Hadtudományi Szemle
15. évfolyam (2022) 2. szám 115–130. • DOI: 10.32563/hsz.2022.2.7

Haig Zsolt[1]

Kibertéri kognitív befolyásolás az információs műveletekben

Cyberspace Cognitive Influence in Information Operations

Absztrakt

Napjaink kibertéri műveletei rávilágítottak arra, hogy a kibertér értelmezése és struktúrája a korábbiakhoz képest tágabban értelmezhető. A kibertér fizikai és kognitív tartományában a klasszikus számítógép-hálózati támadásokon kívül további hatások is előidézhetők. Az információs műveletekben alkalmazott kognitív befolyásolási technikák a kibertérben a hálózatos technológia sajátosságait kihasználva nagyobb eredményességgel alkalmazhatók. A hatékonyság tovább növelhető, ha a kognitív képességeket egymással és más kibertéri technikai képességekkel összehangoltan alkalmazzák. A tanulmány ennek megfelelően az információs műveletekkel összefüggésben a kibertéri kognitív technikákat és azok egymással összehangolt alkalmazását, egymásra hatását mutatja be.

Kulcsszavak: *kibertér, kognitív befolyásolás, kibertéri műveletek, információs műveletek*

Abstract

Today's cyberspace operations have highlighted that the interpretation and structure of cyberspace is broader than before. In the physical and cognitive domains of cyberspace, additional effects can be created beyond the classical computer network attacks. Cognitive influence techniques used in information operations can be applied more effectively in cyberspace by exploiting the specific features of networked technology. Effectiveness can be further enhanced if cognitive capabilities are applied in coordination

[1] Egyetemi tanár, Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Elektronikai Hadviselés Tanszék, e-mail: haig.zsolt@uni-nke.hu

with each other and with other technical capabilities in cyberspace. Accordingly, this paper presents cyberspace cognitive techniques and their coordinated application and interaction in the context of information operations.

Keywords: *cyberspace, cognitive influence, cyberspace operations, information operations*

1. Bevezetés

Napjainkban a regionális feszültségek előfordulási gyakorisága növekszik. E konfliktusok műveleti környezete jelentősen különbözik a tradicionális állam-állam elleni fegyveres konfliktusoktól. Ezeknek az új típusú katonai műveleteknek a negyedik generációs hadviselési modellen belül számos elnevezése van, mint például aszimmetrikus, irreguláris, felkelés elleni vagy hibrid hadviselés, de a kibertéri műveletek is ide tartoznak. A negyedik generációs hadviselésnek egyik fő jellemzője, hogy a katonák mellett civilek is megtalálhatók a műveleti területen, és szemben álló félként pedig nem állami szereplők is megjelennek. A műveleti területen tehát a lakosság és a semleges érintettek is a katonai műveletek részesévé válnak.[2] Ennélfogva pedig a konfliktus a társadalom egészét érinti. Ezért e műveletekben a szemben álló fél mellett a nem állami szereplők és a lakosság befolyásolása kiemelt szerepet kap.

Egy korábbi tanulmány[3] szerint a negyedik generációs katonai műveletekben az információs műveletek során a kognitív befolyásoláson alapuló úgynevezett adaptív információs fölény kialakítására törekszenek. Ez esetben ugyanis nem a saját erők előnyösebb információkezelési és döntési képességén van a hangsúly, hanem a célközönség gondolatainak, véleményének átalakításán, valamint meggyőzésén, esetleg manipulálásán.

A korszerű hálózatos infokommunikációs technológia napjainkban jelentősen növeli a kognitív befolyásolás lehetőségeit. Megfelelően kiépített infokommunikációs infrastruktúra megléte esetén a kibertérben a különféle befolyásoló és manipulációs tevékenységek nagyobb hatékonysággal alkalmazhatók, mint a hagyományos technikák. A kiberteret felhasználva ugyanis a befolyásoló vagy megtévesztő információkat rövid idő alatt nagy tömegekhez lehet eljuttatni. A hatásokat pedig tovább fokozzák az internetes hírportálokon, illetve a közösségi médiában egyre terjedő álhírek, amelyek jelentősen átformálhatják az egyének véleményét. Az álhírek alkalmazása társadalmi, politikai, katonai és marketingszempontból is igen kifizetődő a terjesztőjének, hatékonyságához pedig manapság nemigen fér kétség. Ebből fakadóan az álhírek terjedése a világhálón és benne a közösségi médiában egyelőre megállíthatatlan.[4]

[2] Rózsa Tibor: *Az információs műveletek vizsgálata, különös tekintettel a befolyásolási képességek alkalmazásának lehetőségeire a Magyar Honvédség feladatrendszerében*. Doktori (PhD-) értekezés. Budapest, Nemzeti Közszolgálati Egyetem, 2016.

[3] Zsolt Haig: Novel Interpretation of Information Operations in Today's Changed Operational Environment. *Scientific Bulletin,* 25. (2020), 2. 93–102.

[4] Haig (2020): i. m. 99.

Mindezek alapján a tanulmány célja, hogy a befolyásolás elméletére alapozva kiemelje a kibertéri kognitív tevékenységek fontosságát, ismertesse a befolyásolás és manipuláció kibertéri technikáit, és bemutassa azok információs műveleteken belüli egymásra hatását.

2. A befolyásolás szociálpszichológiai háttere

A társadalmi befolyásolás a szociálpszichológiához kapcsolódó tevékenység, amely a célközönség gondolkodására, viselkedésére, vélekedésére és érzelmeire hat annak érdekében, hogy azok a befolyásoló érdekeinek megfelelően alakuljanak. E tudomány egyik jeles alakja volt Herbert Kelman, aki szerint a társadalmi befolyásolásnak az alábbi formái léteznek:

- megfelelés;
- azonosulás és
- internalizáció.[5]

A *megfelelés* azt jelenti, hogy a befolyásolt célközönség a saját véleményét megtartva fogadja el a befolyásoló érveit, és a célcsoport az addig megszokott viselkedés és attitűd helyett az elvárt hozzáállást és gondolkodást mutatja. A megfelelés a befolyásolás legalsó szintje, így ha a befolyásoló információk és üzenetek megszűnnek, akkor a célközönség a saját korábbi véleményéhez tér vissza. Ennek következtében tartós hatás nem, csak rövid távú viselkedési megfelelés érhető el, ami azt is jelenti, hogy az információs műveletekben alkalmazott kognitív befolyásolás során ezen állapot elérése a legkevésbé kívánatos.

