Várhegyi István

Az információs hadviselés második hulláma

Fejlődéstanilag az információs hadviselés történetét eddig két eljárással, vagyis elméletileg és tapasztalati úton, empirikusan vizsgáltuk. Ezekből kiderült, hogy az információs hadviselés fejlődése időben hullámszerű. Eddig két nagy fejlődési hullámot érzékeltünk, az alábbi időszakaszokkal:

- az információs hadviselés első hulláma (1990–2010);
- az információs hadviselés második hulláma (2010–2030).

Az információs hadviselés fejlődése első hullámának főbb eseményei:

- Első öbölháború: Irak, 1991. (A „Sivatagi vihar" hadjárat volt tulajdonképpen az első digitális és információs hadviselési háború.)
- Második öbölháború: Irak, 2003. (A teljes körű információs hadviselés példája.)
- Dél-szláv háború: Balkán, 1992. (A kiberműveletek kezdeti sikerei: hamis légvédelmi radarcélok bevitele az ellenség vezetési rendszerébe. Megjegyzendő, hogy korábban hasonló elektronikai hadviselési támadóműveleteket hajtottak végre az öbölháborúban és az arab–izraeli háborúkban, radarállomások ellen is.).
- Afganisztáni háború, 2001. (Az információs hadviselés teljes arzenáljának alkalmazása.)
- Orosz–észt háború, 2007. (Storm Worm botnet, rosszindulatú szoftver, elárasztásos hackertámadás, teljes bankrendszeri hackerművelet.)
- Orosz–grúz háború, 2008. (Szolgáltatás megtagadásos támadás a bankrendszer, illetve az elektronikus közigazgatás ellen.[1])
- NATO-válaszlépés 2008-ban. (Észtországban megalakult a NATO Kiberhadviselési Védelmi Központ,[2] amelyhez az alapító okirat aláírásával csatlakozott Észtország, Litvánia, Lettország, Németország, Olaszország, Spanyolország

1 Elosztott szolgáltatás-megtagadás típusú támadás (Distributed Denial of Services – DDoS)

2 Cooperativ Cyber Defence Center of Excellence – CCDCOE

és Szlovákia. Az alapító okirathoz, mint aláírók, 2010-ben az USA, Törökország és Magyarország is csatlakozott.)

– Izrael és az USA, másfelől Irán konfliktusa 2009-től. (A rejtett kiberhadviselés komoly sikere volt a programféreg (Stuxnet-worm,) bevitele az iráni uránipari hálózatba, amelyet kimondottan ipari vezérlőszoftverek megbénítására hoztak létre a WIN CC és bizonyos SCADA rendszerek ellen. A Stuxnetet Izraelben próbálták ki ugyanolyan német eredetű ipari urániumgáz-centrifugákon, amelyeket Irán használ az urándúsításhoz. Ez nagyon sikeres kiberszabotázs volt, mivel a vezérlőrendszer egyrészt azt jelentette, hogy minden rendben van, másrészt a centrifugákat teljes kapacitásra gyorsította fel, majd hirtelen leállította, aminek következtében azok tönkrementek. A termelési másfél éves kiesést szenvedett.)

Összességében megállapítható, hogy az információs hadviselés első hullámában résztvevő felek számítógép-hálózatok elleni támadó képességei, réskereső, adatgyűjtő, kém, támadó és romboló szoftverei, vírusai, módszerei, eljárásai és eszközei jelentősen fejlődtek, mivel tesztelésükre és alkalmazásukra az egymást követő háborúk igen kedvező laboratóriumi tesztelő, és „éles" alkalmazási helyzeteket teremtettek.

A kibernetika a távolból történő működtetés, szabályozás, irányítás tudománya. A kibernetika a kibertérben működik, amelyet gyakran virtuális tér néven is említenek. A kibertér[3] virtuális valóságelemei (entitásai) azok az eszközök, amelyeket az állami, nemzetvédelmi, katonai, magán, tudományos, kritikus infrastruktúra (pénzügyi, bank, ellátó, szállító, egészségügy, katasztrófavédelmi stb.) szektorokban, továbbá a civil társadalomban és az állampolgárok által használt számítógépes rendszerekben (vezetékes, vezeték nélküli, műholdas vagy mobil GSM információs hálózatok, hálózati szoftverek, és az azokhoz tartozó információ-továbbító és feldolgozórendszerek) működtetnek.

A kibertér az információs hadszíntér szerves része, annak egyik megahalmaza, amely a korábbi hadszínterek (szárazföldi, légi, tengeri, űr/kozmikus és információs hadszínterek) mellett, mint legújabb hadszíntér jelent meg. E hadszíntéren – szemben a klasszikus hadszínterekkel – nem valódi (vagyis a mozgási energián alapuló), ún. halálos pusztító hatású fegyverekkel,[4] hanem a nem-mozgási (például az elektromágneses) energia használatán alapuló, működést korlátozó hatású, virtuális fegyverekkel[5] vívják a kibertéri virtuális csatákat. A kibertér virtuális valóságelemei (entitásai) a bitek, bájtok, weblapok, belső számítógépes hálózatok és a globális internethálózat. Ezekben kémkedni hivatalosan nem szabad, de illegális úton lehetséges, ha van rá igény.

A virtuális kibertér kialakulása és fejlődése az információs társadalom vezetékes és mobil hálózatos információtechnológia rohamos fejlődésének köszönhető. E hálózatokhoz való hozzáférés nem mindenütt és nem mindig biztonságos, vagyis bennük biztonsági rések (kapuk) találhatók. Ezért az illetéktelenek részéről történő hoz-

3 cyber space, cyber domain, cyber sphere

4 hard kill kinetic weapons

5 soft kill non-kinetic weapons

záférésnek tág tere van, amit számos formában (hozzáférés, behatolás, meghamisítás, blokkolás, általános és konkrét információszerzés stb.) eredményesen használnak ki a nem etikus hackerek, a fehérgalléros kiberbűnözők, továbbá kiberterroristák, kiberkémek, kiberadatszerzők és kiberharcosok.

Természetes, hogy a kiberteret – a háborút vezérlő hadművészet és a konkrét hadműveletek, illetve az információs hadviselés keretében – szakhadviselési célokra is igénybe veszik. Ezt nevezik kiber-hadviselésnek. E virtuális katonai tevékenységeket általában a kiberháború, világhálós (internetes) háború, globális virtuális hadviselés, kiberhadviselés, kiberhadjárat, kiberhadművelet, kiberütközet, kibercsata, kiberesemény (-incidens) fogalmakkal jelölik. Az előbbiek mellett (tegyük hozzá: nem pontosan) az alacsony intenzitású fegyveres konfliktusok időszakában folytatott kiberháborúra gyakran alkalmazzák a kiberterrorizmus fogalmát.

