HADMÉRNÖK
VÉDELEMINFORMATIKA

18. évfolyam (2023) 2. szám 155–165.
DOI: 10.32567/hm.2023.2.10

Vattai Eszter[1]

A nyílt forrású információszerzés kapcsolata a hadsereggel[2]

Open Source Intelligence in the Context of the Military

Absztrakt

Az infokommunikációs technológiák és az azokkal szoros kapcsolatban lévő közösségimédia-platformok napjaink egyik leggyorsabban változó és fejlődő területei. A jelenben, ha egy képet megosztunk, ha egy posztot kiírunk, vagy elfogadjuk azokat a bizonyos „cookie" beállításokat, minden mozdulatunk és érdeklődési körünk lekövethető. A technológia fejlődése megteremtette azt a különleges helyzetet, hogy a felelőtlen, nem biztonságtudatos felhasználók nagyon könnyen lekövethetővé és lehallgathatóvá váltak.
Kutatásom célja az OSINT-eszközök és az infokommunikációs technológiák komplex vizsgálata katonai aspektusokban. Jelenleg csak nagyon szűk körben vizsgált terület hazánkban a nyílt forrású információszerzés, ennek megfelelően ez ösztönzött arra, hogy ezzel a területtel foglalkozzam.
Előzetes elemzéseim alapján (jellemzően nemzetközi szakirodalmak vizsgálatával) arra a következtetésre jutottam, hogy az OSINT-tevékenységeknek egyre nagyobb hatása lesz a katonai műveletekre, így kiemelten fontosnak tartom egy ilyen irányú kutató-elemző munka végrehajtását.
Kutatási kérdéseimen keresztül tematikusan építettem fel a megállapításokat, amelyeknek részleteit a kutatás első felében ismertetem.

Kulcsszavak: OSINT, nemzetbiztonság, katonai műveletek, orosz–ukrán háború

[1] Hallgató, Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar, e-mail: vattaieszter2001@gmail.com
[2] A publikáció az Innovációs és Technológiai Minisztérium ÚNKP-22-1-I-NKE-34 kódszámú Új Nemzeti Kiválósági Programjának szakmai támogatásával készült.

Abstract

Information and communication technologies and the social media platforms that are closely linked to them are one of the fastest changing and evolving areas today. In the present, by sharing a picture, posting a story, or accepting certain 'cookie' settings, our every move and interest can be tracked. Advances in technology have created the unique situation where irresponsible, insecure users are very easily tracked and intercepted.
The aim of my research is a complex study of OSINT devices and infocommunication technologies in military aspects. Currently, open-source information acquisition is only a very narrowly investigated area in our country, and this is what prompted me to focus on this area. Based on my preliminary analyses (typically by examining international literature), I have concluded that OSINT activities will have an increasing impact on military operations, and therefore I consider it of utmost importance to carry out a research and analysis work in this direction.
Through my research questions, I have structured my findings thematically, the details of which are presented in the first half of this study.

Keywords: OSINT, national security, military operations, Russian-Ukraine conflict

Bevezetés

A nyílt forrású információszerzés (továbbiakban: OSINT[3]) célja alapvetően, hogy a felhasználó információigényeire minél pontosabb, teljesebb, hitelesebb választ tudjon adni, illetve a felhasználó szándékának megfelelő információt biztosítson. Az OSINT teljesen átformálta jelen korunk hírszerzését is. A közösségi média mellett számos más nyílt forrás is rendelkezésre áll.[4] Az interneten keresztül elérhetőek a rádió- és tv-adások, visszakövethetők a publikációk, az újságok. Keresni lehet képekre, videókra, dokumentumokra, vagy akár webkamerákat is lehet nézni. Továbbá az interneten a különböző geolokációs adatokat is le lehet kérdezni.

