lépcsőfoka, ami lehetővé teszi, hogy a mindennapos használati tárgyaink is az internetre kapcsolódjanak. Az IoT az emberek mindennapi életén, illetve az egyre terjedő okosotthonokon és okosvárosokon túl megjelenik szinte az összes társadalom működését biztosító infrastruktúrában, mint például az egészségügy, az energiaellátás, az ipari vállalatok, a közlekedés, szállítás, a kereskedelem, a közbiztonság, illetve a honvédelem. Az otthoni alkalmazások között már ma is megtalálhatók például az okosmérőórák, az otthonok energiamenedzsmentje és egyéb kényelmi funkciók IoT-eszközökkel való biztosítása. A különféle energetikai és ipari infrastruktúrákban alkalmazott szenzorokkal jelentősen csökkenthetők a költségek, folyamatosan monitorozható a rendszer működése, a városi közlekedés eredményesebben szabályozható. A közigazgatási rendszerekben az ügyfélszolgálatok hatékonysága javítható, illetve az online ügyfélszolgálatok terén nyújthatnak plusz lehetőségeket az IoT-megoldások. (Haig 2015) Mindezek alapján ma már kis túlzással kijelenthető, hogy az IoT az információs társadalom infrastruktúrájává válik. Mára szinte minden alapvető infrastruktúra (közlekedés, energia, vízellátás, biztonság, bank és pénzügy stb.) működésében megtalálhatók az IoT-alkalmazások kezdeti megoldásai, az elkövetkezendő években pedig ez a tendencia tovább fog erősödni.

2.2.2.2. Az IoT működése

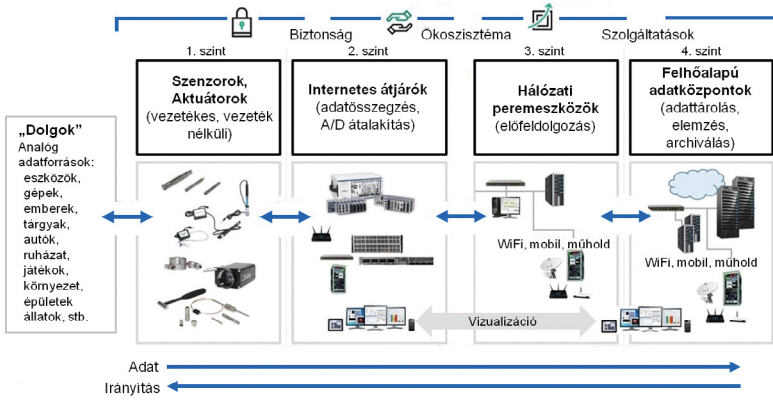
Fuller alapján az IoT felépítése általában négyszintű, amelyben megtalálhatók a szenzorok, az aktuátorok, a kommunikációs eszközök, a hálózati átjárók, a menedzselt szolgáltatások, valamint alkalmazások. Az IoT architektúrája az alábbi négy szintet tartalmazza (8. ábra):

1. szint: hálózatba kapcsolt eszközök, amelyek jellemzően vezeték nélküli érzékelők és aktuátorok;
2. szint: internetátjárók, amelyek adatösszegzőket és analóg-digitális átalakítókat tartalmaznak;
3. szint: hálózati peremeszközök, amelyek az adatok előfeldolgozását végzik;
4. szint: felhőalapú adatközpontok, amelyekben az adatok tényleges kezelése, tárolása és elemzése történik. (Fuller 2016)

Az 1. szinten lévő érzékelők és aktuátorok fizikai eszközök, amelyeket a működés jellegére és tartományára is utalva kiberfizikai eszközöknek is neveznek. A 2., 3. és 4. szinteken lévő folyamatokat pedig rendszerint informatikai eszközök vezérlik.

A szenzorok folyamatosan érzékelik a környezetünkben bekövetkezett állapotváltozásokat, és az ott lévő „dolgokból" mint analóg adatforrásokból az érzékelési tartományukban adatokat gyűjtenek. Ezek a szenzorok a fizikai, kémiai, biológiai stb. állapotváltozásokat egyaránt képesek detektálni, és azokból akár nagy mennyiségű adatot képesek generálni. Az aktuátorok pedig mint beavatkozóeszközök megváltoztathatják azokat a működési feltételeket, amelyeket a szenzorok érzékelnek. Így például egy aktuátor lekapcsolhatja egy berendezés tápegységét, a termosztátot, beállíthatja a légáramlást, vagy akár ipari összeszerelési folyamatban alkalmazott robotok esetében mozgathatja a robot karját és fogómechanizmusát. Az IoT-architektúra 1. szintje tehát magában foglal minden szenzort és aktuátort a régről ismert ipari eszközöktől kezdve a robotkamerákon, levegőminőség-érzékelőkön,

hőmérséklet-mérőkön keresztül a különböző egészségügyi érzékelő és beavatkozóeszközökig (például pulzusmérők) bezárólag.



8. ábra

Az IoT architektúrája

Forrás: FULLER (2016) alapján a szerző szerkesztése

Az adatok feldolgozása alapesetben a felhőalapú adatkezelő rendszerekben történik az IoT-architektúra 4. szintjén. Ugyanakkor bizonyos gyors, azonnali beavatkozást igénylő helyzetekben, amikor nincs idő arra, hogy az adatokat elküldjük mély adatfeldolgozásra a felhőbe, abban az esetben az adatelemzést az első szinten, a hálózat peremén kell megvalósítani. Ilyen helyzetek állhat elő például egészségügyi beavatkozásokban, műtétekben, önvezető autókban, különböző vészhelyzetekben vagy – a katonai alkalmazást tekintve – például egy barát-ellenség felismerő rendszer működésekor.

A különböző fizikai, kémiai, biológiai stb. környezeti változások az alkalmazott szenzorokkal alapvetően analóg módon érzékelhetők. Ezeket az adatokat az IoT 2. szintjén először digitalizálni, majd összegezni kell a további feldolgozáshoz. Az így gyűjtött adatok összegzését

és átalakítását az adatgyűjtő rendszerek végzik, az internetes átjárók pedig átveszik a digitalizált és összegzett adatokat, majd helyi hálózaton vagy az interneten továbbítják az IoT 3. szintjére további feldolgozás céljából.

Az A/D konverterek,[104] adatösszegzők és internetes átjárók a legtöbb esetben a szenzorok és aktuátorok közelében találhatók, és különböző módokon (mint például RS 232,[105] RS 458,[106] USB,[107] SPI,[108] WiFi, Bluetooth stb.) kapcsolódhatnak egymáshoz. Egy szivattyú például jó néhány érzékelőt, illetve a hozzá fizikailag csatlakoztatható analóg-digitális átalakítót és adatösszegzőt tartalmazhat. Ugyanígy egy repülőgép fedélzeti infrabesugárzás-jelzőhöz is fizikailag csatlakoznak azok az eszközök, amelyek a közeledő rakéta hajtóműjének hőkisugárzását reprezentáló analóg jeleket alakítják át digitális jelekké, és összegzik azokat.

A digitalizálást és összegzést követően az adatok a 3. szintre, a hálózatba jutnak a hálózati peremeszközökhöz. Ezek a peremeszközök végzik el a digitalizált adatok előfeldolgozását, mielőtt azok a felhőalapú adatközpontokba kerülnének. A hálózat peremén végzett előfeldolgozásra általában azért van szükség, mert a hatalmas mennyiségű szenzoradat jelentős sávszélességet foglal, illetve túlterhelheti az adattároló és feldolgozóközpontokat. Ez az a szint, ahol a többféle elemzést végző informatikai rendszereket is alkalmazzák. Az előfeldolgozást végző hálózati peremeszközök általában az adatgyűjtő szenzorokhoz közeli helyeken találhatók, de elhelyezhetők akár távoli helyiségekben is.

A hálózat peremén végzett előfeldolgozás után az adatok a 4. szinten lévő, nagy kapacitású, többnyire felhőalapú adatközpontokba kerülnek mélyelemzésre. Itt történik az előfeldolgozott adatok részletes kiérté-

---

[104] Analóg-digitális átalakítók.

[105] Recommended Standard 232 – RS 232, pont-pont kapcsolatot biztosító távközlési adatátviteli szabvány.

[106] Recommended Standard 458 – RS 458, szimmetrikus adatátviteli módot leíró szabvány.

[107] Universal Serial Bus – USB, univerzális soros busz.

[108] Serial Peripheral Interface – SPI, nagy sebességű soros szinkron busz.

kelése és esetlegesen más szenzoradatokkal való összevetése, fúziója. Az értékelés eredményeként a rendszer különféle visszacsatolásokat alkalmazhat, például a kialakított vezérlő és irányító parancsokat visszajuttatva az 1. szintre, megtörténhet az aktuátorok működtetése, beavatkozása a rendszer működési folyamataiba. (FULLER 2016; KOLLÁR 2017a)

A katonai felderítő rendszerekben alkalmazott felügyelet nélküli szenzorhálózatok és az adatfúziós feldolgozó rendszerek hasonló funkcióval bírnak. A harctéren a környezeti adatok megszerzése a különféle harctéri érzékelőkkel történik, és ugyanezek az eszközök végzik a digitális átalakítást is. A különböző paraméterű és tulajdonságú adatok a szenzorrendszer adatgyűjtő és előfeldolgozó egységével kapcsolódnak a hálózathoz. Ez képezi a szenzorhálózat peremeszközét, ahol a nagy mennyiségű adat előfeldolgozása megtörténik. A részletes és mély adatelemzés és ez alapján a felderítési információ előállítása a fúziós adatfeldolgozó központban valósul meg.

2.2.2.3. Az IoT kommunikációs megoldásai

Az IoT-technológia egyik sarkalatos pontja a szenzorok, aktuátorok, valamint az adattárolás és adatfeldolgozás mellett az alkalmazott kommunikációs megoldások. Az IoT-rendszerekben a kommunikációra mind vezetékes, mind pedig vezeték nélküli megoldásokat egyaránt alkalmaznak. Az elérhető hatótávolság szempontjából az IoT-kommunikáció lehet:

- kis hatótávolságú (maximum néhányszor 100 m);
- nagy hatótávolságú (maximum néhányszor 10 km).

Az 1. és 2. szinten alapvetően kis hatótávolságú és kis energiaigényű kommunikáció a jellemző, míg a 3. és 4. szinten már elvárás lehet a nagyobb hatótávolság biztosítása. A peremeszközökkel való kommunikáció esetében szintén lehetőség szerint célszerű a kis energiafelhasználású kommunikációs technológiák alkalmazása.

A vezetékes kommunikációra számtalan megoldás alkalmazható. A legelterjedtebbek közé sorolhatjuk az Ethernet általános célú hálózati szabványt vagy a PLC-kommunikációt,[109] amely az elektromos hálózaton keresztül valósít meg adatátvitelt. A vezetékes kommunikáció alkalmazása az 1. és 2. szinten, vagyis a szenzorok, aktuátorok és internetes átjárók között, esetleg a 3. szinten elhelyezkedő és az előfeldolgozást végző peremeszközöknél kevésbé jellemző. A 4. szinten, a fixen telepített, nagy kapacitású adatközpontokban viszont, ahol nagy mennyiségű adatfeldolgozást kell végezni és nagy méretű adatállományokat kell mozgatn, az adattároló és adatelemző elemek közötti kommunikációra a vezetékes megoldások nagyon jól alkalmazhatók.

Az IoT kommunikációs technológiái között az egyre hatalmasabb mennyiségű szenzor, aktuátor – amelyek igen gyakran nem fix helyen, hanem mozgás közben működnek – és az IoT többi eleme közötti kapcsolatra döntően a vezeték nélküli megoldások jellemzők. A vezeték nélküli, kis hatótávolságú technológiák közé az alábbiak sorolhatók:

- BLE,[110] amely kis energiaigényű, de a hagyományos Bluetooth technikához hasonló hatótávolságot biztosít;
- LiFi,[111] amely a WiFi-szabványhoz hasonló vezeték nélküli kommunikációs mód, azonban nem a rádiófrekvenciás tartományban, hanem – a nagyobb sávszélesség miatt – az optikai tartományban működik;
- NFC,[112] amely maximum 10 cm-es távolságban tesz lehetővé két eszköz közötti kommunikációt;
- RFID,[113] amely a rádiófrekvenciás tartományt használja fel beágyazott címkékben tárolt adatok kiolvasására;
- Thread, amely az IEEE 802.15.4 szabványon alapuló IPv6-os címzést használó hálózati protokoll;

[109] Power-line Communication – PLC.
[110] Bluetooth Low Energy – BLE.
[111] Light-Fidelity – LiFi.
[112] Near-Field Communication – NFC.
[113] Radio-Frequency Identification – RFID.

- WiFi, amely az IEEE 802.11 szabványon alapuló, széles körben használt, helyi hálózati hozzáférést biztosító, vezeték nélküli szabvány, lehetővé teszi, hogy az eszközök megosztott hozzáférési ponton keresztül kommunikáljanak egymással;
- WiFi Direct, amely a hagyományos WiFi egy változata, ahol az eszközök hozzáférési pont nélkül képesek egymással kommunikálni;
- Z-Wave, amely a WiFi-nél alacsonyabb energiaigényű, kis hatótávolságú, rövid késleltetésű és kisebb adatsebességű kommunikációs protokoll, amelyet elsősorban otthonok automatizálásnál alkalmaznak;
- ZigBee, amely szintén az IEE 802.15.4 szabványon alapuló személyi hálózatokban alkalmazott kommunikációs protokoll, alacsony fogyasztás, adatsebesség, költség és nagy áteresztőképesség jellemzőkkel. (Cinkler 2017)

A fenti technológiák alapvetően a szenzorok, aktuátorok és az internetes átjárók, illetve hálózati peremeszközök közötti kommunikáció megvalósítására szolgálnak. Az eszközök általában egymás közelében találhatók, emiatt elegendő a kis hatótávolságú kommunikáció, ami kis kisugárzott teljesítményt is jelent. A kis energiafelhasználás alapvető fontosságú ahhoz, hogy egy telepített szenzor elegendően hosszú ideig képes legyen működni, hiszen itt nemcsak az adóteljesítmény biztosításához kell a tápellátás, hanem a szenzor alapfunkciójához, vagyis az érzékeléshez, illetve a szenzorokat és aktuátorokat vezérlő különböző parancsok vételéhez is. A nagy adatátviteli sebesség sok esetben nem elvárt követelmény, hiszen az érzékelők által vett jelek, mért paraméterek, illetve az aktuátorok működtetéséhez szükséges jelek nem nagy adatállományúak, emiatt az adatátvitel akár néhány 10–100 kbit/s sebességű adatkapcsolaton is megvalósítható, mint például a ZigBee, Z-Wave, RFID vagy az NFC esetében.

A vezeték nélküli, nagy hatótávolságú kommunikációs megoldások közé az alábbiak sorolhatók:

- 2G, amely a GSM-szabvány szerinti kis adatsebességű mobil cellás technológia;

- 3G, amely az UMTS rendszerű közepes adatsebességű mobil cellás kommunikáció;
- 4G LTE, amely a mobilhálózatok nagy sebességű kommunikációs technológiája;
- LTE-Avanced, amely a 4G LTE kommunikációs technológia továbbfejlesztett változata, nagy áteresztőképességgel és rövid késleltetéssel;
- LPWAN,[114] amely költséghatékony, kis energiafelhasználású, nagy távolságú, de kis adatsebességű kommunikációt biztosít; valamint
- a műholdas kommunikáció számos típusa, de köztük is jellemzően a kis antennaméretű VSAT,[115] amellyel keskeny és széles sávú adatátviteli kapcsolat egyaránt megvalósítható.

Az LPWAN az IoT területén az egyik legnagyobb ütemben fejlődő kommunikációs alkalmazáscsoport, amely számos technológiát foglal magában. Ezek közül a legjelentősebbek és legelterjedtebbek az alábbiak:

- LoRaWAN,[116] amely nagy kiterjedésű hálózati alkalmazásokban használt alacsony költségű, kis energiafelhasználású és kis adatsebességű kommunikációs technológia;
- Sigfox, a szabadon felhasználható ISM-sávban[117] működő, kis adatátviteli sávszélességű kommunikációs technológia, amely különböző M2M-alkalmazásokban (intelligens mérők, betegmonitoring, környezetvédelmi szenzorok stb.) előnyösen alkalmazható;
- NB-IoT,[118] amely a mobilszolgáltatók jelenleg meglevő hálózatain futó és az IoT-re optimalizált új, szabványosított mobiltechnológia, ahol a hálózatba kapcsolt elemek alacsony sávszélességen kommunikálnak egymással;

[114] Low Power Wide Area Network – LPWAN.
[115] Very Small Aperture Terminal – VSAT.
[116] Long Range Radio – LoRa.
[117] Industrial, Scientific, Medical Band – ISM.
[118] Narrow Band IoT – NB-IoT.

- Neul, amely az 1 GHz alatti sávban működő, alacsony költségű és kis energiaigényű, skálázható, nagy lefedettséget biztosító kommunikációs megoldás. (Cinkler 2017)

1. táblázat

Az IoT-ben alkalmazott, jellemző adatkommunikációs technológiák összehasonlítása

Technológia	Frekvenciasáv	Hatótáv	Adatsebesség	Teljesítmény
BLE	2,4 GHz	35 m	1–3 Mbit/s	10 mW
NFC	13,56 MHz (ISM)	10 cm	100–420 kbit/s	1–2 mW
RFID	13,56 MHz; 860–930 MHz; 2,4–5,4 GHz	1 m	423 kbit/s	1 mW
Thread	2,4 GHz	160 m	250 kbit/s	100 mW
WiFi, WiFi Direct	2,4/5 GHz	100 m	10–500 Mbit/s	1 W
Z-Wave	900 MHz	30 m	9,6/40/100 kbit/s	1 mW
ZigBee	2,4 GHz	10–160 m	250 kbit/s	100 mW
2G (Edge)	0,9/1,8 GHz	10–25 km	384 kbit/s	1 W
3G (UMTS)	0,9/1,8/2,1 GHz	10–25 km	0,73–56 Mbit/s	1 W
4G LTE	0,9/1,8/2,1/2,6 GHz	10–25 km	10 – néhány 100 Mbit/s	1 W
LoRaWAN	433/780/868/915 MHz	15 km, városban 2–5 km	0,3–50 kbit/s	alacsony
Sigfox	900 MHz (ISM)	30-50 km, városban 3–10 km	0,01–1 Mbit/s	alacsony
NB-IoT	1,8/2,1/2,6 GHz	~ 15 km	~ 250 kbit/s	alacsony
Neul	900 MHz (ISM)	10 km	100 kbit/s	alacsony

Forrás: 11 IoT (2015) alapján a szerző szerkesztése

A nagy hatótávolságú IoT-kommunikációban a masszív és a kritikus felhasználói igények az elsődlegesek. A masszív IoT-adatkapcsolatokat a nagy mennyiségű összekapcsolt eszköz, a kis adatméret és adatsebesség, az olcsó eszközök és az alacsony energiafogyasztás jellemzi.

Erre a célra alkalmasak többek között az ismertetett LoRaWAN, Sigfox, Neul stb. megoldások. A kritikus IoT-kommunikációs igények esetén viszont a kimagasló megbízhatóságot, a nagyfokú rendelkezésre állást, a rövid késleltetést és a nagy adatátviteli sávszélességet kell biztosítani. A cellás rendszereken megvalósított IoT-kommunikáció, különösen a 4G LTE és az LTE-Advanced technológia mindezt biztosítja, a jelenleg fejlesztés alatt álló 5G-technológia pedig vélhetően mindkét elvárásnak megfelel majd.

Az 5G-hálózat a maihoz képest jelentősen alacsonyabb késleltetéssel, lényegesen több felhasználó és eszköz kommunikációs igényeit elégíti ki. Az 5G-hálózat kialakításának célja nem pusztán az adatátviteli sebesség növelése, hanem elsősorban az évtized végére prognosztizált több milliárd eszköz összekapcsolása. Mindezt a tervek szerint úgy valósítja meg, hogy minden eszköz számára a használattól függő, illetve az adatmennyiség, adatsebesség, robusztusság stb. követelményeknek megfelelő internet-hozzáférést biztosít. Az 5G-hálózat kialakítása 2020-ig fokozatosan valósul meg a jelenlegi legfejlettebb LTE, LTE-Advanced és az LTE-Advanced Pro mobiltechnológiák egyes szintjein. Az 5G-hálózat kiépítésével válhatnak teljeskörűen elérhetővé a ma megkezdett okosotthon-, okosváros-, okosautó-koncepciók stb.

Az 5G fejlesztésére megalakított szövetség az NGMNA[119] által kiadott 5G fehér könyv számos követelményt irányoz elő, amelyet az újonnan létrejövő hálózatnak teljesítenie kell. (NGMN 2015) Ezek közül néhány:

- széles sávú hozzáférés mindenhol, sűrűn lakott területeken, belső terekben egyaránt (okosirodák, széles sáv tömegrendezvényeken stb.);
- magas szintű felhasználói mobilitás, járművekben is (nagy sebességű vonatokon, repülőeszközökön, mobil hotspotok stb.);

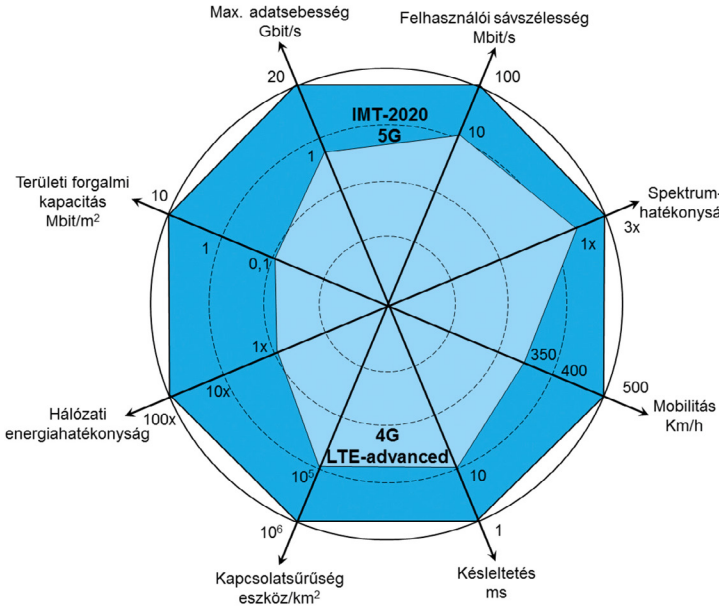
[119] Next Generation Mobile Networks Alliance – NGMNA.

- masszív, alacsony költségű, nagy hatótávolságú gépi kommunikáció az IoT-alkalmazásokban (szenzorhálózatok, folyamatos mobil videomegfigyelő rendszerek, okosruházat stb.);
- rendkívül rövid késleltetésű, extrém valós idejű kommunikáció;
- rugalmas veszélyhelyzeti kommunikáció (például katasztrófahelyzetekben);
- ultra magas szintű rendelkezésre állás és megbízhatóság (automatikus forgalomszabályzás, együttműködő robotok, e-egészségügy, távsebészet stb.); valamint
- hatékony energiafelhasználás (kis energiaigényű eszközök).

A Nemzetközi Távközlési Egyesület[120] ajánlása szerint az 5G-hálózat elvárt képességnövekedését a 4G LTE-Advanced technológiához képest a 4. grafikon szemlélteti. Ez alapján látható, hogy a mai legkorszerűbb mobilhálózati technológiához képest az 5G szinte minden elvárt területen legalább egy nagyságrenddel jobb képességet mutat. Különösen szembeötlő az energiahatékonyság, a kapcsolatsűrűség és a sávszélesség terén tervezett javulás, amelyek az IoT-alkalmazásokban kiemelt jelentőséggel bírnak.

A követelmények teljesítését új, heterogén rádiós rendszerek üzemeltetésével kívánják biztosítani, ahol a hagyományos interfészek mellett új rádiós interfészeket is telepítenek, valamint okos- és aktív rádiós együttműködéssel valósítják meg az interferencia csökkentését. A tervezet szerint az új rádiós interfész működését a mikrohullámú frekvenciatartományban, 6–100 GHz között kell megvalósítani. (Cinkler et al. 2016) Ez alapján pedig az USA Szövetségi Távközlési Bizottsága 2016 júliusában elfogadta, hogy az 5G-hálózat a 28, 37 és 39 GHz-es frekvenciasávokon fog működni. (Snider 2016)

[120] International Telecommunication Union – ITU.



4. grafikon

Az 5G-hálózat tervezett képességnövekedése a 4G LTE-advanced hálózathoz viszonyítva

Forrás: ITU RM 2083-0 (2015) alapján a szerző szerkesztése

A leírtak alapján megállapítható, hogy az IoT megvalósíthatóságának kulcsa a hálózati kommunikációs megoldásokban rejlik. A szenzorok, végberendezések telepítése és elhelyezkedése, illetve azok egyre inkább elvárt mobilitása miatt az IoT negyedik szintjét leszámítva a hálózati kommunikációra a vezeték nélküli megoldások jöhetnek szóba. Erre az előbbiekben bemutatottak szerint számtalan jó megoldás létezik már ma is, ugyanakkor a valódi áttörés az 5G-hálózat kiépítésével és széles körű elterjedésével jön létre.

A mobil környezet miatt azonban a vezeték nélküli kommunikáció alkalmazása az IoT-rendszerek elleni fenyegetések tárházát is jelentősen

növeli. Mivel a hálózat alapvetően az elektromágneses teret használja kommunikáció céljára, ezért az informatikai rendszerek ellen alkalmazott szoftveres logikai támadásokon kívül az e tartományban indított fenyegetéseknek (például felderítés, adatlopás, elektronikai zavarás stb.) is ki van téve, ezért ez a kibertérben jelentkező, új típusú kihívások tárházát növeli. Nemcsak a hatalmas mennyiségű adat kezelése jelent komoly biztonsági kihívást, hanem az új típusú infrastruktúrák létrejöttéből fakadó újfajta logikai és fizikai sérülékenységek kezelése is. A következő fejezetekben e kérdésekkel is foglalkozunk.

2.2.2.4. Az IoT katonai alkalmazhatósága

Mint az előzőekből is látható, az IoT mára az egyik legfelkapottabb és legnagyobb jelentőségű, az emberek életét alapjaiban megváltoztató technológiai innovációnak számít. A polgári életben való elterjedése már most elindult, és a mobilkommunikációs technológiák – köztük is az 5G-hálózat – további fejlődése nyomán a következő évtizedre meghatározóvá válik. Mindez természetszerűleg nem hagyja érintetlenül a védelmi, biztonsági, katonai szektort sem. Az IoT katonai felhasználásának kutatása a polgári alkalmazások megjelenését követően megindult, és ma már számos ország hadereje, illetve a NATO kutatás-fejlesztéssel foglalkozó ügynöksége is nagy energiát fektet e technológia védelmi célú meghonosításába.

Az IoT katonai alkalmazása ugyanakkor nem új keletű koncepció. A 90-es évek végén kialakított hálózatközpontú hadviselési elv[121] (lásd később) a fizikai, az információs és a kognitív tér integrációja révén tulajdonképpen hasonló struktúrát vázol fel. A hálózatközpontú hadviselésben felvázolt érzékelők, beágyazott eszközök, adatbázis-technológia és szoftverelemzés hálózatba való összekapcsolása szorosan tükrözi az IoT lényegét. Az akkori technikai feltételek azonban még nem

[121] Network Centric Warfare – NCW.

tették lehetővé a szenzorokból, információs rendszerekből és a végrehajtói szintből álló hálózat kialakítását. Mára a hálózatos technológia, különösen a nagy adatsebességű kommunikációs megoldások, a felhőalapú számítástechnika, illetve a szenzorok fejlődése mindezt elérhető közelségbe hozta a védelmi szférában is.

Az USA védelmi fejlesztési hivatalának, a DARPA-nak az új kutatási projektje is az IoT keretében a szenzorok és a mesterséges intelligencia kutatására fókuszál. A kutatás-fejlesztés eredményeként azt várják, hogy az eddiginél hatékonyabb felderítőképességet tudnak kialakítani. A jelenleg működő felderítőberendezések, szenzorok mellett kis méretű és olcsó, tömegesen alkalmazható IoT-érzékelőkkel tervezik monitorozni a kritikus csomópontokat, út- és vasútvonalakat, hidakat, illetve a kritikus infrastruktúrákat és környezetüket. A kiterjedten és nagy mennyiségben telepített szenzorokra alapozott IoT-hálózat így nagyobb eredményességgel és hatékonysággal képes még időben felfedezni többek között a piszkos bombákat, a radioaktív sugárzást és egyéb veszélyes eszközöket, anyagokat, amelyek az infrastruktúrát és azokon keresztül a társadalmat fenyegetik. (Murison 2016)

Az IoT katonai alkalmazásának egyik legnagyobb előnye, hogy a nagy mennyiségű és olcsó szenzorokra épülő hálózatnak köszönhetően a korábbiakhoz képest lényegesen több adat szerezhető be az ellenség helyzetéről, technikai eszközeiről, képességeiről, illetve a harctéri környezet változásairól. Az adatok nagy teljesítményű idősoros feldolgozásnak köszönhetően sokkal jobban értelmezhetővé válik a változások időbeli lefolyása. (Kollár 2017b) Az adatokat az IoT-elvnek megfelelően már a szenzorokban vagy azok közvetlen közelében digitalizálják, összegzik, előfeldolgozzák (az IoT 2., 3. szintjén), így ezen a szinten várhatóan kiszűrhetők a megtévesztő információk, illetve a téves, hamis riasztások. A nagy mennyiségű előfeldolgozott adatból az adatközpontokban adatfúziós technikákkal kialakított információt, illetve mesterségesintelligencia-alkalmazásokkal a helyzet megértéséhez szükséges tudást lehet előállítani, amelyet a parancsnoki döntéshozatalban lehet felhasználni.

A NATO Tudományos és Technológiai Szervezete[122] 2016-ban szintén megkezdte az IoT katonai alkalmazhatóságának kutatását. (IST-147 2016) Az IST-147 jelzésű projekt a korábban megkezdett IST-ET-076 „Katonai tárgyak internete",[123] illetve az IST-ET-075, „Szenzorok és kommunikációs hálózatok integrálása"[124] projektekre alapozva vizsgálja az IoT felhasználhatóságát. A kutatás az alapvető katonai műveletek, a helyzetismeret, az egészségügyi ellátás, a határvédelem, illetve az energiagazdálkodás területeire fókuszál. Az STO az IoT katonai alkalmazásának három fő területét jelöli meg, az alábbiak szerint:

- logisztika – az összfegyvernemi műveletek logisztikai támogatásának vezetési és irányítási lehetőségei;
- helyzetismeret – a harchelyzet folyamatos értelmezése, amely magában foglalja az érzékelést, megfigyelést, fenyegetésjelzést és -azonosítást, célmeghatározást, célmegjelölést, a harci technika és az előerő állapotfigyelését, illetve a harctéri környezet változásának folyamatos megfigyelését;
- egészségügyi ellátás – harctéri egészségügyi monitoring, betegfelügyelet stb.

A NATO IoT-kialakítása során alapvető fontosságú követelményként fogalmazódik meg:

- a fejlett M2M-kommunikáció, a robosztusság és a skálázhatóság követelményeit kielégítő hálózati kommunikációs architektúrák kialakítása;
- a nagy mennyiségű adat gyors, fúziós feldolgozását lehetővé tevő adatelemzési technológiák fejlesztése, valamint
- az IoT katonai felhasználhatóságát fenyegető kockázati tényezők és az azok kezelésére szolgáló megoldások meghatározása, mint

[122] Science and Technology Organization – STO.
[123] Internet of Military Things – IoMT.
[124] Integration of Sensors and Communication Networks.

például az IoT-eszközök és a -felhasználók azonosítása, hitelesítése, az objektumszintű védelmi megoldások alkalmazása, illetve a különböző – civil környezetben már bevált – biztonsági megoldások katonai alkalmazhatóságának vizsgálata.

Az IoT katonai alkalmazhatóságával kapcsolatban az egyik legnagyobb kihívást a biztonság jelenti. Az IoT polgári alkalmazása is számos kockázati problémát vet fel, mint például a szenzorok adatainak megváltoztatása, kompromittálása, a hálózati kommunikáció megzavarása vagy az aktuátorokat vezérlő parancsok megváltoztatása. Mindezek pedig a katonai területen fokozottan jelentkezhetnek.

Az IoT harctéri működéséből fakadóan a hálózati kommunikáció alapvetően vezeték nélküli megoldásokon alapul, ami már önmagában számos biztonsági problémát vet fel. A nem megfelelően biztonságos hálózat hozzáférést tesz lehetővé az ellenség számára a szenzorok által gyűjtött adatokhoz, a kiértékelt információkhoz, illetve a parancsnoki döntésekhez. A vezeték nélküli kapcsolaton keresztül nagyobb lehetőség nyílik az adatok manipulációjára, az adatkapcsolat megszakítására, ezáltal pedig a saját helyzetismeret befolyásolására. E biztonsági problémák kezelésére a katonai feladatoknak megfelelő biztonsági megoldásokat kell kialakítani. E biztonsági megoldások megtalálása és meggyőző működése az egyik meghatározó feltétele a katonai IoT-rendszerek széles körű elterjedésének.

2.2.3. Szenzorhálózatok

2.2.3.1. A szenzorok és szenzorhálózatok fogalma, jellemzői

Az IoT-rendszerek tárgyalásakor – azok működéséből és felépítéséből fakadóan – már érintettük a szenzorokat mint az IoT kiberfizikai eszközeit, amelyek a környezetben lévő állapotváltozások érzékelése, illetve a különböző beavatkozási folyamatok révén az IoT-megoldások egyik

lényegi elemét adják. Mivel az IoT működése szempontjából ezek képezik a hálózat első szintjét, ezért ezek az eszközök adják a hálózat elleni fenyegetések, támadások első felületét is. E fenyegetések alapvetően a működésük jellegéből, illetve a kommunikációs megoldásaikból fakadóan alapvetően az elektromágneses tartományban jelentkeznek, ezért ebben az alfejezetben röviden ismertetjük a szenzorok felépítését, érzékelési módjaikat, illetve a hálózatos alkalmazás lehetőségeit mind a polgári, mind pedig a katonai környezetben.

A szenzorok olyan berendezések, amelyek a megfigyelt környezet fizikai, kémiai vagy biológiai állapotváltozásait érzékelik, és a mért mennyiséget vagy paramétert információhordozó jellé alakítják. A szenzorok a frekvenciaspektrum különböző tartományában működnek, az általuk vett jelek továbbíthatók, erősíthetők, szűrhetők és feldolgozhatók. A technológiai fejlődésnek köszönhetően ma már tömegesen állíthatók elő igen kis méretű és olcsó szenzorok, amelyek sokoldalú felhasználhatóságuknak köszönhetően széles körben elterjedtek a polgári szférában (például egészségügy, gyártásmonitorozás, környezetvédelem, okoskörnyezet stb.) és a katonai rendszerekben (például harctéri érzékelőrendszerek, katonák testén, ruházatán elhelyezett szenzorok) egyaránt.

A szenzorokat különböző szempontok szerint osztályozhatjuk, a legelterjedtebb azonban az érzékelt fizikai hatás szerinti energiaszemléletű csoportosítás. Eszerint a szenzorok az alábbi energiákat érzékelik:

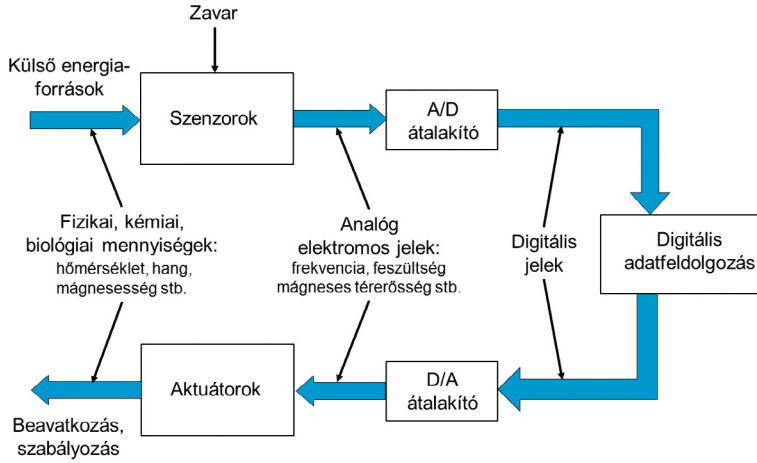
- hőenergia;
- mechanikai energia;
- mágneses energia;
- villamos energia;
- elektromágneses energia;
- kémiai energia.

A szenzorok a környezetben lévő valamilyen energia valamely paraméterének megváltozását érzékelik, és a mért jelnek megfelelő különféle változókat állítanak elő. Ezek a változók képezik a szenzorok kimeneti

jeleit, amelyeket feldolgozva lehet bizonyos szabályozási folyamatokat végrehajtani. A mérendő mennyiség hatására a szenzor kimenetén jellemzően tapasztalható jelenségek az alábbiak lehetnek:

- ellenállás-változás,
- kapacitásváltozás,
- induktivitásváltozás,
- feszültség, feszültségváltozás,
- áram, áramváltozás, valamint
- töltésfelhalmozódás, feltöltöttségváltozás. (BÁNLAKI–LOVAS 2012)

A szenzorok bemeneti és kimeneti jeleit, valamint általános környezetét és működési folyamatát egy szabályzó rendszerben a 9. ábra szemlélteti.



9. ábra

A szenzorok általános működési környezete és működési folyamata

Forrás: a szerző szerkesztése

A szenzorok a következő fő alkotóelemekből épülnek fel:

- érzékelő egységek, amelyek lehetnek akusztikus, szeizmikus, infravörös, mágneses, optikai, nyomás, kémiai, biológiai, nukleáris, mechanikus, termikus érzékelők;
- központi feldolgozóegység;
- memória a mért adatok tárolására és alkalmazások futtatására;
- rádió adó-vevő, amely biztosítja a kommunikációs kapcsolatot a többi csomóponttal, valamint
- energiaellátó egység.

A mai modern szenzorok opcionálisan tartalmazhatnak még beépített GPS-vevőt is, lehetővé téve a pozícióadatok meghatározását és a térinformatikai rendszerek (GIS)[125] adatbázisaihoz való hozzáférést. A helyadatok kiemelten fontosak a különféle felügyelet nélküli harctéri szenzorokban, ahol a kijuttatás módja miatt az egyes szenzorok pozíciója csak a GPS-adatok alapján állapítható meg. Az érzékelt állapotváltozások mellett nagymértékben hozzájárulnak az érzékelt tárgy, objektum pontosabb meghatározásához, az ellenséges harcrend megállapításához stb. (Bognár 2017)

A szenzorokat ma már a legtöbb esetben a szenzoradatok megosztása és a hatékonyabb működés érdekében hálózatba szervezve alkalmazzák. Az IoT-rendszerekben való alkalmazás is tulajdonképpen a hálózatos felhasználást jelenti. Szenzorhálózatoknak a több szenzor együttes működésével megvalósuló komplex érzékelő rendszereket tekintjük. Az egyes szenzorok, csomópontok[126] közötti kommunikáció biztosítása, a hálózat kialakítása leggyakrabban a már korábban ismertetett vezeték nélküli technológiák alkalmazásával valósul meg. Vezeték nélküli szenzorhálózatokban[127] több száz vagy akár több ezer hálózatba kapcsolt érzékelőt alkalmaznak, amelyek összehangolt működésük révén alkalmasak

[125] Geographic Information System – GIS.
[126] Node.
[127] Wireless Sensor Network – WSN.

a környezet állapotváltozásainak rögzítésére, ezáltal pedig egy adott terület vagy objektum időleges vagy folyamatos monitorozására.

A szenzorok a mért paramétereket egy kitüntetett csomóponton, az átjárón[128] keresztül továbbítják az adatfeldolgozó központba. Az átjáróknak fontos szerepe van a szenzorhálózatokban, mivel a szenzorcsomópontok csak korlátozott tárhellyel, számítási kapacitással és energiával rendelkeznek, így rajtuk komplex, számításigényes algoritmusokat nem lehet futtatni. A gateway feladata a különböző szenzorokból származó adatok összegzése és előfeldolgozása, valamint eljuttatása a felhasználás helyére. Az átjárók – mivel általában nagyobb adattároló kapacitással rendelkeznek – alkalmasak az adatok hosszabb távú tárolására, és biztonsági mentéseket is képesek végezni. (Bognár 2017)

2.2.3.2. A szenzorhálózatok architektúrája

A rendkívül sokféle szenzorhálózat működését egy általános hivatkozási modell írja le, amely meghatározza, hogy az egyes csomópontok milyen részfeladatokat látnak el, azokat milyen keretek, szabályok között teszik, illetve milyen interfészeken keresztül tudnak egymással kapcsolatot létesíteni. Általánosságban a számítógép-hálózatokban alkalmazott hivatkozási modellek rétegeket definiálnak, amelyek a hálózat működésének egy-egy önálló szeletét képviselik. Minden réteg egy meghatározott feladattal rendelkezik, amelynek végrehajtásához a közvetlenül alatta található rétegtől kapja az információkat, és az általa előállított eredményt a hierarchiában felette elhelyezkedő rétegnek továbbítja. A leginkább elterjedt hivatkozási modell az OSI-modell,[129] amely az alábbi hét réteget definiálja:

- fizikai réteg,
- adatkapcsolati réteg,

[128] Gateway.

[129] Open Systems Interconnection Reference Model – OSI.

- hálózati réteg,
- szállítási réteg,
- viszonyítási réteg,
- megjelenítési réteg és
- alkalmazási réteg.

A szenzorhálózatoknak ugyanakkor a számítógép-hálózatokhoz képest számos speciális követelményt kell kielégíteniük, mint például:

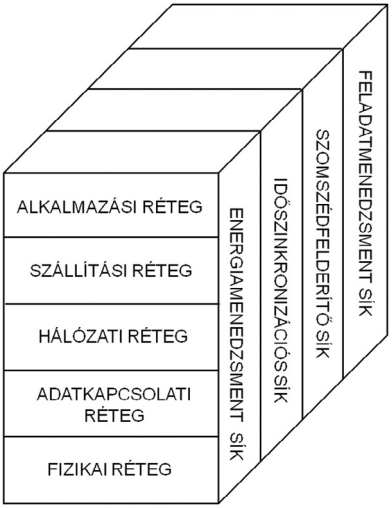
- a rendszer könnyű karbantarthatósága, távoli felügyelete, átprogramozhatóságának lehetősége, amely követelmény teljesíthetőségét nehezíti a dinamikus, önszerveződő hálózati topológia;
- a nagy területi lefedettség, a mért objektumra vonatkozó többforrású adatgyűjtés, ami még több, sokszor heterogén szenzorcsomópontot jelent, ez pedig még bonyolultabb hálózati topológiát eredményez;
- megbízható, alacsony késleltetésű, lehetőség szerint titkosított kommunikáció, amely időszerű adatszolgáltatást biztosít nagyfokú hibatűréssel, illetve adatvesztés elleni védelemmel;
- az adatok azonnali feldolgozhatóságának, értelmezésének, korrelációjának, valamit a különböző forrásból származó adatok fúziójának biztosítása, amely a szenzorok korlátozott számítási és tárhelykapacitása, illetve a számítási algoritmusok energiaigénye miatt csak nehezen teljesíthető. (Winkler et al. 2008; Rawat et al. 2014)

A fenti korlátok miatt a hagyományos számítógépes hálózatban alkalmazott architektúrák és protokollok nem alkalmazhatók hatékonyan. A fenti elvárások fokozottan jelentkeznek a különböző biztonsági célú, illetve védelmi jellegű, katonai szenzorhálózatok esetében, ahol a gyors, sok esetben ad-hoc jellegű telepíthetőség, az összadatforrású felderítés és adatfúzió követelményének való megfelelőség, illetve a biztonságos kommunikáció alapvető elvárás. Mindezek alapján, valamint a szűkös

erőforrások hatékony kihasználása miatt a szenzorhálózatokra optimalizált hálózati architektúra és protokollok kidolgozása szükséges.

A szenzorhálózatokban az OSI-modell ötréteges változatát alkalmazzák, mivel néhány réteg és azok funkciói e rendszerekben nem szükségesek, és nem is valósíthatók meg. A szenzorhálózatokra jellemző hivatkozási modellt protokollveremnek[130] nevezik, amely az alábbi öt réteget definiálja (10. ábra):

- fizikai réteg,
- adatkapcsolati réteg,
- hálózati réteg,
- szállítási réteg, valamint
- alkalmazási réteg. (Nagy 2012a)



10. ábra

Szenzorhálózatok protokollvermének rétegei és síkjai

Forrás: Nagy 2012b alapján a szerző szerkesztése

[130] Protocol Stack.

A fizikai réteg magában foglalja azokat az eszközöket és eljárásokat, amelyek az adatok átviteléhez, az adatkapcsolat létrehozásához, fenntartásához és bontásához szükségesek. Szenzorhálózatokban leginkább a rádiófrekvenciás adatátvitel a jellemző, amelynél a kis energiafelhasználás sokszor fontosabb, mint az adatátviteli sebesség és a késleltetés. Azonban – mint láttuk – már vannak kis energiaigényű, de nagy távolságú és nagyobb kapacitású átviteli megoldások is, mint például az LPWAN, illetve az LTE-Advanced vagy a most fejlesztés alatt álló 5G-technológia.

Az adatkapcsolati réteg legfőbb feladatai a keretképzés, a hibadetektálás, a forgalomszabályozás, valamint a közeghozzáférés vezérlése. A szenzorhálózatokban a nagyszámú és egyidejű kommunikációs igény miatti ütközések elkerülése érdekében statikus vagy dinamikus többszörös közeghozzáférési módokat alkalmaznak. A statikus megoldások esetében az átviteli csatorna FDMA-, TDMA- vagy CDMA-eljárással előre felosztódik. E módszerek viszonylag könnyen megvalósíthatók, ugyanakkor a szenzorhálózatok dinamikus hálózati topológiáját nehezen kezelik. A dinamikus közeghozzáférési módszerek már a csomópontok aktív közreműködését is felhasználják az optimális csatornafelosztáshoz, mint például a vivőjel-érzékeléses többszörös hozzáférés (CSMA)[131] vagy a lekérdezésen alapuló Polling-módszer, illetve az S-MAC,[132] ahol az egymás szomszédságában lévő csomópontok az előre beállított alvás-ébrenlét ütemezés szerint, egymáshoz szinkronizáltan, periodikusan alvó és működő módban vannak. Ezzel jelentősen növelhető az energiagazdálkodás hatékonysága, illetve a rendszerek önszerveződése, skálázhatósága és adaptivitása. (Callaway 2003)

A hálózati réteg feladata szenzorhálózaton belüli adattovábbításra használt útvonal megválasztása, más néven a routing, amely meghatározza, hogy az egyik csomópont a másiknak vagy az átjárónak milyen

[131] Carrier Sense Multiple Access – CSMA.

[132] Medium Access Control for Wireless Sensor Networks (Sensor-MAC) – S-MAC.

útvonalon továbbítsa az általa gyűjtött adatokat. A routingprotokollokat a hálózat topológiája határozza meg, amely szerint az útvonalválasztás lehet hierarchikus vagy elosztott routing, és mindkettőben többféle megoldás is alkalmazható (például LEACH, TEEN, SPIN stb.). (Ács–Buttyán 2007)

A szállítási réteg feladata, hogy megbízható adatátvitelt valósítson meg két eszköz között az alatta lévő hálózati topológiától függetlenül. Szenzorhálózatok esetében akkor van szükség szállítási rétegre, ha a hálózatot külső hálózatról, például az interneten keresztül szeretnénk elérni. Mivel a szenzorok legtöbbször nem rendelkeznek egyedi címzéssel, így a tradicionális hálózatoknál megszokott TCP-alapú megoldások nem alkalmazhatók. Elterjedt megoldás az úgynevezett TCP-splitting, amelynek lényege, hogy az átjáróig a TCP-protokollt alkalmazzák, ezután pedig a hálózatban lévő csomópontok már az UDP-protokoll[133] szerint, datagrammokkal[134] kommunikálnak egymással.

Az alkalmazási réteg biztosítja a megfelelő interfészeket, amelyeken keresztül a felhasználók interakcióba kerülhetnek a hálózattal. A szenzorok limitált erőforrásai miatt azokon operációs rendszerek futtatására nincs mód, emiatt a hagyományos hálózatokban elterjedt adatbázis-kezelő megoldások nem alkalmazhatók. Ezen okok miatt megjelentek a szenzorhálózatokban használatos adatbázis-kezelők, mint például a TinyDB, amely lehetővé teszi, hogy a megszokott SQL-alapú[135] nyelvet használva a lekérdezések a hálózaton belül elosztottan, előfeldolgozást és adatösszegzést lehetővé téve valósuljanak meg. (Akyildiz–Vuran 2010)

A szenzorhálózatokban a rétegek mellett megjelennek különböző síkok is, amelyekben a több réteget is érintő, fontos szolgáltatások

[133] User Datagram Protocol – UDP.
[134] Az adatok kis darabokra (maximum 64 kbyte) bontva továbbítódnak.
[135] Structured Query Language – SQL.

kapnak helyet. A szakirodalom többféle síkkal leírt protokollvermet is definiál, ezek közül a 10. ábra szerinti változat az alábbiakat tartalmazza:

- energiamenedzsment síkja, amely az egyes szenzorcsomópontok hatékony energiafelhasználását menedzseli;
- időszinkronizációs sík, amely az egyes csomópontok időbeli összehangolását végzi;
- szomszédfelderítő sík, amely egy szenzor szomszédjainak felderítését, a szomszédos csomópontok megkeresését, lekérdezését biztosítja;
- feladatmenedzsment síkja, amely az adattömörítés, adattovábbítás, adatfeldolgozás, illetve az elosztott feladat-végrehajtás menedzselését végzi. (Nagy 2012a)

A szenzorhálózatok felépítése és jellemzői alapján megállapítható, hogy habár a bennük rejlő potenciál óriási, sok esetben csak kompromisszumok árán lehet ezeket kihasználni. A problémát az olcsó, kis méretű szenzorok limitált erőforrásai, valamint a vezeték nélküli hálózati kapcsolat korlátai jelentik, ami számos elvárt funkció megvalósítását gátolja.

A technológiai fejlődés azonban megállíthatatlan, a jövőben a szenzorok mérete és előállítási költsége tovább fog csökkenni, kapacitásuk pedig növekvő tendenciát mutat. Az erőforrás-problémák kezelésére pedig az energiahatékony, biztonságos útvonalválasztási megoldásokon és elosztott adatfeldolgozáson alapuló technológiák fejlesztése a cél.

2.2.3.3. Katonai szenzorok és szenzorhálózatok

Katonai szenzorok

A katonai műveletekben – köszönhetően a kifinomult rejtési, álcázási és megtévesztési technikáknak – mára az ellenség élőerejének, harci technikai eszközeinek és rendszereinek felderítésére, várható tevékenységének előrejelzésére az összadatforrású felderítés elve vált megha-

tározóvá. Ez azt jelenti, hogy a harctéren a különböző objektumokról többféle és különböző érzékelési tartományban működő adatszerző eszköz felhasználásával kell az adatokat összegyűjteni, ezáltal biztosítható, hogy az adatfeldolgozás eredményeként előállított felderítési információk megfelelő hitelességgel rendelkezzenek.

Az összadatforrású felderítésre az élőerővel folytatott felderítésen túl a frekvenciaspektrum teljes tartományában alkalmazhatók adatszerző eszközök, amelyek egy részét, mint például a rádiófelderítő eszközöket, radarokat ma még katonák kezelik. A felderítésre használt, egyre többféle adatszerző eszköz azonban ma már kezelő nélkül, autonóm módon működik, aminek nagy előnye, hogy az élőerőt nem veszélyeztetik. Ezek közé tartoznak például a műholdas eszközök, a pilóta nélküli eszközre helyezett felderítőberendezések vagy a harctéren telepített harctéri érzékelők vagy más néven felügyelet nélküli földi szenzorok[136] és a belőlük kialakított hálózatok.

A harctéri szenzorok olyan kis méretű érzékelő és mérőműszerek, amelyek a harctéren letelepítve, kiszórva, a környezeti méret- és állapotváltozásokat, torzulásokat, ingadozásokat stb. képesek érzékelni, mérni és automatikusan jelenteni. A mért adatok kiértékelése alapján fontos azonosító, riasztó, értesítő információkhoz lehet jutni. A harctéri szenzorok alkalmazásával lehetőség nyílik az emberi érzékelőképesség megnövelésére, illetve olyan tartományokban való kiterjesztésére, mint például az infra- vagy az ultraibolya-fénytartomány, amelyekben az ember nem képes észlelni a környezeti változásokat.

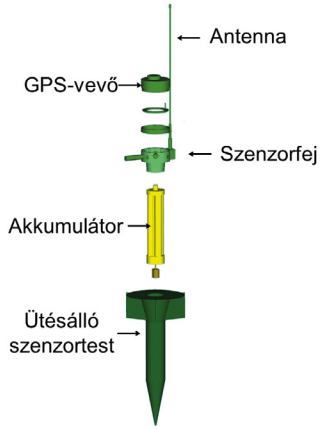
A harctéri szenzorok a frekvenciaspektrum különböző tartományaiban működnek, így fajtái a következők lehetnek:

- akusztikus változásokat érzékelő szenzorok (például hangfelderítő eszközök);
- mechanikai változást érzékelő szenzorok (például mechanikai rezgést, gyorsulást, erőt, légnyomást, helyzetváltoztatást stb. mérő eszközök);

[136] Unattended Ground Sensors – UGS.

- rádiófrekvenciás szenzorok (például térerősséget, feszültséget, áramerősséget, töltést stb. mérő szenzorok);
- hőmérséklet-változást érzékelő szenzorok (például infravörös érzékelők);
- elektrooptikai szenzorok (például fényerősséget mérők, képalkotó infravörös szenzorok stb.);
- mágneses szenzorok (például a mágneses mező intenzitását, sűrűségét, irányát stb. mérők);
- vegyi szenzorok (például gáz halmazállapotú vegyi harcanyagokat, gázkoncentrációt, összetételt, reakciósebességet stb. mérő eszközök);
- radiológiai szenzorok (például radioaktív sugárzási szintet, intenzitást, változást mérő eszközök);
- biológiai szenzorok (például a katonák egészségügyi állapotát mérő szenzorok). (HAIG–VÁRHEGYI 2005)

A felügyelet nélküli földi szenzorokat a föld felszínére vagy a föld alá beásva telepítik. A telepítés történhet kézzel, például kiküldött harcfelderítő járőrök útján, repülőgép vagy helikopter fedélzetéről kiszórva, esetleg tüzérségi lőszerben kilőve. Az érzékelt objektumok helyének, mozgási irányának meghatározásához fontos a telepítés helyének ismerete. Kézi telepítés esetén a szenzor helyadatai ismertek, azokat a telepítést végzők egy digitális térképen akár manuálisan is rögzíthetik. A kiszórással vagy kilövéssel történő telepítés esetén azonban a szenzor általános építőelemei – mint az érzékelő elem, az akkumulátor és a kommunikációs eszköz – mellett a szenzorba beépített helymeghatározó eszköz, például GPS-vevő is szükséges a pozicionáláshoz. Egy légi eszközzel kiszórható szenzor általános felépítését a 11. ábra szemlélteti.



11. ábra

Levegőből kidobható felügyelet nélküli szenzor felépítése

Forrás: a szerző szerkesztése

A szenzorok a kijuttatás, telepítés pillanatától kezdve üzemkész állapotba kerülnek, és nagyon kis energiaigényüknek köszönhetően akkumulátoraikról akár több hétig is képesek működni. A legtöbb fejlett harctéri szenzor a telepítés után készenléti üzemben van, és csak akkor kapcsol be, amikor érzékelési tartományába eső állapotváltozást érzékel. Ezzel a működési móddal jelentősen növelhető az akkumulátor élettartama és ezáltal a szenzor működési időtartama.

Katonai szenzorhálózatok

A szenzorok hálózatos alkalmazásának előnyeit a harctéren is kihasználják. A különféle tartományban működő és érzékelési móddal rendelkező szenzorok a harctéren egy vezeték nélküli szenzorhálózatba integrálhatók. A felügyelet nélküli szenzorhálózat az egyedül álló szenzorokhoz képest nagyobb energiahatékonyságot biztosít, és az elosztott

adatfeldolgozásnak köszönhetően jelentősen növeli a célok felismerésének, detektálásának, helyzetük meghatározásának és a mozgó célok követésének hatékonyságát.

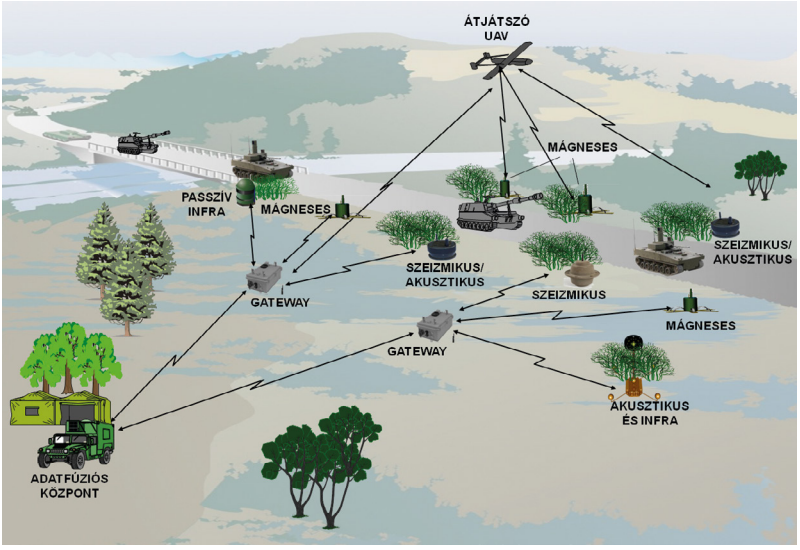
Ennek megfelelően – a polgári megoldásokhoz hasonlóan – a harctéren telepített nagy mennyiségű szenzorból, szenzorcsomópontokból és átjárókból álló, előre definiált vagy ad-hoc szenzorhálózatokat hoznak létre. Ez utóbbi esetben a hálózat elemeit, a szenzorokat, csomópontokat, átjárókat légi eszközből kiszórással vagy tüzérséggel juttatják ki, és helyzetüket a kijuttatást követően GPS segítségével határozzák meg.

A katonai szenzorhálózatok architektúrájának kialakítása alapvetően megegyezik a polgári hálózatoknál leírtakkal. Itt is öt réteget definiálnak a hálózatban, amelyek felelnek a rádiós adatátvitelért, a közeghozzáférés vezérléséért, az útvonalválasztásért, valamint adataggregálást és előfeldolgozást végeznek. Emellett a már ismertetett hálózati síkok végzik a hatékony energiamenedzsmentet, a szomszédos szenzorcsomópontok megkeresését, lekérdezését, feladataik időbeli összehangolását, valamint a csomópontok egyes feladatainak (adattömörítés, adatösszegzés, adatfeldolgozás, adattovábbítás stb.) elosztott végrehajtását menedzselik.

A hálózatban a szenzorok az érzékelt adatokat kódolt formában, meghatározott időközönként juttatják el az adatfeldolgozó központokba. A kommunikációra döntően vezeték nélküli átviteli csatornát alkalmaznak, amellyel szemben alapvető követelmény a kommunikációs csatorna felderítéssel, de különösen zavarással szembeni védelmének biztosítása. A korábban bemutatott civil rádiós technológiák teljes mértékben nem alkalmazhatók a harctéren. Emiatt a harcászati rádiókban elterjedt, kis valószínűséggel felderíthető, kiterjesztett spektrumú digitális megoldások és a korábban ismertetett kis energiaigényű, de nagy hatótávolságú csomagkapcsolt adásmódok kombinációját alkalmazzák a szenzorok és a feldolgozóközpontok közötti kommunikációra. Mivel az energiaellátás korlátozottsága miatt a vezeték nélküli adatkapcsolat csak viszonylag kis hatótávolságot biztosít, ezért a szenzorhálózatban átjátszó adó-vevőket, adatgyűjtő, előfeldolgozó

és adatfúziós gateway-eket alkalmaznak. Egy harctéri szenzorhálózat kiépítését a 12. ábra szemlélteti.

A korszerű harctéri szenzorhálózatokban, a csomópontokban, illetve a gateway-ekben az összegyűjtött adatokon előfeldolgozást végeznek, összegzik a mért paramétereket, különböző spektrális és egyéb jellegzetességeik alapján összehasonlítják és kategorizálják. Az előfeldolgozott adatokat továbbítják az összadatforrású feldolgozóközpontba, ahol részletes mélyelemzésnek, adatfeldolgozásnak vetik alá őket. A szenzorhálózat működési hatékonyságának a kulcsa a szenzorfúzió, amely a különböző tartományú érzékelőktől származó adatok összefűzését jelenti. Az akusztikus, szeizmikus és például az infravörös érzékelőktől származó adatok fúziója azon túl, hogy növeli a célok azonosításának és osztályozásának pontosságát, az irányszögadatok alapján képes a célok pozíciójának meghatározásra is.



12. ábra

Harctéri szenzorhálózat

Forrás: Haig–Várhegyi (2005) alapján a szerző szerkesztése

A felderítő központokban – a térinformatikai adatelemzési módszereket is felhasználva – egy digitális térképen a kijuttatott érzékelők adatai megjeleníthetők, ami lehetőséget biztosít a harcterület, illetve az ott folyó mozgás és tevékenységek észlelésére, illetve megfelelő adatfrissítési gyakorisággal a folyamatos monitorozására, megfigyelésére. (Ványa 2002) Az ellenség helyzetére vonatkozóan így előállított információk a harctéri számítógép-hálózaton megoszthatók, és a műveletben részt vevő saját erők számára megfelelő hozzáférési jogosultság alapján elérhetővé válnak.