A kibertéri események jellemző típusai: a hacker szúrópróba, (vagyis szimatolás, biztonsági réskeresés), a hacker-behatolás, a weboldali hacker-feltörés, a hackerkémkedés, a hacker-adatlopás, a hacker-bűncselekmény és mások. A kibertéri támadások tipikus formái rendszerint a weblap „elsötétítés", a weblap felülírás, a weblap-grafiti, a weblap és a hálózat működésének lezárása, vagyis blokkolása, ártó típusú vírusok bejuttatása és aktivizálása.

A kibertéri hadviselés az információs hadviselésnek szakirányú része, amely állandóan fejlődő kibertéri szakfegyvernemekkel és szakalakulatokkal rendelkezik.

Az első hullám időszakának második felében (2005 után), az információs hadszíntéren belül megjelent a számítógép-hálózatokat is magában foglaló kibertér fogalma, a számítógépes támadó hadviselés (kiberhacker hadviselés) elmélete és gyakorlata.[6] Megjelentek az információs hadviselés katonai és polgári vezetési és irányító elemei, valamint az információs hadviselési alakulatok (például az USA-ban az információs hadviselési kiberparancsnokság;[7] a nemzeti (országos) kritikus infrastruktúra-védelmi programok; a számítógép-hálózatokat ellenőrző és felügyelő védelmi központok,[8] továbbá a speciális alakulatok, amelyek a haderőnemeknél a kiberhadviselés valamelyik szakterületének konkrét feladatait látják el). A hirtelen felmerülő szakember hiányt részben azzal pótolták, hogy más szakmai számú személyeket gyorstanfolyamokon képeztek át a kiberműveletek végzésére. (Egyébként egy alapfokú kiberszakértő kiképzése általában két évet vesz igénybe.)

Az első hullám végére és összlétszámát tekintve, az USA-ban kb. 30 000 főt számláló kiberhacker hadviselési erővel rendelkeznek. Kínában az ilyen feladatú katonai alakulatok összlétszáma feltehetően 60 000 főt (vagy többet) számlál. A többi ország vagy követi, vagy szoros figyelemmel kíséri az amerikai, illetve kínai információs hadviselési és hacker-hadviselési fejleményeket. Az időszakosan igénybe vett civil hackerek létszámát nehéz megbecsülni, mivel nemcsak saját állampolgárokról van szó, hanem külföldi hackereket (csoportokat) is felbérelnek ilyen feladatokra.

---

6 computer network attack operations – CNA

7 US Cyber Command

8 Computer Emergency Rescue Team – CERT

Az első hullám végére (2010) elkészültek a hackerműveletek működési szabályai, eljárásai és folyamatosan fejlesztik a támadó típusú rosszindulatú szoftvereket.[9] Sikeresen alkalmazták vagy tesztelték a támadó rosszindulatú szoftvereket „éles viszonyok" között is, ami által igen fontos tapasztalatokat szereztek. Alkalmazásukban nagy gyakorlatra tettek szert. Figyelemre méltó, hogy az információs hadviselés komplex műveletei között a számítógép-hálózati hadviselést (kiber-hadviselés, hacker-hadviselés), az ellenséges ország teljes vezetékes és vezeték nélküli internet-hálózatára alkalmazták. E műveleteket több alkalommal, a háborút közvetlenül megelőzően, vagy annak bevezető lépéseként (vagyis az első csapás részeként), hadászati meglepetésként alkalmazták, több napig, vagy hétig. Mindezek eredményeképpen megállapítható, hogy az első hullám végére, tehát 2010-re, az információs hadviselés nemkinetikus erejű, és nem fizikai pusztító hatású műveletei a háborúk, a hadjáratok és a hadműveletek szerves részévé váltak, és új fejezeteket nyitottak a hadtudomány történelmében.

Értékelésem szerint – az elért eredmények alapján – az információs hadviselés és kapcsolt részeinek műveleteivel és hatásukkal 2010 után mind az állami, mind pedig a katonai vezetés szintjén már állandóan számolnak. Rejtett formában pedig a célország valamennyi ágazatára és teljes területére kiterjedhet. Az arab (iszlám) országokban 2011. elején kibontakozó forradalmak felszínre hozták a kibertér és azon belül az internet-hálózat, a közösségi civil hálózatok (például a Facebook stb.) fontosságát.

Következtetésként megállapítható, hogy az információs hadviselés első hullámában (1990–2010 között) mesteri módon alkalmazták az információs műveleteket. A hadjáratok katonai vezetői megismerték, megértették és egyre hozzáértőbb módon alkalmazták az információs műveletek támadó és védelmi rendszabályait. Ebben az első hullámban az információs hadviselés korszerű támadó képességeinek megteremtése alapvető feladat volt.

Az első hullám végére „nagykorúvá vált" az információs hadviselés, és benne a kiber-hadviselés, mint alapvetően nem kinetikus hatású hadviselési fajta. Ezért alkalmazásukkal és hatásukkal – békében, feszültség időszakában és háborúban – egyaránt számolni kell. A tudati dimenzióval és a posztmodern tudati hadviseléssel kapcsolatos elméleti kérdések kutatásai felgyorsultak.

Az információs hadviselés fejlődése második hullámának várható fő irányai (2010–2030)

Az információs hadviselés fejlődése 2010-ben lezárult első hullámában bizonyítást nyert, hogy az információs hadviselés – új hadviselési fajtaként – megjelent a hadtudomány rendszerében. Az információs hadviselés a továbbiakban nélkülözhetetlen a fegyveres küzdelem megvívásában és eddigi eredményei alapján annak további fejlődése várható. Megjelenését két fontos változás tette lehetővé:

9 Malicious Softwares – MALWARE

1. a vezetés és a döntéshozatal területén rendkívül módon megnőtt a digitalizáció, a hálózatok, az információ és a vezetési tudás szerepe;
2. az elektronikus információs hálózatok megjelenésével egy új hadszíntér alakult ki, amelyet kibertérnek neveznek.

Az információs hadviselés fejlődésének második hulláma 2010 és 2030 között olyan gazdasági és politikai világkörnyezetben bontakozik ki, amely időben két fejlődési szakaszra (2010–2020 és 2020–2030) osztható. Az eddigi trendek elméleti és gyakorlati vizsgálata alapján a változások főbb jellemzői a következők lehetnek:

– átalakul a világgazdaság szerkezete és vezetése;
– csökkentik a védelmi kiadásokat;
– újabb háború kitörésével nem számolnak;
– változás következik be a hadviselési fajták alkalmazásában;
– fejlődik az információs hadviselés és a kibertéri hadviselés;
– előtérbe kerülnek az állami és polgári hálózatos információs tevékenységek;
– valószínűsíthető a magasabb síkú tudásfejlesztés, a posztmodern tudati hadviselés kialakulása.

