

Nándori Nikoletta Petra¹

HUMINT – Gondolatok az emberi tényező szerepéről a 21. századi titkosszolgálati munkában

*HUMINT – Thoughts on the Role of Human Factors
in the 21st Century in the Secret Service Work*

A titkosszolgálati munka egyik és egyben legrégebbi múlttal rendelkező ága az emberi erőforrásból történő információgyűjtés, elterjedt nevén a HUMINT. A gyakran humán hírszerzésként említett tevékenység széles körű alkalmazása a kormányzati szervek (nemzetbiztonsági szolgálatok) tevékenységének háttértámogatásában sajátos szerepet tölt be. Alkalmazásának számtalan lehetősége biztosított, amelynek jellemzőjeként, a számon tartott előnyei és hátrányai mellett, a mai napig igazolja tevékenységében, hogy a „titkosszolgálati munka” egyik nélkülözhetetlen ágát képviseli.

Kulcsszavak: HUMINT, emberi tényező, humán hírszerzés, információgyűjtés, nemzetbiztonság

One of the oldest branches of intelligence work, the collection of information from human resources, is commonly known as HUMINT. The widespread use of this activity often referred to as human intelligence, plays a special role in supporting the activities of government agencies (national security services). There are many possibilities for its application with all its advantages and disadvantages. To this day, it demonstrates in its operation that it represents an indispensable branch of ‘secret service work’.

Keywords: HUMINT, human factor, human intelligence, information gathering, national security

¹ Nándori Nikoletta Petra r. főhadnagy, doktorandusz, Nemzeti Közsolgálati Egyetem Rendészettudományi Doktori Iskola, ORCID: 0000-0002-3289-4649

Bevezetés

A titkos információgyűjtés legalapvetőbb és legrégebbi ágának gondolkörével foglalkozó tanulmány célja az emberi tényező 21. században betöltött szerepe igazolásának bemutatása. Mindamellet, hogy a titkos információgyűjtés alapvető lehetőségei között tartják számon, ugyanakkor a modern technika világában is betölti szerepét, annak el nem hanyagolható és sokszor ki nem váltható jelentőségével együtt. Az információgyűjtés technikai oldalának fejlődése sajátos módon a kibertérben is egyre több lehetőséget biztosít bizonyos humán jellegű tevékenységekre. Mindez elősegítheti, hogy a szükséges információ beszerzésére a legoptimálisabb technikát válasszák a feladatok maradéktalan teljesítése érdekében.

A HUMINT fogalmi meghatározása

A HUMINT (HUman INTelligence – emberi erőforrással folytatott hírszerzés) Kis-Benedek József meghatározása szerint: „[a] nemzetbiztonsági tevékenység azon eljárása, amelynek a középpontjában az ember áll, akinek ismeretét, képességét a nemzetbiztonsági szolgálatok tervszerűen és szervezett formában használják fel. A HUMINT erre a célra képzett adatszerzők tevékenysége, akik az információkat és az adatokat emberektől, az emberek által használt dokumentumokból és médiából szerzik a szemben álló erők szándékainak, erejének, képességeinek, eljárásainak, taktikájának megismerésére.”²

A HUMINT-kapacitással tehát a nemzetbiztonsági tevékenység során adatszerzést és információgyűjtést végeznek. Az így beszerzett adatok a kormányzati, gazdasági vagy akár a bűnfelderítési munkát végzők számára segíthetik elő a döntéshozatalt és ezáltal eredményességüket. Az emberi erővel folytatott „hírszerzés” klasszikus értelemben vett alkalmazhatóságából adódóan olyan közvetlen közlő vagy áttételek útján keletkező ismeretek felhasználásával és ellenőrzésével végzett felderítő tevékenységet tesz lehetővé, amelynek köszönhetően szélesebb körű információ-mennyiségre lehet szert tenni.

Alkalmazhatóságának sokszínű volta miatt a mai napig elhagyhatatlan és sok esetben megkerülhetetlennek tekinthető adat- és információgyűjtési módszer.