A mikroméretű, elektromechanikus rendszerek (MEMS)[137] technológiájának robbanásszerű fejlődése további lendületet adhat többek között a felügyelet nélküli szenzoroknak is. A rendkívül kis méretű szenzorok, az „intelligens porszemek”[138] a föld felszínén szétszórva vagy a levegőbe kiszórva végeznek megfigyelést, ellenőrző méréseket. A magasabb prioritással rendelkező MEMS-csomópont vagy a gateway MEMS meghatározott időközönként egyenként lekérdezi a mérési eredményeket, amelyeket előfeldolgozás után ugyancsak vezeték nélküli adatkapcsolaton keresztül továbbít az adatfúziós központba. (Haig–Várhegyi 2005)

Létező katonai szenzorhálózatok

Napjainkban számos haditechnikai vállalat fejleszt, és több ország hadereje alkalmaz földi telepítésű, felügyelet nélküli szenzorhálózatokat. Az egyik ilyen az izraeli Elbit TREASURES™[139] elnevezésű, intelligens kommunikációs megoldásokkal kialakított szenzorhálózata, amely lehetővé teszi az előerő és a harcjárművek felderítését, azonosítását és követését. (TREASURES™ é. n.) A rendszerben többféle kis

[137] Micro-electromechanical System – MEMS.
[138] Smart Dust.
[139] Tactical Reconnaissance and Surveillance Enhanced System – TREASURES.

méretű, kis energiaigényű és extrém időjárási körülmények között is működőképes szenzor található. Ezek az alábbiak:

- OCEAN – szeizmikus/akusztikus multidetektor, amely a szélzajok elnyomásával és a szeizmikus és akusztikus jelek fúziójával képes a célpontok detektálására, irányának meghatározására, azonosítására és osztályozására;
- SAND[140] – intelligens, rendkívül hosszú élettartamú és bármilyen terepen alkalmazható szeizmikus szenzor, amely a láthatóságon túli területeken is képes az élőerő és a technika detektálására;
- TALOS – kis teljesítményű, a napenergia felhasználásával is működtethető, az antenna karakterisztikájának köszönhetően 360 fokos lefedettséget biztosító felügyelet nélküli, földi telepítésű radar, amely képes több száz méter távolságban lévő célok érzékelésére és követésére;
- MTR[141] – kis teljesítményű, a napenergia felhasználásával is működtethető kis méretű, harcászati földi radar, amely nagyobb érzékelési távolságot és széles szektorú horizontális és vertikális irányú lefedettséget biztosít;
- MID[142] – kis méretű, a látható fény és az infravörös tartományban működő, fejlett képfelismerő és mozgásdetektáló képességgel, valamint videojel-átvitellel rendelkező érzékelő;
- CHAMELEON 2 – széles látószögű és nagy felbontású éjjel-nappali kamera, amely széles sávú videókommunikációt is biztosít.

A különböző érzékelési tartományban működő szenzorokat a hatékony működés érdekében egy ad-hoc, önszerveződő és speciális kommunikációs protokollokkal kialakított, gateway-eket alkalmazó hálózatba szervezve alkalmazzák. A fejlett érzékelési és adatelemzési algoritmusoknak és egyedi kommunikációs protokolloknak köszönhetően,a rend-

[140] Smart All-terrain Networked Detectors – SAND.
[141] Miniature Tactical Radar – MTR.
[142] Miniature Imaging Device – MID.

szer alacsony téves riasztási ráta mellett nagy valószínűségű detektálást és célazonosítást biztosít.

Egy másik példa az amerikai L3 cég REM-Sense® felügyelet nélküli földi szenzorcsaládja, amely előerő és harcjárművek passzív érzékelésére, osztályozására és követésére szolgál. (REM-Sense® é. n.) A rendszer az amerikai hadsereg és a tengerészgyalogság felderítőképességének fejlesztését célzó, 1999 óta tartó program részét képezi, teljes mértékben interoperábilis azzal. Ez a komplex rendszer számos autonóm üzemmódban működő kis méretű, könnyen telepíthető érzékelőt tartalmaz, amelyeket hidak, útcsomópontok, fontos objektumok közelében és utak mentén helyeznek el azzal a céllal, hogy időben érzékeljék az előerő és a technikai eszközök megjelenését, mozgását, a forgalom változását és annak minőségét. Erre a célra szeizmikus, akusztikus, mágneses és infravörös szenzorokat használnak hálózatos üzemmódban.

A REM-Sense® rendszert az alábbi komponensek alkotják:

- AN/PRS 9A BAIS[143] harctéri behatolásjelző rendszer, amely 3 db szeizmikus/akusztikus szenzort és rádióvevőt, valamint egy kézi rádióadót tartalmaz, amellyel képes az előerő és a harcjárművek észlelésére és a fenyegetés szintjének meghatározására;
- REM-Sense ISR szeizmikus/akusztikus, infravörös és mágneses szenzorból, valamint kézi adóból álló harctéri szenzorrendszer, a korábbi jól bevált REMBASS II[144] továbbfejlesztett változata, amely passzív szenzorjaival képes az előerő és a harcjárművek érzékelésére, azonosítására és mozgási irányának megállapítására;
- BAIS-i felügyelet nélküli, korai előrejelző és behatolásdetektáló rendszer, amely 5 db kis súlyú szeizmikus szenzort, rádióvevőt, valamint egy rádióadót tartalmaz. (18. kép)

[143] Battlefield Anti-Intrusion System – BAIS.
[144] Remotely Battlefield Sensor System – REMBASS.

A kommunikáció céljára alkalmazott rádióadók és rádióvevők a 138–153 MHz-es frekvenciatartományban 6 km távolságig képesek kommunikálni egymással. A hatótávolság rádióátjátszók alkalmazásával növelhető, de opcionálisan a REM-Sense® műholdas átjátszóval globális kommunikációs elérhetőséget is biztosít. A rendszer a szofisztikált jelfeldolgozásnak köszönhetően nagyon alacsony hamis riasztási rátával rendelkezik. A családban lévő szenzorrendszerekkel kiépített összefüggő szenzorhálózat jelentősen növeli a helyzetismeretet[145] és az erők megóvásának[146] képességét.

18. kép

REM-Sense® harctéri szenzorrendszer

Forrás: REM-Sense® (é. n.)

A röviden bemutatott két szenzorrendszeren kívül a haderők igényeinek megfelelően még számos hasonló szenzort magában foglaló, hálózatos

[145] Situational Awareness.

[146] Force Protection.

működésre alkalmas szenzorrendszer fejlesztése folyik. Az ismertetett példákból is látható, hogy e szenzorhálózatok a széles spektrumú érzékelési lehetőségeknek és az adatfúziónak köszönhetően jelentős felderítőképesség-növekedést eredményeznek. Mindez pedig párosul még azzal az előnnyel, hogy alkalmazásuk nem jelent veszélyt a saját személyi állományra, illetve a különböző környezeti feltételek, mostoha időjárási viszonyok nem befolyásolják a felügyelet nélküli szenzorok működését.

2.2.3.4. A szenzorhálózatok biztonsági kérdései

A szenzorhálózatok alkalmazásával kapcsolatban jogosan merül fel a biztonság kérdése. E probléma a polgári hálózatok tervezése és kivitelezése kapcsán is az egyik kulcskérdés, a katonai hálózatoknál pedig még fokozottabban előtérbe kerül. A szenzorok korlátozott erőforrásai, a vezeték nélküli kommunikációból fakadó sérülékenységek, valamint a hálózat közvetlen felügyeletének hiánya jelentősen befolyásolja a különböző biztonsági megoldások alkalmazhatóságát. A szenzorhálózatok legnagyobb sérülékenységi kockázata a vezeték nélküli kommunikációból fakad, mivel a rádiófrekvenciás tartományban fizikai kapcsolódás nélkül lehet hozzáférni a hálózat elemeihez a kommunikációs csatornán keresztül. A szenzorhálózatokkal szembeni fenyegetések az alábbiak lehetnek:

- a hálózati adatforgalom felderítése és a hálózati szenzorcsomópontok, átjárók, adatfeldolgozó központok helyének meghatározása;
- a szenzoradatok módosítása, kompromittálása;
- a szenzorhálózat túlterheléses támadása;
- fizikai hozzáférés esetén a megsemmisítés.

A szenzorok a kijuttatást követően – a többnyire passzív működésből fakadóan, illetve a nagyon kis méretüknek köszönhetően – általában

nehezen felderíthetők. Ugyanakkor a hálózati kommunikáció felfedhető és lehallgatható. A gyakorlatban azonban a sokszor kis teljesítményű adások detektálásához a felderítőeszköznek elég közel kell lennie a rádióadóhoz, ami sok esetben nem vagy csak nehezen valósítható meg. Emiatt általában nem a szenzorcsomópontok és a gateway-ek közötti kommunikáció biztonsága a kritikus, hanem a gateway és az adatfeldolgozó központ közötti, nagyobb távolságú és ebből fakadóan nagyobb teljesítményű kisugárzások lehallgatásának lehetősége. E kommunikációs csatornák esetében – amin keresztül már az összegzett és előfeldolgozott adatok kerülnek továbbításra – lehetőség nyílik arra, hogy a támadó felfedje és lehallgassa az adatcsomagokat, majd azokat dekódolja. Ugyanígy a felderítés következtében meg lehet határozni az egyes csomópontok és átjárók helyét, amit fel lehet használni további támadások kivitelezéséhez. A lehallgatással szembeni védelem érdekében tehát kis valószínűséggel felderíthető adásmódokat és különböző kriptográfiai megoldásokat kell alkalmazni.

A szenzorhálózat felderítése és lehallgatása mellett komoly fenyegetést jelent a hálózat működésének korlátozása. Ez megvalósulhat a hálózat elemeihez való fizikai hozzáféréssel, azok tönkretételével, megsemmisítésével, a szenzoradatok módosításával vagy a hálózati kommunikáció zavarásával. A fizikai hozzáféréssel adatokat lehet kiolvasni az egyes csomópontokból vagy átjárókból, fizikailag meg lehet azokat semmisíteni. Az illetéktelen hozzáféréssel szemben rendszermemória-törléssel vagy felszedés elleni védelemmel, önmegsemmisítéssel lehet védekezni.

A szenzorhálózat ellen alkalmazható a megtévesztés technikája is. Ezt a fenyegetési módot *spoofingnak* nevezik, amely technika azt jelenti, hogy egy idegen szenzorcsomópont a hálózat elemének adja ki magát, és hamis adatokat juttat az adatösszegző és előfeldolgozó gateway-hez, vagy egy idegen gateway hamis adatokat küld az adatfúziós feldolgozóközpontba, amivel kompromittálja a feldolgozandó adatokat. Ennek kiküszöbölésére kriptográfiai eljárások, illetve a hálózat kon-

figurálása során magas szintű hitelesítési technikák alkalmazása célszerű. (WINKLER et al. 2008)

Végül komoly problémát jelent a hálózat túlterheléses támadása, ami megakadályozza, hogy a csomópontok és az átjárók, illetve az adatfeldolgozó központ kommunikálni tudjon egymással. Ez megvalósítható logikai úton, ami a számítógép-hálózatok ellen alkalmazott és elterjedt túlterheléses támadásokhoz[147] hasonlóan a csomópontok és a gateway-ek folyamatos és tömeges lekérdezését jelenti, ez pedig a rendszer lelassulásához és leálláshoz vezet. A túlterheléses támadás történhet a fizikai rétegben, a kommunikációs csatorna célzott vagy széles sávú, elnyomó zavarásával is, mivel különösen a polgári hálózati csomópontok nem rendelkeznek robusztus zavarás elleni védelemmel. A katonai rendszerek esetében emiatt szükséges a nagy zavarvédettségű kommunikációs megoldások alkalmazása.

Összességében megállapíthatjuk, hogy a szenzorhálózatok mind a polgári, mind pedig a katonai alkalmazást tekintve napjaink egyik leginnovatívabb technológiai fejlesztései. A felhőalapú számítástechnikai alkalmazásokkal ötvözve és az IoT-technológiába való integrálásával a szenzorhálózatok alkalmazásában rejlő potenciál óriási, amit ma még sok esetben csak kompromisszumok árán lehet kihasználni. A kutatások az alacsony hamis riasztást produkáló, de nagy detektálási valószínűségű szenzorok kifejlesztésére, az adatfúziós technológia tökéletesítésére, valamint a kis energiafelhasználású szenzorok fejlesztésére fókuszálnak. E téren például a katonai rendszereknél is látott napelemes megoldások alkalmazásában vélhetően nagy potenciál rejlik.

[147] Distributed Denial of Service – DdoS.

2.2.4. Katonai műveleti hálózatkoncepciók

2.2.4.1. Hálózatközpontú hadviselés

Az előző alfejezetekben ismertetett felhőalapú számítástechnika, az IoT és a szenzorhálózatok mind a hálózatos technológiára épülnek. Mindez jól mutatja, hogy a 21. század új típusú társadalmi berendezkedése már ma is, de az elkövetkezendő években még inkább a teljes hálózatos működésre épül. Manuel Castells már közel húsz évvel ezelőtt kifejtette, hogy az információs társadalom csak akkor fogja kihasználni az információs lehetőségeket, ha kialakul a hálózatos társadalom. Castells hálózatos társadalom definíciója szerint: „A hálózatos társadalom olyan társadalom, ahol a kulcsfontosságú társadalmi rendszerek és tevékenységek elektronikus információs hálózatok köré szerveződnek.”[148] (Kreisler 2001) Meglátása szerint az információ mellett a hálózatosítás, a hálózatok rugalmassága és konvergenciája válik a társadalom működésének és fejlődésének központi elemévé.

Ma már ennek jól kivehető jegyeit tapasztaljuk, hiszen mindennapjainkat teljes mértékben átszövi a hálózatos tevékenység (munkavégzés, szórakozás, ügyintézés stb.). Azáltal, hogy a bennünket körülvevő eszközöket, tárgyakat is hálózatba kötjük, és a felhőalapú rendszerek egyre meghatározóbbak lesznek, ez még inkább erősíti a hálózatos társadalom fejlődését.

Mindez természetszerűleg meghatározza a katonai műveleteket támogató infokommunikációs rendszerek fejlődésének irányát is. Mindhárom területen (felhő, IoT, szenzorhálózatok) érintettük azok katonai aspektusait, és rámutattunk arra, hogy napjaink e három meghatározó infokommunikációs innovációja egymással szoros összekapcsoltságban elégíti ki az egyének és a társadalom összességének egyre növekedő információs igényeit. A katonai infokommunikációs rendszerek kialakulását és fejlődését vizsgálva az előző fejezetben is azt láttuk, hogy

[148] Fordította a szerző.

rádióhálózatok, felderítő rendszerek (például az egyesült királyságbeli radarlánc), majd később a számítógépek kialakulása és összekapcsolása révén alapvetően a hálózatos működés válik meghatározóvá. Napjainkra, köszönhetően a civil infokommunikációs technológia fejlődésének és a katonai rendszerekre gyakorolt hatásának, mind a békeidejű, mind pedig a műveleti területen telepített és működtetett hálózatok fejlődése követi a már bevált, illetve a fejlesztés alatt álló, de nagy reményekkel kecsegtető polgári infokommunikációs megoldásokat.

A mai értelemben vett katonai hálózatos gondolkodás és technológiaelméleti alapjait már a 90-es évek végén lefektették neves katonai és hálózatelméleti teoretikusok. Cebrovski, Garstka, Stein és Alberts hálózatközpontú hadviselési (NCW) elmélete, illetve az ez alapján kidolgozott NATO hálózatos koncepciója úttörő szerepet játszott a mai felhőtechnológiát kihasználó, szenzorhálózatokra alapozott és az IoT-megoldásokat is ötvöző katonai műveleti hálózatok kialakításában. (Cebrowski–Garstka 1998; Alberts–Garstka–Stein 1999)

A hálózatközpontú hadviselési koncepció alapvető lényege, hogy a parancsnok és törzse, valamint a végrehajtó erők mindazon valós idejű, pontos és releváns információkhoz hozzáférhessenek, amelyek szükségesek a katonai műveletek vezetéséhez és irányításához, valamint a feladat végrehajtásához. Ez azt jelenti, hogy a felderítés, a döntési folyamat és a végrehajtás infokommunikációs rendszereit egyazon hálózatba kell integrálni, ami által jelentősen növelhető az erők műveleti képessége. Ez a vezetési és irányítási elv a különböző adatszerző eszközök és szenzorok, az adatfeldolgozó és döntés-előkészítő rendszerek, valamint a végrehajtó erők és eszközök egységes hálózatba kapcsolásával valósítható meg.

Ez az elv alapvetően három, egymással szorosan összefüggő és hálózatba szervezhető funkció megvalósítását jelenti, úgymint:

- az ellenségre és a harctéri környezetre vonatkozó adatok valós idejű megszerzését, továbbítását, fúziós adatfeldolgozását, megjelenítését és hatékony felhasználását;

- valós idejű és biztonságos kommunikációt a felderítő adatszerző eszközök, döntéshozók és végrehajtók között;
- decentralizált vezetési struktúra kialakítását, amely minden döntéshozó számára biztosítja a felelősségi és érdekeltségi körébe tartozó fontos adatokhoz való hozzáférést. (Haig–Várhegyi 2005)

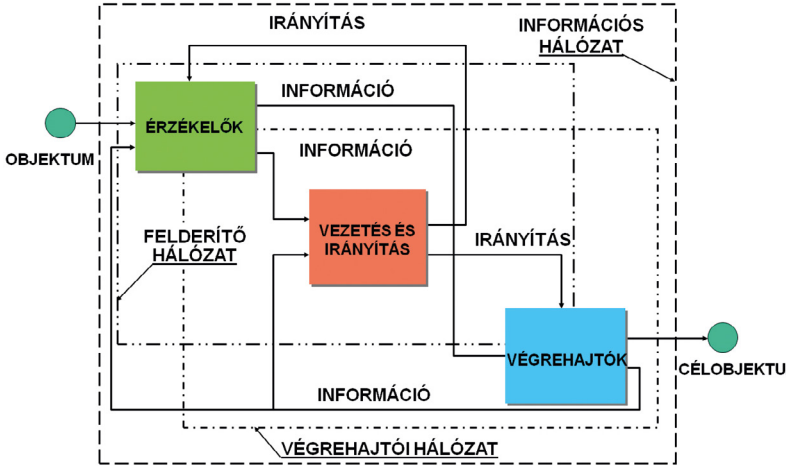
Cebrowski és Garstka szerint a jelzett funkciók tulajdonképpen három egymásba kapcsolódó hálózattal valósítható meg. Ezek a hálózatok az alábbiak:

- a felderítőhálózat,[149] amely a különböző egymással összekapcsolt adatszerző eszközöket, szenzorokat, adatgyűjtő és előfeldolgozó elemeket foglalja magában;
- a végrehajtói hálózat,[150] amely az ellenség erői és eszközei elleni tevékenységet végrehajtó, egymással összekapcsolt erőket, eszközöket, fegyvereket és fegyverrendszereket jelenti;
- az információs vagy más néven vezetési és irányítási hálózat,[151] amely a különböző, egymással összekapcsolt döntés-előkészítő és döntéstámogató elemeket, számítógépeket tartalmazza. (Cebrowski–Garstka 1998)

A hálózatközpontú hadviselés elve szerint a felderítőhálózat és a végrehajtói hálózat az információs hálózaton keresztül kapcsolódik egymáshoz, így alakítva ki egy hálózatok hálózata logikai struktúrát (13. ábra). E struktúrában a hálózatba kapcsolt, különböző érzékelési tartományban működő szenzorokkal megszerzett adatokból adatfúziós technikával lehet előállítani a felderítési információkat, amelyek alapján megalapozottabb, pontosabb döntéseket lehet hozni. A végrehajtó erők és fegyverrendszerek pedig ezen felderítési információkra alapozott megosztott helyzetismeret szerint képesek az ellenséges célpontok ellen tevékenykedni.

---

149 Sensor Grid.
150 Engagement Grid.
151 Information Grid.



13. ábra

A hálózatközpontú hadviselés logikai modellje

Forrás: CEBROWSKI–GARSTKA (1998) alapján a szerző szerkesztése

A felderítőhálózat légi, földi, víz alatti és vízfelszíni, valamint űrben telepített adatszerző eszközökből, szenzorokból, illetve adatgyűjtő és előfeldolgozó elemekből áll, amelyek lehetővé teszik az ellenségről, valamint a harctéri környezetről és annak változásairól szóló valós idejű adatok megszerzését, szűrését, összegzését és előfeldolgozását.

A végrehajtói hálózat az összes elérhető és alkalmazható saját erőt és fegyverrendszert magában foglalja. A végrehajtói hálózat biztosítja, hogy a harcoló erők és fegyverek a megfelelő időben és helyen a megkívánt harctéri hatásokat elérjék. A hálózatközpontú képesség elvének megfelelően a végrehajtói hálózat a felderítési információhoz való kiterjedtebb hozzáférés és a megosztott helyzetismeret alapján valós idejű célmegjelölést biztosít, ami lehetővé teszi az ellenséges célobjektum ellen legoptimálisabban alkalmazható saját erő, fegyver és harceszköz kiválasztását.

Az információs hálózat adja a rendszer átfogó infokommunikációs keretét, számítógép-hálózati infrastruktúráját. A hálózat adattároló és adatfeldolgozó központokból, számítógép-munkaállomásokból, routerekből, a hálózati kommunikációt megvalósító vezetékes és vezeték nélküli távközlési eszközökből, valamint operációs rendszerekből és információmenedzsment-alkalmazásokból áll. Az információs hálózat a fenti eszközökkel és informatikai alkalmazásokkal egységes keretbe foglalja a felderítőhálózatot és a végrehajtói hálózatot, biztosítja a harctéri hálózatalapú fúziós adatfeldolgozást, helyzetértékelést, döntéshozatalt, valamint a rendszer elemei és hálózatai közti kommunikációt. (HAIG et al. 2013)

A hálózatközpontú hadviselési elv egyik rendkívüli előnye abban rejlik, hogy az információáramlás a felderítő rendszertől kezdve a döntéshozón át a végrehajtóig egységes hálózatba szervezetten valósul meg. Ennek egyik pozitívuma, hogy egyrészt a szenzorok által gyűjtött adatok feldolgozása, a helyzet értékelése és a döntés meghozatala, illetve a végrehajtókhoz való eljuttatása jelentősen felgyorsul. A másik fontos előnye, hogy a végrehajtó a művelet végrehajtása érdekében – megfelelő jogosultság alapján – olyan információkhoz is hozzájuthat, amelyek sok más adatforrásból származnak, és amelyek pontosabb helyzetmegítélést, döntést tesznek lehetővé.

2.2.4.2. NATO-hálózatalapú képesség

Az amerikai elképzelések mentén néhány évvel később a NATO is felismerte a hálózatalapú gondolkodás fontosságát. Az információs kor meghatározó szerepének felismerésével a 2002-es prágai NATO csúcstalálkozón fogadták el a NATO új vezetési- és irányításiképesség-fejlesztési programját, amelyet NATO-hálózatalapú képességnek (NNEC)[152] neveztek el. Ez a koncepció több mint tíz éven át a NATO

[152] NATO Network Enabled Capabilities – NNEC.

vezetési és irányítási rendszerének, illetve információs infrastruktúrája fejlesztésének a központi eleme volt.

A NATO 2005-ben megjelent megvalósíthatósági tanulmánya a hálózatalapú képesség egymásra épülő alapelveit az alábbiakban összegzi (NNEC 2005):

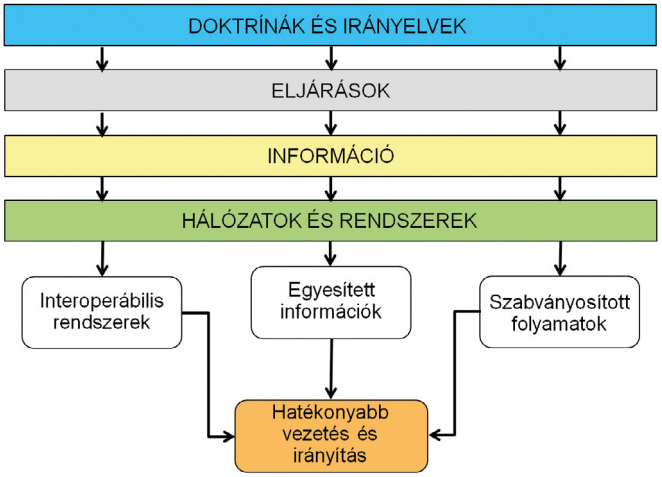
- a hálózati képesség növeli az információmegosztás lehetőségét;
- az információmegosztás képessége javítja az információ minőségét és a megosztott helyzetismeretet;
- a megosztott helyzetismeret biztosítja az együttműködést és a tevékenységek összehangoltságát;
- mindezek pedig számottevően növelik a feladat-végrehajtás hatékonyságát.

A NATO hivatalos megfogalmazása szerint „az NNEC a Szövetség kognitív és technikai képessége, amely a hadászati szinttől a harcászati szintig értelmezett műveleti környezet különböző összetevőit egyesíti egy hálózatos információs infrastruktúrán (NII)[153] keresztül”.[154] (NNEC 2014) Ez azt jelenti, hogy a koalíciós műveletek során a hálózatalapú képesség az információk és szolgáltatások megosztása érdekében egységes struktúrába egyesíti a hálózatokat és a rendszereket, az információkat, az alkalmazott eljárásokat, valamint az irányelveket és a doktrínákat (14. ábra).

A lenti alapelveknek eleget tevő hálózatalapú képesség – hasonlóan a hálózatközpontú hadviselési koncepcióhoz – egy egységes struktúrában összekapcsolva magában foglalja:

- a felderítő adatszerző eszközöket és rendszereket;
- a döntéshozatali rendszereket és döntéshozókat;
- a végrehajtó erőket és fegyverrendszereket, valamint
- a többnemzeti katonai, kormányzati és nem kormányzati intézményeket.

[153] Networking and Information Infrastructure – NII.
[154] Fordította a szerző.



14. ábra

A NATO hálózatalapú képességstruktúrája

Forrás: NNEC (2014) alapján a szerző szerkesztése

A NATO-koncepció, bár jelentős technikai és infrastrukturális képességfejlesztést irányozott elő, deklaráltan egy olyan vezetési és irányítási kultúraváltást vázolt fel, amelynek a középpontjában az ember állt. A NNEC tehát elsődlegesen a műveletekben részt vevő parancsnokok és végrehajtói állomány gondolkodásmódjának megváltoztatását, másodsorban az információs folyamatok átalakítását, végül pedig az infokommunikációs technológia fejlesztését célozta meg.

Az NNEC technikai támogató összetevője a hálózati és információs infrastruktúra (NII), amely lehetővé teszi az együttműködést és az információk megosztását a felhasználók között, a különböző adatelemzési, adathozzáférési és kommunikációs technikákkal jelentősen lerövidíti a döntési ciklus idejét. Ez az infrastruktúra egyben biztosítja a már meglévő hálózatok gyors és folyamatos összekapcsolását, aminek

következtében az információ felhasználásának hatékonysága növekszik. Mindez pedig a NNEC elgondolása szerint hozzájárul az információs fölény kialakításához, ami a korszerű katonai műveletek megvívásának egyik fontos záloga. (NNEC 2014)

Az eddigi különféle hálózatalapú képességfejlesztési törekvések alapvetően mind arra irányultak, hogy az információgyűjtő, döntéshozatali és végrehajtó eszközök, rendszerek összekapcsolásával kialakított hálózattal a haderő képességei jelentősen növelhetők legyenek. Ez a gondolkodásmód és technológia egyértelműen azonosítható a korábbi alfejezetekben a szenzorhálózatoknál, a felhőalapú számítástechnikánál, illetve az IoT-rendszereknél tárgyaltakkal. Többek között emiatt is e technológiák katonai alkalmazása a közeljövőben törvényszerűvé válik. A bemutatottak alapján már most is megfigyelhető, hogy a szenzorhálózatok integráns részét képezik a hálózatalapú koncepciónak. A szenzorokon túlmenően a katonai műveleti erők által alkalmazott eszközök széles skálájának hálózatba kapcsolásával megvalósíthatók a katonai IoT-megoldások.

Az új elgondolások alapján a hálózatalapú koncepció átfogó infokommunikációs keretét adó információs hálózat kialakításában megjelenik a polgári hálózatos technológiai fejlesztés, amely egyértelműen a felhőalapú technológiák felhasználásának irányába mutat. Ezáltal lehetővé válik, hogy a felhasználók a hálózatban kezelt adatokhoz a megfelelő hozzáférési jogosultság alapján, valós időben hozzáférjenek anélkül, hogy az információ tárolásával, a tárolás helyével foglalkozniuk kellene.

Az NNEC mint hálózatos képességfejlesztési program mára elérte életciklusa végét. A több mint tíz év alatt szerzett tapasztalatok egyértelműen igazolták, hogy a haderőfejlesztés egyik alapvető iránya az információs tevékenységek hálózatba szervezése. Az NNEC koncepció során elért eredmények és tapasztalatok felhasználásával a NATO 2015-től egy új program kidolgozását kezdte meg NATO Szövetséges Műveleti Hálózat (FMN) néven, ami a polgári infokommunikációs technológiai fejlesztések terén elért – szenzorhálózatokkal,

felhőalapú technológiával és az IoT-rendszerekkel összefüggő – megoldásokat még intenzívebben használja fel.

2.2.4.3. NATO szövetséges műveleti hálózatépítés

A NATO afganisztáni missziója során számos esetben problémát jelentett, hogy a feladat végrehajtásában részt vevő erők többféle hálózati infrastruktúrát[155] használtak a vezetés és irányítás során. E hálózatok között lényegében érdemi információmegosztás és szolgáltatás nem működött. A hatékonyabb együttműködés érdekében célszerűnek látszott tehát a műveletekben részt vevő erők (nemzetek) között egy műveleti hálózat kialakítása. Ennek magvalósítására 2010-ben hozták létre az Afganisztáni Műveleti Hálózatot (AMN),[156] amely az ISAF-erők[157] műveleti területen telepített alapvető hálózati infrastruktúrája volt. E hálózat az egyes nemzetek hálózatainak összekapcsolásához biztosított egy keretrendszert, amelyen már megvalósultak az alapvető hálózati szolgáltatások, mint például az elektronikus levelezés, VoIP-kommunikáció,[158] védett videokonferencia, megosztott helyzetismeret stb. (Boland 2013)

E hálózat kiépítésének és működésének tapasztalatai alapján a NATO Katonai Bizottsága 2012 végén elfogadott egy jövőbeni műveleti hálózat kialakítására vonatkozó elgondolást. Az afganisztáni missziót követően megkezdett fejlesztés eredményeképpen kidolgoztak egy, az egyes NATO-tagállamok képességeit is figyelembe vevő általános hálózati modellt, ami alapján 2014-re kidolgozták a Szövetséges Műveleti Hálózat (FMN) megvalósítási tervét.

---

155 Például NATO ISAF-Secret, SIPRNet, CENTRIX-GCTF (Combined Enterprise Regional Information Exchange System-Global Counterterrorism Force), további kisebb nemzeti hálózatok.

156 Afghanistan Mission Network – AMN.

157 International Security Assistant Force – ISAF.

158 Voice over Internet Protocol – VoIP.

E terv szerint az FMN a felhasználókat, az információs folyamatokat és az infokommunikációs technológiát magában foglaló szabályozott hálózatos keretrendszer, amely hatékonyan képes támogatni a szövetséges műveleteket. Az FMN a már meglévő hálózati képességek és információmenedzsment-szabványok felhasználásával nagyfokú rugalmasságot és skálázhatóságot, illetve gyors információmegosztást tesz lehetővé, ami növeli a műveletek vezetésében és irányításában való felhasználhatóságát.

Az FMN kialakítása három szintet foglal magában:

- az FMN hálózatirányítást, amely a NATO Katonai Bizottsága szintjén meghatározza a hálózat működésének céljait és a különféle működési szabályokkal, irányelvekkel, folyamatokkal és szabványokkal leírható működési környezetet;
- az FMN hálózati keretet, amely felülről szabályozott módon, a műveleti hálózatok kialakításához, fejlesztéséhez, telepítéséhez és üzemeltetéséhez biztosítja az állandó és folyamatos működési alapot, valamint
- a műveleti hálózatokat, amelyek különböző szövetséges műveletek, gyakorlatok, kiképzési feladatok céljából létrehozott és felülről irányított hálózatos képességeket jelentenek.

E három szint közül a műveleti hálózatok adják az FMN végrehajtói szintjét. A műveleti hálózatokat rugalmas és testre szabott állandó helyű, illetve telepített hálózatok és támogató infrastruktúrák, valamint különféle hálózatos információs folyamatok, eljárások és szabványok alkotják. A műveleti hálózatok az alábbi négyféle képességi szinttel építhetők ki:

- műveleti hálózati elem,[159] amely a saját információs igények és a műveletek alapvető információs igényeinek kielégítésére hálózati és egyéb információs infrastruktúrát biztosít, hálózati információs szolgáltatásokat nyújt;

[159] Mission Network Element – MNE.

- műveletihálózat-kiterjesztés,[160] amely a saját információs igények kielégítésére hálózati és egyéb információs infrastruktúrát biztosít, hálózati információs szolgáltatásokat nyújt, azonban a műveletek alapvető információs igényeit nem képes kielégíteni;
- teljes jogú felhasználó,[161] olyan műveleti hálózatfelhasználó, aki a saját információs igényei kielégítésére nem rendelkezik hálózati és egyéb információs infrastruktúrával, hálózati információs szolgáltatásokat sem nyújt, így más műveleti résztvevő infrastruktúráját és szolgáltatásait használja;
- más felhasználók,[162] akik nem képezik szerves részét a hálózatnak, és nem tartoznak a szövetségi hálózati keret által meghatározott követelmények alá. (FMN é. n.)

A műveleti hálózatok a korábban ismertetett hálózatközpontú hadviselés és NATO-hálózatalapú képességre vonatkozó koncepciók által definiált hálózati elemekből és alhálózatokból épülnek fel. Különösen igaz ez a katonai műveletek során, a műveleti területen telepített hálózat esetében, ahol a felderítő (szenzor)hálózat és a végrehajtó (fegyverrendszer-)hálózat egy információs kerethálózaton keresztül van összekapcsolva. A hálózat kiépítése és működése során igen nagymértékben támaszkodik a felhőalapú technológia által nyújtott szoftver- (SaaS), platform- (PaaS) és infrastruktúra-szolgáltatásokra (IaaS).

Tekintettel a katonai műveletek során keletkező hatalmas mennyiségű adatállományra, azok feldolgozási igényeire, illetve az információmegosztás követelményeire, a felhőalapú megoldások alkalmazása a jövőbeli katonai hálózatokban is elkerülhetetlen. Jól szemlélteti ezt a hálózatépítési irányt Denis Mercier tábornoknak, a szövetséges erők átalakításáért felelős főparancsnokának nyilatkozata, miszerint: „A jövő harci rendszere nem egy harci repülőgép, hanem egy felhőalapú

[160] Mission Network eXtension – MNX.
[161] Hosted Users.
[162] Other Entities.

azonosítással és ember vezette vagy pilóta nélküli platformokkal rendelkező C4ISR rendszer, amelyhez képesnek kell lennünk kapcsolódni. E jövőbeli rendszer kiépítését pedig ma kell elkezdeni." (Janezic 2016) A felhőalapú technológiát kihasználó műveleti hálózat lehetővé teszi a szenzorrendszerekhez, navigációs rendszerekhez, fegyverrendszerekhez, valamint vezetési és irányítási rendszerekhez való kényelmes, igény szerinti hozzáférést, ami pedig napjaink hadereje számára jelentős erősokszorozó képességet jelent.

Az FMN felhőalapú technológiája, amelyet harci felhőnek[163] is neveznek, a katonai jellegéből adódóan és a magas szintű biztonsági követelmények miatt privát, azaz zárt felhő, ami a kezelt adatok minősítése szempontjából titkosított, korlátozott hozzáférésű, valamint publikus, mindenki számára hozzáférhető elemekből épül fel. A felhőalapú szolgáltatások kihasználása szempontjából a műveleti hálózat alkalmas a titkos adatok kezelésére. Emellett a felhő része egy úgynevezett védett üzleti hálózat,[164] amely a korlátozott hozzáférésű adatok kezelését végzi. Ez utóbbi tartalmazza az internet-hozzáférést is, amely a nyilvános internetelérésen[165] keresztül a nem minősített adatokhoz való hozzáférést teszi lehetővé.

A NATO felhő-infrastruktúrájának kialakítása során három nagy kapacitású adatközpontot[166] terveznek létrehozni Monsban, Brüsszelben, illetve Lago Patriában. A centralizált műveleti központ[167] Monsban található, ennek tartalék központja pedig valahol a Benelux államokban. A három adatközpontot a már meglévő NATO-központok[168] bázisán, azok modernizálásával alakítják ki. Ezek látják el az összes NATO-felhőszolgáltatást, és végzik a biztonsági mentéseket. Minden biztonsági

[163] Combat Cloud.
[164] Protected Business Network – PBN.
[165] Public Internet Access – PIA.
[166] Enterprise Data Centre – EDC.
[167] Operation Centre – OpsCen.
[168] SHAPE – Mons, NATO HQ – Brüsszel, JFC – Nápoly.

mentést mindhárom adatközpontra letükrözik, ami biztosítja a folyamatos rendelkezésre állást.

Az adatközpontok mellett különféle helyeken alap-[169] és kiemelt adatcsomópontokat[170] telepítenek. Az alap-adatcsomópontok csak minimális tároló, illetve számítási kapacitással rendelkeznek majd, mivel alapvető funkciójuk a felhőhöz való szinkronizálás. A kiemelt adatcsomópontok viszont a rugalmasság miatt nagyobb kapacitást biztosítanak a helyi felhasználók számára, illetve mindazon alkalmazásoknak, amelyek még nem állnak készen az új architektúra igénybevételére.

A tervek szerint a projekt végére a jelenlegi szolgáltatások 80%-a az adatközpontok köré szerveződik, és felhőalapú szolgáltatásként lesz elérhető, a szolgáltatások fennmaradó 20%-a azonban várhatóan az életciklusa végéhez közeledik, mert jelenlegi formájában nem alkalmas a felhőalapú működésre. Ezek továbbra is hagyományos módon működnek majd tovább, de a cél, amilyen gyorsan csak lehet, a 100%-os felhőalapú szolgáltatás kialakítása. (Lenk 2014)

Amint a fent leírtakból is látható, az FMN egy még kezdeti stádiumban lévő hálózatépítési projekt, amely állandó helyű és telepített műveleti hálózatokból épül fel. A hálózatépítés során a jövőbeli igények kielégítésére messzemenően kihasználják a felhőalapú megoldásokat és az azok által nyújtott előnyöket. A műveleti területen telepített hálózati infrastruktúra felépítése láthatóan követi az FMN előtti hálózatalapú képesség koncepciójában lefektetett elveket, illetve felhasználják az afganisztáni misszióban szerzett hálózatkialakítási tapasztalatokat. Eszerint a hálózat részét képezik a szenzorhálózatok és a végrehajtói hálózatok, amelyek egy információs hálózaton keresztül kapcsolódnak össze. A felhőalapú technológia felhasználásával az adatok különböző adatbányászati és gépi tanulási módszerekkel elemezhetők, fuzionálhatók és megoszthatók. A koncepció kidolgozói szerint az így kialakított hálózati struktúra várhatóan kielégíti mindazon információs

[169] Standard Node – SN.
[170] Enhanced Node – EN.

követelményeket, amelyeket napjaink katonai műveletei megkövetelnek egy támogató infokommunikációs rendszertől, és kulcsfontosságú szerepet fog betölteni a NATO Összekapcsolt Haderők Kezdeményezésben.[171]

Ugyanakkor a hálózat kiépítésének, különösen a felhőtechnológia alkalmazásának komoly korlátja a biztonsági követelmények teljesítése. Az IoT-megoldásokban a vezeték nélküli kommunikációból fakadóan a külső, illetéktelen hozzáférés könnyebben megvalósítható. Ennek köszönhetően mind az adatok, mind az információs útvonalak fizikai és számítógépes támadásoknak, illetve elektronikai zavarásnak lehetnek kitéve.

Láthatóan a polgári felhőalapú technológia és az IoT is komoly biztonsági szempontokat vet fel, de a katonai alkalmazás során még inkább olyan magas szintű titkosítás és kifinomult információbiztonsági megoldások szükségesek, amelyek megfelelnek a bizalmasság, sértetlenség és a rendelkezésre állás katonai kritériumainak. Mindezekre tekintettel a következő fejezetekben megvizsgáljuk, hogy az információs műveleteken belül milyen fenyegetésekkel kell számolnunk, és azok összehangolt alkalmazása milyen hatásokat eredményezhet a kibertérben működő hálózatos rendszerekben.

[171] NATO Connected Forces Initiative – NATO CFI.

3. Információs műveletek

3.1. A műveletek információs környezete

Napjaink információs környezetének jellemzői, mint például az internet megjelenése, az infokommunikációs technológia bővülése, a vezeték nélküli kommunikáció egyre szélesebb körű elterjedése és felhasználása, valamint a közösségi média hatása új és összetett kihívásokat jelentenek a társadalmi folyamatokban és a katonai műveletek során. A korszerű hálózatos környezet lehetővé teszi mind az állami, mind a nem állami szereplők számára, hogy célkitűzéseik hatékony elérése érdekében az információs környezetben tevékenykedjenek, illetve kihasználják az e környezet nyújtotta lehetőségeket.

A katonai műveletek tervezése és végrehajtása során a rendelkezésre álló információ, illetve az információ hiánya mindig is rendkívül fontos szerepet játszott. Emiatt a hadviselés történetében a haderők többnyire olyan katonai műveletek végrehajtására törekedtek, illetve azokat részesítették előnyben, amelyek képesek voltak jelentősen befolyásolni a szemben álló fél információszerzését, a helyzetmegítélését és ezáltal a viselkedését. Ez pedig alapvetően az információs környezetben, a kor színvonalán álló információs képességekkel, illetve a másik fél hasonló képességeire való ráhatással volt elérhető.

Az USA összhaderőnemi információs műveletek doktrínája szerint: „Az információs környezet mindazon egyének, szervezetek és rendszerek összessége, akik és amelyek az információ gyűjtésével, feldolgozásával, szétosztásával foglalkoznak.”[172] (JP 3-13 2014, I-1) A definíció szerint az információs környezet magában foglalja annak valamennyi szereplőjét és erőforrásait, illetve tevékenységeit és folyamatait. Ezzel tartal-

[172] Fordította a szerző.

mában szinte megegyezik a NATO összhaderőnemi információs műveletek doktrínájának meghatározása, miszerint az „információs környezet egy olyan környezet, amely magában foglalja magát az információt, az egyéneket, szervezeteket és rendszereket, amelyek gyűjtik, feldolgozzák és továbbítják az információt, valamint a kognitív, a virtuális és a fizikai teret, amelyekben mindez megvalósul”.[173] (AJP-3.10 2015, LEX-7)

A hálózatos infokommunikációs technológia, benne az internet, a felhőalapú technológia és a vezeték nélküli kommunikációs lehetőségek nagy ütemű fejlődése következtében az információ gyűjtése, feldolgozása és továbbítása helytől függetlenül, bárhol, bármikor megvalósulhat. Emiatt az információs környezet értelmezhető világméretű viszonylatban, illetve bizonyos területi, ágazati szempontból is. Előbbi esetben globális információs környezetről, utóbbi esetben pedig például katonai információs környezetről beszélhetünk.

Az információs társadalom mint globális társadalmi formáció kialakulásával és fejlődésével megjelenik a globális információs környezet. Munk Sándor meghatározása szerint: „A globális információs környezet (információs színtér) információs tevékenységeket végrehajtó szereplők, a tevékenységek végrehajtása során felhasznált eszközök és más erőforrások, valamint a kezelt információk világméretű összessége.” (Munk 2002, 140.) A globális információs környezetnek minden világméretű, regionális és nemzeti szervezet, intézmény és rendszer részét képezi. Technikai infrastruktúráját a globális információgyűjtést, -tárolást, -feldolgozást és -továbbítást végző adatgyűjtő rendszerek, vezetékes és vezeték nélküli kommunikációs hálózatok, számítógép-hálózatok alkotják.

Az információs környezetet értelmezhetjük ágazati megközelítésben is. Eszerint többféle ágazati információs környezetet lehet azonosítani, mint például a közigazgatás, a közlekedés, a rendvédelem vagy a honvédelmi ágazat katonai információs környezete. Könyvünk szempontjából ez utóbbi értelmezése fontos, amelyhez szintén Munk Sándor meghatározását használjuk fel: „A katonai információs kör-

[173] Fordította a szerző.

nyezet alatt a globális információs környezet azon szereplőinek, eszközeinek és erőforrásainak, valamint információinak összességét értjük, amelyek lényeges hatással vannak egy adott katonai művelet végrehajtására."[174] (Munk 2002, 140.) A katonai információs környezet a globális információs környezet részét képezi.

Az információs környezettel a katonai műveletek működési tartományai tovább bővültek. A hadszíntér szárazföldi, tengeri, légi és kozmikus tartományai mint fizikai dimenziók mellett megjelenik az információs hadszíntér is, amely napjainkban egyre fontosabb szerepet kap a katonai műveletekben. E földrajzilag nem megfogható információs hadszíntéren a korszerű információs technológiát is felhasználva technikai és kognitív információs folyamatok zajlanak, illetve az információ megszerzéséért és a szemben álló félnél hatékonyabb felhasználásáért információs küzdelem folyik. Az információs hadszíntér három egymással összefüggő dimenzióból áll, amelyek folyamatosan kölcsönhatásban vannak az egyénekkel, a szervezetekkel és a rendszerekkel. Ezek a dimenziók az alábbiak:

- fizikai dimenzió,
- információs dimenzió és
- kognitív dimenzió. (JP 3-13 2014, I-2)

A fizikai dimenzióban azon valós, fizikailag megfogható infrastruktúrák és eszközök találhatók, amelyek lehetővé teszik az egyének és a szervezetek számára az információkezelési folyamatok végzését. Emellett a különböző információs infrastruktúrák, infokommunikációs rendszerek elemei elleni fizikai támadások, illetve azok védelme is e dimenzióban valósul meg. Ennek megfelelően a fizikai dimenzió magában foglalja a vezetési és irányítási eszközöket és létesítményeket, az írott és nyomtatott papíralapú információhordozókat (újságokat, könyveket), az adatgyűjtő eszközöket és szenzorokat, a kommunikációs eszközöket és létesítményeket,

[174] Az információs környezet és a kapcsolódó kifejezések bővebb tartalmi és fogalomelméleti összefüggéseinek kifejtését lásd Munk (2002).

valamint az adattárolást és feldolgozást végző számítógépeket. A fizikai dimenzióban nemcsak kizárólag katonai vagy nemzeti infokommunikációs eszközök, létesítmények és rendszerek találhatók, hanem a globális információs környezetben a nemzeti, gazdasági és földrajzi határokon keresztül egymáshoz kapcsolódó információs infrastruktúrák is.

Az információs dimenzió az információs hadszíntér azon nem megfogható dimenziója, ahol a különféle információkezelési folyamatok zajlanak. E dimenzióban történik meg a fizikai dimenzióban értelmezett eszközökkel és infrastruktúrákkal az információ gyűjtése, tárolása, feldolgozása, továbbítása. Ezen kívül e dimenzióban értelmezzük egyrészt a különféle információs folyamatok többnyire elektronikus úton való támadását, másrészt a szemben álló fél saját információs folyamatainkra irányuló támadásának megakadályozását is.

A kognitív dimenzió az információs hadszíntér azon dimenziója, ahol az emberek tudati tevékenységet folytatnak, amely az emberek vagy egyes csoportok információfeldolgozását, -észlelését, -értelmezését és döntéshozatalát jelenti. Az emberi döntéshozatali folyamat mellett e dimenzióban zajlik a szemben álló fél politikai és katonai döntéshozóinak, valamint a személyi állomány és a lakosság gondolkodásának, döntésalkotó képességének befolyásolása, másrészről a szemben álló fél ilyen irányú tevékenységével szembeni védelem is. Ezt a dimenziót a kulturális és vallási hiedelmek, normák, erkölcs, motivációk, érzelmek, tapasztalatok, képzettség, mentális egészségi állapot és ideológiák jelentősen befolyásolják. E tényezők meghatározása egy adott környezetben kritikus fontosságú annak megértéséhez, hogy hogyan lehet a legjobban befolyásolni egy adott célközönség gondolkodását és elérni a kívánt hatásokat. Mivel a döntéshozatal alapvetően kognitív folyamat, ezért ez a dimenzió képezi az információs környezet legfontosabb elemét.

Napjaink légi, szárazföldi, vízi és űrbeli hadszíntereit az információs hadszíntér kapcsolja össze. A katonai műveletekben az információ mindig is fontos szerepet játszott, ezért az információs hadszíntér valójában mindig is részét képezte a katonai műveleti hadszíntérnek. E hadszíntér jelentőségének felismerése azonban csak a korszerű, háló-

zatos infokommunikációs rendszerek elterjedését követően következett be, és megítélése csak az információs korszakban vált igazán fontossá.

3.2. Az információs műveletek kialakulása

Az információ szerepét és jelentőségét manapság nem kell különösebben bizonygatni, hiszen mindenki saját magán tapasztalhatja mai társadalmunk egyik meghatározó hajtóerejének súlyát, fontosságát, esetleges hiányának hatásait. Az információ birtoklása, felhasználása mindig is az emberi társadalmak fontos eleme volt, ugyanakkor az elmúlt korokban ennek felismerése korántsem volt annyira világos, mint manapság. Ma viszont a korszerű hálózatos infokommunikációs technológiának köszönhetően – a korábbi hagyományos információkezelési módokhoz képest – az információhoz való hozzáférés sokkal szabadabban és rendkívül sokrétűen valósul meg.

Az információs jólét azonban ráébreszt bennünket arra a tényre is, hogy milyen hatása lehet annak, ha a megfelelő időben nem áll rendelkezésre megfelelő mennyiségű, pontos és releváns információ, vagy ami manapság az egyik legnagyobb probléma, hogy például nem valós információk tömegével próbálják befolyásolni az embereket. Az információ hiánya, pontatlansága, irrelevanciája vagy elavultsága korábban is probléma volt, de manapság ez már a mindennapi tevékenységünkre is jelentős befolyásoló hatással lehet.

A társadalmi élet minden területén már korábban is megfigyelhetők voltak olyan információs tevékenységek, amelyek ilyen helyzetek előidézésére törekedtek. A politikában, a gazdasági életben és katonai területen egyaránt folyamatosan jelen voltak olyan tudatos információs befolyásoló módszerek, az információra hatást gyakorló tevékenységek, mint például a gazdasági hírszerzés, a katonai felderítés, a megtévesztés vagy a propagandatevékenység. A különböző verseny- és konfliktushelyzetekben állandóan megfigyelhető volt az a törekvés, hogy az egyik fél valós idejű, jobb minőségű és pontosabb információkkal rendel-

kezzen a másik féllel szemben, és azokat gyorsabban és hatékonyabban tudja felhasználni. Ez pedig információs előnyt eredményezhet, ami az előbb jelzett tevékenységek szempontjából a siker egyik fontos előfeltétele. Korábban azonban ezek az információs tevékenységek egymástól elszigetelt módon lettek végrehajtva.

Az információs műveletek, vagy ahogy kezdetben nevezték, az információs hadviselés kialakulása a 70-es évekre tehető. Az akkoriban feltörekvő informatikai és elektronikai technológiák fejlődése, valamint a hálózatok, köztük az ARPANET megjelenése arra késztette a katonai teoretikusokat, hogy az információval kapcsolatos támadó, védelmi és befolyásoló tevékenységeket, illetve azok összehangolásának lehetőségeit kutassák. Az elsők között említhető az USA védelmi minisztériumának magyar származású kutatója, Thomas P. Rona, aki a Boeing cég számára 1976-ban készített kutatási jelentésében először használta az *információs háború* kifejezést. (Rona 1976) Ebben rámutatott, hogy az információs infrastruktúrák kulcsfontosságú szerepet játszanak a gazdasági fejlődésben, és sebezhetőségük mind békében, mind pedig háború idején egyaránt jelentősen kihat a társadalmi és gazdasági folyamatokra. Ebből kifolyólag az információs háború keretében az információs tevékenységek, köztük az ellentevékenységi módszerek is összefonódnak egymással, és hatást gyakorolnak a katonai műveletekre.

Az információs műveletek egyes területei természetesen ennél jóval korábban megjelentek már a katonai műveletekben és a politikai, gazdasági életben egyaránt. Ezek közé tartozott a felderítés és a megtévesztés, amely egyidős a háborúval, a lélektani hadviselés, amely szintén régóta részét képezi a katonai információs befolyásolás eszköztárának, vagy a technológiai fejlődésnek köszönhetően az elektronikai eszközök (rádiók, radarok, navigációs eszközök stb.) zavarása. E képességek a két világháború során jelentős fejlődésen mentek keresztül, aminek köszönhetően az alkalmazott technikák és módszerek folyamatosan tökéletesedtek.

A hidegháború idején a keleti és nyugati blokk országai között is zajlottak különféle információs tevékenységek. Ezek sok esetben a politikai diplomácia színterén játszódtak, különböző információs nyomás-

gyakorló tevékenységek vagy intézkedések keretén belül. Ennek egyik példájaként említhető az USA csillagháborús terve, amelynek megvalósítása során bár az amerikaiak értek el komoly eredményeket, de a legfőbb hatása az információs kampánynak volt. Ezzel a Szovjetuniót egy olyan fokozott űrhadviselési versenybe kényszerítették, amelynek költségét az alacsony életszínvonal ellenére is képtelen volt előteremteni. Másik példa a nyugati országokból sugárzott Szabad Európa Rádió (SZER) fellazító propagandája, amelynek célközönsége a keleteurópai országok lakosai voltak. Ezzel szemben a „vasfüggöny" mögött ellenpropagandát, illetve a SZER vételét akadályozó rádiózavarást alkalmaztak, amit a fixen telepített adótornyokból valósítottak meg.

Az információs műveletek teljes körű kialakulásához a végső lökést az információtechnológia rohamos fejlődése adta meg. A katonai műveletekben az információs műveletek mai értelmezés szerinti kezdeti jegyei a sokszor első információs háborúként is emlegetett első Öbölháborúban voltak felfedezhetők. Az 1991-es „Sivatagi Vihar" hadműveletben célzottan és sokszor összehangoltan is alkalmazták azokat az információs tevékenységeket, amelyeknek egyik alapvető céljuk az ellenséges erők vezetési és irányítási képességeinek korlátozása volt.

Ennek érdekében a szövetséges erők közel negyven napon keresztül a levegőből támadták az iraki erők stabil és mobil telepítésű információs célpontjait, megsemmisítették vezetési pontjait, légvédelmi rendszerének fontosabb rádiólokátorait, híradó központjait, rádióátjátszó állomásait stb. Mindeközben folyamatosan zavarták a légvédelmi radarokat és a rádióösszeköttetéseket. A szövetséges erők, kihasználva infokommunikációs technológiai fölényüket, e műveletek során elsősorban az ellenség információtechnikai képességeinek csökkentésére fókuszáltak, miközben alkalmazták azokat a védelmi módszereket és technikákat, amelyek a saját információs lehetőségeik megóvását célozták. Ezek mellett megtévesztő tevékenységeket és a lélektani hadviselés különféle módszereit is alkalmazták. Mindezekhez pedig még hozzájárult az egyrészt szigorúan irányított tájékoztatási tevékenyég és a „CNN-hatásként" ismert média szerepe is, amelynek köszönhetően

a tv-csatornákon keresztül az emberek élőben követhették a háború eseményeit. Mindezek odáig vezettek, hogy a szárazföldi erők rövid idő alatt, jelentősebb ellenállás nélkül képesek voltak Kuvait területéről kiűzni az iraki erőket és így visszaállítani az ország szuverenitását.

Az Öbölháború után, az ott szerzett tapasztalatok alapján intenzív kutatások indultak meg az összehangolt információs tevékenységek terén, amelynek eredményeit először kutatási jelentések, tanulmányok formájában tettek közé. Ezek közül kiemelendő Martin C. Libicki 1995-ben megjelent tanulmánya, amely az elsők között foglalta össze az információs hadviselés elméleti összefüggéseit. (LIBICKI 1995) Libicki is hangsúlyozta a különféle technikai és humán jellegű információs tevékenységek fontosságát, azok összehangolásának szükségességét, és megadta e tevékenységek körét, amelyek az alábbiak:

- vezetési és irányítási hadviselés,
- hírszerzésalapú hadviselés,
- elektronikai hadviselés,
- pszichológiai hadviselés,
- hackerhadviselés,
- gazdasági információs hadviselés és
- kiberhadviselés.

Ez a felosztás a mai doktrinális értelmezések szerint tartalmazta mind a technikai, mind pedig a kognitív információs tevékenységeket. Ugyanakkor e tevékenységek közül a mai értelmezésben már több is hasonló tartalmat jelent, és átfedésben van egymással. Ilyen például a hackerhadviselés és a kiberhadviselés, amelyek igen sok egyezőséget mutatnak egymással, vagy például az elektronikai hadviselés és a pszichológiai hadviselés, amelyek már korábban is az úgynevezett vezetési és irányítási hadviselés részét képezték, és ami szintén szerepelt a Libicki-féle felosztásban.

Egy másik értelmezés Winn Schwartau nevéhez köthető, amely az 1996-ban megjelent *Information Warfare* című könyvében jelent meg. (SCHWARTAU 1996) Schwartau egy másfajta megközelítésben, az infor-

mációs hadviselés szereplői, illetve annak hatóköre szerint az alábbiak szerint osztályozta az információs hadviselést:

- személyes információs hadviselés,
- vállalati információs hadviselés, valamint
- kormányzati információs hadviselés.

A személyes információs hadviselés során egy információs támadás célpontja az ember maga, amelynek eredményeként az egyéni felhasználó személyes adatai veszhetnek el vagy sérülhetnek. A vállalati szintű információs hadviselés egyik fajtája lehet például az ipari kémkedés, amely az egymással gazdasági versenyhelyzetben lévő cégek, cégcsoportok között különböző formákban nyilvánulhat meg. A kormányzati szintű információs hadviselést pedig a legszélesebb körű információs tevékenységként értelmezi, amelyre 1996-ban még egyértelmű példák nem voltak. Ugyanakkor az elmúlt években már ez is megjelent, például a médiában is nagy nyilvánosságot kapott észt és grúz kibertámadások során. 2007-ben Észtországban összehangolt túlterheléses támadások érték az interneten keresztül az észt kritikus infrastruktúrákat, kormányzati oldalakat, aminek köszönhetően közel két hétig nem voltak elérhetők fontos szolgáltatások, Grúziában pedig a történelemben először, a hagyományos katonai műveletekkel párhuzamosan, szintén informatikai támadásokkal tették elérhetetlenné a grúz parlament internetes oldalát.

Schwartau az információs hadviselést alapvetően csak technikai megközelítésben és elsősorban a számítógép-hálózati környezetben zajló információs tevékenységekre értelmezi, vagyis elsősorban az informatikai támadásokat érti alatta. Ez a szemlélet egyébként megegyezik az információs hadviselés általános polgári felfogásával, amely nem számol a kognitív információs képességekkel, mint például a pszichológiai műveletek vagy a megtévesztés. (Haig 2011) Ezáltal ez nemcsak az elnevezés miatt nem felel meg a mai információs műveleti felfogásnak, hanem az alkalmazható információs tevékenységek szempontjából sem.

Mint látható, az összehangolt információs tevékenységekre vonatkozó korai nézetek elsősorban technikai oldalról közelítették meg az információs műveleteket. Ebben természetszerűleg szerepet játszott, hogy ebben az időszakban bontakozott ki teljeskörűen a mai korra is jellemző infokommunikációs technológiai fejlődés. E technológia minden korábbihoz képest nagyobb lehetőséget biztosított az információ kezelésére. Szembetűnő az is, hogy a korai értelmezések e tevékenységek elnevezésére az információs háborút, később az információs hadviselést alkalmazták. Ez a terminológia kellően kihangsúlyozta az információ és az információs technológiák „fegyverként" való alkalmazását, így némileg a technikai megközelítést is sugallta. Az *információs műveletek* fogalma a mai felfogáshoz legközelebb álló katonai értelmezéssel csak később került be a katonai terminológiába.

3.3. Az információs műveletek elméleti alapjai

3.3.1. Információelméleti megközelítés

Wheatley szerint a társadalmakat fejletlen (vagy kevésbé fejlett) és fejlett társadalmakra vagy más szóval első- és másodfokú társadalmi-technológiai civilizációs fejlettségi szintre oszthatjuk. A fejlett társadalmi formációk jogi és erkölcsi törvényekkel, szabályzókkal és szabályokkal irányított módon, szervezetten működnek. Amennyiben ez a szervezettségi rend – valamilyen külső vagy belső negatív hatásoknál fogva – megszűnik, vagyis a törvények és szabályok már nem képesek hatást gyakorolni a társadalomra, akkor bekövetkezik a szabályozatlanság, a társadalmi-technológiai hanyatlás a fejletlen (vagy kevésbé fejlett) szervezettségi szintre. Ebben az állapotban a káosztörvény érvényesül, vagyis a szervezett, irányítható és ellenőrizhető állapot törvényszerűen szervezetlenséggé, irányíthatatlan és ellenőrizhetetlen káosszá alakul át. (WHEATLEY 2001)

Az információs műveletek elmélete is abból az alapfeltevésből indul ki, hogy minden szervezetnek és rendszernek a működéséhez és a rendeltetésszerű feladatai teljesítéséhez szabályozottságra van szüksége, amely releváns, pontos és időszerű, valamint objektív információk alapján érhető el. Amennyiben ezen információkhoz való hozzáférés korlátozottá válik, abban az esetben a szervezet és a rendszer számára megszűnik a külső környezet megismerésének képessége. Ebben az állapotban csak a saját belső, korlátos információs erőforrásaira tud támaszkodni, ami a hosszabb távú működés és tevékenység szempontjából nem elég. Ez pedig egy idő után az adott szervezet vagy rendszer működésképtelenségéhez, szervezeti és rendszerbeli összeomlásához vezet.

