2. fejezet

A kibertéri műveletek fejlődése: a számítógép-hálózati műveletektől a kibertéri befolyásolásig

Haig Zsolt

A kibertéri technológiák fejlődése

Az elmúlt években az infokommunikációs technológiák rohamos fejlődése a korábbi számítógép-hálózati struktúrákon túlmutató, alapvető szemléletváltást idézett elő a hálózatok kialakításában, felépítésében, kapcsolati formáikban, valamint működési környezetük, azaz a kibertér értelmezésében. A paradigmaváltást a hagyományos számítógép-hálózatok mellett elsősorban a vezeték nélküli hálózati technológia egyre erősödő dominanciája jellemzi, ideértve például a vezeték nélküli szenzorhálózatok, az 5G mobilkommunikáció, a gép-gép (*machine to machine* – M2M) kommunikáció és a dolgok internete (*Internet of Things* – IoT) egyre szélesebb körű alkalmazását. Ezek mellett a mesterséges intelligencia, a virtuális/kiterjesztett valóság, a mélytanuló rendszerek, a gépi látás és más hasonló forradalmi technológiák is jelentősen átalakítják a kibertéri tevékenységek jellegét.

Az újfajta vezeték nélküli technológiáknak köszönhetően megfigyelhető, hogy az IoT terjedése következtében egyre több fizikai eszköz, hétköznapi használati tárgy is az internetre csatlakozik. Így az internetre kapcsolódó hálózatos eszközök száma folyamatosan növekszik, amelyek között a vezeték nélküli kommunikációt használók száma egyértelmű dominanciát mutat. A Statista felmérése és prognosztizációja szerint 2018 végén világszerte 22 milliárd IoT-eszköz volt használatban, ami 2025-re várhatóan 30,6 milliárdra, 2030-ra pedig 50 milliárdra nő.[1]

Zheng és Carter elemzése szerint az IoT terjedését alapvetően az olcsó, kis méretű, de nagy teljesítményű szenzorok és aktuátorok megjelenése; a vezeték

[1] Statista: *Number of Internet of Things (IoT) Connected Devices Worldwide in 2018, 2025 and 2030.* (2021. január).

https://doi.org/10.36250/01079_02

https://orcid.org/0000-0002-0326-9086

nélküli kommunikációs technológia bővülése; az adattárolási és feldolgozási kapacitás növekedése; valamint az újszerű szoftveralkalmazások, a jelfeldolgozás és a mesterséges intelligencián alapuló gépi tanulás fejlődése generálja.[2] Az IoT ma már megjelenik az emberek mindennapi életében, az okosotthonokban és az okosvárosokban, valamint a társadalmi működést biztosító infrastruktúrákban, mint például az egészségügy, az energiaellátás, az ipari vállalatok, a közlekedés, a közbiztonság és a honvédelem.

Az IoT-technológia egyik kritikus eleme az adatkommunikáció, különösen a vezeték nélküli megoldások. A szenzor/aktuátor oldalán alapvetően kis hatótávolságú és alacsony energiaigényű kommunikációt használnak, mint például ZigBee, WiFi, BLE *(Bluetooth low energy).* A felhőalapú adatfeldolgozás oldalán azonban többnyire nagyobb hatótávolságú kommunikációra van szükség, amelyet cellás mobilrendszerekkel vagy nagy hatótávolságú, de alacsony fogyasztású eszközökkel valósítanak meg, mint például a Lo-RaWan *(Long Range Radio Wide Area Network)* vagy az NB-IoT *(Narrow Band IoT).*

Az 5G megjelenése és elterjedése az IoT széles körű felhasználásnak egyik fő hajtóereje. Ez az új mobiltechnológia a korábbi rendszerekhez (3G, 4G) képest többek között nagyobb adatátviteli sebességet (elméleti csúcs: 20 Gbit/s; felhasználói: 100+ Mbit/s), rendkívül alacsony késleltetést (1 ms), valamint a 4G-nél nagyobb kapacitást és kapcsolatsűrűséget (10^6 eszköz/km^2) biztosít.[3] Ezek a minőségi jellemzők alapvető fontosságúak az IoT nagymértékű elterjedéséhez, különösen az önvezető járművek és az okosközlekedés számára. Az előrejelzések szerint 2024-re az 5G mobilelőfizetések száma világszerte mintegy 1,9 milliárdra növekedik.[4]

A vezeték nélküli hálózatos tendencia a katonai rendszerekben is megfigyelhető: a polgári technológiák fokozatos megjelenését tapasztalhatjuk a katonai hálózatokban is. A NATO például megkezdte az IoT katonai alkalmazhatóságának kutatását,[5] és az eredmények azt igazolják, hogy az IoT katonai célú felhasználásának, az IoMT *(Internet of Military Things)* vagy IoBT *(Internet*

[2] Denise E. Zheng – William A. Carter: *Leveraging the Internet of Things for a More Efficient and Effective Military.* Center for Strategic & International Studies. Rowman & Littlefield, 2015. szeptember 1–2.

[3] ITU RM 2083: *Recommendation ITU RM 2083-0 (09/2015) Framework and Overall Objectives of the Future Development of IMT for 2020 and Beyond.* 2015.

[4] Statista: *Forecast Number of Mobile 5G Subscriptions Worldwide by Region from 2019 to 2026* (2021. január).

[5] NATO STO: *Military Applications of Internet of Things.* 2016.

of Battlefield Things) -megoldásokon belül számos területe lehet, amelyek közé tartoznak például az automatizált felderítő és vezetési, irányítási rendszerek, a logisztika, a tűzvezetés, az egészségiállapot-monitorozás és egyéb alkalmazások.

