HADMÉRNÖK

XII. Évfolyam „KÖFOP" szám – 2017. október

A KÖZÖSSÉGI MÉDIA, MINT AZ INFORMÁCIÓS HADSZÍNTÉR SPECIÁLIS TARTOMÁNYA

SOCIAL MEDIA AS THE SPECIAL PART OF THE INFORMATION FIELD OF OPERATIONS

BÁNYÁSZ Péter

(ORCID: 0000-0002-7308-9304)

banyasz.peter@uni-nke.hu

Absztrakt

A közösségi média, akár tetszik, akár nem, a mindennapjaink megkerülhetetlen részévé vált. Nem csak a magánemberek, de a civil és politikai szervezetek is rendszeresen használják különböző okokból kifolyólag. A közösségi oldalak azonban számos olyan lehetőséget biztosítanak, amelyek megkerülhetetlenek a katonai-, rendőri- és nemzetbiztonsági szolgálatoknak, hogy hatékonyan elláthassák jogszabályban meghatározott feladataikat. Legyen szó hírszerzésről, lélektani műveletek végzéséről, számítógép-hálózati műveletekről, a közösségi média ezek esetében is rendkívül hasznos eszköz. Jelen tanulmány a közösségi média egy merőben új értelmezésére tesz kísérletet.

A mű a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosítószámú, „A jó kormányzást megalapozó közszolgálat-fejlesztés" elnevezésű kiemelt projektben működtetett Concha Győző Doktori Program keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült.

Kulcsszavak: *közösségi média, információs műveletek, kiberbiztonság*

Abstract

The social media is whether we like it or not the part of our life. Not only the civil people, but the NGO and the political organizations use them because of many different reasons. The social media sites ensure many opportunities for the military-, law enforcement-, secret services to perform their tasks and responsibilities. No matter if it's about intelligence, psychological operations, computer-network operations, the social media is a useful tool. This study represents the social media from a new aspect.

„The work was created in commission of the National University of Public Service under the priority project KÖFOP-2.1.2-VEKOP-15-2016-00001 titled „Public Service Development Establishing Good Governance" in the Concha Doctoral Program.

Keywords: *social media, information operations, cybersecurity*

A kézirat benyújtásának dátuma (Date of the submission): 2017.07.31.
A kézirat elfogadásának dátuma (Date of the acceptance): 2017.10.12.

BEVEZETÉS

2017-re a közösségi oldalak megkerülhetetlenné váltak életünkben. Akár szeretjük őket, akár nem, akár használjuk őket, akár nem, hatásuk alól nem vonhatja ki magát senki. Ennek igazolására Donald Trump 2016-os elnöki kampánya szolgál talán a legjobb példával. Már Barack Obama elnökké választásában is nagy szerepet tulajdonítottak a közösségi média politikai kampányban betöltött szerepében, de 2016-ra a közösségi média több területen igen komoly hatással volt Donald Trump győzelmében, az információbiztonságtól kezdve a big data analízisen keresztül a lélektani műveletek alkalmazásáig bezárólag. Ami egészen biztosan kijelenthető, a Trump kampányban nagy szerepe volt egy Cambridge Analytica nevű big data analízissel és lélektani műveletekkel foglalkozó cégnek[1] [1], rengeteg, a közösségi oldalakon vírusként terjedő álhírt közlő oldalaknak [2], a Demokrata Nemzeti Bizottság, a Clinton-kampány tagjainak, illetve magának Hillary Clintonnak az igen alacsony szintű adat- és információbiztonsági tudatossága, valamint feltehetően az orosz nemzetbiztonsági szolgálatok fentieket ötvöző aktív intézkedései [3].

Jelen tanulmánynak nem célja a Trump kampány e célból történő elemzése, már csak azért sem, mert azok önmagukban egy önálló írást érdemelnek, fontos azonban látni, hogy a példaként említetteket feltehetően nem először, és egészen biztosan nem utoljára alkalmazták katonai, nemzetbiztonsági szolgálatok a közösségi oldalakon. Mindezek azonban csak egy kis szeletét jelentik azoknak az eszközöknek és eljárásoknak, amelyekkel a katonai-, rendészeti- és nemzetbiztonsági szolgálatok hatékonyabban láthatják el jogszabályban meghatározott tevékenységeiket.

A közösségi médiát sokan próbálták meghatározni a saját tudományterületük szemüvegén keresztül. E cikk keretein belül a közösségi média egy új típusú értelmezésére teszek kísérletet: megítélésem szerint a közösségi média az információs hadszíntér egy speciális tartományaként értelmezhető.

KÖZÖSSÉGI MÉDIA SZEREPE

A Kat. IV. fejezete hatálya alá nem tartozó gazdálkodó szervezetek tevékenységük során bár korlátozott mennyiségben, de tárolhatnak, felhasználhatnak, gyárthatnak veszélyes anyagot. Így a Kat. IV. fejezete és a Vhr. hatálya alá nem tartozó gazdálkodó szervezeteknél esetlegesen bekövetkező rendkívüli események során nem zárható ki veszélyes anyag ellenőrizetlenül történő szabadba kerülése. Katasztrófavédelmi szempontból kiemelten fontos kérdés lehet annak megválaszolása, hogy

Az Oxford Dictionaries [4] a közösségi médiát weboldalak és alkalmazások összességeként írja le, amelynek során a felhasználók tartalmat készíthetnek és megoszthatnak a közösségi hálózatokon. Ehhez a definícióhoz köthető Andreas Kaplan- Michael Haenlein által megfogalmazottak, mi szerint a közösségi média „*internetes alkalmazások olyan csoportja, amely a web 2.0 ideológiai és technológiai alapjaira épül, ami elősegíti, hogy kialakuljon és átalakuljon a felhasználó által létrehozott tartalom"* [5].

Mint látható, a kulcs a felhasználói tartalom előállításban ragadható meg. Tartalomelőállításra azonban nem csak az internetes alkalmazások alkalmasak, számos okos mobil eszközre megírt applikációval is könnyedén állíthatunk elő mindenféle tartalmat. Ez alapján a közösségi médiához sorolom a különböző okostelefonokra írt alkalmazásokat is, hiszen egyrészt ezek is a felhasználók közti interakcióra épülnek, másrészt integratív szerepet

[1] Jelentős szerepet tulajdonítanak e cégnek a Brexit kampányban a kilépés pártiak győzelmében is.

