DOI: 10.38146/BSZ.2021.2.2

Dobák Imre – Tóth Tamás

Régi módszerek a kibertérben? (CYBER-HUMINT, OSINT, SOCMINT, Social Engineering)

Old Methods in The Cyberspace? (CYBER-HUMINT, OSINT, SOCMINT, Social Engineering)

Absztrakt

A tanulmány a hagyományos HUMINT (emberi erőforrásokra épülő információgyűjtés) kibertérben való megjelenését, kategóriahatárait vizsgálja, amely napjainkban dinamikusan fejlődő terület. A CYBER-HUMINT kérdésköre az elmúlt tíz évben jelent meg, fogalmi kategóriája pontosan még nem körülhatárolt. Nemzetközi szakirodalma is viszonylag szűkösnek tekinthető, hasonlóan a közösségi oldalakat felhasználó információgyűjtő módszer (SOCMINT) kérdésköréhez. Azonban forrásokban rendkívül gazdag az általánosan elterjedt nyílt forrású információgyűjtés (OSINT), illetve a kiberbiztonság kapcsán egyre inkább előtérbe kerülő Social Engineering jelensége, amelyek metodikái határai gyakran átfedéseket mutatnak a kibertérben végzett, emberi erőforrásokra épülő információgyűjtéssel. A publikáció célja az egyre inkább összefonódó információgyűjtő területek áttekintése, kísérletet téve az elhatárolást elősegítő szempontrendszer előkészítésére.

Kulcsszavak: nemzetbiztonság, HUMINT, CYBER-HUMINT, kibertér, információgyűjtés

Abstract

This study examines the emergence and category boundaries of the traditional HUMINT in the cyberspace, which is a dynamically developing field nowadays. The issue of CYBER-HUMINT has appeared in the last ten years, and

its conceptual category hasn't been still fixed with exact boundaries. Its international literature can be regarded as relatively scarce, similar to the issue of the method of gathering information using social networking sites (SOCMINT). However, there is an abundance of literature on open source information gathering (OSINT) and the phenomenon of social engineering (SE), whose methodological boundaries often overlap with HUMINT in the cyberspace. The aim of the publication is to review the increasingly intertwined areas of information gathering, making an attempt to prepare a system of criteria that promotes demarcation.

Keywords: national security, HUMINT, CYBER-HUMINT, cyberspace, collection of information

Bevezetés

Napjainkban a nyilvánosság széles köre számára is ismert lehet a titkosszolgálatok információgyűjtése során alkalmazott, számos hagyományosnak tekinthető módszer, eljárás. Mind a jogszabályok és a témakörben fellelhető hazai, valamint nemzetközi szakirodalmak, mind a médiában megjelenő források ismerté tették az elmúlt évszázadban még homályba burkolódzó sajátos módszereket. Legyenek ezek akár a technikai megoldásokkal történő információgyűjtés módszerei, vagy az emberi kapcsolatokhoz, erőforrásokhoz köthető különböző megoldások. Amíg az információszerzés gyakorlata a múlt század kezdetén egyértelműen a humán képességek meghatározó súlyát jelezte, addig a technikai eszközök fejlődésével a HUMINT (Human Intelligence – emberi erővel/forrásból történő információgyűjtés) alkalmazásának az információszerzés területein betöltött aránya folyamatosan csökkent. Az internet térhódítása szintén a humán eszközök visszaszorulását eredményezte, hiszen teret nyertek a korszerű, a közvetlen fizikai-emberi kapcsolatot nélkülöző, technikai úton végrehajtható eljárások. Kérdés azonban, hogy az itt megjelenő számos módszer valóban újnak tekinthető-e vagy csak a régi módszerek kibertérben történő megjelenésének lehetünk tanúi. Fialka György általános megfogalmazását idézve napjainkban *„nem új módszerekről beszélünk, hiszen a megfigyelés, információszerzés tevékenysége ősi, e felderítő szakmának már rég meglevő eleme. Változást a tevékenységet támogató eszközök fejlődése által nyújtott lehetőségek adják, melyek dinamikus fejlődése az emberi tevékenységi részét és az információk megszerzési idejét jelentősen csökkentik."* (Fialka, 2018, 189.).