Az információ mennyisége, illetve hiánya azonban csak az egyik igen fontos tényezője a körülmények és a helyzet objektív megítélésének, ugyanis megfelelő mennyiségű információ megléte mellett is bekövetkezhet a fent jelzett állapot, amennyiben az információk minősége nem megfelelő. Amennyiben nem releváns, pontatlan és elavult információk állnak rendelkezésre, vagy az információk között igen nagy számban vannak ilyenek, az is azt eredményezi, hogy e helytelen információkra alapozott helyzetértelmezés nem megfelelő döntéshez vezet. Ez pedig a szervezet és rendszer működőképessége szempontjából ugyanolyan vagy hasonló, esetleg még fokozottabb negatív következményekkel jár.

Az információ ugyanakkor természetszerűleg nem csak szervezetek és rendszerek számára alapvető fontosságú. Ahogy azt korábban is már többször kihangsúlyoztuk, az emberi lét egyik fontos alkotóeleme szintén az információ. Ebből fakadóan a szervezetekre, illetve a rendszerekre vonatkozó fenti információs korlátozó hatások az emberekre is érvényesek. Tehát ha nem áll rendelkezésre elegendő mennyiségű és jó minőségű információ, abban az esetben az ember mindennapi tevékenysége korlátozottá válik, és szintén nem lesz képes objektív döntéseket meghozni. Az ember azonban gondolkodó lény, ami azt jelenti, hogy a szervezetekkel, illetve például a technikai rendszerekkel szemben a racionalitás mellett különféle morális, érzelmi, kulturális, vallási, viselkedésbeli stb. megfontolások alapján hoz döntéseket.

Ez pedig azt is jelenti, hogy ezek mentén az ember az információval manipulálható, befolyásolható, aminek eredményeképpen a gondolkodása és cselekedete a befolyásoló fél által alakítható.

A fentiek alapján bármilyen konfliktushelyzetben, de különösen a katonai műveletekben az alapvető cél a saját oldalon a szervezett rend, az irányíthatóság és ellenőrizhetőség fenntartása, a másik fél oldalán pedig ennek ellenkezője, a szervezetlenség és az irányíthatatlan, ellenőrizhetetlen állapot, vagyis egy sajátos káosz előidézése, ideiglenes kialakítása. E kettős célt a másik fél oldalán negatív, a saját oldalon pedig pozitív irányú, egymással összehangolt információs befolyásoló tevékenységekkel lehet elérni. Az információs műveletek alapvetően erre irányulnak. (Haig–Várhegyi 2005)

Mindezen pozitív és negatív befolyásoló hatások mellett az információs befolyásolás megjelenik az adott konfliktusban semleges szereplők irányában is. Napjaink katonai műveleteire jellemző, hogy sokszor egy ellenség nélküli környezetben kell például béketámogató vagy humanitárius műveleteket folytatni. Ez esetben természetszerűleg nem a káosz előidézése a cél, hanem egy olyan helyzet kialakítása, amely mindkét félnek, tehát a katonai erő és a helyi lakosság számára egyaránt elfogadható. Ezért a katonai erő igen gyakran az információs befolyásolás és együttműködés eszközéhez folyamodik annak érdekében, hogy a katonai feladatok kellő eredményességgel legyenek végrehajtva. Mindezek alapján tehát az információs műveletek egy konfliktus minden szereplőjére hatnak, így a saját félre, a szemben álló másik félre, illetve a semleges érintettekre, polgári szereplőkre egyaránt.

3.3.2. Az információs fölény és a befolyásolás elmélete

3.3.2.1. Az információs fölény klasszikus értelmezése

A saját oldalon pozitív és a másik fél oldalán negatív hatású összehangolt információs tevékenységek értelemszerűen egyfajta előnyt

biztosítanak az e tevékenységeket alkalmazók számára. Ez az előny egy verseny során vagy egy konfliktushelyzetben fölényként jelenik meg, az információs tevékenységek vonatkozásában pedig információs fölényként értelmezhető. A magyar nyelv értelmező szótára szerint a fölény „az a tény, hogy vki, vmi bizonyos szempontból különb, erősebb, fejlettebb a másiknál". (Bárczi–Országh 2016) A fölény tehát egyfajta előnyös helyzetet, megnyilvánuló erőtöbbletet, mennyiségi, minőségi, helyzeti előnyben jelentkező kivételezett állapotot, mástól eltérő, megkülönböztető jelleget takar. Ez az általános meghatározás érvényes az információs fölényre is, ahol az információs jelző alapvetően az információs környezetben értelmezett előnyös helyzetre vonatkozik, és a másik féllel szemben az információnak mennyiségben és minőségben való eredményesebb felhasználására utal.

Munk Sándor szerint katonai értelmezésben az információs fölény két szemben álló fél közötti relatív viszonyt jelenti, amely felhasználható a saját célok, érdekek másik félnél eredményesebb érvényesítésére. (Munk 2001) Értelmezése szerint az információs fölény, vagyis a szemben álló felek információs képességei közötti különbség mértéke időben lehet állandó, ideiglenes, tartós vagy változó. Az információs fölény a szemben álló felek közötti viszonyt jelenti, valamint azt a helyzetet, amelyben ez a viszony fennáll. Ezek alapján az információs fölény az érintett felek információs képességei közötti, az adott fél számára hadműveleti eredményekben realizálható előnyös különbséget mutatja meg.

A kezdeti információs műveleti elméletek fókuszpontjában e fölény megszerzése, fenntartása és a vezetési és irányítási folyamatban való kihasználása állt. Mára a katonai műveletek és a műveleti környezet megváltozásával ez az elsődleges cél módosult. Napjaink katonai műveleteiben ugyanis az összehangolt információs tevékenységek gyakran civil környezetben, a semleges érintettek, esetleg a lakosság irányába valósulnak meg, ahol nem az a cél, hogy a saját erőknek több és jobb minőségű információja legyen, vagy jobban tudja azt felhasználni, hanem a célközönség megnyerése a katonai művelet

céljainak. Ebből a megközelítésből egyes elméletek szerint az információs fölény nem is értelmezhető a polgári környezetben. Más értelmezések szerint, viszont – mint ahogy például Nagy-Britannia információs fölény doktrínájában ez megjelenik – a katonai műveletek jellegétől függően az információs fölény az alábbi kettős megközelítésben értelmezhető:

- hagyományos információs fölény és
- adaptív információs fölény. (JDN 2/13 2013; Rózsa 2016)

A hagyományos információs fölény a klasszikus katonai műveletekben értelmezhető, ahol az egymással szemben álló felek között az infokommunikációs technológiai képességbeli különbségeknek komoly jelentősége van. Ebből kifolyólag e megközelítés alapvetően technológia központú, és az információgyűjtés, -tárolás, -feldolgozás és -továbbítás hatékonyságára összpontosít. A kivívott információs fölény a legtöbb esetben a katonai műveletek teljes spektrumára érvényes.

Az információs fölény hagyományos megközelítése alapvetően az alábbi elveknek való megfelelést jelenti:

- több és jobb minőségű infokommunikációs eszköz és rendszer megléte, ami egy fontos kritérium, de önmagában ennek megléte még nem garantálja az információs fölényt;
- a korszerű technológiának köszönhetően jobb döntés-előkészítés és gyorsabb döntési ciklus;
- az információkezelés terén a parancsnok és a törzs műveleti igényeit kielégítő legjobb gyakorlatok alkalmazása;
- a 6M elvének való megfelelés, amely szerint a megfelelő információ a megfelelő felhasználóknak a megfelelő időben álljon rendelkezésre, ami lehetővé teszi a megfelelő hatások eléréséhez szükséges megfelelő döntés meghozatalát, ami pedig biztosítja a megfelelő eredményességet. (JDN 2/13 2013)

A hagyományos információs fölény megszerzésének és megtartásának három azonos fontosságú oldala van, úgymint:

- információszerzés a parancsnoki döntést befolyásoló tényezőkről, amelyek közé a szemben álló fél helyzete, a saját kötelékek helyzete, valamint a harctéri környezet tartozik;
- a saját információs képességek kihasználása és védelme; valamint
- a másik fél információs képességeinek akadályozása.

Az információs fölény alapját a parancsnoki döntést meghatározó tényezőkről szóló elegendő, pontos, valós idejű és releváns információ biztosítja. Ezekhez az információkhoz részben a szemben álló fél és a környezet felderítése útján, másrészt a saját erők jelentései alapján lehet jutni.

Emellett ki kell alakítani, és eredményesen kell működtetni a saját hálózatos infokommunikációs rendszereket, illetve hatékonyan kell menedzselni az információs folyamatokat. A rendszerek működtetése és az információmenedzsment mellett pedig szükséges a másik fél információs fenyegetései elleni megfelelő védelmi eljárások és intézkedések alkalmazása is.

Mivel a szemben álló fél hasonlóan támaszkodik a saját vezetési és irányítási rendszereire, információs folyamataira és információira, ezért megfelelő képességek birtokában eredményesen kell akadályozni ezen információs rendszereket és folyamatokat, lerontani az információkat, illetve befolyásolni a döntés-előkészítőket, döntéshozókat és a teljes személyi állományt. Ennek eredményeként kevesebb és rossz minőségű információ lesz elérhető a szemben álló fél számára, illetve a humán erőforrás befolyásolása következtében a parancsnok nem lesz képes objektív, valós idejű döntések meghozatalára. (Haig 2011)

Az információs fölény kialakításának alapvető célja, hogy a katonai műveletek végrehajtását meghatározó saját oldali döntések gyorsabbak legyenek, mint a szemben álló félé, és a kialakult helyzet kezelésére megalapozott és releváns reakciókat adjanak. Ennélfogva az elért információs fölény a döntési folyamatban érezteti hatását, vagyis a végcél a döntési fölény elérése. Ennek következtében a saját döntési ciklus ideje a szemben álló fél döntési időciklusához képest rövidebb lesz, tehát a szemben álló félnél gyorsabb lesz a saját információszerzés, helyzetértékelés, döntés

és a feladat végrehajtása. Az időben meghozott és helyes döntésre alapozott feladat-végrehajtás eredményeként új helyzet áll elő a műveleti területen, ami előnyös a döntési fölényben lévő számára és hátrányos a szemben álló félre nézve. A döntési fölény birtokosa ugyanis előbb jut a végrehajtás fázisába, és így képes a kezdeményezést megragadni, valamint akaratát folyamatosan rákényszeríteni a szemben álló félre.

A saját vezetési és irányítási képességek maximális kihasználása és a szemben álló fél hasonló képességének részleges vagy teljes akadályozása a katonai műveletek végrehajtásában érezteti hatását. A saját erők műveletei pontos, időbeli és releváns információk alapján kidolgozott elhatározáson alapulnak. A parancsnok folyamatosan képes követni a saját erők tevékenységét, és a megfelelő időben képes a műveleti helyzetben bekövetkező változásokra reagálni.

Ezzel szemben a másik fél a felderítőképességeinek akadályozása miatt folyamatos információhiányban szenved. Emiatt a parancsnoki döntések pontatlan, nem releváns és többnyire csak valószínűsíthető információkon alapulnak. A kommunikációs csatornák megzavarása miatt az alárendeltekkel való kapcsolattartás bizonytalan vagy lehetetlen, aminek következtében a parancsok és intézkedések nem jutnak le a végrehajtói szintre, illetve az alárendeltek képtelenek helyzetükről tájékoztatni az elöljárót. Ha pedig a feladat végrehajtása irányíthatatlanná és így szervezetlenné válik, bekövetkezik a szervezet és rendszer összeomlása. (HAIG et al. 2013)

3.3.2.2. Az információs fölény adaptív megközelítése – a befolyásolás elmélete

A hagyományos információs fölénnyel szemben az adaptív megközelítés alapvetően nem technikai jellegű. Ehelyett a globális hatásokat is elérő, de helyi kiterjedésű, harcászati szintű információs fölénybe kerül az ellenféllel szemben. Ez sok esetben a szemben álló fél befolyásolásával, manipulálásával érhető el, amely gyakran hatékonyabb-

nak bizonyulhat a technikai eszközök alkalmazásánál. Különösen igaz ez abban az esetben, amikor a szemben álló fél elégtelen vagy hiányos infokommunikációs infrastruktúrával rendelkezik. Ez esetben természetszerűleg nem alkalmazható a hagyományos információs fölény koncepciója, helyette az adaptív megközelítés a célravezető.

Az információs fölény adaptív megközelítése értelmében napjaink katonai műveleteiben a szemben álló fél mellett a műveletek más, nem állami szereplőinek, a semleges érintetteknek és a lakosságnak a befolyásolása is fontos tényezőként jelenik meg. E szereplők közül a vezetők, kulcsszereplők – gyakran például a közösségi média felhasználásával is – a közvéleményt formálják, alakítják, így rajtuk keresztül hatással lehet lenni a szélesebb körű nyilvánosságra is. Ez esetben nem is a szó szoros értelemben vett fölény elérése a cél e szereplőkkel szemben. Az – elsősorban a kognitív dimenzióban érvényesülő – információs tevékenységek inkább arra irányulnak, hogy e szereplők felé folyamatosan olyan információk, üzenetek jussanak el, amelyek a katonai művelet céljainak megfelelően képesek befolyásolni őket.

A társadalmi befolyásolás a szociálpszichológia területei közé tartozó tevékenység, amikor is a befolyásoló hatást gyakorol a célszemély vagy célcsoport tudati tevékenységére, attitűdjére. E tevékenység során olyan hatások elérése a cél, amelynek során a célközönség szellemi beállítottsága, viselkedése, vélekedése és érzelmei megfelelnek a befolyásoló céljainak, elvárásainak. Herbert Kelman a társadalmi befolyásolás alábbi három alapvető formáját határozza meg:

- a megfelelést,
- az azonosulást és
- az internalizációt. (Kelman 1958)

A megfelelés esetében az egyén vagy csoport úgy ért egyet a befolyásolóval, és fogadja el annak érveit, hogy eközben megtartja saját véleményét, és ezzel látszólag megfelel a vele szemben támasztott elvárásoknak. Ez a megközelítés lehetővé teszi a célcsoporttól a megszokott

viselkedés és attitűd helyett a kívánatos és elvárt hozzáállás és gondolkodás elérését. Ha azonban a befolyásoló információ megszűnik, akkor az egyén vagy csoport visszatér a saját korábbi attitűdjéhez, így tartós hatás nem, csak rövid távú viselkedési megfelelés érhető el. Emellett a befolyásoló tevékenység megszűnését követően negatív hozzáállást is okozhat a célközönségben, ezért az információs műveletek keretében alkalmazott befolyásoló tevékenység során ennek az állapotnak az elérése a legkevésbé kívánatos.

Az azonosulás azt jelenti, hogy az azonosuló azért teszi magáévá más személy vagy csoport véleményét, mert olyan szeretne lenni, mint a másik. Az azonosuló megközelítés függ az egyén vagy a csoport befogadóképességétől, illetve a közte és a befolyásolást végző közötti kapcsolat milyenségétől. Ideális körülmények között a befolyásoló tevékenységgel elért attitűdváltozás vélhetően továbbra is fennmarad, és negatív hatásokkal kevésbé kell számolni. Az információs műveletekben ennek az állapotnak az elérése segítheti a befolyásolási célok elérését.

Az internalizáció során a befolyásolt személy teljes mértékben elfogadja, magáévá teszi a másik fél gondolatait, nézeteit, értékeit, és ellenőrzés nélkül is érvényesíti azokat. Ez a megközelítés olyan információkat és üzeneteket alkalmaz, amelyek jól felhasználhatók a befolyásoló céljainak eléréséhez, ugyanakkor megfelelnek a célközönség elfogadott attitűdjeinek is. Az információs műveletek keretében alkalmazott kognitív befolyásoló tevékenységek során ez eredményezi a legjelentősebb, tartós tudati és magatartásbeli változást, de ezt az állapotot a legnehezebb elérni.

Összegzésként a fentiek alapján látható tehát, hogy napjaink katonai műveleteiben az információs fölényt nem csak az infokommunikációs rendszerekre való ráhatással lehet elérni. Bár e rendszerek jelentősen segíthetik a siker feltételeinek megteremtését, a változó műveleti környezet és a műveletek szereplőinek kibővülése megköveteli az információs fölény koncepciójának átértékelését.

Hagyományos konfliktusokban, megfelelő színvonalú infokommunikációs infrastruktúra megléte esetén alkalmazható az információs fölény hagyományos megközelítése azzal a megkötéssel, hogy a technikai képességek mellett a kognitív befolyásoló tevékenységek szerepe mára jelentősen felértékelődött. Az adaptív megközelítés ugyanakkor jobban kihangsúlyozza a kognitív befolyásolóképességek szerepét. E befolyásoló tevékenységek jelentőségét a kibertérben, a hálózatos infokommunikációs technológia nyújtotta szolgáltatásoknak köszönhetően, az internetes hírportálokon, illetve a közösségi médiában egyre terjedő álhírek csak fokozzák.

3.4. Az információs műveletek fejlődése

3.4.1. A fejlődés korai szakasza

Az információs műveletek koncepciója, mint arra korábban utaltunk, a 90-es évek elején alakult ki. Ugyanakkor a vezetési rendszerek elleni összehangolt tevékenység igénye már ezt megelőzően is megjelent az USA haderejében, amely az 1987-ben kiadott JP 3-13 összhaderőnemi vezetési, irányítási és kommunikációs ellentevékenységi doktrína[175] formájában öltött testet. (JP 3-13 1987) Az Öbölháborúban szerzett tapasztalatokat felhasználva 1996-ban felhasználva fejlesztették tovább e doktrínát összhaderőnemi szintű vezetési és irányítási hadviselési doktrínává,[176] amelyben már nemcsak az ellentevékenység, hanem a saját információs képességek védelme is megjelent. (JP 3-13.1 1996)

Ugyanebben az évben azonban az USA szárazföldi haderőneme kiadta az első *FM 100-6 Információs műveletek* című tábori kézikönyvét. (FM 100-6 1996) Ez már értelmezte a korszerű katonai

[175] Command, Control, Communications Countermeasures – C3CM.
[176] JP 3-13.1 Joint Doctrine Command and Control Warfare (1996).

műveletek új színterét, az információs környezetet, kiemelte fontosságát, és rámutatott az információs infrastruktúrák elleni fenyegetések hatásaira. Elsőként fogalmazódott meg benne az információs fölény és uralom kialakításának igénye, illetve a helyzettudatosság és a kognitív hierarchia fontosságának hangsúlyozása.

Az információs műveleteken belül az FM 100-6 három összetevőt különböztet meg: az információs rendszereket, a releváns információkat és felderítést (hírszerzést), valamint a műveleteket. A műveleteken belül a vezetési és irányítási hadviselést,[177] valamint a polgári kapcsolatokkal[178] és a közkapcsolatokkal[179] (tájékoztatással) foglalkozó műveleteket határozza meg. A vezetési és irányítási hadviselés a szemben álló fél információs képességeinek befolyásolására, akadályozására és megsemmisítésére, valamint a saját információs képességek védelmére irányul. A doktrína értelmezi a támadó és védelmi jellegű vezetési és irányítási hadviselést, amely a korábbi doktrínának megfelelően a pszichológiai műveletek, a műveleti biztonság, a megtévesztés, a fizikai pusztítás és az elektronikai hadviselés összehangolt alkalmazását jelenti. (FM 100-6 1996)

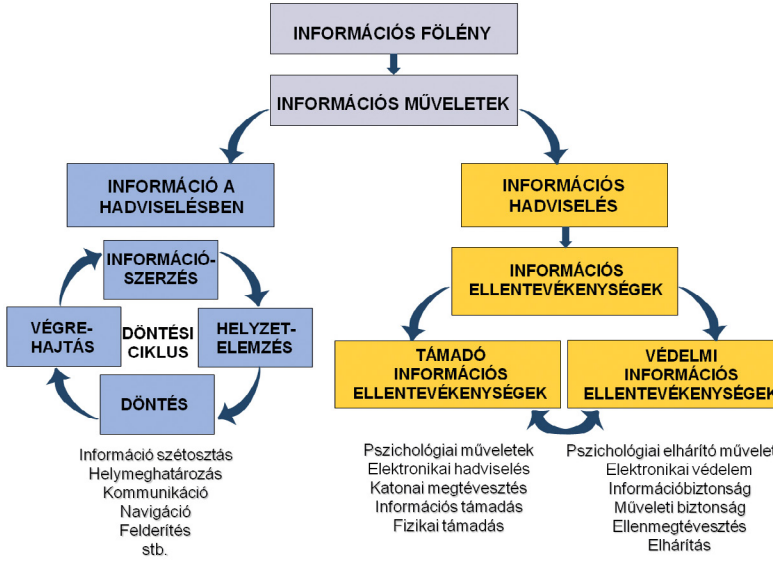
Láthatóan a doktrína a korábbi felfogásokhoz képest szélesebb körűen, a katonai műveletek teljes spektrumában értelmezte az információs műveleteket. Megjelentek benne a különféle információs tevékenységek, bár azok összehangolásának szükségességére és hatásnövelő képességére csak elvétve található benne utalás. Emellett elsőként merült fel doktrína szintjén a polgári szférához kapcsolható információs tevékenységek (polgári kapcsolatok, közkapcsolatok) szerepe a katonai műveletekben. Ugyanakkor a támadó és védelmi képességekben az elnevezés szempontjából is megmaradt a korábbi vezetési és irányítási hadviselési felosztásnál és koncepciónál.

---

177 Command and Control Warfare – C2W.

178 Civil Affairs Operations.

179 Public Affairs Operations.



15. ábra

Az USA légierejének az 1998-as doktrína szerinti információs műveletek koncepciója

Forrás: AFDD 2-5 (1998), 3. alapján a szerző szerkesztése

Két évvel később, 1998-ban AFDD 2-5 jelzéssel az USA légierő is kiadta saját információs műveletek doktrínáját. (AFDD 2-5 1998) Ebben szintén fontos szerepet tulajdonítottak az információs környezetnek, és az információs fölény kivívását mindenképpen elérendő célként fogalmazták meg. A doktrína a szárazföldi haderőnem nézeteihez képest sok tekintetben más meghatározásokat használt. Külön értelmezte az információ hadviselésben betöltött szerepét és az információs hadviselést. Előbbiben alapvetően az információ megszerzése, vagyis a felderítés és az információ ki- és felhasználása, utóbbiban pedig az információ támadó és védelmi „fegyverként” való alkalmazása játszik szerepet. Az információs hadviselésben az információs ellentevé-

kenységek körébe a támadó és a védelmi információs ellentevékenységeket sorolta, ezeken belül pedig sajátos megközelítéssel a 15. ábrán látható információs tevékenységeket értelmezte.

Láthatóan a támadó és védelmi információs ellentevékenységek egymással is szoros kapcsolatban vannak, hiszen például a támadó tevékenységek alá sorolt elektronikai hadviselés része a védelmi tevékenységek közé tartozó elektronikai védelem, a pszichológiai műveletek része a pszichológiai műveleti elhárítás, vagy a katonai megtévesztés részét képezi az ellenmegtévesztés. Ez alapján az információs műveletek egy rendkívül bonyolult és szerteágazó információs tevékenységeket magában foglaló képességnek tűnik. Habár a koncepció fő célként az információs fölény megszerzését határozta meg, de még ez sem tartalmazta az információs műveletek egyik fő alapelvét, az információs tevékenységek integrálását és összehangolását.

A légierő-doktrínával egy időben, szintén 1998-ban jelent meg JP 3-13 jelzéssel az első összhaderőnemi információs műveleti doktrína. Eszerint az „információs műveletek mindazon tevékenységek, amelyek hatással vannak a szemben álló fél információira és információs rendszereire, miközben megvédik a saját információkat és információs rendszereket”.[180] (JP 3-13 1998, I-1) A doktrína támadó és védelmi információs műveleteket különböztetett meg. Alapvető, de nem kizárólagos támadó és védelmi képességeknek tekintette a műveleti biztonságot, a megtévesztést, a pszichológiai műveleteket, az elektronikai hadviselést, valamint az információs objektumok fizikai pusztítását.

A JP 3-13 láthatóan már az átfogóbb megközelítést képviselte. Elsőként hangsúlyozta ki a támadó és védelmi képességek szoros és folyamatos integrációját, valamint a vezetés és irányítás, illetve a felderítőtámogatás hatékony összehangolását. Emellett a szélesebb értelemben vett katonai műveletekben való alkalmazás szükségessége is felfedezhető e húsz évvel ezelőtti koncepcióban, amelyre az infor-

[180] Fordította a szerző.

mációs műveletekkel kapcsolatos tevékenységek körébe sorolt civil kapcsolatok és a tömegtájékoztatás is utal.

Fontos kiemelni, hogy először jelenik meg a számítógép-hálózati támadás lehetősége mint potenciális információs műveleti tevékenység. Ez azért lényeges, mert a haditechnikai fejlesztésekben ekkor jutottak el a harctéri hálózatok kialakításának lehetőségéhez. Ekkor kezdődött el a harcászati internet[181] koncepciójának gyakorlatba való átültetése, amely az e fajta támadások potenciális célpontja a harctéren. Érdekes azonban, hogy a saját hálózatok védelme mint lehetséges alapvető védelmi információs tevékenység még nem jelenik meg.

Látható tehát, hogy a 90-es évek végére az információs műveletek elmélete kialakult, a doktrinális alapjai megteremtődtek. Az akkori elméletek és a gyakorlati alkalmazás azonban még a hagyományos műveleti koncepcióba illettek. Ezekben a katonai műveletekben még egyértelműen azonosíthatók voltak a szereplők, a harctevékenységek a saját erők és az ellenség között zajlottak. Ez az információs műveletek akkori felfogásán is egyértelműen megmutatkozott. Emiatt az információs műveletek támadó és védelmi jellegének megkülönböztetése és kihangsúlyozása teljesen elfogadható nézet volt. A műveletekben a polgári szereplők a mai műveleti környezethez viszonyítva kevésbé voltak jelen, ezért azok, illetve a semleges érintettek befolyásolása csak érintőlegesen jelent meg e felfogásban.

Az információs műveletek elméleti és doktrinális megalapozásában az Amerikai Egyesült Államok mint a világ legfejlettebb haderővel rendelkező országa játszott vezető szerepet. Felismerték az információ jelentős erő- és képességsokszorozó szerepét, amely a korszerű katonai műveletekben a siker egyik fontos záloga. Ebben az időszakban más országnak nem volt információs műveletekkel foglakozó hivatalos stratégiája, irányelve vagy doktrínája. Ugyanakkor több országban megkezdődött e terület intenzív kutatása és az eredmények közzé-

[181] Tactical Internet.

tétele. Oroszország és Kína ekkor még elsősorban csak elvi síkon foglakozott az információs műveletek, illetve az orosz és kínai szóhasználattal *információs hadviselés* elméleti megalapozásával.

3.4.2. A hadviselés és a műveleti környezet változása

A hadviselés a technológiai fejlődésnek köszönhetően, illetve a hadviselésben részt vevők körének és azok képességeinek, lehetőségeinek függvényében folyamatosan változik. E változás fontosabb jellemzőit jól mutatja a hadviselés korszakolása, amely elméletnek egyik jeles képviselője William S. Lind, aki a hadviselést négy generációra osztja. (Lind 1989) Az első három generációt alapvetően azonos paradigma jellemezi, miszerint a háború állami monopólium, amelyet nemzetállamok reguláris erői vívnak abból a célból, hogy megsemmisítsék az ellenség hadviselő képességét, és megtörjék akaraterejét. A negyedik generációs hadviselés azonban szakít ezzel a paradigmával, mivel itt nem állami szereplők is szemben állnak az állam hadviselési monopóliumával. (Kiss 2009) Az egyes generációk korszakhatárainak, jellemzőinek és fő teoretikusainak összehasonlítását mutatja a 2. táblázat.

Napjainkban azt tapasztalhatjuk, hogy a hagyományos háborúkkal szemben a regionális feszültségek megerősödnek, ami világszerte jelentősen növeli a konfliktusok előfordulásának gyakoriságát és intenzitását. Emiatt korunk háborús konfliktusainak műveleti környezete jelentősen különbözik a tradicionális állam-állam elleni, reguláris erőkkel folytatott fegyveres konfliktusoktól. Ezeket az új típusú katonai műveleteket a negyedik generációs hadviselési modellen belül számos elnevezéssel jelölik, mint például: aszimmetrikus, irreguláris, felkelés elleni vagy hibrid hadviselés, de a kiberhadviselés is idesorolható. Ezek a műveletek minden korábbinál átfogóbbak és dinamikusabbak, és az aszimmetrikus hadviselés elveinek megfelelően pedig igen gyakran irreguláris erők állnak szemben reguláris erőkkel. (Balogh 2015)

2. táblázat

A hadviselés generációi

Hadviselés generációi	Első generációs hadviselés	Második generációs hadviselés	Harmadik generációs hadviselés	Negyedik generációs hadviselés
Korszakhatárok	Vesztfáliai béke (1648) – Amerikai polgárháború (1861–1865)	Amerikai polgárháború (1861–1865) – Első világháború (1914–1918)	Második világháború (1939–1945) – Első Öbölháború (1991)	Szovjetunió összeomlása (1991) –
Jellemzők	A hadviselés állami monopólium. A háborúk nemzetállamok között zajlanak. Vonal- és oszlopharcászat. Fő fegyver a muskéta. Megjelenik a sorozott hadsereg.	A fegyvernemek közötti összhang megvalósítása. A tűzerő koncentrálása az ellenség erőinek felmorzsolása érdekében. A nemzetállamok erőforrásainak bevonása, felhasználása.	Manőverező hadviselés (Blitzkrieg). Manőverek, gyorsaság és a meglepés hatékony alkalmazása. Páncélosok önálló fegyvernemként való alkalmazása. Átkarolás, megkerülés és bekerítés. Nem lineáris hadviselés.	Hálózatalapú hadviselés. Kontaktus nélküli háború. Aszimmetrikus hadviselés és irreguláris erők. Állami és nem állami szereplők. Kultúra, politikai, társadalmi tényezők hatásai. Információs műveletek. Globális terrorista szervezetek.
Teoretikusok	Karl von Clausewitz	Ludwig von Moltke	Heinz Guderian, Mihail Tuhacsevszkij, Basil Liddel Hart	William L. Lind

Forrás: Balogh (2015); Lind (1989) alapján szerkesztette Fekete Csanád

Míg a hadviselés első három generációjában a katona, a polgár és az állam egyértelműen szétválasztható és megkülönböztethető, addig a negyedik generációs hadviselés egyik fő jellemzője, hogy a katonák és civilek közötti határ eltűnik, hadviselő félként pedig nem állami szereplők is megjelennek, illetve a műveleti területen a lakosság és a semleges érintettek is a konfliktus részesévé válnak. (Rózsa 2016) Ebből

fakadóan pedig a konfliktus szinte totális formát öltve a társadalom egészét érinti.

A negyedik generációs hadviselésben a béke és a háború időszakai közötti határ elmosódik, az állami és nem állami, vagyis a reguláris és irreguláris erők és szereplők között legtöbbször nincs hadüzenet, és nem létezik jól elkülöníthető és felismerhető harctér sem. A műveletek gyakran egymástól elszigetelt körzetekben, városokban vagy egyre inkább a fizikailag nem megfogható világban, a kibertérben zajlanak. Az ilyen fajta műveleteket napjainkban leginkább hibrid hadviselésként határozzák meg a katonai teoretikusok.

Hoffman megfogalmazása szerint: „[A] hibrid fenyegetések felölelik a hadviselés teljes spektrumát, beleértve a hagyományos képességeket, az irreguláris harceljárásokat és alakulatokat, a válogatás nélküli erőszakot és kényszerítést alkalmazó terrorista akciókat, valamint a bűnügyi zavargásokat. Hibrid háborúkat az állami és a legkülönfélébb nem állami szereplők egyaránt folytathatnak. Ezeket a szerteágazó tevékenységeket egymástól elszigetelt egységek, vagy akár ugyanazon alakulatok is végrehajthatják, de ezek általános műveleti és harcászati irányítása és koordinálása a fő harctéren történik annak érdekében, hogy szinergikus hatásokat érjenek el a konfliktusok pszichológiai és fizikai dimenzióiban egyaránt. Ezen hatások a háború valamennyi szintjén elérhetők."[182] (Hoffman 2007, 8.)

A hibrid műveletekben az egymással szemben álló felek nemcsak tradicionális fegyverekkel próbálják egymást térdre kényszeríteni, hanem olyan fizikai, információs és kognitív képességekkel is, amelyek a társadalmi, gazdasági és kulturális területeken egyaránt éreztetik hatásukat. E támadásokhoz sokszor a pusztító fegyvereken kívül a pszichológiai műveletek eszköztárába tartozó klasszikus kognitív befolyásolási és manipulációs eszközöket és módszereket is alkalmaznak. Emellett ma egyre gyakoribb, hogy akár a legkorszerűbb infokommunikációs

[182] Fordította a szerző.

technológiákat is kihasználva a kibertérben terjesztett álhíreket is felhasználják az emberek és a közvélemény befolyásolására. Ennek következtében ezek a támadások elsősorban nem a reguláris erőket, hanem az emberek gondolkodásán, érzelmeiken keresztül a nem állami szereplőket, köztük is a lakosságot és a semleges érintetteket veszik célba, aminek következtében például a demokratikus elveket és a társadalom jogi kereteit lehet aláásni.

A hibrid hadviselésben a felek a legkorszerűbb infokommunikációs technológiákat és azok alkalmazását ötvözik a hagyományos és az irreguláris hadviselés jellegzetességeivel. A konfliktusok lélektani hatása döntő fontosságúvá válik. A kognitív dimenzióban és a fizikai, illetve az információs dimenziókban elért szinergikus hatások szerepe felértékelődik e műveletekben. A felek sokszor a közvetlen hatások helyett közvetett módszereket alkalmaznak egymással szemben, amelynek a kognitív befolyásolás az egyik meghatározó eleme, és amelyben a kulturális, vallási és etnikai szempontok is jelentős szerepet játszanak. (Rózsa 2016) E kognitív befolyásolás eredményes megvalósításában – az infrastrukturális feltételek megléte esetén – a kibertér és az abban zajló folyamatok, különösen a közösségi média és a hírportálok véleményformáló hatása, valamint az eseményekről valós időben tudósító globális média meghatározó szerepet kap.

Mint látható tehát, napjaink konfliktusaiban a hadviselés és a műveleti környezet változásának vagyunk tanúi. Az információs műveletek szempontjából e változás egyik legfontosabb jellemzője a műveletekben részt vevő és a műveletek által érintett civil szereplők megjelenése és ezáltal a kognitív befolyásolás szerepének felértékelődése. Ez jelentős hatással volt az információs műveletek elméletének, doktrinális leképeződésének és gyakorlati alkalmazásának átalakulására, fejlődésére is. A korábban elsősorban információtechnológiai orientációjú szemléletmód átalakult, és ma már hasonló hangsúllyal jelenik meg a kognitív hatások előidézése. Az emberi gondolkodást, vélekedést, viselkedést célba vevő és az érzelmekre is ható eszközök és módszerek, a befolyásolás és a manipuláció, illetve a civilekkel való együttműködés

szükségessége mára kiegyenlítette az információs műveletek korábbi, alapvetően technokrata megközelítését. Ugyanakkor az infokommunikációs technológiai fejlődésnek köszönhetően a hálózatok, az internet, a Facebook, a Twitter és más közösségimédia-felületek – mint kognitív befolyásolást közvetítő média – jelentősen segíthetik e hatások elérését.

A továbbiakban megvizsgáljuk, hogy napjainkban hol tart az információs műveletek elmélete és doktrinális értelmezése, illetve a hadviselés és a műveleti környezet megváltozása milyen hatásokat eredményezett e koncepciókban. Áttekintjük, hogy melyek azok a fő szempontok, amelyek az egyes mértékadó országok, a NATO és hazánk információs műveletekkel kapcsolatos felfogásában fontosnak tekinthetők, és ezek között milyen összhang, illetve különbségek fedezhetők fel.

3.5. Az információs műveletek kiteljesedése

3.5.1. Az Egyesült Államok információs műveletek koncepciójának változása

Mint látható volt, a 90-es évek végén megtörtént az információs műveletek elméleti és doktrinális megalapozása, a kétezres évektől pedig elkezdődött elméleti kiteljesedése és katonai műveletekben való gyakorlati alkalmazása. Az évek során mind az elméleti megközelítésben, mind pedig a gyakorlati megvalósításban fokozatosan érvényesültek az előzőekben bemutatott hadviselési és műveleti környezeti változások.

Az amerikai koncepcióban bekövetkező változás kezdetét a 2006-ban kiadott, új JP 3-13 összhaderőnemi információs műveletek doktrína mutatta. Eszerint az információs műveletek „az elektronikai hadviselés (EW),[183] számítógép-hálózati műveletek (CNO),[184] pszi-

[183] Electronic Warfare – EW.
[184] Computer Network Operations – CNO.

chológiai műveletek (PSYOP),[185] katonai megtévesztés (MILDEC)[186] és a műveleti biztonság (OPSEC)[187] integrált alkalmazása, összehangoltan bizonyos támogató és kapcsolódó képességekkel, amelyekkel befolyásolja, megzavarja, lerontja, vagy korlátozza a szemben álló fél humán és automatizált döntéshozatali folyamatát, miközben megvédi a saját hasonló képességeket".[188] (JP 3-13 2006, I-1)

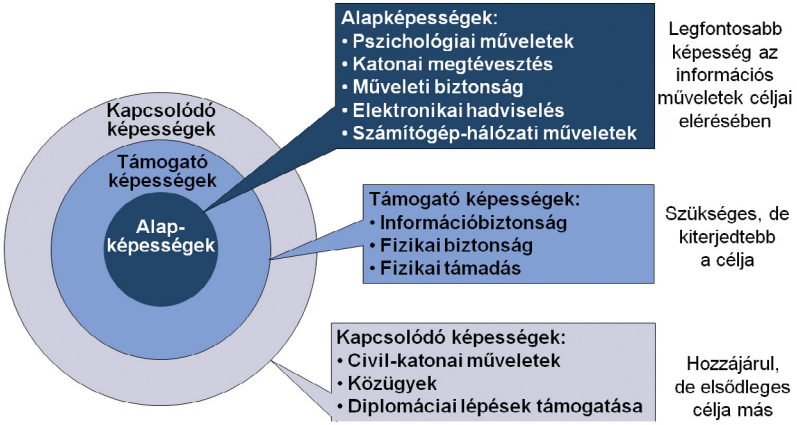
A definícióban előtérbe kerül a már korábban is említett információs tevékenységek közötti koordináló, integráló funkció úgy, hogy emellett hangsúlyozza a különböző támogató és kapcsolódó képességekkel való szoros összhangot. Kiemeli, hogy az információs műveletek az említett képességekkel a szemben álló fél és a saját döntési folyamatra kíván hatást gyakorolni. A definíció egyértelműen nem tesz említést az elérendő célokról, de más helyeken fő célként – hasonlóan a korábbi doktrínához – az információs fölény kivívását és fenntartását határozza meg.

A doktrína a korábbihoz képest jóval több képességet, információs tevékenységet nevesít, amelyek az információs műveletek egyre szélesebb körű értelmezését és szerteágazó hatásmechanizmusát szemlélteti. E tevékenységeket alapképességekként, támogatóképességekként és kapcsolódó képességekként három nagy képességcsoportba kategorizálja. Ezeket a 16. ábra szemlélteti.

Az alapképességek közé azok az információs tevékenységek tartoznak, amelyek integrált és szinkronizált tervezése, illetve végrehajtása az információs környezetben kiemelt fontosságú. A támogatóképességeknek az információs műveletekhez képest alapvetően kiterjedtebb körű katonai célkitűzéseik lehetnek, ugyanakkor azok is az információs környezetben érvényesülnek, és hatást is gyakorolhatnak arra. A kapcsolódó képességeknek pedig vannak közös kapcsolódási pontjaik az információs műveletekkel, azonban elsődleges céljaikban

185 Psychological Operation – PSYOP.
186 Military Deception – MILDEC.
187 Operation Security – OPSEC.
188 Fordította a szerző.

és az alkalmazott tevékenységeikben, eszközeikben és módszereikben jól elkülöníthetők az információs műveletektől. (JP 3-13 2006)



16. ábra

Az USA összhaderőnemi információs műveletek képességei a 2006-os doktrína szerint

Forrás: JP 3-13 (2006) alapján a szerző szerkesztése

Megfigyelhető tehát, hogy a számos információs képesség nevesítésével, összehangolásuk és integrálásuk kihangsúlyozásával az információs műveletek egyre jelentősebb szerepet kaptak az USA katonai műveletek megvívására vonatkozó elgondolásaiban. Ebben az időszakban ugyan a műveleti környezetben bekövetkező változások még nem eredményeztek gyökeres koncepcióváltozást, azonban a fizikai, az információs és a kognitív dimenzióban alkalmazható képességek egyenrangúsága már egyértelműen megfigyelhető.

Fontos változás volt az is, hogy a számítógép-hálózati műveletek teljes körű tevékenységekként jelentek meg a doktrínában. Ez azt jelenti, hogy már nemcsak a számítógép-hálózati támadás, de a felderítés és a védelem is hasonló hangsúlyt kapott benne. Némi zavart okozhat

azonban, hogy a fizikai védelem, az információbiztonság és az elhárítás külön támogatóképességként lett meghatározva, ugyanakkor alapképességként a műveleti biztonság is nevesítve van, amelynek azonban a mai értelmezésünk szerint az előbbi három terület a részét képezi.

Az Egyesült Államok – mint az információs műveletek elméleti és doktrinális megalapozásában élenjáró ország – 2010 után felismerve a katonai műveletek lefolyásának alapvető megváltozását, átértékelte addigi álláspontját és nézeteit az információs műveletekkel kapcsolatban. Számos elméleti alapozó tanulmány elkészítése és az eredmények szintetizálása után 2012-ben kiadták az új összhaderőnemi szintű JP 3-13 információs műveletek doktrínát, amelyet 2014-ben egy információs műveletek értékeléséről szóló fejezettel egészítettek ki. (JP 3-13 2014)

A doktrína a korábbiakhoz hasonlóan az információs környezet értelmezéséből indul ki, és meghatározza benne az egymással kölcsönös kapcsolatban álló dimenzióit, úgymint:

- a megfogható fizikai dimenziót, amely a való világot jelenti;
- az adatközpontú információs dimenziót és
- a humán központú kognitív dimenziót.

Fontos változás, hogy a humán oldali befolyásolás fontosságának felismerése következtében a kognitív dimenziót az információs környezet legfontosabb komponensének tekinti. Emellett külön megemlíti az információs környezetben a kiberteret mint új műveleti színteret. A doktrína az információs környezetben a befolyásolás céljára kiválasztott egyénre vagy csoportra, más néven célközönségre fókuszál, ami jól mutatja azt a paradigmaváltást, amely a kognitív információs képességek szerepének a felértékelődését jelenti.

Ez részben az információs műveletek fogalmából is kitűnik, miszerint „az információs műveletek a katonai műveletek során a szemben álló fél és a potenciális ellenség döntéshozatali folyamatának befolyásolása, megzavarása, lerontása vagy kisajátítása, illetve a saját döntéshozatal védelme érdekében az információval kapcsolatos képességek integrált alkalmazását jelenti összhangban más műveleti tevé-

kenységekkel".[189] (JP 3-13 2014, I-1) Láthatóan a cél az ellenség és a saját döntéshozatali folyamatra való hatásgyakorlás. Ugyanakkor a definíció nem hangsúlyozza külön a műveleti területen harmadik félként megjelenő semleges érintetteket vagy a polgári szereplőket.

A doktrína megszünteti a korábbi alap-, támogató és kapcsolódó képességek szerinti csoportosítást, helyette bevezeti a különféle hatások elérését célzó információval kapcsolatos képességeket. Ezek közé sorolja többek között a stratégiai kommunikációt, a tömegtájékoztatást, a civil-katonai együttműködést, a kibertéri műveleteket, az információbiztonságot, a katonai információs támogató műveleteket, a hírszerzést, a katonai megtévesztést, a műveleti biztonságot, a különleges technikai műveleteket, az elektromágneses spektrum műveleteit és a kulcsfontosságú vezetőkkel való kapcsolatot.

A doktrína egyik fő újdonsága, hogy létrehozza az úgynevezett információs és befolyásolási relációs keretmodellt,[190] amely lépésről lépésre meghatározza, hogy a célközönség információs képességeire mely információval kapcsolatos képességek alkalmazásával, milyen módon lehet hatást gyakorolni. A modell abból indul ki, hogy a műveletek során a megkívánt végállapot eléréséhez a célközönség (egyének és csoportok) attitűdjét, viselkedését, hitét, meggyőződését bizonyos hatásokkal lehet megváltoztatni. Ehhez szükséges a célközönség meghatározása, a viselkedését meghatározó jellemzőinek értékelése és a megfelelő hatásokat kiváltó információs képességek kiválasztása. A doktrína értelmezésében az információval kapcsolatos képességek technikai és kognitív jellegűek lehetnek, de alkalmazásuk során nem az egyes képességek jellege és az alkalmazó a fontos, hanem a végállapot elérése érdekében azok összehangolt, integrált alkalmazására helyeződik a hangsúly. (JP 3-13 2014)

Amint látható, az USA összhaderőnemi információs műveletek doktrínája szakít a korábbi felfogással, amely a különféle információs

[189] Fordította a szerző.

[190] Information and Influence Relational Framework.

képességekre, mint például az elektronikai hadviselésre, műveleti biztonságra, megtévesztésre, pszichológiai műveletekre stb. és azok integrált alkalmazására fókuszált. Ehelyett, bár felsorolja azokat az információs képességeket, amelyekkel információs műveleti célokat lehet elérni, de a végcél elérése érdekében a folyamatot hangsúlyozza. A folyamatot pedig az információs és befolyásolási relációs keretmodell írja le, egyértelműen meghatározva az egyes lépéseket. Ugyan a definícióból nem derül ki egyértelműen, de a célközönség fogalmának bevezetésével kitágítja azoknak a körét, akikre az információs műveletek hatnak. Ez lehetőséget ad arra is, hogy ezen elvek mentén a megváltozott műveleti környezetben a nem állami szereplőkre, semleges érintettekre is kiterjessze az információs műveletek hatókörét.

A célközönség fókuszpontba állítása azt is jelenti, hogy az információs műveletek alapvetően az emberek viselkedését meghatározó szabályok és normák, valamint gondolkodásuk, érzelmeik, meggyőződésük megváltoztatására irányul. Ez közvetlenül a kognitív jellegű képességekkel, közvetve pedig a különféle technikai és infokommunikációs technológiai eszközökkel és eljárásokkal valósítható meg. Ez utóbbi fontosságát támasztja alá, hogy a doktrína az információs környezet definiálásakor annak dimenzióit a korábbi elvekhez hasonlóan értelmezi, de külön megemlíti a kiberteret mint a katonai műveletek egy új, ötödik színterét. Ez pedig azt is jelenti, hogy az információs műveletek megvalósítása szempontjából a kibertérben alkalmazható, illetve ott a hatásokat előidéző információval kapcsolatos képességek egyre fontosabb szerepet játszanak a műveleti célok elérésében.

3.5.2. Az információs műveletek NATO-értelmezése

A kétezres évek elején a NATO is intenzíven kezdett el foglalkozni az információs műveletek alkalmazásának fontosságával és lehetősége-

ivel. A NATO információs műveletekkel foglalkozó irányelveit[191] először 1998-ban adták ki, amelyet 2002-ben, 2005-ben, 2007-ben, majd 2012-ben vizsgáltak felül és dolgoztak át. A 2007-es irányelvek alapján a NATO 2009-ben jelentette meg AJP-3.10 összhaderőnemi információs műveletek doktrínáját, amely egységes keretbe foglalja a NATO összehangolt információs tevékenységinek elveit. (AJP-3.10 2009) A megjelenés idejére a korábban tárgyalt hadviselési változások, a negyedik generációs hadviselés elvei már teljeskörűen érvényesültek. Az afganisztáni műveletek már e műveleti elvek mentén, egy korábbiakban nem megszokott, polgári szereplőket is magában foglaló műveleti környezetben zajlott. A doktrína pedig már jól tükrözte ezt a megváltozott műveleti környezetet, amelyben az információs műveleteknek érvényesülnie kell.

A doktrína meghatározása szerint: „a) Az információs műveletek egy olyan katonai funkció, amely koordinálja a katonai információs tevékenységeket, illetve azokkal kapcsolatos tanácsokat ad abból a célból, hogy megfelelő hatást gyakoroljon a szemben álló fél, a lehetséges szemben álló fél, és az NAC[192] által jóváhagyott felek szándékára, helyzetmegértési folyamatára és képességeire, és ezáltal támogassa a Szövetség missziós célkitűzéseit. b) Az információs tevékenységek hatást gyakorolnak az információra és/vagy az információs rendszerekre. Azokat bármilyen szereplő végrehajthatja, és védelmi rendszabályokat is tartalmaznak."[193] (AJP-3.10 2009, 1–3)

A NATO-doktrína három olyan tevékenységi területet nevesít, amelyeken keresztül az információs műveletek megvalósulnak. Ezek az alábbiak:

- a szemben álló fél, valamint az Észak-atlanti Tanács által jóváhagyott felek észlelésének, magatartásának, viselkedésének megváltoztatására, befolyásolására vagy megerősítésére irányuló információs tevékenységek;

[191] MC 422/3 NATO Military Policy on Information Operations.
[192] NAC – North Atlantic Council.
[193] Fordította a szerző.

- a NATO információs környezetben való manőverszabadságának megőrzésére és megóvására irányuló információs tevékenységek, amelyek biztosítják a döntéshozókat és döntéshozatali folyamatokat támogató adatok és információk védelmét, valamint
- a vezetési képességek elleni tevékenységek, amelyek hatást gyakorolnak a szemben álló felet és más szereplőket támogató mindazon adatokra és információkra, amelyeket a vezetési és irányítási, felderítő, megfigyelő és célfelderítő, valamint fegyverrendszerekben használnak.

Ezeknek megfelelően a doktrína felsorolja mindazon információs képességeket és eljárásokat, amelyek a fenti három tevékenységi területen az információs műveletek célkitűzéseinek elérése érdekében alkalmaz. Ezek az alábbiak:

- pszichológiai műveletek (PSYOPS),
- megjelenés, viselkedés, arculat (PPP),[194]
- műveleti biztonság (OPSEC),
- információbiztonság (INFOSEC),[195]
- megtévesztés,
- elektronikai hadviselés (EW),
- fizikai pusztítás,[196]
- kulcsfontosságú vezetők kezelése (KLE),[197]
- számítógép-hálózati műveletek (CNO), valamint
- civil-katonai együttműködés (CIMIC).[198] (AJP-3.10 2009)

Mint látható, a NATO-doktrínában megjelent az információs műveletek lényege, ami a különböző katonai információs tevékenységek koordinálását, szinkronizálását és szinergikus alkalmazását jelenti. Az informá-

[194] Presence, Posture and Profile – PPP.
[195] Information Security – INFOSEC.
[196] Physical Destruction.
[197] Key Leader Engagement – KLE.
[198] Civil-Military Cooperation – CIMIC.

ciós tevékenységek összehangolt alkalmazása során a befolyásoló tevékenységek, az ellentevékenységek és a védelmi tevékenységek közötti szoros kapcsolat kialakítására helyeződik a hangsúly. Ennek eredményeként a felsorolt információs képességek és eljárások koordinációjának fő célja a különböző célcsoportok (saját erők, szemben álló fél és más jóváhagyott célközönség) akaratának, megértésének és képességének befolyásolása. Mindez az ember kognitív képességeire hatva közvetlenül, illetve technikai képességeket felhasználva közvetve valósul meg.

Szembetűnő ugyanakkor, hogy a NATO-doktrínában az információs műveletek célkitűzései nincsenek egyértelműen megfogalmazva, és az információs fölény kivívására és megtartására irányuló törekvés markánsan nem fogalmazódik meg. E fölényképesség mint célkitűzés egyértelműen háttérbe szorul, szemben az USA ekkor érvényben lévő doktrínájával, ahol ez kiemelt helyet és szerepet kapott. (Haig 2011) Ez már jól mutatja azt a paradigmaváltást, ami a hadviselés és a műveleti környezet megváltozásának következménye. Míg a klasszikus háborús konfliktusokban az ellenséggel szembeni információs fölényre való törekvés releváns célkitűzés lehet, addig a polgári szereplőket is magában foglaló műveleti környezetben a lakosság és más szereplőkkel szemben nem ez az alapvető cél, hanem azok viselkedésének, gondolkodásának formálása, saját céljaink elfogadtatása. Ez pedig már egyértelműen fellelhető volt a NATO első információs műveletek doktrínájában is.

2015-ben a NATO megújította az AJP 3.10 doktrínáját, amelyben pontosította az információs műveletekkel kapcsolatos hat évvel korábbi nézeteit és felfogását. (AJP-3.10 2015) A megújított doktrína kiemeli, hogy az új globális biztonsági környezetben az állam-állam elleni konfliktusok háttérbe szorulnak, helyettük viszont a nem konvencionális műveletek, az aszimmetrikus hadviselési módok kerülnek előtérbe. Ez a műveletekben részt vevők körének változásával is együtt jár, és a nem állami szereplők jelentősége felértékelődik. Emellett az információs forradalomnak köszönhetően az internet, a mobiltechnológia és a közösségi média olyan új lehetőségeket nyitott meg az informá-

cióhoz való hozzáférésben, az információmegosztásban, a kapcsolattartásban és a döntések meghozatalában, amelyeket a műveletekben részt vevő szereplők egyaránt igyekeznek kihasználni.

Ebből kiindulva a doktrína az információs környezetet két alapvető szempont szerint értelmezi. Az első szempont szerint az információs környezetet a fizikai, a virtuális és a kognitív tartományok alkotják. A második szempont az információs környezet egyes elemei vagy rétegei közötti kölcsönös kapcsolatra fókuszál. Ez a felosztás részletezettebb az előbbinél, mivel az egyes tartományokat további rétegekre bontja. Eszerint az információs környezet rétegei közé sorolja:

- a valós világot és az abban zajló eseményeket;
- az információcserét biztosító hálózati kapcsolatokat;
- az információt;
- a személyiséget, ideértve azokat az interfészeszközöket, okostelefonokat, tableteket, laptopokat stb., amelyek az információt kezelik;
- az embereket, egyéni szereplőket és
- a társadalmi csoportokat, amelyek értelmezik az információt, és kihasználják az információs környezetet. (AJP-3.10 2015)

Az első szempont szerinti felosztás többnyire megfelel a korábban alkalmazott és a 3.1. alfejezetben is bemutatott felosztásnak. Fontos változás azonban, hogy a korábban használt *információs tartomány* vagy *dimenzió* helyett a *virtuális* jelzőt alkalmazza a doktrína, ami mindenképpen a kibertér megjelenésére utal, és annak jelentőségét támasztja alá. A második szempont szerinti felosztásban pedig az előző tartományokat tovább bontva mutatja be az információs környezetet. A fizikai tartományhoz sorolja a valós világot és a hálózatokat, a virtuális tartomány lefedi az információs réteget, végül pedig a kognitív tartomány a személyiségeket, az embereket és az általuk létrehozott közösségi csoportokat tartalmazza. Ez utóbbi felosztás jól szemlélteti azt a nézetet, miszerint az információs környezetben keletkező, abban létrehozott információk végső soron a kognitív térben, az emberek és az általuk

kialakított csoportok, közösségek (hálók) szintjén fejtik ki hatásukat. A hálózatok-, az információ- és a személyiségrétegnek nevezett interfészkapcsolat pedig egyértelműen utal a rendkívüli mértékben terjedő infokommunikációs technológiákra és azok hálózatos alkalmazására a kibertérben.

A doktrína kihangsúlyozza a stratégiai kommunikáció és a média szerepét a katonai műveletekben, ami biztosítja, hogy a műveletek során előidézett hatások megfelelő módon és formában legyenek kommunikálva a közvélemény felé. Felismeri, hogy az elektronikus médiának, az internetnek és a közösségi hálózatoknak köszönhetően soha nem látott lehetőségek nyílnak meg a valós és hamis információk, álhírek terjesztése terén, aminek köszönhetően rendkívül gyorsan, széles tömegekhez juthatnak el ezek az információk. Mindez a korlátozás nélküli és szabályozatlan médiafelület pedig újfajta lehetőségeket biztosít mind a NATO, mind pedig a vele szemben álló felek, illetve a nem állami szereplők számára egyaránt. Ebben az információs műveletek és az e műveleteket tervező törzs kulcsfontosságú szerepet kap, mivel az információs környezet elemzése révén a műveleti parancsnok jobban megértheti, hogy miként lehet kihasználni ezeket a lehetőségeket és kezelni az e környezetben jelentkező kockázatokat.

A doktrína megfogalmazásában: „a) Az információs műveletek az információs tevékenységeket elemző, tervező, értékelő és integráló törzsfunkció, amelyet annak érdekében végeznek, hogy a kívánt hatást gyakoroljanak a szemben álló fél, a potenciális szemben álló fél és az NAC által jóváhagyott felek szándékára, helyzetmegértési folyamatára és képességeire, és ezáltal támogassa a Szövetség missziós célkitűzéseit. b) Az információs tevékenységek hatást gyakorolnak az információra és/vagy az információs rendszerekre. Azokat bármely szereplő végrehajthatja, és védelmi rendszabályokat is tartalmaznak.”[199] (AJP-3.10 2015, 1–5.) Mint látható, a definícióban a korábbihoz képest a lényeges változás az, hogy míg a korábbi meghatározás egy általános

[199] Fordította a szerző.

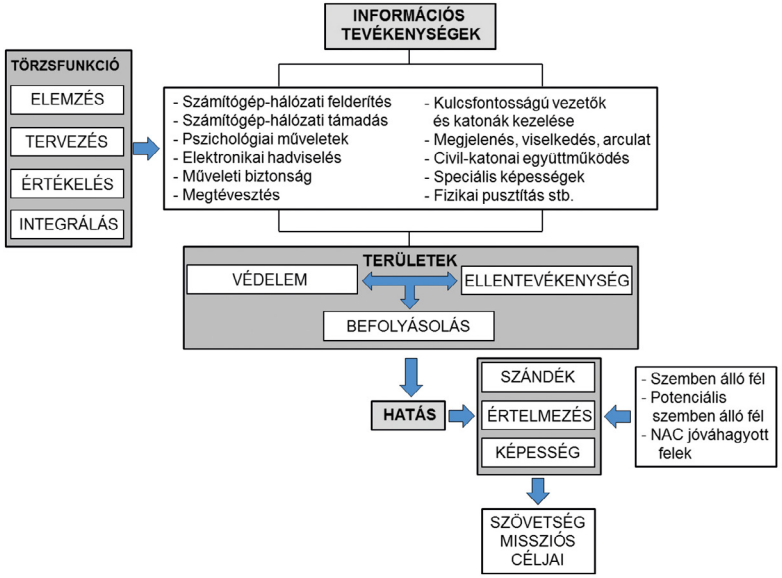
katonai funkciónak tekintette az információs műveleteket, addig az új doktrína egy törzsfunkciónak tekinti azt. Ez azért lényeges, mert ezáltal világosan kitűnik, hogy az információs műveletek egy olyan információs tevékenységeket integráló képesség, amelyben a legfőbb szerep a koordinációt végző törzsre hárul.

Az új doktrína is a műveletekben szereplők akaratára, helyzetértelmezésére és képességeire fókuszál, és az azokra gyakorolt hatásokban határozza meg az információs műveletek lényegét. Hasonlóan a korábbi doktrínához, az új is az információs műveletek három egymással kölcsönös kapcsolatban álló területét különbözteti meg. Ezek (17. ábra):

- az információs környezetben zajló saját információs tevékenységek megóvása;
- a NATO által meghatározott szereplők viselkedésének, értelmezési képességeinek és attitűdjének befolyásolása, megerősítése; illetve
- a szemben álló fél propagandájával szembeni tevékenység, valamint a vezetési és irányítási funkciója és képességei elleni tevékenység.

A doktrína a tételes és egzakt felsorolás helyett röviden ismerteti azokat a technikákat és képességeket, amelyek az információs műveletek alapját képezik. Kihangsúlyozza, hogy ezek nem jelentik az információs műveletekben alkalmazható tevékenységek teljes tárházát. A felsorolt képességek kis eltérésekkel megegyeznek a korábbi doktrínában foglaltakkal. Szembetűnő azonban, hogy a korábbi számítógép-hálózati műveletek helyett itt külön nevesíti a számítógép-hálózati felderítést (CNE)[200] és a számítógép-hálózati támadást (CNA),[201] a védelem területét viszont nem jeleníti meg. Megemlíti azonban a kibertéri műveleteket, de részletesebben nem fejti ki, hogy mit ért alatta, csupán a kiberteret határozza meg az információs környezet részeként. (AJP-3.10 2015)

[200] Computer Network Exploitation – CNE.
[201] Computer Network Attack – CNA.



17. ábra

A NATO információs műveletek értelmezése

Forrás: AJP-3.10 (2015), 1–6. alapján a szerző szerkesztése

Összességében látható, hogy a doktrína legfrissebb kiadása több területen megegyezik a korábbival. Az információs műveletek definíciója, fókuszpontja és területeinek meghatározása alapvetően nem változott, csupán törzsfunkciójellegének megjelenése jelenti a definícióban a lényegi változást. A 2015-ös doktrína hasonlóan a különféle információs képességek integrációjára és összehangolására helyezi a hangsúlyt, ugyanakkor nem adja meg az alkalmazható információs tevékenységek teljes körét. Helyette csak azokat ismerteti röviden, amelyek vélhetően a leginkább hozzájárulhatnak az információs műveletek célkitűzéseinek eléréséhez. Ebből pedig az is kiolvasható, hogy a doktrína a felsoroltakon kívül még számos nem nevesített információs képességgel is számol.