A titkos kapcsolat alkalmazása a HUMINT-tevékenységek fontos területe, ahol az egyik legfontosabb kérdés épp a kapcsolattartás módja, annak kiépítése és működtetése. A kapcsolatnak a megszerzett információt el kell juttatnia a szervezethez, minél pontosabban, lehetőség szerint időben és mindenekelőtt titokban. Mindehhez megfelelő kommunikációs csatornát kell üzemeltetni. A kapcsolattartás lehet személyes vagy személytelen. Az ellenérdekelt fél számára azonban éppen ez az a fajta kommunikációs csatorna, amely a leginkább támadható, ezért kell éppen ennek a védelmére kiemelt figyelmet fordítani.³ A kapcsolattartás formái az idők folyamán átalakuláson mentek keresztül, ahol a hagyományosnak tekinthető elemek mellett a technikai fejlődésnek köszönhetően ma már kellő körütekintés mellett alkalmazhatóak az akár

² KIS-BENEDEK 2014, 155–156.

³ KÁROLY et al. 2019, 5–6.

interneten alapuló, ennél fogva fizikai kontaktust nem igénylő, technikai szinten megvalósuló kapcsolattartási csatornák.

Az emberi erővel folytatott felderítés egy másik fogalmi meghatározása alapján, annak gyakorlati alkalmazhatóságát ismertetjük. Eszerint, magában foglalja mindazokat az ember által végzett adat- és információgyűjtési eljárásokat, amelyek az emberi érzékszervek vagy ember által közvetlenül kezelt műszerek felhasználásával válnak elvégezhetővé. Idesorolhatók ebben a tekintetben a figyelők és a felderítők által végzett tevékenységek is.⁴

A HUMINT és a TECHINT kapcsolata

A leggyakrabban alkalmazott, általánosan használt felosztás alapján, a titkosszolgálati tevékenységen belül a titkos információgyűjtést két nagy alapkategória mentén szokták felosztani, a humán típusú és a technikai típusú területekre (például HUMINT, TECHINT). A történelem során ezek alkalmazási formái és szerepük is jelentősen megváltozott és alkalmazkodott a kor felderítési igényeihez. A fenti alkalmazza Pomerleau 2017. évben a témában megjelent tanulmányát, amely a hírszerzés két fő kategóriájaként különbözteti meg a TECHINT- és a HUMINT-területeket. A hírszerző ügynökségek akkori protokollja szerint az emberi tényező szerepe a technológia segítségével beszerezhető információk tekintetében alulmaradt, amely következőképpen a csökkentett finanszírozásából is leszűrhető. A tanulmány kitér arra is, hogy a HUMINT nem nélkülözhető, még háttérbe sem szorul, hiszen az emberi tulajdonságokra építő információgyűjtési területekre mindig szükség lesz.⁵ Nem támaszkodik ugyanis a technikára és éppen ez az, ami egyben előnyként is jelenhet meg. Nehézséget jelenthet például, hogy a technikai információgyűjtés során felhalmozott hatalmas mennyiségű adathalmazokból a szükséges adatok kinyerése sok esetben hosszadalmas és bonyolult (például titkosított anyagok) feldolgozói és elemzői munka eredményessége révén valósulhat meg.⁶

A technikai információgyűjtés során tárolt adathalmaz lehetőséget biztosít feldolgozásának többoldalú elemzésére. Merülhetnek fel olyan információ- vagy adatigények, amelyek esetenként elsőre nem tűnnek relevánsnak, de a későbbiek folyamán azonban azzá válnak. A technikai úton szerzett információ ezáltal teszi lehetővé azt a fajta objektív adatgyűjtést, amely tárolhatóságából adódóan válik akár célirányosan visszakereshetővé. Ebben az objektivitásban is rejlik a technikai adatszerzés sajátja, amely az emberi erőforrással végzett információszerzésről nem minden esetben mondható el. Az emberi tulajdonságok révén a szubjektivitás teszi egyedivé még a HUMINT-tevékenységet, ami viszont a TECHINT esetében nem mondható el. Az emberi érzelmek révén továbbá olyan spontán döntéshozatalra képesek, amely a technikai eszközök esetében nem kivitelezhető.