Az *azonosulás* során a célközönség azért azonosul a befolyásoló véleményével, mert olyan szeretne lenni, mint ő. Az azonosuló befolyásolás függ a célcsoport befogadó képességétől, valamint a közte és a befolyásolást végző közötti kapcsolat formájától és minőségétől. Optimális esetben az azonosulással elért gondolkodás- és viselkedésváltozás hosszabb ideig is fennmaradhat, így negatív hatásokkal kevésbé kell számolni. Emiatt az információs műveletek keretében végzett kognitív befolyásolással elért ilyen állapot segítheti a befolyásolási célok teljesítését.

Az *internalizáció* esetében a befolyásolt célközönség teljes mértékben elfogadja a befolyásoló nézeteit, és magára nézve fenntarás nélkül érvényesíti azokat. Az információs műveleti kognitív befolyásolás esetén ez tartós tudati és viselkedésbéli változást eredményez, ugyanakkor ennek az állapotnak az elérése is a legnehezebb.

[5] Herbert C. Kelman: Compliance, Identification, and Internalization: Three Processes of Attitude Change. *Journal of Conflict Resolution,* 2. (1958), 1. 51–60.

3. Az információs műveletek és a kibertéri műveletek értelmezése

Az információs műveletek újszerű értelmezését egy korábbi tanulmányban már elemztük.[6] Ennek lényege, hogy az információs műveletek az információs környezet fizikai, információs és kognitív dimenziójában érvényesülő, integrált, egymással összehangolt és koordinált információs tevékenységek összessége, ami a műveletek célkitűzéseinek elérése érdekében közvetlenül kognitív befolyásolással, illetve közvetetten technikai ellentevékenységgel és védelmi tevékenységekkel hatásokat gyakorol a műveletekben érintett célközönség szándékára, helyzetértelmezésére és képességeire.

Általános megközelítésben az információs műveletek technikai és kognitív képességei közé az alábbiakat sorolhatjuk:

- technikai képességek:
  - elektronikai hadviselés;
  - számítógép-hálózati műveletek;
  - információs célpontok fizikai megsemmisítése;
  - műveleti biztonság technikai képességei;
  - megtévesztés technikai képességei;
- kognitív képességek:
  - pszichológiai műveletek (*psychological operations,* PSYOPS);
  - közügyek és tömegtájékoztatás;
  - civil-katonai együttműködés (*civil-military cooperation,* CIMIC);
  - műveleti biztonság kognitív képességei;
  - megtévesztés kognitív képességei.[7]

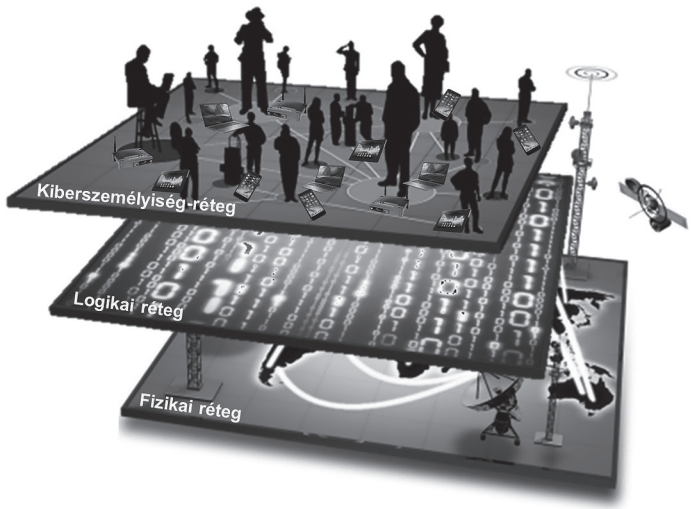
Napjainkra az információs műveletekben a technikai információs képességek mellett a kognitív térben a célközönséggel szembeni közvetlen információs hatások jelentősége felértékelődött. Az információs műveletek kognitív képességei az információ tartalmára fókuszálnak, és pozitív, negatív vagy semleges befolyásolási technikákat, tájékoztatási eszközöket és módszereket alkalmazva közvetlenül érik el a célközönséget. E képességek alkalmazása során különféle eszközöket és módszereket használnak, és jól megszerkesztett üzenetekkel, közvetlenül az emberek tudati tevékenységére hatnak. Az információs műveletek kognitív képességeinek célja minden esetben a humánum befolyásolása, manipulálása, a hatásuk tehát az információs környezet kognitív dimenziójában jelentkezik. Emellett a hálózatos technológia rohamos terjedése következtében a kibertér az információs környezet fontos tartományának tekinthető, így az e tartományban zajló kibertéri műveletek egyre jelentősebbé válnak.

A NATO kibertéri műveletek doktrínája általánosságban adja meg a kibertér definícióját, amely szerint az egy „globális tartomány, amely magában foglal minden egymással összekapcsolt kommunikációs, információtechnológiai és egyéb elektronikus

[6] Haig (2020): i. m. 97–99.
[7] Haig Zsolt: *Információs műveletek a kibertérben*. Budapest, Dialóg Campus, 2018. 215.

rendszert, hálózatot és azok adatait, beleértve az elkülönült vagy független rendszereket is, amelyek adatokat dolgoznak fel, tárolnak vagy továbbítanak".[8]

A kibertér az információs környezet része, így annak mindhárom dimenziójában, vagyis a fizikai, az információs és a kognitív tartományban egyaránt megjelenik. Az előzőkben hivatkozott doktrína és más irodalmak is a kibertér három rétegét értelmezik, úgymint: fizikai réteg, logikai réteg és kiberszemélyiség-réteg (1. ábra).[9]



1. ábra: A kibertér struktúrája
Forrás: a szerző szerkesztése NATO (2020. január): i. m. 3.; C. Inglis: Cyberspace – Making Some Sense of It All. Journal of Information Warfare, 15. (2016), 2. 21. alapján

A fizikai réteg hardverekből, infrastruktúrákból és kapcsolódó eszközökből áll, amelyek a kibertérben az információ tárolását, szállítását és feldolgozását végzik. Ide tartoznak a hálózati infrastruktúrák, számítógépek, szerverek, routerek, vezetékes és vezeték nélküli kapcsolatok stb. A hálózatos vezeték nélküli kapcsolatok növekedése miatt a fizikailag definiálható elektromágneses spektrum, azon belül is különösen a rádiófrekvenciás tartomány is a fizikai réteghez sorolandó.