Katonai műveletek előtt az információk körülbelül 80%-át nyílt forrásokból gyűjtik össze. Magyar vonatkozásban az Információs Hivatal (IH) gyűjti össze az információkat és szűri ki ezek közül a feladatellátáshoz a legmegfelelőbbeket.[5]

A releváns hazai és nemzetközi szakirodalmak elemzése mellett a következő kutatási módszereket alkalmaztam: kérdőíves felmérés a közösségimédia-használat és digitális higiénia kérdéskörökben a magyar szerződéses és hivatásos katonák körében, továbbá interjú készítése a Magyar Honvédség felső vezetésében dolgozó szakemberekkel, a nyílt forrású információszerzés hatásairól napjaink műveleti környezetére. Az OSINT rendkívül fontos napjaink katonai műveleteiben, ezért a célom ezeknek az állításoknak a megválaszolása és bizonyítása.

A kutatásom kezdetén a következő kutatási kérdéseket fogalmaztam meg:

[3] Open Source Intelligence.
[4] Bányász 2015: 16.
[5] Dezső 2018: 100.

- Milyen új megoldásokat és kihívásokat jelent a katonai műveletekben a nyílt forrású információszerzés szélesebb körben történő elterjedése?
- Melyek azok az OSINT-alkalmazások és -szolgáltatások, amelyek segíthetik a parancsnokokat a döntéshozatali folyamatok során?

Ezek alapján a következő hipotéziseket fogalmaztam meg:

1. Véleményem szerint a nyílt forrású információszerzés felgyorsíthatja a műveleti információk gyűjtését, amely gyorsíthatja a döntéshozatali folyamatokat, valamint az információs fölény megszerzését.
2. Az orosz–ukrán konfliktusban megjelent OSINT-technikák nagymértékben támogathatják a szemben álló feleket az ellenséges csapatok helyének, mozgásának azonosításában.

A nyílt forrású információszerzés szerepe a katonai szervezeteknél

„A világunkat elárasztó adat- és információmennyiség célirányos monitorozására és kutatására aligha lenne lehetőség a nyílt forrásból származó információgyűjtés nélkül. A nemzetbiztonsági szolgálatok eszköztárában az OSINT egyre inkább meghatározó szerepet tölt be."[6]

A nemzetbiztonsági szolgálatoknál fontos azt elemezni, hogy milyen adatot vagy információt szeretnénk megszerezni, ennek értelmében a képességek és lehetőségek jelentős mértékben függnek az adatszerzés jellegétől és módjától.

Az információszerzést pedig az alábbi hírszerzési ágak végzik:

- emberi erőforrásokkal folytatott hírszerzés (HUMINT[7]);
- rádióelektronikai felderítés (SIGINT[8]);
- nyílt forrású hírszerzés (OSINT);
- képfelderítés (IMINT[9]);
- mérés és jelmeghatározó hírszerzés (MASINT[10]);
- kiberhírszerzés (CYBINT[11]).[12]

„A magyar nemzetbiztonsági gondolkodásban – a titkos információgyűjtés jogi szabályozásának elsődlegessége mellett – főként a hírszerzés-felderítés (intelligence) fogalomrendszerét és az ott megjelenő egyes ágakat (így pl. HUMINT, SIGINT, OSINT stb.) vehetjük alapul. Ennek kereteit tekintve azonban nem feltétlenül lehet és indokolt minden hazai információgyűjtő tevékenységet a jelzett fogalomrendszerbe besorolni, már csak az egyes területek eltérő adottsága vagy akár rendeltetése okán sem."[13]

6 Szabó 2019.
7 Human intelligence.
8 Signal intelligence.
9 Imagery intelligence.
10 Measurement and signature intelligence.
11 Cyber intelligence.
12 Vida 2018: 119.
13 Dobák 2018: 99.

Az egyik kiemelt szakasz az OSINT tekintetében a döntéshozatal. „A nemzetbiztonsági szolgálatok eszköztárában lévő lehetőségeket aszerint is érdemes tehát megvizsgálni, hogy jellemzőik által milyen hatást gyakorolhatnak a döntéshozók munkájára. Ez az OSINT estében is szükségszerű."[14] Tehát különböző szolgálatoknak érdemes összpontosítaniuk az alkalmazási kockázatokra.