A mai hálózatos technológiák és az internethez való hozzáférés egyik alapvető kérdése a mobilitás, ami miatt a hálózatok tipikus kommunikációs módszere egyre inkább az elektromágneses spektrumot használó vezeték nélküli kapcsolatokra helyeződik. E tartomány használata kibővíti a potenciális támadási lehetőségeket, például a rádiófelderítés és a rádiózavarás vagy a GPS-zavarás és a *spoofing* révén, ami még tovább növeli a hálózatba kapcsolt rendszerek sebezhetőségét.

A kibertéri hálózatos technológiákban a másik igen jelentős tendencia, hogy a közösségi média terjedésével intenzíven növekszik a kibertér kognitív információs és interakciós célú használata. Ma az emberek információs tevékenységeiket nagyrészt az interneten, különösen a közösségi médiában végzik. Ennek eredményeként mint felhasználók a kibertér szereplőjévé válnak, és ezen keresztül célzott információkkal minden eddiginél könnyebben elérhetők, ezáltal befolyásolhatók, vagy akár manipulálhatók. Mindez azt is jelenti, hogy a kibertér komplexitása miatt a fenyegetések is összetettebbekké, a támadási felületek pedig egyre változatosabbakká és kiterjedtebbekké válnak.

A kibertér értelmezése

A kibertéri műveletek és különösen az e műveletekben alkalmazható szerteágazó információs tevékenységek megértéséhez mindenekelőtt szükséges a kibertér értelmezése. Ahogy az első fejezetben is olvasható, a kibertérnek számos értelmezése lehetséges. Jelen fejezetben egy újabb, elsősorban katonai megközelítésű értelmezéssel gazdagítjuk a korábbi definíciókat. A *Tallinn Manual* meghatározása szerint a kibertér „a számítógépes hálózati adattárolásra, módosításra és cserére szolgáló, fizikai és nem fizikai összetevőkből kialakított környezet”.[6] A definíció fontos megállapítása, hogy a kibertér nemcsak virtuális, azaz nem fizikai összetevőkből, hanem fizikai komponensekből is áll.

[6] Michael N. Schmitt (szerk.): *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge, Cambridge University Press, 2017. 564.

Ugyanakkor az előzőekben bemutatott vezeték nélküli hálózatos technológiák radikális elterjedése a kibertér újszerű, kiterjesztett megközelítését eredményezte. Ez azt jelenti, hogy a kibertér értelmezésében a fizikailag és matematikailag is jól definiálható elektromágneses spektrum új elemként jelenik meg, amit számos meghatározás is alátámaszt. Egyik ezek közül Sanjeev Relia definíciója, amely szerint:

> „A kibertér az az ember alkotta digitális közeg, amelyet az elektromágneses spektrumban az elektronikai eszközök felhasználásával az emberek közötti adat- és információgyűjtésre, tárolásra és továbbításra használnak, és amely szervezeti, kulturális, nemzeti vagy politikai határok nélkül azonnali, határtalan, globális kapcsolatokat tesz lehetővé."[7]

Idesorolandó Daniel Kuehl meghatározása is, aki azt állítja, hogy

> „a kibertér az információs környezetben egy olyan globális tartomány, amelynek egyedi és megkülönböztető jellegzetessége, hogy az egymással összefüggő és hálózatba kapcsolt infokommunikációs rendszerekben az információ létrehozását, tárolását, módosítását, cseréjét és felhasználását végző elektronikai és elektromágneses spektrumot használó eszközök működnek".[8]

A hadtudomány az elsők között ismerte fel a kibertér átfogó és kibővített értelmezését, és azt a katonai műveleti környezet és az információs környezet egyik fontos területének tekinti. A nagyhatalmak és a NATO is nagy hangsúlyt fektet arra, hogy a kiberteret és az abban zajló műveleteket meghatározza. A NATO AJP-3.20 összhaderőnemi kibertéri műveleti doktrínája szerint a kibertér „minden olyan összekapcsolt kommunikációs, informatikai és egyéb elektronikai rendszerekből, hálózatokból és az azokban kezelt adatokból álló globális tartomány, beleértve az önálló vagy független rendszereket is, amelyek adatokat dolgoznak fel, tárolnak vagy továbbítanak".[9]

A hivatkozott kibertéri definíciókat elemezve az alábbi következtetéseket vonhatjuk le: a kibertér mesterségesen létrehozott tartomány, amely például a közösségi médiának köszönhetően újfajta személyközi kapcsolatokat,

[7] Sanjeev Relia: *Cyber Warfare: Its Implications on National Security.* New Delhi, Vij Books India Pvt Ltd., 2015. 22–23.

[8] Daniel Kuehl: From Cyberspace to Cyberpower: Defining the Problem. In Franklin D. Kramer – Stuart H. Starr – Larry K. Wentz (szerk.): *Cyberpower and National Security.* University of Nebraska Press, 2009. 27.

[9] AJP-3.20: *Allied Joint Doctrine For Cyberspace Operations. Edition A Version 1.* NATO Standardization Office, 2020. január 4.

kapcsolati hálókat biztosít az emberek számára. Ki kell azonban emelnünk azt a tényt, hogy a kibertér mint újfajta kapcsolati tér nem kizárólag az emberek számára áll rendelkezésre.

Ke Xu és szerzőtársai rávilágítanak a kibertér azon természetére, amelyet az emberek, a számítógépek és az intelligens eszközök összekapcsolódása jellemez. Ez az összekapcsolódás megfigyelhető az IoT-nak és a meglévő hálózati rendszereknek az integrációjában, beleértve az internetet, a felhőalapú számítástechnikát, a cellás mobilhálózatokat, valamint a közösségi és ipari hálózatokat. Rámutatnak, hogy a heterogén hálózatos technológiák integrációja a kibertéri hálózati innováció fő mozgatórugójává vált.[10]

A bemutatott definíciók elemzése és szintézise alapján megfogalmazható a kibertér újszerű, átfogó definíciója.

