Dr. Kovács László mk. őrnagy, főiskolai docens
Zrínyi Miklós Nemzetvédelmi Egyetem
Bolyai János Katonai Műszaki Kar
Informatikai tanszék
kovacs.laszlo@zmne.hu

TERRORIZMUS A DIGITÁLIS HADSZÍNTÉREN?

Jelen írás nem elemzés és nem válaszkeresés. Egyetlen célja kérdések felvetése. Olyan kérdéseké, mint például a következők: alkalmasak-e a mai modern hadseregek a terrorizmus elleni harcra? Lehetséges-e a digitális, csúcstechnikát és fegyverzetet alkalmazó hadseregeket terroristák üldözésére használni? Mit érnek ezek a fegyverek a - sokszor gerilla hadviselést, vagy azok módszereit használó - terrorista csoportok ellen? Jó befektetés volt-e a sokszor csillagászati összegek elköltése a csúcsfegyverzet és technika kifejlesztésére és beszerzésére?

This paper is neither an analysis nor answer finding. There is only one aim of it: make clear questions about the field of terrorism vs high-tech armed forces. Some questions like these: Is the modern armed forces able to fight against terrorism? Is it possible to use this digital, high-tech weaponry in the war on terrorism or against terrorists who use guerrilla warfare? Was it profitable to spend such a high amount of money to develop these weapon systems?

A különböző médiumok jóvoltából naponta hallunk robbantásos merényletekről, öngyilkos terrorakciókról, áldozatokról és sebesültekről Irakból és Afganisztánból egyaránt. A 2003. március 19-e óta eltelt közel három év alatt az amerikai fegyveres erőknek már több mint ezer katonája halt meg Irakban. Az áldozatok döntő többsége nem az első 21 napon – a klasszikus katonai műveletekben – vesztette életét, hanem az azóta eltelt időszak alatt. Ennek megfelelően több tucat kérdés merül fel az okokat keresve. Milyen körülmények között kell ellátniuk a stabilizáló, vagy a rendfenntartó erőknek a feladataikat? Fel voltak-e készülve a gerilla hadviselés legkülönfélébb módszereit folytató szembenálló fél tevékenységeire a háború előtt? Várható volt-e egyáltalán, hogy nagyon sok esetben nem is iraki, hanem más muzulmán országokból (vagy ahogy a napi híradásokból kiderül, sokszor nyugat-európai országokban lévő muzulmán csoportokból) toborzott és Irakba érkezett szembenálló féllel kell majd az esetek jelentős részében városi gerillaharcot folytatniuk? Alkalmas-e a felszerelés – kezdve a szállító járművektől, az egyéni védőfelszerelésen át a vezetési és kommunikációs eszközökig - erre az elhúzódó feladatra? Megfelelőek-e a kiképzés alatt elsajátított harceljárási módszerek ilyen körülmények között?

A felszerelést illetően el kell mondani, hogy 21. század elején a hadügyben egyre több szó esik a digitális technika és technológia dominanciájáról. Az információs technológiai forradalom eredményeit a katonák is használják a különböző műveletekben. A precíziós fegyvereket, a számítógépes vezetési rendszereket és még számtalan modern eszközt illetve berendezést megtaláljuk napjaink modern hadseregeinek felszerelései között. Ezen a téren az egyik élenjáró az USA. A hagyományos, évtizedek óta használt fegyvereket néhány éve még csak kiegészítették, ma azonban már le is váltják a digitális, számítógép vezérelt eszközök. Összefoglaló és csoportosító fogalomként ezt a technikai átfegyverzést *digitalizációnak* nevezik, amely a gyakorlatban nagyon sok esetben együtt jár azoknak az eljárásoknak az átalakulásával is, amelyek során ezeket az eszközöket alkalmazzák. Az átfegyverzést követően mindezek hatására kialakul a harctér egy újfajta értelmezése is. Ez a *digitális harctér*. Ez azt a szegmensét jelöli a harctérnek, amely több dimenzióból áll, és digitalizált