Minden tevékenység mozgatóeleme a különböző médiumokon alapszik. Igaz az, hogy a titkos információgyűjtés forrásaiból származó információk esetében megvan a kockázata annak, hogy a minősített információk előbb-utóbb nyílt információkká alakulnak át és a médiában is megjelenhetnek.[15] A titkos információgyűjtés eszközeinek és módszereinek alkalmazása útján megszerzett minősített információknak az OSINT lehetőségeivel történő visszaellenőrzése pedig szinte lehetetlen. Viszont, ezekből az információkból is lehet szűrni különböző adatokat, amelyek hasznosak lehetnek a szolgálatok számára. Vagy éppen az információk kikerülése kárt is okozhat egy másik országnak. Ismertetőként mutatom be a különböző adatok kikerülésének veszélyességi szintjeit hazai vonatkozásban, amely kategóriába tudjuk helyezni az OSINT által szerzett információkat.[16]

„(4) Amennyiben az adat nyilvánosságra hozatala, jogosulatlan megszerzése, módosítása vagy felhasználása, illetéktelen személy részére hozzáférhetővé, valamint az arra jogosult részére hozzáférhetetlenné tétele

a) rendkívül súlyosan károsítja a minősítéssel védhető közérdeket, akkor »Szigorúan titkos!«,
b) súlyosan károsítja a minősítéssel védhető közérdeket, akkor »Titkos!«,
c) károsítja a minősítéssel védhető közérdeket, akkor »Bizalmas!«,
d) hátrányosan érinti a minősítéssel védhető közérdeket, akkor »Korlátozott terjesztésű!« minősítési szintű."[17]

Ezt az elemzés fázisában kell mérlegelni, és a következtetéseket levonni belőle.

További, az OSINT-tal szorosan összetartozó, kibontakozó hírszerzés az úgynevezett cyber intelligence (CYBINT) vagyis a kiberhírszerzés. Az ilyen típusú hírszerzés a fizikai kémkedés és a védelem keveréke a modern információs technológiával.

A kiberhírszerzés védelmet nyújt az olyan digitális fenyegetésekkel szemben, mint a vírusok, hackerek és terroristák, amelyek célja érzékeny információk ellopása az interneten keresztül.[18]

A CYBINT és az OSINT közti különbségnek az tekinthető, hogy míg a CYBINT-nél szükséges hackertevékenységet folytatni, addig az OSINT-nál ez nem túl nagy mértékben jelenik meg, hiszen lényegében csak a digitális lábnyomokat gyűjtjük össze.

Ehhez az alfejezethez zárszóként Vida Csaba véleményezését közlöm, amely a saját meglátásommal is egybefügg;

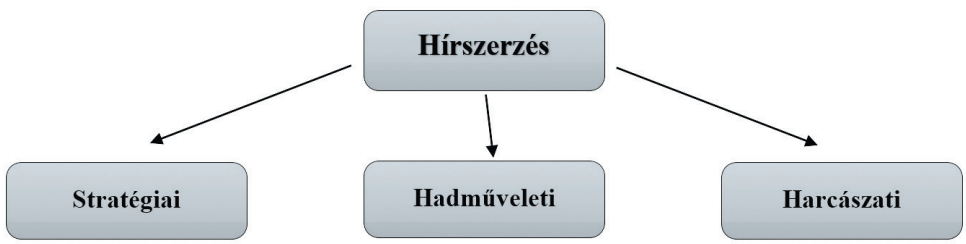
[14] Szabó 2019.
[15] Tóth 2020.
[16] Tóth 2021.
[17] 2009. évi CLV. törvény, II. Fejezet, 4. §.
[18] Lásd: https://usnwc.libguides.com/c.php?g=494120&p=3381599