HUMINT a kibertérben – CYBER-HUMINT

Jelen tanulmány a HUMINT tevékenységének kibertérben való megjelenésére helyezi a hangsúlyt, amely tevékenységhez – a NATO (North Atlantic Treaty Organisation, Észak-atlanti Szerződés Szervezete) szakterminológiája alapján – azon információgyűjtő módszerek és eszközök összessége sorolható, melyek során az információk emberi erőforrás által kerülnek beszerzésre és elsősorban humán forrásokból származnak (NATO, 2019, 63–64.). Ennek kapcsán elvi kérdésként merül fel, hogy napjainkban a humán és a technikai információgyűjtési területek sajátos közeledéséről vagy teljesen új területek fejlődéséről beszélhetünk a kibertérben. A háttérben azt láthatjuk, hogy a nemzetbiztonsági szervezeti struktúrákban hagyományosan a technikai és humán területek egymástól való elkülönülése dominál, továbbá a költségvetési források túlnyomó többsége is a technikai információszerző tevékenységekhez kapcsolódik. Példaként az Amerikai Egyesült Államok (USA) egyes ASI [All Source Intelligence – összadatforrású információgyűjtés: az adat- és információgyűjtés (HUMINT, SIGINT, IMINT stb.), feldolgozás, elemzés-értékelés egyes eszközeinek és módszereinek összessége] képességeinek szervezeti elkülönítése hozható, akár a HUMINT és a globális SIGINT [Signal Intelligence – rádióelektronikai (jel) információgyűjtés: azon információgyűjtő módszerek és eszközök összessége, melyek az ellenérdekelt fél kommunikációs és nem kommunikációs kisugárzó eszközeinek észleléséből szolgáltatnak adatokat és információkat] tevékenység vonatkozásában. A domináns SIGINT eszközök mellett egyre nagyobb teret nyer a szintén technikai IMINT (Imagery Intelligence – képi felderítés) képesség, a képi felderítéshez kapcsolódó műholdak vagy az UAV-k (Unmanned Aerial Vehicle – pilóta nélküli jármű) rendkívül elterjedt alkalmazásának köszönhetően (Johnson, 2010, 17.).

Látható azonban egy másik folyamat is, amely a humán jellegű információgyűjtési megoldások digitális világhoz való igazodását jelzik, és amelyek vizsgálata kapcsán kiinduló elemként tekinthetünk a HUMINT tevékenység alábbi hagyományos jellemzőire, előnyeire, hátrányaira:

- A HUMINT alkalmazása során lehetővé válik a technikai eszközökkel nem megismerhető törekvések, mélységi információk konspirált felfedése, amelyben kiemelt szerepet kaphat a közvetlen emberi kommunikáció és észlelés, valamint akár az azonnali döntéshozatal lehetősége.
- A tevékenység működtetésének költségei a technikai módszerekhez viszonyítva alacsonyabbnak tekinthetők.
- Jelen van a szubjektivitás, valamint a humán jellegű kapcsolatok kiépítésének időigényessége, mely akár hosszas előkészítést, szakmai előrelátást

igényelhet a releváns információkhoz való hozzáférés időben elhúzódó megvalósításáig.

- Alkalmazásának lehetőségei közvetlenül kapcsolódnak a humán források rendelkezésre állásához és megbízhatóságához, amelyek hiánya a területen képességvesztéshez és dezinformálódáshoz vezethet, azaz megszűnik az érdemi, valós és ellenőrzött információkhoz való hozzáférés lehetősége.
- Előfordulhat, hogy az információgyűjtéssel érintett személyek köre a technikai és infokommunikációs eszközök alkalmazását illegális tevékenységeik (például terrorizmus) során szándékosan minimalizálják, elkerülik, így ellehetetlenítve a technikai módszerek alkalmazásának eredményességét.
- A HUMINT irányai (például hírszerzés, elhárítás, terrorelhárítás, bűnüldözés) ugyanakkor rendkívül sokoldalúak lehetnek, annak ellenére, hogy módszereik számos elemében azonos eljárásokat és elveket tükröznek vissza.

Egyes nyugati szakirodalmi forrásokban a jövőre kitekintve annak elvi kérdését is felvetik, hogy érdemes-e adott esetekben a HUMINT műveletek során az állományt közvetlen veszélynek kitenni, ha az adott információ megszerezhető technikai úton, például UAV alkalmazásával (Crosston & Valli, 2017). Más források ezzel szemben a két terület közeledésének sajátosságaira hívják fel a figyelmet, amely bizonyos ismeretek, képességek közös kialakításának szükségességét vetítik előre, különösen a technikai ismereteket igénylő, humán jellegű információgyűjtési területek vonatkozásában (Károly et al., 2019, 60–61.). A két hagyományos információgyűjtési ág egymáshoz való viszonyát még összetettebbé teszi, hogy napjainkban már számos információ alapvetően nyílt, technikai jellegű forrásban áll rendelkezésre – melyek OSINT (Open-Source Intelligence – nyíltforrású információgyűjtés)[1] útján is beszerezhetők –, illetve az emberi kapcsolatokat előtérbe helyező közösségi oldalakon is hozzáférhetők – akár az úgynevezett SOCMINT (Social Media Intelligence – közösségi médiából történő információgyűjtés)[2] során. Ezen információk elérése azonban a technikai ismeretek mellett egy napjainkban divatos terület, a humán információgyűjtés sajátosságaihoz sorolható – úgynevezett Social Engineering[3] (a továbbiakban: SE) – módszereit is igényelhetik.

1 Azon információgyűjtő módszerek és eszközök összessége, melyek forrásai a nyilvánosság számára is elérhető, nem titkosított olyan információk, amelyek hozzáférése vagy terjesztése korlátozott (NATO, 2019)

2 Azon információgyűjtő eszközök és módszerek összessége, melyek forrása a közösségi média, az egyes felhasználók közösségi médiában folytatott tevékenységéhez kapcsolódó adatok (Omand, Bartlett & Miller, 2012).