A logikai réteg a digitális információs és parancsréteg, amely adatokból és kódokból áll, mint például *firmware*-ek, operációs rendszerek, átviteli és címzési protokollok, szoftveralkalmazások, valamint adatkomponensek, adatbázisok.

A kiberszemélyiség-réteg a szervezetek és egyének virtuális reprezentációiból áll. Ezek közé tartoznak az e-mail-címek, felhasználói azonosítók, közösségimédia-fiókok, IP- és MAC-címek stb. A fentieken kívül e réteg teszi lehetővé a személyek kapcsolati hálóinak kialakítását, valamint a közösségi háló tagjainak interakcióit.

A kibertérben az egymással szemben álló felek különféle műveleteket folytatnak, amelyek érintik a kibertér mindhárom rétegét. A kibertéri műveleteknek ma

[8] NATO: *AJP-3.20 Allied Joint Doctrine for Cyberspace Operations.* Edition A Version 1, NATO Standardization Office, (2020. január). 4.
[9] NATO (2020. január): i. m. 3.; Joint Chiefs of Staff: *JP 3-12 Cyberspace Operations* (2018. június 8.). I-2–I-4.

már számos értelmezése ismert. A NATO szakterületi doktrínája megadja a kibertéri műveletek általános definícióját, miszerint „a kibertérben vagy azon keresztül végzett tevékenységek, amelyeknek célja a saját erők cselekvési szabadságának megőrzése a kibertérben és/vagy a parancsnokok céljainak elérését szolgáló hatások előidézése".[10]

A kibertéri műveletek szoros összefüggést mutatnak az információs műveletekkel. A célok és az alkalmazható eszközök és módszerek sok esetben ugyanazok, illetve át is fedhetik egymást. A különbség abban áll, hogy míg az információs műveletek a teljes információs környezetben zajlanak, addig a kibertéri műveletek az információs környezet egy speciális színterén, a hálózatos infokommunikációs technológia által kreált kibertérben folynak. Az információs környezet és a kibertér szoros összefüggése lehetővé teszi, hogy az információs műveletek definíciójának analógiája mentén a NATO meghatározásánál konkrétabban definiáljuk és értelmezzük a kibertéri műveleteket. Ez alapján a kibertéri műveletek a kibertérben alkalmazott információs tevékenységek koordinált alkalmazásának összessége, amelyek, az infokommunikációs hálózatokat felhasználva, a közvetlen kognitív, illetve közvetett technikai eszközökkel és módszerekkel hatásokat gyakorolnak a műveletekben részt vevő célközönség szándékára, helyzetértelmezésére és képességeire.

Általánosan bevett gyakorlat szerint a kibertéri műveletek értelmezésekor általában klasszikus számítógép-hálózati támadás és védelem technikai módszerek alkalmazását hangsúlyozzák, mint például a hálózathoz, adatokhoz, adatbázisokhoz való hozzáférés; kártékony programokkal adatbázisok módosítása, törlése; túlterheléses támadások stb., illetve az ezek elleni védekezés lehetőségei.

Ugyanakkor a kibertér háromrétegű értelmezése és az azokban megvalósuló kibertéri műveletek kapcsán a kognitív képességek egyre fontosabbakká válnak. Ezek a képességek a kibertérben való befolyásolásra és manipulálásra fókuszálnak. A tanulmány témája szempontjából a kognitív befolyásolás és manipuláció a kibertér mindhárom rétegében megvalósulhat a hálózatos infokommunikációs rendszereken keresztül továbbított valós vagy hamis információkkal, hatásuk azonban minden esetben a kiberszemélyiség-rétegen keresztül a felhasználókban közvetlenül jelentkezik.

4. Kognitív információs műveletek a kibertérben

A hálózatos infokommunikációs technológia igen jó lehetőségeket teremt a kognitív hatásokat előidéző különféle eszközök és módszerek alkalmazására. Az internet és benne a közösségi média pedig jelentősen kiszélesítik a kognitív befolyásolás és manipuláció lehetőségeit. Ezeknek az új kibertéri technológiáknak számos olyan tulajdonsága van, amelyek meghatározzák a különféle kognitív információs tevékenységek alkalmazásának hatékonyságát.

[10] NATO (2020. január): i. m. 4.

4.1. Kibertéri kognitív információs tevékenységek jellemzői

Svetoka elemzése rámutat, hogy a kibertéri technológiák a hagyományos befolyásolási módszerekhez képest az alábbi hatékonyságnövelő tulajdonságokkal rendelkeznek:

- *hozzáférhetőség:* a vezeték nélküli mobil technológiáknak, okostelefonoknak köszönhetően az információkhoz való hozzáférés és azok megosztása jelentősen leegyszerűsödik bárki számára;
- *sebesség:* a röplapokhoz, újságokhoz és más hagyományos információterjesztő formákhoz képest a közösségi médiában a befolyásoló vagy manipulációs célú üzenetek igen gyorsan terjeszthetők, ami lehetővé teszi, hogy azok hatása is sokkal gyorsabban jelentkezzen;
- *anonimitás*: a névtelenség és gyakran a beazonosíthatatlanság nagyobb szabadságot ad a vélemények kifejtésének;
- *információdömping*: a közösségi médiában rendkívül sok a lényegtelen, nem releváns, esetleg hamis információ, amelyeket igen nehéz beazonosítani és elkülöníteni a valós tényeket tartalmazó információktól;
- *földrajzi és információtartalmi határok nélküliség:* az előző sajátosságokból adódóan is a hagyományos médiához képest sokszor tartalmi megkötések és földrajzi határok nélkül lehet információt megosztani és terjeszteni.[11]

E sajátosságok alapján a kibertér befolyásolási célból való felhasználásának egyik legnagyobb előnye, hogy a célok elérése érdekében gondosan megválogatott információk rövid idő alatt széles tömegeket érhetnek el, és a megcélzott közönség is megsokszorozódhat. Emellett a vezetők vagy véleményvezérek közösségi oldalakon való célzott befolyásolásával az irányításuk alatt álló csoport tagjainak véleménye, gondolkodása is könnyebben alakítható, esetleg manipulálható.