> „A kibertér egy az ember által mesterségesen létrehozott olyan dinamikusan változó tartomány, amelyben az információ gyűjtését, tárolását, feldolgozását, továbbítását és felhasználását végző, egymással hálózatba kapcsolt, és az elektromágneses spektrumot is felhasználó infokommunikációs eszközök és rendszerek működnek, lehetővé téve ezzel az emberek és a különféle eszközök közötti folyamatos és globális kapcsolatot."[11]

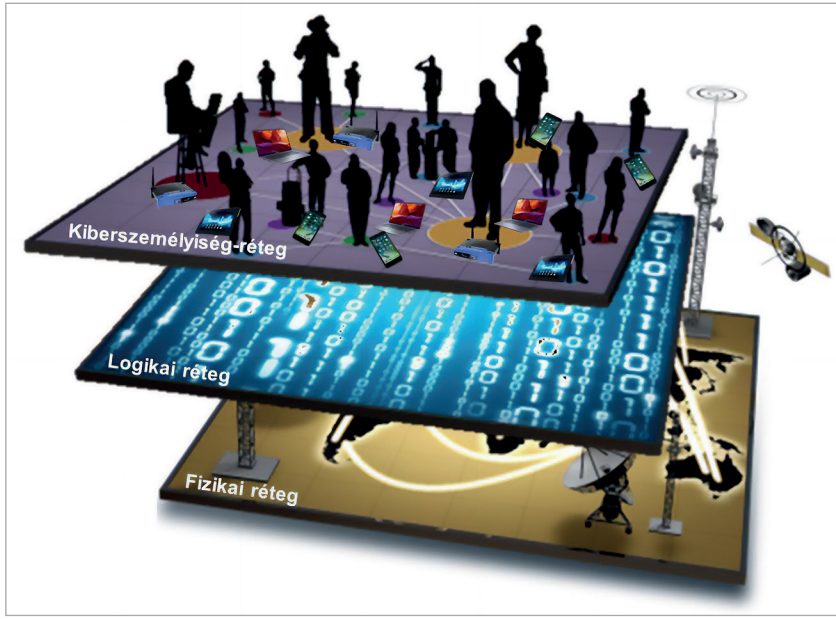
Ez a meghatározás rámutat, hogy a kibertér ma már nemcsak az interperszonális kapcsolatok, hanem az ember-gép és az M2M-kapcsolatok színterévé is vált. Ezenkívül lehetőséget ad a kibertéri műveleteknek az eddiginél szélesebb körű értelmezésére, amely a hálózatok és komponenseik elleni tipikus logikai szoftveres fenyegetéseken és védelmen túl az elektromágneses spektrumban és a kognitív térben alkalmazható technikákat és módszereket is magában foglalja (bővebben lásd később).

A fenti meghatározás alátámasztja a kibertér struktúrájának újszerű megközelítését is. A kibertérrel foglalkozó különféle szakirodalmi munkák és katonai doktrínák a kiberteret háromrétegű struktúrában ábrázolják, amely rétegek szorosan illeszkednek az információs környezet dimenzióihoz. E rétegek: a fizikai réteg, a logikai réteg és a kiberszemélyiség-réteg *(1. ábra)*.[12]

[10] Ke Xu – Yi Qu – Kun Yang: A Tutorial on Internet of Things: From a Heterogeneous Network Integration Perspective. *IEEE Network,* 30. (2016), 2. 102–108.

[11] Haig Zsolt: *Információs műveletek a kibertérben.* Budapest, Dialóg Campus, 2018. 226.

[12] AJP-3.20 (2020): i. m. 3; JP 3-12: *Cyberspace Operations.* 2018. június 8. I-3.



1. ábra: A kibertér struktúrája

Forrás: a szerző szerkesztése az AJP-3.20 (2020): i. m. 3. és a USNA: *Aspects and Pillars of Cyber Security* (é. n.) alapján

A fizikai réteg az adatok és információk kibertérbeni gyűjtését, tárolását, feldolgozását és továbbítását végző eszközökből áll. Idetartoznak a hálózati infrastruktúrák, számítógépek, szerverek, *routerek, hubok, switchek,* vezetékes és vezeték nélküli kommunikációs eszközök, valamint az adattároláshoz, az adatfeldolgozáshoz és az adatátvitelhez elengedhetetlen egyéb berendezések.[13] A fentieken kívül e rétegbe tartoznak a kiberfizikai eszközök, valamint a fizikailag definiálható elektromágneses spektrum is, azon belül is különösen a rádiófrekvenciás tartomány.

A logikai réteg a hálózatok virtuális tere, amely a kibertér fizikailag nem megfogható elemeit tartalmazza. E réteg adatokból és kódokból áll, mint például

[13] AJP-3.20 (2020): i. m. 3.

az operációs rendszerek, a protokollok, a szoftveralkalmazások, a *firmware,* valamint egyéb szoftverek és adatkomponensek.

A kiberszemélyiség-réteg a szervezetek és az egyének virtuális reprezentációiból áll. Idetartoznak az e-mail-címek, a felhasználói azonosítók, a közösségimédia-fiókok, az avatarok, az álnevek, az egyéni IP- és MAC-címek stb.[14] E rétegen keresztül lehet közvetlenül elérni a felhasználókat.

A kibertér e rétegeinek azonosítása lehetőséget ad arra, hogy az információs műveletekkel összefüggésben, a kibertéri műveletek keretében értelmezzük a három rétegben folytatható információs tevékenységeket.

Az információs műveletek rövid áttekintése

Ahhoz, hogy az információs műveletekkel összefüggésben értelmezzük a kibertéri műveleteket, célszerű röviden áttekinteni az információs műveletek lényegét és információs képességeit. Az információs műveletek működési területe az információs környezet, amelyben fizikai, információs és kognitív dimenziók értelmezhetők. A kibertér e környezet egyre fontosabb és jelentősebb részét képezi, és mint ahogy az előzőekben láttuk, az információs környezet mindhárom dimenzióját érinti.