⁴ FÜZESI 2004, 26.

⁵ POMERLEAU 2017.

⁶ POMERLEAU 2017.

Ami általánosságban leszögezhető, hogy az emberekkel szemben folytatott információgyűjtés elképzelhetetlen humán erőforrás nélkül, ahogyan a technikai hírszerzés sem képzelhető el a technikai eszközök nélkül.

A HUMINT, OSINT és a SOCMINT

Az emberi kapcsolatok és a közöttük fellépő interakciók alkotják azt a fajta szociális hálózatot, amely magát a társadalmat is működteti. Ez a fajta szociális hálózat az internet globális elterjedésének és a technikai vívmányok fejlődésének köszönhetően már nem csupán az emberek közötti fizikailag is kézzel fogható interakciók révén tud megvalósulni, hanem a kibertér világában is.

Az OSINT (Open Source Intelligence – nyílt hozzáférésű hírszerzés) fogalmi meghatározása szerint magában foglalja mindazokat a médiaforrásokat, közérdekű adatokat, szakértői és kutatási adatokat,⁷ amelyek külön engedély igénybevétele nélkül bárki számára hozzáférhetők. A titkosszolgálatok is figyelemmel kísérik a nyílt információs forrásokat, amely források például a sajtókiadványok, a tömegkommunikáció műsorai, nyílt adatbázisok – információs rendszerek és az internet. Az ebből a tevékenységből származó adathalmazból szakszerű elemzési technikával lehetséges kiszűrni a szükséges információkat.⁸

A közösségi hálózatok, a különböző és egyben népszerűnek is számító közösségi médiumok – úgy mint a Facebook, Twitter, Instagram és LinkedIn csak, hogy néhányat említsünk – messze bővelkednek a kibertársadalomban jelen lévő felhasználóktól, vagyis az állampolgároktól kinyerhető információkban. Az ezzel kapcsolatos információszerzéssel ellenben ma már a SOCMINT⁹ elnevezésű hírszerzési ág foglalkozik. A SOCMINT (Social Media Intelligence – közösségi médiában folytatott hírszerzés) fogalmi meghatározása Sir David Omand (GCHQ volt igazgatója; Egyesült Királyság) nevéhez köthető, amely szerint a SOCMINT döntő mértékben járulhat hozzá a közbiztonság eléréséhez: a bűncselekmények azonosításához, a rendellenességek és veszélyek korai előrejelzéséhez vagy a helyzet tudatosság felépítéséhez a gyorsan változó helyzetekben. A szociális média tartalmának megértése lehetőséget kínál az elhárító szolgálatok jobb megértésére és a felkérő szervek hírigényének kiszolgálására.¹⁰

Arról, hogy a SOCMINT a hírszerzési lehetőségek külön ágát képviseli vagy csupán módszerben/elnevezésében más, megoszlanak a vélemények.¹¹ Az általánosan elfogadott vélemény szerint az OSINT egyik ágaként van jelen a hírszerzési lehetőségek között, annak mint egyfajta elemzési és értékelési módszereként.¹² A közösségi médián keresztül beszerezhető információk döntő mértékben járulnak hozzá a közbiztonsághoz, a bűncselekmények azonosításához, a rendellenességek korai

⁷ CSIZNER 2019, 20.

⁸ GÁL 2014, 51.

⁹ OMAND–BARTLETT–MILLER 2012, 9.

¹⁰ www.protectiveintelligence-network.net/services-and-solutions/geo-fenced-social-media-intelligence-monitoring-and-analysis (A letöltés dátuma: 2020. 03. 15.)

¹¹ BÁNYÁSZ 2018, 116.

¹² OMAND–BARTLETT–MILLER 2012, 52.

felismeréséhez a gyorsan változó helyzetekben. A közösségi média alakítja a társadalmat, amiből kifolyólag egyre több információt osztunk meg a közösségi hálózatokon keresztül, létrehozva ezáltal a digitális társadalmat. A társadalom fejlődésével és a kommunikáció új módszereinek elfogadásával elengedhetetlen, hogy az állami testületek lépést tartsanak ezekkel a változásokkal.¹³ A kockázatfigyelés hasznos lehet a gazdasági és a társadalmi oldalról is.