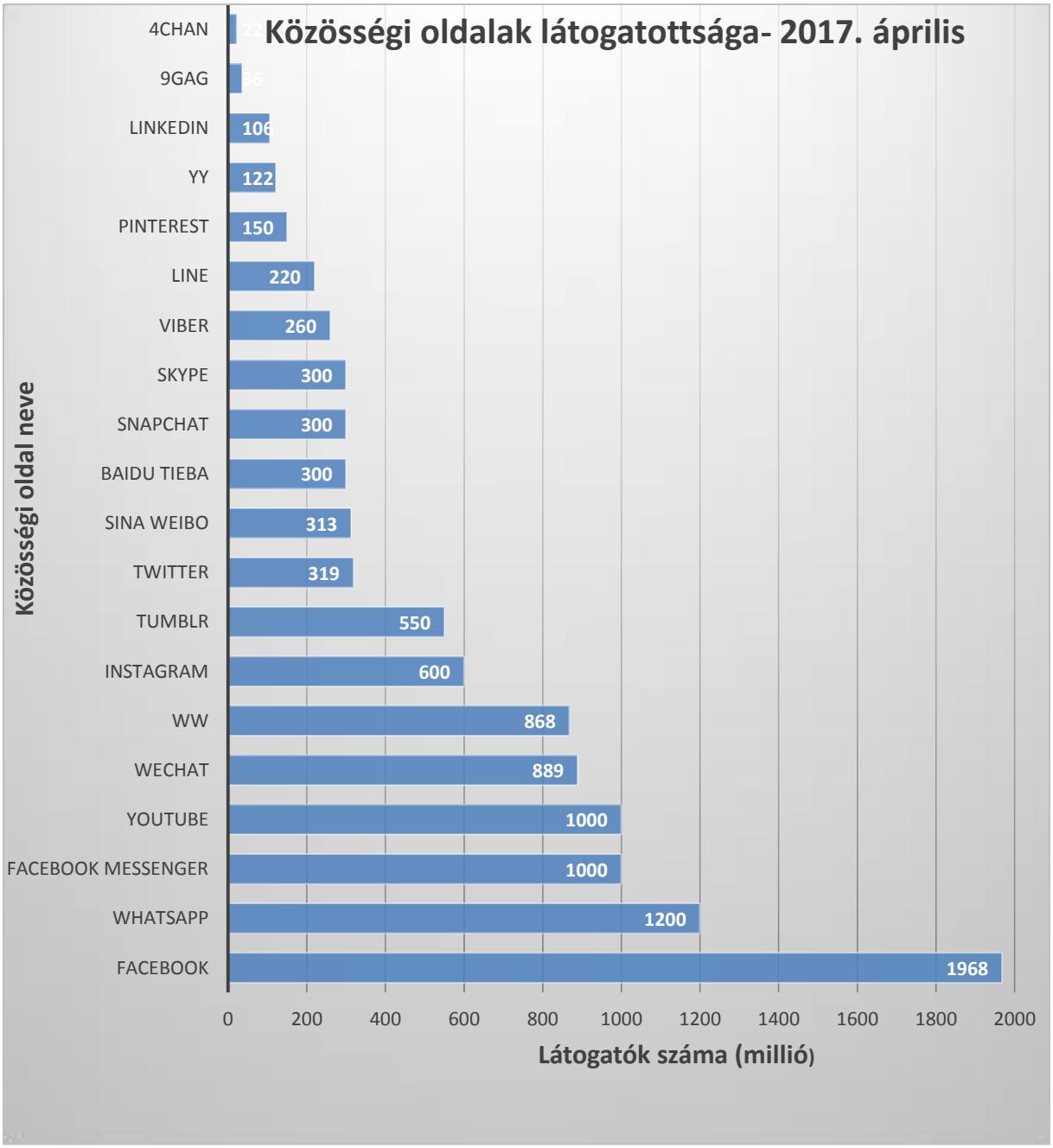
töltenek be a különböző közösségi eszközök közt. Megítélésem szerint ezt a Google példája igazolja leginkább: a kezdetben keresőszolgáltatóként működő cég mára egy személyben integrálja a különböző közösségi eszközöket (blogszolgáltató, fénykép- és videómegosztó, közösségi hálózat, okostelefon platform stb.).

Az integráció elsősorban a közösségi oldalak és a gazdasági alrendszer kölcsönös, egymásra ható interakcióiból fakad, hiszen évről évre jelentős mértékben növekszik az online hirdetési piac, amelyből az oldalak igyekeznek a lehető legnagyobb profitot maximalizálni. Mindez konstans innovációhoz vezet, ugyanis a felhasználók akkor termelik a reklámbevételt, ha az oldalt böngészik. A felhasználók megtartása és számuk növelése érdekében a közösségi oldalaknak folyamatosan meg kell újulni, aminek egyik eszköze, hogy a vetélytársak jobb szolgáltatásait vagy felvásárolják, és úgy integrálják magukba (pl. az Instagram vagy a WhatApp Facebook által történő felvásárlása) vagy hasonlókat vezetnek be (pl. a Snapchat mintájára jelent meg 2017 tavaszán a Facebook „Napom" funkciója).

A felhasználók megtartásának egy másik fontos eszköze, hogy olyan tartalommal találkozzanak, amelyek egészen biztos érdekli őket. A Facebookon a felhasználóknak átlagosan több száz ismerőse van, nem ritka az ezer fölötti ismerősszám sem. Tartalomgyártási szokásoktól függően olyan mértékű tartalommal találkozna a felhasználó, ami minden bizonnyal elriasztaná az oldalról, hiszen mindenkit egy behatárolható tartalom érdekel elsősorban, és az is egy behatárolt csoportból. Az érdeklődésnek megfelelő tartalom azonban könnyen elvész a megosztott tartalmak tengerében, így a Facebook egy olyan algoritmust dolgozott ki, ami a felhasználók viselkedését elemezve megpróbálja kitalálni, mi érdekli a felhasználót, és csak azt a tartalmat jeleníti meg előtte, elrejtve minden olyan megosztást, ami az algoritmus szerint nem érdekelheti. Magának az algoritmusnak a pontos működése nem ismert, csupán részinformációkat ismerünk. Ezek alapján tudható, hogy több mint 29 ezer szempont alapján vizsgálja a felhasználók viselkedését a Facebook – ebből nagyjából hatszázra tehető azon indikátorok száma, amelyeket külső adatbrókerektől vásárolnak meg –: az olyan egyértelmű dolgoktól kezdve, hogy kikkel beszélünk, kiknek kattintunk leggyakrabban a megosztásaira, milyen tartalmakat likeolunk stb., az olyan kevésbé evidens, ám érhető dolgokon keresztül, hogy hol tartózkodik általában az egerünk böngészés közben (a hirdetések elhelyezése okán fontos), az olyan nehezen magyarázható dolgokig bezárólag, hogy milyen tartalmat töröltünk ki, mielőtt elküldtük volna ismerőseinknek. Ez utóbbit egy, a Facebook által végzett kutatásaiból tudjuk, amit hivatalosan az öncenzúra vizsgálatával indokolt a cég [6].