„[…] egy régi hírszerzési ágként az OSINT a hírszerzési ciklus adatszerzési szakaszának integrált része, bár a korábbiakhoz képest jóval nagyobb hangsúlyt kapott, és esetenként egyedül is képes biztosítani a szükséges adatokat. Az OSINT esetében azonban ügyelni kell arra, hogy a hírszerzés ne váljon egyoldalúvá, mert a hatékony és eredményes munkához továbbra is szükség van a többi hírszerzési ág által megszerzett adatokra és információkra. A CYBINT-tel kapcsolatban más a helyzet, mert az alapvetően nem információszerző hírszerzési ág, hanem funkcióját vizsgálva inkább a fedett és a titkos hírszerzési akciókhoz lehet hasonlítani."[19]

Az orosz–ukrán háború OSINT-vonatkozásai

A közösségi média a nyílt forrású információgyűjtés aranybányája, és az egyének vagy a csapatmozgások felderítésére számos ingyenes, legális eszköz áll rendelkezésre, amit az előzőekben is kiemeltem.

Háborús helyzetben háromfelé lehet osztani a hírszerzést, ahogyan az 1. ábra szemlélteti.



1. ábra: A hírszerzés felosztása
Forrás: a szerző szerkesztése

A stratégiai szintű hírszerzéshez tartoznak a HUMINT és az OSINT eszközei is (például attasék, nagykövetek küldése).

A hadműveleti szintű hírszerzési feladatot főképpen a különleges erők és a mélységi felderítők végzik el. Fontos továbbá a SIGINT – jelhírszerzés – és az IMINT – képi hírszerzés – is ebben a szakaszban.

A harcászati szintű hírszerzés már csak felderítésnek tekinthető a parancsnok információigényei alapján; legjobb megoldása a drónokkal való felderítés.

Mindössze egy héttel azután, hogy Oroszország teljes körű inváziót indított Ukrajnában, az OSINT-ot széles körben kezdték el használni a hírekből és a közösségi médiából származó tényellenőrző narratívák megértésére.

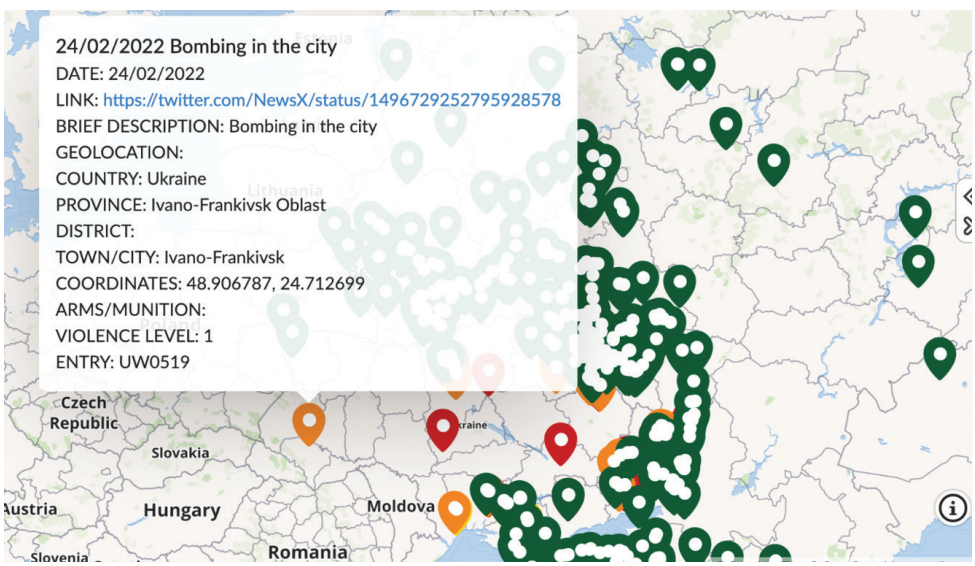
Kiemeltem ezek közül a három legfontosabb lekövetést:

- A katonai csapatok mozgásának lekövetéséhez a közösségi média tartalmaiból vett rendszámadatokat például arra használták, hogy járműveket kapcsoljanak

[19] Vida 2013.