A kibevilág adta anonimitás lehetőséget ad a profil mögött álló valódi személyazonosság részbeni vagy teljes megváltoztatására. Ezek a sokszor a realitástól messze távol álló adatok más képet mutatnak egy adott emberről. Az ilyen adatokból leszűrt információk pedig akár a valóságtól teljesen eltérő téves következtetések sorát eredményezhetik. De ez oda-vissza érvényes. Legalább annyira tévútra vihet a humán információgyűjtés korlátaiban vagy épp a szubjektivitásában rejlő anomáliák sora, mint a technikai információgyűjtés korlátaiból adódó információk értelmezésének sokoldalú volta. Talán épp ezért is válik jelentőssé a fúzió lehetőségeinek kiaknázása.

A HUMINT, TECHINT és a hálózatok

Az emberi társadalom által alkotott kapcsolati hálózat hasonlóképpen van jelen a technika világában is. Az emberi kapcsolatok hálózatot alkotnak, a világhálóhoz hasonlóan. Ha már hálózatról van szó, akkor kerül előtérbe a hálózat kutatás lehetősége ebben a témakörben is.

„A hálózat kutatás elsődleges választás lehet azokban az esetekben, amikor egy rendszer különböző szereplői, tényezői vagy éppen eseményei közötti összefüggéseket szeretnénk leírni jól mérhető adatok alapján, valamint abban az esetben is hasznos, amikor a kevésbé transzparens összefüggések feltárása a cél. A hálózatelemzés segítségével tehát lehetőség nyílik direkt és indirekt, látható és »láthatatlan« összefüggések feltárására nagy mennyiségű, strukturálatlan adat esetén is.”¹⁴

Ezáltal is tovább lehetne fejleszteni a humán és a technikai információgyűjtést, továbbá a közöttük fennálló és nélkülözhetetlen kapcsolatot. A technikai eszközök fejlődése és az emberi erőforrások közötti kapcsolat a hálózat kutatás szempontjából történő elemzése továbbmélyítheti és ezáltal is hatékonyabbá teheti a munkavégzést a nemzetbiztonsági szolgálatok számára.

A humán információgyűjtés sikerességének kulcsa a kapcsolatteremtésben és a hírszerző tevékenységével összefüggésben kialakított és fenntartott kapcsolati hálózatának működtetésében rejlik. Ami mindehhez még kapcsolódik a technikai információgyűjtéssel és a hálózatokkal az pedig az, hogy a digitális világban a kapcsolattartás számos formája ismert. A Tsai-Ching Lu, David L. Allen és Hankyu Moon feltalálók szabadalma¹⁵ a humán hírszerzés elemzésének támogatására készült. Az eszerint bemutatott rendszer észleli a felhasználók közötti, a dinamikus információ hálózaton belüli társadalmi kapcsolatok változásait, és több integrált modulon

¹³ OMAND–BARTLETT–MILLER 2012, 9.

¹⁴ SZÓCSKA et.al. 2019, 10.

¹⁵ LU–ALLEN–MOON 2016.

keresztül teszi lehetővé a dinamikus információs hálózat jelenlegi társadalmi helyzetének megértését.¹⁶

A digitális rendszerből és a humán hírszerzésből származó információk együttes elemzése teheti még hatékonyabbá a hírszerzés két ágának sajátosságaiból eredő esetleges anomáliák kiküszöbölését is.

Az emberi tényező létjogosultsága a 21. században

Bár a technika fejlődésével az információgyűjtő tevékenység egyre szélesebb körben tudja lehetőségeit bővíteni, a klasszikus értelemben vett emberi erőforrásból érkező információk továbbra is nélkülözhetetlenek. Azzal, hogy az emberi interakciók jelentős mértékben a kibertérbe tevődnek át, a globalizációs társadalom online világában tömegesen váltak elérhetővé az emberek által hátrahagyott információk digitális halmazai, amelyek az emberi viselkedés mintegy lábnyomaként értelmezhetők a virtuális térben.