Átalakul a világgazdaság szerkezete és vezetése (2010–2020):

Kína folytatja erőteljes gazdasági fejlődését, amely lehetővé teszi, hogy a világgazdaság első számú vezető hatalmává váljon. Mint trónkövetelő, az USA-val szemben nem ellenség, hanem versenytárs, aki növekvő gazdasági hatalmának arányában, globális politikai tényezőként kíván beleszólni a világ dolgaiba. E szándékát nyíltan bejelentette, de törekvéseihez katonai eszközöket nem kíván felhasználni, mert még nincs felkészülve a helyi háborúnál nagyobb méretű regionális, vagy kontinentális, illetve óceáni fegyveres konfliktusra. (Ilyen nagyméretű katonai vállalkozáshoz ereje még nem elegendő.) Mindazonáltal 2011-re elérte, hogy – az USA-t kivéve – a Csendes-óceán térségében a legerősebb katonai hatalommá lépett elő. Katonai fejlesztési elképzelései és saját, hazai gyártású fegyver-prototípusai ugyanakkor azt jelzik, hogy a legfejlettebb fegyverrendszereket és haditechnikai eszközöket kívánja kifejleszteni, vagy megszerezni. Azok sorában a következő – figyelemre méltó – hazai fejlesztésű és gyártású eszköztípusok találhatók:

– atombombák, illetve atomrakéta-fejek;
– navigációs űrállomások, vadászűrhajók;
– interkontinentális ballisztikus atomrakéták, föld-levegő, föld-föld és föld-tenger (hajó) osztályú rakétarendszerek, rakétahordozó atom-tengeralattjárók;
– repülőgép-hordozó anyahajók (építés alatt);
– ötödik generációs lopakodó vadászrepülőgépek (J–20), csapásmérő pilótanélküli repülőeszközök;[10]
– korszerű rádiólokátorok, fejlett felderítő és tűzvezető rendszerek, korszerű légvédelmi rakéták;
– korszerű harckocsik, digitális hadsereg.

10 Pilótanélküli repülőeszköz – Unmanned Aerial Vehicle

Külön kiemelendő, hogy a kínai haderő vezetése ismeri a korszerű vezetési és hálózatos hadviselés elveit. Jelentősen előre haladt a haderő digitalizálásában. Ismeri az információs hadviselés módszereit. Jól felkészült a kiber-hadviselés terén, amit a szárazföldi haderő éles gyakorlatain is rendszeresen kipróbál. Több ezer jól képzett, számítógép-hálózatok ellen bevethető, „hacker-katonával" rendelkezik.

2010-ben megépítette a Tianhe–1A típusjelzésű szuperszámítógépet, amely a világ legnagyobb teljesítményű (2,6 Petaflops) számítógépének számít. Ez lehetővé teszi, hogy Kína az élvonalba kerüljön a tudományos és katonai kutatások terén. Ilyen számítógépes háttérrel támasztja alá a Holdra-szállásra és a Mars bolygó felderítésére vonatkozó törekvéseit.

Eredményei alapján napjainkban Kína – az USA-t nem számolva – a legerősebb és legfejlettebb katonai erővel rendelkezik Ázsia keleti partjainál, és közvetlen katonai nyomást képes gyakorolni a Csendes-óceán csatlakozó térségeire. Az USA óvatosan kezeli azokat az információkat és feltevéseket, miszerint Kína rendelkezik olyan ballisztikus rakétákkal és felderítő műholdakkal, később pedig saját navigációs műhold-rendszerrel, amelyek segítségével képes fenyegetni, vagy megsemmisíteni a kínai szárazföld közelében manőverező amerikai repülőgép-anyahajókat.

Kína növekvő gazdasági hatalma időközben fontos politikai tőkévé alakult, amelyet regionális gazdasági, vagy globális hatalmi érdekeinek érvényesítésére használ Taiwan, India, Vietnam, Dél-Korea és részben Japán ellenében. Nemzetközi szinten egyre inkább elvárja, hogy globális nagyhatalomként kezeljék. Igényli, hogy a világ valamennyi fontos kérdésében és érdemben kifejthesse véleményét. Fontos megemlíteni, hogy már napjainkban is képes a Dél-kínai-tengeren akadályokat gördíteni a szabad hajózás elé.

Az EU és az európai export-hatalmak (elsősorban Németország, Franciaország Olaszország, az Egyesült Királyság, Svédország), továbbá az USA is keresi Kínával a párbeszéd és a kereskedelmi forgalom növelésének lehetőségét. *Obama* elnök hangsúlyozta, hogy Kína nem ellenség, hanem versenytárs. Az USA-ban ugyan haditechnikai embargó van érvényben Kínával szemben, de e rendszabályokat gyakran kijátsszák. Emellett számos panasz érkezik kínai ipari vállalatok ellen, amelyekben ipari kémkedéssel és külföldi prototípusok lemásolásával vádolják őket. E műszaki információk és gyártási titkok birtokában olcsó, de korszerű fegyver-szállítóként jelenik meg a nemzetközi piacon. (Hangsúlyozni kell, hogy egy korszerű haditechnikai eszköz kifejlesztéséhez 5–10 év szükséges, mely fejlesztési időt a külföldi eszközök lemásolásával Kína igyekszik lerövidíteni.)

Kínával kapcsolatban – az emberi jogi kérdések kivételével – a NATO-nak nincsenek vitás kérdései. Oroszországnak Kínával való gazdasági kapcsolata jó. Kínával hosszú távú olaj- és gázszállítási szerződéseket kötöttek, amihez kínai kölcsönöket vettek igénybe.

Kína hatalmas devizatartalékával néhány évtizeden belül a világ bankárává válhat. Évenkénti gazdasági növekedésének üteme 10% körüli. Tíz év alatt – többek között – tíz darab, kb. tízmillió lakossal rendelkező, megapoliszt és az azokhoz csatlakozó legkorszerűbb infrastruktúrát, mágneses gyorsvasutat kívánnak felépíteni. A kínai gazdaság fejlesztése hatalmas szívóhatást fejt ki a nyersanyagok iránt. Óriási méretű villamos-energia-, olaj-, gáz- és más fajtájú nyersanyag-, illetve élelmiszer-

igényeket támaszt a világpiacon. (Többek között ezért tapasztaljuk azt, hogy gyors ütemben növekednek a nyersanyagárak.) Hatására világszerte növekszik e termékek iránti kereslet és növekednek azok árai. Az elektronikai ipar terén Kína rendkívül kedvező helyzetben van, mivel az elektronikai és a nanotechnológiai[11] iparágak számára nélkülözhetetlen ritka földfémek lelőhelyeinek 80%-a Kínában található. [12]

Afrikában főleg a gáz- és olajmezők kitermelését segíti, azok termékeit pedig óriás tartályhajókkal szállítja Kínába. Már bejelentette részesedési igényét az északi-sarki medencében feltárandó nyersanyag-lelőhelyekre, noha nem határos a sarki tengerrel. Amennyiben Oroszország gáz- és nyersolaj kapacitásának többségét Kína leköti, akkor az EU (és azon belül Magyarország) energiaellátása komoly veszélybe kerülhet.