Az információs műveletek kifejezés olyan katonai műveleti képességet jelent, amelynek általános célja a katonai műveletek támogatása az információs környezetben. Ezt az általános célt a műveletek jellegétől, környezetétől és célközönségétől függően információs fölény kialakításával és/vagy befolyásoló hatások előidézésével érheti el. A hagyományos katonai műveletekben az információs fölény alapvetően technikai kérdés, amelyet a szemben álló fél információs képességeinek gyengítésével és a saját képességek védelmével lehet elérni. A 4. generációs műveletekben azonban az információs műveleteket gyakran nem ellenséges erők ellen hajtják végre, hanem a célközönséget semleges, civil szereplők képezik. E műveletekben a cél nem a képességek gyengítése, hanem a civil szereplők meggyőzése vagy befolyásolása. Ezt a befolyásoláson alapuló adaptív információs fölény révén lehet elérni.[15]

[14] AJP-3.20 (2020): i. m. 3–4.

[15] Joint Doctrine Note 2/13: Information Superiority. Swindon, Ministry of Defence, 2013. 1–4.

> „Az információs műveletek az információs környezetben érvényesülő információs képességek integrált, összehangolt és koordinált alkalmazására irányuló tevékenységek összessége, amelyek a műveletek célkitűzéseinek elérése érdekében, kognitív képességekkel közvetlenül, ill. technikai képességekkel közvetetten hatásokat gyakorolnak a műveletekben résztvevő célközönség szándékára, helyzetértelmezésére és képességeire."[16]

A meghatározás alapján az információs műveletek lényege és erősokszorozó jellege a különféle információs képességek integrációjában és a műveleti céloknak megfelelő összehangolásában rejlik. Ezek az információs képességek attól függően, hogy milyen dimenziókra hatnak, két nagy csoportba sorolhatók: technikai képességek és kognitív képességek.

A technikai képességek az információkezelési folyamatokra összpontosítanak, nevezetesen az információgyűjtésre, -tárolásra, -feldolgozásra és -továbbításra, és közvetetten gyakorolnak hatásokat a célközönségre. Ezzel szemben a kognitív képességek különböző információközvetítő eszközök és módszerek használatával az információ tartalmára fókuszálnak, és közvetlenül az emberek tudati tevékenységét célozzák meg előre megtervezett üzenetekkel.

A fentiek alapján az információs műveletek technikai és kognitív képességei közé a következőket sorolhatjuk:

- technikai képességek:
  - elektronikai hadviselés (*electronic warfare* – EW);
  - számítógép-hálózati műveletek (*computer network operations* – CNO);
  - információs célpontok fizikai megsemmisítése;
  - műveleti biztonság technikai képességei;
  - megtévesztés technikai képességei;
- kognitív képességek:
  - pszichológiai műveletek (*psychological operations* – PSYOPS);
  - civil-katonai együttműködés;
  - a műveletbiztonság kognitív képességei;
  - a megtévesztés kognitív képességei.[17]

A célközönségnek megfelelő technikai és kognitív képességek szinkronizált és integrált alkalmazása biztosítja az információs műveletek céljainak elérését, és ezáltal a katonai műveletek sikeres támogatását.

[16] Haig (2018): i. m. 210.
[17] Haig (2018): i. m. 215.

Kibertéri műveletek

A kibertéri műveletek értelmezéséhez az információs műveletekkel analóg módon célszerű megvizsgálni, hogy e műveletekben a fölény kialakítható-e, és ha igen, akkor mely információs tevékenységek és milyen módon alkalmazhatók ennek érdekében. Az alábbi alfejezetekben e kérdéseket tekintjük át.

Kibertéri fölény és kibertéri befolyásoló hatások

A kibertér jelentőségének felismerésével párhuzamosan a katonai doktrínákban is megjelent a kibertéri fölény értelmezése. Az amerikai hadsereg 2017-ben kiadott FM 3-12 doktrínája az alábbiak szerint definiálja a kibertéri fölényt: „a kibertéri fölény egy katonai erő kibertéri dominanciájának azon foka, amely lehetővé teszi számára, ill. a kapcsolódó földi, légi, tengeri és űrbéli erők számára, hogy adott időben és helyen biztonságos és megbízható műveleteket folytasson anélkül, hogy az ellenség vagy a szemben álló fél akadályozná abban."[18] A kibertéri műveletek számos analógiát mutatnak az információs műveletekkel, amelyek közül az egyik a fölény kialakítására való törekvés. A kibertéri fölény az információs fölénynek az a része, amely a hálózatba kapcsolt infokommunikációs rendszerek felhasználásával érhető el, és ennek eredményeként a saját képességek jelentősen megnőnek.

A 4. generációs hibrid műveletekben, ahol gyakran nincs ellenség, vagy nem azonosítható egyértelműen, a hagyományos információs fölényhez hasonlóan a fentieknek megfelelően nem lehet kialakítani a kibertéri fölényt. Ebben az esetben ugyanis a kibertámadások és a kibertéri negatív befolyásoló tevékenységek nem alkalmazhatóak a civil szereplőkkel szemben. A cél ehelyett a pozitív befolyásolással kialakított adaptív kibertéri fölény megteremtése.

A kibertéri műveletek értelmezése

A kibertéri műveletek kialakulása katonai megközelítésben az információs műveletekhez kötődik, azon belül a számítógép-hálózatok harctéri megjelenésével

[18] FM 3-12: *Cyberspace and Electronic Warfare Operations.* Washington DC, Headquarters Department of the Army, 2017. április 1–3.

közel egy időben a CNO-hoz vezethető vissza. Habár az USA szárazföldi haderejének 1996-os első információsműveletek-doktrínája[19] még nem tartalmazta ezt a fajta képességet, két évvel később az összhaderőnemi információs műveletek doktrínája[20] már beemelte a számítógép-hálózati támadást (*computer network attack* – CNA) és az informatikai biztonságot *(computer security)* az információs műveletek elemei közé. A CNO komplex képességként pedig elsőként az amerikai összhaderőnemi információs műveletek 2006-os doktrínájában jelent meg mint az információs műveletek alapvető képessége.[21]

A kibertéri műveletek fogalma tehát a CNO-ból fejlődött ki, de a korábban bemutatott kibertéri technológia fejlődése és a kibertér komplex értelmezése következtében ma már annak nem csak egyedüli képességét jelenti. A NATO kibertériműveletek-doktrínája általánosságban fogalmazza meg a kibertéri műveleteket, amelynek értelmében e műveletek „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".[22] A doktrína a támadó és védelmi célú kibertéri műveleteket különbözteti meg.