Nem nehéz belátni, ha egy oldal ennyi mindent tud rólunk, azt nem csupán marketing célokra használhatja fel.

De mik a legnépszerűbb oldalak 2017-ben? Az 1. számú ábráról a Facebook dominanciája olvasható le [7].



1. ábra Közösségi oldalak látogatottsága 2017. áprilisában (saját szerkesztés, Forrás: Statista.com)

Meg kell jegyezni, az ábrán több olyan közösségi oldal is helyet kapott, amelyek Észak-Amerikában vagy Nyugat-Európában kevésbé ismertek, azonban más területeken nagy népszerűségnek örvendenek (ilyen pl. a kínai Sina Weibo). Ennek egy művelet megtervezésénél van jelentősége, hiszen míg az Egyesült Államokban a Twitter nagy népszerűségnek örvend, addig Magyarországban elvétve használják. Az ábrán nem csupán közösségi hálózatokat találhatunk, több csevegő alkalmazás helyet kapott (pl. WhatsApp, Facebook Messenger, Skype, Viber), de kép- és videómegosztó oldalakat, blogokat, fórumokat (pl. 4chan) is láthatunk. Az ábrán nem a napi elérések (daily active user, DaU) szerepelnek, hanem a regisztráltak száma, kivéve a 9gag esetében, ott a Facebook oldal

követőinek a száma látható (36 millió). A Facebook népszerűsége okán érdemes az oldal DaU-ját is figyelembe venni, ami a 2017-es első negyedévi jelentés alapján 1,28 milliárd embert jelent [8]. Ez napi elérés tekintetében rendkívül jelentősnek mondható,[2] különösen abból a szempontból, hogy az internetezők növekvő aránya a Facebookot tekinti elsődleges hírforrásnak.

Nem szabad elfelejtkezni arról sem, hogy egyre több esetben alakul ki függőség ezeknek az oldalaknak a használatával kapcsolatban. A brit Royal Society for Public Health felmérést készített a közösségi oldalak egészségkárosító hatásairól a tinédzserek körében. A túlzott közösségi média használat magányosságot, szorongást okoz a használók körében [10].

A közösségi média fogalmából kiindulva az első közösségi oldalak így már a 90-es évek elején megjelentek, hiszen a fórumok, IRC, chat oldalak is hasonló elven működtek, az igazi áttörés azonban a 2000-es évek közepén következett be, amikor robbanás szerűen kezdtek fejlődni a közösségi oldalak. A közösségi oldalakban rejlő lehetőségeket korán felismerték a nemzetbiztonsági szolgálatok is, ahogy ezt az Edward Snowden által kiszivárogtatott iratokból tudjuk [11].

A KIBERTÉR, MINT HADSZÍNTÉR

Annak érdekében, hogy a közösségi média címben megfogalmazott jellemzőjét igazoljam, szükségesnek mutatkozik a kibertér ez irányú fejlődését bemutatnom. A kibertér kifejezést William Gibson sci-fi író használta először az 1982-ben megjelent Izzó króm című novellájában, majd az 1984-es Neurománc című regényében, és innen szivárgott át a köztudatba. Gibson a kibertér fogalma alatt hálózatba kapcsolt számítógép-terminálokról közvetlenül elérhető digitális teret értett. A kibertér kifejezés a görög kyber (hajózni) szóból származik, és hajózásra alkalmas teret jelent. A Neurománc óta különböző fogalmi meghatározások születtek a kibertérre, de földrajzi értelemben az infokommunikációs technológiákban megnyilvánuló térfogalmat jelent, nem pedig a technológiára utal [12]. A kibertér térszerkezetének leírására számos kísérlet született geometriai, formai, szerkezeti jellemzőinek meghatározásával. A térgeometriai jellemzők feltárása azonban nem egyszerű, hiszen a kibertér számos különböző, eltérő funkciójú tartományból tevődik össze, illetve mindegyike mesterségesen konstruált. A különböző térfelfogásokat az alapján alkották meg, hogy a fogalom használói a kibertér mely csoportjával foglalkoztak [13]. Ez alapján beszélünk:

- koncepcionális térfelfogásról- ez alatt gyakorlatilag az Internetet értjük;
- infrastrukturális térfelfogásról- ez alapvetően a fizikai dimenziót öleli fel, beleértve a szervereket, gerinchálózatokat stb.;
- oldal térképek terei;
- sajátos „páva” modellek terei;
- virtuális világok.

[2] Ezzel a Facebook globálisan a második leglátogatottabb weboldal. Sokat mondó, hogy a Similar Web, internetes forgalmat figyelő honlap top 10-es listája az alábbiak szerint alakult: Google, Facebook, YouTube, Yahoo, VKontakte, Wikipedia, Twitter, Live, Google.com.br, Amazon. Az Amazont leszámítva mindegyik oldal beletartozik a közösségi média fogalmába. A Googlet a korábban kifejtett integratív tulajdonsága alapján sorolom ide. Érdekességként megemlíthető, hogy a 11. helyen a kínai Baidu nevű közösségi oldal szerepel [9]

Bár a kibertér szakít a klasszikus térfelfogással, mivel számos fizikai alapvonást nem képes értelmezni, amelyek hatására a tér halmazt alkot, mégis felfedezhetőek bizonyos térszerkezeti elemek, de ezek által teljesen új interpretációt jelentve a virtuális térben. Ilyen kategóriaként értelmezhető a külső és belső tér, a hely, a helyzet, a távolság, az irány, a határ, illetve a különböző szintek. Mészáros Rezső A kibertér társadalomföldrajzi megközelítése című munkájában különböző viszonyrendszereket jellemez, a kibertér és az egyén, a társadalom, a politikai-, gazdasági alrendszerek kapcsolatában. Az elmúlt évtizedben azonban kialakult a kibertér, mint hadszíntér értelmezése.