Hatalmi változások a világgazdaságban (2020–2030)

Ebben az időszakban felgyorsulnak azok a változások, amelyeket a 2010–2020 közötti időszakot érintően már említettünk. A követő évtizedekben, 2030-ig (illetve azon túl), a gazdasági hatalmak között Kína az első helyre kerül. A második gazdasági világhatalom az USA lesz, harmadik pedig India lehet. Negyedik helyre Brazília, az ötödik helyre Japán, hatodik helyre Oroszország, hetedik helyre Németország kerülhet. Franciaország a nyolcadik, Nagy-Britannia a kilencedik helyre esélyes, míg a tizedik helyre Mexikó pályázik. A várható változások és hatalmi helyezések befolyásolják az információs hadviselés (azon belül a kiberhadviselés) elterjedését és fejlődését.

A globális felmelegedés 2030-ra és azon túl már közvetlenül érezteti hatását, és a tengerek szintjének emelkedése hatással lehet a vezető országok hatalmi sorrendjére. Együttesen több százmilliós lélekszámú nagyvárosok kerülhetnek víz alá. A gyorsan kialakuló elárasztásos katasztrófák jelentősen meggyengíthetik az érintett országok gazdasági teljesítő képességét. Az éghajlatváltozás pedig rendkívüli módon megnehezítheti a világ élelmiszertermelését és ellátását.

Közeli hatások: csökkentik a védelmi kiadásokat (2010–2015)

Valószínű, hogy 2015-ig a világgazdasági válság, és a folyamatban levő afganisztáni háborús tevékenységek magas költségei miatt szinte valamennyi érintett országban (átlagosan 15–20%-kal) csökkentik a védelmi kiadásokat. Folyamatban levő programokat átminősítenek, lelassítanak, törölnek, vagy megvalósításukat későbbi időpontra halasztják. Új eszközök beszerzésére pályázatokat nem írnak ki. A katonai kutatások és a laboratóriumi fejlesztések terén csak a legfontosabb programokat, és azokat is csak korlátozott kapacitással folytatják.

A védelmi költségvetések relatív csökkentése igen kedvezőtlen hatást gyakorol a hadiipar termelésére. Megrendelések hiányában hadiipari üzemeket zárnak be. Elvész a speciálisan képzett munkaerő és a gyakorlati tudás. Csökkentik a repülőgépek,

11 nanométer = 10^{-9} méter

12 Egy villamos-meghajtású autóhoz 7 kilogramm tiszta lithium ritka földfém szükséges.

hadihajók, nehéz harci járművek mennyiségi termelését, mivel 2020-ig nagyméretű háborúra nem számítanak. Az aszimmetrikus háborúk nem igénylik nagy mennyiségű nehéztechnika pusztulását. A hadiipari export is jelentősen csökken, mivel a legkorszerűbb hadieszközök ára rendkívül magas (egy ötödik generációs F–35 típusú repülőgép ára közel 100 millió dollárba kerül). A hadiipari export világpiacán – viszonylag korszerű, és főleg olcsóbb eszközökkel – már Kína is megjelent.

Újabb nagyobb háború kitörésével nem számolnak (2010–2020 között)

A trendkutatók 2020-ig nagyobb méretű háborúra nem számítanak. Irak után, 2015-ig Afganisztánból is kivonják a béketeremtő és fenntartó erőket. Emellett a stratégiai elemzők úgy vélik, hogy fellobbanhatnak kisebb vagy nagyobb helyi zavargások vagy a szomszédokkal való fegyveres konfliktusok. (A 2011 elején kibontakozó iszlám forradalmak távolabbi hatását még nem lehet érdemben megítélni.)

A terrorizmust támogató iszlám országok nagyobb szabású háború kirobbantására nincsenek felkészülve. Irán rakétafenyegetései erősítik a nyugati hatalmaknak azt az elhatározását, hogy kiépítik a rakétapajzsot. Minél nagyobb a fenyegetés, annál gyorsabban épül a rakétapajzs. Addig azonban az információs hadviselésen belül tág tér kínálkozik a kibertéri műveletek legújabb módszerei és eszközei eredményes kipróbálására (ld. a Stuxnet nevű pusztító programféreg alkalmazását az iráni urándúsító központban).

Kína és Oroszország közvetlenül még fegyveres konfliktus esetén sem érdekelt Irán támogatásában. Az iszlám vallási forradalmak terjedését alapvető érdekekből kifolyólag nem támogatják. A kibontakozó arab forradalmak hosszú időre szólóan idézhetnek elő nyugtalanságot, ami közvetlenül érintheti a NATO és az EU érdekeit (átvitt értelemben Magyarország érdekeit is). Az sem zárható ki, hogy a szélsőséges iszlamisták e forradalmak kapcsán tulajdonképpen az olajár tartós emelését fegyverként alkalmazzák a Nyugat ellen.

A hadiipari termelés lassú növekedése valószínűleg 2015 és 2020 között indul be. Ennek során – az iraki és afganisztáni háborúk harctéri tapasztalatai alapján – egyrészt javítják a szárazföldi erők harcjárműveinek páncélvédettségét, korszerűsítik a vezetési és felderítő képességet. Ezt követően felkészülnek a 2020–2030 közötti időszakra, amelyben – egyebek mellett – az információs hadviseléshez felhasználható legkorszerűbb űr, légi, tengeri és szárazföldi haditechnikai eszközöket (közöttük információs hadviselési) eszközöket alkalmazhatnak.

A *kibertéri hidegháború* fogalmának megjelenése azt jelzi, hogy a trendelemzők szerint a kiberháború különböző módszereit („meleg háború" bekövetkezése nélkül) önállóan is alkalmazhatják. Ez az előfeltevés azt javasolja a világ vezetői számára, hogy a kibertéri hadviselés kérdéseivel intenzíven kell foglalkozni. Meg kell teremteni annak védelmi és támadó eszközeit, nemcsak szövetségi, nemzetvédelmi, katonai síkon, de az állami és közösségi kritikus infrastruktúra védelme, továbbá a magán szektor, vállalati szektor, sőt a civil-csoportok és az egyének kiberszabadságának megőrzése érdekében is.

Az információs hadviselés első hullámának tapasztalatai világosan jelzik, hogy a kiberhadviselést és annak műveleteit szívesen alkalmazzák az aszimmetrikus

hadviselést folytató államok vagy terrorista csoportok. Ezért támogatni kell azt a törekvést, hogy a felkészülésbe célszerű bevonni az egyetemeket (például a Zrínyi Miklós Nemzetvédelmi Egyetem [ZMNE] etikus hackerképző védelmi tanfolyamait). Világos, hogy a kibertérben 2011-ben épül ki egy NATO szövetségi „kiberpajzs". Ez alatt annyira leszünk megvédve, amennyi figyelmet és költséget erre a feladatra fordítunk.

A 2011 januárjának végén, Észak-Afrikában és másutt az interneten keresztül szervezett és irányított iszlám belső forrongások jelzik, hogy a hatalmon levő erők milyen eszközökkel válaszolnak. Belső kibertéri védelmi rendszabályként fokozták az ellenőrző lehallgatást, leállították a mobiltelefon-szolgáltatást, az SMS-szolgáltatást, az interneten keresztül történő elektronikus levelezést (e-mail) és a közösségi információcserét (Facebook, Twitter stb.).