eszközöket – jelentős részben számítógép-hálózatokat – foglal magában. A digitális rendszereknek köszönhetően e szegmensben lehetővé válik a minden idős tevékenység (nap-, és évszak függetlenül). További fontos tényező, hogy nem vonalas a harcrend kialakítása, és szintén nagyon fontos jellemzőként jelenik meg az erők alkalmazási sorrendje.[1] Lehetővé válik e technológia alkalmazásával ez elektronikus céltervezés, amely jelentős – nagyon sok esetben felbecsülhetetlen – segítséget jelent, a céltervezés egyébként rendkívül összetett, komplex folyamatában. Van azonban néhány igen fontos követelmény e digitális harcmezővel szemben is. A távoli felderítés és a pontos célazonosítás és célkövetés azon kívül, hogy lehetőségként is megjelenik – köszönhetően az új, javarészt digitális felderítő eszközöknek és rendszereknek –, alapvető követelmény. A precíziós fegyverek rendkívül drága volta megköveteli az *egy lövés egy találat* elv maradéktalan alkalmazását. Bár a közhiedelemben elterjedt vélekedés, hogy számtalan precíziós fegyver, rakéta és lőszer áll például az Egyesült Államok rendelkezésére, ezek száma korántsem végtelen. Sőt nagyon is korlátozott az ilyen eszközöknek a száma, amelyeket egy-egy konfliktusban fel lehet használni. Ennek megfelelően az ezek által pusztítandó céloknak a kiválogatása igen-igen komoly feladat. Mindezekből következik, hogy a nyers túlerőnél, vagy a nehézfegyverek számánál ma már jóval fontosabb az *információ* megléte. A digitalizáció lehetővé teszi, hogy alkalmazója információs fölényre tegyen szert – azaz több, pontosabb és jobban használható információval rendelkezzen, mint a szembenálló fél –, és ezt hadműveleti fölényre váltsa. Az információért folyó küzdelmet *információs hadviselésnek*, illetve *információs műveleteknek* nevezik.

Azonban az eddig elmondottak a hagyományos hadviselési elvekre épülnek. Ezek hagyományos ellenséggel számolnak. 2001. szeptember 11-ét követően azonban alapjaiban változott meg sok minden, amit addig a hadviselésről gondoltunk.

A terrorizmus vált az egyik legrettegettebb fenyegetéssé, amely természetszerűleg ki is váltotta a nyugati államoknak azt a koalícióját, amely hol egységesen, hol komoly viták és ellentétek között gyakorlatilag háborút hirdetett a terrorizmus ellen. Bár már az 1991-es római NATO csúcs is elvégezte a kihívások és fenyegetések elemzését, amelyen a terrorizmus került a hidegháborút követő időszak egyik legfontosabb veszélyforrásává, azonban ezt követően a 2001. szeptember 11-ei események döbbentették csak rá a világot, hogy milyen veszélyes is a terrorizmus valójában.

„*Nézzünk szembe a ténnyel: a terrorizmus hosszú idő óta jelen van, és valójában a hidegháború vége előtti időkre nyúlik vissza. De míg a terroristákat sok merénylet miatt terheli felelősség, soha nem jelentettek veszélyt a világ létezésére. Leggonoszabb formájában a terrorista fenyegetést a tömegpusztító fegyverek (WMD) által képviselt fenyegetéssel együtt kell vizsgálni, habár a terroristák igazából még nem vetettek be ilyen fegyvereket. Legalábbis eddig nem. Egyértelmű, hogy a terrorizmus és a tömegpusztító fegyverek baljós kombinációja hatalmas veszélyt jelent. De a különbség e fenyegetés és a hidegháború egymás biztos elpusztításának veszélyét hordozó fenyegetése között az, hogy az utóbbi a létezésünket tette kérdésessé*."[2]