Lényeges változást jelent azonban a műveleti környezet változásának és a műveletekben részt vevő szereplők kibővülésének markáns kihangsúlyozása. Emellett a doktrína részletesebben értelmezi az információs környezetet, és kiemeli benne a hálózatos információs technológia, a mobil infokommunikációs eszközök, az internet és a közösségi média hatásának és szerepének felértékelődését. Ez pedig már jól láthatóan előrevetíti a kibertér megjelenését és beemelését a katonai műveletek dimenziói közé. Ez egy évvel később, 2016-ban formálisan is megtörtént, amikor a varsói NATO-csúcson a tagállamok állam- és kormányfői a kiberteret a szárazföld, a levegő, a tenger és az űr mellett az ötödik műveleti dimenzióként fogadták el, amelyben a NATO-nak a többi dimenzióhoz hasonlóan megfelelő műveleti képességekkel kell rendelkeznie.

3.5.3. Oroszország információs hadviselésének fejlődése

Oroszország információs műveletekkel összefüggő nézeteinek, kezdeti stratégiai koncepcióinak megszületése a kétezres évek elejére tehető. Természetesen az információs műveletek különféle információs tevékenységei, mint például a rádióelektronikai harc,[202] a lélektani hadviselés, a megtévesztés stb. már régóta részét képezték az orosz katonai eszköztárnak, és alkalmazták is azokat, azonban azok nem képeztek egy egységes, integrált rendszert. Az információs műveletek – orosz terminológiával az információs hadviselés, illetve információs konfrontáció – mint potenciális információs fenyegetés lehetőségét elsőként a 2000-ben megjelent információbiztonsági doktrínában fogalmazták meg hivatalosan. Ebben megállapítják, hogy az Orosz Föderáció információbiztonságát a már számos országban kifejlesztett információs hadviselési koncepcióból származó fenyegetések jelentik, amelyek célja, hogy az információs és távközlési rendszerek, információ-

[202] Az elektronikai hadviselés orosz terminológiája.

források normális működésének megzavarásával, valamint az azokhoz való jogosulatlan hozzáféréssel különféle hatásokat gyakoroljanak más országok információs szférájára. (RUSSIA INFOSEC DOCTRINE 2000)

A nyugati országokban, elsősorban az Egyesült Államokban az információs műveletek koncepciója ekkor már doktrinális alapokon nyugodott. Ezeket és a 90-es évek katonai műveleteiben, különösen az Öbölháborúban szerzett tapasztalatokat számos orosz katonai szakértő, például Vlagyimir Sz. Pirumov és Szergej P. Rasztorgujev is tanulmányozta. Roland Heickerö – hivatkozva Pirumov elemzésére – az alábbiakban foglalja össze a korai orosz információs hadviselés békeidős és háborús alkalmazásának lényegét:

- Békeidőben az információs hadviselés szoros kapcsolatban áll a társadalmi és a kormányzati szintű információbiztonsággal. Végrehajtása titokban történik, amelynek során különböző hírszerzési, politikai és pszichológiai műveleteket, valamint vírusokat és egyéb rosszindulatú szoftvereket felhasználó számítógép-hálózati műveleteket alkalmaznak.
- Háborús időszakban az információs hadviselés az ellenség feletti információs fölény kivívására és fenntartására, valamint az ország saját információinak és információs rendszereinek megvédésére irányul. Az információs hadviselés a hagyományos hadviselési módokat különféle információs és felderítőtevékenységekkel támogatja. Ezek közé tartozik például a katonai információs rendszerek pusztítása, az elektronikai ellentevékenység, a rosszindulatú programok alkalmazása, valamint az információ torzítása, meghamisítása és manipulálása a pszichológiai műveletek eszközeivel. (HEICKERÖ 2010)

Jól látható, hogy ez a megközelítés teljes mértékben illeszkedett az USA első információs műveletek doktrínájához, ami megnyilvánult az információs fölény kialakítására irányuló célkitűzésben, illetve az alkalmazható eszközökben és módszerekben is.

Timothy L. Thomas az orosz Rasztorgujev információs hadviselés formális elméletét bemutató tanulmányára (RASZTORGUJEV 2003) hivatkozva kifejti, hogy orosz nézetek szerint az információs hadviselés az információs szférában, kizárólag információs fegyverek használatával folytatott államok közötti harcként határozható meg. Az információs fegyverek hatásának célja egy adott információs rendszerről megfelelő ismeretek megszerzése, majd azok célorientált felhasználása annak érdekében, hogy torzítsa a másik fél valós világról alkotott képét. Információs fegyver lehet minden olyan technikai, biológiai vagy társadalmi eszköz vagy rendszer, amelyet adatok célzott előállítására, feldolgozására, továbbítására, megjelenítésére és/vagy az adatokkal kapcsolatos folyamatok akadályozására használhatnak. (THOMAS 2004)

Az orosz nézetek az információs hadviselést információs-technikai és információs-pszichológiai oldalról közelítik meg. Az információs-technikai oldal alapvetően az információs rendszerek technikai eszközökkel történő támadását vagy védelmét jelenti a rádióelektronikai harc és a számítógép-hálózati hadviselés módszereivel. Az információs-technikai konfrontáció eszközei és eljárásai közé sorolják a technikai hírszerzés eszközeit, az információ védelmére szolgáló eszközöket és intézkedéseket, a mikrohullámú és az ultrahangfegyvereket, a rádióelektronikai ellentevékenységi (rádióelektronikai zavaró) eszközöket és módszereket, az elektromágneses impulzus fegyvereket, valamint a speciális szoftvereket és hardvereszközöket.

Az információs-pszichológiai oldal a szemben álló fél, a közvélemény és a tömegek gondolkodásának, viselkedésének, érzelmeinek a kognitív tartományban való befolyásolását, manipulálását, a döntéshozatali folyamatok akadályozását és végül a kedvező politikai hatások előidézését célozzák. Ennek érdekében már a 60-as években megkezdték az úgynevezett reflexív kontroll módszerének kifejlesztését, ami azt jelenti, hogy a célcsoport felé olyan célzott, megfelelően előkészített információkat juttatnak el, amelyek arra ösztönzik őket, hogy saját akaratukból az információt közlő érdekeinek megfelelően cselekedjenek. Az információs-pszichológiai eszköztárba tartoznak a lélektani had-

viselés módszerei, a tömegtájékoztatási eszközök, a nem halálos fegyverek, a pszichotronikai eszközök és a különféle speciális gyógyszerészeti eszközök is. (THOMAS 2004)

Az elmúlt években az orosz információs hadviselés elmélete továbbfejlődött. A korai koncepciókból is kitűnt, hogy a technikai képességek mellett hasonló súllyal számoltak a különböző kognitív képességek alkalmazásával. Mindez talán részben betudható a nyugati országokhoz, különösen az Egyesült Államokhoz viszonyított akkori technikai lemaradásnak is.[203] A kétezres évek elején még az elektronikai rendszerek támadása és védelme, illetve a számítógép-hálózatok működésének korlátozása és védelme terén kevésbé voltak felkészülve, ezért olyan területeken keresték a kitörési pontokat, ahol jó eséllyel kelhettek versenyre a nyugati országok információs képességeivel. Ennek megfelelően korábban ismerték fel, és tulajdonítottak nagyobb jelentőséget az emberek befolyásolásában rejlő lehetőségeknek. Emiatt nagy energiákat mozgattak meg e terület kutatására és fejlesztésére, illetve a pszichológiai hadviselés hatásainak vizsgálatára.

2013-ban Geraszimov vezérezredes, orosz vezérkari főnök egy tanulmányában kifejtette, hogy az információs tér tág lehetőségeket teremt az aszimmetrikus képességeknek, amelyekkel jelentősen lehet korlátozni az ellenség harci potenciálját. A korszerű, új információs technológiák lehetővé teszik, hogy a műveletekben részt vevő erők és a vezető szervek közötti térbeli, időbeli elszigeteltség és az információs hiány jelentősen csökkenjen. Emiatt szükségesnek látja az információs térben zajló tevékenységek tökéletesítését, beleértve a saját információs objektumok védelmét is. (GERASIMOV 2016) Ez már összhangban van az előzőekben jelzett információs tevékenység koncepciójával, amelyben fellelhető az orosz információs konfrontáció ket-

[203] Mára ez már nem annyira egyértelmű, elég csak megvizsgálni az orosz elektronikai hadviselési eszközök új generációit és a kiberbiztonság területén működő neves orosz cégeket, mint például a Kaspersky Labet.

tőssége és egymást kiegészítő jellege, vagyis az információs-technikai és az információs-pszichológiai képességek érvényesülése.

A vezérkari főnök által megfogalmazott gondolatok jól illeszkednek az Orosz Föderáció fegyveres erőinek információs tevékenységi koncepciójához, amely az információs hadviselést az információs térben zajló államok közötti konfrontációnak tekinti. A stratégiai koncepció definíciója szerint: „Az információs hadviselés az információs térben lévő két vagy több állam közötti konfrontáció, amelyet azzal a céllal folytatnak, hogy károkat okozzanak az információs rendszerekben, folyamatokban és erőforrásokban, kritikus és egyéb struktúrákban, aláássák a politikai, gazdasági és társadalmi rendszereket, a lakosság tömeges pszichológiai manipulációjával destabilizálják az államot és a társadalmat, valamint hogy arra kényszerítsék az államot, hogy a szemben álló fél számára kedvező döntéseket hozzon."[204] (Russian InfoSpace Activities 2012) Az információs konfrontáció elmélete jól szemlélteti az orosz koncepció lényegét: az információs térben való folyamatos szembenállást, a szemben álló felek folyamatos egymásra hatását.

A koncepció az információs térben folytatott tevékenységek alapelveiként az alábbiakat emeli ki:

- *jogszerűség:* a nemzeti szuverenitás tiszteletben tartása és más államok belügyeibe való be nem avatkozás;
- *prioritás:* az információs térben jelentkező fenyegetésekkel kapcsolatos információk gyűjtése, az információforrások védelme;
- *komplexitás:* az információs térben folyó tevékenység egy egységes, komplex rendszert képez, amelyben a különböző információs tevékenységeket (például felderítést, rádióelektronikai harcot, műveleti megtévesztést, saját információs képességek védelmét stb.) egymással integrálva kell végrehajtani;
- *interakció:* a védelmi tevékenységek koordinálása más szövetségi végrehajtó testületekkel;

[204] Fordította a szerző.

- *együttműködés:* információs és technológiai fenyegetések felderítése és a megelőzés érdekében globális szintű együttműködés kialakítása;
- *innováció:* szakképzett személyi állomány toborzása, illetve az információs térben alkalmazható korszerű eszközök hazai kifejlesztése és gyártása. (Russian InfoSpace Activities 2012)

A fenti alapelvek formailag megfelelnek egy stratégiai dokumentum elvárásainak és a nemzetközi közösség normáinak. Ugyanakkor azt láthattuk, hogy az elmúlt években ezen alapelvek közül néhány a gyakorlatban nem érvényesült. Elég csak a jogszerűség elvére gondolni, amely a be nem avatkozás politikáját fogalmazza meg. Ezzel szemben azonban például az ukrajnai konfliktusban, a Krím félsziget annektálásakor vagy az amerikai elnökválasztási kampány feltételezett manipulálásakor ez az alapelv éppen ellentétesen jelentkezett. Többek között eme ellentmondást is vizsgálta Uku Arold, aki az orosz információs hadviseléssel foglalkozó tudományos publikációkat is felhasználva az alábbi alapelveket fogalmazza meg:

- *aszimmetria:* az információs képességek védelme mindig egy lépéssel követi a támadóképességeket;
- *dominancia:* a fölény megszerzése érdekében a médiafelületek és a véleményformálók számának növelése, hálózati túlterheléses támadások és elektronikai zavarás alkalmazása a másik fél hivatalos információs csatornái és a vele szimpatizáló média ellen, a szemben álló felek hitelességének megkérdőjelezése, karaktergyilkosság alkalmazása, az érzelmekre ható információkkal tömeges belső konfliktusok előidézése;
- *rejtettség:* információközvetítők (proxy) alkalmazásával a hamis információt terjesztő elrejtése a hitelesség fenntartása érdekében, a hivatalos szóvivők és politikusok számára referenciaként szolgáló feláldozható források alkalmazása, információ terjesztése trollok segítségével;

- *meglepés:* félrevezetéssel a kezdeményezés megszerzése, gazdasági, diplomáciai, információs és jogi befolyásolási módszerek gyakori váltogatásával a figyelem elterelése, hamis remények keltése;
- *erőegyensúly alakítása:* többpólusú globális biztonsági rendszer kialakítása, amelyben Oroszország a manipulációs képességeinek köszönhetően a „nemzetközi ügyek intézőjévé" válhat, globálisan hozzáférhető információs intézmények létrehozása és megerősítése;
- *nemzetközi szabályzók hiánya:* napjaink konfliktusaiban a háború és a béke, illetve a szemben álló felek megkülönböztethetetlensége, az információs konfrontációs szakemberek bátorítása a kreatív, jogi határokat megsértő tevékenységek folytatására;
- *hosszú távú hatás:* az orosz jogi és biztonsági körökben az információs konfrontáció eszközei és rendszabályai tömegpusztító fegyvernek számítanak, az információs konfrontáció eszközeivel lehetőség nyílik a „megfagyott" konfliktusok szinten tartására, esetleges újjáélesztésére;
- *szövetségesek és szemben álló felek kombinálása:* az oszd meg és uralkodj elvének érvényesítése, a megosztottság és nemzeti sebezhetőségek kihasználása a szövetségesek megzavarása céljából. (Arold 2016)

Tekintettel Oroszország elmúlt években játszott nemzetközi szerepvállalásaira, illetve a különböző konfliktusokban való részvételére, ezek az elvek vélhetően közelebb állnak a valósághoz. A 2008-as grúziai háborúban már tanúi lehettünk az orosz információs hadviselés kezdeti lépéseinek, amikor is az orosz erők – hazafias hackercsoportok által megtámogatva – a hagyományos háborús cselekményekkel párhuzamosan információs kampányt és támadásokat is folytattak. Az információs kampány célkitűzései a grúz erők műveletei hitelességének és Miheil Szaakasvili grúz elnök szavahihetőségének megkérdőjelezése, a Dél-Oszétiába bevonuló orosz erők legitimálása, a grúz

kommunikációs csatornák elvágása és a kormányzati internetes tartalmak elérhetetlenné tétele voltak. (Rózsa 2016) E támadások során a hagyományos háború keretei között a hírszerzés, felderítés, elektronikai zavarás mellett elsőként indítottak támadást a kibertérben a grúz parlament, a külügyminisztérium, a hadügyminisztérium és az elnök saját weboldalai ellen. Ezek a weboldalak a túlterheléses támadások következtében elérhetetlenné váltak, illetve az oldalak tartalmát átírták, a grúz elnök portréját átrajzolták. Emellett pedig félrevezető és az ország lejáratására alkalmas dezinformációs weboldalakat is létrehoztak. (Vámosi–Szedlák 2008)

Rózsa Tibor elemzésében rámutat, hogy a média felhasználása az orosz érdekek érvényesítésében kiemelt szerepet játszik. A Baltikumban, Ukrajnában és Moldovában számos olyan orosz sajtóorgánum található, amelyek alkalmasak arra, hogy vallási és kulturális üzenetekkel formálják az orosz nemzetiségű lakosság véleményét. A helyi és regionális médiafelületek mellett az utóbbi években több olyan tv-csatorna is megjelent, amelyek alkalmasak a nemzetközi közvélemény alakítására. Ezek közül is az egyik legjelentősebb az angol nyelvű *Russia Today,* amely már a grúziai konfliktusban is szerepet kapott az események orosz félnek kedvező interpretálásában. (Rózsa 2016) A 2014-ben kezdődött ukrajnai konfliktusban Oroszország például e tv-csatornát is felhasználva, a korábbiakhoz képest még intenzívebb médiakampányt indított az ukrán helyzet orosz értelmezésének alátámasztására, illetve a nyugati média ellensúlyozása és a közvélemény befolyásolása érdekében.

Az ukrajnai konfliktusban a hagyományos médiát felhasználó információs kampány mellett mindkét fél részéről megfigyelhetők voltak a kibertérben zajló információs tevékenységek is. Ezek közé sorolható például az ukrán távközlési szolgáltatás elleni fizikai és információs támadások, az ukrán elektromos hálózat elleni kibertámadás vagy a kormányzati weboldalak elleni túlterheléses támadások. (Fekete 2015) Ugyanakkor orosz oldalon felismerték a médiában mint információs „puha fegyverben” rejlő lehetőségeket, miszerint

az elektronikus média és különösen az internetes hírportálok, illetve a közösségi média kiváló lehetőségeket nyújtanak mind a valós, mind a hamis információk terjesztésében.

A politikai célú hamis információk és álhírek terjesztésében rejlő potenciált pedig azóta is többször kihasználták. Elég csak napjainkban az információhoz való hozzáférés nagy problémáját, az álhírek terjedését említeni, amelyeket a közvélekedés egyértelműen Oroszországhoz köt. Mindezt alátámasztja például a médiában szinte már tényként közölt amerikai, német és francia elnökválasztási kampányba való beavatkozás, amelyet természetesen orosz részről tagadnak. Ugyanakkor egyre több vizsgálati eredmény és jelentés lát napvilágot, amely az amerikai választási kampányba való orosz beavatkozás tényét támasztja alá. Legutóbb a CIA,[205] az FBI[206] és az NSA[207] közös jelentése került nyilvánosságra, amely egyértelműen kijelenti, hogy a 2016-os amerikai elnökválasztás elleni információs kampányt Vlagyimir Putyin rendelte el, és Oroszország áll mögötte. (ICA Report 2017)

Az Egyesült Államok Szenátusának egy bizottsági meghallgatására készült 2015-ös jelentésben (Clapper 2015) James Clapper, nemzeti hírszerzési igazgató kijelentette, hogy az orosz fegyveres erők kötelékében egy számítógép-hálózati műveletek végrehajtására alkalmas speciális egységet hoznak létre. Emellett orosz kibertéri szereplők az ipari vezérlőrendszerek ellen alkalmazható olyan eszközöket fejlesztenek ki, amelyek alkalmasak arra, hogy távolról elérjék, és megtámadják velük az elektromos hálózatot, a városi tömegközlekedést irányítórendszereket, a repülésirányítást, illetve az olaj- és gázelosztó hálózatokat, e képességekkel pedig jelentős károkat tudnak előidézni a kibertérben.

Láthatóan Oroszország információs hadviselési elvei az elmúlt években hatalmasat változtak. A kezdeti nyugati elvek átvételére épülő

[205] Central Intelligence Agency – CIA.
[206] Federal Bureau of Investigation – FBI.
[207] National Security Agency – NSA.

gondolkodásmód mára egy teljesen önálló, saját arculattal rendelkező információs hadviselési koncepcióvá alakult. A korai nyugati hatású, technológiaorientált megközelítés az ország viszonylagos technikai lemaradása miatt nem volt tartható. A különböző konfliktusok tapasztalatainak elemzése, az aszimmetrikus módszerek felismerése és a megtévesztés, valamint a lélektani műveletek terén szerzett tapasztalatok a technológiaközpontú információs hadviselési koncepciótól való eltéréshez vezettek. Nézeteik szerint az információstechnológia-orientált tevékenységek mellett egyenrangú szerepet kapnak a kognitív hatások előidézését célzó módszerek, így felfogásuk szerint az információstechnikai és az információs-pszichológiai tevékenységek képezik az információs hadviselés két azonos fontosságú oldalát.

Az információs teret, a nyugati országok nézeteit meghaladóan, a szárazföld, a levegő, a tengeri és az űr mellett egyenrangú műveleti tartományként értelmezik.[208] Ez azt is eredményezte, hogy míg a nyugati elméletek és doktrínák az információs műveleteket egyfajta támogató funkcióként definiálják, addig az orosz felfogás a hagyományos műveletekkel egyenrangú tevékenységként tekint az információs hadviselésre. Az utóbbi években megalkotott stratégiák is jól szemléltetik ezt a szemléletmódot, illetve az információs térben folyó folyamatos konfrontációként határozzák meg e tevékenységet, amely békében és háborús időszakban egyaránt zajlik, és amelynek legfőbb stratégiai célja a többpólusú világrend kialakítása.

Az utóbbi években a globális információs környezetben, benne a kibertérben megjelenő új típusú tömegtájékoztatási módszerek, az internetes hírportálok, blogok és a közösségi média jelentőségének felismerésével a kognitív befolyásolás egy új terepét fedezték fel. A stratégiai, politikai és katonai célok elérése érdekében ezért intenzíven használják és kihasználják ezeket az új médiafelületeket. Az ezeken keresztül közvetített, gyakran hamis információkkal, álhírekkel emberek tömegeit érik

[208] A 2016-os varsói csúcson a NATO is a műveletek ötödik dimenziójaként definiálta a kiberteret.

el, akiknek tudati tevékenységét, gondolkodását, érzelmeit, véleményét befolyásolják, manipulálják saját céljaiknak megfelelően.

Mindezek alapján kijelenthető, hogy mára Oroszország az információs hadviselési képességek terén fokozatosan ledolgozta lemaradását, utolérte a nyugati országokat és a NATO-t. Egyes területeken, különösen a kibertér kognitív befolyásolásra és manipulációra való felhasználása terén meg is előzte azokat, aminek köszönhetően napjainkban hatékonyan képes érvényesíteni az orosz érdekeket az információs térben.

3.5.4. Kína információs hadviselési felfogása

A 90-es évek végén a kínai információs hadviselési nézetek tulajdonképpen az akkor haladónak számító amerikai elvek átvételét jelentették. A Kínai Népi Felszabadító Hadsereg folyamatosan tanulmányozta az amerikaiak információs műveletekkel összefüggő nézeteit, doktrínáit, valamint a hálózatközpontú hadviselés elméletét. Emellett az Öbölháborúban és a balkáni konfliktusban alkalmazott információs tevékenységek tapasztalatainak feldolgozása is jelentősen hozzájárult Kína kezdeti információs hadviselési elméleteinek kialakulásához.

1998-ban, a jövő hadviselésével kapcsolatos kínai nézeteket összefoglaló tanulmánykötetben Wang Pufeng vezérőrnagy hosszasan elemzi az akkor kialakuló információs hadviselés jelentőségét és a hadviselés alakulására gyakorolt hatását. A tábornok kijelentette: „[A] közeljövőben az információs hadviselés fogja meghatározni a háború jellegét és kimenetelét. Mi felismertük az információs hadviselés e fejlődési irányát, és látjuk, hogy ez lesz a kínai katonai és harci készség modernizálásának hajtóereje. Ez a fejlődési irány különösen kritikus lesz a jövőbeli háborúkban a győzelem kivívásához.” (Pufeng 1998, 318.)

Az információhoz való hozzáférés akadályozása, a stratégiai megtévesztés, a pszichológiai befolyásolás és a manipuláció már régóta szerves részét képezi a kínai katonai doktrínáknak, ezért az információs

hadviselést mint e képességek és a kibertéri technikák összehangolt alkalmazását Kína egyre inkább preferálja. Az információs hadviselést egyfajta aszimmetrikus képességnek tekintik, amely lehetővé teszi számukra a hagyományos harci technikai eszközökben való viszonylagos elmaradottságuk kompenzálását.

Az előbb hivatkozott tanulmánykötetben megjelent írásukban Wang Baocun és Li Fei, a pekingi Hadtudományi Akadémia munkatársai az információs hadviselést a csúcstechnológiás harctéren zajló harci műveletként írják le, amelyben mindkét fél az információ megszerzése, kontrollálása és felhasználása terén folytatott versengésben kihasználja a saját információtechnológiai képességeit, eszközeit és rendszereit. E rendszereket az információ gyűjtésére és annak megakadályozására, az információforrások elnyomására és azok védelmére, megtévesztésre és ellenmegtévesztésre, illetve az információs célpontok pusztítására és azok védelemére alkalmazzák. Az akkori amerikai nézetekhez hasonlóan támadó és védelmi területet különböztettek meg, amelyek során a megtévesztés, a műveleti biztonság, a pszichológiai műveletek, a fizikai pusztítás és az elektronikai hadviselés mint öt fő alkotóelem alkalmazható. (Baocun–Fei 1998) Láthatóan a korai kínai nézetek az USA-doktrínák átvételén alapultak, és azokhoz hasonlóan elsősorban a technológiaközpontú megközelítést alkalmazták.

Dai Qingmin vezérőrnagy, a vezérkar információs hadviselésért felelős igazgatója az információs hadviselést mint alapvető harctéri képességet az információs környezetben zajló műveletek sorozataként definiálja, amelyeknek alapvető formája a katonai információs rendszerek mint közvetlen műveleti célpontok ellen irányuló elektronikai hadviselés és a számítógép-hálózati hadviselés. (Anand 2006) E műveletek során az alábbi tevékenységekre fókuszálnak:

- az ellenség információinak vagy információs rendszereinek megzavarása vagy szabotálása;
- az ellenség információs harci képességének gyengítése;
- az ellenség összezavarásával kedvező feltételek kialakítása a saját erők számára;

- az ellenség felderítési lehetőségeinek korlátozása és a saját lehetőségek erősítése;
- az ellenség hamis információkkal való félrevezetése;
- hamis helyzetértelmezés kialakítása és meglepő információs támadások végrehajtása;
- az ellenség meggyőzése arról, hogy ami valós, az hamis, és fordítva, valamint
- az ellenség döntéshozóinak összezavarása.

Az elektronikai hadviselés és a számítógép-hálózati hadviselés fontosságát jól mutatja, hogy e két tevékenység együttes alkalmazása az úgynevezett „integrált hálózatos elektronikai hadviselés" koncepciójában jelenik meg. E koncepció szerint az elektronikai hadviselés és a számítógép-hálózati hadviselés integrált harctéri alkalmazása arra irányul, hogy megzavarja az ellenség harctéri hálózatos információs rendszereinek normál működését, és megvédje a sajátját. Az integrált hálózatos elektronikai hadviselés célja az információs dimenzióban a harctéri információs fölény kivívása. Az információs dimenziót[209] az elektromágneses tér, a számítógépes hálózati tér és a döntéshozók kognitív tartománya alkotja, amelyre két formában, az információs rendszerek elleni támadással és a kognitív tevékenységekkel lehet hatással lenni. A kínai álláspont szerint az információs fölényt az alábbiak jellemzik:

- egy olyan integrált harci állapot, amely nagyban befolyásolhatja a háború teljes kimenetelét;
- lehetővé teszi az információs dimenzióban való manőverszabadságot, és
- az információs dimenzióban zajló események révén hatással van a fizikai dimenzióban zajló tevékenységekre. (Thomas 2004)

[209] Az információs dimenzió kínai megközelítése elnevezésében nem egyezik meg a 3.1. alfejezetben bemutatott információs környezet és dimenzióinak értelmezésével.

Láthatóan a 2000-es évek elején a kínai információs hadviselési koncepciókban az elektronikai hadviselés és a számítógép-hálózati hadviselés kiemelt jelentőséggel bírt. Ez jól szemlélteti azt az alapvetően technikai megközelítést, amely részben az amerikai információs műveleti elméletek átvételéből származik. Mindezek mellett pedig e koncepcióra vélhetően hatással volt a szintén ebben az időben kialakuló hálózatközpontú hadviselési modell is, amely a hadviselés, illetve a vezetés és irányítás egy gyökeresen új módszerét képviselte.

A kínai haderőben a számítógép-hálózati támadási képességekre ma egy erősen fejlesztendő területként tekintenek, mivel meglátásuk szerint ezek a támadások hosszabb érvényességűek lehetnek, mint a hagyományos eszközök által előidézett hatások, és emellett alkalmazója is rejtve maradhat. Ezért a számítógép-hálózati támadás egy relatíve gyengébb haderő számára az egyik leghatékonyabb eszköz, hogy harcot folytasson egy erősebbel szemben. Meglátásuk szerint az ilyen típusú támadással kényszeríteni lehet az ellenséget, hogy harc nélkül adja fel céljait.

Ez a felfogás megjelent Kína 2015 májusában kiadott Nemzeti Katonai Stratégiájában is, amely kijelenti, hogy a hadügyi forradalom mára egy teljesen új szakaszba lépett. Napjainkban a nemzetközi stratégiai kihívások a kibertérben is egyre erőteljesebben jelentkeznek, ezért egyre több ország fejleszt ki kibertérben alkalmazható katonai képességet. Mivel a kibertér a katonai biztonság terén is fokozott súllyal van jelen, ezért Kína felgyorsítja egy kibertéri erő kifejlesztését, növeli a kibertéri helyzettudatosságát és a kibervédelmét, támogatja a nemzetközi kibertéri együttműködésben való részvételét, biztosítja a nemzeti hálózat- és információbiztonságot, valamint a nemzeti biztonság és a társadalmi stabilitás fenntartását. (Kanwal 2017)

Kína az elmúlt években számos alkalommal tesztelte kibertámadási képességét, bár ezt folyamatosan tagadta. Ezeket a támadásokat különböző hackercsoportok követték el, és zömében az Egyesült Államok ellen irányultak. Az amerikai kiberbiztonsági szervek 2000 óta számos kormányzati és vállalati rendszer elleni incidenst észleltek.

Ezek közé tartozott például az elhíresült Titan Rain fedőnevű támadássorozat, amely 2002-ben indult, és amelynek során kínai hackerek 10-20 terabájtnyi adatot töltöttek le a megtámadott számítógépekről. Az amerikai hatóságok 2005-ben is detektáltak kínai területről kiinduló támadásokat, amelyek több nagyvállalat és kutatóintézet, mint például a SANS Institute, a Lockheed Martin, a Sandia National Laboratories, a Redstone Arsenal és a NASA számítógép-hálózatait érintették. 2008 áprilisában pedig kínai hackerek összehangolt támadást indítottak a CNN hírtelevízió ellen, ami a csatorna weboldalainak lelassulásához vezetett. (Kovács 2009)

A kognitív térben zajló információs hadviseléssel kapcsolatban más haderőkhöz hasonlóan vélekednek. Meglátásuk szerint a lélektani műveletek célpontjai minden esetben az emberek, a döntéshozók, ezért fontosnak tartják a kognitív tartományban való befolyásolásukat, manipulálásukat annak érdekében, hogy megváltoztassák gondolataikat, vélekedésüket, viselkedésüket és érzelmeiket. E műveletek célcsoportjába mind a katonai erő, mind pedig a polgári lakosság beletartozik. Az alkalmazható eszközök és módszerek közé sorolják a katonai erőfeszítések támogatása érdekében a média manipulálását, a propagandatevékenység hagyományos módszereit, mint például a szórólapokat, a rádió- és tv-műsorok terjesztését és egyéb, e célra felhasználható kommunikációs eszközöket. Az információs hadviselés többi eleméhez hasonlóan a pszichológiai műveleteket békeidőben, válság idején és háborúban egyaránt alkalmazhatónak tartják. (Anand 2006)

A kibertéri képességek technológiai fejlesztése mellett tehát – hasonlóan a nyugati elméletekhez – a kognitív tér befolyásolása is megjelenik a kínai információs hadviselési elméletekben. A kínai értelmezés az információs dimenzió részének tekinti a kognitív tartományt. Ez eltér a nyugati felfogástól, ami az információs környezetben mint egy átfogó információs térben határozza meg az információs műveletek fizikai, információs és kognitív dimenzióját. Meglátásuk szerint – bár a kibertérben alkalmazott hálózatos információs technológiai képességek és tevékenységek ma az egyik legjelentősebb fejlesz-

tendő terület – a kognitív tartományban elért hatások is jelentősen befolyásolhatják a műveletek kimenetelét. Ez a gondolkodásmód erősen kötődik Szun Ce tanításaihoz, amelyekben az ellenség harc nélküli legyőzésének fortélyait, különösen a megtévesztés és nem utolsósorban a parancsnok kognitív képességeire való ráhatását mutatta be.

Összegzésként megállapítható, hogy Kína információs hadviselési elgondolása többnyire illeszkedik a világ vezető országainak nézeteihez. Az információs hadviselés műveleti környezetét hasonlóan közelíti meg, bár az *információs környezet* helyett az *információs dimenzió* kategóriáját használja, amelynek részeként értelmezi a kognitív tartományt. Ez azonban pusztán csak terminológiai eltérést jelent. Megfigyelhető azonban, hogy az információs fölény kivívását az információs hadviselés alapvető célkitűzésének tekinti, szemben a mai nyugati nézetekkel, amelyek csak a hagyományos konfliktusok esetén, az ellenséggel szemben tekintik ezt elérendő célnak. A hibrid hadviselés körülményei között pedig, inkább a célközönség befolyásolására helyeződik a hangsúly. A kínai koncepcióból azonban ez nem olvasható ki ilyen hangsúllyal, vélhetően azért, mert Kína részvétele napjaink ilyen jellegű konfliktusaiban más nyugati országokéhoz képest kisebb arányú.

Fontos kiemelni, hogy a kínai koncepció külön kihangsúlyozza a hálózatos információs technológiai képességek szerepét az információs fölény elérésében. Az integrált hálózatos elektronikai hadviselési képességek, benne a számítógép-hálózati hadviselés és az elektronikai hadviselés összehangolt, integrált alkalmazása a kibertérben folytatott eredményes tevékenység zálogaként jelenik meg. Ez összhangban van azzal a tendenciával, amely megfigyelhető a mai kibertéri tevékenységekkel kapcsolatban, miszerint – köszönhetően a vezeték nélküli technológiák rohamos elterjedésének – a kibertér és az elektromágneses spektrum egyre inkább átfedésbe kerül egymással. Mindez jelentős azonosságot mutat az USA FM 3-12 *Kibertéri és elektronikai*

hadviselési műveletek doktrínájával,[210] amely szintén e két terület egyre inkább egymásba olvadását prognosztizálja.

Emellett a kínai koncepció is fontos szerepet tulajdonít a kognitív tartomány befolyásolásának. E tekintetben hasonló megközelítést alkalmaznak, mint az USA és a NATO. E tevékenységeket béke és háborús konfliktusok során egyaránt alkalmazhatónak vélik. A kibertér befolyásolási célú felhasználása vélhetően a kínai gondolkodásban is felmerül, de olyan markánsan nem jelenik meg, mint ahogy például az orosz információs konfrontációs stratégiában. Ehelyett a hagyományos pszichológiai műveleti eszközöket és eljárásokat nevesítik, illetve fontos lehetőségeket látnak a döntéshozók félrevezetésében is.

3.5.5. Az információs műveletek hazai megközelítése

Az információs műveletek 2002-ben, a Magyar Honvédség (MH) Összhaderőnemi Doktrína első kiadásában jelentek meg először egy önálló fejezetként. (MH ÖHD 2002) Elemezve a doktrínafejezetben foglaltakat, megállapítható, hogy az információs műveletek meghatározásában és tartalmában is alapvetően megegyezett az 1998-as első amerikai JP 3-13 doktrínában foglaltakkal. A doktrína támadó és védelmi információs műveleteket különböztetett meg, amelyek során a katonai és a nem-katonai tevékenységek összehangolt alkalmazása az információs fölény és a vezetési és irányítási fölény kivívásával a hadműveleti előny elérését célozza.

A doktrínában a terület kiforratlanságát mutatja, hogy az információs műveletek mellett foglalkozik a vezetési és irányítási hadviselés kérdésével is, amelynek szintén támadó és védelmi fajtáját különbözteti meg. Ugyanakkor nem mutatja be, hogy milyen összefüggés van e két terület között. Ettől eltekintve, a doktrínában az információs műveletek mint az egyik fontos műveleti támogatási fajta megjelenése abban

[210] FM 3-12 Cyberspace and Electronic Warfare Operations Doctrine.

az időben igen előremutató volt, mivel akkor még az amerikai haderőn kívül más szövetségi ország és a NATO sem rendelkezett információs műveletekre vonatkozó doktrínával.

A doktrína 2007-ben átdolgozott 2. kiadása a korábbinál bővebb tartalommal foglalkozik e kérdéssel. (ÁLT/27 2007) Ebben egy fejezet tárgyalja az információs műveletek fontosabb összefüggéseit, meghatározását és a fejezeten belül külön alfejezetekben jelennek meg az egyes információs képességek. Alapvetően az információs műveletek fogalma, értelmezése, célja, illetve a védelmi és támadó aspektusai megegyeznek a korábbi doktrínában találhatókkal. Mindemellett a doktrínában foglaltak többnyire összhangban vannak az információs műveletek általános elméleti összefüggéseivel, és több területen kapcsolódnak más haderők és részben a NATO doktrínáihoz. Új elemként jelenik meg benne az információbiztonság külön kihangsúlyozása. Emellett pedig szembetűnő, hogy a civil-katonai együttműködést és a tömegtájékoztatást nem az információs műveleteken belül, hanem önállóan értelmezi a doktrína.

A 2012-ben megjelent MH Összhaderőnemi Doktrína harmadik kiadása alapvetően más filozófia szerint épül fel, mint a korábbiak, és csak érintőlegesen tartalmazza a műveletek támogatásával összefüggő feladatokat. (ÁLT/43 2012), így az információs műveletek is csak egy bekezdés erejéig jelenik meg benne. Ebben azonban már érezhető az a megközelítés, amely a hadviselés és a műveleti környezet változásából fakad, és amelyet a NATO információs műveletek doktrínája is takart.

Az MH első információs műveletek doktrínája öt évvel a NATO hasonló kiadványa után, 2014-ben jelent meg. (ÁLT/57 2014) A doktrína kidolgozása során már megkezdődött a 2015-ben megjelent NATO doktrína 2. kiadásának kidolgozása is, így annak lényeges tartalmi elemeit már figyelembe vették a kidolgozók. Az MH kiadvány felvezetésként elemzi napjaink információs környezetét, az információ szerepét és jelentőségét, a média hatását, az információs technológiában rejlő veszélyeket, valamint a stratégiai kommunikáció fontosságát és kapcsolatát az információs műveletekkel. Az információs művele-

teket az alábbiak szerint definiálja: „a) Az INFOOPS az információs környezet elemzéséhez és a hatástervezéshez kapcsolódó törzsfunkció. Tervezi, koordinálja, majd értékeli az információs tevékenységeket, integrálja azokat a katonai műveletek sorába annak érdekében, hogy elérje a kívánt hatást a célközönség akaratában, megértésében és képességeiben a küldetés célkitűzéseinek teljesítéséhez. A célközönséget a szemben álló felek, a lehetséges szemben álló felek és más, a politikai szint által jóváhagyott személyek és meghatározott csoportok alkotják. b) Az információs tevékenységek azok az akciók/cselekmények, illetve bevezetett rendszabályok, melyek célja, hogy hatást gyakoroljanak az információra és/vagy az információs rendszerekre az információs környezetben, a kívánt változás elérése érdekében." (Ált/57 2014, 1–7.)

Az információs tevékenységeket szintén a NATO-elveknek megfelelően, az alábbi három fő területen határozza meg:

- a célközönség percepcióját, érzetét, viselkedését, befolyásoló információs tevékenységek;
- a saját erők, döntéshozók, döntési folyamatok, információk védelmét biztosító információs tevékenységek, valamint
- a vezetési képességek megbontására irányuló információs tevékenységek.

A doktrína kihangsúlyozza, hogy az információs műveletek célkitűzéseit az információra vagy információs rendszerekre hatást gyakorló katonai képességekkel, eszközökkel és azok előre tervezett koordinációjával és szinkronizálásával lehet elérni. Ezért a célkitűzések elérése érdekében a doktrína meghatározza az információs tevékenységekhez kapcsolódó alábbi képességeket:

- lélektani műveletek,
- megjelenés, viselkedés és arculat,
- műveleti biztonság,
- információbiztonság,
- megtévesztés,
- elektronikai hadviselés,

- fizikai megsemmisítés,
- kulcsbeosztású vezetőkkel való érintkezés,
- számítógépes hálózati műveletek, valamint
- civil-katonai együttműködés. (ÁLT/57 2014)

Mint látható, az információs műveletek definíciója, információs tevékenységei és képességei szorosan illeszkednek a NATO 2015-ös doktrínájának alapvető tartalmi elemeihez. A definíció fontos elemének tekinthető az információs műveletek törzsfunkciójellegének, elemző, tervező, koordináló és integráló funkciójának kihangsúlyozása, valamint a célközönség akaratára, helyzetmegértési folyamatára és képességeire való ráhatás szükségességének kiemelése. A műveleti környezet változásával összefüggésben lényeges a célközönség széles értelemben vett meghatározása, amelybe beletartoznak a tényleges és lehetséges szemben álló felek, valamint az egyéb jóváhagyott személyek és csoportok.

Az információs tevékenységek és képességek kategorizálása szinte megegyezik a NATO felfogásával. Ezeket elemezve megállapítható, hogy az MH információs műveletek értelmezése – összefüggésben a katonai műveletek és azok környezetének, illetve a szereplőknek a változásával – a kezdeti nézetekhez képest átalakult. Ezzel van összefüggésben, hogy a NATO-doktrínához hasonlóan hangsúlyozza az információs műveletek döntéshozókra gyakorolt befolyásoló hatását és a nem-kinetikus képességek fontosságát. Ugyanakkor néhány képesség vonatkozásában, mint például az információbiztonság és a műveleti biztonság esetén félreérthető és egymást részben vagy egészben átfedő módon vannak meghatározva az információs műveletek képességei.

Összességben látható, hogy az információs műveletek a 2000-es évek elejétől kezdve jelen vannak az MH műveleti gondolkodásában. Értelmezésére kezdetben az amerikai megközelítés volt jellemző, amely összecseng majd minden ország és haderő gondolkodásával. Felismerték és műveleti koncepcióvá emelték az információs műveleteket. Az elmúlt években azonban a kognitív dimenzió felértékelődése és a missziós szerepvállalásoknak köszönhetően fokozatosan átalakult

az információs műveletek megítélése. A 2010-es évektől pedig jelentősen érezhető a koncepció változása és a NATO-elveknek való megfelelés, amit jól tükröz az MH első információs műveletek doktrínája is.

3.6. Az információs műveleti koncepciók szintézise és átfogó értelmezése

3.6.1. Az információs műveletek fogalma

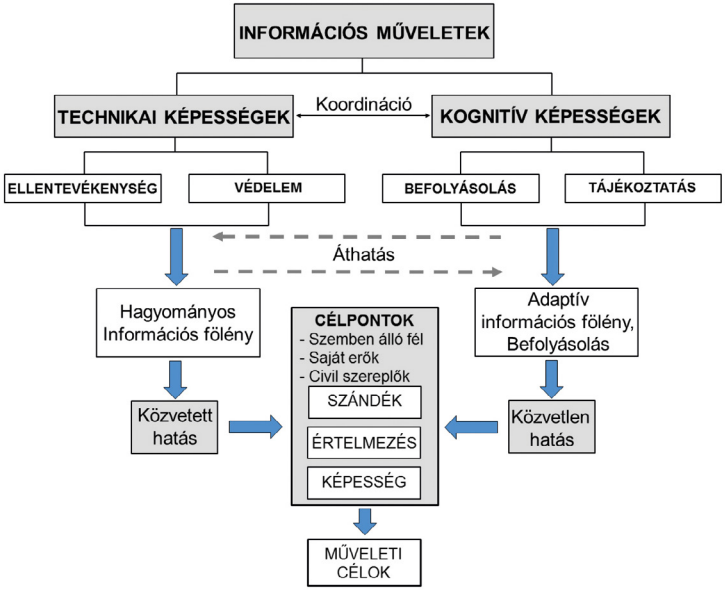
Az információs műveletek elmélete és gyakorlata az elmúlt több mint negyed század alatt jelentős fejlődésen ment keresztül. A 20. század közepétől fokozatosan meginduló, majd felgyorsuló információs forradalom következtében az évszázad végére az információs technológia a mindennapi élet meghatározójává, a társadalmi, gazdasági és hadügyi fejlődés alapvető mozgatórugójává vált. E technológia egyre szélesebb körű alkalmazása jelentős mértékben hozzájárult az információ szerepének és fontosságának erősödéséhez, ami kihatott a katonai műveletek átalakulására is.

A műveletek során a saját oldali információkezelési és döntési képességek kihasználása és védelme, illetve a szemben álló fél információs lehetőségeinek gyengítése egyre jelentősebb szerepet kapott. Ez pedig magával hozta egy új műveleti képesség, az információs műveletek kialakulását. Kezdetben az Egyesült Államok, majd utána egyre több ország, köztük Oroszország, Kína és hazánk, valamint a NATO is kialakította saját információs műveleti koncepcióját. Mindeközben a hadviselés is megváltozott, megjelent a negyedik generációs hadviselés, és a műveletekben részt vevők köre is kibővült és átalakult. Az információs műveletek fejlődését és a különböző országok nézeteit az előző alfejezetekben elemeztük. Ezek szintézise alapján az információs műveletek lényegét és napjaink műveleti környezetére is érvényes értelmezését az alábbiakban összegezhetjük.

A korábban ismertetett meghatározások elemzése és szintézise alapján az információs műveletek átfogó definíciója a következők szerint fogal-

mazható meg: *Az információs műveletek az információs környezetben érvényesülő információs képességek integrált, összehangolt és koordinált alkalmazására irányuló tevékenységek összessége, amelyek a műveletek célkitűzéseinek elérése érdekében, kognitív képességekkel közvetlenül, illetve technikai képességekkel közvetetten hatásokat gyakorolnak a műveletekben részt vevő célközönség szándékára, helyzetértelmezésére és képességeire.*

A fenti átfogó definíció értelmezi az információs műveletek műveleti tartományát, kihangsúlyozza integráló és koordináló funkcióját, meghatározza általános célkitűzését és elérésének két fő információs képességcsoportját, valamint a célközönségét. A definíció szerinti információs műveletek értelmezését a 18. ábra szemlélteti.



18. ábra

Az információs műveletek átfogó értelmezése

Forrás: a szerző szerkesztése

3.6.2. Az információs műveletek műveleti tartománya

Az információs műveletek az információs technológia fejlődésével és az információ katonai műveletekben játszott szerepének felértékelődésével kialakuló és az információs környezetben érvényesülő újfajta műveleti képesség. Az információs környezet a fizikai, az információs és a kognitív dimenziót magában foglaló információs műveleti tartomány, amelyben a különféle információkezelési és döntési folyamatok zajlanak, illetve az információs képességek megvalósulnak.

Az információs környezet korábbi, elsősorban technikai megközelítése napjainkra egyensúlyba került, és a kognitív térben a célközönséggel szembeni közvetlen információs hatások jelentősége felértékelődött. Emellett a hálózatos infokommunikációs technológia rohamos ütemű elterjedésének köszönhetően, e környezetnek a kibertér egyre fontosabb és jelentősebb tartományát adja, amely érinti az információs környezet mindhárom dimenzióját. A kibertérben jelentkező hatások ugyanis nemcsak a teljesen nyilvánvaló számítógép-hálózati környezetben érvényesülnek, hanem a kibertéri technológiák teljes spektrumában, köztük többek között a kiberfizikai rendszerekben, illetve az internetes média és a közösségi háló befolyásoló hatásának eredményeként az emberek és csoportok, közösségek kognitív képességeiben is. Ennek bővebb kifejtésére a következő fejezetben kerül sor.

3.6.3. Az információs műveletek célpontjai

Az információs műveletek célpontjai minden esetben a műveletek jellegétől függenek, de alapvetően az alábbi három nagy csoportba sorolhatók:

- a szemben álló fél,
- a saját erők, valamint
- a civil szereplők.

A klasszikus háborús katonai műveletekben az információs műveletek alapvető célcsoportja egyrészt a szemben álló fél, amely ellen alapvetően negatív hatású információs képességek alkalmazhatók, másrészt a saját erők, akiknek az irányába pozitív jellegű és védelmi célú információs műveletek alkalmazhatók. Emellett a célközönség közé tartozik az ellenséggel, illetve a saját erőkkel szimpatizáló lakosság, valamint a semleges érintettek is, akiket meg kell nyerni a saját katonai műveletek célkitűzéseinek elfogadására.

A napjainkra jellemző negyedik generációs katonai műveletekben, ahol gyakran nincs, illetve sokszor rejtve marad a nyilvánvaló ellenség, az elsődleges célcsoportot a civil szereplők jelentik. Az irányukba alkalmazható információs műveletek szempontjából célszerű megkülönböztetni:

- a katonai műveletben nem állami szereplőként, irreguláris erőként, gyakran fegyveres csoportként részt vevőket, valamint
- a műveleti területen élő lakosságot.

Az előbbiek ellen a negatív hatású információs képességek alkalmazása is elfogadható és gyakran célravezető. A lakossággal szemben azonban célszerű olyan információs műveleteket folytatni és ezen belül olyan pozitív megerősítő üzeneteket továbbítani, amelyekkel el lehet nyerni a bizalmukat, szimpátiájukat, és aminek eredményeként jó esély van arra, hogy elfogadják a műveletek céljait, és ne akadályozzák azok elérését.

3.6.4. Az információs műveletek célja

Az információs műveletek általános célja a katonai műveletek információs környezetben való támogatása. Ezt az általános célt a műveletek jellegétől, környezetétől, illetve célközönségétől függően az információs fölény és/vagy a befolyásoló hatások kialakításával lehet elérni. A hagyományos értelmezésű információs fölény a háborús konfliktusokban, alapvetően az ellenséggel szemben értelmezhető

információs műveleti célként. Ennek a lényege, hogy a saját információkezelési (gyűjtés, tárolás, feldolgozás, továbbítás) és döntési képességek az információs környezet mindhárom dimenziójában előnyösebb tulajdonságokkal bírnak, mint a szemben álló félé. A saját oldali helyzetértelmezést biztosító információk időszerűsége, pontossága és relevanciája jobb, mint a szemben álló félé.

Az információs fölény feltételezi, hogy a szemben álló fél rendelkezik megfelelő színvonalú információs infrastruktúrával, illetve infokommunikációs rendszerekkel. Ezeken keresztül pedig közvetve eredményesen korlátozhatók az információkezelési és döntési képességei. Emellett természetesen a kognitív befolyásolási technikák is alkalmazhatók az információs fölény eléréséhez. Ezekkel közvetlenül lehet negatív hatásokat elérni a célcsoport helyzetértelmezésében, szándékaiban és képességeiben, vagyis érvényesül a technikai és a kognitív képességek közötti áthatás.

A negyedik generációs katonai műveletekben az információs fölény klasszikus kialakításának modellje nem alkalmazható teljeskörűen, mivel a műveletekben a civil szereplők is jelentős súllyal vannak jelen. Velük szemben az adaptív információs fölény kialakítása lehet célravezető, amely esetben nem feltétlenül a saját oldali előnyösebb információkezelési és döntési képességeken van a hangsúly, hanem azon, hogy hogyan lehet a gondolataikat és vélekedésüket alakítani, meggyőzni őket vagy a viselkedésüket megváltoztatni. Ez esetben a közvetett információs technikai módszerek gyakran kevésbé alkalmazhatók. Többek között emiatt az adaptív információs fölény jobban kihangsúlyozza a célközönségre közvetlenül ható kognitív befolyásolóképességek szerepét. Ugyanakkor elégséges infokommunikációs feltételek megléte esetén a közvetett technikai módszerek is hozzájárulhatnak az adaptív információs fölény kialakításához. Ez esetben tehát itt is megfigyelhető a kognitív és a technikai képességek közötti áthatás.

Amennyiben e célközönség, illetve közülük is a véleményformálók rendelkeznek hálózatos infokommunikációs képességekkel, internetes hozzáféréssel, használják a közösségi médiát, akkor e köz-

vetlen befolyásoló hatás a kiberteret kihasználva ezeken a médiumokon keresztül nagyobb hatékonysággal érheti el őket. Mindezeket a hatásokat tovább fokozzák az internetes hírportálokon, illetve a közösségi médiában egyre terjedő álhírek, amelyek, mint ahogyan azt tapasztalhatjuk, jelentősen átformálhatják az egyének véleményét. Az álhírek alkalmazása társadalmi, politikai, katonai és marketingszempontból is igen kifizetődő a terjesztőjének, hatékonyságához pedig manapság nemigen fér kétség. Ebből fakadóan az álhírek terjedése a világhálón és benne a közösségi médiában egyelőre megállíthatatlan.

3.6.5. Az információs műveletek képességei

Az előző alfejezetben ismertetett célok elérése érdekében, a meghatározott célcsoportokkal szemben, az információs műveletekbe integrálva különféle egymással összehangolt és koordinált információs képességeket alkalmaznak. Ezek az információs képességek attól függően, hogy hatásukat az információs környezet mely dimenziójában fejtik ki, az alábbi két nagy csoportra oszthatók:

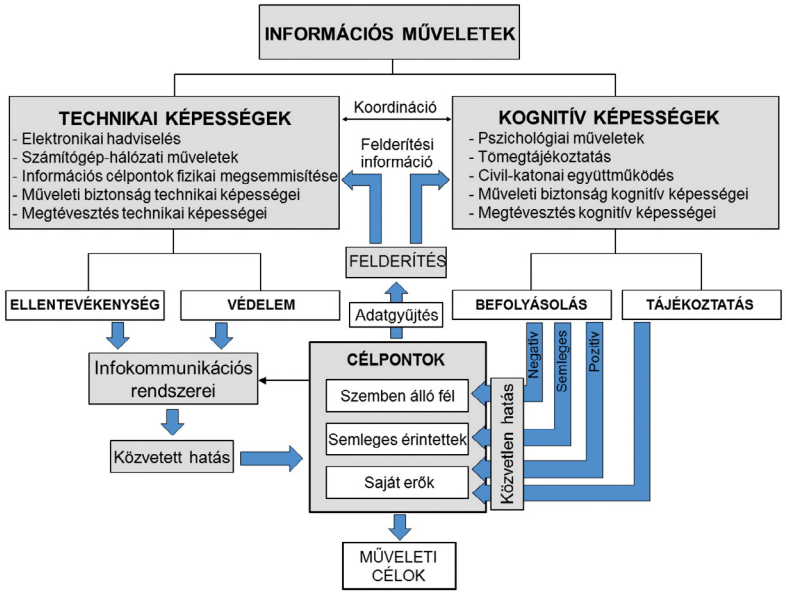
- technikai képességek, illetve
- kognitív képességek.

A technikai képességek az információkezelési folyamatokra, azaz az információgyűjtésre, -tárolásra, -feldolgozásra és -továbbításra fókuszálnak. E képességek alapvetően az infokommunikációs technológia felhasználásával közvetve, az infokommunikációs rendszereken keresztül gyakorolnak hatást a célközönségre. Ebből fakadóan a célpontjai minden esetben az infokommunikációs rendszerek, hálózatok és azok elemei. A technikai képességek tehát hatásukat az információs környezet fizikai és információs dimenziójában fejti ki. Céljukat tekintve lehetnek a szemben álló fél információs rendszerei elleni tevékenységek, illetve a saját információs rendszerek védelmére irányuló tevékenységek.

A kognitív képességek ezzel szemben az információ tartalmára fókuszálnak, amelynek során különféle közvetítőeszközöket és -módszereket felhasználva, előre megtervezett üzenetekkel, közvetlenül az emberek tudati tevékenységét veszik célba. Ennek megfelelően a kognitív képességek célpontja minden esetben az ember, tehát hatásuk az információs környezet kognitív dimenziójában érvényesül. Céljukat tekintve e képességek lehetnek pozitív, negatív és semleges befolyásoló, illetve tájékoztató jellegű tevékenységek. A pozitív befolyásolás a saját személyi állomány és a szimpatizáló civil közvélemény felé irányuló megerősítő üzenetek formájában valósul meg. A negatív befolyásolás a szemben álló fél és a nem állami szereplők, irreguláris erők, esetleg nem szimpatizáns civil csoportok irányában alkalmazott figyelmeztető, fenyegető, gyakran megtévesztő jellegű üzenetekkel fejti ki hatását, a semleges befolyásolás pedig a semleges érintettek felé továbbított, a műveleti célokat elfogadtató, megnyerő hatású üzenetekkel fejti ki hatását.

Ezek alapján az információs műveletek technikai és kognitív képességei közé az alábbiakat sorolhatjuk (19. ábra):

- technikai képességek:
  - elektronikai hadviselés,
  - számítógép-hálózati műveletek,
  - információs célpontok fizikai megsemmisítése,
  - műveleti biztonság technikai képességei,
  - megtévesztés technikai képességei,
- kognitív képességek:
  - pszichológiai műveletek,
  - tömegtájékoztatás,
  - civil-katonai együttműködés,
  - műveleti biztonság kognitív képességei,
  - megtévesztés kognitív képességei.



19. ábra

Az információs műveletek információs képességei és hatásuk

Forrás: a szerző szerkesztése

Láthatóan a műveleti biztonság és a megtévesztés mindkét információs képességcsoportban is megtalálható, mivel mindkettőnek vannak technikai és kognitív aspektusai. A megtévesztés megvalósítható a technikai felderítés félrevezetésére szolgáló technikai eszközökkel, mint például imitált eszközök, makettek alkalmazásával, dezinformációs kommunikációval, elektronikai úton imitált célpontokkal, megtévesztő szoftverekkel stb. Emellett a klasszikus megtévesztéssel a humán felderítés vezethető félre, illetve idetartoznak az álhírek is, amelyek akár hagyományos módon, szóbeszéddel, írott vagy nyomtatott formában, illetve az elektronikus médián, benne az interneten keresztül terjeszthetők.

A műveleti biztonság, amelynek célközönsége a saját erők, szintén besorolható mindkét információs képességcsoportba. A különböző elektronikus információvédelmi megoldások tipikusan a technikai jellegű információs tevékenységek közé tartoznak, míg például a kritikus vagy minősített információkat kezelő személyek kiválasztása, ellenőrzése vagy a hírszerzés elhárítása inkább a kognitív jellegű tevékenységek közé sorolhatók.

Az információs képességekkel kapcsolatban fontos említést tenni a felderítésről is. A felderítés nem képezi szerves részét az információs műveleteknek, mivel információszerző alapfunkciójából fakadóan egyik célcsoportra sem gyakorol semmilyen hatást. Ugyanakkor az információs képességek megtervezéséhez és összehangolt alkalmazásához szükséges információkat e tevékenység biztosítja. A szerteágazó információs képességek a felderítés minden ágának bevonását igénylik, a hiteles felderítési információk pedig az összadatforrású felderítéssel állíthatók elő.

A mai információs műveleti doktrínák alapvetően az információs képességek integrációjára, koordinációjára, összehangolására fókuszálnak, és arra az elemző, értékelő, tervező és szervező munkára (törzsfunkcióra), amely az információs műveletek lényegét adja. Az információs műveletek integráló funkciójának kiemelése mellett azonban a különböző információs képességek szerepe, fontossága sem elhanyagolható, hiszen ezek koordinációja adja azt a hatásnövelő erőt, amely éppen az információs műveletek lényege.

A mai doktrínák a kezdeti koncepciókkal ellentétben ezek hangsúlyozására, kifejtésére kevésbé fektetnek hangsúlyt. Az információs képességek többsége (például pszichológiai műveletek, elektronikai hadviselés, civil-katonai együttműködés stb.) általában megtalálható külön-külön doktrínákban, de az információs műveletekre vonatkozó doktrínákba csak az említés és egy-egy fogalmi meghatározás szintjén jelennek meg. Ezért a következő fejezetben e képességek közül részletesebben is megvizsgáljuk azokat, amelyeknek értelmezhető a kibertéri alkalmazása.

Vákát oldal

4. Információs műveleti képességek a kibertérben

4.1. A kibertér

4.1.1. A kibertér meghatározása

A hálózatos eszközök térhódítása következtében napjainkban az információs környezet és így az információs hadszíntér egyre nagyobb szeletét teszi ki a kibertér. A korszerű hálózatos infokommunikációs eszközök alkalmazásával kapcsolatban egyre gyakrabban találkozunk ezzel a kifejezéssel, vagy használjuk a *kiber* előtagot különösen a biztonsághoz és védelemhez kapcsolódó szókapcsolatok esetén, mint például a kibertámadás, a kiberbiztonság, a kibervédelem vagy a kiberhadviselés. De valójában mi is a kibertér, hogyan lehet értelmezni, és mi tartozik bele ebbe a tartományba? Az információs műveletek kibertéri megjelenése szempontjából és a későbbiekben tárgyalt kérdések miatt fontos, hogy meghatározzuk, hogy mit is értünk e fogalom alatt.

A *kiber* szó a kibernetikából származtatható, amelyet Norbert Wiener amerikai matematikus alkalmazott elsőként az élő szervezetekben, illetve gépekben végbemenő kommunikáció, vezérlés és információfeldolgozás általános, összefoglaló tudományának meghatározására. Mindazonáltal a *kibernetika* kifejezés a görög *kübernétész* szóból ered, amelynek jelentése *kormányos*. A *kibertér* kifejezést pedig először William Gibson használta, aki az 1984-ben megjelent *Neuromancer* című novellájában írta le a hálózatba kapcsolt számítógépekkel elérhető digitális tér irodalmi meghatározását. Gibson *kibertérre* vonatkozó meghatározását követően rendkívül sokféle megközelítés és értelmezés látott napvilágot, ami rámutat arra, hogy mennyire sokakat érintő és foglalkoztató területről van szó. Az elmúlt bő 30 év

alatt e kifejezést a legkülönbözőbb tudományterületeken, mint például a matematika, a fizika, az informatika és más mérnöki tudományok használják a saját szakterületeiknek megfelelő jelentéstartalommal.

A kezdeti, majd később széles körben elfogadott értelmezés szerint a kiberteret a számítógép-hálózatok és a rajtuk található szolgáltatások és információk alkotta virtuális világ összefoglaló neveként azonosították. Az infokommunikációs technológiával foglalkozó szakértők és a felhasználók sokasága szerint a *kibertér* egy számítógépekkel és kommunikációs kapcsolatokkal kialakított, globális hálózatra alapozott, többdimenziós, mesterségesen létrehozott virtuális valóság. Ezt támasztja alá az *Encyclopædia Britannica* definíciója is, miszerint „a kibertér egy alaktalan (amorf), vélhetően »virtuális« világ, amelyet számítógépek, internet-alapú eszközök, szerverek, routerek és az internet infrastruktúra egyéb elemei közötti kapcsolatok hoznak létre”.[211] (Bussell 2013) A kibertér meghatározásával kapcsolatban tehát általánosan elterjedt nézet még ma is, hogy az a számítógép-hálózatokkal és benne az internettel van összefüggésben.