Abból a feltevésből kiindulva, hogy belátható időn, vagyis 20–30 éven belül Keletről, továbbra is „enyhe tavaszi szél fúj", a nehézfegyverek beszerzésénél a fejlesztési költségek egy részét célszerű átcsoportosítani a kibertéri védelemre. Ismeretes, hogy egy ötödik generációs, többcélú, lopakodó típusú vadász-repülőgép beszerzési ára elérheti a 100 millió dollárt. Ehhez gépenként közel azonos nagyságú költségeket kell hozzászámítani olyan feladatokra, mint a hosszú távú üzemeltetés, a kötelező műszaki karbantartás, a tartalék hajtómű biztosítása, a fedélzeti elektronika időközi korszerűsítése, valamint a felhasznált fegyverzet és lőszer pótlása. Úgy véljük, hogy gépenként közel 200 millió dollár megtakarítással számolva, már lehet valamit kezdeni az információs hadviselés, és benne a kiber-hadviselésre történő felkészülés során.

Változás a hadviselési fajták alkalmazásában (2020–2030)

Ebben az időszakban a nemzetközi terrorizmus által kedvelt aszimmetrikus háborúk helyenként még megtalálhatók, de már újból a nagyobb méretű és szomszédos államok közötti háborúk kérdései kerülnek előtérbe (egyes értelmezések szerint elsősorban Kína és India között, illetve komoly feszültség alakulhat ki Kína és az USA között). Erre utalnak azok az amerikai jelzések, amelyek szerint felülvizsgálják a korábbi hivatalos háborús elgondolásokat és hadműveleti elveket (ezeken belül a korábbi „légi-földi", a „légi-tengeri", a „tengeri-földi", „tengerpart-melléki" hadviselési és hadműveleti elveket). Helyettük előtérbe kerülnek a „globális elsőcsapás", a „távoli célokra történő azonnali légi csapások", továbbá az internettel behálózott „információs hadszíntéren folyó kibertéri műveletek" elméletei.

Bizonyára nem véletlen, hogy az USA-ban sürgetik egy új, egyes változataiban pilótanélküli (UAV), lopakodó típusú, stratégiai bombázó mielőbbi kifejlesztését (150–180 gépről van szó). Felgyorsították a repülőgép-anyahajó fedélzeti pilótanélküli, lopakodó típusú, többcélú vadászrepülőgépek (XB–47B) fejlesztését. 2013-ra pedig megkezdik az ilyen korszerű UAV-kel való tengeri kísérleteket.

Eközben Kínában komolyan foglalkoznak olyan futurisztikus repülőeszközök és földközeli kozmikus harci űreszközök kifejlesztésével, mint például:

– pilótanélküli, lopakodó típusú hadászati bombázók;
– szupersebességű (Mach–5) globális lopakodó bombázók;
– hipersebességű (Mach–15) globális, alakváltoztató bombázók;

– az alsó kozmikus űrben működő navigációs műholdrendszer;
– vezetési, kommunikációs és csapásmérő harci műholdállomások.

Ilyen típusú harci eszközök említésénél önkéntelenül felmerül az „ellenfél lefejezésének" hadászati elgondolása, amit távolból, váratlanul és az első csapás keretében lehet végrehajtani. Könnyen belátható, hogy az említett elsőcsapás-típusú eszközök kifejlesztésére csak néhány, tudományosan, technikailag és katonailag rendkívül fejlett ország képes.

A radikális iszlám országok ballisztikus rakétafenyegetése kellő ellentevékenységi lépéseket vonhat maga után, ha elérik a közvetlen veszélyeztetési szintet.

Az információs hadviselés és a kibertéri hadviselés fejlődése (2010–2030)

Az információs hadviselés alkalmazás-szinten az öbölháborúkban, majd a balkáni háborúban és az afganisztáni háborúkban jelent meg. Később, az aszimmetrikus háború kapcsán, kiderült, hogy a katonai és nem katonai szakterületek szoros kapcsolatban vannak egymással, egymást átfedik. Elmosódik az éles határ a harctér (hadműveleti terület) és a korábbi értelemben vett hátország között. Továbbá az is világossá vált, hogy a vezetékes és vezeték nélküli, valamint űrkommunikációs hálózatokba kapcsolt, és számítógép által vezérelt kritikus infrastruktúrák működésének korlátozása már nemcsak kinetikus tűzeszközökkel (ún. pusztító hatású légi, tüzérségi, vagy rakétacsapásokkal) lehetséges, hanem nem kinetikus számítógép-hálózati eszközökkel (ún. nem halálos, korlátozó hatású, rosszindulatú programokkal stb.) is.

A számítógépek, illetve azok hálózatainak megjelenése a vezetési rendszerekben, jelentősen felértékelte az információ és a megalapozott döntéshozatal szerepét. Ekkor jelent meg a hadviselés új dimenziójának és a hadviselés egy új fajtájának fogalma, amit információs hadszíntéren vívnak, és amit információs hadviselésnek neveztek el. Az információs hadviselés tartalmáról kiderült, hogy gyűjtőfogalomként használják: egyidejűleg több szakterülettel van funkcionális kapcsolatban. Céljai elérése érdekében mind kinetikus, mind pedig nem kinetikus csapásmérő eszközöket használ. Fő feladata az optimális vezetői döntéshez szükséges megbízható információk megszerzése, a saját információ védelme, illetve annak eredményes felhasználása.

E folyamat tulajdonképpen az időhadviseléssel függ össze, mert aki a döntéshozatalhoz szükséges pontos célinformációkat ellenfelénél hamarabb szerzi meg, az időfölénybe kerül. E képesség jelentőségét a precíziós csapások korában (aminek lényege: egy lövés – biztos találat) nem lehet túlbecsülni. Ebben támadó és védelmi információs műveleteket egyaránt alkalmaznak. A fő feladat elvégzését az információs hadviselés nem önállóan, hanem több szakirányú szolgálattal együtt látja el. Közöttük egy új szakirányú, nem kinetikus fegyvernem jelent meg, aminek tevékenységeit kibertéri műveleteknek neveznek.

A kibertéri műveletek, mint új szaktevékenységi fajta, az információs hadszíntér egy új részterületén: a kiber-hadszíntéren működik. Az információs hadviselés mindhárom dimenziójában (ti. a fizikai, az információs vagy kibertéri, illetve a kognitív dimenziókban) végzett közös tevékenység együttes feladata az információs rendszerek támadása vagy védelme. Ennek alapján bátran kijelenthetjük, hogy az emlí-

tett katonai tevékenységi fajták az információs műveletek (INFOOPS) keretében egyre szorosabban kapcsolódnak egymáshoz. Tevékenységükkel tulajdonképpen csaknem teljesen lefedik a nem kinetikus (non-kinetic) hatású fegyverek teljes működési területét.