A felsorolt hatékonyságnövelő tulajdonságokra alapozva a befolyásolás mindhárom formája, vagyis a megfelelés, az azonosulás és az internalizáció is hatékonyabban elérhető a kibertérben. A leginkább kívánatos internalizáció kialakítása a kibertéri technológia felhasználásával jóval eredményesebben valósítható meg. A kibertéri kognitív módszerekkel nagyobb hatékonysággal lehet elérni, hogy a befolyásolt célközönség teljes mértékben elfogadja a befolyásoló nézeteit, és magára nézve fenntartás nélkül érvényesítse azokat. E módszer további nagy előnye, hogy az anonimitást kihasználva a kibertérben a befolyásoló könnyebben rejtve maradhat, így a célközönség csak az információ tartalmára fókuszálhat, és azt nem tudja összekapcsolni a befolyásoló személyével. Ez pedig jó lehetőségeket kínál a befolyásoló számára akár szélsőséges narratívák, álhírek vagy manipuláló információk terjesztésére is.

[11] Sanda Svetoka: *Social Media as a Tool of Hybrid Warfare*. Riga, NATO Strategic Communications Centre of Excellence, 2016. 5–6.

4.2. Kibertéri kognitív információs tevékenységek

Az előzőkben bemutatott információs műveletek képességei és a kibertéri műveletek jellege alapján a kibertérben is alkalmazható és különféle kognitív hatásokat előidéző információs képességek közé sorolhatjuk:

- a pszichológiai műveleteket (PSYOPS);
- a kognitív megtévesztést;
- a civil-katonai együttműködést (CIMIC) és
- a kognitív műveleti biztonságot.

A PSYOPS-ot és a kognitív megtévesztést a befolyásolás, illetve a manipuláció kategóriájába sorolhatjuk, a CIMIC és a kognitív műveleti biztonság pedig alapvetően a tájékoztatás és kapcsolatépítés, valamint a biztonságtudatosság területéhez tartozik.

A *PSYOPS* a NATO meghatározása szerint a „jóváhagyott célközönség felé irányuló kommunikációs módszerek és egyéb eszközök felhasználásával tervezett tevékenységek, amelyek célja, hogy befolyásolják a politikai és katonai célok elérésére hatással lévő felfogást, attitűdöt és viselkedést".[12]

A célközönség helyes kiválasztása és meghatározása az egyik kritikus pontja a PSYOPS végrehajtásának, ugyanis az üzenetek tartalmának és a célba juttatás módszereinek alkalmazkodni kell a befolyásoltak etnikai, kulturális, vallási és egyéb értékeihez, valamint a célterületen lévő infrastrukturális lehetőségekhez. Mivel a NATO-doktrína szerint a PSYOPS valós és hiteles információkon alapul, az üzenetek tartalmának összeállításakor – a célközönség sebezhetőségének figyelembevételével – hitelt érdemlő, de befolyásoló hatású témákat kell kiválasztani.[13]

Kedvező infrastrukturális feltételek megléte esetén a PSYOPS-üzenetek célba juttatására a hagyományos módszerek mellett, mint például röplapok, szóbeli kommunikáció, nyomtatott sajtó stb. a legkorszerűbb hálózatos technológiák is felhasználhatók. Ennek megfelelően a kibertéri PSYOPS során a hálózatos rendszereket felhasználva, valós információkon alapuló üzeneteket közvetítenek a kiválasztott célközönség felé. Az internet, a közösségi média és a mobil kommunikáció széles lehetőségeket nyújtanak a hatékony PSYOPS megvalósításában, amelyet a befolyásolók egyre eredményesebben használnak ki. Emiatt a kibertéri PSYOPS-ot a fizikai és logikai rétegben alkalmazzák, hatása azonban minden esetben a kiberszemélyiség-rétegben, vagyis a felhasználók kognitív tudatában jelentkezik (lásd az 1. táblázatot).

A legismertebb kibertéri PSYOPS-műveletek közé sorolhatjuk többek között a 2016-os amerikai elnökválasztási kampány befolyásolását, amelyben többek között szerepet játszott a Cambridge Analytica és a Facebook felhasználói adatbotránya és a szentpétervári székhelyű Internetkutató Ügynökség *(Agentstvo Internet Issledovaniya)* nevű „trollgyár" is.[14] Az orosz–ukrán konfliktus 2022. február 24-ig terjedő szakaszában – a hibrid hadviselés elveinek megfelelően – a technikai

[12] Ministry of Defence: *AJP-3.10.1 Allied Joint Doctrine for Psychological Operations*. Edition B Version 1, NATO Standardization Office, 2014. Lex-8.

[13] Ministry of Defence (2014): i. m.

[14] Kovács László – Krasznay Csaba: Mert övék a hatalom: Az internet politikát (is) befolyásoló hatása a 2016-os amerikai elnökválasztás során. *Nemzet és Biztonság,* 10. (2017), 3. 14.

kiberképességek mellett a kognitív módszerek is jelentős szerepet kaptak az orosz érdekek érvényesítésében. A hagyományos média *(Sputnik, Russia Today)* mellett az online médiát és a közösségi hálót is nagy hatékonysággal használták a célzott üzenetek továbbítására.

A 2022. február 24-én kitört orosz–ukrán forró háborúban pedig azt láthatjuk, hogy a pszichológiai műveleteket mindkét fél egyaránt nagy intenzitással alkalmazza mind a saját lakosság meggyőzésére, támogatásának elnyerésére és fenntartására, mind pedig a nemzetközi közvélemény befolyásolására. Az ukrán elnök szinte naponta szólítja meg a nemzetközi közvéleményt, illetve az egyes országokat, hogy támogassák Ukrajnát a háborúban, és hozzanak még szigorúbb intézkedéseket Oroszországgal szemben. Az ukrán lélektani műveletek részét képezik és az Oroszország elleni fellépés fokozását célozzák azok az internetes portálokon és a közösségi médiában terjesztett képek, videók is, amelyek például a bucsai civilek megölését mutatják be, és amit Oroszország tagad és provokációnak tart. Az orosz vezetés pedig az információs kontrollt alkalmazza, amikor korlátozza a Facebook vagy a Twitter elérését az orosz lakosság számára, illetve a hírcsatornákon a „különleges katonai művelet" jogosságát hirdeti, amivel a lakosság és az egész társadalom támogatását akarja elérni.