A kibertér definiálására a magyar stratégiai gondolkodásban is születtek kísérletek. A Magyarország Nemzeti Kiberbiztonsági Stratégiája a következő megfogalmazást tartalmazza: „*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*” [14]. Ezzel szemben a Magyar Honvédség Kibervédelmi Szakmai Koncepciója az alábbiakban alapján definiálja a kiberteret: „*az elektromágneses spektrum használatával meghatározató, dinamikusan változó tartomány, mely összekapcsolt hálózatok, eszközök és kiegészítő fizikai infrastruktúrák közötti adatok kezelésére szolgál*” [15].

Haig Zsolt megállapítását kölcsönözve „*egyértelműen kijelenthetjük, a kibertér fontos jellemzője, hogy abban az elektromágneses spektrumot felhasználva és/vagy vezetékes kapcsolaton keresztül hálózatba kötött infokommunikációs rendszerek működnek, amelyek különböző elektronikus információkezelési tevékenységeket (elektronikai úton végrehajtott adatszerzés, adatfeldolgozás, adattárolás, kommunikáció stb.) végeznek. A különböző hálózatba kapcsolt infokommunikációs rendszerek az információs környezet azon tartományát használják, amelyben e rendszerek működnek, léteznek (fizikai dimenzióban), a különböző elektronikus információkezelési folyamatok zajlanak (információs dimenzióban), valamint e rendszerek elleni tevékenység és védelem megvalósul (fizikai és információs dimenzióban). Ebből következően tehát a kibertér az információs környezet fizikai és információs dimenziójában értelmezhető*” [16].

Az Észak- Atlanti Szövetség (továbbiakban NATO) 2010 novemberében Lisszabonban elfogadott stratégiai koncepciójának egyik újdonságának tekinthető a kibervédelem hangsúlyos megjelenése [17]. Az afganisztáni hadszíntér kezdetétől visszatérő elem, hogy biztosítani kell a NATO cselekvőképességét azokon a területeken, amelyek bár nem tartoznak a Szövetség illetékessége alá, de a mindennapok, különösen a műveletek során nagy mértékben függ tőle [18]. A Szövetséges Transzformációs Parancsnokság parancsnoka, Abrial vezérezredes utasítást adott ki a stratégiai elemzőrészlegnek egy tanulmány elkészítésére, ami feltárja a NATO sebezhetőségét a globális közös tereken [19]. Jelentős lépésnek tekinthető a 2016. július 8-9. között Varsóban megrendezett NATO-csúcs, ahol a Szervezet a kibervédelmet a NATO kollektív védelmi feladatai közé sorolták. E mellett azt is deklarálták, hogy a NATO támogatni fogja a tagállamokat érő kiberfenyegetettség csökkentésére vonatkozó kutatásokat, együttműködéseket. [20]

A globális közös terek a nemzetközi jogban a res communis omnium usus, vagyis a szabadon használható terület fogalmába tartoznak bele. Az államok felségjoga csak bizonyos km-ig terjed, ezt meghaladva nem érvényesíthetik. A res communis omnium usus hatályába tartozik a nyílt tenger,[3] a tengerfenék, az Antarktisz és a világűr. A hivatkozott tanulmányban azonban a korábbi földrajzi kategóriák, mint a tengerek és óceánok, légtér és világűr

[3]A tengerparti államhoz tartozik a partja mentén elterülő sáv, ami a parttól számított 12 mérföldet (kb. 22,2 km) foglalja magába.

kibővülnek a virtuális dimenzióval, a kibertérrel. A globális közös terek nem köthetőek egy adott nemzet szuverenitásához, de a bennük rejlő biztonsági kihívások jelentősnek tekinthetőek a NATO és tagországai számára. De nem csak a belőlük származó biztonsági kihívások miatt számít relevánsnak e négy dimenzió védelme, a NATO műveleteiben aktívan használja e területek mindegyikét, legyen szó pl. csapatok mozgatásáról tengeren, levegőben, kommunikáció biztosításáról, a vezetés-irányítás fenntartásáról a kibertérben, a világűrben. Ezek mellett a NATO feladata a tagországok érdekeinek védelme is, ami többek között a kereskedelemben, távközlésben, kutatásban is jelentkezik. Ahhoz, hogy a Szövetség képes legyen mind a négy dimenzióban végrehajtani feladatait, jelentős felderítő, stratégiai elemző, tervező, vezetési, képességfejlesztési, logisztikai, műveleti előkészítő tevékenységet követel meg. Bár mind a négy közös tér esetében találunk azonosságot, ezért összekapcsolódnak, átfedik egymást (lásd pl. a vezetés-irányítás fenntartását), de mindegyik egyben rendszer specifikus jellemzőkkel is leírható.

Az információs eszközök napjainkban tapasztalt elterjedése okán az információs tevékenységek az információs környezetben, vagy más néven, az információs színtéren zajlanak. Segítségül hívva az USA összhaderőnemi információs műveletek doktrínáját, „*az információs környezet mindazon egyének, szervezetek és rendszerek összessége akik, és amelyek az információ gyűjtésével, feldolgozásával, szétosztásával foglalkoznak*” [21]. Az információs környezet megjelenése kibővítette a katonai műveleteket, illetve további tartományokkal egészítette ki [22]. A hadszíntér fizikai dimenziója kiegészült ezáltal egy nem földrajzi dimenzióval, amely a katonai információs környezet kialakulásához, vagyis az információs hadszíntér megjelenéséhez vezetett. Az információs hadszíntéren folytatott műveleteket, amelyek az információ megszerzéséért, megtartásáért, hatékony felhasználásáért végeznek, információs műveleteknek nevezzük. Az információs jelző azonban nem csak az említett tevékenységek végzésére utal, egyben azt is jelenti, hogy a hagyományos katonai műveleteket jelentősen támogatják az infokommunikációs technológiák. Az információs hadszíntér magában foglalja a valós és virtuális tereket, eszközöket, helyeket, rendszereket, amelyekben az információ megszerzésével, előállításával, felhasználásával, értékelésével, elemzésével, felhasználásával, védelmével foglalkoznak. Ebből következően az információs hadszíntér a hadszíntér egy speciális tartománya, amelyen belül a szemben álló felek az információ birtoklásáért, a másiknál hatékonyabb felhasználásáért versengenek.

Az információs hadviselés célja az információs fölény, illetve ennek birtoklását követően a vezetési fölény megszerzése, a saját oldali vezetési folyamat számára az időcsökkentés, míg az ellenfél számára az időnövelés. Az információs hadviselés tevékenységi körébe soroljuk az alábbiakat:

- műveleti biztonság;
- dezinformáció;
- lélektani műveletek;
- információs célpontok fizikai pusztítása;
- elektronikai hadviselés;
- számítógép-hálózati műveletek [23].