A vezeték nélküli kommunikációs technológiák súlyának növekedése és a hálózatos technológiákban ma már megkerülhetetlen alkalmazása a kibertér egy újfajta, kibővített megközelítését eredményezte. Ezalatt azt értjük, hogy ma már a felhasználók nagy része a hálózathoz és így az internethez való csatlakozásra számottevő mértékben a vezeték nélküli rádiófrekvenciás kapcsolatot használja. A mobil cellás adatátviteli technológiák, a Wi-Fi-technológia és más, például az IoT-rendszereknél a korábbiakban is bemutatott kis és nagyobb hatótávolságú adatkommunikációs megoldások folyamatos és nagy ütemű fejlődése ezt a tendenciát tovább erősíti. Ez pedig azt is jelenti, hogy a kibertér értelmezésében megjelenik egy új térelem, a fizikailag jól definiálható és matematikai eszközökkel leírható elektromágneses tartomány.

Az elektromágneses tartomány kibertérben való megjelenését mutatja például Margaret Rouse-nak a TechTarget IT enciklopédia

[211] Fordította a szerző.

és oktatóközpont munkatársának a definíciója, amely szerint a kibertér „az elektronika és az elektromágneses spektrum használatával jellemzett tartomány, melyben az adatok tárolására, módosítására és cseréjére hálózatos rendszereket és támogató fizikai infrastruktúrákat használnak. Valójában a kibertér a számítógépeken és távközlési hálózatokon keresztül az emberek összekapcsolására szolgál, a fizikai elhelyezkedésükre való tekintet nélkül".[212] (Rouse 2008) Megjegyzendő ugyanakkor, hogy csupán csak az elektronikával és az elektromágneses spektrum használatával jellemezni a kiberteret jelentős szűkítése ennek a tartománynak. A kibertérben ugyanis még ma is és várhatóan még hosszú időn át gyakran vezetékes kommunikációt és a nagy kapacitású kapcsolatokban optikai kábeleket alkalmaznak a hálózati elemek összekapcsolására. Ezenkívül az *elektronika* kifejezés sokak számára nem feltétlenül jelenti az informatikai eszközök használatát is. Fontos felismerés azonban, hogy a kibertér, bármennyire is információtechnológia-orientált tartomány, ma már az emberek közötti újfajta kapcsolatok kialakítására és fenntartására is szolgál.

Szintén az elektromágneses tér felhasználását és az emberek közötti kapcsolatok új színterét emeli ki Sanjeev Relia a könyvében, aki szerint: „A kibertér az ember által létrehozott digitális médium, amelyet az elektromágneses spektrumban az elektronikus eszközök felhasználásával az adatok gyűjtésére, tárolására és továbbítására használnak, lehetővé téve ezzel az emberek között a szervezeti, kulturális, nemzeti vagy politikai határok nélküli azonnali és globális kapcsolatot."[213] (Relia 2015, 22–23.) E definícióban is kizárólagossággal szerepel az elektromágneses spektrum használata, amelyet már az előző definíció esetében is kifogásoltunk, mint a kibertérben való kommunikációs lehetőségek korlátozását. Fontos felismerés azonban e meghatározásban a kibertér ember által létrehozott mesterséges jellege, valamint az emberek közötti kapcsolat hangsúlyozása. Erre igen jó példa a közösségi média, ahol

[212] Fordította a szerző.
[213] Fordította a szerző.

a legújabb hálózatos technológiát felhasználva az emberek újfajta kapcsolatokat létesíthetnek, kapcsolati hálót alakíthatnak ki.

Ez utóbbi esetében azonban szintén megjegyzendő, hogy a kibertér nem pusztán az emberek számára biztosít egy újfajta kapcsolati teret. Az IoT megjelenésével, az M2M-kommunikációval, mint azt korábban is írtuk, lehetővé válik a fizikai eszközök hálózatba kapcsolása, és a különféle okosalkalmazásokkal (önvezető autó, okosotthon, okosváros stb.) az emberek számára hasznos és kényelmi szolgáltatások érhetők el. Ez esetben tehát a kibertérben nem az emberek közötti kapcsolatról beszélünk, még akkor sem, ha az emberek számára közvetve nyújtanak szolgáltatásokat.

Egy másik érdekes megközelítés szerint a kibertérnek térbeli értelmezése is van, amely értelmezés a földrajztudományhoz kapcsolódik. Mészáros Rezső a kiberteret egy új földrajzi térként határozza meg: „A kibertér térgeometriáinak meghatározása komplikált feladat. Egyrészt azért, mert a kibertér sok különböző tartományból áll, és mindegyiknek megvan a saját formája és szerkezete, másrészt azért, mert ezek a térgeometriák és térformák mesterséges eredetűek. […] A kibertér térgeometriái tehát bonyolult tartománygyűjteményekből épülnek fel, ezek közül némelyik kifejezetten térbeli, és közvetlen földrajzi mintái (hivatkozási alapjai) vannak, mások mintáikat ugyan a való világból veszik, de kifejezetten térbeli formájuk és a térre jellemző tulajdonságaik nincsenek (névsorok, weboldalak), és vannak olyanok is, amelyeknek nincs a földrajz világából vett mintájuk, térformáik, és a térre jellemző tulajdonságaik sincsenek (ilyenek a számítógépes adatállományok allokációs táblázatai). De bármelyik esetet vesszük, akármilyen geometria fedezhető fel bennük, azt mesterséges úton állították elő, és csak megjelenített (kivetített) térkonstrukció formájában léteznek.” (Mészáros 2001)

A kibertér térbeli jellegének vonatkozásában fontos hangsúlyozni, hogy azt minden esetben mesterségesen hozzák létre, illetve különféle megjelenített térformában létezik. Megértéséhez ezért egyre többen megkísérlik láthatóvá tenni a kibertér téralakzatait. Ennek ábrázolása manapság a tudományos-fantasztikus filmművészetben a legszembe-

tűnőbb, ahol a kibertérben zajló tevékenységek megjelenítésére gyakran amorf formákat, a digitális jelleget mutató 0 és 1 számsorfolyamokat, labirintusokat, egymásba nyíló tereket stb. alkalmaznak.

A fentebb ismertetett néhány meghatározás alapján látható, hogy a kibertérnek mára többféle értelmezése is létezik, függően attól, hogy ki és milyen aspektusból vizsgálja azt. Mindenesetre szembetűnő, hogy egyre több olyan interpretáció is jelen van a kibertér értelmezési tartományában, amely túlmutat a pusztán csak számítógépek alkotta világon és ezáltal a kibertér szűk körű értelmezésén. Ezt támasztja alá az ITU 2008-ban megjelent, kiberbiztonságot áttekintő dokumentuma is, amelyben a kiberkörnyezet definícióját a következőképpen adja meg: „közvetlenül vagy közvetett módon hálózatba kötött felhasználók, hálózatok, eszközök, szoftverek, folyamatok, tárolt vagy továbbított információk, alkalmazások, szolgáltatások és rendszerek összessége". (ITU-T X.1205 2008, 2.)

Mint látható, e definíció nem a *kiberteret* határozza meg, hanem az azzal szinonim fogalomként kezelhető kiberkörnyezetet. Ugyanakkor jól szemlélteti a meghatározás, hogy e környezet részét képezi minden olyan eszköz, rendszer, folyamat, információ és felhasználó, aki és amely hálózatos kapcsolattal rendelkezik. Nem tesz különbséget a kommunikáció módja és a hálózatba kapcsolt eszközök fajtája között, ehelyett az információkezelésre fókuszál. E megközelítés alapján pedig a kiberkörnyezet és így a kibertér része minden olyan vezetékes vagy vezeték nélküli kommunikációs móddal hálózatba kapcsolt eszköz, rendszer, amely információt gyűjt, tárol, feldolgoz és továbbít.

A *kibertér* ilyen átfogó és kiterjesztett értelmezését a hadtudomány az elsők között ismerte fel, és deklarálta, hogy azt a katonai műveleti környezet és így az információs hadszíntér egyik fontos tartományának tekinti. A kibertér katonai meghatározását elsőként az USA 2006-ban kiadott Kibertéri Műveletek Nemzeti Katonai Stratégiája[214] tartalmazta. Eszerint „a kibertér egy olyan tartomány, ahol hálózatos rendsze-

[214] National Military Strategy for Cyberspace Operations.

rekben és fizikai infrastruktúrákban működő elektronikai eszközöket és az elektromágneses spektrumot használják fel az adatok tárolására, cseréjére és módosítására".[215] (DoD 2006, ix.)

Az USA védelmi minisztériuma 2017-ben kiadott katonai terminológiai szótára[216] módosította az előbbi meghatározást. Eszerint a kibertér „az információs környezetben, az egymással kölcsönös függőségben lévő információs infrastruktúrák hálózata és a bennük lévő adatok által létrehozott globális tartomány, amely magában foglalja az internetet, a távközlési hálózatokat, a számítógépes rendszereket valamint a beépített feldolgozó és vezérlő elemeket".[217] (DoD 2017, 58.) Mint látható, az első definíció a hálózatos technológiát, az ott működő elektronikai eszközöket és az elektromágneses spektrumot tekinti a kibertér alapvető összetevőinek. A későbbi definíció viszont részben finomítja azt, és egy átfogóbb meghatározást alkalmaz. Hangsúlyozza, hogy a kibertér az információs környezet része, egy olyan globális tartomány, amelyet hálózatba kapcsolt információs infrastruktúrák és az általuk kezelt adatok hoznak létre. Ezek az infrastruktúrák pedig felölelik az infokommunikációs eszközök széles spektrumát, benne az internetet, a vezetékes és vezeték nélküli távközlő hálózatokat, a számítógép-hálózatokat és a különféle érzékelő, feldolgozó és vezérlő eszközöket. Láthatóan nem hangsúlyozza kizárólagosan sem a vezeték nélküli, sem pedig a vezetékes kommunikációs kapcsolatokat, illetve a kibertér által lehetővé váló emberi kapcsolatokra, kapcsolati hálókra sem tér ki.

Szintén a katonai megközelítést mutatja az amerikai Nemzetvédelmi Egyetem professzorának, Daniel Kuehlnek a definíciója, amely talán az eddigiek közül a legátfogóbb és legalaposabb. Véleménye szerint „a kibertér egy olyan dinamikusan változó műveleti tartomány, amelynek egyedi és megkülönböztető jellegzetessége, hogy az egy-

[215] Fordította a szerző.
[216] Joint Publication 1-02, DoD Dictionary of Military and Associated Terms.
[217] Fordította a szerző.

mással hálózatba kapcsolt infokommunikációs rendszerekben és a kapcsolódó infrastruktúrákban az információ létrehozását, tárolását, módosítását, cseréjét és felhasználását végző elektronikai és elektromágneses spektrumot használó eszközök működnek".[218] (Kuehl 2009, 28.) E meghatározás láthatóan hangsúlyozza a kibertér hálózatos jellegét, az információkezelést végző eszközöket, a kapcsolat jellegében pedig megjeleníti az elektromágneses spektrum használatát. Fontos elemként jelenik meg e definícióban a kibertér dinamikájának hangsúlyozása, amely rámutat annak folyamatosan változó és egyben bővülő jellegére. E változást és bővülést mutatja például az e térben alkalmazható eszközök sokasága és sokfélesége (lásd például fizikai eszközök hálózatba kapcsolása, szenzortechnológia, IoT), a kommunikációs módok fejlődése és hangsúlyeltolódása (vezetékestől a vezeték nélküli felé, M2M-kapcsolatok), illetve az emberek mint felhasználók kibertérben való összekapcsolása.

A hazai hivatalos kibertér meghatározások közül kettőt emelünk ki. Az első *Magyarország Nemzeti Kiberbiztonsági Stratégiája* című dokumentumban található, amely szerint: „A kibertér globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét jelenti." [1139/2013. (III. 21.) Korm. határozat, 2.] A Magyar Honvédség Kibervédelmi Szakmai Koncepciója szintén definiálja a kiberteret, amely szerint a „kibertér az elektromágneses spektrum használatával meghatározható, dinamikusan változó tartomány, mely az összekapcsolt hálózatok, eszközök és kiegészítő fizikai infrastruktúrák közötti adatok kezelésére szolgál". [60/2013. (IX. 30.) HM utasítás] Láthatóan mindkét értelmezés illeszkedik a fentebb idézett, elsősorban katonai megközelítésekhez. Kiemelendő viszont, hogy a kiberbiztonsági stratégia fontosnak tartja kihangsúlyozni a kibertérben zajló társadalmi és gazdasági folyamatokat. Ez pedig jól rávilágít arra a tényre, hogy

[218] Fordította a szerző.

mára a globális, hálózatos infokommunikációs technológia által kezelt információ a társadalom és gazdaság fejlődésének fő hajtóerejévé vált.

Összegezve a fenti definíciókat megállapítható, hogy a legtöbb egy adott nézőpont alapján határozza meg a kiberteret. Mindegyik definícióban közös pont, hogy hangsúlyozzák a kibertér hálózatos jellegét, némelyik kihangsúlyozza az internetet is, a többség viszont nem tesz különbséget a hálózatok típusa és mérete között. Egyes meghatározások a kibertérben zajló folyamatokra, mások pedig az abban működő eszközökre és rendszerekre fókuszálnak. Egyes értelmezések a hálózatos rendszerek működési tartományaként az elektromágneses spektrumot külön, esetleg kizárólagos jelleggel is meghatározzák, mások viszont nem hangsúlyozzák ki a hálózati kapcsolat közegét. (Haig 2015) Ezen kívül fontos új elemként jelenik meg egynéhány értelmezésben, a kibertér humánközpontúsága is, ami egyrészt az ember által kreált mesterséges környezetre, másrészt pedig az emberek kibertérben megvalósuló, új típusú kapcsolati formájára utal.

Mint azt a különféle hálózatos infokommunikációs rendszerek tárgyalásakor is láttuk, a mobilitás követelményének eleget téve a kibertérben a hálózati kommunikáció már nemcsak helyhez kötött, vezetékes rendszerekre korlátozódik, hanem nagy hangsúlyt kapnak az elektromágneses spektrumban megvalósított különféle vezeték nélküli megoldások is. Így például napjaink feltörekvő technológiájának számító IoT-rendszerekben is alapvetően a szenzorok és az adatfeldolgozó elemek, illetve az aktuátorok közötti adatátvitel a már tárgyalt vezeték nélküli megoldásokkal valósul meg.

A bemutatott meghatározások analízise és szintézise alapján az alábbiak szerint fogalmazható meg a kibertér átfogó definíciója. *A kibertér az ember által mesterségesen létrehozott, dinamikusan változó tartomány, amelyben az információ gyűjtését, tárolását, feldolgozását, továbbítását és felhasználását végző, egymással hálózatba kapcsolt és az elektromágneses spektrumot is felhasználó infokommunikációs eszközök és rendszerek működnek, lehetővé téve ezzel*

az emberek és a különféle eszközök közötti folyamatos és globális kapcsolatot.

A fenti meghatározás eleget tesz:

- az emberek közötti új típusú kapcsolati igényeknek,
- az IoT-elvnek megfelelően akár a fizikai eszközök összekapcsolhatóságának, valamint
- az elektromágneses spektrum használatára vonatkozó elvárásoknak is.

A katonai műveletekben a mobilitási követelmény még markánsabban jelentkezik. Harcászati-hadműveleti szinten a manőverező erők híradása, illetve a számítógép-hálózatok kialakítása az elektromágneses spektrumban szinte kizárólag rádiófrekvenciás eszközökkel valósítható meg. A harctéri szenzorhálózatokban is a szenzorcsomópontok és a gateway-ek, valamint az adatfúziós feldolgozóközpontok között rádiókapcsolaton keresztül valósul meg az adatátvitel. A harctéren az elektronikai eszközökből (például szenzorokból, rádiókból, radarokból, navigációs eszközökből, harctéri követő és azonosító berendezésekből stb.) és számítógépekből ma már olyan komplex hálózatokat alakítanak ki, amelyeknek közös műveleti környezetüket a kibertér képezi. E hálózatok pedig csak kisebb részben – többnyire a stacionerobjektumokban, illetve a vezetési pontokon belül – alkalmaznak vezetékes kapcsolatot, döntően azonban a vezeték nélküli eszközökkel valósítják meg a hálózati kommunikációt. A kibertér katonai értelmezésében tehát – többek között a kommunikáció szempontjából is – még markánsabban helyet kap az elektromágneses spektrum. (Haig–Várhegyi 2008)

Jelenleg azonban még a katonai műveletekben sem valósult meg a teljes hálózatosítás, ami azt jelenti, hogy nem minden elektromágneses spektrumban működő eszköz van hálózatba kötve. Számos elektronikai berendezés önállóan működik a harctéren, mint például az önállóan működő felügyelet nélküli szenzorok, egyszeri felhasználású zavaróesz-

közök, rádió-távirányítású házi készítésű robbanóeszközök[219] stb. Ezért a kibertér még katonai értelmezésben sem azonosítható teljes mértékben az elektromágneses spektrum felhasználásával, mivel az csak a hálózatos elektronikai rendszerekre értelmezhető. Ugyanakkor mind a civil, mind pedig a katonai alkalmazásokban egyértelműen megfigyelhető a hálózatosítás irányába való elmozdulás. Jó példa erre civil oldalon a felhőalapú technológia, az IoT vagy katonai területen a harci felhő, az IoMT, a harcászati internet vagy a hálózatos harctéri felügyelt nélküli szenzorrendszerek. (Haig 2015)

Mint látjuk tehát, a kibertér és az elektromágneses spektrum kapcsolatában konvergencia tapasztalható. A mobilitási követelményeknek eleget téve azt tapasztaljuk, hogy e két tartomány egyre inkább átfedi egymást. Ez azt jelenti, hogy e két tartománynak az információs környezetben a hálózatos infokommunikációs rendszerek működését tekintve közös halmaza van. Mivel az előzőekben is vázoltak szerint a teljes konvergencia még nem valósult meg, ezért e közös halmazt például többen is kiber-elektromágneses tartománynak nevezik, amelyben összehangolt hálózatos tevékenységek folynak. Ezt a gondolatot támasztja alá az USA szárazföldi haderő kiber-elektromágneses tevékenységeket leíró doktrínája is. (FM 3-38 2012) Szemléletes azonban, hogy öt évvel később, 2017-ben e doktrínát is felváltotta egy újabb, amely még szorosabb kapcsolódást mutat az elektromágneses spektrumban zajló elektronikai hadviselés és a kibertéri műveletek között. (FM 3-12 2017)

Az elektromágneses spektrum kibertéri megjelenésének hangsúlyozása azért fontos kérdés, mert az egyre nagyobb arányú rádiófrekvenciás kommunikáció alkalmazása fokozza a különféle hálózatok elleni fenyegetések lehetőségét. A vezeték nélküli kommunikációt használva, a vezetékes összeköttetéshez képest sokkal könnyebben, fizikai kapcsolódás nélkül lehet hozzáférni a hálózathoz, azon keresztül pedig könnyebben lehet felderíteni és támadni is a hálózatot és annak elemeit.

[219] Radio Controlled Improvised Explosion Devices – RC-IED.

Ez a hálózat védelme és a kiberbiztonság szempontjából komoly kihívást jelent a rendszert tervezők és felhasználók számára egyaránt.

4.1.2. A kibertér struktúrája

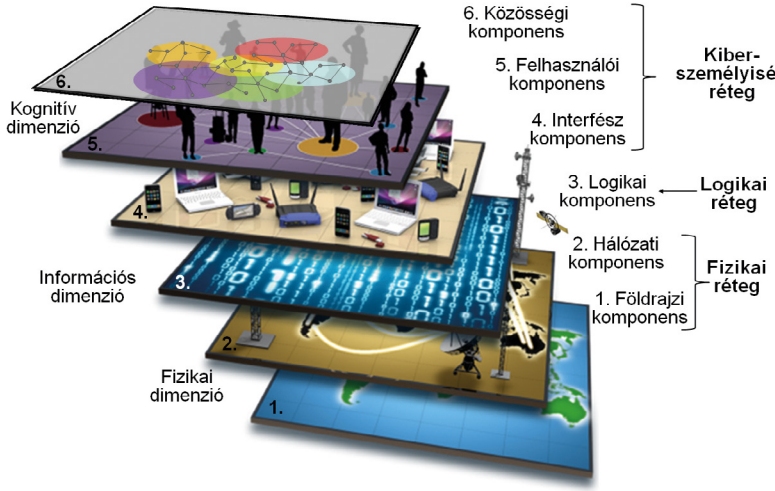
A kibertér, mint láttuk, az információs környezet része, így az összetevői is illeszkednek ahhoz. A korábbi kibertérfelfogások egyfajta virtuális térként fogták fel e tartományt, és csak az információs környezet információs dimenziójában értelmezték azt. Mint azt az előzőekben megvizsgáltuk, a fizikai eszközök hálózatosításával, a felhasználók, emberek közösségi hálózatos kapcsolati formáival, illetve a vezeték nélküli kommunikáció dominanciájával ez a felfogás mára túlhaladottá vált. A kibertér eszerint az információs környezet mindhárom dimenziójában, vagyis a fizikai, az információs és a kognitív tartományban egyaránt értelmezhető.

A különböző hálózatba kapcsolt infokommunikációs rendszerek és azok fizikailag értelmezhető elemei (adatgyűjtő eszközök, szerverek, routerek, kommunikációs eszközök stb.) egy fizikailag jól megfogható, valós világban léteznek. Az egyes eszközök, berendezések a fizikai térben definiálhatók, földrajzi elhelyezkedésük meghatározható. A fenti eszközökön megvalósuló információs folyamatok, az adatok gyűjtése, tárolása, feldolgozása és továbbítása – mint elektronikus információkezelési folyamatok – az információs dimenzióban zajlanak. A kibertér ugyanakkor nem feltétlenül az információ továbbítására és feldolgozásra van a legnagyobb hatással, hanem az emberek társadalmi viszonyaira és a kapcsolataik alakulására. Emiatt a kibertérnek van egy kognitív dimenzióban értelmezhető tartománya is, ahol az emberek a hálózatban kezelt információt értelmezik, illetve egymással interakcióba kerülnek.

A kibertér értelmezésével foglalkozó különféle szakirodalmak e dimenziókat többnyire rétegeknek nevezi, amelyek szorosan illeszkednek az információs környezet dimenzióihoz. A rétegeken belül, a további szofisztikáltabb megközelítésben különféle eltérő megnevezésű

komponenseket is értelmeznek, amelyek az egymással való kapcsolatokat is definiálják. [JP 3-12 (R) 2013; Porche et al. 2017; Relia 2015; Cyber Primer 2016] Ezek felhasználásával és továbbgondolásával a kibertér rétegei és komponensei közé az alábbiakat sorolhatjuk (20. ábra):

- fizikai réteg:
  - földrajzi komponens,
  - hálózati komponens;
- logikai réteg;
- kiberszemélyiség réteg:[220]
  - interfész komponens,
  - felhasználói komponens, valamint
  - közösségi komponens.



20. ábra

A kibertér struktúrája

Forrás: USNA (é. n.) és Cyber Primer (2016) alapján a szerző szerkesztése

[220] Cyber-persona layer – magyarra nehezen átültethető, de talán a *kiberszemélyiség* kifejezés tükrözi leginkább azt a tartalmat, amely a felhasználókat, azok hálózathoz kapcsolódását és ezáltal a közösségi hálózat kialakítását írja le.

A fizikai réteg földrajzi és hálózati komponensekből áll. A földrajzi komponens a hálózat hardverelemeinek és infrastruktúrájának földrajzi elhelyezkedésére vonatkozik, ugyanis a korábbi meghatározás szerint a kibertér alapvetően a természetes földrajzi környezetben, az ember által mesterségesen létrehozott tartomány. A hálózati komponens a hálózat hardver-alkotóelemeinek és infrastruktúráinak fajtáját, típusát mutatja meg. Ezek közé tartozhatnak többek között a szenzorok, adattároló központok, szerverek, routerek, vezetékek, optikai kábelek, rádiófrekvenciás adatátviteli eszközök, mobil cellás bázisállomások, műholdas eszközök stb., de idetartozik az elektromágneses spektrum is mint a vezeték nélküli hálózati kommunikáció fizikailag definiálható tartománya. E rétegben értelmezhető a már korábban többször is kihangsúlyozott kiberfizikai tartomány is, amely a szoftveresen vezérelt és felügyelt, hálózatba kötött kiberfizikai eszközök működési környezete, mint ahogy azt az IoT-rendszerekben működő szenzorok, aktuátorok, kontrollerek esetében láttuk.

A logikai réteg a hálózat virtuális tere, amely alapvetően a kibertér fizikailag nem megfogható elemeit tartalmazza. A korábbi felfogások a kiberteret kizárólag ezzel a réteggel azonosították. A logikai réteg elmei lehetnek a hálózatban kezelt információk, átviteli és címzési protokollok, szoftveralkalmazások, hálózati szolgáltatók és felhasználók adatai, internetes domainnevek, információbiztonsági megoldások stb.

A kiberszemélyiség rétege interfész-, felhasználói, illetve közösségi komponensekből áll. Tulajdonképpen ez az a réteg, amelyik a kiberteret megszemélyesíti. Ez jelenti a hálózat felhasználóinak digitális reprezentációját a kibertérben. E rétegben a kibertér szereplőinek olyan személyazonossága jelenik meg, amelyet például információszerzésre és befolyásolásra is felhasználnak, miközben valós személyazonosságuk és hovatartozásuk rejtve marad. (DoD 2011) A kiberszemélyiség rétegben az interfészkomponens a felhasználók saját hardver és szoftver eszközeivel köti össze az embereket a kibertér logikai és fizikai rétegével és azokon keresztül pedig egymással. Ebbe tartoznak bele a felhasználó hálózathoz kapcsolódó saját, személyi infokommunikációs

eszközei, mint például a személyi számítógépek, laptopok, tabletek, okostelefonok, navigációs eszközök stb.

A felhasználói komponens a hálózaton lévő személyeket jelenti, akik egyedi címekkel, azonosítókkal, például IP-címmel, e-mail-címekkel rendelkeznek a hálózaton. A hálózatban egy személynek akár többféle személyisége is lehet, például többféle közösségi médiafelületen lehet regisztrált felhasználó, több e-mail-fiókkal rendelkezhet, vagy különféle eszközökkel, számítógéppel, tablettel, okostelefonnal csatlakozhat a hálózathoz. De több személy ugyanazt a hálózati megszemélyesítést meg is oszthatja egymás között, például egy többfelhasználós e-mail-fiók használatával.

A kiberszemélyiség réteg harmadik és legfelső szintje a közösségi komponens, amely a hálózaton lévő személyek kapcsolati hálóját, interakcióit jelenti. A közösségi média felhasználásának fokozódása miatt e komponens jelentősége a kibertérben egyre jelentősebb. Az emberek igen nagy száma már e felületet használja fel egyrészt információszerzésre, másrészt pedig a saját maga által létrehozott információk (például fotók, videók) megosztására. Az egyének így ma már nemcsak passzív felhasználói a kibertérnek, hanem aktív cselekvői is. A közösségi komponens tehát az emberi kölcsönhatásokkal kapcsolatos, és az egyes felhasználókhoz kötődő tulajdonságokról, például a kultúráról, a vallásról, szokásokról, az érdeklődési körről, a kommunikációs lehetőségekről, valamint személyükről és személyiségükről oszt meg információt.

A fenti rétegek rövid ismertetése alapján látható, hogy azok, bár némileg eltérő elnevezéssel, de teljesen illeszkednek az információs környezet dimenzióihoz. Sajátosságuk, hogy további egymáshoz kapcsolódó komponensekre bonthatók. E rétegek és összetevők tulajdonságai megmutatják, hogy a kibertérben zajló információs műveletek melyik rétegben, milyen eszközökkel, technikákkal és eljárásokkal valósíthatók meg, kik és mik lehetnek azok lehetséges célpontjai, illetve milyen hatások érhetők el az egyes információs műveleti képességekkel.

Ennek megfelelően az egyes rétegekben különféle információs támadásokat lehet folytatni:

- a fizikai rétegben például a hálózati kommunikációs eszközök ellen elektronikai felderítés, lehallgatás vagy zavarás útján, de akár fizikailag is megsemmisíthető, tönkretehető egy hálózati fizikai infrastruktúra-elem;
- a logikai rétegben például a szoftverek, operációs rendszerek vagy a kezelt adatok elleni rosszindulatú programokkal, amelyekkel korlátozni vagy működésképtelenné lehet tenni a hálózatot vagy annak elemeit, illetve törölni vagy kompromittálni lehet az adatbázisokat;
- a kiberszemélyiség rétegben célzott üzenetekkel, hírekkel, álhírekkel stb. lehet információs támadást folytatni, amelyek befolyásolhatják a hálózatot használó személyeket és rajtuk keresztül akár a nagyobb közösségeket is.

Az információs műveleteken belüli védelmi eljárások hasonlóan e rétegekben valósulnak meg:

- a fizikai rétegben például lehallgatás és zavarás elleni védelemmel;
- a logikai rétegben például tűzfalakkal, vírusirtó alkalmazásokkal, hozzáférés szabályozással, illetve
- a kiberszemélyiség rétegben például a felhasználók biztonságtudatosságának erősítésével.

Ezeket a kibertérben alkalmazható eljárásokat és technikákat, illetve azok hatásait a következőkben részletezzük.

4.2. Kibertéri műveletek

4.2.1. A kiberfölény és a kibertéri befolyásoló hatások

Az információs műveletek technikai és kognitív információs képességeinek összehangolt kibertéri alkalmazásával fölényt lehet kialakítani a szemben álló féllel szemben, és befolyásoló hatást lehet elérni a semleges szereplőknél. A kibertérben érvényesülő, összehangolt információs tevékenységek esetében a hálózatos képességek saját oldalon való kialakítása, működtetése, illetve a másik fél oldalán való gyengítése, lerontása döntő fontosságú lehet egy hagyományos konfliktusban. Ezért a kiterjesztett értelmezésű kibertérben folyó tevékenységek során a cél a szemben álló fél feletti kiberfölény megszerzése és megtartása.

A kibertér jelentőségének felismerésével párhuzamosan a kiberfölény értelmezése is megjelent a katonai doktrínákban. Az amerikai szárazföldi haderő 2017-ben kiadott FM 3-12 *Kibertéri és elektronikai hadviselési műveletek* doktrínájának meghatározása szerint a kiberfölény egy katonai erő kibertér-dominanciájának azon foka, amely lehetővé teszi számára, illetve a kapcsolódó földi, légi, tengeri és űrbéli erők számára, hogy adott időben és helyen biztonságos és megbízható műveleteket folytasson anélkül, hogy az ellenség vagy a szemben álló fél akadályozná abban. A kiberfölény lehetővé teszi, támogatja, biztosítja és megkönnyíti mindazon harci képességek kihasználását, amelyek befolyásolják, támogatják és lehetővé teszik mindenfajta harcfeladat végrehajtását és a mindennapi tevékenységet. (FM 3-12 2017, 1–3.) A kiberfölény az információs fölény azon részét képezi, amelyet hálózatos infokommunikációs technológia felhasználásával lehet elérni, és amelynek következtében a saját képességek jelentős mértékben megnőnek.

Az információs fölényhez hasonlóan a kiberfölény kivívásának és megtartásának is három egyenrangú és egymással szoros kapcsolatban lévő eleme különböztethető meg:

- a különböző elektronikai és informatikai adatgyűjtő eszközökkel, szenzorokkal, valamint kommunikációs eszközökkel az infor-

máció biztosítása a másik fél képességeiről, a saját lehetőségekről és a környezetről;
- a másik fél hálózatos infokommunikációs rendszerei működésének akadályozása, az információ feldolgozásának, továbbításának korlátozása és megnehezítése, valamint a döntéshozók és a személyi állomány infokommunikációs hálózatokon keresztüli befolyásolása;
- a saját hálózatos információs képességek, valamint a saját döntéshozók és a személyi állomány védelme a másik fél hálózaton keresztül megvalósított különböző logikai és fizikai (elektronikai) támadásaival, valamint befolyásolási kísérleteivel szemben.

Az információ biztosítása egyrészt a másik fél elektronikai rendszereinek, számítógép-hálózatainak felderítését, másrészt a saját helyzetéről szóló információk elektronikus feldolgozását, tárolását és továbbítását, harmadrészt pedig a környezetről szóló adatok elektronikai rendszerekkel, eszközökkel való megszerzését, feldolgozását, továbbítását jelenti. E tevékenységek és képességek a kibertér fizikai és a logikai rétegében valósulnak meg, és hatásukat is itt érik el.

A másik fél hálózatos infokommunikációs rendszerei működésének korlátozása, akadályozása egyrészt a számítógép-hálózatokba való behatolással és ennek következtében például adatbázisok tönkretételével, módosításával, hozzáférés akadályozásával, szoftveres és hardveres hibák előidézésével valósítható meg, másrészt az elektromágneses tartományban különböző támadási módszerek alkalmazásával is korlátozható e rendszerek működése. Idesorolhatók például az alábbiak:
- elektronikai zavaró eszközökkel a kommunikációs rendszerek megbontása;
- adatszerző eszközök, szenzorok zavarása, megtévesztése;
- navigációs rendszerek zavarása, megtévesztése;
- elektronikai megtévesztő tevékenységek folytatása vagy
- nagyenergiájú impulzusfegyverekkel (e-bomba) az elektronikai eszközök, számítógépek tönkretétele.

A döntéshozók és a személyi állomány befolyásolása a hálózaton keresztül továbbított valós és hamis üzenetekkel érhető el. A másik féllel szembeni korlátozó, akadályozó, befolyásoló tevékenységek és -képességek a kibertér mindhárom rétegében alkalmazhatók, és hatásaik is szintén mindhárom rétegben érvényesülnek.

A saját hálózatos információs képességeknek a másik fél logikai és fizikai (elektronikai) úton végrehajtott különböző támadásaival szembeni védelme magában foglalja a saját hálózatos infokommunikációs rendszereinkben rejlő lehetőségek maximális kihasználását, illetve e rendszereink elektronikai és számítógép-hálózati védelmét. (Haig–Várhegyi 2008) A saját döntéshozók és a személyi állomány hálózaton keresztüli befolyásolásával szembeni védelem pedig részben az információbiztonsági tudatosság növelésével, felkészítéssel, illetve a befolyásolással elért hatások minimalizálásával érhető el.

A nem hagyományos, negyedik generációs, hibrid műveletekben, ahol a nyilvánvaló ellenség gyakran nincs jelen, a hagyományos információs fölényhez hasonlóan a hagyományos kiberfölény sem értelmezhető teljeskörűen. E műveletekben, mint azt már többször hangsúlyoztuk, a célközönséget sokszor a nem állami szereplők és a polgári lakosság képviseli. Velük szemben, ahogy azt az információs fölény koncepciójánál is láttuk, a kibertéri ellentevékenység és a negatív hatású befolyásolás alkalmazása nem célravezető. Helyettük a pozitív befolyásolásra és tájékoztatásra irányuló hatásokat előidéző adaptív kiberfölény kialakítása az elérendő cél.

4.2.2. A kibertéri műveletek értelmezése

A hagyományos és az adaptív kiberfölény előző alfejezet szerinti értelmezése egyértelműen az információs fölényhez kapcsolódik, annak azon részét képezi, amelyet a kibertérben lehet kivívni. Mint ahogy a kiberfölényt az információs fölény részeként értelmezzük, úgy annak

kivívása is az információs műveletek részeként értelmezhető kibertéri műveletekkel valósítható meg.

Az információs műveletek meghatározásából kiindulva a kibertéri műveleteket az alábbiak szerint definiálhatjuk: *A kibertéri műveletek a kibertérben érvényesülő információs képességek integrált, összehangolt és koordinált alkalmazására irányuló tevékenységek összessége, amelyek a műveletek célkitűzéseinek elérése érdekében, a kibertéri hálózatos infokommunikációs rendszereket felhasználva, a kognitív képességekkel közvetlenül, illetve a technikai képességekkel közvetetten hatásokat gyakorolnak a műveletekben részt vevő célközönség szándékára, helyzetértelmezésére és képességeire.*

Tekintettel a kibertér kiterjesztett értelmezésére, az itt folytatott műveletek között a technikai képességek körébe tartozó tevékenységek közé sorolhatjuk például:

- a számítógép-hálózatokba való bejutást, azok felderítését;
- az adatbázisokhoz való hozzáférést, azok módosítását, tönkretételét;
- a szerverek túlterhelésével a hozzáférés akadályozását;
- a távközlési hálózatok lehallgatását;
- az adatszerző és kommunikációs eszközök, rendszerek zavarását;
- a navigációs rendszerek elleni elektronikai támadás különböző formáit, valamint
- a szemben álló fél fentiekben részletezett hasonló tevékenységeivel szembeni védelmet.

A kibertérben zajló kognitív képességek a hálózatos infokommunikációs rendszereken keresztül a célközönség felé eljuttatott valós és hamis üzenetek, valamint tájékoztató és együttműködő információk eljuttatására szolgáló technikákkal valósíthatók meg. Ezek közé tartozhatnak például az internetes hírportálokon, a közösségi médián és részben a hagyományos elektronikus médián (tv, rádió) keresztül terjesztett üzenetek, hírek, amelyek alkalmasak a széles körű közvélemény, a kiválasztott célcsoportok és célszemélyek befolyásolására és tájékoztatására. A felsorolt tevékenységek csak néhány kiragadott példát mutatnak be arról a széles

palettáról, amelyek támadó céllal alkalmazhatók a másik fél hálózatos infokommunikációs rendszerei és a felhasználók ellen, illetve védelmi jelleggel a saját hasonló rendszereink védelme és az emberek felkészítése, biztonságtudatosságának erősítése érdekében.

Mint arra korábban már utaltunk, a kibertérben zajló tevékenységek egyre gyakrabban járulnak hozzá a katonai célok eléréséhez. Erre utalnak azok a már megtörtént események, amelyek során az egymással szemben álló felek a fegyveres konfliktusokkal összehangolva folytattak kibertámadó tevékenységet, mint ahogyan az tapasztalható volt például a grúziai és a kelet-ukrajnai konfliktusokban is. Ezek a műveletek elsősorban a másik fél infokommunikációs rendszereinek korlátozására irányultak, és ezeken keresztül pedig valamilyen létfontosságú infrastruktúra működésében idéztek elő komoly károkat.

Így például 2008-ban a grúz parlament és kormányzati oldalak váltak elérhetetlenné, vagy 2015 decemberében a Krím félsziget elcsatolása után az ukrán energiaellátásban keletkezett egy jelentős területen szolgáltatáskiesés, amelyet a BlackEnergy nevű backdoorkártevővel idéztek elő a támadók. (Lipovsky–Cherepanov 2016) Mindkét eset köthető volt aktuális katonai műveletekhez, ami alapján mind Grúzia, mind pedig Ukrajna azt vélelmezte, hogy Oroszország áll a támadások hátterében. Ilyen típusú kibertéri műveleteket mind a reguláris, mind pedig az irreguláris erők vagy akár civil hackercsoportok is végrehajthatnak a katonai műveletek és a politikai célok támogatása érdekében.

Napjaink behálózott társadalmának köszönhetően, a kibertéri műveletek alkalmazása azonban nem csak és kizárólagosan a katonai műveletekhez kapcsolódnak. Ma már napi rendszerességgel találkozunk olyan híradásokkal, amelyek arról számolnak be, hogy különféle hackercsoportok, politikai célok vagy gazdasági haszon reményében kibertámadásokat hajtanak végre kormányzati szervek, intézmények, gazdasági szervezetek stb. ellen. E fizikai és logikai rétegben indított támadások a megtámadott szervezet hálózatos infrastruktúrájában idéznek elő szolgáltatáskiesést, adatbázismódosítást, adatlopást stb., és hatásaik is a kibertér fizikai és logikai rétegében jelentkeznek.

Emellett ma egyre gyakrabban találkozunk olyan kibertéri hatásokkal is, amikor a cél nem valamilyen információs infrastruktúra működésképtelenségének előidézése, hanem a hálózatot használók és rajtuk keresztül a szélesebb körű közvélemény befolyásolása. Ezek a „puha támadások" nem tesznek kárt sem az adatokban és az információkban, sem pedig az infokommunikációs rendszer hardver- és szoftverelemeiben. Ehelyett a hálózat nyújtotta technológiai lehetőségeket kihasználva politikai és ideológiai üzenetek terjesztésével az emberekben és a társadalom széles köreiben kívánnak olyan befolyásoló hatásokat elérni, amelyek az üzenetek, hírek terjesztőjének az érdekeit szolgálják.

Jó példa erre napjainkban az amerikai elnökválasztási kampányba való orosz beavatkozás,[221] az álhírek terjesztése és ezzel az elnökválasztás eredményének befolyásolása. Mindezek pedig azt is bizonyítják, hogy a kibertérben zajló műveletek megszüntetik az éles határokat a clausewitzi értelemben vívott háború és a szintén politikai célok érdekében, békeidőben folytatott tevékenységek között. Ez pedig a kibertér és a benne zajló ellentevékenységek, védelmi és befolyásoló tevékenységek egyik legfontosabb sajátossága.

A 3. fejezetben meghatároztuk az információs műveletek technikai és kognitív képességeit, amelyek összehangolt alkalmazásával az információs műveletek céljai elérhetők. A technikai információs képességek az infokommunikációs rendszerekkel és hálózatokkal vannak közvetlen kapcsolatban. Az információs ellentevékenységek és a védelem egyrészt ezeken a hálózatokon keresztül, többnyire az infokommunikációs eszközök felhasználásával valósulnak meg, másrészt azok célpontjait is e rendszerek, hálózatok és elemeik képezik. A kognitív információs képességek ezzel szemben a befolyásoló és tájékoztató technikákkal gyakorolnak hatásokat, közvetlenül az embereket veszik célba.

[221] A beavatkozás ténye jelenleg még nem bizonyított, de számos bizottsági meghallgatás, dokumentum és amerikai hírszerző szolgálati jelentés jelenik meg, amelyek a beavatkozást támasztják alá, például ICA Report 2017.

3. táblázat

Kibertéri műveletek információs képességei

Képesség	Célpont	Tevékenység	Kibertéri rétegben	
			Tevé-kenység	Hatás
Elektronikai felderítés	Hálózati elektronikai eszközök, vezeték nélküli kommunikáció	Rádióelektronikai felderítés, képi felderítés, műszeres felderítés, nyílt forrású felderítés	Fizikai	Fizikai
Számítógép-hálózati műveletek	Hálózat, szoftverek, operációs rendszerek, adatbázisok, hardverelemek, kiberfizikai eszközök	Számítógép-hálózati felderítés, támadás, védelem, például malware, DDoS, adatbázistörlés, -módosítás, hardverrongálás stb.	Logikai	Logikai, fizikai
Elektronikai hadviselés	Hálózati elektronikai eszközök, szenzorok, vezeték nélküli kommunikáció, navigáció, kiberfizikai eszközök	Elektronikai felderítés, elektronikai zavarás, elektronikai megtévesztés, elektronikai pusztítás, elektronikai védelem	Fizikai	Fizikai
Fizikai megsemmisítés	Hálózati információs infrastruktúra-elemek, hardver eszközök	Információs célpontok megsemmisítése, rongálása	Fizikai	Fizikai
Műveleti biztonság	Hálózati infrastruktúra-elemek, adatbázisok, kommunikáció, emberek	Elektronikus információbiztonság, fizikai biztonság, személyi biztonság, rejtjelzés, biztonságtudatosság stb.	Fizikai, logikai, kiberszemélyiség	Fizikai, logikai, kiberszemélyiség
Megtévesztés	Hálózat, szenzorok, adatbázisok, kommunikáció, emberek, közösségi csoportok	Elektronikai megtévesztés, imitálás, dezinformáció, spoofing, social engineering, álhírek stb.	Fizikai, logikai, kiberszemélyiség	Fizikai, logikai, kiberszemélyiség
Pszichológiai műveletek	Emberek, közösségi csoportok	Befolyásolás internetes hírportálokon, közösségi médián, e-mailen keresztül, social engineering	Fizikai, logikai, Kiberszemélyiség	Kiberszemélyiség
Civil-katonai együttműködés	Emberek, közösségi csoportok, igazgatási szervek	Befolyásolás, együttműködés, kapcsolatalakítás e-mailen, internetes hírportálokon, közösségi médián keresztül	Fizikai, logikai, kiberszemélyiség	Kiberszemélyiség
Tömegtájékoztatás	Emberek, közösségi csoportok	Tájékoztatás internetes hírportálokon, közösségi médián, e-mailen keresztül	Fizikai, logikai, kiberszemélyiség	Kiberszemélyiség

Forrás: a szerző szerkesztése

A kibertérben alkalmazható információs képességeket összefoglaló 3. táblázat szemlélteti az egyes képességek célpontjait (célcsoportjait), a célpontok ellen alkalmazható tevékenységeket, védelmi módszereket és befolyásoló hatásokat, valamint e tevékenységeknek a kibertér egyes rétegeivel való kapcsolódását. Mindegyik képesség eredményes alkalmazásához elengedhetetlen a pontos, valós idejű és releváns felderítési információ. Ezért, habár a felderítés nem képezi részét az információs műveletek képességeinek, a táblázat tartalmazza az elektronikai felderítés kibertéri megjelenését is.

Amint azt az előző alfejezetben megvizsgáltuk, az infokommunikációs hálózatok működési környezete a kibertérben értelmezhető, azon belül is a fizikai rétegben találhatók meg a földrajzilag is definiálható hálózati elemek, mint például a szerverek, adatközpontok, adatkapcsolati kábelek, mobiltávközlési bázisállomások és mobilkapcsoló-központok stb., a kibertér logikai rétegében pedig a hálózatos adatkezelési folyamatok zajlanak. Ezek alapján a technikai információs képességek alapvetően a kibertér fizikai és logikai rétegeihez kapcsolódnak, azokban valósulnak meg, és hatásukat is ott fejtik ki.

A kognitív információs képességek ezzel szemben a humánumra fókuszálnak, az emberek és a társadalmi csoportok attitűdjét, véleményét, gondolkodását, viselkedését formálják, alakítják. Ez alapján a célpontjait, célcsoportjait is az emberek, csoportok, közösségek adják. A célközönség felé irányuló befolyásoló, tájékoztató hatások elérése azonban napjainkban már nem csak a hagyományos kognitív technikákkal valósítható meg. A korszerű hálózatos technológiának köszönhetően az internet, a közösségi hálózatok és akár az infokommunikációs eszközökön keresztül eljuttatott célzott üzenetek felhasználása ma már szinte mindennapossá vált. Így kognitív befolyásoló hatásokat el lehet érni hagyományos kognitív információs módszerekkel (például személyközi kommunikációval, hagyományos médiával stb.), illetve az infokommunikációs technológiát felhasználva, technikai módszerekkel a kibertérben. Ez alapján tehát a kognitív információs képességek alkalmazásának színtere szintén lehet a kibertér, annak fizikai

és logikai rétege is, az ezeken keresztül eljuttatott üzenetek pedig a kiberszemélyiség rétegben fejtik ki hatásukat.

A következő alfejezetben röviden áttekintjük, hogy az egyes kibertéri információs tevékenységek mit takarnak, és hogyan illeszkednek a kibertéri műveletekhez. A fizikai megsemmisítést terjedelmi korlátok miatt bővebben nem tárgyaljuk, ugyanakkor e képesség szintén részét képezi a kibertéri információs műveleteknek. A tevékenység jellegét tekintve a fizikai megsemmisítés alapvetően a fizikai rétegben lévő hardverelemek, eszközök ellen alkalmazható különböző kinetikus hatású fegyverek, eszközök, valamint a megsemmisítést, rongálást végrehajtó erők, csoportok alkalmazását jelenti. Célpontjai a hálózatos infrastruktúra hardvereszközei (például szerverközpontok, optikai kábelek, mobilkommunikációs bázisállomások stb.), ezért a hatását is a kibertér fizikai rétegében fejti ki.

4.2.3. A kibertéri műveletek információs képességei

4.2.3.1. Elektronikai felderítés

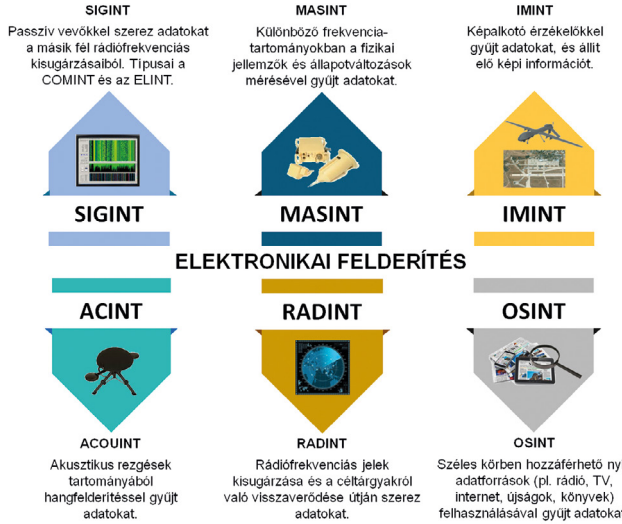
Az elektronikai felderítés az általános felderítés azon részét képezi, amelynek során az adatszerző technikai eszközök a teljes frekvenciaspektrumban adatokat gyűjtenek a szemben álló félről és a környezetről, majd a megszerzett adatokat akár automatikusan is az adatfúziós adatfeldolgozó központokba továbbítják, ahol felderítési információkat állítanak elő belőlük. Definíciószerűen: „az elektronikai felderítés fogalma alatt az elektronikai eszközökkel, különböző hullámtartományokban végzett adatszerzést és ezen adatok feldolgozását értjük, amely megjelenhet több adatforrástípus esetében is”. (Haig et al. 2013, 96.) Adatforrás lehet minden olyan eszköz, objektum, tárgy vagy személy, amelyről az adatszerző eszközökkel információ szerezhető be.

Az elektronikai felderítés fajtái az adatszerzés módjától függően az alábbiak lehetnek (21. ábra):

- rádióelektronikai felderítés,[222] amely passzív vevőberendezésekkel szerez adatokat a szemben álló fél *rádiófrekvenciás tartományban* működő elektronikai eszközeinek kisugárzásaiból. A SIGINT típusai az alábbiak:
  - rádiófelderítés, amely[223] a szemben álló fél kommunikációs rendszereiben működő kisugárzó eszközeinek, rádióadóinak felfedésével, iránymérésével és lehallgatásával szerez információt;
  - rádiótechnikai felderítés,[224] amely a szemben álló fél nem kommunikációs célú berendezéseinek (radarok, távirányító és távvezérlő eszközök) rádiófrekvenciás kisugárzásait érzékeli, elemzi, és állít elő belőlük felderítési információt;
- műszeres mérésen alapuló felderítés,[225] amely a különböző frekvenciatartományokban a különféle fizikai jellemzők és állapotváltozások műszeres mérésével gyűjt adatokat, mint például a hőmérséklet, mágnesesség, szeizmikus rezgés stb. mérésén alapuló szenzorok vagy az elektronikai berendezések működése során keletkezett nem szándékos kisugárzások felderítése;
- képi felderítés,[226] amely a fotografikus, radar-, elektrooptikai, infravörös, illetve multispektrális érzékelőkkel szerez adatokat, és állít elő képi információt;
- hangfelderítés,[227] amely az akusztikus rezgések tartományából gyűjt adatokat;
- radarfelderítés,[228] amely rádiófrekvenciás jelek kisugárzása és a céltárgyakról való visszaverődése útján szerez adatokat, valamint

[222] Signal Intelligence – SIGINT.
[223] Communication Intelligence – COMINT.
[224] Electronic Intelligence – ELINT.
[225] Measurement Intelligence – MASINT.
[226] Imagery Intelligence – IMINT.
[227] Acoustic Intelligence – ACINT.
[228] Radar Intelligence – RADINT.

- nyílt forrású felderítés,[229] amely a széles körben hozzáférhető nyílt adatforrások (például rádió-, televízióadás, internet, újságok, könyvek) felhasználásával gyűjt adatokat. (HAIG et al. 2013)



21. ábra

Az elektronikai felderítés fajtái

Forrás: HAIG et al. (2013) alapján a szerző szerkesztése

A megszerzett adatokat a legkorszerűbb adatfúziós technológia alkalmazásával dolgozzák fel, és állítanak elő belőlük felderítési információt. Az adatfúzió biztosítja a különböző érzékelési tartományú adatszerző eszközök által szerzett adatok feldolgozását, összegzését és az eredmények szétosztását. Mivel egy adott objektumról több forrásból (például radarfelderítéssel, képi felderítéssel, rádiófelderítéssel stb.) szerezhetők adatok, így ezek fúziója révén a felderítési információk hitelesebbé válnak, és ezáltal például a megtévesztés, félrevezetés hatékonysága jelen-

[229] Open Source Intelligence – OSINT.

tősen csökkenthető. A megszerzett és kiértékelt adatokból előállított felderítési információk a szemben álló fél képességeinek, lehetőségeinek és szándékának megismerésén túl célinformációként felhasználhatók a hatékony támadás kivitelezéséhez is.

A kibertérben alkalmazható elektronikai felderítés elsősorban a SIGINT-en belüli rádiófelderítéshez köthető, mivel ez biztosítja a hálózatok vezeték nélküli kommunikációjának felderítését. Ezáltal a rádiófrekvenciás tartományban felfedhetők a vezeték nélküli hálózatok, hozzáférhetővé válnak az adatbázisok, amelyekből adatokat lehet megszerezni, illetve megállapíthatók a hálózat gyenge pontjai. Emellett a kibertérben alkalmazhatók a hálózatba szervezett, felügyelet nélküli szenzorok, amelyek a különféle érzékelési tartományokban a környezetükből gyűjtik az adatokat, majd hálózati kapcsolaton keresztül juttatják el az adatgyűjtő és feldolgozóközpontokba.

Mindezek alapján kijelenthető, hogy az elektronikai felderítés eszközei a kibertér fizikai rétegében működnek, és ennek következtében szintén e rétegben működő eszközökről és állapotváltozásokról szereznek adatokat. Természetesen nem minden fajta elektronikai felderítés zajlik a kibertérben. Csak azokat a felderítési módokat soroljuk ebbe a körbe, amelyek vagy a hálózati eszközöket és a hálózati kommunikációt derítik fel, vagy pedig amelyek hálózatos környezetben működnek, mint például a hálózatos, felügyelet nélküli szenzorok vagy a civil IoT- és a katonai IoMT-technológiák.

4.2.3.2. Számítógép-hálózati műveletek

A kibertéri támadó és védelmi tevékenységeket gyakran csak a számítógép-hálózati környezetben, illetve elsősorban az interneten zajló tevékenységekkel azonosítják. Emiatt például a kiberműveleteket[230] sokszor kizárólag a számítógép-hálózatok elleni támadásokkal és védelemmel szokták

[230] Cyber Operations.

azonosítani. Mint azonban ezt már korábbiakban kifejtettük, a kibertér értelmezését és tartományait tekintve napjainkban ez erős leszűkítése lenne e műveleteknek. Emiatt e tevékenységre a NATO-ban és számos országban is használt *számítógép-hálózati műveletek* kifejezést alkalmazzuk. Ugyanakkor az is nyilvánvaló, hogy a hálózatos tevékenységekkel összefüggésben ez az a képesség, amelyik teljes mértékben, minden elemében és tevékenységében illeszkedik a kibertéri műveletekhez.

Definíciószerűen a számítógép-hálózati műveletek egyrészt a másik fél hálózatos számítógépes rendszerei felderítésére, adatok megszerzésére, működésük korlátozására, akadályozására, befolyásolására irányul a számítógép-hálózati felderítés és támadás módszereivel, másrészt pedig a saját hasonló hálózatok működését biztosítja a számítógép-hálózati védelem eszközeivel és technikáival.

A számítógép-hálózati műveletek magukban foglalják:

- a számítógép-hálózatok struktúrájának feltárását;
- a forgalmi jellemzőik alapján a hierarchikus és működési sajátosságaik meghatározását;
- a hálózaton folytatott adatáramlás tartalmának regisztrálását;
- a hálózatban tárolt adatokhoz való jogosulatlan hozzáférést és azok ellopását;
- a hálózatokban folyó megtévesztő és zavaró tevékenységet;
- a számítógépes programok módosítását, futtatásuk megakadályozását, rendszerhibák előidézését;
- hardveres meghibásodások előidézését;
- a hálózatban tárolt adatbázisok megváltoztatását, törlését, zárolását, és
- a másik fél hasonló tevékenységeivel szembeni védelmet.

A számítógép-hálózati műveletek fajtái (22. ábra):

- a számítógép-hálózati felderítés;
- a számítógép-hálózati támadás, valamint
- a számítógép-hálózati védelem.[231]

[231] Computer Network Defence – CND.

22. ábra

Számítógép-hálózati műveletek

Forrás: a szerző szerkesztése

A számítógép-hálózati felderítés a hálózatok struktúrájának feltérképezését, az adatbázisokhoz való illetéktelen hozzáférést és a támadható pontok meghatározását jelenti. Megvalósulhat a szemben álló fél számítógépes rendszereibe való szoftveres vagy hardveres úton való behatolással. Célja az adatbázisokban tárolt adatokhoz, információkhoz való hozzáférés és azok felderítési céllal való hasznosítása, illetve a későbbi károkozással járó támadás kivitelezéséhez a hálózat támadható pontjainak és a támadás leghatékonyabb formáinak meghatározása. A felderítés az elszenvedő hálózat részéről általában nem észlelhető formában valósul meg, így a hálózat üzemeltetője és felhasználója számára a felderítés ténye többnyire nem ismert.

A számítógép-hálózati támadás szoftveres vagy hardveres úton való behatolást jelent a másik fél számítógép-hálózataiba, az adatbázisokban tárolt adatok tönkretétele, módosítása, manipulálása vagy hozzá-

férhetetlenné tétele, valamint a hálózat egésze, illetve egyes szoftver- és hardverelemei működésének akadályozása érdekében. A támadás a számítógép-hálózati elemekben és az általuk vezérelt fizikai eszközökben való fizikai károkozást is eredményezhet, amelyet a szoftverek módosításával vagy manipulációjával lehet elérni.[232] A támadás a felderítéssel ellentétben effektív károkozást eredményez, amely a hálózat üzemeltetője és felhasználója számára érzékelhető hatásokban nyilvánul meg (adatvesztés, szoftver- és hardverhibák, hozzáférés-korlátozás stb.)

A számítógép-hálózati felderítésre és támadásra a támadó különböző eszközöket és módszereket alkalmazhat. A felderítés és támadás eszközei a kártékony rosszindulatú programok, más néven a malware-ek,[233] amelyek anélkül jutnak be a hálózaton keresztül a számítógépekbe, hogy arra a hálózat üzemeltetője vagy felhasználója engedélyt adott volna. A malware-ek a hálózatba való illetéktelen bejutástól kezdve, a működés megzavarásán és az adatlopáson keresztül a rendszer feletti vezérlés átvételéig számtalan rosszindulatú funkcióval rendelkeznek. A legismertebb malware-ek közé tartoznak többek között a számítógépvírusok, programférgek, trójai programok, jelszólopók, backdoorprogramok, zsarolóvírusok, spyware-programok, keyloggerek stb. A malware-ek terjedése rohamosan nő, naponta több tucat újfajta rosszindulatú program keletkezik, amelyek egyre nagyobb mértékű károkat okoznak. A hagyományos malware-ek mellett pedig az okostelefonok elleni mobilvírusok terjedése is egyre növekvő mérteket ölt. (Haig 2015)

A támadás során a különböző malware-eket használják fel a hálózatba való behatoláshoz, a működésének akadályozásához, megbontásához, illetve az adatokhoz való hozzáféréshez. A támadásra sokféle módszer és eljárás létezik, amelyek a malware-eken keresztül használják ki a hálózat sebezhetőségét. A teljesség igénye nélkül a legismer-

[232] Lásd az iráni atomreaktor urándúsító centrifugáját megrongáló Stuxnet nevű programféreg alkalmazását.

[233] Malicious Software – Malware.

tebbek például a túlterheléses támadások, adathalász-támadások vagy a mobilhálózatokat kihasználó közbeékelődéses támadások stb.

A számítógép-hálózati védelem a saját hálózat működésének és a benne tárolt adatoknak a védelmét jelenti a jogosulatlan behatolással és hozzáféréssel szemben. A védelem megvalósítható aktív és passzív védelmi eszközökkel, módszerekkel és technikákkal. A passzív védelmi módszerek és eszközök lehetnek például:

- a tűzfalak,
- a vírusirtók,
- a hozzáférés-szabályozás, valamint
- a behatolásdetektálás és -megelőzés.

Az aktív védelem közé sorolhatók:

- a megelőző támadások,
- az ellentámadások és
- az aktív megtévesztés. (HOLDAWAY 2001)

Az aktív védelem alkalmazása – azon túl, hogy szintén megnehezíti a támadónak a hálózathoz való hozzáférést – számos esetben tényleges károkozással is jár. Ebből adódóan e módszerek csak bizonyos helyzetekben és meghatározott feltételek megléte mellett alkalmazhatók. Ilyen például a katonai alkalmazás, amikor például a pusztító hatású kinetikus fegyverek alkalmazása is megengedett.

A számítógép-hálózati védelem módszereinek és eszközeinek együttes és komplex alkalmazása növeli a számítógép-hálózatok biztonságát. Eredményes védelem alkalmazása esetén biztosítható a CIA-alapelv, vagyis a hálózatban tárolt adatok esetében a bizalmasság (hozzáférés-védelem) és a sértetlenség (adatok törlése, módosítása elleni védelem), illetve a hálózati funkciók esetében a rendelkezésre állás (szolgáltatás működésének megakadályozása elleni védelem). (HAIG–VÁRHEGYI 2008)

A számítógép-hálózati műveletek a kibertérben alkalmazható képességek közül a legegyértelműbben kapcsolhatók a kibertéri műveletekhez, és teljes egészében részét képezik a kibertéri műveleteknek.