2022. március 31-én egy közösségimédia-csúcstalálkozón[15] a szakértők megállapították, hogy Oroszország, aki eddig élen járt a kibertéri befolyásolásban, a háborúban hátrányos helyzetbe került Ukrajnával szemben e téren. Az ukrán tisztviselők és civilek aktívan használják a közösségi hálózatot a közvélemény megnyerésére és a támogatások megszerzésére. Volodimir Zelenszkij elnök pedig hatékonyan alkalmazza a hagyományos, a közösségi és a titkosított médiát egyaránt az információk terjesztésére. A Telegram erre különösen jó platform, amelyet az ukránok sikeresen használnak a tartalom terjesztésére és a hasonló gondolkodású közönséggel való kapcsolatteremtésre szerte a világon.

A videó különösen fontossá vált a háború eseményeinek bemutatásában. Szinte minden platformon elérhetővé váltak a videókkal támogatott közösségimédia-tartalmak, amelyeknek igen erős a befolyásoló hatásuk. Ukrajna például számos videót mutat be Zelenszkij elnökről, amint a lebombázott és feldúlt városokban tájékozódik, ezzel is hangsúlyozva vezetői képességét és hajlandóságát a harc folytatására. Ezzel szemben Oroszország például Vlagyimir Putyin elnök beszédeit sugározza, vagy olyan felvételeket mutat be, amelyeken Putyin az íróasztalánál ül. Ezek azonban ma már nem elég hatékonyak szemben a rövid idejű, gyorsan közzé tehető videótartalmakkal.[16]

Megjegyzendő ugyanakkor, hogy a kibertéri PSYOPS-célú kognitív befolyásolás igen gyakran nem a valós tényeken alapul, ezért e tevékenység átcsúszik a kognitív megtévesztés területére, így pedig a klasszikus NATO-értelmezés szerinti lélektani műveletek és a megtévesztés közötti határ egyre inkább elmosódik. A tapasztalatok azt mutatják, hogy a kibertéri PSYOPS gyakran nagyobb erőbefektetést igényel, azonban ugyanakkora vagy még nagyobb hatást hamis információk terjesztésével, álhírekkel is el lehet érni. Ez esetben az eredmény ugyanaz, csak a megvalósítás módja különbözik.

[15] Sara Brown: In Russia–Ukraine War, Social Media Stokes Ingenuity, Disinformation. *MIT Sloan,* 2022. április 6.
[16] Brown (2022): i. m.

A *kognitív megtévesztés* napjaink egyik gyakran alkalmazott kibertéri manipulációs technikája. A NATO értelmezésében a megtévesztés „olyan szándékos tevékenységeket jelent, amelyek a megcélzott döntéshozók félrevezetésére irányulnak annak érdekében, hogy azok a parancsnok céljai szempontjából előnyös módon cselekedjenek".[17]

A kibertérben a megtévesztés megvalósítható technikai módszerekkel (mint például a *spoofing* vagy közbeékelődéses támadás), illetve kognitív információs tevékenységekkel, és alkalmazható hálózatok támadására, védelmére vagy a felhasználók kognitív befolyásolására egyaránt.

A kibertérben folytatott kognitív megtévesztés egyik hatásos technikája a *social engineering,* amely az emberi hiszékenységet aknázza ki. A *social engineering* tulajdonképpen olyan lélektani manipuláció, amely az emberek bizalomra való hajlamát használja ki a számítógép-hálózatokba való bejutáshoz. E tevékenység keretében a felhasználóktól a hálózat gyenge pontjaira vonatkozó érzékeny adatokat, jelszavakat szereznek meg manipulációval, megtévesztéssel, esetleg zsarolás útján. Ezzel a módszerrel könnyedén megkerülhetők a különféle biztonsági megoldások, mint például tűzfalak vagy behatolásdetektáló rendszerek, így csak kisebb erőbefektetés szükséges a hálózat technikai jellegű támadásához.

A másik elterjedt kognitív befolyásolási technika az álhírek terjesztése. Az álhírek olyan szándékosan közzétett és valós hírként interpretált valótlan információk, amelyek célja, hogy félrevezessék a célközönséget. Létrehozásukat és terjesztésüket elsősorban gazdasági haszonszerzés és politikai befolyásolás generálja, de jelentős a katonai célokra való felhasználásuk is.

Az álhírek terjesztése nem új keletű, azonban az internet és a közösségi média különösen jó táptalajt biztosít a hamis információk nagy tömegekhez való gyors eljuttatásához. A kibertéri hálózatos technológiák e tekintetben kiemelten fontos szerepet játszanak, mivel azok sajátosságai jelentősen növelik az emberek félreinformálásának hatékonyságát. A szenzációhajhász, „nagy érdeklődést kiváltó" információk mielőbbi megosztásának lehetősége hozzájárul az álhírek rohamos terjedéséhez, aminek köszönhetően az emberek manipulációs lehetőségei mára új színteret kaptak.

A közösségi médiában megvalósított álhírterjesztéshez három fontos összetevő szükséges. Ezek az az alábbiak:

- az online eszközök, szolgáltatások és a humán erőforrás, akik, és amelyek lehetnek trollok, követők, lájkolók, automaták, esetleg álhírterjesztő *botnethálózatok*
- a közösségi hálózatok mint a terjesztés médiumai, valamint
- a motiváció, amely alapvetően gazdasági, politikai és katonai jellegű lehet.[18]

A legjelentősebb hatásokat a szakszerűen összeállított, nagy számban generált, és terjesztett politikai és katonai célú álhírek okozzák, amelyeket szervezetten, különféle csoportok vagy úgynevezett „álhírgyárak" hoznak létre. Oroszország számos alkalommal használt álhírgyárak által előállított és terjesztett hamis információkat. A legismertebb álhírgyár a korábban említett Internetkutató Ügynökség, amely fizetett

[17] NATO: *AJP-3.10.2 Allied Joint Doctrine for Operations Security and Deception.* Edition A Version 2, NATO Standardization Office, (2020. március). 4.