A NATO információs műveletekkel foglalkozó 2009-ben kiadott doktrínája (továbbiakban AJP-3.10) [24] az alábbi képességeket, eszközöket és eljárásokat határozta meg az információs célkitűzésekre vonatkozóan:

- PSYOPS;
- megjelenés, viselkedés, arculat (továbbiakban PPP);
- műveleti biztonság (továbbiakban OPSEC);
- információbiztonság (továbbiakban INFOSEC);
- megtévesztés (továbbiakban MILDEC);

- elektronikai hadviselés (továbbiakban EW);
- fizikai pusztítás;
- kulcsfontosságú vezetőkkel kapcsolatos tevékenység (KLE);
- számítógép-hálózati műveletek (továbbiakban CNO);
- civil-katonai együttműködés (továbbiakban CIMIC).

Az információs hadviselés támadó és védelmi célból egyaránt alkalmazható a katonai, politikai, gazdasági tevékenységek mindegyik színterén. A támadó jellegű információs hadviselés célja, hogy a speciális érdekekre vagy speciális fenyegetésekre választ adva hatást gyakoroljanak a másik félre, akár békében, válságban vagy konfliktus idején, a védelmi információs hadviselés célja pedig, hogy megvédje a saját információkat, illetve fenntartsa az információkhoz való hozzáférést, továbbá elősegítse az információs rendszerek hatékony használatát.

A KÖZÖSSÉGI MÉDIA, MINT AZ INFORMÁCIÓS HADSZÍNTÉR SPECIÁLIS TARTOMÁNYA

Úgy vélem, nem szorul különösen bizonyításra, hogy a közösségi média a kibertér egy tartománya, hiszen az interakciók rajta keresztül zajlanak. Abban az esetben, ha az információs hadszíntér tartományaként nevesítjük a közösségi médiát, azonosítanunk kell

- a tartomány kereteit,
- illetve azokat a területeket, amelyeken az információs műveletek végzésében szerepet játszik.

A tartomány keretei a közösségi média és az egyén, illetve a társadalmi alrendszerek viszonyrendszerében vizsgálandóak. A közösségi média fogalmából adódik, hogy alapvetően az egyének interakciójából épül fel. Ez a társas viszonyrendszer a közösségi média különböző alkotóin folytatott kommunikáción keresztül realizálódik. Különbséget kell tenni azonban az egyes generációk között, hiszen eltérő attitűdök jellemzik mind az internet, mind a közösségi média használatban, illetve egy esetleges művelet során a célcsoportok meghatározását követően figyelmet kell szentelni ezekre a jellemzőkre.

Az egyes generációkat demográfiai jellemzők, elsősorban a születési év alapján határozzák meg. Érdemes azonban emellett egy másik aspektust is figyelembe venni, amelyet Mark Prensky fogalmazott meg Digitális bennszülöttek, digitális bevándorlók című munkájában [25]. A szerző az amerikai oktatási rendszer minőségének romlásával kapcsolatban megfogalmazott kritikákból indul ki tanulmányában, de következtetései egyéb területek vonatkozásában is helytállóak. Prenksy úgy gondolja, a minőségromlás kiváltója a fiatalok radikális megváltozásában keresendő, ami a digitális technológiák elterjedéséből fakad. Az új generáció véleménye szerint nem fokozatosan alakult ki, nem csupán a nyelvük, öltözködésük, értékrendjük változott az előző generációkhoz mérten. Ez a fajta technológiai robbanás szerinte szingularitásként is értelmezhető.[4] A mai diákok[5] tekinthetőek ennek az első generációnak, akik beleszülettek az IKT elterjedésébe. Az őket körülvevő környezet, a vele való interakció alapjaiban változtatta meg a gondolkodásukat, az információ feldolgozását. Prensky hivatkozik Dr. Bruce D. Berryre, a Baylor College of Medicine professzorára, akinek

[4] A technológiai szingularitás a sci-fi irodalomban és a jövőkutatásban egy olyan lehetséges jövőbeli eseményt ír le, amelyben a technológiai fejlődés olyan mértékben felgyorsul, hogy az elszakad társadalmi változásoktól, és a szingularitás bekövetkezte előtt élők képtelenek értelmezni.

[5] A tanulmány 2001-ben jelent meg, így az állítást ekkorra kell értelmezni.

állítása szerint „*az eltérő tapasztalatok eltérő agyi felépítést eredményeznek*". Jelenleg is vitatják ezen állítást abban a tekintetben, hogy ez a változás valóban végbement-e fizikai valójában vagy csupán elméleti szinten, a gondolkodásban valósult meg.[6] Ettől eltekintve célszerű az IKT használata szempontjából megkülönböztetni a különböző generációkat. Prensky ezt a digitális bennszülöttek és digitális bevándorolók fogalmának megalkotásával teszi meg. A digitális bennszülöttek értelemszerűen az új generáció tagjai, akik „anyanyelvi szinten" beszélik az információs környezetet. Ezzel szemben a digitális bevándorlók nem születtek bele az IKT világába, csupán életük során valamikor elkezdték használni az új technológiákat. A digitális bevándorló bár folyamatosan tanulja, igyekszik elsajátítani a digitális nyelvet, azonban mindig megmarad az „akcentusa", ami az internet szerepének másodlagos értelmezéséből származik.[7] A digitális bennszülötteket újabban a C-generációként[8] nevesítik. A C-generáció, ellentétben az az "X", „Y" vagy "Z"[9] generációkkal nem születési év szerint alkot csoportot, hanem életmód alapján.

Ez a fajta eltérés azonban nem csupán az iskolákban van jelen, ugyanúgy létező probléma a családokban, a munkahelyeken. A C-generáció számára a közösségi média és okostelefon használat készségszinten történik, már-már a Maslow-féle szükséglet hierarchia legalsó szintjén, a fiziológiai szükségletek szintén jelentkezik. Jellemző rájuk továbbá, hogy napjaik nagy részét online töltik, a tartalomfogyasztást, a kapcsolattartást elsődlegesen ezeken az eszközökön végzik, illetve elvárják, hogy az élet minden területén érvényesüljenek a közösségi alapelvek, mint a transzparencia, hozzáférés, megoszthatóság, bevonás, kommentelhetőség. A különböző generációk különböző szintű adat- és információérzékenységgel rendelkeznek, de összességében elmondható, egyikük esetében sem túl magas.