A digitális lábnyom, a világháló használata során jön létre. Magában foglalja a felkeresett weboldalakat, e-maileket és az online szolgáltatásokhoz kapcsolódó adatokat. Fajtáját tekintve kétféleképpen válik megközelíthetővé, az egyik a „passzív digitális lábnyom”, amely olyan adat és nyomvonal, amelyet akaratlanul hagy maga után az interneten a felhasználó. Például az, amikor ellátogat egy weboldalra és a web-szerver naplózza az IP-címet, amely azonosítja az internetszolgáltatót és a hozzáférés helyét. A másik fajtája pedig az „aktív digitális lábnyom”, amely magában foglalja azokat az adatokat, amelyeket szándékosan továbbít a felhasználó az interneten. Az e-mail küldése például hozzájárul az „aktív digitális lábnyomhoz”, ugyanis a szolgáltatás igénybevételéhez személyesen vár el adatokat a felhasználótól, amelyet az végül megad.¹⁷ Mint a nemzetközi példák mutatják, ezen adatok a nemzetbiztonsági szolgálatok számára is fontossá válhatnak, amelyek megszerzése gyakran a technikai területeken túlmutató humán képességeket is igényel. Ezért fontos lépést tartani a technika fejlődésével és ötvözni a HUMINT és a TECHINT egymást kiegészítő lehetőségeit. A két ág véleményem szerint egy egymásra épülő és egymást segítő hírszerzési módszert tesz lehetővé, a hatékonyság maximalizálása érdekében.

Erre az álláspontra helyezkedik több olyan publikáció is, amely a témában íródott. A fejlett országokban a HUMINT és a TECHINT összehangolására koncentrálnak, amely olyan jövőbeli problémákat vet fel, ami sokkal bonyolultabbá és kihívásokkal telivé fogja tenni a nemzetbiztonsági szolgálatok munkáját.¹⁸

A HUMINT/TECHINT együttműködésre általános példaként a drónhasználatot említik. A klasszikus értelemben vett emberi erővel folytatott hírszerzés számára a technikai újítások új kihívást jelentenek. Példaként említhető, hogy a számítógépes korszakban a HUMINT még komplexebbé válik, és az információgyűjtő tevékenységet végző embereknek meg kell érteniük a technológia jelentőségének szerepét

¹⁶ LU–ALLEN–MOON 2016.

¹⁷ *Digital Footprint* 2014.

¹⁸ CROSTON–VALLI 2017, 68–69.

a műveletekben, hiszen az információgyűjtés gyorsabban fejlődik mint korábban bármikor.¹⁹ Ezekhez az új kihívásokhoz természetesen a képzést is alakítani és fejlesztetni szükséges.

Itt kerülhet előtérbe a kritikai jövőkutatás, amely a jelenben létező jövőt, az emberi előrelátást, vagyis a foresightot helyezi kutatása középpontjába. A minden embernél működő evolúciós adottság egyben képesség is. Az emberi előrelátás az ember teljes mentális kapacitásával foglalkozik. Mindemellett a jövővel és a jövőre irányuló racionális gondolkodása mellett az érzelmekben, hitben és hiedelmekben is testet ölt egyúttal. A feladata egyrészt a közösségi jövőelképzelések kritikai szemléletmódjának képviselése, másrészt pedig olyan eljárások fejlesztése, amelyek segítségével bekapcsolódhat a közösségi szintű jövőelképzelések alakításába. A kritikai jövőkutató ezzel a munkájával nem előrejelzéseket készít, hanem foresight-készítési eljárást szervez és segít.²⁰ A humán hírszerzés nemcsak a fizikai kontaktus révén megvalósuló emberi kapcsolatok hálózatában tud megvalósulni, hanem a gondolatok és az érzelmek szintjén is, amire a technika nem képes. Szintetizálni kell a megszerzett ismereteket, megnézni, hogy melyek azok, amelyeknek dominálniuk kell. Fel kell építeni a megfelelő taktikát a meggyőzésre, néha hallgatni kell megérzéseinkre is.²¹

A foresight-eljárás alapjait a technikai fejlődés és annak társadalmi hatásaival foglalkozó lehetséges jövőképek és modellek jelentették.²² Az információgyűjtés technikai és emberi ágának tudományos összehangolására van szükség, vagyis a hagyományos emberi hírszerzésbe kell beépíteni a modern technikai lehetőségeket.