[18] Lion Gu – Vladimir Kropotov – Fyodor Yarochkin: *The Fake News Machine. How Propagandists Abuse the Internet and Manipulate the Public.* TrendLabs Research Paper, 2017. 6–8.

trollokat alkalmaz arra, hogy a közösségi médiában az orosz kormány számára kedvező álhírkampányt folytasson. Az ügynökség a 2016-os amerikai elnökválasztásba való beavatkozás mellett részt vett többek között a szíriai konfliktus során alkalmazott befolyásolási és manipulációs kampányban is.[19]

A kibertéri megtévesztés a 2014-óta tartó ukrajnai konfliktusban is jelentős szerepet játszik mindkét fél oldalán. Egy kutatás például igazolta, hogy 2014-től a Twitteren jelentősen megnőtt az Ukrajnával foglalkozó bejegyzések száma. Ezeket a befolyásoló, manipuláló üzeneteket és nagyon gyakran álhíreket döntően szintén a szentpétervári trollgyár állította elő. 2014. július 18-án, a malajziai repülőgép lezuhanásának napján például több mint 44 ezer, a következő napon pedig több mint 25 ezer üzenetet tettek közzé. Ezekben 297 fiók terjesztett olyan információkat, amelyek szerint Ukrajna volt a felelős a maláj gép lelövéséért.[20]

A 2022. február 24-e óta tartó orosz–ukrán háborúban a kibertéri megtévesztés mindkét fél részéről rendkívüli méreteket ölt. Mindezeket pedig kiegészítik a háborúban közvetlenül nem részt vevő, de valamelyik oldal felé elkötelezettek által kreált különféle álhírek, hamisított videók, amelyek a háborús felek és a semleges közvélemény megtévesztését célozzák. A közösségi médiában, internetes portálokon rendre nagy számban jelennek meg olyan hírek, információk, amelyek valódiságtartalma erősen megkérdőjelezhető. Az egyik ilyen, elsősorban videótartalmak közzétételére szolgáló platform a fiatalok körében rendkívül népszerű TikTok kínai videómegosztó közösségi hálózati szolgáltatás.

A Meta – a Facebook és az Instagram anyavállalatának – jelentése a közösségi média dezinformációinak megugrását jelezte, beleértve az Oroszország ukrajnai inváziójához kapcsolódó tartalmak növekedését is. A jelentés szerint a Kremlhez köthető csoportok dezinformációkat terjesztenek az ukrajnai invázióról, miközben odahaza felerősítik az oroszbarát összeesküvés-elméleteket. A Meta például több tucat ukrán parancsnok közösségimédia-fiókjának feltörését detektálta és akadályozta meg, amelyeken megpróbáltak videókat feltölteni legyőzött és magukat megadó ukrán katonákról. A támadást egy Ghostwriter néven ismert hackerszervezetre vezették vissza, amelyet korábban Oroszország szövetségesével, Fehéroroszországgal hoztak kapcsolatba.[21]

A videótartalmak mind ez idáig bizonyító erejűnek számítottak, azonban a *deepfake* megjelenésével már e felvételek sem mindig a valóságot mutatják, A *deepfake* egy mélytanuláson és hamisításon alapuló szintetikus médiatechnika, amely esetében egy képen vagy videón lévő személyt meggyőzően manipulálnak annak érdekében, hogy elhitessék, olyasmit csinál vagy mond, amit valójában nem tett vagy mondott. A deepfake-technikát mindkét fél alkalmazza. Putyinról például manipulált videót osztottak meg a Twitteren, amelyen az látszik, hogy arra buzdítja az orosz katonákat, hogy tegyék le a fegyvert, és térjenek haza. A Deutsche Welle oroszországi szolgáltatása

[19] Samuel Charap – Elina Treyger – Edward Geist: *Understanding Russia's Intervention in Syria.* Research Report. RAND Corporation, 2019.

[20] Oleksandr Nadelnyuk: How Russian "Troll factory" Tried to Effect on Ukraine's Agenda. Analysis of 755 000 Tweets. *VoxUkraine,* (é. n.).

[21] Kari Paul: Russian Disinformation Surged on Social Media After Invasion of Ukraine, Meta Reports. *The Guardian,* 2022. április 7.

azonban leleplezte a manipulációt. Egy Zelenszkijt ábrázoló manipulált videó pedig márciusban terjedt el a közösségi médiában, amelyen láthatóan az ukrán vezető azt mondja katonáinak, hogy tegyék le a fegyvert, és adják meg magukat Oroszországnak. Üzenetét a *Ukraine 24* műsorszolgáltató honlapján is közzétették, de a hírügynökség nem sokkal ezután közleményt tett közzé, miszerint az oldalt feltörték, a hamisított videót pedig eltávolították.[22]

A *civil-katonai együttműködés (CIMIC)* napjainkban a megváltozott műveleti környezetben kiemelt fontosságúvá vált, ugyanis a katonai feladatok végrehajtása gyakran a lakossággal és a közigazgatási szervekkel való együttműködésben valósul meg. A műveletekben részt vevő katonai erők és a civil szervek közti kapcsolatok kialakítása a CIMIC feladata, amely esetben a kibertér szintén jelentős hatékonyságnövelő színtér lehet. A NATO vonatkozó doktrína szerint a CIMIC „a NATO parancsnokok és a civil szereplők, köztük a nemzeti lakosság és a helyi hatóságok, valamint a nemzetközi, nemzeti és nem kormányzati szervezetek és ügynökségek közötti koordináció és együttműködés a műveletek támogatása érdekében".[23]

A CIMIC során a kapcsolatteremtés, -építés és együttműködés elsősorban a személyes kapcsolatok kialakításával valósulhat meg. Megfelelő hálózatos infrastruktúrával rendelkező műveleti területen azonban a kibertéri hálózatos technológiák, mint a mobil kommunikáció, az e-mail és az elektronikus online médiaszolgáltatások (weboldalak, közösségi média) jelentősen lerövidíthetik és hatékonyabbá tehetik a kapcsolat kialakítását. A kibertéri CIMIC során tehát a fizikai és a logikai rétegben alkalmazhatunk különféle eszközöket és módszereket, a hatásuk pedig a kiberszemélyiség-rétegben érvényesül (lásd 1. táblázat).