össze a kormányzati szervekkel. A műholdfelvételek képei továbbá az orosz járművek mozgását is meghatározhatják.
- Felmérni az éppen zajló eseményeket és a sérülteket. Miközben a felhasználók fotókat és videókat tesznek közzé az eseményekről, az elemzők figyelemmel kísérhetik a támadásokat, és valós időben értékelhetik a károkat. A nyilvános közösségimédia-tartalmak és a műholdképek szintén segítenek az elemzőknek abban, hogy pontosan meghatározzák a tevékenységek földrajzi helyét.
- Ellenőrizni a dezinformált tartalmakat. Az elemzők használnak olyan alkalmazásokat, amelyek lehetővé teszik az események idő és hely szerinti csoportosítását. Több cég is foglalkozik ilyen típusú adatszelektációval.

A Center for Information Resilience cég intelligens térképe a Russia–Ukraine Monitor Map. A cég nyílt forrású információkból dokumentálja és ellenőrzi az információk hitelességét az ukrajnai konfliktus során történt jelentős eseményekről, majd egy térkép segítségével vizualizálja azt. Célja, hogy megbízható információkat nyújtson a politikai döntéshozók, újságírók, valamint igazságügyi szervek számára a változó helyzetekről. A Bellingcat és a Conflict Intelligence Team is képes hozzájárulni a térképek bővítéséhez azáltal, hogy a projekthez felülvizsgált összes tartalmat összegyűjtik, és megőrzésre elküldik a Mnemonicnak.[20] Erre látható példa a 2. ábrán.



2. ábra: Ivano-Frankivszkban történt bombamerénylet részletes kimutatása a térképen
Forrás: www.bellingcat.com/news/2022/02/27/follow-the-russia-ukraine-monitor-map/

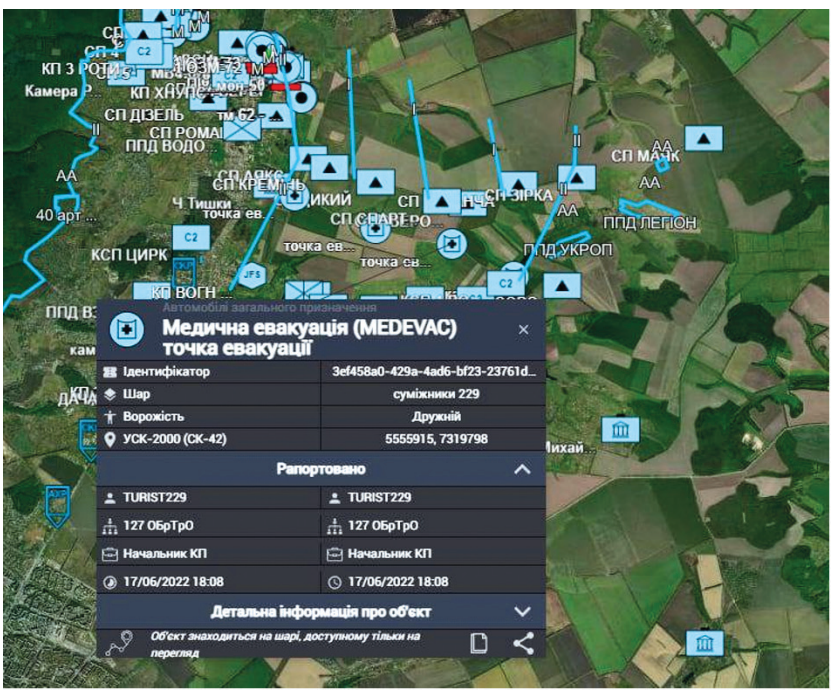
[20] A Mnemonic kiberbiztonsági szolgáltató egyértelmű válaszokat és utakat kínál összetett biztonsági kihívásokra. Lásd: www.mnemonic.io/company/

A következőkben a Joker-botrányról szóló következtetéseimet mutatom be, amelyben az ukrán katonai parancsnokság által használt amerikai „Delta" programot feltörte a „Joker DPR"[21] hackercsoport.