A kibertéri alkalmazhatóságát egyértelműen alátámasztja, hogy teljes mértékben hálózatos tevékenységet értünk alatta, amely a kibertér logikai rétegében zajlik, és hatása is zömében e rétegben jelentkezik. Meg kell jegyeznünk, hogy számos szakirodalom a kiberműveleteket vagy más szóhasználattal a *kiberhadviselést* tipikusan csak ezzel a képességgel azonosítja. Ez azonban, mint azt korábbiakban is kifejtettük, erős leszűkítését jelenti a kibertérben zajló információs műveleteknek.

4.2.3.3. Elektronikai hadviselés

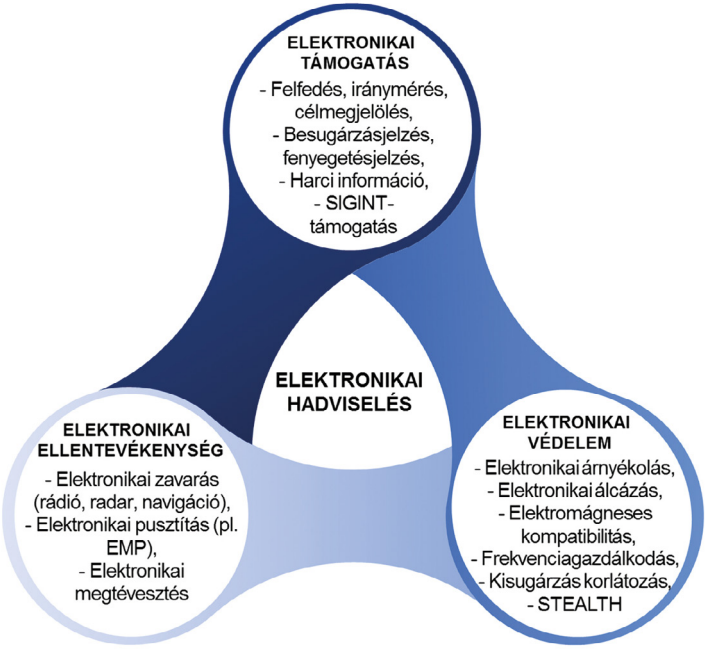
Az elektronikai hadviselés egy olyan műveleti képesség, amely az elektromágneses környezetben fejti ki hatását. Az elektronikai hadviselés létrejötte szinte egyidős a katonai rádióhíradás megjelenésével, hiszen már ekkor igényként jelentkezett a rádiótáviratok elfogása, lehallgatása, illetve a rádióösszeköttetések megzavarása. Az elmúlt több mint egy évszázadban a rádión kívül rendkívül sokféle új technológia jelent meg az elektromágneses térben, amelyek az elektronikai hadviselés fejlődését is alapvetően meghatározták (lásd I. fejezet).

Az MH Összhaderőnemi Elektronikai Hadviselési Doktrína meghatározása szerint: „az elektronikai hadviselés olyan hatás-alapú katonai tevékenységek/műveletek összessége, amelyek elektromágneses környezetben, az elektromágneses energia tudatos használatával biztosítják az elektromágneses műveletek részeként végrehajtott támadó és védelmi jellegű hatások/célok elérését”. [MD 3.6 (2), 12.] A definíció alapján az elektronikai hadviselés magában foglalja:

- az elektromágneses kisugárzások felkutatását, felfedését és azonosítását;
- az elektromágneses energia felhasználását a szemben álló fél elektromágneses spektrumban működő eszközei működésének korlátozása és akadályozása céljából, valamint
- a saját eszközök számára az elektromágneses spektrum használatának biztosítását.

Az elektronikai hadviselés egymással szorosan összefüggő területei az alábbiak (23. ábra):

- az elektronikai támogató tevékenység,
- az elektronikai ellentevékenység és
- az elektronikai védelem.



23. ábra

Elektronikai hadviselés

Forrás: a szerző szerkesztése

Az elektronikai támogató tevékenység egyfajta speciális felderítés, amely a szemben álló fél elektromágneses kisugárzásainak érzékelésével, azonosításával és azok felhasználásával célinformációt biztosít az elektronikai ellentevékenység és az elektronikai védelem végrehaj-

tásához. Az elektronikai támogatásnak célmegjelölő és fenyegetésjelző funkciója van. A célmegjelölő funkció azt jelenti, hogy felfedi és azonosítja a másik fél elektromágneses kisugárzásait, meghatározza a kisugárzó eszközök működési helyét, rögzíti és elemzi a vett jeleket, majd ezek alapján célinformációt biztosít az elektronikai ellentevékenységet végző erők és eszközök számára. Ezt a funkciót gyakran a rádióelektronikai felderítéssel közösen, ugyanazon eszközöket alkalmazva látja el. A fenyegetésjelző funkció során különféle besugárzásjelző szenzorokkal érzékelik a fenyegetést jelentő elektromágneses kisugárzásokat, amelyeket például egy radar- vagy infravörös önirányítású rakéta indítása és közeledése okoz. Ez alapján a rendszer kijelzi és azonosítja a különböző fenyegetéseket, illetve aktivizálja például egy repülőgép önvédelmi rendszerét.

Az elektronikai ellentevékenység az elektronikai hadviselés aktív támadóképessége, amely az elektromágneses energiát, benne az irányított energiákat is felhasználja a szemben álló fél elektronikai eszközei működésének korlátozására, akadályozására. Az elektronikai ellentevékenységnek három területe van:

- az elektronikai zavarás, amelynek során különféle zavaró berendezésekkel, például rádió-, radar-, navigációs stb. zavaró eszközökkel akadályozható vagy korlátozható a szemben álló fél elektronikai eszközeinek vagy rendszereinek hatékony működése;
- az elektronikai pusztítás, amely elektromágneses és egyéb irányított energiák, például elektromágneses impulzus fegyverek vagy önirányítású fegyverek alkalmazásával tartós vagy ideiglenes károkozást okoz a szemben álló fél elektronikai eszközeiben;
- az elektronikai megtévesztés, amelynek során az elektronikai kisugárzások manipulálásával, torzításával vagy imitálásával lehet befolyásolni a szemben álló fél elektronikai rendszereit, elsősorban felderítőeszközeit.

Az elektronikai védelem az elektronikai hadviselés azon területe, amely biztosítja az elektromágneses spektrum saját részről történő haté-

kony használatát a szemben álló fél elektronikai felderítése, támogató és ellentevékenysége, valamint a saját nem szándékos elektromágneses interferenciák ellenére is. Az elektronikai védelem aktív és passzív védelmi eszközök, tevékenységek, módszerek és rendszabályok alkalmazásával biztosítja a saját elektronikai berendezések és más technikai eszközök, valamint az előerő megóvását. Az alkalmazható eszközök és módszerek közé tartoznak például az álcázás, a rejtés, a kisugárzáskorlátozás, a frekvenciamenedzsment, az elektromágneses árnyékolások, továbbá a korszerű, kis valószínűséggel felderíthető adásmódok (például frekvenciaugratás) alkalmazása.

Az elektronikai hadviselés a hálózatos környezetben működő vezeték nélküli elektronikai rendszerek felderítése és célmegjelölése, az ellenük alkalmazott ellentevékenységi megoldások, valamint a saját eszközök védelme szempontjából alkalmazható a kibertéri műveletekben. Mivel ma a mobilhálózatos technológiák egyre nagyobb térnyerésének vagyunk tanúi, emiatt a kibertérben az elektromágneses spektrum szerepe egyre jelentősebbé válik. A hálózati kommunikációt biztosító vezeték nélküli megoldások, a mobiltávközlésben tapasztalható paradigmaváltozás, a vezeték nélküli szenzorhálózatok mind-mind potenciális célpontját jelentik az elektronikai hadviselésnek, mint ahogy azt a kibertér meghatározását tárgyaló 4.1.1. alfejezetben is kifejtettük. Ki kell azonban újra hangsúlyoznunk, hogy ennek ellenére még nem minden elektronikai eszköz és rendszer működik hálózatos környezetben (például RCIED-eszközök, hagyományos rádió és radarrendszerek stb.), ezért ezek a hagyományos értelmezésű elektronikai hadviselésnek képezik a célpontjait.

Az elektronikai hadviselés az információs környezet fizikai dimenziójában, azon belül is az elektromágneses spektrumban zajlik, és ott is fejti ki hatását. Ez alapján az infokommunikációs hálózatok elektronikai rendszereinek felderítése és az ellenük alkalmazható elektronikai támadási megoldások, valamint a saját hasonló elektronikai rendszerek védelmének színtere a kibertér fizikai rétege és az elektronikai hadviselés hatásai is e rétegben jelentkeznek.

4.2.3.4. Műveleti biztonság

A korszerű felderítő-, megfigyelő és célmegjelölő rendszerek napjainkban jelentős veszélyeket és fenyegetéseket jelentenek a saját erők és képességek számára. Amennyiben a szemben álló fél képes hozzáférni a saját fontos információinkhoz, és ezáltal megbízható ismeretekkel rendelkezik a saját erőink képességeiről, alkalmazási lehetőségeiről, akkor jelentősen csökkentheti a feladataink végrehajtásának sikerességét. Ennek megakadályozása a műveletek egyik fontos védelmi képessége, amely hozzájárul a saját erők megóvásához, és amelynek egyik alapvető módja a műveleti biztonság.

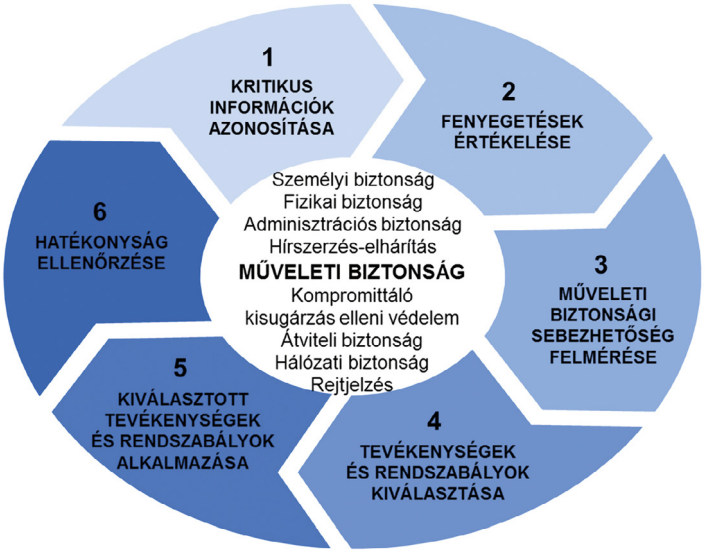
A műveleti biztonság olyan folyamatok, tevékenységek és rendszabályok összessége, amely meghatározza és folyamatosan kontrollálja a saját kritikus információkat, valamint aktív és passzív eszközök és módszerek alkalmazásával csökkenti annak kockázatát, hogy a másik fél kihasználja a sebezhetőségeinket. E képesség tehát egy olyan folyamatot takar, amely aktív és passzív eszközökkel és módszerekkel kockázatarányos biztonságot nyújt a saját erők alkalmazásához úgy, hogy megfosztja a szemben álló felet mindazon kritikus információktól, amelyek szükségesek számára a saját tevékenységének vezetéséhez, irányításához és végrehajtásához. (Haig–Várhegyi 2005)

A műveleti biztonság tehát nem más, mint:

- mindazon saját tevékenységek meghatározása, amelyek a szemben álló fél felderítő rendszereivel felfedhetők és megfigyelhetők;
- mindazon sebezhetőségek és kritikus információk meghatározása, amelyekhez a szemben álló fél hozzáférhet, és amelyek elfogadhatatlan kockázatot jelentenek a saját erők számára;
- mindazon tevékenységek és rendszabályok kiválasztása, végrehajtása, amelyekkel kiküszöbölhető vagy egy elfogadható kockázati szintre csökkenthető a saját tevékenységek és rendszerek sebezhetősége a felderítéssel és ellentevékenységgel szemben. (AR 530-1 2014)

A műveleti biztonság egy értékelő, elemző, tervező és ellenőrző folyamat, amelynek során meg kell határozni a leghatékonyabban alkalmazható biztonsági megoldásokat. A kritikus információkhoz való hozzáférés megakadályozására többféle tevékenység, intézkedés és módszer is alkalmazható. A teljesség igénye nélkül a legalapvetőbb módszerek közé az alábbiak sorolhatók:

- a személyi biztonság;
- az elektronikus információbiztonság:
  - az átviteli biztonság,
  - a kompromittáló kisugárzás elleni védelem,
  - a rejtjelzési biztonság,
  - a hálózati biztonság;
- a fizikai biztonság;
- az adminisztrációs biztonság és
- a hírszerzés-elhárítás.
- A műveleti biztonság egy ciklikusan ismétlődő tevékenységsor, amelynek megvalósítása során az alábbi, egymás után következő feladatokat kell végrehajtani (24. ábra):
- a kritikus információk azonosítása;
- a műveleti biztonságot érintő fenyegetések és kockázatok értékelése;
- a műveleti biztonsági sebezhetőség felmérése;
- a műveleti biztonság tevékenységeinek és rendszabályainak kiválasztása;
- a kiválasztott tevékenységek és rendszabályok alkalmazása; valamint
- a műveleti biztonság hatékonyságának ellenőrzése. (Haig–Várhegyi 2005)



24. ábra

A műveleti biztonság módszerei és folyamata

Forrás: a szerző szerkesztése

Mint láttuk, a műveleti biztonság lényege, hogy egy kockázatértékelési folyamat részeként meghatározza mindazon tevékenységeket és rendszabályokat, amelyek alkalmazása csökkentheti a másik fél felderítőtevékenysége által kihasználható sebezhetőségeket. A kibertéri műveletek szempontjából az egyes tevékenységek és rendszabályok meghatározása a lényeges, mivel ezek közül néhány alkalmazása kapcsolható a kibertér egyes rétegeihez.

Az információs műveleti képességek közül a műveleti biztonságnak van technikai és kognitív aspektusa is. A fizikai és logikai rétegben a műveleti biztonság technikai aspektusa az elektronikus információbiztonság egyes területeiben és rendszabályaiban jelenhet meg. A kibertér logikai rétegében alkalmazott hálózatbiztonság és a rejt-

jelzés például tipikusan kibertéri tevékenység, és szoros kapcsolatban áll a már korábban bemutatott számítógép-hálózati védelemmel.

A hálózatban alkalmazott elektronikai és informatikai eszközök működéséből fakadó nem szándékos elektromágneses kisugárzások elleni védelem vagy a vezeték nélküli átviteli csatornák védelme szintén a kibertéri védelmi megoldások részének tekinthetők. E védelmi tevékenységek az alkalmazható eszközök és rendszabályok vonatkozásában szoros kapcsolatot mutatnak az elektronikai védelemmel. Az egyes védelmi eszközök és technikák a kibertér fizikai rétegében alkalmazhatók, és hatásukat is ott fejtik ki. Emiatt az elektronikus információbiztonság információs műveleteknek megfelelő elvek szerinti összehangolása a számítógép-hálózati védelemmel és az elektronikai védelemmel elengedhetetlen.

A műveleti biztonság kognitív képességei is összefüggésbe hozhatók a kibertérrel. Itt elsősorban a felhasználók felkészítésére és biztonságtudatosságának fejlesztésére lehet gondolni. Ez alapvetően a hálózat használata során alkalmazott hozzáférési szabályok betartását, a jelszavak alkalmazását és kezelését, illetve a különféle biztonsági képzéseket jelentheti. A műveleti biztonság e területe mind megvalósítását, mind pedig hatását tekintve a kibertér kiberszemélyiség rétegéhez kapcsolható.

4.2.3.5. Megtévesztés

A megtévesztés a természet, az állatvilág és az emberiség létfenntartásának, túlélőképességének egyik fontos eleme. A megtévesztés egyidős az emberek közötti konfrontáció és háborúskodás kialakulásával. A másik fél megtévesztése, félrevezetése, becsapása a túlélési erőfeszítések során alakult ki, amely az évszázadok során a hatalom egyik kedvelt eszközévé vált, és amelyet az ember azóta is folyamatosan alkalmaz. A háborúkban a katonai megtévesztés csatákat eldöntő tényezőként jelenik meg, és gyakran kiemelkedő szerepet játszott a győze-

lem kivívásában. Jó példa erre a második világháborúban a normandiai partraszállás vagy az 1990-es első Öbölháborúban a szárazföldi műveletek előkészítése.

A megtévesztés alatt mindazon tevékenységek összességét értjük, amelyekkel a másik fél döntéshozói szándékosan félrevezethetők a saját képességeinket, szándékunkat, elhelyezkedésünket és műveleteinket illetően, és ezáltal a másik felet olyan helyzetbe hozzuk, hogy tetteivel vagy tétlenségével a saját céljaink eléréséhez járul hozzá. A megtévesztés a másik fél félrevezetését és hamis információval való befolyásolását jelenti, amelyet a saját lehetőségeinkről és várható tevékenységünkről szóló információk manipulációjával, torzításával vagy a tények meghamisításával lehet elérni.

A megtévesztés a fenti hatásokat csak abban az esetben képes elérni, ha a hamis információk, téves értékelések, következtetések a másik fél számára hihetőek, ellenőrizhetőek, más forrásokkal is megerősíthetőek és egyértelműek. A megtévesztés elsősorban a felderítés félrevezetésére szolgál, ezért a másik fél adatszerző képességének, adatfeldolgozási és döntési folyamatának megbízható ismerete a sikeres megtévesztés előfeltétele. (Haig–Várhegyi 2005)

A megtévesztés az elektronikai és informatikai rendszerek elterjedéséig hagyományos technikákkal valósult meg. A rádióhíradás, a radarok, majd később a számítógépek és hálózatok létrejöttével a megtévesztésben egyre nagyobb szerepet kaptak a technikai módszerek. Az első lépést az optikai felderítés ellen alkalmazott makettek jelentették, majd a rádiófelderítés ellen dezinformációs rádióadásokat alkalmaztak, illetve a rádiólokátorok ellen alkalmazott dipólokkal, illetve imitációs zavarokkal vezették félre a felderítő- és célkövető radarokat. A technikai eszközökkel folytatott megtévesztési technikák folyamatosan tökéletesedtek, és mára már a hálózaton keresztül a kibertérben is intenzív félrevezetési és befolyásolási módszereknek vagyunk tanúi. Ezzel a megtévesztés végleg kilépett a szűken vett katonai alkalmazási területről, és ma már a politikai és gazdasági életben is egyaránt alkalmazott információs tevékenységként értelmezhető.

A kibertérben a megtévesztés megvalósítható technikai és kognitív információs képességekkel, és alkalmazható ellentevékenységi módszerként, védelmi tevékenységként vagy kognitív befolyásolásra egyaránt. Az ellentevékenységi célú megtévesztési módszerek leggyakrabban az úgynevezett megszemélyesítés technikáját alkalmazzák. Ez a kibertér fizikai rétegében megvalósulhat például:

- légi célok imitálásával a radarok ellen alkalmazott válaszimpulzus zavarással;
- egy rádiórendszerben dezinformációs adások sugárzásával;
- a másik fél rádiórendszerébe való belépéssel, mintha a megtévesztő állomás annak egy vezető vagy tagállomása lenne;
- megtévesztő GPS-jelek sugárzásával,[234] aminek köszönhetően a GPS-vevő a pozíciót tévesen határozza meg stb.

A kibertér logikai rétegében a megtévesztés malware-ekkel vagy megtévesztő hálózati tevékenységgel valósítható meg. Ilyen eszközök és módszerek lehetnek például:

- trójai programok bejuttatása a számítógépes rendszerbe;
- IP spoofinggal, az adatcsomagot küldő személyazonosságának elrejtése vagy egy másik számítógépes rendszer megszemélyesítése;
- nigériai csalásokkal pénzadományok szerzése;
- phishingtechnikákkal[235] személyes adatok, belépési kódok, bankszámlaadatok megszerzése;
- man in the middle, azaz közbeékelődéses támadás, amelynek során a támadó kiadja magát egy hozzáférési pontnak, és ezáltal hozzáfér a kommunikációs csatornához stb.

A megtévesztés védelmi célú felhasználása az aktív védelem kategóriájába sorolható. Az aktív védelem az elektromágneses spektrumban már

[234] GPS spoofing.
[235] Adathalászat.

régóta használt megoldás. Idesorolhatjuk például a radarok ellen alkalmazható megelőző aktív elektronikai zavarást vagy a passzív dipólok kiszórását, illetve az infracsapdák kilövését. A kibertér logikai rétegében is alkalmazható módszer az aktív megtévesztés, amelynek egyik leggyakrabban alkalmazott megoldása a csali számítógépes rendszer, a honeypot. A honeypot egy olyan számítógépes rendszer, amely hálózati erőforrások, tevékenységek, adatbázisok és adatforgalmak szimulálásával a támadások detektálására szolgál. Hatékony működése esetén emellett információval szolgálhat a támadási kísérletekről, a sikeres támadásokról, a behatolások eszközeiről, a támadó szándékairól, valamint a valódi hálózat sérülékenységeiről is. (SZABÓ 2011) A honeypotnak nincs valós felhasználói szolgáltatása, így normál körülmények között nem küld és nem fogad adatcsomagokat. Amennyiben ez mégis bekövetkezik, az a támadás vagy jogosulatlan hozzáférés egyértelmű jelének tekinthető.

A megtévesztés a kibertéri kognitív befolyásolásnak is az egyik gyakran alkalmazott módszere. A kibertérben folytatott kognitív megtévesztés hatásos technikája a hamis hírek vagy mai közkeletű kifejezéssel az álhírek terjesztése, illetve a social engineering. Az álhírek napjainkban rendkívüli mértékben terjednek, amelyeket mind politikai, mind pedig gazdasági haszonszerzésre egyaránt felhasználnak. Az álhírek terjedésének a kibertéri hálózatos technológia rendkívül jó táptalajt biztosít. Az interneten keresztül terjesztett álhírek ma már szinte minden hírportálon több-kevesebb sikerrel megjelennek, és a felgyorsult hírversenynek köszönhetően kiszűrésük is egyre komolyabb problémát jelent a szerkesztőségek számára. Az álhírek nagy tömegekhez való eljutását jelentősen elősegíti az is, hogy az emberek a közösségi médiában igen gyakran ellenőrizetlenül osztják meg egymás között a híreket és így az álhíreket is.

A másik igen elterjedt kognitív befolyásolási technika a social engineering, amely az emberek hiszékenységét használja ki. A *social engineering* tulajdonképpen nem más, mint egy olyan pszichológiai művelet, amely általában nem valós tényeket, információt közvetít az áldozat felé annak

érdekében, hogy elnyerje bizalmát. E technika az emberek természetes, bizalomra való hajlamát használja ki a hálózatokba való bejutáshoz. Ezt a tevékenységet gyakran a kibertérben megvalósuló *pszichológiai manipulációnak* is nevezik, amely találóan írja le e technika lényegét. A manipulációra használt információnak köszönhetően egy hálózati jogosultsággal rendelkező felhasználó bizalmas adatokat ad át egy jogosulatlan személy számára, vagy lehetőséget biztosít a rendszerbe történő belépésre. Az így megszerzett információkat pedig eredményesen lehet felhasználni a különféle technikai jellegű támadási módszereknél. E tevékenység igen nagy szerepet játszhat abban, hogy a támadó megkerülhesse a különböző biztonsági megoldásokat, mint például a tűzfalakat vagy a behatolásdetektáló és -megelőző rendszereket.

A social engineering megvalósítható technikai és kognitív módszerekkel egyaránt. A technikai módszerek esetében a támadó közvetett módon a kibertér fizikai vagy logikai rétegében, valamilyen infokommunikációs eszközön keresztül lép kapcsolatba az áldozattal. Erre a célra alkalmasak az informatikai eszközökön létrehozott becsapós tartalmak, amelyek segítségével a kívánt információ egyszerűen megszerezhető. Ezek közé sorolható például az adathalászat körébe tartozó e-mail-alapú phishing, a VoIP[236] (hang)alapú vishing, az SMS-alapú smishing, illetve a vezetők infokommunikációs eszközeit célzó támadás, a whailing.

A kognitív módszerek alkalmazása során a támadó és az áldozat között közvetlen kapcsolat jön létre. E technikák közé sorolható például:

- a segítség kérése, segítség nyújtása, kölcsönösség kihasználása;
- a képernyőről adatok (például jelszavak) titokban történő lelesése;
- egy személyt követve, annak tudtával vagy tudtán kívüli bejutás egy helyiségbe, például irodába; illetve
- információk felkutatása a papírhulladékban. (Kovács 2012)

[236] Voice over Internet Protocol.

A kibertéri megtévesztés során alkalmazható ellentevékenységek, védelmi módszerek és befolyásoló technikák – mint láttuk – a kibertér mindhárom rétegében alkalmazhatók, és hatásuk is mindhárom rétegben jelentkezik. Ugyanakkor míg az ellentevékenység és a védelem során használt megoldások eredménye a fizikai és logikai rétegben jelentkezik, addig a kognitív megtévesztési technikák a kognitív dimenzióban, tehát a kiberszemélyiség rétegben fejtik ki hatásukat. A kibertérben megvalósuló megtévesztés – az információs műveletek alapelvének megfelelően – a pszichológiai műveletekkel, a műveleti biztonsággal, az elektronikai hadviseléssel és a számítógép-hálózati műveletekkel összehangolva, egymás hatásait kihasználva pedig még nagyobb hatékonyságot eredményezhet.

4.2.3.6. Pszichológiai műveletek

Mint azt korábban is már kifejtettük, napjaink katonai műveleteiben és tágabb értelmezésben mindenféle társadalmi tevékenységben az információs környezetnek meghatározó szerepe van. E környezet részét képező kognitív térben zajló tevékenységek mind a műveletek szempontjából, mind pedig politikai és gazdasági értelemben egyaránt jelentősek. A kognitív térben zajló információs tevékenységek egyik legjelentősebb hatásokat elérő képessége a pszichológiai műveletek vagy más kifejezéssel lélektani műveletek. A pszichológiai műveletek alapvetően azon a felismerésen alapulnak, hogy az ember személyére, tudati tevékenységére gyakorolt sajátos ráhatások eredményeként az egyén, a csoport vagy egy nagyobb közösség viselkedése, magatartása, attitűdje széles határok között alakítható és szükség szerint akár manipulálható is.

A NATO meghatározása szerint: „A pszichológiai műveletek olyan tervezett tevékenységek, amelyek a célközönség felé irányított kommunikációs módszereket és egyéb eszközöket alkalmaznak annak érdekében, hogy befolyásolják a politikai és katonai célok elérésére hatással lévő észlelési, megértési folyamatot, az attitűdöt és magatartást.”

(AAP-06 2014, 2-P-10) A definíció szerint tehát a pszichológiai műveletek alapvetően egyfajta speciális kommunikációs tevékenységek, amelyek arra irányulnak, hogy a szemben álló fél, a saját személyi állomány és a semleges érintettek kognitív folyamatait célzott üzenetekkel olyan módon befolyásolja, hogy az a saját politikai és katonai célok eléréséhez járuljon hozzá. A pszichológiai műveletek céljait az alábbiakban lehet összefoglalni:

- hatást gyakorolni a szemben álló fél gondolkodására, érzelmeire, befolyásolni viselkedését, szándékát;
- erősíteni a baráti, illetve a lojális lakosság szimpátiáját a politikai és katonai célok elérését szolgáló műveletek során;
- elnyerni az el nem kötelezett vagy határozatlan célcsoport támogatását és együttműködési készségét; valamint
- csökkenteni a szemben álló fél pszichológiai műveleteinek saját erőkre gyakorolt hatásait.

A fenti célok elérése érdekében alkalmazott pszichológiai műveletek sikere függ:

- a célközönség kiválasztástól és pontos meghatározásától,
- az üzenetek tartalmának összeállításától és
- az üzenetek eljuttatásának módjától.

A célközönség kiválasztása és meghatározása során figyelembe kell venni, hogy különböző politikai, társadalmi, kulturális, etnikai, vallási és katonai csoportok egyaránt potenciális célcsoportjai lehetnek a pszichológiai művelteknek. Ebből adódóan az alkalmazott eljárásoknak és az üzeneteknek szorosan illeszkedni kell a szemben álló fél és a műveleti területen élő lakosság kultúrájához, hitvilágához, vallási szokásaikhoz, nemzeti identitásukhoz és értékeikhez. Ezekre való tekintettel kell értékelni és meghatározni, hogy milyen lesz a kiválasztott célcsoport pszichológiai sebezhetősége. Ennek során meg kell állapítani:

- a célközönség meggyőzhetőségét;
- a célközönség akaratának, cselekedeteinek befolyásolhatóságát;

- a célcsoport elvárt reagálását és nem utolsósorban
- a célcsoport elérhetőségét a felhasználható média különböző típusaival.

Az üzenetek meghatározása során olyan hiteles témákat kell kiválasztani és a célcsoport sebezhetőségének megfelelően kidolgozni, amely hiteles, elfogadható és befolyásoló hatású. A NATO-elvek szerinti pszichológiai műveletek mindenkor valós információn alapulnak. Ebben alapvetően különbözik a megtévesztéstől, ahol épp ellenkezőleg, hamis információval érik el a célt. Mindezekre tekintettel, a témáknak:

- részletes háttér-információkra alapozottan valósnak, hitelesnek és ellenőrizhetőnek kell lenniük;
- támogatniuk kell a saját tevékenységet és a pszichológiai műveletek célkitűzéseit; továbbá
- olyan cselekvési irányt kell mutatniuk, ami észszerűnek és reálisnak tűnik a célcsoport számára. (Haig–Várhegyi 2005)

Az üzenetek eljuttatásának módja az elmúlt időkben jelentősen változott. Kezdetben a szóbeli kommunikáció, a röplapok, a nyomtatott médiatermékek, később a hangos beszélők jelentették az üzenet közvetítésének eszközeit. Mára az adott terület és a célcsoport infrastruktúrájától függően a legkorszerűbb infokommunikációs technológiák is felhasználhatók pszichológiai műveleti célokra. Természetesen ahol nincs kiépített információs infrastruktúra, elektronikus kommunikáció és internet, ott a hagyományos üzenetközvetítési módokat kell és lehet csak alkalmazni. Ahol viszont rendelkezésre állnak e technológiák, és az emberek nagymértékben használják mindennapjaikban az internetet és a közösségi oldalakat, ott a kibertéri pszichológiai műveletek jelentős eredményekkel kecsegtetnek. Ezt természetszerűleg felismerték a pszichológiai műveleteket folytató szervezetek, intézmények, de akár bűnöző csoportok és terrorista szervezetek is, és egyre intenzívebben kihasználják a bennük rejlő lehetőségeket.

A kibertéri megtévesztéshez viszonyítva alapvető különbség, hogy a kibertéri pszichológiai műveletek a legkorszerűbb hálózatos technológia felhasználásával valós információkra alapozott üzeneteket közvetítenek a kiválasztott célcsoport irányába. Az üzenetek továbbítására rádió- és tv-sugárzást, mobiltávközlést, illetve az internetes portálokat és a közösségi médiát használják fel. Emiatt a tevékenység a kibertér fizikai és logikai rétegében folyik, hatása azonban minden esetben a hálózatot használók tudatában, tehát a kiberszemélyiség rétegben jelentkezik.

4.2.3.7. Civil-katonai együttműködés

A megváltozott műveleti környezetben a katonai feladatok végrehajtása gyakran a műveleti területen élő lakosság és a közigazgatási szervek közreműködésével történik. A béketámogató és békefenntartó műveletek során a műveletekben részt vevő erőknek megfelelő kapcsolatot kell kialakítaniuk a civil szereplőkkel. Ha az elmúlt korok háborúit megvizsgáljuk, akkor láthatjuk, hogy a katonai és a polgári szervezetek között mindig is létezett kapcsolat. A 4. generációs műveletekben és a békeműveletekben azonban ez az együttműködés a katonai feladatok sikerének egyik alapvető fontosságú elemévé vált. Ma a haderők kibővült feladatrendszere egyre jobban igényli a polgári szféra bevonását a katonai feladatok végrehajtásába és a különböző civil szervezetekkel, intézményekkel való együttműködését. Emellett a helyi szervekkel és a lakossággal kialakított kölcsönösen jó kapcsolat nagymértékben növeli a semleges vagy ellenséges területen feladatot végrehajtó erők biztonságát. (Haig–Várhegyi 2005)

Az MH Összhaderőnemi Doktrína szerint a civil-katonai együttműködés „koordinálja a civil környezetet érintő tevékenységeket, illetve kiépíti és fenntartja az együttműködést a parancsnok és a katonai műveletek civil környezetét alkotó különféle civil szereplők (helyi lakosság; nemzeti és nemzetközi, kormányzati és nem-kormányzati szervezetek

és ügynökségek képviselői) között a támogatott parancsnok céljainak, küldetésének eredményes elérése érdekében". (ÁLT/43 2012) A civil-katonai együttműködés egy koordinációra épülő információs képesség, amely alapvetően az információs műveletek célközönsége közül a semleges érintettekkel, az állami és közigazgatási szervekkel közösen valósul meg. Hatékonyságát jelentősen befolyásolja, hogy milyen mértékben sikerül a megfelelő kapcsolatot kialakítani a helyi szervekkel.

A civil-katonai együttműködés célja egy olyan környezet kialakítása és fenntartása, illetve olyan feltételek biztosítása, amelyek segíthetik a katonai erőket a feladataik eredményes végrehajtásában. Minden területre kiterjedő együttműködés megteremtésére és fenntartására törekszik a műveleti területen élő helyi lakossággal és az intézményekkel annak érdekében, hogy olyan feltételek jöjjenek létre, amelyek a lehető legnagyobb erkölcsi, anyagi és katonai előnyöket biztosítják a műveletet végrehajtó erők számára. (HAIG–VÁRHEGYI 2005)

A civil-katonai együttműködés megvalósításának leggyakoribb és leghatékonyabb módja a személyes kapcsolatok kialakítása. Emellett napjainkban a kapcsolatépítésre jó megoldásokat nyújtanak a kibertérben alkalmazható hálózatos technológiák. Ezek közé tartozhatnak a mobiltávközlési lehetőségek, az elektronikus média nyújtotta szolgáltatások, az internetes portálok, weboldalak vagy a közösségi média felületei. A kibertér felhasználásával történő együttműködés és kapcsolat kialakítása során a fizikai és a logikai rétegben alkalmazott eszközök és módszerek kerülhetnek szóba, hatásuk viszont minden esetben a kiberszemélyiség rétegben jelentkezik. Ezek a kapcsolatteremtő, építő és együttműködési lehetőségeket biztosító megoldások azonban csak egy megfelelő hálózatos infrastruktúrával rendelkező területen alkalmazhatók. Emiatt megállapíthatjuk, hogy a civil-katonai együttműködés megvalósításában a kibertéri technológiák és módszerek a többi információs képességhez képest kevésbé játszanak szerepet.

4.2.3.8. Tömegtájékoztatás

A tömegtájékoztatás a 20. század elejétől fogva valamilyen formában folyamatosan jelen volt a katonai környezetben, ami gyakran konfliktusokhoz vezetett a katonai vezetés és a média között. Ugyanakkor a katonai szférának szüksége van a tájékoztatásra, hiszen a demokratikus társadalmakban a haderőnek minél átláthatóbbá kell tennie magát. Ezt az átláthatóságot többek között a média tudja biztosítani, amelynek köszönhetően növelhető a honvédelmi ágazat társadalmi elfogadottsága és pozitív megítélése. A katonai területen ennek biztosítására mára megjelent egy teljesen elfogadott információs képesség, amelyet a polgári tömegkommunikáció elméletből származtatva tömegtájékoztatásnak neveznek.

A tömegtájékoztatás rendszerint egy olyan egyirányú kommunikációs tevékenység, amely során az előre megszerkesztett üzenetek, hírek a média segítségével jutnak el a hallgatóság nagy tömegeihez. A tömegtájékoztatás megkülönböztető jellegzetessége másfajta kommunikációs módokkal szemben, hogy általában egyirányú kommunikációt jelent. Ezt a jellegzetességét napjaink internetes és közösségi médiát használó tájékoztató módszerei árnyalják, mivel egyre gyakrabban van lehetőség a hírekhez hozzászólni, véleményt alkotni, amely pedig már egyfajta visszacsatolást jelent az üzenet küldőjének. A tömegtájékoztatás fontos eleme, hogy a közlendő üzenet gondosan megszerkesztett, amely illeszkedik a hallgatóság befogadóképességéhez. Másik fontos eleme, hogy a személyközi kommunikációval ellentétben a tömegtájékoztatás egy adott médiumon keresztül a hallgatóság széles rétegeihez, egymástól szétszórtan található nagy tömegekhez juttathatja el az üzenetet.

A tömegtájékoztatás egy olyan háromelemű kommunikációs folyamat, amelyben először is szükség van egy úgynevezett adóra, aki a közlendő információt közzé szeretné tenni. Másodszor szükséges egy vevő vagy befogadó, aki az üzenetet veszi. A tájékoztatás hatékonysága szempontjából fontos a befogadó célcsoport meghatározása, akihez

az üzenetet az adó el kívánja juttatni. A célcsoport jellege, típusa, infrastrukturális ellátottsága megmutatja, hogy milyen kommunikációs technikát és médiumot célszerű alkalmazni az üzenet hatékony eljuttatására. A tömegtájékoztatás harmadik eleme a közvetítő, amely az üzenetet továbbítja a vevő, befogadó felé. Ezt a funkciót a különböző médiumok látják el. (HAIG–VÁRHEGYI 2005)

A tömegtájékoztatás közvetítőeszközeként kezdetben az írott sajtót használták, majd az elektronikus hírközlés fejlődésével megjelent a rádió és a televízió. A rádió- és tv-műsorok alkalmasak arra, hogy a befogadó célközönség világképét, társadalmi tudatát, világnézetét és végső soron a közvéleményt formálják. A hagyományos elektronikus média és műsorai csökkentik a nézők/hallgatók közötti véleménykülönbséget, viszont növelik az uniformizálás mértékét. Ez annak köszönhető, hogy a nézők, hallgatók leginkább csak passzív befogadók, csak azt látják a világ történéseiből, amit a média megmutat számunkra. Ezzel ellentétben az interneten megjelenő hírek világában a célközönségnek nagyságrendekkel nagyobb lehetősége van a sokszínű tájékozódásra.

A hagyományos elektronikus média még mindig jelentős szeletét képezi a tömegtájékoztatás médiaeszköztárának, azonban ma már a technológiai fejlődésnek köszönhetően az online média, a hírportálok, az internetes blogok, a közösségi háló (Twitter, Facebook) és a mobilkommunikáció jelentős előretörését tapasztalhatjuk. Az új hálózatos technológia adta rendkívül szerteágazó lehetőségek gyakorlatilag megszüntetik a személyközi és a tömegkommunikáció közti határokat. Az interneten megjelenő hírekhez ma már bárki a nagy nyilvánosság előtt szólhat hozzá, fejtheti ki véleményét, ami által a személyközi kommunikáció is tömeges jelleget ölt.

Az online média világában is egyre több hang és mozgóképi információ jelenik meg a különböző weboldalakon, egyes esetekben pedig az online média egyenesen átveszi a hagyományos tv- és rádióműsorsugárzás szerepét. Ma már igen sok rádió- és tv-társaság online módon vagy egy későbbi időpontban letölthető, archív formában is elérhetővé

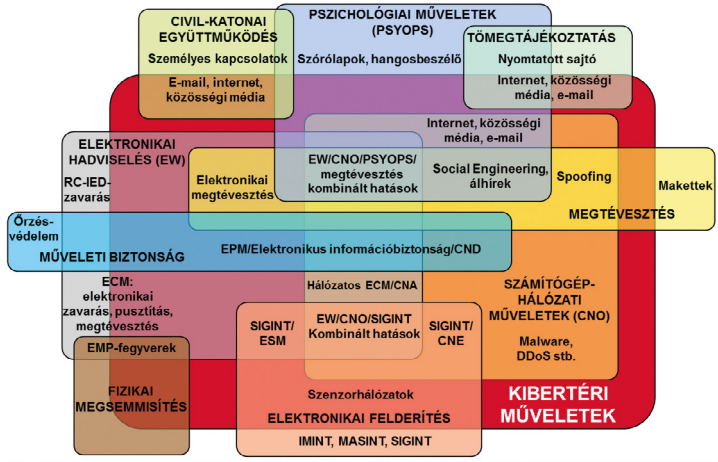
teszi műsorait. Ennek is köszönhetően az online média megváltoztatja az információhoz való hozzáférési szokásokat, mivel az interneten mindenki akkor juthat aktuális, naprakész információhoz, amikor éppen szüksége van rá. (Haig 2015)

Összegzésként megállapíthatjuk, hogy a tömegtájékoztatás napjainkban mind a polgári, mind pedig a katonai területen egyre inkább átvevődik az elektronikus média felületeire. A hagyományos elektronikus média még napjainkban is a legszélesebb rétegekhez elérő tájékoztatási forma, de emellett a kibertérben alkalmazható technológiák fokozott előretörését tapasztalhatjuk. Az internetes portálok, a közösségi média, a multimédiás felületek és a hagyományos hírszolgáltatók online tartalmai számos olyan előnnyel bírnak, amellyel a hagyományos média nem tud versenyezni. Ezek alapján a kibertérben értelmezett tömegtájékoztatás az alkalmazott média tekintetében a fizikai és a logikai rétegben valósul meg, hatása pedig minden esetben a kognitív dimenzióban, a kiberszemélyiség rétegben érezhető.

4.3. A kibertéri információs tevékenységek kölcsönhatása

A kibertérben zajló információs tevékenységek – az információs műveletek alapelvének megfelelően – igen gyakran szoros kapcsolódást, összefüggést mutatnak egymással, egymást részben átfedik, és kölcsönösen hatnak egymásra. Ez az egymásra hatás azt jelenti, hogy:

- egy kibertéri tevékenység egy másik tevékenységgel együtt alkalmazva eredményez összetett, megnövelt hatást, vagy
- egy kibertéri tevékenység egy másik fajta képesség esetében is értelmezhető, illetve
- a kibertér egy bizonyos rétegében végrehajtott információs tevékenység egy másik rétegben fejti ki hatását. Ezt a képességbeli átfedést és egymásra hatást szemlélteti a 25. ábra.



25. ábra

Kibertéri műveletek információs képességeinek kölcsönhatása

Forrás: a szerző szerkesztése

Az előző alfejezetekben megvizsgáltuk az információs műveletek technikai és kognitív információs képességeit. Következtetésként megállapítottuk, hogy azok megjelennek a kibertérben is, és egyre markánsabban kapcsolódnak a kibertéri műveletekhez. Ez a kapcsolódás lehet teljes körű, mint például a számítógép-hálózati műveletek esetében, vagy részleges. Ez utóbbi esetben a kapcsolódás lehet jelentős, több területen is megjelenő, mint például az elektronikai hadviselés, a műveleti biztonság vagy a megtévesztés esetében, vagy csak egy kis területet érintő, mint például a civil-katonai együttműködés során. Emellett a technikai és kognitív információs képességek között is felfedezhető az egymásra hatás, ami azt jelenti, hogy például egy technikai képesség által előidézett hatás a kognitív tartományban jelentkezik. A következő két alfe-

jezetben néhány példán keresztül bemutatjuk a technikai és a kognitív információs képességek kibertéri kapcsolódásait, és igazoljuk az egyes kibertéri tevékenységek közötti átfedéseket és egymásra hatásukat.

4.3.1. Kibertéri technikai információs képességek

4.3.1.1. Kibertéri technikai információs képességek egymásra hatása

A technikai információs képességeken belül a számítógép-hálózati műveletek egyértelműen csak a hálózatos környezetben zajlanak, ezért e tevékenységek teljes egészében részét képezik a kibertéri műveleteknek. A hálózati felderítő- és támadó műveletek során alkalmazott malware-ek, túlterheléses támadások (DDoS) és a vírusirtókkal, tűzfalakkal, kriptográfiával stb. megvalósított védelmi hálózati tevékenységek tipikusan eleget tesznek a kibertéri műveletek elvárásainak. E műveletek a klasszikus hálózati ellentevékenység keretében logikai úton idéznek elő működési zavarokat, leállást, adatvesztést stb. a hálózatban, illetve biztosítják a hálózat védelmét.

A vezeték nélküli hálózatok terjedése azonban kibővíti a hálózathoz való hozzáférés lehetőségeit. Mivel a kommunikáció az elektromágneses spektrumban zajlik, így a hálózatok e kommunikációs közegen keresztül is elérhetők, felderíthetők és akár korlátozhatók is. A SIGINT-technikákkal, azon belül is a rádiófelderítési módszerekkel eredményesen lehet hozzáférni e hálózatokhoz, lehallgatni az adatforgalmat, adatbázisokba lehet bejutni, bizalmas adatokat lehet megszerezni. Ahogy e hálózatok terjednek, a SIGINT egyre szorosabb kapcsolatba kerül a számítógép-hálózati felderítéssel, és így már a logikai hozzáférésen túl a kibertér fizikai rétegében is megvalósulhat a hálózatok lehallgatása.

A felderítésen túl tényleges károkozással járó támadás is megvalósítható a vezeték nélküli hálózatok ellen. Az elektronikai hadviselés keretén belül elektronikai zavarással lehet megbénítani a hálózati forgalmat, ami akár egy DDoS-támadásnak is felfogható azzal a különb-

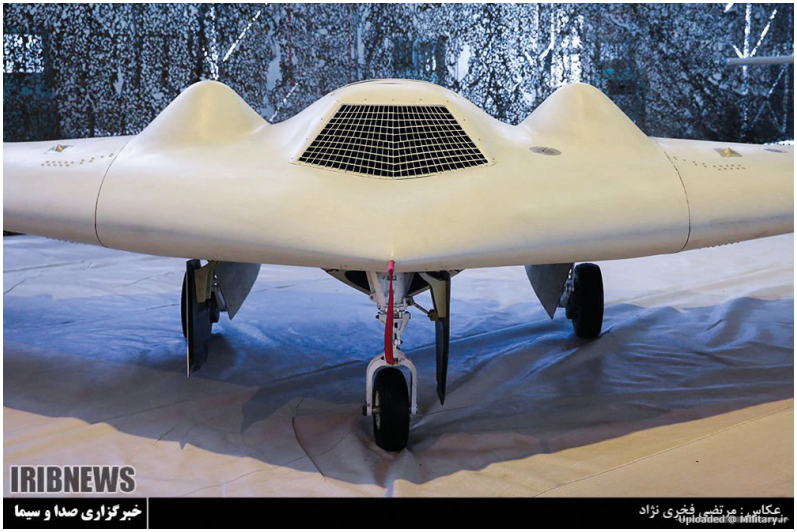
séggel, hogy ezt nem logikai úton, a szerverek tömeges lekérdezésével oldják meg, hanem a kommunikációs csatorna megzavarásával a fizikai rétegben kivitelezve. Az eredmény tulajdonképpen ugyanaz, a felhasználó nem tud hozzáférni a szolgáltatáshoz.

A hálózatos technológia egyre nagyobb részét kitevő IoT-rendszerekben és a szenzorhálózatokban például a szenzorok mint kiberfizikai eszközök korlátozása logikai támadással, kártékony programokkal vagy fizikai úton zavarással valósulhat meg. Mivel e rendszerek működésükből fakadóan vezeték nélküli kommunikációt használnak, ezért a malware-eket is az elektromágneses spektrumban, e kommunikációs csatornán keresztül lehet bejuttatni. Ezen kívül a szenzorok egymás közti, valamint a szenzorok és feldolgozóközpontok közötti rádiókommunikációja is zavarható.

A helyadatokat igénylő hálózatos rendszerekben, mint például az IoT vagy a felügyelet nélküli szenzorhálózatok műholdas navigációt (GPS, Glonass) alkalmaznak, amelyek a GPS-frekvenciákon célzottan zavarhatók, illetve megtéveszthetők. A megtévesztésre használt GPS spoofing[237] és a GPS meaconing[238] technikáknak köszönhetően a GPS-vevő hamis helyadatokat fog meghatározni. A működéséből fakadóan (kis jelszint, ismert frekvencia) a GPS rendszer mind a hagyományos, nagy teljesítményű célzott zavarással, mind pedig az előbb említett megtévesztés módszerével könnyen támadható. Ezt kihasználva, 2011 decemberében az irániak a GPS spoofing módszerével egy amerikai RQ-170 Sentinel fedőnevű pilóta nélküli repülőgépet (19. kép) térítettek el, és szállítottak le iráni területen. (Ványa 2015)

[237] Hamis C/A jelek sugárzása a vevő felé.

[238] A műholdról érkező jel késleltetett újrasugárzása.



19. kép

Az Iránban eltérített és leszállított RQ-170 Sentinel pilóta nélküli repülőgép

Forrás: REM-SENSE® (é. n.)

A GPS rendszerekhez hasonlóan a hálózatba kapcsolt légi irányítórendszerek, felderítő, légtérfigyelő és légvédelmi rádiólokátorok működése is eredményesen korlátozható elektronikai támadási módszerekkel. Nagy teljesítményű folyamatos zajzavarral lefoghatók a radarok, illetve válaszimpulzus-zavarással célokat lehet imitálni a vevőegységekben, amellyel megtéveszthető a felderítő és célkövető üzemmódjuk. Ezek már régóta ismert elektronikai ellentevékenységi technikák, amelyeket a korszerű szoftvervezérelt rádiók és radarok esetében a logikai támadásokkal kiegészítve, malware-ek bejuttatásával lehet még hatékonyabbá tenni.

Ezt támasztja alá például az az izraeli támadás is, amelyet egy szíriai nukleáris létesítmény ellen hajtottak végre 2007 szeptemberében.

Az izraeli légierő a szír hálózatos légvédelmi rendszer elleni kombinált támadásnak köszönhetően képes volt áthatolni a légvédelmi radarrendszeren anélkül, hogy felfedezték volna a behatolást. A támadás során a radarzavarással egy időben, a levegőből lefogták a rendszer rövid és ultrarövid hullámú kommunikációs csatornáit. Emellett pedig a hálózat adatkommunikációs csatornáján keresztül behatoltak a rendszer számítógép-hálózatába is. Ugyan a támadás részletei még titkos minősítésűek, de a legtöbb szakértő egyetért abban, hogy a légvédelmi rendszer lefogását a légi elektronikai hadviselés és a számítógép-hálózati támadás kombinációjával hajtották végre. (MacKenzie 2017; Ward 2017)

Ezzel pedig el is értünk a technikai módszerekkel megvalósított megtévesztés területére, amely szintén szoros kapcsolódást mutat egyes kibertéri műveletekkel. A megtévesztés történhet például hamis célok létrehozásával a radar vevőjében, vagy dezinformációs közlemények sugárzásával, illetve a kibertéren kívül, például makettek alkalmazásával. De a megtévesztés nemcsak az elektromágneses spektrumban valósítható meg, hanem a logikai rétegben a számítógép-hálózatok ellen is alkalmazható. Ennek támadó formája például a már korábban említett spoofing, amelynek során az adatok meghamisításával a támadó elfedi kilétét, vagy másnak adja ki magát, és így például jogosulatlan hozzáférés szerezhető bizonyos rendszerekhez. Ilyen ismert megtévesztő támadások például az IP spoofing, az ARP[239] spoofing vagy a MAC[240] spoofing.

Ez utóbbit a vezeték nélküli hálózatok ellen alkalmazzák rádiófrekvenciás csatornán keresztül. E hálózatokban egy másik igen elterjedt megtévesztési forma a man-in-the-middle, azaz a közbeékelődéses támadás, amikor a támadó egy nyilvános helyen egy vezeték nélküli hozzáférési pontot generál. A hálózatra ezen keresztül csatlakoznak fel az eszközök, aminek köszönhetően a kommunikációs csatorna lehallgatható, és így adatokhoz lehet hozzáférni.

[239] Address Resolution Protocol – ARP.
[240] Media Access Control – MAC.

A támadás mellett védelmi célra is alkalmazható a megtévesztés akár az elektromágneses tartományban, akár a logikai jellegű védelem esetében. Ez utóbbira példa a már korábban bemutatott megtévesztő hálózati tevékenység és forgalom, amelyet az úgynevezett honeypot hálózattal lehet megvalósítani, és amely szorosan kapcsolódik a műveleti biztonsághoz is. Emellett számos olyan műveleti biztonsági módszer, eljárás és technika is ismert, amelyek kapcsolódnak az elektronikai védelemhez vagy a számítógép-hálózati védelemhez. Ilyen például a hálózatban működő eszközök (monitorok, billentyűzet stb.) kompromittáló kisugárzás elleni védelme vagy az átviteli biztonság, amelyek a fizikai rétegben alkalmazott védelmi megoldások, és amelyek részét képezik az elektronikai hadviselésen belüli elektronikai védelemnek is. A logikai rétegben pedig a hálózatbiztonság és a rejtjelbiztonság értelmezhető, amelyek a számítógép-hálózati védelem alapvető védelmi módszerei is egyben.

A kibertérben alkalmazott támadások célpontjai között egyre nagyobb hányadot tesznek ki azok a különféle ipari, energetikai, egészségügyi, közlekedési stb. kiberfizikai rendszerek, amelyek ma már a hálózaton keresztül is elérhetők, és ipari irányítórendszereken[241] keresztül vezérelhetők. Ahogyan azt láttuk, az IoT-rendszerek elterjedése exponenciálisan növekszik, emellett pedig egyre több fizikai rendszert a hálózaton keresztül ipari irányítórendszerek vezérelnek. A kiberfizikai technológiák egy rendszerbe integrálják a fizikai működési folyamatokat, a számítási erőforrásokat és igen gyakran a vezeték nélküli kommunikációs képességeket.

Ez viszont jelentősen növeli e rendszerek kibertérbeli fenyegetettségét és a különböző fizikai hatások, működési zavarok bekövetkezését. E rendszerek elleni támadások megnyilvánulhatnak a fizikai eszközök tönkretételében, a számítástechnikai erőforrások elleni logikai támadásokban vagy a hálózati kommunikáció megakadályozásában, megzavarásában. Ezek alapján a szándékos támadások a kibertér logikai

[241] Industrial Control System – ICS.

és fizikai rétegében történnek. Mivel egy vezérlési folyamatot érintő logikai támadás, egy vírus bejuttatása a rendszerbe sokszor rádiófrekvenciás úton történik, ezért a támadáshoz gyakran mindkét réteget felhasználják. A támadás hatása pedig a fizikai térben érzékelhető, amely például a rendszer meghibásodásában, üzemzavarokban jelentkezik.

Marin Ivezic az elmúlt 35 évben 35 kibertéri incidenst azonosított, amelyek közül 21 volt célzott, szándékos károkozást előidéző támadás. (Ivezic 2017) Az első 1982-ben volt, amelyet a szibériai gázvezetékhálózat ellen hajtottak végre. Ezt követően a 2000-es években szaporodtak meg az ilyen jellegű incidensek. Ezek közül a legismertebb az iráni atomerőmű elleni támadás, amelyet a Stuxnet nevű programféreggel hajtottak végre. Hasonlóan nagy figyelmet kapott a 2016-os, BlackEnergy néven elhíresült ukrajnai energiaellátó rendszer elleni orosz hackerek által elkövetett támadás, amelynek következtében 80 ezer ember maradt villamosenergia-ellátás nélkül. Az incidenseket áttekintve megfigyelhető, hogy az utóbbi években jelentősen megnőtt a szándékos, célzott kibertámadások száma, ami arra enged következtetni, hogy a támadók a politikai, katonai és gazdasági célok elérése érdekében egyre gyakrabban nyúlnak az ilyen típusú fenyegetési formákhoz.

Mint az előbbi példákból is látható, a különféle információs tevékenységek sok területen illeszkednek a kibertéri műveletekbe, és sok esetben megfigyelhető közöttük az átfedés, egymásra hatás. Ezek a kibertér különböző rétegeiben érvényesülő, gyakran egymást kiegészítő tevékenységek együttes, összehangolt alkalmazása kombinált hatásokat eredményez, ami jelentősen növelheti a kibertéri műveletek eredményességét. Ezeknek az integráló hatásoknak a felismerése vezet oda, hogy több ország is olyan kibertéri műveleti képesség kialakítását tervezi, illetve kezdte meg, amiben integráltan jelennek meg a fizikai és a logikai rétegben alkalmazható kibertéri tevékenységek. Ez azt jelenti, hogy megkezdődött az elektronikai hadviselés, a rádióelektronikai felderítés és a számítógép-hálózati műveletek integrációs

folyamata, amelynek már doktrínákban és szervezetekben is megnyilvánuló eredményei is vannak.

4.3.1.2. Kína integrált hálózatos elektronikai hadviselési stratégiája

Az integrációs törekvésbe pontosan beleillik Kína integrált hálózatos elektronikai hadviselés stratégiája. Mint arra korábban a kínai információs hadviselési felfogás elemzésekor is rámutattunk, kínai teoretikusok már a 2000-es évek elején felismerték a vezeték nélküli hálózatok elterjedése és az elektronikai hadviselés közti összefüggést, miszerint a hálózati kommunikáció és ezáltal a számítógép-hálózatok az elektromágneses tartományban jelentősen korlátozhatók. Meglátásuk szerint a konfliktusokban az elektromágneses spektrum kihasználása gyakorolja a legnagyobb hatást a kibertéri műveletekre. A katonai műveletekben a hálózati tevékenység és az elektronikai hadviselés szervesen összekapcsolódik, és együttes hatásuk meghatározóvá válik.

Az integrált hálózatos elektronikai hadviselés lényege, hogy az infokommunikációs hálózatok fizikai elemei elleni támadást és védelmet a hálózati hadviselésbe integrálja. Ezzel az információs hadviselés tartományát és hatását kiterjeszti a korábbi felfogás szerinti virtuális világon túli fizikai valóságba, ahol a szenzorok, routerek és rádiókommunikációs eszközök működnek. A koncepció szerint a hálózati hadviselésre hatással vannak az elektromágneses spektrum felhasználására és uralmára irányuló erőfeszítések, az elektronikai rendszerek működését pedig közvetlenül befolyásolják a hálózatok működésének korlátozásával összefüggő tevékenységek. Az ellenséges rendszerek korlátozását célzó összehangolt tevékenységek során tehát a hálózati hadviselés és az elektronikai hadviselés kölcsönösen kiegészítik egymást. Ezáltal a két képesség egymás hatásait, technikáit és műveleti környezetét kihasználva, a kibertér fizikai és a logikai rétegében egymást kölcsönösen támogatva igen hatékony integrált kibertéri műveleti képességet alkotnak. (Cheng 2017)

A koncepciónak megfelelően a Kínai Népi Felszabadító Hadsereg vezérkara megkezdte az új koncepciónak megfelelő struktúra kialakítását. Ugyan egyértelmű szervezeti struktúra még nem került nyilvánosságra, de a kínai információs hadviseléssel foglalkozó kutatók tanulmányai alapján következtetni lehet az egyes területek felelősségi viszonyaira. (Sharma 2010) (Krekel et al. 2009) A vezérkar elektronikai ellentevékenységért felelős 4. igazgatósága már a 90-es évek végétől felügyeli az információs hadviselés területét is. Emellett a kutatások arra utalnak, hogy a számítógép-hálózati támadóképesség felügyeletét is ez az igazgatóság látja el. Az igazgatóságot pedig több éven keresztül az a Dai Qingmin vezérőrnagy vezette, aki az integrált hálózatos elektronikai hadviselés koncepcióját kidolgozta a kétezres évek elején. A vezérkar harmadik igazgatósága a rádióelektronikai felderítésért felel, és emellett a számítógép-hálózati felderítés és a védelem területét is vélhetően ez az igazgatóság felügyeli. A két igazgatóság kialakítása arra utal, hogy ugyan a támadó, valamint a felderítő- és védelmi képességek elkülönülten jelennek meg, de a kibertér fizikai és logikai rétegében zajló információs tevékenységek integrált, összehangolt alkalmazása képezi a kínai kibertéri tevékenység fő irányvonalát.

4.3.1.3. Az USA kibertéri és elektronikai hadviselési műveletek koncepciója

A technikai információs képességek kibertéri alkalmazásának szükségességét az amerikai katonai szakértők is felismerték, és megállapították, hogy az elektromágneses tartomány és a hálózatok működési tartománya között egyre jelentősebb átfedés tapasztalható. Ezt az átfedést az úgynevezett kiber-elektromágneses tartománnyal jellemezték, és az ebben zajló műveletekre 2014-ben megalkottak egy új műveleti elgondolást FM 3-38 *Kiber-elektromágneses tevékenységek*[242] címmel,

[242] *Cyber Electromagnetic Activities* (2014). [FM 3-38].

amely a szárazföldi haderő kibertéri műveleteinek koncepcióját adta. A doktrína érdekessége volt, hogy a kiber-elektromágneses tevékenységek közé a kibertéri műveleteken és az elektronikai hadviselésen kívül a spektrumgazdálkodási műveleteket is besorolta, ami az elektromágneses tartományban működő eszközök frekvenciamenedzsmentjét jelenti. A doktrína értelmezése szerint a kiber-elektromágneses tevékenységek integrálják és szinkronizálják e képességeket annak érdekében, hogy egymást kiegészítő és erősítő hatásokat lehessen elérni. Felismerték, hogy az e tevékenységek közötti koordináció hiánya csökkenti a hatékonyságot, emellett pedig konfliktusokat és kölcsönös interferenciákat eredményezhet az elektromágneses spektrumot használó eszközök és rendszerek között. (FM 3-38 2014)

Három évvel később, 2017-ben megjelent az integrációt még szorosabbra fonó FM 3-12 *Kibertéri és elektronikai hadviselési műveletek* doktrína. (FM 3-12 2017) A doktrína kiemeli, hogy a kibertérben és benne az elektromágneses spektrumban a szemben álló féllel szemben kialakított fölény döntő fontosságú a modern katonai műveletekben. Ezért a haderőnek képesnek kell lennie a hálózatos műveletek és az elektronikai hadviselési képességek kiaknázására. Mindez csak szoros koordinációval valósítható meg, ami a hálózatos képességek és az elektronikai hadviselés integrálását, egymáshoz való szinkronizálását jelenti.