A *kognitív műveleti biztonság* szintén fontos szerepet játszik a kibertéri kognitív információs műveletekben. A NATO információs műveletek doktrína szerint: „A műveleti biztonság (OPSEC) egy folyamat, amely passzív vagy aktív eszközökkel és módszerekkel megfelelő szintű biztonságot nyújt a katonai művelet vagy gyakorlat számára azáltal, hogy megakadályozza, hogy az ellenség tudomást szerezzen a saját erők elhelyezkedéséről, képességeiről vagy szándékairól."[24]

Az információs műveleti képességek közül a műveleti biztonságnak a kibertérben – a megtévesztéshez hasonlóan – van technikai és kognitív értelmezése is. A műveleti biztonság technikai módszerei a fizikai és a logikai rétegben alkalmazott fizikai biztonság és elektronikus információbiztonság rendszabályaiban értelmezhetők. A kibertéri kognitív műveleti biztonság képességei elsősorban a felhasználók képzésére, felkészítésére és biztonságtudatosságának fejlesztésére fókuszálnak. A felhasználók biztonságtudatossági felkészítése elsősorban a hálózat különféle szolgáltatásaihoz való hozzáférési szabályok betartására, a jelszókezelésre, illetve az alapvető vírusvédelmi megoldásokra irányul. A kognitív műveleti biztonság alkalmazását és hatását tekintve is a kiberszemélyiség-rétegben jelenik meg (lásd 1. táblázat).

[22] Rachel Baig: Fact Check: The Deepfakes in the Disinformation War between Russia and Ukraine. *DW,* 2022. március 18.

[23] NATO: *AJP-3.10 Allied Joint Doctrine for Information Operations*. Edition A Version 1, NATO Standardization Office, (2015). LEX-3.

[24] NATO (2015): i. m. LEX-8.

Az 1. táblázat a kibertéri kognitív információs tevékenységeket foglalja össze a célközönség és a tevékenységek jellege, valamint a kibertér rétegei szerint.

1. táblázat: Kibertéri kognitív tevékenységek

Kibertéri kognitív tevékenység	Célközönség	Eszközök és módszerek	Kibertéri réteg	
			Tevékenység	Hatás
Pszichológiai műveletek	Emberek, közösségi csoportok	Befolyásolás internetes hírportálokon, közösségi médián, e-mailen keresztül, social engineering	Fizikai, logikai, kiberszemélyiség	Kiberszemélyiség
Kognitív megtévesztés	Emberek, közösségi csoportok	social engineering, álhírek stb.	Fizikai, logikai, kiberszemélyiség	Kiberszemélyiség
Kognitív műveleti biztonság	Emberek	Kiberbiztonsági képzések, biztonságtudatosság stb.	Kiberszemélyiség	Kiberszemélyiség
Civil-katonai együttműködés	Emberek, közösségi csoportok, kormányzatai és közigazgatási szervek	Befolyásolás, együttműködés, kapcsolatalakítás mobilkommunikáción, e-mailen, internetes hírportálokon, közösségi médián keresztül	Fizikai, logikai, kiberszemélyiség	Kiberszemélyiség

Forrás: a szerző szerkesztése Haig (2018): i. m. 240. alapján

A kibertéri műveletek lényege az információs műveletekhez hasonlóan a különböző információs tevékenységek összehangolásában és integrálásában rejlik. Ennek köszönhetően a kibertéri kognitív információs tevékenységek szoros kapcsolatban állnak egymással, gyakran pedig a határok is elmosódnak köztük, lásd a kibertéri kognitív megtévesztés és PSYOPS viszonyát. Ennek során mindegyik kognitív tevékenység a kiberteret, vagyis az internetet és benne a közösségi médiát használja fel. Az egyes tevékenységek egymástól elkülönülten értelmezhetők, és a végrehajtás során a kibertérnek akár mindhárom rétegét felhasználhatják. Ugyanakkor a hatások mindegyik esetben a kibertér kiberszemélyiség-rétegében érvényesülnek, és ezen keresztül a célközönség kognitív képességeit, tudatát, gondolkodását, viselkedését befolyásolják. Az információs műveletek analógiájának mentén tehát a kibertéri kognitív képességek egymással és a kibertéri technikai képességekkel való összehangolt tervezése és végrehajtása jelentősen növeli az egyes tevékenységek egymásra gyakorolt hatását és azok eredményességét.

5. Összegzés, következtetések

Napjainkra a hálózatos technológiáknak és a közösségi hálózatoknak köszönhetően a kibertér újszerű értelmezést nyert. E tér ma már nem csupán virtuális, logikai tartományként értelmezhető, hanem amellett a fizikai és a kognitív tartomány is fontos részét képezi. Ebben a tartományban az információs műveletekkel szoros kapcsolódást mutató, annak részét képező kibertéri műveletek zajlanak. Az információs műveletekkel analóg módon, a kibertéri műveletekben is az integrált, egymás hatásait kihasználó technikai és kognitív információs tevékenységeket alkalmazzuk, de nem a teljes információs környezetben, hanem annak csak a hálózatokkal jellemezhető tartományában, vagyis a kibertérben.

Az információs műveletekben kiemelt fontosságú a célközönség kognitív befolyásolása, a kibertéri műveletekben pedig ma ez a tevékenység szintén jelentősen felértékelődik. Ahol megvan az infrastrukturális feltétele, és a célközönség aktívan használja a hálózatos infokommunikációs technológiát, vagyis a kiberteret, ott a kibertéri kognitív befolyásolás és manipuláció jelentős erősokszorzó képességet jelenthet.

A kibertéri kognitív tevékenységek szorosan kötődnek az információs műveletek kognitív képességeihez, céljukat tekintve megegyeznek azokkal, ugyanakkor a hatások eléréséhez a kibertéri műveletekben az internetet és benne a közösségi médiát használják. Alapvető céljuk a befolyásolás és a manipuláció, amely megvalósulhat hiteles és valós információkkal, valamint manipulált üzenetekkel, álhírekkel. A kibertéri befolyásolásra ennek megfelelően elsősorban az információs műveletek kognitív tevékenységeit, vagyis a PSYOPS-ot és a kognitív megtévesztést használják, emellett pedig alkalmazható még a CIMIC és a kognitív műveleti biztonság is.