Korábban az ukrán média nyilvánosságra hozta az ukrán katonák által használt külföldi modern technológiákat és szoftvereket, amelyeket amerikaiaktól kaptak. Az ukrán katonák megalázták az oroszokat, mondván, hogy túl messze vannak az ilyen technológiáktól.

Az oroszok viszont, mondhatni, nem törődtek a saját rendszereik fejlesztésével, és feltörték az ellenség által használtakat. November 1-jén a DPR sajtószolgálatának vezetője, Daniil Bezsonov megerősítette, hogy a DPR hadserege hozzáférést kapott az ellenséges szoftverhez.

Hogy világos legyen, ez egy parancsnoki és irányítási program, amelyben a baráti és ellenséges csapatokra vonatkozó összes adat szerepel, és rendszeresen frissül, többek között a hírszerzési forrásokból származó információkkal, és amelynek egy aktuális állapotát a 3. ábra szemlélteti.[22]



3. ábra: Képernyőfotó a Delta rendszeren tárolt információkról

Forrás: https://southfront.org/us-delta-program-used-by-ukrainian-military-command-hacked-by-joker-dpr-hacker-team/

[21] Donetsk People's Republic.

[22] Lásd: https://southfront.org/us-delta-program-used-by-ukrainian-military-command-hacked-by-joker-dpr-hacker-team/

A katonai szakértőkkel végrehajtott kérdőíves felmérés következtetései

Befejezésként az interjúalanyokkal folytatott beszélgetés részleteit prezentálom. Az ő válaszaik elemzése után jutottam a következő állításokra, megválaszolva ezzel a kutatási kérdéseimet.

Milyen megoldásokat jelent a katonai műveletekben az OSINT szélesebb körben történő terjedése?

A katonai műveletekhez való szigorú kapcsolódást nehéz kívülről megítélni, de a jelenség gyökere abban rejlik, hogy azzal, hogy az infokommunikációs eszközök, onlineközösség-megoldások széles körben elterjedtek a társadalom tagjai között, mindenki (és nem csak a katonai szereplők) szükségszerűen fordul ezekhez. Kritikus eseményeknél, például fegyveres konfliktusnál az információk kiemelt szerepet kapnak, így minden forrásból (köztük a nyílt) is várják az aktuális, a helyzet megítélését segítő adatokat. Például az orosz–ukrán háború első napjaiban a keleti területen élő lakosság tömegesen osztotta meg az orosz csapatmozgásokra vonatkozó információkat (például Twitteren). Ezek nemcsak szöveges, hanem képi információk, fotók, videók is. Ezek a művelet szempontjából pozitív jellegűek lehetnek, hiszen a helyszínen lévő személyek általuk rendkívül értékes információkat nyújthatnak. Azonban ezen adatokkal vagy azok egyes elemeivel kapcsolatban felmerülhet a hitelesség kérdése. Könnyen előfordulhat, hogy e nyílt források tudatos alakításával az elérhető információk akár dezinformációs elemeket is tartalmazhatnak.

Az OSINT kapcsán létezik egy úgynevezett CNN-effektus, amikor a média a tudósítás és hírek tájékoztatásának szándékával akár hamarabb adott helyszínen lehet, mint más szereplők, így ebben az esetben ők lesznek az információk elsődleges forrásai (ez esetben is a hitelesség és a függetlenség kérdése merülhet fel). További hátránya (nézőpont kérdése) is lehet, hogy könnyen bemérhetővé válik az adott célpont.

A kihívások leküzdésére minden bizonnyal a mesterséges intelligencia használata és annak tanítása lesz majd a megoldás.

Mely alkalmazások segíthetik a parancsnokokat a döntéshozatal során?