A kibertéri műveleteknek az információs műveletekkel való szoros kapcsolódása, illetve a kibertér kibővített értelmezése lehetőséget ad arra, hogy a fenti doktrína meghatározásához képest konkrétabban definiáljuk a kibertéri műveleteket. Ezekre figyelemmel, a kibertéri műveletek alatt a kibertérben érvényesülő információs képességek integrált, összehangolt és koordinált alkalmazására irányuló tevékenységek összességét értjük, amelyek a műveleti célok érdekében, a kibertéri hálózatos infokommunikációs rendszereket felhasználva hatásokat gyakorolnak a műveletekben részt vevő célközönség szándékára, helyzetértelmezésére és képességeire. Fontos hangsúlyozni, hogy mint ahogy az információs műveletekkel, úgy a kibertéri műveletekkel is minden esetben az emberre, a felhasználóra, vagyis a célközönségre kívánunk hatást gyakorolni. Ezt a kibertérben a hálózatos infokommunikációs technológiát felhasználva, kognitív információs képességekkel közvetlenül, illetve technikai információs képességekkel közvetetten érhetjük el.[23]

[19] FM 100-6: *Information Operations.* Washington DC, Headquarters Department of the Army, 1996. augusztus.

[20] JP 3-13: *Joint Doctrine for Information Operations* (1998. okóber 8.).

[21] JP 3-13: *Joint Doctrine for Information Operations* (2006. február 13.). II-4.

[22] AJP-3.20 (2020): i. m. 4.

[23] Haig (2018): i. m. 237.

A kibertéri műveletek effajta értelmezése a NATO és az USA korábban hivatkozott kiberműveleti doktrínáinak a továbbgondolása, amelynek alapját az adja, hogy az információs műveletekhez hasonlóan az adott műveleti térben, vagyis a kibertérben értelmezhető információs képességek integrációja és a műveleti céloknak megfelelő összehangolása a korábbi szűken vett értelmezéshez képest nagyobb lehetőségeket és műveleti hatékonyságot biztosít.

A kibertéri műveletek információs képességei

A kibertér kiterjesztett értelmezését figyelembe véve az információs műveletek szinte mindegyik korábban felsorolt technikai és kognitív információs képessége alkalmazható a kibertéri műveletekben támadó, védelmi, valamint befolyásolási céllal.

Támadásra és védelemre a kibertér fizikai és logikai rétegében alapvetően a különféle technikai képességekkel számolhatunk, amelyek közül a legjellemzőbb és legelterjedtebb a logikai rétegben megvalósuló klasszikus CNO, amelynek keretében hálózati felderítő-, támadó- és védelmi tevékenységek alkalmazhatók. Emellett a fizikai rétegben a vezeték nélküli technológiáknak köszönhetően egyre fokozottabban számolhatunk a hálózatos rendszerek és a hálózati kommunikáció elektronikai alapú felderítésével, azon belül is elsősorban a rádiófrekvenciás tartományban a rádióelektronikai felderítéssel (*signal intelligence* – SIGINT), valamint ezek elektromágneses spektrumban való támadásával (például zavarásával) és védelmével, vagyis az EW-vel. E technikai képességeken belül a teljesség igénye nélkül az alábbi támadó- és védelmi tevékenységek alkalmazhatók:

- a számítógép-hálózatokhoz való hozzáférés és azok felderítése, kihasználása (CNO);
- az adatbázisokhoz való hozzáférés, azok módosítása és megsemmisítése (CNO);
- kártékony programokkal *(malicious software – malware)* a hálózat és elemei működésének korlátozása (CNO);
- túlterheléses támadásokkal (*distributed denial of service* – DDoS) a szolgáltatásokhoz való hozzáférés akadályozása (CNO);
- a hálózati kommunikáció felfedése és lehallgatása (SIGINT);
- az adatgyűjtő szenzorok és hálózati kommunikációs eszközök és rendszerek elektronikai zavarása (EW);

– a hálózatos rendszerekben alkalmazott navigációs rendszerek elleni elektronikai támadások különböző formái, például elektronikai zavarás, hamisítás (EW); valamint
– védelem a másik fél hasonló tevékenységei ellen (CNO, EW).

A kibertér és az elektromágneses spektrum közötti konvergencia a vezeték nélküli hálózatos technológiáknak köszönhetően egyre markánsabbá válik. A teljes konvergencia azonban még nem valósult meg, de például az amerikai hadsereg 2017-ben kiadott szakmai doktrínája[24] már kellően alátámasztja az elektromágneses spektrumban zajló EW és a kibertéri műveletek közötti egyre szorosabb kapcsolatot, különösen azért, mert az elektromágneses spektrumban alkalmazható technikák kibővítik a hálózatok elleni fenyegetések lehetőségét.