Az internet és a közösségi hálózat nagy előnye, hogy e médiumokat felhasználva sokkal eredményesebben lehet megvalósítani a kognitív befolyásolást és manipulációt. Minderre jó példa az álhírek terjedése, az elmúlt évek néhány nagy nyilvánosságot kapó eseményei, mint például az amerikai elnökválasztási kampányba való beavatkozás, valamint az ukrajnai háborúban mindkét fél részéről megfigyelhető kibertéri befolyásolás és manipuláció.

Összességében megállapíthatjuk, hogy a hálózatos technológiák evolúciójából, az információs műveletek fejlődéséből, illetve a kibertér és a kibertéri tevékenységek elemzéséből levonható következtetések, valamint az elmúlt évek megtörtént és a jelenleg is zajló háború kibertéri eseményei alapján igazolható, hogy:

- a kibertér meghatározása és struktúrája új értelmezést nyert, a virtuális logikai réteg mellett a fizikai és kiberszemélyiség-réteg is fontos tartományaiként jelennek meg;
- a kibertéri kognitív információs tevékenységek a kibertér mindhárom rétegében megvalósulhatnak, hatásaik azonban minden esetben a kiberszemélyiség-rétegben érvényesülnek;
- a kibertérben a megszokott technikai információs tevékenységek, mint például a számítógép-hálózatok támadása és védelme mellett a kognitív képességeknek is egyre növekvő jelentőségük van;
- a kibertéri kognitív tevékenységek egymással, illetve kibertéri technikai képességekkel való összehangolásának jelentős hatása van.

Mindez azt jelenti, hogy a NATO és a nemzeti haderő fejlesztése során előtérbe kerülő kibertéri képességek kialakításakor nemcsak a kiberelrettentés és a kibervédelem területe kell hogy fókuszba kerüljön, hanem törekedni kell a kognitív kiberképességek megteremtésére is. Ehhez pedig megfelelő szervezeti struktúrára és a társadalmi befolyásolásban jártas és a hálózatos infokommunikációs technológiát jól alkalmazó, képzett szakemberekre van szükség.

Felhasznált irodalom

Baig, Rachel: Fact Check: The Deepfakes in the Disinformation War between Russia and Ukraine. *DW,* 2022. március 18. Online: www.dw.com/en/fact-check-the-deepfakes-in-the-disinformation-war-between-russia-and-ukraine/a-61166433

Brown, Sara: In Russia–Ukraine War, Social Media Stokes Ingenuity, Disinformation. *MIT Sloan,* 2022. április 6. Online: https://mitsloan.mit.edu/ideas-made-to-matter/russia-ukraine-war-social-media-stokes-ingenuity-disinformation

Charap, Samuel – Elina Treyger – Edward Geist: *Understanding Russia's Intervention in Syria.* Research Report. RAND Corporation, 2019. Online: www.rand.org/content/dam/rand/pubs/research_reports/RR3100/RR3180/RAND_RR3180.pdf

Gu, Lion – Vladimir Kropotov – Fyodor Yarochkin: *The Fake News Machine. How Propagandists Abuse the Internet and Manipulate the Public.* A TrendLabs Research Paper, 2017. Online: https://documents.trendmicro.com/assets/white_papers/wp-fake-news-machine-how-propagandists-abuse-the-internet.pdf

Haig Zsolt: *Információs műveletek a kibertérben.* Budapest, Dialóg Campus, 2018.

Haig, Zsolt: Novel Interpretation of Information Operations in Today's Changed Operational Environment. *Scientific Bulletin,* 25. (2020), 2. 93–102. Online: https://doi.org/10.2478/bsaft-2020-0013

Inglis, C: Cyberspace – Making Some Sense of It All. *Journal of Information Warfare,* 15. (2016), 2. 17–26. Online: www.jstor.org/stable/26487528?seq=1

Joint Chiefs of Staff: *JP 3-12 Cyberspace Operations* (2018. június 8.). Online: www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf

Kelman, Herbert C.: Compliance, Identification, and Internalization: Three Processes of Attitude Change. *Journal of Conflict Resolution,* 2. (1958), 1. 51–60. Online: https://doi.org/10.1177/002200275800200106

Kovács László – Krasznay Csaba: Mert övék a hatalom: Az internet politikát (is) befolyásoló hatása a 2016-os amerikai elnökválasztás során. *Nemzet és Biztonság,* 10. (2017), 3. 3–15. Online: https://doi.org/10.32576/nb.2017.3.1

Ministry of Defence: *AJP-3.10.1 Allied Joint Doctrine for Psychological Operations.* Edition B Version 1, NATO Standardization Office, 2014. Online: https://bit.ly/3Bva39r

Nadelnyuk, Oleksandr: How Russian "Troll Factory" Tried to Effect on Ukraine's Agenda. Analysis of 755 000 Tweets. *VoxUkraine,* (é. n.). Online: https://voxukraine.org//longreads/twitter-database/index-en.html

NATO: *AJP-3.10 Allied Joint Doctrine for Information Operations.* Edition A Version 1, NATO Standardization Office, (2015).

NATO: *AJP-3.20 Allied Joint Doctrine for Cyberspace Operations.* Edition A Version 1, NATO Standardization Office, (2020. január). Online: https://bit.ly/3B5YCDu

NATO: *AJP-3.10.2 Allied Joint Doctrine for Operations Security and Deception.* Edition A Version 2, NATO Standardization Office, (2020. március). Online: https://bit.ly/3QEdVt6

Paul, Kari: Russian Disinformation Surged on Social Media After Invasion of Ukraine, Meta Reports. *The Guardian,* 2022. április 7. Online: www.theguardian.com/world/2022/apr/07/propaganda-social-media-surge-invasion-ukraine-meta-reports

Rózsa Tibor: *Az információs műveletek vizsgálata, különös tekintettel a befolyásolási képességek alkalmazásának lehetőségeire a Magyar Honvédség feladatrendszerében.* Doktori (PhD-) értekezés. Budapest, Nemzeti Közszolgálati Egyetem, 2016. Online: https://doi.org/10.17625/NKE.2017.04

Svetoka, Sanda: *Social Media as a Tool of Hybrid Warfare.* Riga, NATO Strategic Communications Centre of Excellence, 2016. Online: www.stratcomcoe.org/social-media-tool-hybrid-warfare