A társadalom, és ez által a közösségi médiával való kapcsolata nem értelmezhető, ha nem a társadalmi alrendszerek szempontjából elemezzük. Talcott Parsons nyomán a társadalom alrendszereit a mintafenntartó kulturális rendszerre, a célelérési politikai rendszerre, az adaptív gazdasági rendszerre és integratív alrendszerét a szocietális közösségre bontjuk [26]. A rendszerek funkciók mentén határolódnak el egymástól, a határok azonban nem szilárdak, összemosódnak, interpenetrációs zónákat hozva létre. Napjainkban úgy vélem, nem kérdéses, hogy a kibertér befolyással bír a társadalmi folyamatokra, intézményekre, térszerkezetekre. A fizikai határok felszámolásával valós időben vehetünk részt akár más földrészek történéseiben, nem csak szemlélőként, de akár aktív szereplői is lehetünk az eseményeknek.[10] Az internet polgári életben megjelenésével sokan hangoztatták, hogy az egyének kibertérben való léte a társadalomi szerkezetek bomlásához, a földrajzi tér aprózódásához fog vezetni, amelynek a következménye egy fokozatosan antiszociálisabbá váló társadalom lesz. A közösségi média elterjedése azonban ezt cáfolni látszik. A közösségi média mozgósító ereje nem csupán a kibertérben, de a való életben is jelentősnek tekinthető, ahogy többek között a Stop Online Piracy Act[11] elleni fellépés vagy az arab-tavasz eseményei is alátámasztják. A

[6] Gondoljunk csak az emberi evolúcióra, amely nem kifejezetten évtizedek alatt következik be.
[7] Például kinyomtatja az e-maileket, vagy telefonon érdeklődik azok kézbesítéséről stb.
[8] Connect, create, contribute, communicate, content creating generation, vagyis kommunikáló, létrehozó, hozzájáruló, kommunikáló, tartalomgyártó generáció
[9] Az „X" generáció alatt 1965 és 1980 között, „Y" generáció alatt 1980 és 1995 között, „Z" generáció alatt pedig az 1996-tól születetteket értjük.
[10] Emlékezzünk a 2011-es egyiptomi vagy tunéziai forradalmakra, amikor az Anonymous hacktivista csoport alternatív kapcsolatokat hozott létre és tartott fenn, válaszul, amikor az országok kormánya lekapcsolta az internetet, ezzel is támogatva a tüntetőket-
[11] 2011-ben, az amerikai Törvényhozás elé benyújtott törvénytervezet, a Stop Online Piracy Act, amely az online kalózkodás ellen eddig nem látott szigorral és kiterjesztett jogkörrel lépett volna fel. A törvénytervezet

globalitás azonban kritikaként is megjelenik a közösségi médiával szemben, mondván, a globális kultúra ily mértékű térnyerése a hagyományos kulturális kapcsolatokat, helyi tradíciókat gyengíti, illetve az amerikai világrend terjesztését segíti.

Annak érdekében, hogy azonosítsam a közösségi média információs műveletekben való alkalmazási területeit, az AJP-3.10-ben meghatározott képességeket, eszközöket és eljárásokat, érdemes megítélésem szerint segítségül hívni. Az AJP-3.10 alapján az alábbi területeken alkalmazható információs műveletek végzésére a közösségi média:

- PSYOPS;
- PPP;
- OPSEC;
- INFOSEC;
- KLE;
- CNO;
- CIMIC;

A lélektani műveletek általánosságban olyan tevékenységet takarnak, amelynek során a szembenálló felek céljaik elérése érdekében tudatos lélektani ráhatással kívánja elérni [27]. Lélektani műveleteket már a hadviselés kezdetétől alkalmaztak. A PSYOPS célcsoportja nem csupán az ellenség lehet, ugyanúgy folyhat semleges, bizonytalan, el nem kötelezett célcsoportokkal szemben, ahogy irányulhat a szövetségesek, saját lakosság befolyásolására. A NATO lélektani műveli doktrínája [28] a célzott információközlést fogalmazza meg alapvető gyakorlatként. A célzott információközlés rendkívül széles skálán mozoghat. A fogalmat korábban propagandaként nevesítették, azonban a propaganda alapvetően ideológiai indíttatású volt. Eljárások tekintetében megkülönböztetünk fehér, azaz ismert, szürke, azaz ismeretlen, illetve fekete, azaz a valóságtól eltérő célzott információközlést. A technikai és technológiai innovációval párhuzamosan bővültek az információterjesztés médiumai. Napjainkban az egyik legjelentősebb csatorna az internet és azon belül a közösségi média. A különböző közösségi hálózatok, blogok, fórumok, de kép és videómegosztó oldalak mind lehetőséget biztosítanak propaganda-ellenpropaganda folytatására, amelyekre az egyes államok kiterjedt szervezeteket tartanak fenn.[12]

A megjelenés, viselkedés, arculat megfelelő tervezése nem csak egy adott szervezet számára tekinthető relevánsnak, ugyanolyan jelentőségű a szervezet által képviselt célok, feladatok végrehajtása szempontjából is. Nem véletlen tehát, hogy a NATO intenzív közösségi média jelenléttel kívánja erősíteni a nyitott diplomácia jegyében a Szövetség hidegháborútól eltérő barátságos, együttműködő szervezet képét [29], illetve a NATO műveletek (pl. az International Security Assistance Force) stratégiai kommunikációjában is komoly szerepet játszik [30]. E tekintetben a Magyar Honvédség is élenjáró, a közösségi

---

támogatói között volt maga Barack Obama elnök is, a Kongresszus sok tagjával egyetemben. Azonban az Anonymous hackerei, valamint az online közösségek nyomására, akik mögött ott sorakoztak a nagy amerikai tech cégek, mint a Google, Facebook, E-bay, Yahoo egyre többen hátráltak ki a tervezet mögül, ami Barack Obama támogatásának visszavonásával a SOPA bukását jelentette. Az eset legfontosabb tanulsága a nagy tech cégek a politikai döntéshozatal befolyásolásában betöltött szerepe. Egy, az amerikai Törvényhozás által elfogadott törvény az Amerikai Egyesült Államok polgáraira vonatkozó normatív szabályozás. A nemzetközi jog alapja a nemzetállamok szuverenitásán nyugszik. Az által, hogy egy törvénytervezetet az internetezők nyomására vontak vissza, amelyben nem csupán az amerikai internethasználók nyilvánítottak véleményt, hanem világszerte tömegek, jogi értelemben az amerikai szuverenitás csorbulását fedezhetjük fel. Mindez nagyon veszélyes precedens lehet a jövőre nézve.