Az EW sok tekintetben hasonlít a CNO-hoz. Mindkettő fő feladata az infokommunikációs rendszerek felderítése, támadása és védelme, de míg az előbbi ezeket az elektromágneses spektrumban, fizikai hatások előidézésével éri el, addig az utóbbi mindezeket logikai módszerekkel, például *malware*-ekkel végzi. Az EW a kibertérben a hálózati eszközök és a hálózati kommunikáció elektronikai megfigyelésében (SIGINT, elektronikai támogatás), elektronikai támadásában (elektronikai zavarás, megtévesztés és megsemmisítés), valamint a saját rendszerek elektronikai védelmében nyilvánul meg. Egy további szoros kapcsolódási pont, hogy a vezeték nélküli hálózatokba a különféle *malware*-ek a rádiófrekvenciás tartományt felhasználva juttathatók be. Ez sajátos és újszerű elektronikai támadási technikának tekinthető, amely a rádiófrekvenciás zavarás helyett a fizikai és logikai módszereket ötvözi. Ez különösen nagy fontosságot kap a szoftvervezérelt rádiórendszerekkel (*software defined radio* – SDR) megvalósított hálózati kommunikáció esetében.

A hálózatos technológia jelentősen kiterjeszti a kognitív hatásokat előidéző képességek lehetőségeit, alkalmazási módjait is a kibertérben. Az internet és azon belül a közösségi média új lehetőségeket nyitott a kognitív befolyásolás terén, amit egyre nagyobb mértékben használnak ki az egyes szereplők. Ez azt jelenti, hogy az internetes médiafelületeket és a közösségi szolgáltatásokat kognitív hatások előidézésére használják.

Kibertéri befolyásolásra, illetve megtévesztésre és manipulációra a kibertér kiberszemélyiség-rétegében a kognitív képességek közül elsősorban a PSYOPS és a megtévesztés alkalmazható. Az előbbi körébe tartozhatnak az internetes

[24] FM 3-12 (2017): i. m.

hírportálokon és a közösségi médián keresztül terjesztett valós üzenetek és hírek, amelyek képesek befolyásolni a kiválasztott célcsoportot vagy célszemélyeket, illetve a közvéleményt. Az utóbbi körébe pedig az álhírekkel megvalósított félretájékoztatás, félrevezetés és manipuláció sorolható.

A kibertér befolyásolási célból való felhasználásának egyik legnagyobb előnye, hogy az üzenetek rövid idő alatt széles tömegekhez juthatnak el, aminek köszönhetően az információ terjedési sebessége és célcsoportja megsokszorozódik. Mindezeken túl a véleményvezérek közösségi oldalakon keresztüli megcélzásával a befolyásuk alatt lévők jóval könnyebben elérhetők, és az üzenetek is hatékonyabban célt érnek és érvényesülnek. A teljesség igénye nélkül a kibertéri műveletek legjellemzőbb információs képességeit, célpontjait, valamint eszközeit és módszereit az *1. táblázat* foglalja össze.

1. táblázat: A kibertéri műveletek legjellemzőbb információs képességei

Kibertéri műveleti képesség	**Célpontok**	**Eszközök és módszerek**
Számítógép-hálózati műveletek	Hálózat, szoftverek, operációs rendszerek, adatbázisok, hardverelemek, kiberfizikai eszközök	Számítógép-hálózati felderítés, támadás, védelem, például *malware,* DDoS, adatbázistörlés, -módosítás, APT-támadás stb.
Elektronikai felderítés	Hálózati elektronikai eszközök, vezeték nélküli kommunikáció	SIGINT, műszeres felderítés, nyílt forrású felderítés
Elektronikai hadviselés	Hálózati elektronikai eszközök, szenzorok, vezeték nélküli kommunikáció, navigáció, kiberfizikai eszközök	Elektronikai felderítés, elektronikai zavarás, elektronikai megtévesztés, elektronikai megsemmisítés, elektronikai védelem
Pszichológiai műveletek	Emberek, közösségi csoportok	Befolyásolás internetes hírportálokon, közösségi médián, e-mail-en keresztül, *social engineering*
Megtévesztés	Hálózat, szenzorok, adatbázisok, kommunikáció, emberek, közösségi csoportok	Elektronikai megtévesztés, imitálás, dezinformáció, *spoofing, social engineering,* álhírek stb.

Forrás: Haig (2018): i. m. 240.

A politika, a gazdaság és az egész társadalom működésének hálózatos infokommunikációs technológiától való függősége ahhoz vezetett, hogy mára a kibertérből érkező fenyegetések egyre gyakoribbakká váltak. Szinte naponta hallani újabb és újabb kibertámadásokról, amelyek akár technikai, akár kognitív tevékenységek formájában valósulnak meg. Többnyire a technikai oldalhoz sorolható például a katona-politikai hatású és a NATO kibertéri gondolkodását is megváltoztató 2007-es Észtország elleni DDoS-támadássorozat,[25] vagy például a 2021. májusi jelentős gazdasági károkat és üzemanyaghiányt okozó zsarolóvírus-támadás az észak-amerikai Colonial Pipeline olajvezetékhálózat ellen.[26] A legismertebb kognitív kibertámadásokhoz pedig többek között a 2016-os amerikai elnökválasztási kampány befolyásolása sorolható, amelyben többek között szerepet játszott a Cambridge Analytica és a Facebook felhasználói adatbotránya,[27] illetve a szentpétervári székhelyű Internetkutató Ügynökség (Internet Research Agency – IRA)[28] nevű „trollgyár" is.

Bár e néhány kiragadott példa esetében is megfigyelhető volt, hogy többféle információs tevékenységet is alkalmaztak a támadók, azoknak a kibertéri műveletekre jellemző összehangolt és integrált alkalmazása leginkább az orosz–ukrán konfliktusban figyelhető meg. E konfliktusban ugyanis egyértelműen felismerhető a hibrid hadviselés keretében alkalmazott kibertéri műveletek korábban bemutatott komplexitása, amelyet a 2. táblázat is szemléltet. A válságot megelőzően mind orosz, mind ukrán hackercsoportok több száz DDoS- és *defacement* támadást intéztek állami szervek weboldalai ellen. A válság kirobbanását követően az ukrán mobiltávközlési hálózatot és a vezetési és irányítási rendszereket korlátozták egyrészt a szolgáltató létesítményének elfoglalását követően odatelepített blokkolókkal, valamint az EW rendszerekben alkalmazott különféle zavaró berendezésekkel.[29] 2015 decemberében az ukrán áramellátásban volt

[25] Kovács László: *A kibertér védelme.* Budapest, Dialóg Campus, 2018. 145.