Az innovációs technológiai újítások teret engednek a nemzetbiztonság területén történő és hasznosítható elemeknek. Ezeket a technikai újításokat nagyszerűen lehet kombinálni az emberi erőforrás lehetőségeinek maximalizálásával. Legyen szó a humán forrásból érkező információk szerepének ellenőrzéséről, megerősítéséről vagy háttértámogatásáról. Általános tendencia, hogy amint a HUMINT és a TECHINT közötti kapcsolat egymást kiegészítve tud együttműködni, akkor új szintekre tudja hozni a nemzetbiztonsági szolgálatok munkáját.

Összegzés

A humán jellegű információgyűjtés véleményem szerint a jövőben is vitathatatlanul nélkülözhetetlen, és fontos tényezője marad a nemzetbiztonsági szolgálatok titkos információgyűjtő tevékenységének. Az emberi erőforrásból beszerezhető információk a technikai fejlődés ellenére továbbra is nagy jelentőséggel bírnak. Az említett példákon túlmenően megszámlálhatatlan azon információtípusok és források tárháza, amelyek a modern technikai újításoknak köszönhetően elérhetők, vagy sajátos megoldásokat, eljárásokat használva hozzáférhetővé válhatnak a műveleti területen dolgozók számára.

¹⁹ GIOE 2017, 227.

²⁰ HIDEG 2012, 12.

²¹ KÁROLY et.al. 2019, 24.

²² DRUSZA 2019, 213.

A nemzetbiztonsági érdek hatékonyságának érvényesülése a HUMINT és a TECHINT innovatív ötvözésében rejlik. A két fő erőforrás lehetőségei és az azok közötti kapcsolati pontok eredményes használatának valóban csak a kreativitás szabhat határt. Ehhez a szervezeti kultúra megújulására és rugalmassá tételére van szükség, mindemellett a humán erőforrás kapacitásbővítésére is nagyobb hangsúlyt kell fektetni mint valaha. A technológiai újításokkal lépést kell tartani ahhoz, hogy a nemzetbiztonságért felelős szervezetek képessége fejlődhessen, vagy ami még jobb, két lépéssel megelőzze a másik felet.

Alkalmazott rövidítések

- GCHQ Government Communications Headquarters – Kormányzati Kommunikációs Központ
- HUMINT Human Intelligence – Emberi erőforrással folytatott hírszerzés
- OSINT Open Source Intelligence – Nyílt forráskódú hírszerzés
- SOCMINT/SMI Social Media Intelligence – Közösségi médiában folytatott hírszerzés
- TECHINT Technical Intelligence – Technológiai hírszerzés