Számos megoldás nyíltan elérhető a neten, a komolyabb változatok már csak előfizetés ellenében, gondolhatunk itt például az információbrókerekre, akik fizetés ellenében szolgáltatnak adatokat, vagy akár biztosítják az adott célra kifejlesztett szoftvereiket.

Akár ajánlhatók bizonyos felületek, azonban ezeket a másik fél a már említett módon akár ki is használhatja a befolyásolás érdekében. Felmerül a nyílt források hitelességének a kérdése, így például a média szerepe is, amelyet a felek szintén kihasználhatnak saját érdekeik érvényesítésére.

Az OSINT és megoldásai esetében a legnagyobb gond tehát az információk hitelességének kérdése, amelyek konfliktusos helyzetekben tömegesen jelennek meg, és szinte lehetetlen csak erre a forrásra hagyatkozva megállapítani azok valódiságát.

A parancsnokokat kielégítő két legfontosabb információ igénye az ellenségről és a terepről szerzett információk, megszerzésükben segíthetik őket a drónfelvételek is, amelyeket az aktuális időben készítenek el, és biztosan hitelesek.

Fontossá válnak az OSINT előnyei:

- akár ingyenes megoldások;
- nem kell hozzá engedély;
- tömegesen keletkeznek információk (ez akár gond is lehet);
- az információk a helyszínről érkezhetnek (például Twitter-videó);
- olcsóbb lehet, mint a HUMINT.

Ezenfelül hátrányai:

- tömegessége, amiből nehéz kiszűrni a számunkra értékeset;
- sokféle nyílt platform, amely forrásként szolgálhat;
- nehéz kiszűrni a hiteles információt.

Továbbá nagyobb hangsúlyt kell fektetni a Cyber Threat Intelligence-re (CTI) is.

Háborús helyzetben a HUMINT vagy az OSINT a célravezetőbb?

Mindkét felderítési fajta együttes alkalmazása (természetesen a többi felderítési móddal együtt) szükséges. A közeli és a távolabbi jövőben is szükség lesz a HUMINT-ra is. Ezek nem kizárólagosságot, hanem együttműködést jelentenek. A minden forrású felderítés (ASI, all source intelligence) elve továbbra is működik.

Amennyiben nincs adott helyszínen HUMINT-forrás, akkor szükségszerűen fordulnak az OSINT-hoz. Ha csak OSINT van, akkor a már jelzett hitelességi és tömegességi problémák adódnak.

Ugyanakkor megfelelő szakmai tudással a civil szereplő is akár mélyebb információt kiásható, mint egy HUMINT-forrás.

10 év távlatában mennyire fog fejlődni a technológia ahhoz, hogy egyre kevesebb legyen az adatszivárgás?

A technológia folyamatosan fog fejlődni, amivel mindenképpen szükséges a lépést tartani, azonban többnyire ezek magas költségű licenszek, szolgáltatások keretében valósulnak majd meg, amelyet nem tud minden szervezet finanszírozni.

Annak ellenére is, hogy a technológia a védelemben is hatalmas fejlődésen megy keresztül, a jövőben is lesz adatszivárgás. A technológia mellett ebben a kulcs az emberi tényező lesz, hiszen a védelem egyik igen markáns tényezője az ember. Meg lehet zsarolni, téveszteni, vagy más módszerekkel rá lehet venni a hibázásra. Ugyanakkor a technológiai és technikai fejlődés elérheti azt a szintet, amikor a humán eredetű veszélyek nagymértékben csökkenthetők, mert a viselkedésalapú védelem, azaz amikor a felhasználó eddigi tevékenységétől eltérő viselkedését automatizáltan figyeli/ellenőrzi, nagy segítséget jelenthet majd.

Ami talán még érdekes lehet, hogy a hibrid hadviselés esetében a célok között jelenik meg a másik fél társadalmára való hatásgyakorlás, ahol értelemszerűen előtérbe fognak kerülni a nyílt infokommunikációs felületek, hiszen ezeket érik el a társadalom tagjai.