[26] Renee Dudley – Daniel Golden: The Colonial Pipeline Ransomware Hackers Had a Secret Weapon: Self-promoting Cybersecurity Firms. *MIT Technology Review,* 2021. május 24.

[27] Kovács László – Krasznay Csaba: „Mert övék a hatalom": Az internet politikát (is) befolyásoló hatása a 2016-os amerikai elnökválasztás során. *SVKK Elemzések,* (2017), 9.

[28] Jason Parham: Facebook and the Price of Tech Utopia. *Wired.com,* 2018. április 10.

[29] Sergey Sukhankin: Russian Electronic Warfare in Ukraine: Between Real and Imaginable. *Eurasia Daily Monitor,* 71. (2017), 14.

szolgáltatáskiesés, amelyet egy APT-támadás keretében a BlackEnergy nevű trójaival idéztek elő.[30]

2. táblázat: Az orosz–ukrán konfliktus kibertéri műveletek célpontjai, képességei és hatásai

Célpontok	Ukrán és orosz intézmények, hálózatok, csatlakoztatott eszközök, ipari vezérlőrendszerek, média, lakosság és semleges érintettek
Eszközök és módszerek	DDoS, weboldal defacement, *malware*-ek (BlackEnergy, Snake, Operation Armageddon, X-Agent, CrashOverride, NotPetya, BadRabbit, VPNFilter, Python/Telebot), elektronikai lehallgatás, zavarás, hagyományos elektronikus és online média, közösségi oldalak, Internetkutató Ügynökség, propaganda- és álhírkampányok
Hatások, eredmények	Szolgáltatáshoz való hozzáférés akadályozása, adatlopás, kommunikáció akadályozása, ukrán erőművek elleni támadás miatt több órás áramkimaradás, sérült számítógépek, eszközök és rendszerek, célközönség befolyásolása, manipulálása, félrevezetése
Időtartam	2013 novemberétől napjainkig

Forrás: Haig (2018): i. m. 240.

E technikai kiberképességek mellett a kognitív képességek 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. Egy vizsgálat például igazolta, hogy 2014-től kezdve a Twitteren ugrásszerűen megnőtt az Ukrajnával foglalkozó tweetek száma. Ezeket a befolyásoló, manipuláló üzeneteket és gyakran álhíreket döntően a már említett szentpétervári „trollgyár" állította elő. Kiemelendő például, hogy 2014. július 18-án, a malajziai repülőgép lezuhanásának napján több mint 44 000, a következő napon pedig több mint 25 000 üzenetet tettek közzé. Ezekben a tweetekben 297 fiók terjesztett olyan információkat, amelyek szerint Ukrajna volt a felelős a maláj gép lelövéséért.[31]

A néhány kiragadott példa és a konfliktus kibertéri műveleteit összefoglaló *2. táblázat* is jól szemlélteti e műveletek komplexitását, és azt, hogy mind

[30] Marie Baezner – Patrice Robin: *Cyber and Information Warfare in the Ukrainian Conflict, Version 2.* Center for Security Studies (CSS), ETH Zürich, 2018. október 10.

[31] Oleksandr Nadelnyuk: How Russian "Troll Factory" Tried to Effect on Ukraine's Agenda. Analysis of 755 000 tweets. *VoxUkraine,* é. n.

a reguláris és irreguláris erők, mind a civil hackercsoportok által folytatott műveletek egyre gyakrabban járulnak hozzá katonai és politikai célok eléréséhez.

Következtetések

Mára a hálózatok kialakítása, a hálózati elemek és azok struktúrája, valamint a hálózati kommunikáció megvalósítása a hagyományos számítógép-hálózatokhoz képest jelentős átalakuláson ment keresztül. A felhőtechnológia, az IoT- és az M2M-kapcsolatoknak köszönhetően a kiberfizikai érzékelőkkel és aktuátorokkal rendelkező hálózatokban megvalósul a teljes összekapcsolódás, ahogyan azt például az okosotthon- és az okosváros-koncepciók is alátámasztják.

A közösségi hálózatok térnyerésének és fokozódó szerepének eredményeképpen pedig az emberek is egyre inkább a hálózatok részesévé válnak. Mindez rávilágít a kibertér azon természetére, ahol az emberek, a számítógépek és az intelligens eszközök egymással összekapcsolódnak. A kibertér mára az interperszonális kapcsolatok mellett az ember-gép és a gép-gép kapcsolatok színterévé vált.

Az egyének közösségi hálózaton való könnyebb elérhetőségének következtében, valamint a vezeték nélküli technológia természetéből adódóan az újfajta hálózatok a jól ismert szoftveres támadások mellett számos korábban nem jellemző sebezhetőséggel, fenyegetéssel is szembesülnek, mint például az érzékelők által gyűjtött adatok módosítása, a vezeték nélküli adatkommunikáció lehallgatása és/vagy elektronikai zavarása, illetve az emberek kognitív befolyásolása, manipulálása.

A kibertérben zajló katonai műveletek szempontjából az új technológiák és az újfajta sebezhetőségek szükségessé tették a kibertérnek és struktúrájának újraértelmezését. Ennek megfelelően a tisztán logikai felfogás mellett a fizikai tér, beleértve az elektromágneses spektrumot is, valamint a kognitív tartomány is fontos részét képezi a kibertérnek. A kibertér háromrétegű (fizikai, logikai és kiberszemélyiség-réteg) struktúrája lehetőséget ad a kibertéri műveletek komplexebb értelmezésére, amely nem korlátozódik kizárólag a CNO-ra. E komplex értelmezés lényege, hogy a kibertéri műveletek keretében az információs műveletekhez hasonlóan, olyan egymással összehangolt technikai és kognitív információs képességeket lehet alkalmazni, amelyek egymás hatásait kihasználva a kibertérben érvényesülnek. Ez pedig a korábbi értelmezéshez képest nagyobb lehetőségeket és műveleti hatékonyságot biztosít az alkalmazók számára.