Felhasznált irodalom

- BÁNYÁSZ Péter (2018): *A közösségi média térnyerése a védelmi szférában*. Doktori értekezés. Budapest, Nemzeti Közsolgálati Egyetem. Elérhető: https://hhk.uni-nke.hu/document/hhk-uni-nke-hu/BP_PhD_%C3%A9rtekez%C3%A9s%20-tervezet_20180508.pdf (A letöltés dátuma: 2020. 03. 15.)
- CROSTON, Matthew – VALLI, Frank (2017): *An Intelligence Civil War: „HUMINT” vs. „TECHINT”*. *Cyber, Intelligence, and Security*, Vol. 1, No. 1. 67–82. Elérhető: <https://www.inss.org.il/publication/intelligence-civil-war-humint-vs-techint/> (A letöltés dátuma: 2020. 03. 13.)
- CSIZNER Zoltán (2019): *Az OSINT határai*. *Nemzetbiztonsági Szemle*, 7. évf. 2. sz. 19–31. DOI: <https://doi.org/10.32561/nsz.201a9.2.2>
- DRUSZA Tamás (2019): *Jövőbeni kihívások a (polgári) nemzetbiztonsági elhárítás területén*. In DRUSZA Tamás szerk.: *A magyar elhárítás fejlődése*. Budapest, Dialóg Campus Kiadó.
- FÜZESI Ottó (2004): *A felderítés elméleti és gyakorlati kérdéseinek vizsgálata, különös tekintettel, az emberi erővel folytatott felderítésre*. Doktori értekezés. Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem Hadtudományi Kar, Művelési támogató tanszék. Elérhető: <https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/11979/ertekezés.pdf?sequence=1> (A letöltés dátuma: 2020. 04. 26.)
- GÁL István László (2014): *Az OSINT (Open Source Intelligence) mint a kémkedés lehetséges elkövetési magatartása*. *JURA*, 20. évf. 1. sz. 51–55.

- GIOE, David V. (2017): *'The More Things Change': HUMINT in the Cyber Age*. The Palgrave Handbook of Security, Risk and Intelligence. London, Palgrave Macmillan. DOI: https://doi.org/10.1057/978-1-137-53675-4_12
- HIDEG Éva (2012): Az interaktív jövőkutatás elmélete és módszertana. In HIDEG Éva – NOVÁKY E. szerk.: *Jövőkutatás – interaktívan*. Budapest, Aula Kiadó. 9–35.
- KÁROLY László – DRUSZA Tamás – REGÉNYI Kund – LAUFER Balázs (2019): *Információszerezés kapcsolati forrásai*. Budapest, Nemzeti Közszerzői Egyetem.
- KIS-BENEDEK József (2014): Az emberi erővel folytatott hírszerzés. In DOBÁK Imre szerk.: *A nemzetbiztonság általános elmélete*. Budapest, Nemzeti Közszerzői Egyetem. 153–162. Elérhető: <http://m.ludita.uni-nke.hu/repozitorium/bitstream/handle/11410/8567/Teljes%20sz%C3%B6veg%21?sequence=1&isAllowed=y> (A letöltés dátuma: 2020. 03. 25.)
- LU, Tsai-Ching – ALLEN, David L. – MOON, Hankyu (2016): *System and method of computational social network development environment for human intelligence*. Elérhető: <https://patents.google.com/patent/US9317567B1/en> (A letöltés dátuma: 2020. 04. 28.)
- OMAND, Sir David – BARTLETT, Jamie – MILLER, Carl (2012): *"A balance between security and privacy online must be struck..."* London, Demos. Elérhető: www.demos.co.uk/files/_Intelligence_-_web.pdf?1335197327 (A letöltés dátuma: 2020. 03. 15.)
- SZÓCSKA Miklós – JOÓ Tamás – GÁL András Levente – LŐRINCZ Orsolya – AUER Ádám – PALICZ Tamás (2019): A hálózatok kutatás alkalmazhatósága a közszolgáltatások fejlesztésében. In AUER Ádám – JOÓ Tamás szerk.: *Hálózatok a közszolgáltatásban*. Budapest, Dialóg Campus Kiadó. 9–26. Elérhető: https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/14555/712_Halozatok_a_kozszolgalatban_WEB.pdf?sequence=1 (A letöltés dátuma: 2020. 04. 26.)

Internetes források

- Digital Footprint* (2014). Elérhető: https://techterms.com/definition/digital_footprint (A letöltés dátuma: 2020. 03. 17.)
- Geo-fenced Social Media Intelligence Monitoring & Analysis*. Elérhető: www.protectiveintelligencenetwork.net/services-and-solutions/geo-fenced-social-media-intelligence-monitoring-and-analysis (A letöltés dátuma: 2020. 03. 15.)
- POMERLEAU, Mark (2017): Is technology a threat to human intelligence? Elérhető: www.c4isrnet.com/intel-geoint/2017/08/25/is-technology-a-threat-to-human-intelligence/ (A letöltés dátuma: 2020. 03. 15.)