További radikális megoldást jelenthet még a teljes telefontilalom, amelyet az ukrán–orosz háborúban is bevezettek, azonban ez hosszú távon nem tartható cselekvési forma.

Összefoglaló gondolatok

Tisztázom azt az állítást, hogy a mai technológia és energiaellátás nélkül a fent felsorolt technológiák és eszközök nem is léteznének, és a megfelelő kommunikációs eszközök az alappillérei az elektronikus hírszerzésnek egyaránt.

A publikációban a katonaság és az OSINT összefonódását vettem alapul, és hogy ez a jelen időszakban is mennyire számottevő kérdéskör. Elsősorban a katonai ágazatok, majd a nemzetbiztonsági szolgálatok mentén kerestem az irányt, hiszen ők a fő mozgatórugói egy állam információszerzésének. Ezután érintettem a jelen időnk egyik fő konfliktusát, az orosz–ukrán háborút, reflektálva arra, hogy az OSINT mennyire befolyásolja a háború kimenetelét, és mennyire elterjed a híre az egész világon szinte másodpercről másodpercre; ezt nevezhetjük technológiai csodának is, ugyanakkor sokkal nagyobb technikai problémákkal és változó helyzetekkel kell szembenéznie a mai kor parancsnokainak. Ezért is szerettem volna interjút készíteni hazánk felső vezetőivel, akik tapasztalatukkal és hozzáértésükkel tudtak válaszolni a feltett kutatási kérdéseimre.

A hipotéziseket elemezve a következő megállapításokra jutottam: az orosz–ukrán háború kitűnő példa volt az 1. hipotézisem alátámasztására, hiszen ott is megnyilvánult, mennyire meg tud változni egy hadszíntér, ha nem kívánt információ kerül fel az internetre. Hasonlóképpen vélekedem a 2. hipotézisemmel kapcsolatban is, hiszen több olyan példát ismerhettünk meg mi is a közösségi médiából, amely alátámasztotta, hogy bizonyos csapatok úgy mértek csapást az ellenségre, hogy előtte a közösségi médiából tájékozódtak.

Irodalomjegyzék

Bányász Péter (2015): A közösségi média, mint a nyílt forrású információszerzés fontos területe. *Nemzetbiztonsági Szemle,* 3(2), 21–36. Online: http://uni-nke.hu/uploads/media_items/nbszemle-20152-banyasz.original.pdf

Dezső Lajos (2018): A nemzetbiztonsági szolgálatok. In Resperger István (szerk.): *Nemzetbiztonsági alapismeretek*. Budapest: Dialóg Campus, 95–109.

Dobák Imre (2018): Az információgyűjtésről általában. In Resperger István (szerk.): *A nemzetbiztonság elmélete a közszolgálatban.* Budapest: Dialóg Campus, 74–83.

Szabó Károly (2019): Az OSINT – Gondolatok a tevékenységről és az alkalmazás közegéről. *Nemzetbiztonsági Szemle*, 7(2), 68–82. Online: https://doi.org/10.32561/nsz.2019.2.6

Tóth András (2020): Information-Sharing Challenges and Issues in Multinational Operations, Part 1. *Revista Academiei Fortelor Terestre,* 25(4), 307–316. Online: https://doi.org/10.2478/raft-2020-0037

Tóth András (2021): Information-Sharing Challenges and Issues in Multinational Operations, Part 2. *Revista Academiei Fortelor Terestre,*26(1), 22–30. Online: https://doi.org/10.2478/raft-2021-0004

Vida Csaba (2013): Létezik-e még a hírszerzési ciklus? Miről szól a hírszerzés? *Felderítő Szemle,* 12(1), 43–57. Online: www.knbsz.gov.hu/hu/publikaciok.html#fsz2013-1

Vida Csaba (2018): Hírszerzés. In Resperger István (szerk.): *Nemzetbiztonsági alapismeretek*. Budapest: Dialóg Campus, 111–132.

Jogi forrás

2009. évi CLV. törvény a minősített adat védelméről