Ezek a kibertéri információs képességek az alábbiak lehetnek:

- a logikai rétegben alkalmazott logikai (szoftveralapú) információs képességek, mint például *malware*-ek, DDoS-támadások, APT-támadások, tűzfalak, vírusirtók stb.;
- a fizikai rétegben és benne az elektromágneses spektrumban folytatott elektronikai felderítés (különösen a SIGINT), elektronikai zavarás, megtévesztés és megsemmisítés, valamint a fizikai és elektronikai védelem módszerei stb.;
- a kiberszemélyiség-rétegben, azaz a kognitív tartományban valós és hiteles vagy félrevezető információkon alapuló kognitív képességek, mint a PSYOPS, a megtévesztés, az álhírek stb.

A kibertéri műveletek hatékonysága tehát nagymértékben függ a kibertér mindhárom rétegében zajló információs tevékenységek összehangoltságától. A tapasztalatok pedig azt is mutatják, hogy a kibertér által biztosított hálózati technológiáknak köszönhetően nemcsak a katonai műveletekben, hanem a politikai és gazdasági konfliktushelyzetekben is a kibertéri műveletekbe integrált és egymással összehangolt információs tevékenységek nagyobb eredményességgel alkalmazhatók.

Irodalomjegyzék

AJP-3.20: *Allied Joint Doctrine For Cyberspace Operations. Edition A Version 1.* NATO Standardization Office, 2020. január 4.

Baezner, Marie – Patrice Robin: *Cyber and Information Warfare in the Ukrainian Conflict, Version 2.* Center for Security Studies (CSS), ETH Zürich, 2018. október. Online: www.researchgate.net/publication/322364443_Cyber_and_Information_warfare_in_the_Ukrainian_conflict

Dudley, Renee – Daniel Golden: The Colonial Pipeline Ransomware Hackers Had a Secret Weapon: Self-promoting Cybersecurity Firms. *MIT Technology Review*, 2021. május 24. Online: www.technologyreview.com/2021/05/24/1025195/colonial-pipeline-ransomware-bitdefender/

FM 100-6: *Information Operations.* Washington DC, Headquarters Department of the Army, 1996. április

FM 3-12: *Cyberspace and Electronic Warfare Operations.* Washington DC, Headquarters Department of the Army, 2017. április 1–3. Online: https://irp.fas.org/doddir/army/fm3-12.pdf

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

ITU RM 2083: *Recommendation ITU RM 2083-0 (09/2015) Framework and Overall Objectives of the Future Development of IMT for 2020 and Beyond.* 2015. Online: www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.2083-0-201509-I!!PDF-E.pdf

Joint Doctrine Note 2/13: Information Superiority. Swindon, Ministry of Defence, 2013. Online: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/819814/archive_doctrine_uk_info_superiority_jdn_2_13.pdf

JP 3-12: *Cyberspace Operations.* 2018. június 8.

JP 3-13: *Joint Doctrine for Information Operations* (2006. február 13.).

JP 3-13: *Joint Doctrine for Information Operations* (1998. október 8.).

Kovács László – Krasznay Csaba: „Mert övék a hatalom": Az internet politikát (is) befolyásoló hatása a 2016-osamerikai elnökválasztás során. *SVKK Elemzések,* (2017), 9. Online: https://bit.ly/3Ox1FKi

Kovács László: *A kibertér védelme.* Budapest, Dialóg Campus, 2018.

Kuehl, Daniel: From Cyberspace to Cyberpower: Defining the Problem. In Franklin D. Kramer – Stuart H. Starr – Larry K. Wentz (szerk.): *Cyberpower and National Security.* University of Nebraska Press, 2009. 24–42.

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 STO: *Military Applications of Internet of Things.* 2016. Online: www.sto.nato.int/Lists/test1/activitydetails.aspx?ID=16536

Parham, Jason: Facebook and the Price of Tech Utopia. *Wired.com,* 2018. április 10. Online: www.wired.com/story/facebook-price-of-tech-utopia

Relia, Sanjeev: *Cyber Warfare: Its Implications on National Security.* New Delhi, Vij Books India Pvt Ltd., 2015.

Schmitt, Michael N. (szerk.): *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge, Cambridge University Press, 2017.

Statista: *Forecast Number of Mobile 5G Subscriptions Worldwide by Region from 2019 to 2026* (2021. január). Online: www.statista.com/statistics/760275/5g-mobile-subscriptions-worldwide/

Statista: *Number of Internet of Things (IoT) Connected Devices Worldwide in 2018, 2025 and 2030* (2021. január). Online: www.statista.com/statistics/802690/worldwide-connected-devices-by-access-technology/

Sukhankin, Sergey: Russian Electronic Warfare in Ukraine: Between Real and Imaginable. *Eurasia Daily Monitor,* 71. (2017), 14. Online: https://jamestown.org/program/russian-electronic-warfare-ukraine-real-imaginable/

USNA: *Aspects and Pillars of Cyber Security* (é. n.). Online: www.usna.edu/CyberDept/sy110/calendar.php?type=class&event=2

Xu, Ke – Yi Qu – Kun Yang: A Tutorial on Internet of Things: From a Heterogeneous Network Integration Perspective. *IEEE Network,* 30. (2016), 2. 102–108. Online: https://doi.org/10.1109/MNET.2016.7437031

Zheng, Denise E. – William A. Carter: *Leveraging the Internet of Things for a More Efficient and Effective Military.* Center for Strategic & International Studies. Rowman & Littlefield, 2015. szeptember. Online: https://cdn.mashreghnews.ir/files/fa/news/1395/2/29/1638212_510.pdf