A doktrína az információs környezetben meghatározza a kibertér három rétegét, a fizikai, a logikai és a kiberszemélyiség rétegeket, és a fizikai rétegben az elektromágneses spektrumot, ami az elektronikai hadviselés műveleti környezete. Részletesen tárgyalja a kibertéri és elektronikai hadviselési műveletek támadó és védelmi oldalát, az elérhető erőforrásokat és módszereket, valamint a tevékenységek koordinációját és tervezését. Meghatározza a tervezést végző Kiber-elektromágneses Tevékenység Munkacsoport[243] feladatait és a tervezés egyes lépéseit.

[243] Cyberspace Electromagnetic Activities Working Group.

A doktrína külön kihangsúlyozza az integráció szükségessége mellett a koordináció elmaradásából fakadó hátrányokat is. Felhívja a figyelmet, hogy emiatt a kibertéri tevékenységek hatékonysága elmarad a kívánt szinttől, és emellett jelentősen növelheti a műveletekben részt vevők közti belső konfliktusokat. Mindezeken túl a koordinálatlanság kölcsönös interferenciákat okozhat az elektromágneses spektrumot használó eszközök, rendszerek és szervezetek között.

Tanulmányozva a doktrínát megállapítható, hogy a kibertéri műveletek szempontjából az USA szárazföldi haderejében sem valósult meg még a teljes integráció. Ez abból is látható, hogy a doktrína külön-külön értelmezi és tárgyalja a két alapvető képességet, és csak a koordináció fontosságát hangsúlyozza. Ugyanakkor az is látható, hogy ahogyan a hálózati kommunikáció minél inkább a vezeték nélküli kommunikációra épül, és az elektromágneses spektrum egyre nagyobb szerepet kap a kibertérben, úgy egyre szorosabbá válik az integráció is. Megfigyelhető, hogy az elmúlt évek civil és katonai infokommunikációs hálózati fejlődésének tendenciája egyértelműen ebbe az irányba mutat, ami alapján prognosztizálható az egyre nagyobb mértékű átfedés.

Az is világosan látszik, hogy az amerikai felfogás szerint a kibertéri műveletek fejlesztésében az elektronikai hadviselés, a rádióelektronikai felderítés és a kibertéri hálózati műveletek eddigi különállásának megszüntetése az egyik legfontosabb prioritássá lépett elő. Ezt igazolja a doktrína címe is, amely egyértelműen utal arra, hogy a kibertérben az elektronikai hadviselés és a kibertéri hálózatos műveletek integrált és összehangolt tervezésével és alkalmazásával érhetők el az elvárt célok.

A doktrína fejlesztésén túl ezt támasztja alá az is, hogy 2016-ban a hadsereg vezérkarán, a G-3/5/7 hivatalon belül egy új igazgatóságot hoztak létre, amelynek feladata, hogy irányítsa a kibertéri képességek összehangolását. Patricia Frost vezérőrnagy, a hadsereg kiberigazgatója ezzel kapcsolatban kifejtette, hogy a kibertérben eddig tapasztalható hiányosságok kiküszöbölése érdekében olyan kultúraváltásra van szükség, amely megszünteti a hírszerzés, az elektronikai hadvi-

selés, a kiberműveletek és az információs műveletek eddigi szétválasztását. (JONTZ 2017)

4.3.1.4. Kiberparancsnokságok kialakítása

Ez az integrációs szándék a doktrínaalkotáson túl a szervezeti struktúrában is egyre inkább felfedezhető. Az Egyesült Államok az elmúlt két évtizedben folyamatosan fejlesztette a támadó és a védelmi kibertéri képességeit. Ennek egyik fontos lépése volt a Stratégiai Parancsnokság[244] alárendeltségében 2010-ben megalakított Kiber Parancsnokság,[245] amely központosította a védelmi és támadó kibertéri műveletek vezetését és irányítását, valamint a végrehajtó szervezeteket. E szervezet fő feladata, hogy az USA és a szövetségesei számára biztosítsa a kibertérben való cselekvési szabadságot, és ezzel párhuzamosan akadályozza a szemben álló felek ilyen lehetőségét. A Kiber Parancsnokság alárendeltségében mind a négy haderőnemnek saját kiberparancsnoksága működik. (USCYBERCOM 2016)

E szervezet komponensei közül terjedelmi korlátok miatt csak a Hadsereg Kiber Parancsnokságát[246] mutatjuk be röviden, amely jól szemlélteti a kibertéri integrált képességek strukturálását. A szervezet weboldalán található ismertető szerint a Kiber Parancsnokság az USA szárazföldi hadereje kibertérben folyó tevékenységének koordinálásáért és végrehajtásáért felelős szervezete, amely ellátja a hadsereg hálózatainak, adatbázisainak és kiberfegyver-rendszereinek védelmét. A parancsnokság vezeti és irányítja az integrált elektronikai hadviselési, információs és kiberműveleteket, és fenntartja a kiberbiztonságot. A Hadsereg Kiber Parancsnokságának feladatai közé tartozik:

---

[244] US Strategic Command – USSTRATCOM.
[245] US Cyber Command – USCYBERCOM.
[246] Army Cyber Command – ARCYBER.

- a hadsereg globális hálózatait érintő kibertéri fenyegetések folyamatos figyelemmel kísérése;
- együttműködve más szervezetekkel és ipari partnerekkel a kibertéri fölényképesség folyamatos fejlesztése;
- a hálózatok korszerűsítése és a védelmi kibertéri műveletek fejlesztése, illetve
- a támadó és védelmi jellegű kibertéri képességek alkalmazása a rosszindulatú fenyegetésekkel szemben.

A Hadsereg Kiber Parancsnokságának alárendeltségébe tartozik többek között:

- az 1. Információs Műveletek Parancsnokság,[247] amely két zászlóaljból áll, és többek között felelős a műveleti biztonság szervezéséért, az információs képességek, mint például elektronikai hadviselés, megtévesztés stb. képzéséért, felkészítéséért, gyakorlatok tervezéséért stb.;
- a Kibervédelmi Dandár,[248] amely a hadsereg hálózatainak kibervédelmét látja el; és
- a 780. Katonai Felderítő Dandár,[249] amely a rádióelektronikai felderítést és a kiberműveleteket végrehajtó két zászlóaljból áll. (ARCYBER é. n.; Army Cyber é. n.)

A feladatkör és szervezeti struktúra alapján látható, hogy a Kiber Parancsnokság az egyik alapvető szervezeti megtestesítője annak az erőfeszítésnek, amely például az FM 3-12 doktrínából is kitűnik, és amely a kibertérben folytatott különböző információs tevékenységek integrációját tűzi zászlajára. Láthatóan az információs műveletek több képessége is, mint például a műveleti biztonság, a rádióelektronikai felderítés és az elektronikai hadviselés – amely a felderítődandáron belül

[247] 1st Information Operations Command.
[248] Cyber Protection Brigade.
[249] 780. Military Intelligence Brigade.

található –, valamint a támadó és védelmi kiberműveletek összehangolt alkalmazása megjelenik a szervezetben.

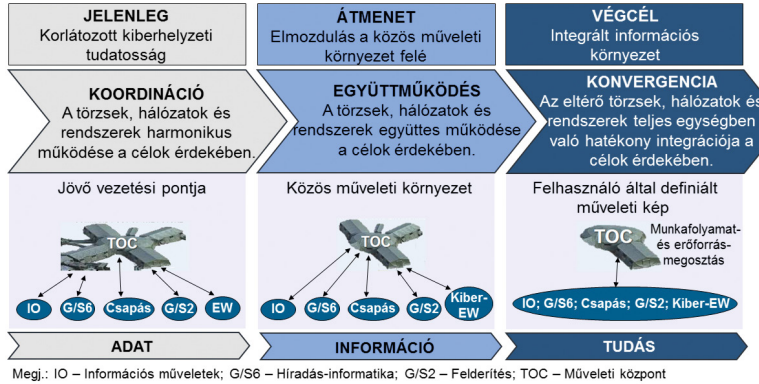
Emellett a Kiber Parancsnokság működteti a Kiber Kiválósági Központot[250] is, amelynek elsőrendű feladatköre a szinergikus hatások elérése érdekében a kibertéri tevékenységek és képességek összehangolása. E célból a központ részt vesz a doktrínafejlesztésben és a kibertéri műveleteket végrehajtó személyi állomány kiképzésében, felkészítésében. A központ parancsnoka, Stephen G. Fogarty vezérőrnagy ezzel kapcsolatban kijelentette, hogy a híradás, a kiberműveletek, az elektronikai hadviselés és a felderítés integrációja szempontjából a doktrína kidolgozás, valamint a képzés és felkészítés a központ egyforma fontosságú feladatát képezi. (Levering 2014)

Ezt a gondolkodást tükrözi a központ parancsnokának előadása is – amelynek lényegét a 26. ábra szemlélteti. Ebből látszik, hogy a jelenlegi helyzetből indulnak ki, a feladatok elosztására építenek; a kiberhelyzeti tudatosság még korlátozott, és egy átmeneti időszakot követően a végcél a teljes integráció megvalósítása. Az új doktrína és a Kiber Parancsnokság struktúrája már az átmeneti koncepciót testesíti meg, amelyben az egyes elemek, képességek bár még elkülönülten, de már egy közös műveleti környezet kialakítása irányába mozdultak el. A távolabbi végcél pedig a minden információs képesség teljes körű összeolvasztásával kialakított, integrált információs környezet elérése.

Hasonló stratégiai, doktrinális és struktúrakialakítási törekvések figyelhetők meg más NATO-országokban is, mint például Nagy Britanniában, Franciaországban és Németországban. 2012-ben a brit védelmi minisztérium alárendeltségében kezdte meg tevékenységét az Összhaderőnemi Kibererők Parancsnoksága,[251] amely vezető szerepet játszik a kibertéri képességek integrálásában és fejlesztésében. Franciaország 2017-ben hozta létre a Kibervédelmi Parancsnokságot,[252]

[250] Cyber Center of Excellence.
[251] Joint Cyber Forces Command.
[252] Commandement de Cyberdéfense.

amelyet 2019-ig 2600 szakemberrel töltenek fel, és akik közül közel 600-an a támadó kiberképességekre fókuszálnak. (Barbieri–Darnis–Polito 2018) Németország 2017-ben a Bundeswehren belül alakította ki a Kiber- és Információs Tér Parancsnokságot,[253] amelynek alárendeltségében többek között kiberműveleti, kibervédelmi, híradó és informatikai, technikai felderítő- és elektronikai hadviselési szervezetek, valamint képzést folytató iskolák találhatók. (Gotkowska 2017)



26. ábra

Az USA Hadsereg Kiber Parancsnokság integrációs folyamata

Forrás: Fogarty (2015) alapján a szerző szerkesztése

Összességében a kibertéri műveletekkel összefüggő stratégiai koncepciók és doktrínák, valamint a kiberszervezetek elemzése alapján egyértelműen megfigyelhető az a tendencia, amely a kibertérben alkalmazható információs tevékenységek szoros koordinációja és az együttes hatások elérésében rejlő előnyök kihasználása irányába mutat. A kibertéri technikai információs képességek integrációját – a hatásalapú megközelítés alapján – az egymásra gyakorolt hatások maximális kihasz-

[253] Kommando Cyber- und Informationsraum.

nálása indokolja. A vezeték nélküli hálózatos technológiák működési környezete jó lehetőséget teremt a rádióelektronikai felderítés, a számítógép-hálózati műveletek, az elektronikai hadviselés, illetve a műveleti biztonság és a megtévesztés technikai módszereinek összehangolt alkalmazására. A hálózatos technológia egy másik aspektusa, az emberek kibertérben való hálózatba szervezése lehetőséget biztosít arra, hogy a fizikai és logikai rétegben a technikai képességek alkalmazásával kognitív befolyásoló hatásokat eredményezzenek a kiberszemélyiség rétegben.

4.3.2. Kibertéri kognitív befolyásolás

4.3.2.1. Kibertéri kognitív információs tevékenységek egymásra hatása

Az információs műveletek képességei közül a kibertérben alkalmazható és hatásokat előidéző kognitív információs képességek közé a pszichológiai műveleteket, a tömegtájékoztatást és a civil-katonai együttműködést, illetve a megtévesztés és a műveleti biztonság humán oldalát soroljuk. Mint azt korábbiakban is elemeztük, a hálózatos technológia jelentősen kiterjeszti a kognitív hatásokat előidéző képességek lehetőségeit, alkalmazási módjait. Az internet és azon belül a közösségi média új lehetőségeket nyitott a kognitív befolyásolás terén, amit egyre nagyobb mértékben használnak ki az egyes szereplők. Ez azt jelenti, hogy a technikai képességeket, nevezetesen az internetes médiafelületeket és a közösségi szolgáltatásokat kognitív hatások előidézésére használják.

Svetoka és Reynolds szerint a hálózatos infokommunikációs technológiák – a hagyományos technikákhoz képest – a kognitív befolyásolás hatékonyságát jelentősen növelő alábbi sajátosságokkal rendelkeznek:

- *hozzáférhetőség:* a mobil eszközöknek, például okostelefonoknak köszönhetően az információ valós idejű gyűjtése, megosztása és elérése rendkívül egyszerűvé válik bárki számára;

- *sebesség:* az interneten és azon belül különösen a közösségi médiában nagy mennyiségű információ rendkívül gyorsan terjeszthető, emiatt pedig az információ hatása is nagyon rövid idő alatt jelentkezik;
- *anonimitás:* lehetővé teszi, hogy az emberek szabadon fejezzék ki véleményüket, így a névtelen felhasználóknak jó lehetőségük nyílik a célközönség manipulálására;
- *információdömping:* naponta hatalmas mennyiségű információ keletkezik, amelyek közül igen sok fontos lehet a széles nyilvánosság számára (veszélyjelzések, forgalmi információk stb.), de a legnagyobb mennyiséget a kevésbé releváns információk jelentik, amelyeket a közösségi média felhasználói állítanak elő. E hatalmas mennyiségből igen nehéz kiválogatni és megkülönböztetni a valós, hiteles és fontos információt a kevésbé fontostól vagy a valótlantól;
- *nincsenek sem földrajzi, sem pedig információtartalmi határok:* az interneten, a közösségi médiában és a blogokon bárki, bármilyen információt, hírt, posztot bármikor közzétehet, ma már ez nem pusztán a nagy hírszolgáltató szervezetek privilégiuma. Így azok a szereplők is (például kisebbségek, radikális és szélsőséges csoportok stb.), akik a hagyományos médiában nem tudnak megnyilvánulni, az új médián keresztül megoszthatják nézeteiket, véleményüket, és a közönség széles köreit érhetik el. (Svetoka–Reynolds 2016)

E sajátosságokat kihasználva a közösségi média számos előnyös tulajdonsággal bír, aminek köszönhetőnek az emberek bizonyos társadalmi kérdésekre, humanitárius segítségnyújtásra, katasztrófahelyzetek kezelésére könnyen mobilizálhatók. A kibertér befolyásolási célból való felhasználásának egyik legnagyobb előnye ugyanakkor, hogy a célok elérése érdekében összeállított üzenetek rövid idő alatt széles tömegekhez jutnak el. Ez egyrészt az internetes weboldalakon, portálokon közétett híreknek, üzeneteknek tulajdonítható, másrészt ezen információk

a közösségi oldalakon továbbadhatók a közösségi háló tagjai számára, aminek köszönhetően az információ terjedési sebessége és célcsoportja megsokszorozódik. Mindezeken túlmenően a véleményvezérek közösségi oldalakon keresztüli megcélzásával a befolyásuk alatt lévők jóval könnyebben elérhetők, az üzenetek is hatékonyabban célt érnek és érvényesülnek.

Ezen előnyöket kihasználva, a befolyásolás mindhárom formája, tehát a korábban már ismertetett megfelelés, az azonosulás és az internalizáció is hatékonyan alkalmazható a kibertérben. Közülük is az internalizáció – mint a leghatékonyabb befolyásoló technika – a kibertéri technológia felhasználásával jóval eredményesebben valósítható meg. A kibertérben alkalmazott kognitív technikákkal nagy hatékonysággal el lehet érni, hogy a befolyásolt személy teljes mértékben elfogadja, és onnantól fogva akár magáénak vallja a befolyásoló fél gondolatait. Ez a kibertérben megvalósítható olyan formában is, amikor a befolyásoló rejtve marad, és csak az üzenet önmagában fejti ki a hatást. A kibertér egy olyan szabályozatlan környezet, amelyben az anonimitás igen nagy lehetőséget biztosít a szélsőséges nézetek terjesztésére és akár a szándékos félretájékoztatásra is. Mindezt pedig anélkül lehet megtenni, hogy a befolyásolást végző felfedné kilétét.

Az előbb felsorolt sajátosságok alapján az internet és benne a közösségi média egyre inkább dominánssá válik a tájékoztatás területén is. A hagyományos tájékoztatásra szolgáló hírcsatornák (újság, tv, rádió) mellett, illetve lassan azokat háttérbe szorítva az internet biztosítja a leggyorsabb tájékozódási lehetőséget. Ugyanakkor a tömegtájékoztatás tájékoztató jellege átalakulóban van. A kimondottan tájékoztató funkciója kiegészül, és egyre gyakrabban jelenik meg a tájékoztatás mellett a befolyásolási funkció. Ez pedig azt is jelenti, hogy a tömegtájékoztatás és a pszichológiai műveletek, valamint egyre gyakrabban a megtévesztés (lásd álhírek) közötti határ elmosódik. Ezt a tendenciát pedig az interneten terjesztett hírek csak még jobban felerősítik. A hírverseny tipikus példája annak, ahogyan a hírszolgáltatók megpróbálnak versenyezni egymással, hogy ki tud gyorsabban friss, átütő híreket megjelentetni. Ez pedig azzal jár, hogy a hírek forrásának

és valódiságának ellenőrzése elmarad, így igen gyakran még a nagyobb hírportálokon is az álhírek a valódi hírek közé kerülnek. A közösségi hálón pedig a hír ellenőrzésének az igénye sem merül fel, a felhasználók kontroll nélkül osztják meg azokat.

A fentiekben leírtak alapján tehát megállapítható, hogy a kibertéri kognitív befolyásolás megvalósítható mind valós és hiteles, mind pedig valótlan, hamis információkkal. A valós információkon alapuló befolyásolás tulajdonképpen a pszichológiai műveletekkel, míg a hamis információkra épülő befolyásolás a megtévesztés technikáival érhető el. Mint ahogyan azt korábban is értelmeztük, a NATO által is vallott elvek szerint a klasszikus pszichológiai műveletek hangsúlyozottan csak valós és hiteles információra alapozva befolyásolják a célközönséget, de mint látjuk, a valótlan információk és álhírek egyre jobban tejednek, amelyekkel szintén komoly befolyásoló hatások érhetők el. Ez azonban a klasszikus felfogás szerint a megtévesztés területe közé tartozik, hiszen bár a végső cél a befolyásolás, de ezt félrevezetéssel valósítják meg. Mint arra korábban is rámutattunk, a kibertérben megvalósított kognitív megtévesztés két alapvető és leginkább alkalmazott fajtája a social engineering és az álhírek. Mindkét technika manapság virágkorát éli. Az ellenük való védekezésben pedig a műveleti biztonság kognitív oldala is jelentős szerepet kap, ami elsősorban a biztonságtudatos felhasználói magatartásban érhető tetten.

Láthatóan tehát a kibertéri kognitív információs tevékenységek szoros kapcsolatot mutatnak egymással. Az alkalmazott technikák mindegyike a kiberteret használja ki, azon belül is döntően az internetet és benne a közösségi médiát. Az egyes tevékenységek – bár taxonómiailag elkülönülnek egymástól – a következők: valós információra épülő pszichológiai műveletek, álhírekkel operáló megtévesztés, az egyre inkább határterületen működő tömegtájékoztatás. A hatások ugyanakkor mindegyik esetben a kognitív térben jelentkeznek, nevezetesen a kibertér kiberszemélyiség rétegének felhasználói és a közösségi komponenseiben, vagyis az emberek és a közösségek szintjén. Mindez

alapján pedig bizonyíthatóan megfigyelhető a kibertéri kognitív információs tevékenységek szoros egymásra hatása.

4.3.2.2. Álhírek a kibertérben

Ma a kibertérben megvalósuló kognitív megtévesztés nagyütemben terjedő fajtája az álhír. Álhírek korábban is léteztek, azonban az internet és a közösségi hálózat nyújtotta megoldások soha nem látott lehetőségeket adnak terjedésüknek. Ahhoz, hogy az *álhír* fogalmát megértsük, a *hír* fogalmából kell kiindulnunk. A magyar nyelv értelmező szótára szerint a hírnek többféle értelmezése van, függően attól, hogy milyen kontextusban használjuk. Könyvünk témája szempontjából kettőt emelünk ki: a hír „Vkiről, vmiről élőszóval vagy írásban küldött v. vitt értesítés; üzenet. […] A közzététel céljával írott, nyomtatott v. rádióban, televízióban bemondott rövidebb tudósítás, közlemény." (Bárczi–Országh 2016) Ez utóbbi meghatározás a lényegesebb a téma szempontjából, mivel ez alapvetően a médiában megjelenő hírre vonatkoztatható. A médiában megjelenő hír egy esemény kapcsán arra ad tényszerű választ, hogy ki, mit, mikor, hol, miért és hogyan tett, cselekedett. Vagyis a hír esetében a hangsúly a tényszerűségen van.

Az álhír ezzel szemben: „Téves értesülésből származó v. megtévesztés céljával terjesztett, valótlannak bizonyuló hír." (Bárczi–Országh 2016) E meghatározás alapján az álhír jellegét tekintve három kategóriába csoportosítható:

- téves hírforrásból, értesülésből származó, de jóhiszeműen és nem szándékosan terjesztett;
- téves hírforrásból, értesülésből származó és szándékosan, rosszhiszeműen, valamilyen ártó szándékkal terjesztett, illetve
- félrevezetés megtévesztés céljából előállított és szándékosan, ártó szándékkal terjesztett.

A megtévesztés keretében a pszichológiai befolyásolás céljából alkalmazott álhírekre egyértelműen ez utóbbi kategóriát lehet értelmezni. Ebből a megközelítésből az álhírek olyan előre eltervezett és szándékosan publikált, valótlan információkat tartalmazó hírek, amelyeknek célja elsősorban a félrevezetés. Ezeket a tartalmakat a készítőik általában valamilyen politikai befolyás megszerzésére vagy gazdasági haszonszerzésre használják fel. Összeállításukkor és megszerkesztésükkor általában az információ szenzációjellegére fókuszálnak, ami biztosítja az emberek figyelmének felkeltését.

Mint korábban többször is kihangsúlyoztuk, a pszichológiai műveletek valós és hiteles információval érik el befolyásoló hatásukat, míg a megtévesztés célja a félrevezetés, amelyet valótlan, hamis információ továbbításával, hozzáférhetővé tételével valósít meg. Megállapítható tehát, hogy ugyanazt a hatást nagyobb erőfeszítés árán valós információval, kisebb erőbefektetéssel, hamis álhírekkel is el lehet érni. Az eredmény ugyanaz, csak a megvalósítás módja különbözik. Talán pontosan ez ma az álhírek ilyen mérvű terjedésének az egyik oka, hogy ugyanazt az eredményt kevesebb erő- és eszközbefektetéssel, illetve nagyobb hatékonyságot ugyanolyan ráfordítással is el lehet érni.

Ebből a megfontolásból a hamis információn alapuló hírek – vagy ahogyan ma elterjedten használjuk, az álhírek – az internet előtt is jelentős szerepet játszottak a megtévesztési céllal folytatott kognitív befolyásolásban. A kibertéri technológiák, a bárki által létrehozott blogok, a hírversenyben lépést tartani akaró hírportálok és a közösségi média lehetőségei azonban jelentősen növelik az emberek félrevezetését célzó tevékenység hatékonyságát. Az ilyen híreket aztán az emberek a közösségi hálózaton tömegesen osztják meg egymással. Rohamos terjedésük így különösebb probléma nélkül megoldható, és ezáltal jól felhasználhatók például a politikai üzenetek széles nyilvánossághoz való eljuttatására.

A Trend Micro egy tanulmánya megállapítja, hogy a közösségi médiában megvalósított álhírkampányhoz három fontos összetevő szükséges. Mindezt a tűzháromszöghöz hasonlóan egymás kölcsönhatásában

értelmezi, és álhírháromszögnek nevezi (27. ábra). A három összetevő bármelyikének hiánya megnehezítheti, esetleg ellehetetleníti az álhírek hatékony terjesztését. Az összetevők az alábbiak:

- az online eszközök és szolgáltatások, akik és amik között megtalálhatók a fizetett trollok, követők, lájkolók, de alkalmaznak automatákat, botokat[254] is;
- a közösségi hálózatok, amelyek – köszönhetően annak, hogy az emberek egyre több időt töltenek el ezeken az oldalakon –, a legmegfelelőbb környezetét adják az álhírek terjesztésének, valamint
- a motiváció, amely a pénzbeli haszonszerzéstől kezdve a politikai célok eléréséig széles spektrumot fog át. (Gu–Kropotov–Yarochkin 2017)

27. ábra

Álhírháromszög

Forrás: Gu–Kropotov–Yarochkin (2017) alapján a szerző szerkesztése

[254] A botok alkalmasak szoftveresen bejegyzések megosztására, lájkolásra vagy Twitter-hashtagek felfuttatására.

Az álhírek rohamos terjedése az elmúlt néhány évben figyelhető meg egyértelműen. Az internet kiváló lehetőséget biztosít egyrészt a gazdasági célú, pénzszerzést, profitnövelést előtérbe helyező álhíroldalak kialakításának, másrészt a politikai célokat szolgáló álhírgyárak létrejöttének. Ma rengeteg olyan álhíroldallal találkozhatunk, amelyet pénzszerzési céllal üzemeltetnek. Ezek az oldalak szenzációhajhász, „kattintásvadász" címekkel operálnak, amelyekre rákattintva például olyan reklámokkal teletűzdelt oldalra vezetik az olvasót, amelyek bevételt termelnek az oldal működtetőjének. A felhasználók védelme érdekében már számos weboldal listázza ezeket az álhíroldalakat, de ennek ellenére számuk egyre növekszik.

Az álhírterjesztő oldalak gyakran a website spoofing technikát alkalmazzák. Az álhíroldalra csalogatás céljából a kattintásvadász linkek olyan URL-címekre mutatnak, amelyek egy-két betű eltéréssel megegyeznek egy neves és hiteles forrásnak tartott weboldal címével. A félrevezető URL-cím és az autentikusnak tűnő híroldalak ilyen kombinációja eredményesen téveszti meg a szenzációra éhes olvasókat. A múltban több ilyen oldal is működött, amelyek például az *MSNBC,* a *CNN* vagy az *ABC News* oldalakra hasonlítottak. Hazánkban is hatalmas mértékben terjednek az ilyen oldalak, amelyekre egyre többen hívják fel a figyelmet. A 20. kép például az *ABC News*-ra hasonlító, de már megszűnt álhíroldalt, illetve a nepszava.hu online oldalára hasonlító című és még mindig működő álhíroldalt mutat. A képeken jól láthatók az URL-címbeli eltérések a valódi oldalak címétől.

Társadalmi szempontból a politikai célú álhírek okozzák a legnagyobb problémát. Ezek egyik elterjedt formája az úgynevezett „álhírgyárak" által profin megszerkesztett, sorozatban generált és terjesztett álhírek. E területen Oroszország jár az élen. Az elmúlt években Oroszország számos alkalommal támaszkodott az ilyen álhírgyárak által szisztematikusan előállított és terjesztett hamis információkra. A legismertebbek talán a *Sputnik* és a *Russia Today* elektronikus médiumok, illetve a Szentpéterváron működő *Internet Kutató*

Ügynökség,[255] amelyeket már összefüggésbe hoztak az ukrajnai eseményekkel, a Krím félsziget annektálásával és a szíriai eseményekkel kapcsolatos információs befolyásolással, valamint az amerikai elnökválasztásba való beavatkozással is. (Chee 2017) Bár hivatalos kapcsolat nincs az IRA és a Kreml között, azonban az elmúlt években folytatott tevékenysége egyértelműen az orosz kormányzati érdekeket szolgálta. Megfigyelhető egyébként, hogy az orosz kormány a kibertéri műveleteket többnyire nem állami szereplőkkel valósítja meg. Ezáltal nem lehet a szoros kapcsolatot bizonyítani, és az állami szerepvállalás könnyebben letagadható.

20. kép

Az ABC News és a Népszava online oldalára hasonlító álhíroldalak

Forrás: anepszava.com; Hughes (2016) alapján a szerző szerkesztése

Az ügynökség fizetett trollok százait alkalmazza annak érdekében, hogy az orosz kormány számára kedvező álhírkampányt folytasson elsősorban a közösségi médiában. A trollok feladata, hogy erősítsék a politi-

[255] Internet Research Agency – IRA.

kai érdekeknek megfelelő gondolatokat, narratívákat úgy, hogy eközben negatív kommentekkel és álhírekkel ellehetetlenítik és gyengítik az ezzel ellentétes véleményeket. A trollkodás az internetes fórumokkal egyidős, azonban ilyen tudatos politikai célú alkalmazása csak az utóbbi években vált elterjedtté. (Kovács–Krasznay 2017) Mint utaltunk rá, a trollgyárat szoros összefüggésbe hozták az amerikai elnökválasztási kampánynyal is, aminek köszönhetően vált ismertté.

A félrevezetésre alapozott kognitív befolyásolás egyre hatékonyabb módszer a civil társadalom véleményének alakításában. Mindezt a kibertéri hálózatos technológiák és az ezek használatán alapuló közösségi hálózatok még jelentősebben felerősítik. Ezt a tendenciát igazolja az amerikai elnökválasztással összefüggésben a Cambridge Analytica botránya, miszerint a cég illegálisan 87 millió Facebook-felhasználó személyes adataihoz fért hozzá, amelyeket aztán Donald Trump elnökválasztási kampányában használtak fel. Emellett pedig egyre több bizonyíték lát napvilágot arról, hogy a valószínűsíthető orosz beavatkozás és választási manipuláció nagy része is a Facebookon keresztül történt.

A napokban, 2018 áprilisában zajlik éppen Mark Zuckerberg kongresszusi meghallgatása, ahol a Facebook alapítója és vezetője elismerte a Facebook szerepét az ügyben, és ígéretet tett arra, hogy komoly biztonsági intézkedéseket tesznek annak érdekében, hogy még egyszer ne fordulhasson elő hasonló eset. A biztonsági intézkedések többek között érintik az álhírek Facebookon való terjedésének megakadályozását is. Ezen intézkedések egyik első lépése közé tartozik, hogy megkezdték az orosz álhírgyár, az IRA bejegyzéseinek eltávolítását a közösségi oldalról. (Parham 2018)

Ugyanakkor az is érzékelhető, hogy a tömegesen nyilvánosságra kerülő álhírek és álhíroldalak, illetve a Facebook-botrány növelheti az emberek rezisztenciáját a hamis hírekkel szemben, illetve másik oldalról, már a valós híreket is kétkedéssel fogadják. Az álhírek terjedésével szembeni alapvető lépéseket részben a szolgáltatóknak kell megtenniük. Ebbe a sorba illeszkedik többek között az előbbiekben említett intézkedés, de ilyen kezdeményezés volt például a közösségi oldalak

azon szolgáltatása, miszerint a felhasználók megjelölhetik az álhírnek tartott bejegyzéseket. Emellett egyre több olyan oldal létezik, amelyek az álhírek leleplezésével, indexelésével foglalkoznak, mint például a Fact. Check.org, a Snopes.com vagy hazai vonatkozásban például a Hvg.hu és az Urbanlegends.hu folyamatosan frissülő oldalai.

A legfontosabb azonban, hogy az emberek ez irányú biztonságtudatossága is erősödik. Erre vonatkozóan már számos felvilágosító kampánnyal találkozhatunk, mint például a Könyvtári Egyesületek és Szervezetek Nemzetközi Szövetségének[256] felvilágosító plakátja (28. ábra), amelyet a Szövetség honlapján úgy propagálnak, hogy: „Töltsd le, nyomtasd ki, fordítsd le és oszd meg az otthonodban, a könyvtárban, a helyi közösségedben és a közösségi média hálózatokon!”[257] (IFLA 2017)

Az álhírek, vagyis a hamis információn alapuló kognitív befolyásolás a katonai műveletekben is alkalmazható információs műveleti technika. A műveletekben részt vevők ily módon szintén befolyásolhatók. A félrevezetésre alapozott tudati hatások előidézése nem új keletű. Az úgynevezett „fekete pszichológiai műveletek” például sokáig elfogadott technika volt az USA haderejében. A NATO-elvek szerint azonban ez nem elfogadott módszer, csak a valós és hiteles információn alapuló pszichológiai műveletek. Ha viszont e tevékenységet megtévesztési kategóriaként értelmezzük, akkor ez valóban egy hatékony befolyásolási módszer lehet. A hálózatos technológia és a közösségi média pedig, ahogy látjuk, ezt a hatékonyságot jelentősen tudja növelni. Ki kell azonban hangsúlyozni, hogy ez a megközelítés csak a szemben álló fél irányában alkalmazható, a semleges érintettek és a lakosság ilyen módszerekkel való befolyásolása nem megengedhető.

[256] International Federation of Library Associations and Institutions – IFLA.

[257] Fordította a szerző.

28. ábra

Az IFLA álhírek elleni kampányának felvilágosító plakátja

Forrás: IFLA (2017)

4.3.2.3. Kibertér és terrorizmus

A pszichológiai műveleteket vizsgálva megállapítható, hogy a kibertérben a korszerű hálózatos infokommunikációs technológia az információs műveletek e képességét is egy új dimenzióba helyezte. Ma már a pár évvel ezelőtt korszerűnek tartott rádió- és tv-műsor-szóráson alapuló, illetve az SMS-t[258] és MMS-t[259] használó propagandatevékenység sem tartozik a legkorszerűbb formák közé. A web2 szolgáltatásai, a multimédiás tartalmak, a blogok és a közösségi média megváltoztatta, és jelentősen növelte az üzenetek megfelelő célcsoportokhoz való eljuttatásának hatékonyságát. Ezt pedig a politikai ellenfeleken, reguláris katonai szervezeteken, titkosszolgálatokon kívül felismerték a különféle rossz szándékú emberek, csoportok, terrorista szervezetek is, és intenzíven fel is használják e médiát a céljaik eléréséhez.

Az internet és benne a közösségi média terrorista célú felhasználása alkalmas a nyilvánosság elérésére, a propagandaanyagok terjesztésére, adománygyűjtésre, toborzásra és mozgósításra, hálózatépítésre, adatbányászatra stb. (Kovács 2006) A terrorista szervezetek eredményesen kombinálják a modern multimédiás propagandát és a fejlett kommunikációt a kifinomult pszichológiai műveletek céljai érdekében. Weboldalakon, közösségimédia-felületeken tesznek közzé videó- és audiófelvételeket, fényképeket, illetve közleményeket. Bár a közösségi médiaszolgáltatók próbálják megakadályozni az ilyen jellegű tevékenységeket, sorra szüntetik meg a terrorista csoportok Facebook-, Twitter- és más közösségi oldalait, ennek ellenére újabb és újabb felületeket hoznak létre, amelyeken terjesztik ideológiájukat, és toborozzák újabb tagjaikat.

Gabriel Weimann rámutatott, hogy a terroristák internetfelhasználása exponenciálisan növekszik. Míg 1998-ban mindösszesen 12 terrorista weboldal volt a világhálón, addig 2015-re ez a szám 9800-ra emelkedett. (Weimann 2015) Ebben egyre jelentősebb hányadot tesznek ki a különböző

[258] Short Message Service – SMS.
[259] Multimedia Message Service – MMS.

közösségimédia-megjelenések. Az is megfigyelhető, hogy a web2-szolgáltatásokat elsősorban az újabb szerveződésű terrorcsoportok használják.

Az egyik legjelentősebb terrorszervezet az al-Káida, amelyik a legrégebb óta és a legszélesebb körben használja ki az internet nyújtotta lehetőségeket. Ugyanakkor az tapasztalható, hogy e szervezet sokáig még a hagyományos internetes technikákat használta: weboldalakon, fórumoldalakon keresztül terjesztette ideológiáját, illetve folytatott aktív propagandatevékenységet. Az al-Káida a pszichológiai hadviselés érdekében eredményesen használja ki a multimédiás tartalomszolgáltatás és a korszerű kommunikációs lehetőségeket. A terrorszervezet nagy hangsúlyt fektet emellett az onlinemagazin-típusú propagandára. Erre az egyik legalkalmasabb eszköze például az *Inspire* című angol nyelvű magazin, amely az ideológia terjesztésén és a propagandatevékenységen túl bemutatja a sikeres akciókat, illetve egyfajta kézikönyvként szolgál a terrorista támadási technikák kivitelezéséhez, például a házi készítésű robbanóeszközök előállításához. A 21. kép a magazin 2014. évi téli számának tartalomjegyzékét szemlélteti, amelyben például több propagandacikk, illetve egy házi készítésű bombaszakértővel készült interjú mellett a 66. oldaltól kezdve hosszú oldalakon keresztül azt mutatják be, hogy hogyan lehet összeállítani egy olyan bombát, amelyet el lehet rejteni a repülőtéri biztonsági átvizsgálás elől.

Az Iszlám Állam[260] az internet felhasználását az al-Káidától leste el, és hamar felismerte az új technológiában rejlő előnyöket. A közösségi média előretörésével tovább is lépett, és az egyik legaktívabb használójává vált az internet eme új médiájának. Gabriel Weimann szerint a közösségi oldalon keresztül kitűnően tudja érvényesíteni az úgynevezett narrowcasting technikát,[261] amelynek köszönhetően bizonyos ideológiailag érzékeny célközönséghez célzottan tudják eljuttatni üzeneteiket. (Weimann 2015)

---

[260] Gyakran az *ISIS* angol betűszóval is említik, amely az *Islamic State of Iraq and Syria* rövidítése.

[261] Egy műsorszóró médium használatát jelenti különleges érdeklődésű közönség célzott elérésére. Ezzel szemben a broadcasting a széles tömegekhez juttatja el az információt.

21. kép

Az Inspire magazin 2014. évi téli számának tartalomjegyzéke

Forrás: INSPIRE (2014)

Bányász Péter egy elemzésében rámutat, hogy az ISIS mennyire hatékonyan alkalmazza a multimédiás lehetőségeket. (BÁNYÁSZ 2016) A terrorszervezet propagandacélú és kivégzéseket bemutató vagy imitáló nagy felbontású videókat tesz közzé a közösségi videómegosztó oldalakon. Emellett a közösségi médiát előszeretettel használja toborzásra és hálózatépítésre. Mivel a közösségi oldalak igen kedveltek a nyugati fiatalok körében, ezt kihasználva számos fiatalkorút szerveztek be, akik – feladva addigi életvitelüket – az Iszlám Állam szolgálatába álltak. A kifejezetten fiatalok érdeklődésére számot tartó, profin előállított videókkal, hashtages Twitter-kampányokkal az ISIS-t egy fiatalos csoportként mutatják be. Ennek köszönhetően az elmúlt években több olyan híradás látott napvilágot, amely nyugati fiatalok beszervezéséről és a dzsihád szolgálatába állásáról tudósít. Weimann kutatásai

azt mutatják, hogy az elmúlt években 30 ezer külföldi, zömében fiatal csatlakozott az ISIS-hez. Ez egy rendkívül magas szám. Egyetlen terrorszervezet sem mondhatja el magáról, hogy a többnyire online toborzásnak köszönhetően ennyi, zömében nem iszlám vallású embert tudott volna a szolgálatába állítani. (Weimann 2015)

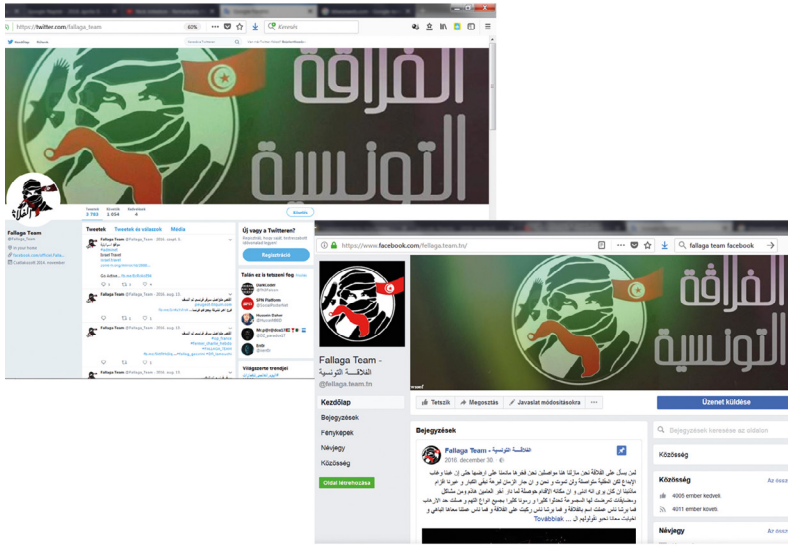
A fentiek alapján megállapítható, hogy mind ez idáig az interneten megnyilvánuló terrorizmus három szakasza azonosítható. Az első szakaszt a kezdetleges weboldalak passzív használata jellemezte. A második szakaszban, a 2000-es évek elején, a terroristák interaktív módon kezdtek el kommunikálni a szimpatizánsokkal. A weboldalak mellett csevegőszobákat és fórumokat használtak az ideológia terjesztését szolgáló propaganda céljára. A harmadik szakaszban pedig, a web2-szolgáltatások térnyerését követően elkezdték intenzíven használni a közösségi médiát. (Weimann 2015) A régebbi terrorszervezetek végigjárták mindhárom szakaszt, és például az al-Káida az Iszlám Államtól tanulta el napjaink új médiumának használatát. Az ISIS azonban szinte a kezdetektől intenzíven használja a közösségi médiát.

A különböző közösségi médiaszolgáltatók is felismerték, hogy a terrorizmus egyre nagyobb arányban használja e médiafelületet saját céljai elérése érekében. Emiatt a legtöbb szolgáltató – a biztonsági szervek nyomásának is eleget téve – beszüntette és törölte a terrorszervezetek fiókjait. Emiatt például a legtöbb terrorszervezeteknek ma már nincs sem Facebook-, sem Twitter-, sem Youtube-fiókja. Helyette a dark weben[262] mutatnak aktivitást, amelyet a keresőmotorok, például a Google nem indexel, és amit általában valamilyen illegális tevékenységre használnak.

Napjainkban azt tapasztalhatjuk, hogy a dark webet egyre inkább preferálják a terrorszervezetek, mivel az ottani online aktivitásuk rejtve marad a biztonsági szervek előtt, szemben a nyilvános webbel, ahol minden tevékenységük, bejegyzésük nyomon követhető. Weimann rámutat, hogy

[262] A dark web a deep web legmélyebb rétege, amely olyan illegális tartalmakat tartalmaz, amelyeket szándékosan elrejtettek, és amelyeket csak speciális böngészőkkel (például a TOR) lehet elérni.

a dark weben való megjelenés a párizsi terrortámadás után vált aktívabbá és egyértelműbbé. Az ISIS is elsősorban az internet e sötét tartományában folytatja propaganda- és toborzó tevékenységét. Médiakiadványa, az *Al-Hayet Media Center* készített például egy olyan útmutatót, amelyben bemutatják, hogy az érdeklődők, szimpatizánsok hogyan tudják elérni a dark weben lévő fórumokat. Mindezt pedig a Telegram nevű titkosított kommunikációs alkalmazáson keresztül terjesztették. (Weimann 2016):



22. kép

A Fallaga Team Twitter- és Facebook-oldala

Forrás: Fallaga Team Twitter (2018); Fallaga Team Facebook (2018)

Bár a terrorista szervezetek korábbi intenzív nyilvános weben való megjelenése visszaszorult, azért az megfigyelhető, hogy a kisebb szervezeteknek még mindig vannak internetes felületeik, gyerekeknek szóló weboldalakkal találkozhatunk, illetve a terrorizmussal szimpatizáló csoportok még mindig megtalálhatók a közösségimédia-felületeken. Példa-

ként hozható a Falaga Team, amely egy tunéziai iszlamista hackercsoport, és igen nagy aktivitást mutat a Facebookon, Twitteren (22. kép) és a Youtube-on egyaránt. A csoport magyar szempontból azzal vált híressé, hogy 2015-ben a röszkei menekülttáborban történt incidens[263] miatt törökországi IP-címről indítottak hackertámadást az N1TV ellen, amit a Fallaga Team vállalt magára. (HVG 2015)

Láthatóan tehát a terrorszervezetek intenzíven használják a kiberteret a céljaik eléréséhez. Birtokában vannak a legkorszerűbb hálózatos technológiának, és például a pénzügyi adományok egy részét is e technológia beszerzésére, fejlesztésére fordítják. Felismerték, hogy a pszichológiai befolyásolás egyik leghatékonyabb eszköze ma a kibertér és benne kiemelten a közösségi média. Az iszlám terrorizmus e technológia felhasználása tekintetében ugyanakkor egy elég sajátos helyzetben van, hiszen bár előszeretettel használják az internetet és alkalmazzák a modern infokommunikációs technológiát, ugyanakkor pedig a vallásukból és radikalizmusukból fakadóan elutasítják a modern életforma mindenfajta megjelenési módját. Legfőbb ellenségük is a nyugati társadalom, amely már évek óta alapvetően e technológia alapjain nyugszik, és fejleszti információs társadalmi jellegét.

Ma a terrorizmus elleni küzdelemben a hagyományos intézkedések mellett a kibertérben való védelemre és biztonságra is kiemelt figyelmet kell fordítani. A kormányoknak és a nemzetközi szerveknek olyan intézkedéseket, szervezeti struktúrákat kell kialakítaniuk, amelyek lehetővé teszik a terrorizmussal szembeni hatékony fellépést a kibertérben is. A szolgáltatókat folyamatosan rá kell kényszeríteni a nemkívánatos tartalmak, weboldalak, közösségimédia-fiókok eltávolítására. E tekintetben a korábbi évekhez képest már történt előrelépés. A terrorellenes szerveknek folyamatosan monitorozniuk kell a kibertéri aktivitást, fel kell térképezni a weboldalakat, közösségi médiafelületeket, figyelni kell

[263] Az N1TV riporternője a táborban menekülteket rugdosott, amiért jogerősen elmarasztalták. Később a Kúria bűncselekmény hiányában felmentette a korábban első- és másodfokon is garázdaságért elítélt operatőrt.

a rajtuk folyó információs tevékenységet, és meg kell tenniük a szükséges lépéseket. A nyilvános weben való aktivitás többek között ennek köszönhetően is visszaszorult, de mint látható, a kibertérben újabb és újabb lehetőségek nyílnak meg előttük, és találják meg a kapcsolattartás és kognitív befolyásolás új módjait és technikáit. A hatékony terrorizmus elleni fellépésben a nemzeti és nemzetközi szerveknek, hatóságoknak ezeket a kibertérben megjelenő kihívásokat is kezelniük kell.

Vákát oldal

Összegzés, következtetések

Az infokommunikációs technológia az elmúlt közel kétszáz évben hatalmas fejlődésen ment keresztül. Az elektronikus kommunikáció megjelenésének és intenzív fejlődésének köszönhetően az információ meghatározóvá vált a társadalmi, gazdasági, politikai folyamatokban és így a katonai műveletekben is. A távközlés és az elektronikai eszközökkel végzett adatszerzés, valamint más vezeték nélküli megoldások egyre nagyobb mennyiségű adat előállítását és továbbítását teszik lehetővé. A hatalmas mennyiségű adat kezelését pedig a számítástechnika fejlődése és a számítógépek összekapcsolása révén létrejövő hálózatok biztosítják.

A vezetékes és a vezeték nélküli hálózatok, valamint az azokban alkalmazott infokommunikációs eszközök korunk információs társadalmának működését és fejlődését meghatározó elemekké váltak. A hálózatok kialakítása, a gépek, kiberfizikai eszközök, valamint az emberek életének hálózatba szervezése minden korábbi képzeletet felülmúl. Mára értelmet nyer és beigazolódik Manuel Castells megállapítása, miszerint a 21. század társadalmában a kulcsfontosságú társadalmi rendszerek és tevékenységek az elektronikus információs hálózatok köré szerveződnek. Castells információtechnológia-paradigmájában az információ mellett a hálózatok kialakítása, a hálózatok rugalmassága és konvergenciája, valamint a technológiának köszönhetően a technikai eszközök mellett az egyének hálózatba kapcsolása is a társadalom működésének központi elemét képezi. (Kreisler 2001)

Napjaink infokommunikációs technológiai fejlődésének üteme és intenzitása minden eddigi léptéket felülmúl. Napról napra emelkedő ütemben növekszik a hálózatos formában előállított és kezelt adatok mennyisége. Az IoT-technológiával és a felhőalapú számítástechnikával fémjelzett, újfajta hálózatos megoldások azon túl, hogy generálják

a nagy mennyiségű adatokat, a korábbiakhoz képest hatékonyabb adattárolási és feldolgozási megoldásokat is kínálnak. Az IoT láthatóan az egyik nagy áttörést jelenti a mai és jövőbeni hálózatok fejlődésében. Az M2M-kapcsolatoknak köszönhetően a kiberfizikai tartományban működő különféle érzékelőkkel és beavatkozóelemekkel kialakított hálózatban megvalósul a teljes összekapcsoltság, amit jól szemléltetnek például az okosotthon- és okosváros-koncepciók.

A szenzorhálózatok, az IoT és a felhőtechnológia nyújtotta adatkezelési előnyök éreztetik hatásukat a védelmi szektorban is, különösen a katonai hálózatos technológiák terén. A katonai infokommunikációs hálózatépítési törekvésekben jól látható a polgári technológiák lassú, de fokozatos meghonosítása. A NATO Szövetséges Műveleti Hálózatának kialakítási elve a hálózatközpontú hadviselésre és a hálózatalapú képességek koncepciójára építve egyértelműen a polgári szférában már eredményesnek bizonyult megoldásokra utaló jegyeket hordozza. A hálózatalapú képességnek megfelelően az érzékelők, beágyazott eszközök, adatbázis-technológia és szoftverelemzés hálózatba való összekapcsolása szorosan tükrözi az IoT lényegét. Az IoT-elvű, nagy mennyiségű felügyelet nélküli érzékelőkből álló szenzorhálózat a korábbiakhoz képest lényegesen több adat megszerzését biztosítja a szemben álló fél helyzetéről, technikai eszközeiről, képességeiről, illetve a harctéri környezet változásairól. Ezek felhőalapú tárolása, feldolgozása és az információk megosztása pedig hatékonyabb vezetést és irányítást, illetve döntést tesz lehetővé.

Napjaink új, feltörekvő hálózatos technológiái érezhetően számos előnyös tulajdonsággal bírnak, amelyeket a katonai hálózatokban is eredményesen lehet alkalmazni. Ugyanakkor a jellemzően vezeték nélküli technológia sajátosságából fakadóan e hálózatok kialakítása és alkalmazása során többféle sebezhetőséggel is számolni kell. Az IoT és a felhőtechnológia katonai alkalmazása sokfajta kockázatot is hordoz magában, mint például a szenzorok adatainak módosítása, kompromittálása, az adatokhoz való illetéktelen hozzáférés, a hálózati kommunikáció megzavarása vagy a különféle beavatkozóelemeket vezérlő

parancsok megváltoztatása. Emiatt e hálózati megoldások biztonsági aspektusai a polgári felhasználások során is, de különösen a katonai alkalmazásokban kiemelt jelentőséggel bírnak.

Az infokommunikációs hálózatokkal szembeni fenyegetések az információs környezetből származnak. Katonai értelmezés szerint az e környezetben megvalósuló komplex információs tevékenységeket az információs műveletek koncepciója foglalja egy egységes rendszerbe. Az elmúlt több mint húsz év során az információs műveletek kezdeti elvei, képességei és megvalósulási formái folyamatos átalakuláson mentek keresztül. A koncepció lényege nem változott, vagyis a különböző információs képességek összehangolása és integrációja képezi ma is az információs műveletek lényegét.

A megváltozott műveleti környezet, a negyedik generációs hadviselés és a polgári szereplők megjelenése ugyanakkor jelentős hatással volt a technikai és a kognitív információs képességek szerepére és súlyára. A változás lényege, hogy a korábbi technikai szemléletű információs műveletek filozófiája átalakult, és ma már a kognitív képességek jelentősége ugyanolyan fontossággal bír. A másik fontos változás, hogy a hálózatos technológiák térnyerése miatt a kibertér mind a technikai, mind pedig a kognitív információs képességek terén egyre fontosabb szerepet kap az információs műveletekben.

Az elmúlt években a vezeték nélküli hálózatos technológiáknak és az emberek közösségi hálózatba szervezésének köszönhetően a kibertér értelmezése szintén megváltozott, kiszélesedett. Az újszerű megközelítésben a pusztán logikai felfogás mellett a fizikai tér, az elektromágneses spektrum és a kognitív tartomány is fontos részét képezi a kibertérnek. Ez az értelmezés lehetőséget nyújt arra, hogy a kibertéri műveleteket komplexebben értelmezzük, és az információs műveleteknél megszokott módon az integrált, egymás hatásait kihasználó technikai és kognitív információs képességeket is alkalmazzuk a kibertérben.

A kibertéri információs műveletek ezek alapján a kibertér alábbi rétegeiben valósulnak meg:

- a logikai rétegben a megszokott és az általánosan elfogadott számítógép-hálózatokban alkalmazott, logikai jellegű információs tevékenységekkel;
- a fizikai rétegben, vagyis az elektromágneses tartományban a felderítés, az elektronikai támadás, valamint a fizikai és elektronikai védelem módszereivel, továbbá
- a kiberszemélyiség rétegben, azaz a kognitív térben a valós és hiteles, valamint a félrevezető információn alapuló kognitív tevékenységekkel.

A kibertérben zajló információs tevékenységek ma már tehát túlmutatnak a konvencionális logikai információs módszereken, és a vezeték nélküli technológiák esetében hatékony megoldások alkalmazhatók az elektromágneses térben, valamint a közösségi média esetében a kognitív tartományban egyaránt. A kibertér újfajta értelmezésében, az emberek által létrehozott közösségi hálózati környezetben ráadásul sokkal eredményesebben lehet megvalósítani a kognitív befolyásolást. Mindezek mellett, köszönhetően a kibertér nyújtotta hálózatos lehetőségeknek, azt is tapasztalhatjuk, hogy az információs műveleti képességek és hatások a katonai műveleteken túl megjelennek a politikai és gazdasági konfliktushelyzetekben is.

A hálózatos technológiák evolúciójából, az információs műveletek fejlődéséből, illetve a kibertér és a kibertéri tevékenységek elemzéséből levonható következtetések, valamint az elmúlt évek megtörtént kibertéri eseményei alapján igazolható, hogy:

1. a hálózatok értelmezése mára alapvetően megváltozott, és kibővült a szokványos számítógép-hálózatokon túlmutató kiberfizikai eszközök hálózatával és az emberek által kialakított közösségi hálózatokkal;

2. az információs műveletek koncepciója átalakult, a képességekben kiegészült, a technikai és kognitív képességek egymással egyenrangúakká váltak;
3. a kibertér és az ott zajló tevékenységek értelmezése – köszönhetően a vezeték nélküli hálózatoknak és az emberek által kialakított közösségi hálózatoknak – kibővült: a fizikai, a logikai és a kognitív tartományai egyenrangú fontosságúakká váltak, amelyek mindegyikében kibertéri tevékenységek folytathatók;
4. a kibertérben egyaránt megjelennek a technikai és a kognitív információs képességek, bennük pedig értelmezhető az információs műveletek mindegyik képessége.

Mindezen információs tevékenységek pedig az információs műveletek alapelvének megfelelően jelentősen nagyobb hatékonyságot mutatnak, ha a kibertérben is egymással integráltan, összehangoltan vannak alkalmazva, és így felhasználhatók befolyásolásra, ellentevékenységre és védelemre egyaránt.

Vákát oldal

Irodalomjegyzék

11 IoT (2015): *11 Internet of Things (IoT) Protocols You Need to Know About* (2015). Elérhető: https://www.rs-online.com/designspark/eleven-internet-of-things-iot-protocols-you-need-to-know-about (A letöltés időpontja: 2018. 04. 27.)

1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról

60/2013. (IX. 30.) HM utasítás a Magyar Honvédség Kibervédelmi Szakmai Koncepciójának kiadásáról

AAP-06 (2014): *NATO Glossary of Terms and Definitions (English and French).* Elérhető: http://wcnjk.wp.mil.pl/plik/file/N_20130808_AAP6EN.pdf (A letöltés időpontja: 2018. 04. 27.)

Ács Gergely – Buttyán Levente (2007): A Taxonomy of Routing Protocols for Wireless Sensor Networks. *Híradástechnika,* 62. évf. 1. sz. 32–40.

AEHF (é. n.): *Advanced EHF Payloads.* Elérhető: http://www.northropgrumman.com/Capabilities/AdvancedEHFPayloads/Pages/default.aspx (A letöltés időpontja: 2018. 04. 27.)

AFDD 2-5 (1998): *Information Operations. Air Force Doctrine Document.* Elérhető: http://webapp1.dlib.indiana.edu/virtual_disk_library/index.cgi/4240529/FID2862/pdfdocs/jel/service/afdd2_5.pdf (A letöltés időpontja: 2018. 04. 27.)

AI MK. VIII (é. n.): Royal Air Force Radar, 1939–1945. *Wikimedia Commons.* Fotó © Royal Air Force official photographer (a kép publikus felhasználású). Elérhető: https://commons.wikimedia.org/wiki/File:AI_Mk._VIIA_radar_in_Bristol_Beaufighter_VIF_CH16665.jpg (A letöltés időpontja: 2018. 04. 27.)

AJP-3.10 (2009): *Allied Joint Doctrine for Information Operations.* Elérhető: https://info.publicintelligence.net/NATO-IO.pdf (A letöltés időpontja: 2018. 04. 27.)

AJP-3.10 (2015): *Allied Joint Doctrine for Information Operations.*

Akyildiz, Ian F. – Vuran, Mehmet Can (2010): *Wireless Sensor Networks.* Chichester, Wiley.

Alberts, David S. – Garstka, John J. – Stein, Frederick P. (1999): *Network Centric Warfare: Developing and Leveraging Information Superiority.* [h. n.], CCRP Publication Series.

Ált/27 (2007): *Magyar Honvédség Összhaderőnemi Doktrína* (2007). 2. kiadás. A Magyar Honvédség kiadványa.

Ált/43 (2012): *Magyar Honvédség Összhaderőnemi Doktrína* (2012). 3. kiadás. A Magyar Honvédség kiadványa.

Ált/57 (2014): *Információs műveletek Doktrína* (2014). 1. kiadás. A Magyar Honvédség kiadványa.

Anand, Vinod (2006): Chinese Concepts and Capabilities of Information Warfare. *Strategic Analysis,* Vol. 30, No. 4.

AR 530-1 (2014): *Operation Security* (2014). Washington, D.C., Headquarters Department of the Army.

ARCYBER (é. n.): *U.S. Army Cyber Command.* Elérhető: http://www.arcyber.army.mil/Organization/About-Army-Cyber (A letöltés időpontja: 2018. 04. 27.)

Army Cyber (é. n.): *About Army Cyber Command.* Elérhető: https://www.goarmy.com/army-cyber/about-army-cyber-command.html (A letöltés időpontja: 2018. 04. 27.)

Arold, Uku (2016): Peculiarities of Russian information operations. *Sõjateadlane Estonian Journal of Military Studies,* Vol. 6, No. 2. 13–41.

ARPANET 1974 (2007): Symbolic representation of the Arpanet as of September 1974. *Wikimedia Commons.* © Yngvar. Elérhető: https://commons.wikimedia.org/wiki/File:Arpanet_1974.svg (A letöltés időpontja: 2018. 04. 27.)

Balás B. Dénes (2009): *A távírótól a rádióig – A rádiótechnika története az 1800-as évektől a II. világháborúig.* Budapest, Ad Librum.

Baló György – Lipovecz Iván szerk. (1988): *Tények könyve 1988.* Budapest, Computerworld–Móra. Elérhető: http://www.arcanum.hu/hu/online-kiadvanyok/TenyekKonyve-tenyek-konyve-1/1988-2/technika-tudomanyok-206A/a-szamitastechnika-tortenete-2238 (A letöltés időpontja: 2018. 04. 27.)

Balogh Fatime et al. (2015): A hibrid hadviselés különös tekintettel a mobil kommunikációra. *Hadmérnök,* 10. évf. 4. sz. 127–137. Elérhető: http://www.hadmernok.hu/154_12_balogf_na_joe.pdf (A letöltés időpontja: 2018. 04. 27.)

Bánlaki Pál – Lovas Antal (2012): *Szenzorika és anyagai.* Budapest, Typotex.

Bányász Péter (2016): A közösségi média szerepe a lélektani műveletekben az elmúlt időszak válságainak tükrében. *Szakmai Szemle,* 13. évf. 1. sz. 61–81.

Baocun, Wang – Fei, Li (1998): Information Warfare. In Pillsbury, Michael ed.: *Chinese Views of Future Warfare.* Washington D.C., National Defense University Press. 327–341.

Barbieri, Cristian – Darnis, Jean-Pierre – Polito, Carolina (2018): Non-proliferation Regime for Cyber Weapons. A Tentative Study. *Documenti IAI,* 18/03. Elérhető: http://www.iai.it/sites/default/files/iai1803.pdf (A letöltés időpontja: 2018. 04. 27.)