Nem katonai, állami és polgári hálózatos információs civil tevékenységek

A katonai műveletek mellett megjelentek olyan állami (országos, nemzeti) és polgári (ipari, kereskedelmi, szolgáltatási) számítógép-hálózatokra épülő szakirányú tevékenységek és műveletek, amelyekkel saját rendszereik védelmét látják el. Mivel pontos szaknyelvük még nem alakult ki, ezért működési területük megnevezésére néhány katonai hadviselési jelzőt használnak. E polgári hálózatos rendszerek a háború és béke időszakának teljes vertikumában működnek. Értelmezésük szerint a következő idő-, állapot- és szakterületekre terjednek ki: béke, hidegháború, háború; nemzeti és vállalati vezetés; kritikus infrastruktúra-szolgálat. A katonáktól átvett jelzőket gyakran olyan polgári tevékenységek megnevezésében is megtaláljuk, mint gazdasági hadviselés, kereskedelmi háború, ipari kémkedés, hálózatos hacker-tevékenység és mások.

A nem katonai célú kibertéri műveletek a politikai és polgári mozgalmak területein olyan hálózat-alapú tevékenységekhez kapcsolódnak, amelyek a társadalom különböző csoportjait szervezik és vezetik, pozitív vagy negatív értelemben egyaránt (ilyennek tekinthetők például a közösségi csoportszervező Facebook, Twitter, YouTube és más elnevezésű hálózatos körök, közösségek, társaságok). Ezek figyelése nem katonai feladat, de nemzetbiztonsági szakterület, főleg amióta az aszimmetrikus hadviselés terroristái szívesen épülnek be ilyen típusú hálózatokba. Céljuk az, hogy saját tagjaikat e hálózatokon keresztül, rejtett módon szervezzék, vezessék és irányítsák.

Mivel az aszimmetrikus hadviselés gyakran kis létszámú terroristacsoportokra épül, az információs hadviselés nagy figyelmet fordít a rejtőzködő egyének személyi profiljának elkészítésére. Erre kiváló lehetőséget nyújt egy hálózatos kisközösség, ahol a tagok kitárulkoznak és szinte mindent, önként elmondanak magukról. Ezért nemzetbiztonsági szinten, továbbá állami és vállalati szinten nem ajánlják, sőt gyakran kifejezetten tiltják, az ilyen csoportba, vagyis hálózatos közösségi portálba való belépést és az ottani kitárulkozást. Fontos megemlíteni, hogy az észak-afrikai iszlám országokban 2011 elején kibontakozott „iszlám mecset forradalmi változásokat" a Facebook felhasználásával szervezték és irányították.

Mindezek azt jelentik, hogy a teljes társadalmi tevékenységben jelen vannak az információs és kibernetikai hadviselés különböző szaktevékenységei. Ezek működésének intenzitása a második hullám végéig (2030-ig) várhatóan fokozódni fog. Ennek megbízható jele az, hogy a hálózatvédelmi vállalatok mennyisége, létszáma és azok nyeresége gyors ütemben növekszik (néhol ötszörös méretű növekedés tapasztalható). Ezt a gazdasági felfutást eredményesen használják ki az USA, India, Oroszország, Németország, Franciaország és az Egyesült Királyság szakirányú számítógépes, hálózatos, szoftveres és biztonsági vállalatai. E vállalatok nemcsak exportra termelnek, hanem szoros kapcsolatban vannak a saját nemzeti katonai információs hadviselési és kiberműveleti szervekkel, hiszen saját országuknak is szállítanak informatikai és hálózatos védelmi vagy támadó szoftvereket és eszközöket.

Magasabb síkú tudásfejlesztés

Az információs hadviselés alapeleme az információ, de központi kérdése a megszerzett, tovább fejlesztett, alkalmazott vezetői tudás. Az információ a hálózatba szervezett információs társadalom döntésrendszerének alapeleme. Legmagasabb fejlettségi foka az információs fölény. Ez azt jelenti, hogy a saját vezető több, pontosabb, megbízhatóbb döntéseket képes meghozni, mivel a „döntésre-képes" információk előbb jutnak birtokába, mint a versenytársnak, ellenfélnek, ellenségnek.

Az információs fölénynél fejlettebb és magasabb minőségű döntési képességet jelent az *intuíciós tudásfölény*. Ez a fajta tudásfölény az információs társadalmat követő, és többségében az intuícióra támaszkodó döntések társadalmában a döntésrendszer alapeleme. Ennek birtokában valamennyi emberi döntési helyzetben gyorsan, pontosan és helyesen tudunk dönteni. Ez ugyanis nem a racionális, analitikus gondolkodási eljárásra épül, hanem a tudatfeletti, holisztikus gondolkodásra, amelyben nem a részeket, hanem az egészet, és benne a mátrix-kapcsolatokat egyszerre látjuk.

Az intuíciós tudásfölény a helyzet, az összefüggések és a lényeg (tartalom) gyors felismerését, megértését és értelmezését teszi lehetővé. Az intuíciós tudásfölény az emberi intuícióra épül, amely minden embernek saját mentális (cognitiv) tudati képessége, csak nem mindenkinél egyformán fejlett. Az intuíciós képesség mentális koncentrációs és egyéb gyakorlatokkal fejleszthető. Közös érdekünk, hogy ezt a képességet széleskörű, csoportmunkát alkalmazó, interdiszciplináris kutatásokra támaszkodva mindenkinél kialakítsuk, majd tovább fejlesszük.

A tudás fajtái, és egymásra épülő, tartalmi összefüggései a következők:
- tanult tudás;
- alkalmazott tudás;
- alkotó tudás;
- vezetői intuíciós tudás;
- vezetői intuíciós bölcsesség.

A *tanult tudás* az, amit a társadalmi szocializáció és az iskolai tanulmányok során sajátítunk el. Ez teszi lehetővé, hogy felnőtt korban a társadalomnak jó szakemberei és hasznos tagjai lehessünk. Az *alkalmazott tudás* a tanult tudásra épül, amit gyakran rutintudásnak, hétköznapi szakmai tudásnak is neveznek. Ennek szakirányú összetevői:
- általános szakmai felismerő, megkülönböztető és megítélő képesség;
- általános szakmai reagáló képesség;
- általános szakmai kreatív képesség.

E képességek a tanult tudásnak hosszú idő alatt történő alkalmazása és felhalmozása révén alakulnak ki és fejlődnek.

Az *alkotó tudás* mesterember- és alkotóművész-szintű szakértői tudás, más néven kreatív fejlesztő tudás, a tanult tudás területének mind horizontális (szélességi), mind pedig vertikális (mélységi) kiterjesztése, amivel bővíteni lehet az addig megszerzett „tanult tudást" és az „alkalmazott tudást". Ennek összetevő elemei:
- szakmai tapasztalatokra támaszkodó ítélő erő;
- szövegértelmezés és tartalomalapú felismerő képesség (kontextus alapú felismerés);

– komplex holisztikus rálátási képesség, amiben nemcsak a részeket, hanem, az egészet is egyszerre látják;
– kreatív képesség, amivel újat lehet alkotni;
– intuíció alapú innovációs képesség, aminek alapján a már meglévő eszközökkel, újabb feladatok megoldását lehet megvalósítani;
– újdonság és új ötlet felismerési képesség;
– felfedező képesség;
– feltalálói, találmányt kivitelező képesség.