[12] A témáról bővebben lásd: Bányász Péter: A közösségi média szerepe a lélektani műveletekben az elmúlt időszak válságainak tükrében, In. Szakmai Szemle, 2016/1.

média jelenléte professzionálisként értékelhető. A sikeres PPP tervezés a fentieken kívül segít a szervezet pozitív percepcionálásának megteremtésében, növelheti a lakosság körében való támogatottságát, illetve a toborzásban is szerepet játszhat.

A műveleti biztonság megteremtése elengedhetetlen az információs hadszíntéren. Az OPSEC alatt olyan folyamatok, tevékenységek és rendszabályok összességét értjük, amely aktív és passzív eszközök alkalmazásával megfelelő biztonságot nyújt az adott tevékenység számára azáltal, hogy megakadályozza az ellenséget, hogy hozzáférjen a számára releváns információkhoz [31]. A közösségi média a műveleti biztonságot közvetetten befolyásolja, ami a nem megfelelő adat- és információbiztonságból eredhet. Több esetben fordult elő, hogy műveleteket kellett elhalasztani, mert a katonák közösségi oldalon tárgyalták meg az adott művelet[13] vagy olyan információkat posztoltak, amelyekhez való hozzáféréssel támadást indítottak a katonák ellen.[14]

Az információbiztonság bár kapcsolódik a műveleti biztonsághoz, de sokkal szélesebb spektrumban értelmezendő. Az internet és közösségi média használat az információ- és adatérzékenység szempontjából számos kockázatot rejt. Ahogy a digitális bevándorlók és bennszülöttek esetében is említettem, az egyes generációk eltérő hangsúlyt fektetnek erre vonatkozóan, de egyikük esetében sem tekinthető kimagaslónak. A közösségi oldalakon rengeteg információ gyűjthető be a célpontokról, amit aztán támadásra használhatnak. A különböző hírszerző eljárásokat aktívan használják mind állami, mind civil szereplők.

Kulcsfontosságú vezetőkkel kapcsolatos tevékenység a közösségi média esetében elsősorban az általuk mindennap használt infokommunikációs eszközök védelméhez kapcsolódik. Ezen eszközök nem megfelelő használata, a vezetők alacsony információ- és adatérzékenysége megnyitja az utat a támadóknak, hogy az ezeken az eszközökön tárolt érzékeny információkhoz jussanak hozzá [34], így míg egyik oldalról a védelem kulcsfontosságú vezetők védelme jelentkezik feladatként, addig másik oldalról a szembenálló felek kulcsfontosságú vezetők által használt közösségi eszközök feltérképezése információszerzés reményében.

Számítógép-hálózati műveletek esetében a közösségi média támogató funkcióval bír. A CNO kettős célt szolgálnak, amely egyrészt a hálózatok felderítésében, adatokhoz történő hozzáférésben, másrészt az adatok, információk befolyásolásában, tönkretételében, a hálózatok működésének diszfunkcionális működésének elérésében realizálódnak. A közösségi média lehetőséget biztosít olyan rosszindulatú programok elterjesztésére, amely hozzáférést biztosítanak a támadóknak a megfertőzött eszközökhöz, amelyeket ezt követően a céljaiknak megfelelően felhasználhatnak.

A Civil- Katonai Együttműködés szempontjából kulcsfontosságú szerepet tölthet be a közösségi média, hiszen a nem háborús katonai feladatok ellátása esetében a civil környezet hatással van a katonai műveletek végzésére. A civil környezet nagyban megkönnyítheti vagy megnehezítheti a feladat végrehajtását. A civil környezet műveleti területenként eltérő lehet, de minden esetben magában foglalja a terület lakosságát, a kormányzati, nem kormányzati szereplőket. Annak érdekében, hogy a civil környezet megkönnyítse a katonai feladatok végzését, rendkívül fontos a támogatásuknak az elnyerése, amelynek egyik eszközéül a CIMIC csoportok szolgálnak. A közösségi média megfelelő használata segíthet növelni az együttműködést a civil környezet és a katonai erők között, ezáltal nagyobb mozgásteret

[13] Pl. egy izraeli katona egy ciszjordániai tervezett akció helyét és idejét osztotta meg [32].

[14] Pl. egy iraki bázisra új helikopterek érkeztek egy repülőegység számára, és az ott szolgálatot teljesítő katonák a róluk készült képeket feltöltött közösségi oldalakra. A képek azonban a geolokációs adatokat is tartalmazták, amelyet visszafejtettek az iraki ellenállók és sikeresen lokalizálták a helikopterek elhelyezkedését, amelynek következtében négy AH-64-es Apache helikoptert semmisítettek meg aknavetős támadással [33].

biztosíthat a parancsnoknak morális, materiális, környezeti, stratégiai, hadműveleti, harcászati előnyök kihasználása érdekében, illetve hosszútávon segíthet kialakítani egy olyan civil környezetet, amely növeli a konfliktus békés lezárását, a nemzetközi erők kivonása után a béke fenntartását. Értelemszerűen a közösségi média alkalmazási területe ez esetben a civil környezet támogatásának megnyerése, a beavatkozó nemzetközi erők részvételének legitimizálása.

KÖVETKEZTETÉSEK

Tanulmányomban a közösségi média egy új típusú értelmezésére törekedtem. Reményeim szerint igazoltam, hogy a közösségi média az elterjedtsége okán megkerülhetetlen tényezővé teszi a politikai döntéshozók, a katonai, rendvédelmi és nemzetbiztonsági szervezetek számára. Bemutattam a kibertérnek, mint hadszíntérnek a kialakulását, aminek nyomán meghatároztam a közösségi média e speciális tartományát. A tanulmány terjedelmi korlátai nem teszik lehetővé, hogy az egyes eljárásokat, eszközöket bővebben vizsgáljam, ugyanis mindegyike egy külön-külön kutatás részét képezhetik, ezen írás keretei között csupán egy általános ismertetésre vállalkoztam.

FELHASZNÁLT IRODALOM

[1] GRASSEGGER, H. – KROGERUS, M.: *The Data That Turned the World Upside Down*, In. Motherboard, 2017. január 28., https://motherboard.vice.com/en_us/article/how-our-likes-helped-trump-win (letöltve: 2017.06.19.)