Az terrorizmus elleni közös fellépés ellenére azonban még ma sincs egységes megfogalmazás magára a terrorizmusra. Mindegyik megfogalmazás abból a szemszögből értelmezi a terrorizmust, amely a definíciót alkotó sajátja. Ennek megfelelően nemcsak minden szervezet, hanem még nagyon sok esetben a különböző országok is más és más

[1] Az erők alkalmazási sorrendje alapvető fontosságú a legújabban megjelent hadviselési elv a Hatás Alapú Műveletek (Effect Based Operations – EBO) tervezése, illetve végrehajtása során. A hatás alapú műveletek esetében a különböző tevékenységek különböző elsődleges, illetve másodlagos hatásait úgy tervezik meg, hogy azok egy-egy ponton találkozzanak, azok egymást kiegészítik, megsokszorozzák, így erősítve a külön-külön végrehajtott akciók eredményeként létrejövő jóval kisebb hatásokat.

[2] Vita: Olyan nagyok-e a kihívások, amelyekkel a NATO napjainkban szembesül, mint a hidegháború idején? http://www.nato.int/docu/review/2003/issue4/hungarian/debate.html

meghatározást értenek ez alatt. Természetesen a terrorista szervezetek is eltérő fogalmat alkotnak például az olyan akciókról, mint az amerikaiak iraki beavatkozása, hiszen ezt ők erősen állami terrorizmusnak tartják, a saját akcióikat pedig gyakran szabadságharcként értelmezik.

Vegyes tehát a kép. Ráadásul máris itt van egy újabb fajta terrorizmus. Ez, pedig az *információs terrorizmus*. Mivel a nyugati országok gyakorlatilag mindegyike – bár eltérő módon, de – óriási mértékben ki van szolgáltatva azoknak az információs rendszereknek, amelyek a társadalmat, vagy funkcionális feladataikban, vagy alapvető működésükben támogatják.[3] Ezt a kiszolgáltatottságot használja ki az információs terrorizmus, amely nem jelent mást, mint az információs infrastruktúrákat felhasználó – alapvetően kritikus információs infrastruktúra elleni támadás módszereit alkalmazó – csoport vagy szervezet által elkövetett támadás, amelyekkel képesek a számítógép-hálózatokba szoftveres, vagy hardveres úton beavatkozni a céljaik elérése érdekében. A célok tekintetében az információs terrorizmusnak szoros a kapcsolata a hagyományos terrorizmussal, ám a módszerek újak. Az információs infrastruktúrák elleni információs támadás kombinálható hagyományos fizikai támadással is. Óriási tehát a veszélye ennek az új terrorizmusnak, hiszen ha sikerül bármilyen kis károkat is okozni a társadalmainkat működtető információs infrastruktúrákban, akár fizikai támadással, akár információs úton, az hatalmas anyagi és emberi áldozatokkal járhat.

De térjünk vissza a hagyományos terrorizmusra, illetve az ellene folytatott háborúra, hiszen a terrorizmus elleni háború valóságos katonai műveletekké vált Afganisztánban és Irakban. Mindkét országban, de leginkább Irak esetében szembesültek a műveleteket folytató katonák (és természetesen a mindig gyors és látványos eredményeket látni akaró politikusok), hogy nem mindig – sőt az esetek többségében egyáltalán nem –, érvényesek a hagyományos hadműveleti elvek. Nézzük, mivel találták szembe magukat a katonák:

- közigazgatás hiánya;
- 50-60 %-os munkanélkilüség;
- vallási és etnikai ellentétek (pl.: Síita, Szunnita)
- aszimmetrikus fenyegetések;
- helyi rendfenntartók hiánya vagy képzetlensége;
- külföldről beáramló fegyverek és „terroristák” (pl.: Irán, Szaúd-Arábia);
- civil lakosságra való nyomásgyakorlás (pl.: öngyilkos merényletek) – *terror*;
- naponta több támadás járőrök, konvojok ellen;
- hagyományos katonai akciók nem érnek el látványos eredményeket.