Bárczi Géza – Országh László szerk. (2016): *A magyar nyelv értelmező szótára, I–VII. kötet.* Elektronikus kiadás (első kiadás: 1959–1962). Budapest, Akadémiai Kiadó. Elérhető: http://mek.oszk.hu/adatbazis/magyar-nyelv-ertelmezo-szotara/elolap.php (A letöltés időpontja: 2018. 04. 27.)

Bartolits István (2000): *A távközlés regénye.* Elérhető: http://w3.tmit.bme.hu/thsz/TavkReg.pdf (A letöltés időpontja: 2018. 04. 27.). Eredeti megjelenés: Élet és Irodalom, 44. évf. 19–28. számok.

Beckh, Joachim (2005): *Blitz & Anker.* Band 2. *Informationstechnik, Geschichte & Hintergründe.* Norderstedt, Books on Demand.

Bognár Eszter (2017): Az elektronikai felderítés korszerű eszközei: felügyelet nélküli szenzorhálózatok. *Hadmérnök,* 12. évf. 1. ksz. 190–203. Elérhető: http://hadmernok.hu/170k_15_bognar.pdf (A letöltés időpontja: 2018. 04. 27.)

Boland, Rita (2013): Changing the Course of Coalition Connectivity. AFCEA.org, 2013. 05. 01. Elérhető: https://www.afcea.org/content/Changing-Course-Coalition-Connectivity (A letöltés időpontja: 2018. 04. 27.)

Broadway (é. n.): View of Broadway, north from Cortlandt and Maiden Lane, New York City, c. 1885–87. *Wikimedia Commons.* (A kép publikus felhasználású) Elérhető: https://commons.wikimedia.org/wiki/File:Broadway-1885-APL.jpeg (A letöltés időpontja: 2018. 04. 27.)

Browser Statistics (2017): https://www.w3schools.com/browsers/default.asp (A letöltés időpontja: 2018. 04. 27.)

Bussell, Jennifer (2013): Cyberspace. *Britannica.com,* 2013. 03. 12. Elérhető: https://www.britannica.com/topic/cyberspace (A letöltés időpontja: 2018. 04. 27.)

Callaway, Edgar H. Jr. (2003): *Wireless Sensor Networks: Architectures and Protocols.* New York, Auerbach.

Carberry, Sean D. (2017): Army and IBM head to the cloud. *FCW.com,* 2017. 01. 26. Elérhető: https://fcw.com/articles/2017/01/26/army-cloud-ibm-carberry.aspx (A letöltés időpontja: 2018. 04. 27.)

Cebrowski, Arthur K. – Garstka, John J. (1998): Network-Centric Warfare: Its origin and future. *US Naval Institute Proceedings Magazine,* Vol. 124/1/1, No. 139. 28–35.

Chain Home (1945): Chain Home radar installation at Poling, Sussex, 1945. *Wikimedia Commons.* Fotó © Royal Air Force official photographer (a kép publikus felhasználású). Elérhető: https://commons.wikimedia.org/wiki/File:-Chain_Home_radar_installation_at_Poling,_Sussex,_1945._CH15173.jpg (A letöltés időpontja: 2018. 04. 27.)

Chee, Foo Yun (2017): NATO says it sees sharp rise in Russian disinformation since Crimea seizure. *Reuters,* 2017. 02. 11. Elérhető: https://www.reuters.com/article/us-ukraine-crisis-russia-media/nato-says-it-sees-sharp-rise-in-russian-disinformation-since-crimea-seizure-idUSKBN15Q0MG (A letöltés időpontja: 2018. 04. 27.)

Cheng, Dean (2017): *Cyber Dragon. Inside China's Information Warfare and Cyber Operations.* Santa Barbara, Praeger.

Cinkler Tibor (2017): *Tárgyak internete IoT: D2D, M2M.* Elérhető: http://w3.tmit.bme.hu/kh2/kh2-16_IoT.pdf (A letöltés időpontja: 2018. 04. 27.)

Cinkler Tibor et al. (2016)*:* 5G hálózatok architektúrája. *Híradástechnika,* 71. évf. 1. sz. 40–46.

Cisco (2017): *The Zettabyte Era: Trends and Analysis.* (Updated: June 7, 2017). Elérhető: https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/vni-hyperconnectivity-wp.pdf (A letöltés időpontja: 2018. 04. 27.)

Clapper, James R. (2015): *Worldwide Threat Assessment of the US Intelligence Community.* Elérhető: https://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf (A letöltés időpontja: 2018. 04. 27.)

Colossus (1943): Colossus codebreaking computer in operation. *Wikimedia Commons.* (A kép publikus felhasználású.) Elérhető: https://commons.wikimedia.org/wiki/File:Colossus.jpg (A letöltés időpontja: 2018. 04. 27.)

Cyber Primer (2016): *Cyber Primer* (2016). 2nd ed. Swindon, MOD DCDC. Elérhető: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/549291/20160720-Cyber_Primer_ed_2_secured.pdf (A letöltés időpontja: 2018. 04. 27.)

Danchik, Robert J. – Pryor, Lee (1990): The Navy Navigation Satellite System (Transit). *Johns Hopkins APL Technical Digest,* Vol. 11, Nos. 1–2. Elérhető: http://www.jhuapl.edu/techdigest/views/pdfs/V11_1-2_1990/V11_1-2_1990_Danchik.pdf (A letöltés időpontja: 2018. 04. 27.)

Difference Engine (2010): Babbage Difference Engine. *Wikimedia Commons.* Fotó © Jitze Couperus. Elérhető: https://commons.wikimedia.org/wiki/File:-Babbage_Difference_Engine_(1).jpg (Fotó: Jitze Couperus) (A letöltés időpontja: 2018. 04. 27.)

DoD (2006): *National Military Strategy for Cyberspace Operations.* Elérhető: https://nsarchive2.gwu.edu//NSAEBB/NSAEBB424/docs/Cyber-023.pdf (A letöltés időpontja: 2018. 04. 27.)

DoD (2011): *Terms & Definitions of Interest for DoD Counterintelligence Professionals.* Elérhető: https://www.dni.gov/files/NCSC/documents/ci/CI_Glossary.pdf (A letöltés időpontja: 2018. 04. 27.)

EMC² (2014): *The Digital Universe of Opportunities.* Elérhető: http://www.emc.com/collateral/analyst-reports/idc-digital-universe-2014.pdf (A letöltés időpontja: 2018. 04. 27.)

Ericson HotLine (é. n.): Ericsson Hotline NMT 450. *Wikimedia Commons.* Fotó © Norwegian Telecom Museum. Elérhető: https://commons.wikimedia.org/wiki/File:Ericsson_Hotline_004.jpg (A letöltés időpontja: 2018. 04. 27.)

Evans, Dave (2011): The Internet of Things: How the Next Evolution of the Internet is Changing Everything. *Cisco White Paper,* April 2011. Elérhető:

https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf (A letöltés időpontja: 2018. 04. 27.)

Fallaga Team Facebook (2018): https://ar-ar.facebook.com/Official.Fallaga (A letöltés időpontja: 2018. 04. 27.)

Fallaga Team Twitter (2018): https://twitter.com/fallaga_team (A letöltés időpontja: 2018. 04. 27.)

Fekete Csanád (2015): *A kiberhadviselés fejlődése és az ukrán válság.* Elérhető: http://biztonsagpolitika.hu/publikaciok-2015/fekete-csanad-a-kiberhadviseles-fejlodese-es-az-ukran-valsag-2 (A letöltés időpontja: 2018. 04. 27.)

FM 100-6 (1996): *Information Operations.* Washington, D.C., Headquarters, Department of the Army. Elérhető: http://www.bits.de/NRANEU/others/amd-us-archive/fm100-6(96).pdf (A letöltés időpontja: 2018. 04. 27.)

FM 3-12 (2017): *Cyberspace and Electronic Warfare Operations.* Washington, D.C., Headquarters, Department of the Army. Elérhető: https://fas.org/irp/doddir/army/fm3-12.pdf (A letöltés időpontja: 2018. 04. 27.)

FM 3-38 (2012): *Cyber Electromagnetic Activities.* Washington, D.C., Headquarters, Department of the Army. Elérhető: http://fas.org/irp/doddir/army/fm3-38.pdf (A letöltés időpontja: 2018. 04. 27.)

FMN (é.n.): *Federated Mission Networking.* Elérhető: http://www.act.nato.int/fmn (A letöltés időpontja: 2018. 04. 27.)

Fogarty, Stephen G. (2015): *Cyber Center of Excellence.* Elérhető: https://www.slideshare.net/afcea/opening-ceremony-and-welcome-mg-fogarty-at-technet-augusta-2015 (A letöltés időpontja: 2018. 04. 27.)

Forstner Bertalan – Ekler Péter – Kelényi Imre (2008): *Bevezetés a mobilprogramozásba. Gyors prototípus-fejlesztés Python és Java nyelven.* Bicske, SZAK Kiadó.

Freya (é. n.): FuMG 401 “Freya LZ”. *Wikimedia Commons.* Fotó © The US National Archives and Records Administration. Elérhető: https://commons.wikimedia.org/wiki/File:Freya-radar-lz.jpg (a kép publikus felhasználású) (A letöltés időpontja: 2018. 04. 27.)

FUG 202 – FUG 220 (1945): FuG 220 and FuG 202 radar of Me 110 1945. *Wikimedia Commons.* Fotó © Saidman, RAF official photographer (a kép publikus felhasználású). Elérhető: https://commons.wikimedia.org/wiki/

File:FuG_220_and_FuG_202_radar_of_Me_110_1945.jpg (A letöltés időpontja: 2018. 04. 27.)

Fuller, J. R. (2016): The 4 stages of an IoT architecture. *TechBeacon.com,* 2016. 05. 26. Elérhető: https://techbeacon.com/4-stages-iot-architecture (A letöltés időpontja: 2018. 04. 27.)

Gartner (é. n.): *Gartner Hype Cycle.* Elérhető: https://www.gartner.com/technology/research/methodologies/hype-cycle.jsp (A letöltés időpontja: 2018. 04. 27.)

GEOG 862 (é. n.): *GPS and GNSS for Geospatial Professionals.* Elérhető: https://www.e-education.psu.edu/geog862/print/book/export/html/1405 (A letöltés időpontja: 2018. 04. 27.)

Gerasimov, Valery (2016): The Value of Science is in the Foresight. New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations. *Military Review,* January–February 2016. 23–29. Elérhető: https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20160228_art008.pdf (A letöltés időpontja: 2018. 04. 27.) Orosz nyelven eredetileg megjelent a Военно-промышленный курьер 2013. 02. 27-i számában. Fordította: Robert Coalson.

Gotkowska, Justyna (2017): The Cyber and Information Space: a new formation in the Bundeswehr. *OSW.WAW.pl,* 2017. 04. 12. Elérhető: https://www.osw.waw.pl/en/publikacje/analyses/2017-04-12/cyber-and-information-space-a-new-formation-bundeswehr (A letöltés időpontja: 2018. 04. 27.)

Gu, Lion – Kropotov, Vladimir – Yarochkin, Fyodor (2017): *The Fake News Machine How Propagandists Abuse the Internet and Manipulate the Public.* A TrendLabs Research Paper. Elérhető: https://documents.trendmicro.com/assets/white_papers/wp-fake-news-machine-how-propagandists-abuse-the-internet.pdf (A letöltés időpontja: 2018. 04. 27.)

Haig Zsolt – Várhegyi István (2005): *Hadviselés az információs hadszíntéren.* Budapest, Zrínyi.

Haig Zsolt – Várhegyi István (2008): A cybertér és a cyberhadviselés értelmezése. *Hadtudomány,* 18. évf. elektr. sz. Elérhető: http://mhtt.eu/hadtudomany/2008/2008_elektronikus/2008_e_2.pdf (A letöltés időpontja: 2018. 04. 27.)

HAIG Zsolt (2011): Az információs hadviselés kialakulása, katonai értelmezése. *Hadtudomány,* 21. évf. 1–2. sz. 12–28.

HAIG Zsolt (2015): *Információ – Társadalom – Biztonság.* Budapest, NKE Szolgáltató.

HAIG Zsolt et al. (2013): *Az infokommunikációs technológia hatása a hadtudományokra.* Budapest, NKE.

HALE, Benjamin (2015): *The History of Social Media: Social Networking Evolution!* Elérhető: http://historycooperative.org/the-history-of-social-media (A letöltés időpontja: 2018. 04. 27.)

HAZAY István szerk. (2005): *A digitális televízió szolgáltatásai.* Budapest, ORTT Alkalmazott Kommunikációtudományi Intézet –Typotex.

HEICKERÖ, Roland (2010): Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations. *FOI Swedish Defence Research Agency Defence Analysis,* No. FOI-R–2970–SE. Elérhető: http://www.highseclabs.com/data/foir2970.pdf (A letöltés időpontja: 2018. 04. 27.)

HOFFMAN, Frank G. (2007): *Conflict in the 21st Century: The Rise of Hybrid Wars.* Arlington, Potomac Institute for Policy Studies. Elérhető: http://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf (A letöltés időpontja: 2018. 04. 27.)

HOLDAWAY, Eric J. (2001): *Active Computer Network Defense: An Assessment.* Maxwell, Air Command and Staff College.

HOLPP, Wolfgang (2004): *The Century of Radar – from Christian Hülsmeyer to Shuttle Radar Topography Mission.* Elérhető: https://www.100-jahre-radar.fraunhofer.de/vortraege/Holpp-The_Century_of_Radar.pdf (A letöltés időpontja: 2018. 04. 27.)

HUGHES TELEGRAPH (2009): Letter-Printing Telegraph Set built by Siemens and Halske in Saint Petersburg, Russia, ca. 1900. *Wikimedia Commons.* Fotó © Ambanmba (a kép publikus felhasználású). Elérhető: https://commons.wikimedia.org/wiki/File:Printing_Telegraph.jpg (A letöltés időpontja: 2018. 04. 27.)

HUGHES, Brian (2016): How to fix the fake news problem. *Edition.CNN.com,* 2016. 11. 16. Elérhető: https://edition.cnn.com/2016/11/16/opinions/how-to-fix-the-fake-news-problem-hughes/index.html (A letöltés időpontja: 2018. 04. 27.)

Huurdeman, Anton A. (2003): *The Worldwide History of Telecommunications.* Hoboken, John Wiley & Sons.

HVG (2015): Hackerek támadtak az N1TV oldalára. *HVG.hu,* 2015. 09. 11. Elérhető: http://hvg.hu/itthon/20150911_Hackerek_tamadtak_az_N1_TV_oldalara (A letöltés időpontja: 2018. 04. 27.)

IC Replica (2015): Replica of first integrated circuit by Jack Kilby. *Wikimedia Commons.* Fotó © Florian Schäffer. Elérhető: https://commons.wikimedia.org/wiki/File:Replica_IC.png (A letöltés időpontja: 2018. 04. 27.)

ICA Report (2017): *Assessing Russian Activities and Intentions in Recent US Elections* (2017). Elérhető: https://www.dni.gov/files/documents/ICA_2017_01.pdf (A letöltés időpontja: 2018. 04. 27.)

IFLA (2017): How to Spot Fake News. IFLA.org. Elérhető: https://www.ifla.org/publications/node/11174 (A letöltés időpontja: 2018. 04. 27.)

Inspire (2014): *Inspire Magazine,* Winter 2014, Issue 13. Elérhető: https://azelin.files.wordpress.com/2015/09/inspire-magazine-issue-13.pdf (A letöltés időpontja: 2018. 04. 27.)

Intel C4004 (2016): A processor Intel C4004 with grey traces. *Wikimedia Commons.* Fotó © Thomas Nguyen. Elérhető: https://commons.wikimedia.org/wiki/File:Intel_C4004.jpg (Fotó:) (A letöltés időpontja: 2018. 04. 27.)

Intelsat (é. n.): *Intelsat history.* Elérhető: http://www.intelsat.com/about-us/history (A letöltés időpontja: 2018. 04. 27.)

IST-147 (2016): *Military Applications of Internet of Things (IST-147)* (2016). Elérhető: https://www.sto.nato.int/Lists/test1/activitydetails.aspx?ID=16536 (A letöltés időpontja: 2018. 04. 27.)

ITU RM 2083-0 (2015): *Recommendation ITU RM 2083-0 (09/2015). Framework and overall objectives of the future development of IMT for 2020 and beyond* (2015). Elérhető: https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.2083-0-201509-I!!PDF-E.pdf (A letöltés időpontja: 2018. 04. 27.)

ITU-T X.1205 (2008): *Overview of cybersecurity.* Elérhető: https://www.itu.int/rec/t-rec-x.1205-200804-i (A letöltés időpontja: 2018. 04. 27.)

Ivezic, Marin (2017): Timeline of Key Cyber-Kinetic Attacks, Incidents and Research. *Ivezic.com,* 2017. 05. 20. Elérhető: http://ivezic.com/cyber-kine-

tic-security/timeline-key-cyber-kinetic-attacks-incidents-research (A letöltés időpontja: 2018. 04. 27.)

Janezic, Detlef (2016): *FMN for Coalition Operations*. Elérhető: https://www.afcea.de/fileadmin/user_upload/Sonderveranstaltungen/FA_mit_FueUstgKdoBw/13-NCIA-FMN1.pdf (A letöltés időpontja: 2018. 04. 27.)

JDN 2/13 (2013): *Joint Doctrine Note 2/13. Information Superiority* (2013). Swindon, MOD DCDC. Elérhető: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/239342/20130813_JDN_2_13_Info_Super.pdf (A letöltés időpontja: 2018. 04. 27.)

Jontz, Sandra (2017): Army Accelerates Cyber, EW Integration. AFCEA.org, 2017. 06. 29. Elérhető: https://www.afcea.org/content/army-accelerates-cyber-ew-integration (A letöltés időpontja: 2018. 04. 27.)

JP 1-02 (2017): *DoD Dictionary of Military and Associated Terms* (2017). Elérhető: http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf (A letöltés időpontja: 2018. 04. 27.)

JP 3-12 (R) (2013): *Cyberspace Operations* (2013). Elérhető: https://fas.org/irp/doddir/dod/jp3_12r.pdf (A letöltés időpontja: 2018. 04. 27.)

JP 3-13 (1987): *Command, Control, and Communications Countermeasures in Joint Military Operations* (1987).

JP 3-13 (1998): *Joint Doctrine for Information Operations* (1998). Elérhető: http://www.c4i.org/jp3_13.pdf (A letöltés időpontja: 2018. 04. 27.)

JP 3-13 (2006): *Information Operations* (2006). Elérhető: https://www.globalsecurity.org/intell/library/policy/dod/joint/jp3_13_2006.pdf (A letöltés időpontja: 2018. 04. 27.)

JP 3-13 (2012): *Information Operations* (2012). Elérhető: https://fas.org/irp/doddir/dod/jp3_13.pdf (A letöltés időpontja: 2018. 04. 27.)

JP 3-13 (2014): *Information Operations* (2014). Elérhető: https://fas.org/irp/doddir/dod/jp3_13.pdf (A letöltés időpontja: 2018. 04. 27.)

JP 3-13.1 (1996): *Joint Doctrine Command and Control Warfare (C2W).* Elérhető: http://www.iwar.org.uk/rma/resources/c4i/jp3_13_1.pdf (A letöltés időpontja: 2018. 04. 27.)

JUDGE, Kevin (2014): A Short History of Computer Viruses. *Antivirus.Comodo.com,* 2014. 09. 04. Elérhető: https://antivirus.comodo.com/blog/computer-safety/short-history-computer-viruses (A letöltés időpontja: 2018. 04. 27.)

KANWAL, Gurmeet (2017): Acupuncture Warfare: China's Cyberwar Doctrine and Implications for India. *IndianDefenceReview.com,* 2017. 07. 30. Elérhető: http://www.indiandefencereview.com/spotlights/acupuncture-warfare-chinas-cyberwar-doctrine-and-implications-for-india (A letöltés időpontja: 2018. 04. 27.)

KELMAN, Herbert C. (1958): Compliance, identification, and internalization: Three processes of attitude change. *Journal of Conflict Resolution,* Vol. 2, No. 1. 51–60. Elérhető: https://scholar.harvard.edu/hckelman/files/Compliance_identification_and_internalization.pdf (A letöltés időpontja: 2018. 04. 27.)

KISS Álmos Péter (2009): Generációk a hadviselésben – a negyedik generáció. *Hadtudományi Szemle,* 2. évf. 2. sz. 10–18. Elérhető: http://archiv.uni-nke.hu/downloads/kutatas/folyoiratok/hadtudomanyi_szemle/szamok/2009/2009_2/2009_2_hm_kiss_almos_10_18.pdf (A letöltés időpontja: 2018. 04. 27.)

KOI Tamás (2010): Húsz éves a magyar mobiltelefónia. *hwsw.hu,* 2010. 10. 15. Elérhető: https://www.hwsw.hu/hirek/45472/mobil-mobiltelefon-mobiltelefonia-westel-450-900-pannon-gsm-vodafone-telenor.html (A letöltés időpontja: 2018. 04. 27.)

KOLLÁR Csaba (2017a): IoT a gyakorlatban, az információbiztonság fókuszában I. Az IoT működése, fejlődési tendenciái. *Bolyai Szemle,* 26. évf. 1. sz. 41–54. Elérhető: https://folyoiratok.uni-nke.hu/document/uni-nke-hu/Bolyai_Szemle_2017_01_web.pdf (A letöltés időpontja: 2018. 04. 27.)

KOLLÁR Csaba (2017b): Az IoT katonai felhasználási lehetőségei és a fejlesztés irányai. *Hadmérnök,* 12. évf. 4. sz. 146–158. Elérhető: http://hadmernok.hu/174_15_kollar.pdf (A letöltés időpontja: 2018. 04. 27.)

KOVÁCS László – KRASZNAY Csaba (2017): „Mert övék a hatalom": Az internet politikát (is) befolyásoló hatása a 2016-os amerikai elnökválasztás során. *Stratégiai Védelmi Kutatóközpont Elemzések,* 2017/9. Elérhető: http://archiv.netk.uni-nke.hu/uploads/media_items/svkk-elemzesek-2017-9-az-internet-politi-

kat-is-befolyasolo-hatasa-a-2016-os-amerikai-elnokvalasztas-soran-kovacs-l-krasznay-cs.original.pdf (A letöltés időpontja: 2018. 04. 27.)

Kovács László (2006): Az információs terrorizmus eszköztára. *Hadmérnök,* Robothadviselés konferencia különszám. Elérhető: http://www.hadmernok.hu/kulonszamok/robothadviseles6/kovacs_rw6.html (A letöltés időpontja: 2018. 04. 27.)

Kovács László (2009): Információs hadviselés kínai módra. *Nemzet és Biztonság,* 2. évf. 7. sz. 35–44. Elérhető: http://www.nemzetesbiztonsag.hu/cikkek/kovacs_laszlo-informacios_hadviseles_kinai_modra.pdf (A letöltés időpontja: 2018. 04. 27.)

Kovács László (2012): Számítógép-hálózati hadviselés: veszélyek és a védelem lehetséges megoldásai Magyarországon. Budapest, ZMNE.

Kreisler, Harry (2001): Identity and Change in the Network Society. Conversation with Manuel Castells. *Globetrotter.berkeley.edu,* 2001. 05. 09. Elérhető: http://globetrotter.berkeley.edu/people/Castells/castells-con4.html (A letöltés időpontja: 2018. 04. 27.)

Krekel, Bryan et al. (2009): *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation.* McLean, Northrop Grumman Corporation. Elérhető: https://nsarchive2.gwu.edu//NSAEBB/NSAEBB424/docs/Cyber-030.pdf (A letöltés időpontja: 2018. 04. 27.)

Kuehl, Daniel (2009): From Cyberspace to Cyberpower: Defining the Problem. In Kramer, F. D. et al. eds.: *Cyberpower and National Security.* Dulles, Potomac Books. 24–42.

Leibniz (2016): Rechenmaschine von Leibniz (Nachbau). *Wikimedia Commons.* Fotó © Eremeev. Elérhető: https://commons.wikimedia.org/wiki/File:Rechenmaschine_von_Leibniz_(Nachbau)_04.jpg (A letöltés időpontja: 2018. 04. 27.)

Lenk, Peter J. (2014): NATO's First Step to the Cloud: Overview and Business Drivers. *ITM White Paper No. 1,* 2014. 08. 31. Elérhető: https://www.ncia.nato.int/it-modernization/PublishingImages/Pages/default/WP1%20-%20One%20Small%20Step.pdf (A letöltés időpontja: 2018. 04. 27.)

LEVERING, Laura (2014): Cyber Center of Excellence CG Shares Vision at Town Hall. *Army.mil,* 2014. 11. 07. Elérhető: https://www.army.mil/article/137882/cyber_center_of_excellence_cg_shares_vision_at_town_hall (A letöltés időpontja: 2018. 04. 27.)

LIBICKI, Martin C. (1995): *What is Information Warfare?* Washington, D.C., National Defense University.

LIND, William S. et al. (1989): The Changing Face of War: Into the Fourth Generation. *Marine Corps Gazette,* Vol. 73, No. 10. 22–26.

LIPOVSKY, Robert – CHEREPANOV, Anton (2016): BlackEnergy trojan strikes again: Attacks Ukrainian electric power industry. *WeLiveSecurity.com,* 2016. 01. 04. Elérhető: https://www.welivesecurity.com/2016/01/04/blackenergy-trojan-strikes-again-attacks-ukrainian-electric-power-industry (A letöltés időpontja: 2018. 04. 27.)

MACKENZIE, Paul J. (2017): *NATO Joint Air Power and Offensive Cyber Operations.* Kalkar, The Joint Air Power Competence Centre. Elérhető: https://www.japcc.org/wp-content/uploads/JAPCC_OCO_screen.pdf (A letöltés időpontja: 2018. 04. 27.)

MARCONI (1901): Guglielmo Marconi 1901 wireless signal. *Wikimedia Commons.* Fotó © Published on LIFE (a kép publikus felhasználású). Elérhető: https://commons.wikimedia.org/wiki/File:Guglielmo_Marconi_1901_wireless_signal.jpg (A letöltés időpontja: 2018. 04. 27.)

MD 3.6 (2) (2014): *Magyar Honvédség Összhaderőnemi Elektronikai Hadviselés Doktrína.* 2. kiadás. A Magyar Honvédség kiadványa.

MÉSZÁROS Rezső (2001): A kibertér társadalomföldrajzi megközelítése. *Magyar Tudomány,* 48. (108.) évf. 7. sz. 769–779. Elérhető: http://www.matud.iif.hu/01jul/meszaros.html (A letöltés időpontja: 2018. 04. 27.)

MH ÖHD (2002): *Magyar Honvédség Összhaderőnemi Doktrína.* Honvédelmi Minisztérium, Honvéd Vezérkar Hadműveleti Csoportfőnökség kiadványa.

MICROSOFT AZURE (é. n.): *Mi a felhő-számítástechnika?* Elérhető: https://azure.microsoft.com/hu-hu/overview/what-is-cloud-computing (A letöltés időpontja: 2018. 04. 27.)

MILLAR, George (1983): *A nagy lokátor-háború.* Budapest, Kossuth.

MILSTAR (2015): *Milstar Satellite Communications System.* Elérhető: http://www.af.mil/About-Us/Fact-Sheets/Display/Article/104563/milstar-satellite-communications-system (A letöltés időpontja: 2018. 04. 27.)

MOTOROLA (2014): Motorola Carphone Model TLD-1100, 1964, view 1 – National Electronics Museum. *Wikimedia Commons.* Fotó © Daderot (a kép publikus felhasználású). Elérhető: https://commons.wikimedia.org/wiki/File:-Motorola_Carphone_Model_TLD-1100,_1964,_view_1_-_National_Electronics_Museum_-_DSC00184.JPG (A letöltés időpontja: 2018. 04. 27.)

MUNK Sándor (2001): Az információs fölényről. *Hadtudomány,* 11. évf. 3. sz. 43–52.

MUNK Sándor (2002): Információs színtér, információs környezet, információs infrastruktúra. *Nemzetvédelmi Egyetemi Közlemények,* 6. évf. 2. sz. 133–154. Elérhető: http://m.ludita.uni-nke.hu/repozitorium/bitstream/handle/11410/1083/nek_2002_2_munk.pdf?sequence=1&isAllowed=y (A letöltés időpontja: 2018. 04. 27.)

MURISON, Malek (2016): DARPA wants to militarise the IoT. *InternetofBusiness.com,* 2016. 09. 01. Elérhető: https://internetofbusiness.com/darpa-wants-militarise-iot (A letöltés időpontja: 2018. 04. 27.)

NAGY Tibor István (2012a): Szenzorhálózatok szoftverfejlesztési kérdései. *Hadmérnök,* 7. évf. 1. sz. 192–201. Elérhető: http://hadmernok.hu/2012_1_nagyt1.pdf (A letöltés időpontja: 2018. 04. 27.)

NAGY Tibor István (2012b): Hálózati réteg a szenzorhálózatokban. *Hadmérnök,* 7. évf. 3. sz. 123–130. Elérhető: http://hadmernok.hu/2012_3_nagytiboristvan.pdf (A letöltés időpontja: 2018. 04. 27.)

NAUGHTON, John (2000): *A Brief History of the Future. The Origins of the Internet.* London, Phoenix.

NGMN (2015): *NGMN 5G White Paper.* Elérhető: https://www.ngmn.org/fileadmin/ngmn/content/downloads/Technical/2015/NGMN_5G_White_Paper_V1_0.pdf (A letöltés időpontja: 2018. 04. 27.)

NJIT (é. n.): *The Progressing Issue of Overloaded Wi-Fi Consumption.* Elérhető: http://graduatedegrees.online.njit.edu/resources/msee/msee-infographics/wi-fi-overload-and-future-wi-fi-consumption-new-jersey-institute-of-technology (A letöltés időpontja: 2018. 04. 27.)

NNEC (2005): *NATO Network Enabled Capability Feasibility Study. Executive Summary: Version 2.0.* Elérhető: http://www.dodccrp.org/files/nnec_fs_executive_summary_2.0_nu.pdf (A letöltés időpontja: 2018. 04. 27.)

NNEC (2014): *NATO Network Enabled Capability (NNEC).* Elérhető: http://www.act.nato.int/nnec (A letöltés időpontja: 2018. 04. 27.)

O'Regan, Gerard (2012): *A Brief History of Computing.* 2nd ed. London, Springer.

Osborne 1 (2010): Osborne 1 portable computer – early model. *Wikimedia Commons.* Fotó © Bilby. Elérhető: https://commons.wikimedia.org/wiki/File:Osborne_1_open.jpg (a kép publikus felhasználású) (A letöltés időpontja: 2018. 04. 27.)

Panetta, Kasey (2017): Top Trends in the Gartner Hype Cycle for Emerging Technologies, 2017. *Gartner.com,* 2017. 08. 15. Elérhető: https://www.gartner.com/smarterwithgartner/top-trends-in-the-gartner-hype-cycle-for-emerging-technologies-2017 (A letöltés időpontja: 2018. 04. 27.)

Papp László (2003): *A technika új csodája: a globális helymeghatározás.* Elérhető: http://www.origo.hu/mindentudasegyeteme/pap/20030623paplaszlo41.html (A letöltés időpontja: 2018. 04. 27.)

Parham, Jason (2018): Facebook and the Price of Tech Utopia. *Wired.com,* 2018. 04. 10. Elérhető: https://www.wired.com/story/facebook-price-of-tech-utopia (A letöltés időpontja: 2018. 04. 27.)

Pascalin (2008): Pascalin calculator. *Flickr.com.* Fotó © Marcin Wichary. Elérhető: https://www.flickr.com/photos/mwichary/2632674049 (A letöltés időpontja: 2018. 04. 27.)

Porche, Isaac R. III et al. (2017): *Tactical Cyber. Building a Strategy for Cyber Support to Corps and Below.* Santa Monica, RAND Corporation.

Pufeng, Wang (1998): Information Warfare. In Pillsbury, Michael ed.: *Chinese Views of Future Warfare.* Washington D.C., National Defense University Press. 317–326.

Radio-Electronics.com (é. n.): *GPS History, Dates & Timeline.* Elérhető: http://www.radio-electronics.com/info/satellite/gps/history-dates.php (A letöltés időpontja: 2018. 04. 27.)

Rasztorgujev (2002) = Расторгуев, Сергей Павлович (2002): Введение в формальную теорию информационной войны. [An Introduction to the Formal Theory of Information Warfare]. Москва, Вузовская книга.

Rawat, Priyanka et al. (2014): Wireless sensor networks: a survey on recent developments and potential synergies. *The Journal of Supercomputing,* Vol. 68, No. 1. 1–48. Elérhető: https://link.springer.com/article/10.1007/s11227-013-1021-9 (A letöltés időpontja: 2018. 04. 27.)

RCA Victor 1939 (2014): Television, RCA Victor TRK 12, 1939, Wolfsonian-FIU Museum. *Wikimedia Commons.* Fotó © Wmpearl (a kép publikus felhasználású). Elérhető: https://commons.wikimedia.org/wiki/File:Television,_RCA_Victor_TRK_12,_1939,_Wolfsonian-FIU_Museum_(detail).JPG (A letöltés időpontja: 2018. 04. 27.)

Relia, Sanjeev (2015): *Cyber Warfare: Its Implications on National Security.* New Delhi, Vij Books.

REM-Sense® (é. n.) = http://www2.l3t.com/cs-east/what-we-do/products/ugs_rem-sense.htm (A letöltés időpontja: 2018. 04. 27.)

Rona, Thomas P. (1976): *Weapon Systems and Information Warfare.* Seattle, Boeing Aerospace Co. Elérhető: https://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Science_and_Technology/09-F-0070-Weapon-Systems-and-Information-War.pdf (A letöltés időpontja: 2018. 04. 27.)

Rouse, Margaret (2008): Cyberspace. *TechTarget.com.* Elérhető: http://searchmicroservices.techtarget.com/definition/cyberspace (A letöltés időpontja: 2018. 04. 27.)

Rózsa Tibor (2016): *Az információs műveletek vizsgálata, különös tekintettel a befolyásolási képességek alkalmazásának lehetőségeire a magyar honvédség feladatrendszerében.* PhD-értekezés kézirata. Budapest, NKE Hadtudományi Doktori Iskola. Elérhető: http://archiv.hhk.uni-nke.hu/uploads/media_items/rozsa-tibor-ezredes-az-informacios-muveletek-alkalmazasanak-lehetosegei-a-magyar-honvedseg-feladatrendszereben.original.pdf (A letöltés időpontja: 2018. 04. 27.)

RQ-170 Sentinel (2018): ی‌ی‌ا‌ک‌ی‌ر‌م‌آ ز‌ی‌ر‌گ‌ر‌ا‌د‌ا‌ر د‌ا‌ب‌ه‌پ RQ170. *Wikimedia Commons.* Fotó © Amirhosseinrostamy75ir. Elérhető: https://commons.wikimedia.org/

wiki/File:پاب‌ه‌پ رادار زی‌رگ‌آ زی‌م‌ی‌اک‌ی‌ی RQ170.jpg (A letöltés időpontja: 2018. 04. 27.)

Russia INFOSEC doctrine (2000): *Information Security Doctrine of the Russian Federation*. Elérhető: https://info.publicintelligence.net/RU-InformationSecurity-2000.pdf (A letöltés időpontja: 2018. 04. 27.)

Russian InfoSpace Activities (2012): *Russian Federation Armed Forces' Information Space Activities Concept.* Elérhető: http://eng.mil.ru/en/science/publications/more.htm?id=10845074@cmsArticle (A letöltés időpontja: 2018. 04. 27.)

SAGE (2005): IBM's $10 Billion Machine. *Wikimedia Commons.* Fotó © Steve Jurvetson. Elérhető: https://commons.wikimedia.org/wiki/File:IBM%27s_$10_Billion_Machine.jpg (A letöltés időpontja: 2018. 04. 27.)

Sallai Gyula – Abos Imre (2007): A távközlés, információ- és médiatechnológia konvergenciája. *Magyar Tudomány,* 168. évf. 7. sz. 844–851. Elérhető: http://epa.oszk.hu/00600/00691/00043/pdf/844-851.pdf (A letöltés időpontja: 2018. 04. 27.)

Schwartau, Winn (1996): *Information Warfare: Cyberterrorism – Protecting Your Personal Security in the Electronic Age.* 2nd ed. New York, Thunder's Mouth Press.

SCR-268 (1943): IBM's $10 Billion Machine. *Wikimedia Commons.* Fotó © Steve Jurvetson (a kép publikus felhasználású). Elérhető: https://commons.wikimedia.org/wiki/File:%22Three_soldiers_of_the_United_States_Army_sit_in_place_at_a_radar_used_by_the_90th_Coast_Artillery_in_Casablanca,_French_-_NARA_-_531325.jpg (A letöltés időpontja: 2018. 04. 27.)

Sharma, Deepak (2010): Integrated Network Electronic Warfare: China's New Concept of Information Warfare. *Journal of Defence Studies,* Vol. 4, No. 2. 36–49. Elérhető: https://idsa.in/system/files/jds_4_2_dsharma.pdf (A letöltés időpontja: 2018. 04. 27.)

Snider, Mike (2016): FCC approves spectrum for 5G advances. *USAToday.com,* 2016. 07. 14. Elérhető: https://www.usatoday.com/story/tech/news/2016/07/14/fcc-approves-spectrum-5g-advances/87081242 (A letöltés időpontja: 2018. 04. 27.)

Soós Gábor András – Szabó Zoltán (2013): *Cloud computing.* Elérhető: http://opti.tmit.bme.hu/~cinkler/HSzA/2013tavasz/4_12_Soos_Szabo_CloudComputing (A letöltés időpontja: 2018. 04. 27.)

Svetoka, Sanda – Reynolds, Anna eds. (2016): *Social Media as a Tool of Hybrid Warfare.* Riga, NATO Strategic Communications Centre of Excellence. Elérhető: https://www.stratcomcoe.org/social-media-tool-hybrid-warfare (A letöltés időpontja: 2018. 04. 27.)

Syncom II. (2012): Syncom II, communication satellite. *Wikimedia Commons.* Fotó © San Diego Air & Space Museum (a kép publikus felhasználású). Elérhető: https://commons.wikimedia.org/wiki/File:Syncom_II.jpg (A letöltés időpontja: 2018. 04. 27.)

Szabó András (2011): Preventív hálózatvédelmi rendszerek alkalmazási lehetőségei a támadások detektálására, valamint a módszerek elemzésére I. rész. *Hadmérnök,* 6. évf. 4. sz. 239–249. Elérhető: http://hadmernok.hu/2011_4_szaboa.pdf (A letöltés időpontja: 2018. 04. 27.)

Tanenbaum, Andrew S. – Wetherall, David J. (2013): *Számítógép-hálózatok.* Budapest, Panem.

Telefunken 1936 (é. n.): Telefunken 1936. *Wikimedia Commons.* Fotó © Eirik Newth. Elérhető: https://commons.wikimedia.org/wiki/File:Telefunken_1936.jpg (Fotó:) (A letöltés időpontja: 2018. 04. 27.)

Telstar II. (1964): Telstar II Satellite Parade of Progress. *Wikimedia Commons.* Fotó © NASA (a kép publikus felhasználású). Elérhető: https://commons.wikimedia.org/wiki/File:Telstar_II_Satellite_Parade_of_Progress.jpg (A letöltés időpontja: 2018. 04. 27.)

Thomas, Timothy L. (2004): *Comparing US, Russian, and Chinese Information Operations Concepts.* Elérhető: http://www.dodccrp.org/events/2004_CCRTS/CD/papers/064.pdf (A letöltés időpontja: 2018. 04. 27.)

Thompson, George Raynor – Back, George I. (é. n.): *Military communication.* Elérhető: https://www.britannica.com/technology/military-communication (A letöltés időpontja: 2018. 04. 27.)

Ţigănuş, Dănuţ (2015): Cloud computing in private defence networks. *Romanian Military Thinking,* 2015/3. 64–73. Elérhető: http://eds.a.ebscohost.com/eds/

pdfviewer/pdfviewer?vid=3&sid=7042d8e1-b2cf-45d8-a9f5-87055a5835-1e%40sessionmgr4010 (A letöltés időpontja: 2018. 04. 27.)

TREASURES™ (é.n.): *Tactical Reconnaissance and Surveillance Enhanced System.* Elérhető: http://elbitsystems.com/media/TREASURES.pdf (A letöltés időpontja: 2018. 04. 27.)

T-System (2012): Állami tulajdonba kerül a Pro-M Zrt. Elérhető: http://www.t-systems.hu/10008955.html (A letöltés időpontja: 2018. 04. 27.)

USCYBERCOM (2016) = http://www.stratcom.mil/Media/Factsheets/Factsheet-View/Article/960492/us-cyber-command-uscybercom (A letöltés időpontja: 2018. 04. 27.)

USNA (é. n.): *Introduction to the Cyber Domain.* Elérhető: https://www.usna.edu/CyberDept/sy110/lec/crsIntro/lec.html (A letöltés időpontja: 2018. 04. 27.)

Vámosi Gergő – Szedlák Ádám (2008): Az interneten is zajlik az orosz-grúz összecsapás. *Origo.hu,* 2008. 08. 11. Elérhető: http://www.origo.hu/tech-bazis/internet/20080811-az-interneten-is-zajlik-az-oroszgruz-osszecsapas.html (A letöltés időpontja: 2018. 04. 27.)

Ványa László (2002): *Az elektronikai hadviselés eszközeinek, rendszereinek és vezetésének korszerűsítése az új kihívások tükrében, különös tekintettel az elektronikai ellentevékenységre.* PhD-értekezés kézirata. Budapest, ZMNE. Elérhető: http://archiv.uni-nke.hu/downloads/konyvtar/digitgy/phd/2003/vanya_laszlo.pdf (A letöltés időpontja: 2018. 04. 27.)

Ványa László (2015): Navigációs berendezések zavarása és megtévesztése. *Repüléstudományi Közlemények,* 17. évf. 2. sz. 7–16. Elérhető: http://epa.oszk.hu/02600/02694/00068/pdf/EPA02694_rtk_2015_2_007-016.pdf (A letöltés időpontja: 2018. 04. 27.)

Ward, Carroll (2017): Israel's Cyber Shot at Syria. *Military.com,* 2007. 11. 26. Elérhető: https://www.military.com/defensetech/2007/11/26/israels-cyber-shot-at-syria (A letöltés időpontja: 2018. 04. 27.)

Weimann, Gabriel (2015): Terrorism in cyberspace. *Fathom Journal,* 2015/Summer. Elérhető: http://fathomjournal.org/terrorism-in-cyberspace (A letöltés időpontja: 2018. 04. 27.)

Weimann, Gabriel (2016): Terrorist Migration to the Dark Web. *Perspectives on Terrorism,* Vol 10, No. 3. 40–44. Elérhető: http://www.terrorismanalysts.

com/pt/index.php/pot/article/download/513/1013 (A letöltés időpontja: 2018. 04. 27.)

WHEATLEY, Margaret J. (2001): *Vezetés és a modern természettudomány – rendszer a káoszban.* Budapest, SHL Kiadó.

WINKLER, Michael et al. (2008): Theoretical and practical aspects of military wireless sensor networks. *Journal of Telecommunications and Information Technology,* No. 2. 37–45. Elérhető: https://pdfs.semanticscholar.org/3c70/4b6f60f782ff63e00603b4abeb099ac5eb94.pdf (A letöltés időpontja: 2018. 04. 27.)

WURZBURG D (1945): German Würzburg radar D antenna (FuMG.39) at the Atlantic Wall near Duindorp, The Hague. *Wikimedia Commons.* Fotó © Piet van der Ham. Elérhető: https://commons.wikimedia.org/wiki/File:Atlantic_Wall_near_Duindorp,_The_Hague,_radar.jpg (A letöltés időpontja: 2018. 04. 27.)

ZHENG, Denise E. – CARTER, William A. (2015): *Leveraging the Internet of Things for a More Efficient and Effective Military.* Washington, D.C. – Lanham, Center for Strategic and International Studies – Rowman & Littlefield. Elérhető: https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/150915_Zheng_LeveragingInternet_WEB.pdf (A letöltés időpontja: 2018. 04. 27.)

ZUSE Z3 (é. n.): Zuse Z3 computer with Finder relays. *Wikimedia Commons.* Fotó © Dksen (a kép publikus felhasználású). Elérhető: https://commons.wikimedia.org/wiki/File:Finder_Relais_Zuse_Z3.jpg (A letöltés időpontja: 2018. 04. 27.)

Rövidítések jegyzéke

ACINT	Acoustic Intelligence
ADSL	Asymmetric Digital Subscriber Line
AEHF	Advanced Extremely High Frequency
AMN	Afghanistan Mission Network
AMPS	Advanced Mobile Phone System
ANS	Advanced Networks and Services
ARCYBER	Army Cyber Command
ARP	Address Resolution Protocol
ARPA	Advanced Research Project Agency
ASI	All Source Intelligence
BAIS	Battlefield Anti-Intrusion System
BLE	Bluetooth Low Energy
C2	Command and Control
C2W	Command and Control Warfare
C3CM	Command, Control, Communications, Countermeasures
CAGR	Compound Annual Growth Rate
CDMA	Code Division Multiple Access
CIA	Confidentiality, Integrity, Availability
CIA	Central Intelligence Agency
CIMIC	Civil-Military Cooperation
CNA	Computer Network Attack
CND	Computer Network Defence
CNE	Computer Network Exploitation
CNO	Computer Network Operations
COMINT	Communication Intelligence
CSMA	Carrier Sense Multiple Access
DCS	Digital Cellular System
DDoS	Distributed Denial of Service
DNS	Domain Name System
DSL	Digital Subscriber Line
EDC	Enterprise Data Centre
EDGE	Enhanced Data Rates for Global Evolution

EDR	Egységes Digitális Rádiórendszer
EDSAC	Electronic Delay Storage Automatic Calculator
EDVAC	Electronic Discrete Variable Automatic Computer
ELINT	Electronic Intelligence
EN	Enhanced Node
ENIAC	Electronic Numerical Integrator and Computer
ETSI	European Telecommunications Standards Institute
EW	Electronic Warfare
FBI	Federal Bureau of Investigation
FDMA	Frequency Division Multiple Access
FMN	Federated Mission Networking
FTP	File Transfer Protocol
FTTH	Fiber to the Home
GEO	Geostationary Earth Orbit
GIS	Geographic Information System
GNSS	Global Navigation Satellite System
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications / Groupe Spécial Mobile
HSPA	High-Speed Packet Access
HTML	Hypertext Markup Language
HTTP	Hypertext Transport Protocol
HTTPS	HTTP Secure
IaaS	Infrastructure as a Service
ICS	Industrial Control System
IDS	Intrusion Detection System
IFLA	International Federation of Library Associations and Institutions
IMINT	Imagery Intelligence
IMP	Interface Message Processors
IMTS	Improved Mobile Telephone System
INFOSEC	Information Security
IoE	Internet of Everything
IoMT	Internet of Military Things
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
IRA	Internet Research Agency
ISAF	International Security Assistant Force
ISM	Industrial, Scientific, Medical Band

ITU	International Telecommunication Union
KLE	Key Leader Engagement
LAN	Local Area Network
LDR	Low Data Rate
LEO	Low Earth Orbit
LiFi	Light-Fidelity
LoRa	Long Range Radio
LPWAN	Low Power Wide Area Network
LTE	Long Term Evolution
M2M	Machine to Machine
MAC	Media Access Control
Malware	Malicious Software
MASINT	Measurement Intelligence
MCS	Mobile Control Station
MDR	Medium Data Rate
MDTRS	Mobile Digital Trunked Radio System
MEMS	Micro-electromechanical System
MEO	Medium Earth Orbit
MID	Miniature Imaging Device
MILDEC	Military Deception
MILSTAR	Military Strategic and Tactical Relay
MMS	Multimedia Messaging Service
MMS	Multimedia Message Service
MNE	Mission Network Element
MNX	Mission Network eXtension
MTR	Miniature Tactical Radar
NAC	North Atlantic Council
NATO CFI	NATO Connected Forces Initiative
Navstar GPS	Navstar Global Positioning System
NB-IoT	Narrow Band IoT
NCS	Network Control Protocol
NCW	Network Centric Warfare
NFC	Near-Field Communication
NGMNA	Next Generation Mobile Networks Alliance
NII	Networking and Information Infrastructure
NMT	Nordic Mobile Telephone
NNEC	NATO Network Enabled Capabilities
NORAD	North American Aerospace Defense Command

NSA	National Security Agency
NSFNET	National Science Foundation Network
NSSS	Navy Navigation Satellite System
OpsCen	Operation Centre
OPSEC	Operation Security
OSI	Open Systems Interconnection Reference Model
OSINT	Open Source Intelligence
PaaS	Platform as a Service
PBN	Protected Business Network
PC	Personal Computer
PIA	Public Internet Access
PLC	Power-line Communication
PPP	Presence, Posture and Profile
PSTN	Public Switched Telephone Network
PSYOP	Psychological Operation
RADAR	Radio Detection and Ranging
RADINT	Radar Intelligence
RAM	Random Access Memory
RC-IED	Radio Controlled Improvised Explosion Devices
REMBASS	Remotely Battlefield Sensor System
RFID	Radio Frequency Identification
ROM	Read Only Memory
RTMS	Radio Telephone Mobile System
SaaS	Software as a Service
SABRE	Semi-Automated Business Research Environment
SAGE	Semi-Automated Ground Environment
SAND	Smart All-terrain Networked Detectors
SCAMP	Single Channel Anti-Jam Man Portable
SIGINT	Signal Intelligence
SIM	Subscriber Identity Module
SIPRNet	Secret Internet Protocol Router Network
S-MAC	Medium Access Control for Wireless Sensor Networks (Sensor MAC)
SMAR-T	Secure Mobile Anti-Jam Reliable Tactical Terminal
SMS	Short Message Service
SN	Standard Node
SQL	Structured Query Language
SRI	Stanford Research Institute
STO	Science and Technology Organization

TACAN	Tactical Air Navigation
TACS	Total Access Communication System
TCP/IP	Transmission Control Protocol/Internet Protocol
TDMA	Time Division Multiple Access
TETRA	Terrestrial Trunked Radio
TREASURES	Tactical Reconnaissance and Surveillance Enhanced System
UAV	Unmanned Aerial Vehicle
UCLA	University of California at Los Angeles
UCSB	University of California at Santa Barbara
UDP	User Datagram Protocol
UGS	Unattended Ground Sensors
UMTS	Universal Mobile Telecommunication System
UNIVAC	Universal Automatic Computer
URL	Uniform Resource Locator
USCYBERCOM	US Cyber Command
USSTRATCOM	US Strategic Command
VoIP	Voice over Internet Protocol
VOR/DME	VHF Omnidirectional Range/Distance Measurement Equipment
VSAT	Very Small Aperture Terminal
WCDMA	Wideband Code Division Multiple Access
WSN	Wireless Sensor Network
XDR	Extended Data Rate

Vákát oldal

Képek jegyzéke

1. kép	*Hughes-féle betűnyomó távíró* *Forrás*: Hughes Telegraph 2009	18
2. kép	*Telefon- és távíróvonalak Broadway utcáin 1885–87-ben, egy korabeli képeslapon* *Forrás*: Broadway (é. n.)	19
3. kép	*Marconi a szikratávíróval (jobbra) és a kohérer detektoros vevővel (balra) 1901-ben* *Forrás*: Marconi (1901)	21
4. a) kép	*Telefunken FE III katódsugárcsöves televízió 1936-ból* *Forrás*: Telefunken 1936 (é. n.)	23
4. b) kép	*RCA Viktor TRK 12, a világ első teljes egészében elektronikus letapogatású, 343 soros és 30 kép/másodperc jelmegjelenítésű televíziója 1939-ből* *Forrás*: RCA Victor 1939 (2014)	23
5. a) kép	*A német Freya felderítőradar* *Forrás:* Freya (é. n.)	28
5. b) kép	*Würzburg D* célkövető radar *Forrás*: Wurzburg D (1945)	28
6. a) kép	*Az egyesült királyságbeli „Chain Home” radarhálózat antennatornyai* *Forrás*: Chain Home (1945)	29
6. b) kép	*Amerikai SCR-268 célkövető radar* *Forrás*: SCR-268 (1943)	29
7. a) kép	*Messerschmitt Me 110G-4 repülőgép orrán a FUG 202 (középen) és FUG 220 radarok antennái* *Forrás*: FUG 202 – FUG 220 (1945)	30
7. b) kép	*Bristol Beaufighter Mk VIF orrában az AI Mk. VIII radarral* *Forrás*: AI MK. VIII (é. n.)	30
8. kép	*Motorola TLD-1100 gépjárműbe szerelhető IMTS rendszerű mobiltelefon 1964-ből* *Forrás*: Motorola (2014)	36
9. a) kép	*A Jack Kilby által kifejlesztett első integrált áramkör másolata* *Forrás*: IC Replica (2015)	37

9. b) kép	*Az első mikroprocesszor, az Intel 4004-es 1971-ből* *Forrás*: Intel C4004 (2016)	37
10. kép	*NMT 450 rendszerű Ericson HotLine mobiltelefon* *Forrás*: Ericson HotLine (é. n.)	40
11. a) kép	*Telstar műhold* *Forrás*: Telstar II. (1964)	46
11. b) kép	*Syncom II. GEO-műhold* *Forrás*: Syncom II. (2012)	46
12. a) kép	*Blaise Pascal Pascaline nevű számológépe* *Forrás*: Pascalin (2008)	55
12. b) kép	*Leibniz léptetőhengeres számológépének rekonstrukciója* *Forrás*: Leibniz (2016)	55
13. kép	*A Babbage elképzelése szerint megépített Difference Engine No. 2* *Forrás*: Difference Engine (2010)	56
14. kép	*Konrad Zuse Z3 mechanikus relés számítógépének másolata* *Forrás*: Zuse Z3 (é. n.)	57
15. kép	*A Colossus* *Forrás*: Colossus (1943)	58
16. kép	*SAGE félautomata légvédelmi vezetési rendszer* *Forrás:* SAGE (2005)	60
17. kép	*Osborne 1, az első hordozható számítógép* *Forrás*: Osborne 1 (2010)	63
18. kép	*REM-Sense® harctéri szenzorrendszer* *Forrás*: REM-Sense® (é. n.)	131
19. kép	*Az Iránban eltérített és leszállított RQ-170 Sentinel pilóta nélküli repülőgép* *Forrás*: REM-Sense® (é. n.)	273
20. kép	*Az ABC News és a Népszava online oldalára hasonlító álhíroldalak* *Forrás:* anepszava.com; Hughes (2016) alapján a szerző szerkesztése	293
21. kép	*Az Inspire magazin 2014. évi téli számának tartalomjegyzéke* *Forrás*: Inspire (2014)	299
22. kép	*A Fallaga Team Twitter- és Facebook-oldala* *Forrás*: Fallaga Team Twitter (2018); Fallaga Team Facebook (2018)	301

Ábrák jegyzéke

1. ábra *Cellás elv*
Forrás: a szerző szerkesztése 39
2. ábra *A Milstar rendszer*
Forrás: Haig–Várhegyi 2005 50
3. ábra *A GNSS rendszer várható teljes kiépítettségben*
Forrás: GEOG 862 (é. n.) alapján a szerző szerkesztése 54
4. ábra a) *Decentralizált, vonalkapcsolt és* b) *elosztott, csomagkapcsolt hálózati topológia*
Forrás: a szerző szerkesztése 65
5. ábra *Az ARPNAET 1974-es kiépítettsége*
Forrás: ARPANET 1974 (2007) 67
6. ábra *Feltörekvő technológiák Hype-ciklusa 2017-ben*
Forrás: Panetta (2017) alapján a szerző szerkesztése 87
7. ábra *Felhőalapú számítástechnika*
Forrás: Microsoft Azure (é. n.) alapján, a szerző szerkesztése 93
8. ábra *Az IoT architektúrája*
Forrás: Fuller (2016) alapján a szerző szerkesztése 100
9. ábra *A szenzorok általános működési környezete és működési folyamata*
Forrás: a szerző szerkesztése 115
10. ábra *Szenzorhálózatok protokollvermének* rétegei és síkjai
Forrás: Nagy 2012b alapján a szerző szerkesztése 119
11. ábra *Levegőből kidobható felügyelet nélküli szenzor felépítése*
Forrás: a szerző szerkesztése 125
12. ábra *Harctéri szenzorhálózat*
Forrás: Haig–Várhegyi (2005) alapján a szerző szerkesztése 127
13. ábra *Hálózatközpontú hadviselés logikai modellje*
Forrás: Cebrowski–Garstka (1998) alapján a szerző szerkesztése 138
14. ábra *A NATO hálózatalapú képességstruktúrája*
Forrás: NNEC (2014) alapján a szerző szerkesztése 141
15. ábra *Az USA légierejének 1998-as doktrína szerinti információs műveletek koncepciója*
Forrás: AFDD 2-5 (1998), 3. alapján a szerző szerkesztése 169

16. ábra *Az USA* összhaderőnemi *információs műveletek képességei a 2006-os doktrína szerint*
Forrás: JP 3-13 (2006) alapján a szerző szerkesztése 178
17. ábra *A NATO információs műveletek értelmezése*
Forrás: AJP-3.10 (2015), 1–6. alapján a szerző szerkesztése 188
18. ábra *Az információs műveletek átfogó értelmezése*
Forrás: a szerző szerkesztése 210
19. ábra *Az információs műveletek információs képességei és hatásuk*
Forrás: a szerző szerkesztése 216
20. ábra *A kibertér struktúrája*
Forrás: USNA (é. n.) és Cyber Primer (2016) alapján a szerző szerkesztése 230
21. ábra *Az elektronikai felderítés fajtái*
Forrás: Haig et al. (2013) alapján a szerző szerkesztése 244
22. ábra *Számítógép-hálózati műveletek*
Forrás: a szerző szerkesztése 247
23. ábra *Elektronikai hadviselés*
Forrás: a szerző szerkesztése 251
24. ábra *A műveleti biztonság módszerei és folyamata*
Forrás: a szerző szerkesztése 256
25. ábra *Kibertéri műveletek információs képességeinek kölcsönhatása*
Forrás: a szerző szerkesztése 270
26. ábra *Az USA Hadsereg Kiber Parancsnokság integrációs folyamata*
Forrás: Fogarty (2015) alapján a szerző szerkesztése 284
27. ábra *Álhírháromszög*
Forrás: Gu–Kropotov–Yarochkin (2017) alapján a szerző szerkesztése 291
28. ábra *Az IFLA álhírek elleni kampányának felvilágosító plakátja*
Forrás: IFLA (2017) 296

Táblázatok jegyzéke

1. táblázat *Az IoT-ben alkalmazott jellemző adatkommunikációs technológiák összehasonlítása*
Forrás: 11 IoT (2015) alapján a szerző szerkesztése 106

2. táblázat *A hadviselés generációi*
Forrás: Balogh (2015); Lind (1989) alapján szerkesztette Fekete Csanád 173

3. táblázat *Kibertéri műveletek információs képességei*
Forrás: a szerző szerkesztése 240

Vákát oldal

Grafikonok jegyzéke

1. grafikon *Web-böngészők felhasználói részarányának alakulása az elmúlt tíz évben*
Forrás: Browser Statistics (2017) alapján a szerző szerkesztése 71

2. grafikon *Eszközspecifikus havi adatforgalom növekedési előrejelzés*
Forrás: Cisco (2017) alapján a szerző szerkesztése 78

3. grafikon *M2M-kapcsolatok növekedési trendje szektoronként*
Forrás: Cisco (2017) alapján a szerző szerkesztése 80

4. grafikon *Az 5G-hálózat tervezett képességnövekedése a 4G LTE-advanced hálózathoz viszonyítva*
Forrás: ITU RM 2083-0 (2015) alapján a szerző szerkesztése 109

A Dialóg Campus Kiadó
a Nemzeti Közszolgálati Egyetem könyvkiadója.

Nordex Nonprofit Kft. – Dialóg Campus Kiadó
www.dialogcampus.hu
www.uni-nke.hu
1083 Budapest, Ludovika tér 2.
Telefon: (30) 426 6116
E-mail: kiado@uni-nke.hu
A kiadásért felel: Petró Ildikó ügyvezető

Felelős szerkesztő: Kilián Zsolt
Olvasószerkesztő: Tar Krisztina
Korrektor: Sós Dóra Gabriella
Tördelőszerkesztő: Stubnya Tibor
Nyomdai kivitelezés: Pátria Nyomda Zrt.
Felelős vezető: Simon László vezérigazgató

ISBN 978-615-5945-04-5 (nyomtatott)
ISBN 978-615-5945-05-2 (elektronikus)

Napjainkban a kibertéri hálózatos technológiák teljes mértékben áthatják és meghatározzák az emberek életét. A hálózatok hagyományos felhasználása mellett egyre nagyobb szerepet kapnak az interneten keresztül egymással összekapcsolt fizikai eszközök, újfajta hálózatos technológiák jelennek meg a kibertérben, emellett pedig a közösségi média használatával a felhasználók is részeseivé válnak a hálózatnak. Mindennek köszönhetően a kibertér értelmezése átalakul, és a benne jelentkező fenyegetések is jelentősen kibővülnek, a komplex információs műveletek a kibertérben is érvényesülnek. Mindezek alátámasztására a könyv bemutatja az infokommunikáció fejlődésének főbb mérföldköveit, ismerteti napjaink meghatározó hálózatos infokommunikációs technológiai fejlődési irányait, továbbá elemzi az információs műveletek kialakulásának, fejlődésének és átalakulásának tendenciáit. Végül pedig a kibertér újszerű megközelítése révén meghatározza az egyes információs műveleti képességek kibertéri megjelenési formáit és alkalmazási lehetőségeit.

A kiadvány
a KÖFOP-2.1.2-VEKOP-15-2016-00001
„A jó kormányzást megalapozó
közszolgálat-fejlesztés” című projekt
keretében került kiadásra.

SZÉCHENYI 2020

Magyarország Kormánya

Európai Unió
Európai Szociális Alap

BEFEKTETÉS A JÖVŐBE