[2] SUBRAMANIAN, S.: *Inside The Macedonian Fake-News Complex*, In. Wired, 2017. február 15., https://www.wired.com/2017/02/veles-macedonia-fake-news/ (letöltve 2017.06.19.)

[3] OFFICE of the DIRECTOR of NATIONAL INTELLIGENCE: *Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution*, In. DNI, 2017. január 6., https://www.dni.gov/files/documents/ICA_2017_01.pdf (letöltve: 2017.06.19.)

[4] *Definition of social media in English,* In. Oxford Dictionaries, http://www.oxforddictionaries.com/definition/english/social-media

[5] KAPLAN, A.- HAENLEIN, M.: *Users of the world, unite! The challenges and opportunities of Social Media*, Business Horizons, 2010.

[6] DAS, S.- KRAMER, A.: Self-censorship on Facebook, In. Facebook Research, https://research.fb.com/wp-content/uploads/2016/11/self-censorship-on-facebook.pdf (letöltve 2017.06.19.)

[7] *Most famous social network sites worldwide as of April 2017, ranked by number of active users (in millions),* In. Statista.com, https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/ (letöltve 2017.06.19.)

[8] *Facebook Reports First Quarter 2017 Results*, In. Facebook Investor Relations, 2017. május 3., https://investor.fb.com/investor-news/press-release-details/2017/Facebook-Reports-First-Quarter-2017-Results/default.aspx (letöltve 2017.06.20.)

[9] *Top Website Ranking*, In. Similar Web, https://www.similarweb.com/top-websites (letöltve 2017.06.20.)

[10] ROYAL SOCIETY FOR PUBLIC HEALTH: *#StatusOfMind- Social Media and young peolple's menthal health and wellbeing*, In. RSPH, https://www.rsph.org.uk/our-work/policy/social-media-and-young-people-s-mental-health-and-wellbeing.html (letöltve 2017.06.20.)

[11] GREENWALD, G.: *A Snowden-ügy*, HVG Kiadó, 2014.

[12] MÉSZÁROS R.: *A kibertér társadalomföldrajzi megközelítése*, In. Magyar Tudomány, 2001/7., 769-779. o.

[13] JAKOBI Á.: *A virtuális világ terei- Reflexiók Mészáros Rezső „A kibertér társadalomföldrajzi megközelítése" című tanulmányához*, In. Magyar Tudomány, 2002/11., 1482-1491. o.

[14] 1139/2013, (III. 21.) Korm. határozat *Magyarország Nemzet Kiberbiztonsági stratégiájáról*, In. Magyar Közlöny, 2013/47.

[15] 60/2013. (IX. 30.) HM *utasítás a Magyar Honvédség Kibervédelmi Szakmai Koncepciójának kiadásáról*, In. Honvédelmi Közlöny, CXL évfolyam 10. szám, 2013.

[16] HAIG Zs.: *Információ- Társadalom- Biztonság*, NKE Szolgáltató Kft., Budapest, 2015.

[17] VARGA G.: *A NATO új, lisszaboni stratégiai koncepciója*, In. Nemzet és Biztonság, 2010/10, 79-86. o.

[18] BABOS T.: *„Globális közös terek" a NATO-ban*, In. Nemzet és Biztonság, 2011/3., 34-46. o.

[19] BARETT et. al.: *Assured Access to the Global Commons*, Supreme Allied Command Transformation, North Atlantic Treaty Organization, Norfolk, Virgina USA, April 2011.

[20] *Warsaw Summit Communiqué*, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016 [online], 2016. július 9., https://ccdcoe.org/sites/default/files/documents/NATO-160709-WarsawSummitCommunique.pdf

[21] Joint Publication 3-13, Information Operations, 27 November 2012 by United States Government US Army, p. I-1.m

[22] HAIG et. al.: *Elektronikai hadviselés* (szerk. Németh András), Nemzeti Közszolgálati Egyetem, Budapest, 2014.

[23] HAIG Zs.- VÁRHEGYI I.: *Hadviselés az információs hadszíntéren*, Zrínyi Kiadó, Budapest, 2005.

[24] AJP-3.10 *Allied Joint Doctrine for Information Operation*, 2009., https://info.publicintelligence.net/NATO-IO.pdf

[25] PRENSKY, M.: *Digital Natives, Digital Immigrants*, On the Horizon. MCB University Press, Vol. 9 Iss: 5, No. 5,2001. október, p. 1-6.

[26] PARSONS, T.: *Theoretical Orientations*, In. The system of modern societies, Englewood Cliffs, New Jersey, Prentice-Hall, 1971.

[27] PIX G.: *A lélektani műveletek jellemzőinek vizsgálata*, Doktori (PhD) értekezés, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2005.

[28] AJP-3.7. *NATO Military Policy on Psychological Operations*, 2003., https://info.publicintelligence.net/NATO-PSYOPS-Policy-2003.pdf

[29] SZIJJ D.: *Ne kényszerítsd, formáld át! - A nyilvános diplomácia és a közösségi média jelentősége mindennapjainkban és a NATO Public Diplomacy Division tevékenységében*, In. Biztonságpolitika.hu, 2011. december 15., http://old.biztonsagpolitika.hu/?id=16&aid=1217&title=ne-kenyszeritsd-formald-at-a-nyilvanos-diplomacia-es-a-kozossegi-media-jelentosege-mindennapjainkban-es-a-nato-public-diplomacy-division-tevekenysegeben (letöltve 2017.06.20.)

[30] NÉMETH J. L.: *A (stratégiai) kommunikáció és a háború kapcsolata napjainkban*, In. Hadtudomány, XXIII/1-2. szám, 2013., 129-139. o.

[31] MUHA et. al.: *Az informatikai biztonság kézikönyve* (szerk. Szenes Katalin), Verlag Dashöfer, Budapest, 2007.

[32] MTI: *Izrael lefújt egy katonai akciót a Facebook miatt*, In. Metropol, 2010. március 3., http://www.metropol.hu/cikk/535056 (letöltve 2017.06.20.)

[33] RODEWIG, C.: *Geotagging poses security risks*, In. Army.mil, 2012. március 7., http://www.army.mil/article/75165/Geotagging_poses_security_risks/ (letöltve 2017.06.20.)

[34] KOVÁCS Z.: *Hordozható infokommunikációs eszközök használatához kapcsolódó biztonságtudatossági képzési tematika védett vezetők számára*, In. Hadmérnök, IX/3. szám, pp. 182-190., 2014.