Mindezek összegzett hatása oda vezetett, hogy a hagyományos katonai műveletek helyett úgynevezett „*Unconventional Warfare*”-t, azaz nem konvencionális elvek és szabályok szerinti műveleteket kénytelenek folyamatosan végrehajtani a katonák.

És mit jelent ebben az esetben a digitális csúcstechnika? – hiszen e kérdés mozgatja jelen vizsgálódást. Jelent-e valami előnyt, hogy high-tech fegyverzetet, kommunikációt, vagy akár műholdakat tud használni, például az USA? A válasz összetett és nem is teljesen egyértelmű. Teljesen pozitív lehet a válasz abban a tekintetben, hogy a high-tech eszközök és rendszerek alkalmazása és használata, akár a mindennapi járőrözésben is előnyöket jelent. Előnyöket, mert ezek segítségével gyorsabb, pontosabb a felderítés és az értékelés, ezáltal a feladatok konkrét végrehajtásának megtervezése is hatékonyabb lehet. Sokkal eredményesebb lehet a parancsnokok és az alárendeltek, vagy az együttműködők kapcsolattartása,

[3] Az információs infrastruktúrákat alapvetően két részre oszthatjuk: támogató és funkcionális infrastruktúrákra. Támogató információs infrastruktúra többek között például a villamos energia hálózat, gáz, vagy vízhálózat; funkcionális információs infrastruktúra többek között például a banki vagy pénzügyi rendszer, a kommunikáció rendszere, stb.

koordinálása a modern kommunikációs eszközöknek köszönhetően. A hatékonyság itt nagyon sok esetben a veszélyes helyek elkerülését, a terrorista gyanú személyek felkutatását és megtalálását, valamint a jóval kevesebb saját oldali veszteséget jelentheti. Ráadásul a gyorsabb információcsere hatékonyabb reagálást tehet lehetővé. Azaz kijelenthető, hogy a csúcstechnika ebben az esetbe is életeket menthet a saját oldalon. Mindezek azonban megkövetelik a valós idejű felderítést, ennek teljes integritását valamint ezen eszközök, rendszerek maximális kihasználását és megbízható működését.

Nem egyértelmű és pozitív a válasz azonban abban az esetben, ha öngyilkos merénylőkkel, útszéli távirányítású robbantásokkal állunk szemben. Ebben az esetben is lehet – sőt kell is – alkalmazni a digitális technikát, hiszen egy útszéli rádió-távirányítású pokolgép hatékonyan blokkolható szélessávú rádiózavaró eszközzel, amelyet az úton haladó járműre szerelnek. De, ez sem jelent minden esetben teljes védelmet. Mégis a megelőzésben, a felkészülésben, vagy akár az elkövetők felkutatásában hatékony szerep hárulhat a csúcstechnikára. Például a pokolgépes merényletek közvetlen környezetében lévő járókelőktől kézi számítógép segítségével vett ujjlenyomat, annak adatbázisban való rögzítése és feldolgozása szintén komoly eredményeket jelenthet az elkövetők körének felderítésében.

Természetesen a helyzet teljes rendezéséhez nem elegendő használni és alkalmazni a csúcstechnikát képviselő eszközöket, rendszereket. A megoldás nem csak a katonák kezében van. Elsősorban politikai és gazdasági stabilizálásra van szükség, amely közös és párhuzamos katonai és politikai erőfeszítéseket igényel. Ennek során ki kell használni azokat az előnyöket, amelyeket a digitális technika jelent, hiszen ha nem is csak a hagyományos digitális hadszíntéren, de a nem-konvencionális, gerilla hadviselésben is létjogosultságuk van ezen eszközöknek.

Az előadás és a publikáció a Magyar Tudományos Akadémia Bolyai János Kutatási Ösztöndíjának támogatásával készült.

This paper and presentation was supported by the János Bolyai Research Scholarship of the Hungarian Academy of Sciences