A *vezetői intuíciós tudás*[13] katonai síkon parancsnoki tudás. Az információs hadviselés, a kognitív hadviselés keretében, ezzel a tudásfajtával külön foglalkozik, mert szerepét a nemzetvédelmi és konkrét katonai műveletekben meghatározónak tartja. A vezetői intuíciós tudás összetevő képességelemei:

– az összefüggések, azonosságok és hasonlóságok felismerése, a különbözőségek megállapítása, a változások és az új jelenségek észrevétele;
– helyes ítéletalkotás (vezetői döntés), ami a gyakorlati tapasztalatokra és a fejlett megkülönböztető képességre támaszkodik;
– racionális tudás, ésszerű logikai tudás, („jang-típusú" tudás);
– az intuitív alapú irracionális tudás (nem racionális tudás, jin-típusú tudás, amely a „hatodik érzéket" is tartalmazza) más néven a nem-logikus gondolkodásra épülő tudás.

Ez utóbbi jellemző tulajdonságai: ösztönös döntés, megérzés-ráérzés alapú megértés és felismerés, empatikusan megértő, beleérző, átélő, belső (meditatív, „jin-típusú") spontán megismerés. Ennek a vezetői tudásfajtának szerves részét képezi az irracionális döntési képesség. Az ilyen típusú vezető nem azt teszi, amit a többi vezető (látszólag kilóg a sorból), és szembe megy az általános hagyományos irányvonallal, a trendivel. Döntései rendszerint eredményesek, de kudarcokat is megélhet. (Az ilyen vezetőre jellemző példa: Mózes, Nagy Sándor, Napóleon, Kutuzov, Churchill, De Gaulle és más kiemelkedő vezetők vagy napjainkban a magyar származású Soros György, a nemzetközi pénzügyi guru.)

A *vezetői intuitív bölcsesség*, más néven vezetői tapasztalat, a tanult tudás, az alkalmazott tudás, az alkotói tudás és a vezetői gyakorlat teljes ideje, és a kifejlesztett vezetői képességek összessége. Ennek speciális részképességeit képezik:

– A tíz-százalékos változásérzékelés képessége, más néven a trendfordulóra való ráérzés (művészi megnevezéssel: a nano- és mikro-repedések vezetők általi észlelése és felismerése).
– A kritikus tömeg (a 20–25%-nyi critical mass) megjelenésének felismerése, amely magában hordozza azt az erőt, amely képes megváltoztatni az addigi irányvonalat. (Ennek művészi megnevezése: a nano- és hajszálvékony repedéseknek vezetői szintű észrevétele, következményeinek felismerése és azok mérlegelése.)
– A kulcsfontosságú problémák kiválasztásának képessége, amelyekkel egyidejűleg számos alárendelt problémát is megoldanak (Korábban ezeket „súlyponti

13 exellence knowledge, intuition based leader/management/commander knowledge

kérdéseknek" nevezték). Ezt a képességet napjainkban fejlett megkülönböztető képességnek nevezik.

– A spontán megvilágosodás, a micro-illumination, intuíció-alapú közvetlen és azonnali megértés, felismerés, meglátás, a megoldás azonnali megtalálása. Ennek művészi megnevezése: az épületen megjelenő nagyobb repedések következményeinek gyors felismerése és velük kapcsolatban közvetlen és azonnali probléma-megoldó döntésre való jutás.

A spontán megvilágosodás olyan érzékek feletti érzékelési képességcsomag megjelenésével jár együtt, amit általában és gyűjtőnéven a „hatodik érzéknek" neveznek. A megvilágosodással olyan magasabb (mögöttes) elme-tudati képességek nyílnak meg, amelyekkel képesek vagyunk „megérezni" a tárgyaló felünk (vitapartnerünk, versenytársunk, ellenfelünk, ellenségünk) várható vagy váratlan cselekedetei mögött rejtőzködő valódi szándékot, indítékot és rejtett célokat. Ezt a képességet a győztes olimpiai versenyzők közül sokan ismerik, illetve hasznosítják: a fizikai sportokban, például a vívóknál, a teniszben és máshol, ahol pillanatok alatt kell helyesen dönteni. Katonai dimenzióban nagyon jó lenne, ha a harcoló erők a közvetlen harcban rendelkeznének ilyen képességgel. Magasabb parancsnoki és törzsszolgálati síkon az intuitív alapú gondolkodással magasabb hozzáadott értéket képviselő szellemi és fizikai terméket lehet előállítani, ami tudás fölényre támaszkodik.

A spontán megvilágosodás értelmezésének számos ősi vallási és modern pszichológiai, transz-perszonális pszichológiai, valamint vezetéstudományi leírását ismerjük. Az információs hadviselés elméleti kutatásának egyik fontos és új irányát képezik az elkövetkező években ezek komplex és egyidejűleg több tudományág általi vizsgálata, tanulmányhozása és azok eredményeinek a gyakorlatba való átültetése. E kutatásokat az információs hadviselés irányítása mellett kell végezni. Ellenkező esetben csupán egycsatornás szaktudományi problémává válnak.

Hangsúlyozni kell, hogy ilyen fajta kognitív tudás-metodikát más országok nem adnak át, mivel azok féltve őrzött titkoknak számítanak.

A magasabb vezetői tudás megszerzése érdekében az információs hadviselés fejlődésének második hullámában (2020–2030 között), olyan posztmodern elme-tudományi kognitív kutatásokat is folytatnak, amelyeket arra használnak, hogy közvetlenül nyerjenek döntést befolyásoló információkat a felső elmetudati információ-forrásokból.

Az információs hadviselés három dimenzióban: a fizikai, az információs vagy kibertéri és a kognitív, vagyis tudati dimenzióban működik. A végső cél, hogy a vezető fejében olyan fejlett elmeállapotot és gondolatokat idézzünk elő, aminek következtében a saját parancsnok jó, optimális és gyors döntést tud hozni, az ellenséges parancsnoknál pedig ennek ellenkezőjét érjük el.

A magasabb elmetudati források a nehezen hozzáférhető tudat feletti világban, a posztmodern transzperszonális világban találhatók, katonai vonatkozásban egy új hadszíntéren, a tudati térben.[14] A tudati tér másik neve: a mentális-gondolkodás tere. Ezen információs forrásokból ellenőrzött tudatmódosító eszközökkel és más meditációs technikával az irracionális döntésekhez lehet intuíció alapú információkat

14 conscioussnes, or mind sphere, domain

nyerni. Elképzelhető, hogy a katonai felső vezetők utánpótlására szolgáló törzs- és vezérkari felkészítő tanfolyamokon ilyen információkról is hallanak majd a „tábornokjelölt" hallgatók. A téma bonyolultsága komplex, multidiszciplináris, egyetemi kutatásokat igényel, és nem a távoli jövőbe utalható feladat. E tudati források (elmecsatornák) feltárása a legfejlettebb országokban a második világháború óta intenzíven folyik. Eredményes technikájuk a fejlett országok titkos szolgálatainak féltett titkait képezik. A ZMNE mindig is élenjárt a legújabb nemzetvédelmi szakterületek és feladatok elméleti feltárásában. Úgy véljük, hogy a katonai vezetéshez kapcsolódó tudati tér kutatása terén is élen jár majd.

Következtetések

Az információs hadviselés második hullámának végére (2030) a világhatalmak versengését különböző méretű, időtartamú és intenzitású információs hadviselési műveletek kísérhetik. Azon belül az információs környezetben, a kibertérben és tudati térben barátságtalan „információs hidegháborús" incidensek, akciók és műveletek végrehajtására kerülhet sor. Ezért a fejlett országokban ezek ellen intenzíven felkészülnek.

A kibertér védelme minden olyan társadalmi tevékenységi (NATO és EU szövetségi, kormányzati, miniszteriális és állami, közigazgatási, magán-vállalati, civil közösségi és magán-személyes) kört lefed, ahol hálózatos információs tevékenységek folynak. A honvédség kibervédelmi erői szervezetszerűen a saját hálózati rendszereit védik. Abból az elvből kiindulva, hogy mindenki személyesen felelős saját „vagyonának" védelméért, nem lehetnek felelősek a többi tevékenységi kör védelméért. Mindazonáltal szoros együttműködésnek kell kiépülnie a honvédségi kibervédelmi szervek és a nem katonai kibervédelmi szervek és szakemberek között. A honvédség élenjár a kibervédelem elméletének és gyakorlatának fejlesztésében, tapasztalatait szívesen átadja a magánszektornak is. A ZMNE mint közszolgálati egyetem intenzív etikus hacker-kutatásai lehetőséget nyújtanak arra, hogy az egyetem az össznemzeti kibervédelmi szakképzés központjává váljon.

Az információs hadviselés második hullámának végére, 2030 körül, már eszköz-alkalmazási szinten beérnek a nanotechnológiai és metaanyag-technikai kutatások és fejlesztések eredményei. Ezek több olyan új fegyver, haditechnikai eszköz, támadó és védő képesség megjelenését teszik lehetővé, amelyek közvetlenül vagy közvetve, de lényegesen befolyásolhatják az információs hadviselés további fejlődését. Ilyenek lehetnek az elektromágneses és információtechnikai eszközök vonatkozásában a következők:

- A kommunikáció és számítástechnikákban olyan változások, mint például a „felhő-technológia", komoly kihívást jelent a hálózatos kommunikációs eszközök követése és ellenőrzése terén.
- A „hálózatos katona" és a szenzoros robotkommunikáció megköveteli a jó minőségű beszéd, adat, vezérlő és video típusú kommunikáció állandó harctéri jelenlétét. Ezek az eszközök jelentős mértékű mini akku ellátást igényelnek. Ezért kutatják a gyengeáramú energia-források legújabb fajtáit.
- A nano-stealth technológiák, vagyis a katonák és a nehéz fegyverek, harcjárművek „láthatatlanná tétele", fényelnyelő, fényeltérítő, fényvisszaverő nanotükrök segítségével történik.

– Megjelennek a katonák által hordozható, orvlövészt felderítő, kis súlyú elektronikus hangfelderítő eszközök.
– Az út menti és az öngyilkos merénylőnél levő rejtett bombák egyidejűleg multi-spektrális kombinált felderítést igényelnek, lehetőleg miniatürizált eszközökkel.
– A multi-spektrális, miniatürizált, kombinált felderítő eszközök megjelenése napirenden lesz, amelyek akár támadó (zavaró, elfojtó stb.), akár védelmi képességekkel is rendelkezhetnek.
– A multimédiás felderítési adatok analizálásánál megjelenik a kézi számítógépes, fúziós adatfeldolgozás. A kibertérbe behatolók (hackerek) érzékelésére rendkívül gyors forrásfelkutató (forensic) és a távolból történő eszközkikapcsoló (blokkoló) technikákat alkalmaznak.
– A katonai és társadalmi (közösségi) rendszerek hálózatos fejlődése tovább halad. Eközben olyan új, polgári rendeltetésű, vezeték nélküli, mobil, szuper fejlett, kommunikációs eszközök jelennek meg, amelyeknek ismeretlen technikáját a lassan fejlődő katonai felderítő eszközök nehezen képesek követni.
– Az információs hadviseléshez tartozó és a kibontakozás állapotában levő, tudati hadviselés keretében arra törekszenek, hogy az ellenséges vezetők, az irreguláris harcosok, a terroristák, a nem barátságos lakosság tudatát olyan mértékben befolyásolják, hogy azok ellenségből, barátokká, majd együttműködővé váljanak.
– Tovább folyik a földi, légi, tengeri és űrrobotok méretének csökkentése. A nano-miniatürizálás technikája lehetővé teszi, hogy a távvezérelt vagy önállóan működő harceszközök tömege csökkenjen, és a miniatürizált eszközök fedélzetén egyidejűleg több támadó és védő (felderítő, csapásmérő és elhárító) eszközfajtát helyezzenek el, vagy tömörítsenek.
– A magasabb törzsekbe kiválasztott és a vezérkari tisztek felkészítése terén előtérbe kerülhetnek a tudati hadviselésen belül a „magas síkú intuitív tudás" megszerzésének legújabb tantárgyai, amelyeknek kidolgozása az egyetem fontos feladata lehet.

FELHASZNÁLT IRODALOM

Haig Zsolt–Várhegyi István: Hadviselés az információs hadszíntéren. Zrínyi, 2005. ISBN 963 327 391 9

Haig Zsolt–Várhegyi István: A cybertér és a cyberhadviselés értelmezése. Hadtudomány, 2008/elektronikus szám. ISSN 1215-4121 http://mhtt.eu/Hadtudomány/2008/.2008._elektronikus/2008 e. 2.pdf.

Wanderer A.: Különleges szellemi képességek. Kézirat. 2011.

Lőrinc Kálmán: A vezetésről. Hadtudomány, 2010/4. 78–88. p. ISSN 1215-4121

Kőszegvári Tibor: Kína fegyveres erői. Hadtudomány, 2010/4. 58–67 p. ISSN 1215-4121

Észtország kiberkatonákat képez. Népszabadság, 2011. 01. 15.

History and way ahead. NATO Cooperative Cyber Defence Centre of Excellence weboldal: http://www.ccdcoe.org/12.html/.

Wendel Minnich: China ramps up missile threat with DF–16 anti ship ballistic missiles (ASBM) and DF–21D anti ship cruise missiles (ASCM). Defense News, 2011. 03. 21.