3 Social Engineering: információszerzés céljából, az ellenérdekelt humánerő technikai eszközök felhasználásával vagy azok alkalmazása nélkül végrehajtott manipulálása, az érdekelt fél információigényének kielégítése érdekében (Tóth, 2019, 46.).

A humán információgyűjtési területek jelentősége az elmúlt évekre visszatekintve két szempontból mindenképpen alátámasztottnak tűnik.

- Egyrészről a különböző kockázatok, kihívások és fenyegetések a társadalom olyan tagjainak irányából érkeztek, akik kiszűrése, valamint a biztonságot negatívan befolyásoló folyamatok észlelése és azonosítása csak rendkívül korlátozottan volt lehetséges a hagyományos technikai információgyűjtő eszközökkel. Gondoljunk csak a korábbi évek Nyugat-Európában elkövetett terrorcselekményeire, vagy akár az illegális migráció köré szerveződő embercsempész hálózatok működésére.
- Másrészről a technikai-felderítési lehetőségek alkalmazásának hatékonysága egyes esetekben mérsékeltnek tekinthető. A célszemélyek nem használják hagyományos infokommunikációs eszközeiket jogellenes tevékenységükkel kapcsolatos közlésekre, illetve kerülik az érzékeny információk hagyományos hírközlő hálózaton történő továbbítását. Így a hírközlő hálózatból esetlegesen kinyert információk nem hozhatók összefüggésbe az ellenőrzés alapjául szolgáló normasértő tevékenységgel. A mára már általánosan elérhető titkosítási protokollok, melyek jelentőségére az elmúlt évtized európai terrorcselekményei szintén felhívták a figyelmet, ugyancsak tovább nehezíthetik az információgyűjtéssel érintett célszemélyek kommunikációjának felderítésére és ellenőrzésére szakosodott szervezetek munkáját. A terrorizmus diverzifikációja, hálózatosodása okozta kihívás egy igen egzakt példa a technikai információgyűjtés nehézségeire, valamint a humán alapú képességek újbóli felértékelődésére. Példaként az izraeli Nemzetközi Terrorelhárítási Intézet[4] kutatási igazgatójának, Dr. Eitan Azani beszámolója említhető, amely alapján az Iszlám Állam terrorszervezet vonatkozásában a toborzás, a háttértámogatás, a pénzügyi finanszírozás, valamint maga a műveleti tevékenység is hálózatépítő folyamatokon, kapcsolati hálókon alapult (Azani, 2018.). A zárt, főleg titkosított protokollokkal ellátott internetes kommunikációs csatornákat alkalmazó terrorista sejtek, decentralizált hálózatok kommunikációja pedig gyakran csak korlátozottan ellenőrizhető technikai úton. Az e csoportokba történő humán forrás létesítése nélkül, a belső érdemi információk csak rendkívül korlátozottan hozzáférhetők a biztonsági szervek számára.

Nem hagyható figyelmen kívül továbbá az sem, hogy a humán műveleti ismeretek és erőforrás a technikai területeken sem nélkülözhető, hiszen ezen tevékenységek nagy részének is van emberi vonatkozása, ahol a feladat

4 International Institute for Counter-Terrorism (ICT), Izrael.

meghatározása, engedélyezése, az információk értelmezése, értékelése már magához az emberi erőforráshoz kapcsolódik. Emellett a technikai úton beszerzett információk is valamely emberi tevékenységhez kapcsolódhatnak. Például egy adott hírközlő hálózaton folytatott kommunikáció során, az emberi tevékenység (például kommunikáló felek beazonosítása, közleménye) és a technikai adatok (például helyadatok, eszközazonosítók) együttesen alkotnak releváns információt. A technikai és humán információgyűjtő módszerek viszonyát tekintve a jövőben egyfajta integrált alkalmazás válhat előremutatóvá, ahol a technikai megoldások hangsúlyos szerepet kaphatnak a HUMINT támogatásában. Ezek között kell kiemelni a társadalomban általánosan használt olyan elektronikus infokommunikációs lehetőségeket, különösen a kibertérben az internettechnológiára épülő OTT[5] szolgáltatásokat, amelyek segítségével a korábban csak nehezen megszerezhető információkat ma már rövid időn belül tömegesen elérhetjük. Az internettechnológiára épülő OTT szolgáltatások mindenki számára könnyen hozzáférhetők a meglévő infokommunikációs eszközökkel, csekély számítástechnikai tudással is használhatók, legtöbbször ingyenesen igénybe vehetők (Kovács, 2015, 136.). Ugyanígy napjainkban a hagyományos HUMINT-hoz szükséges kapcsolattartási tevékenység során is alkalmazásra kerülhetnek az információtovábbítás biztonságosnak vélt technikai megoldásai. John Sano írásában felhívja a figyelmet arra, hogy amellett, hogy számtalan pozitívuma van annak, hogy a hagyományos HUMINT tevékenység egyre inkább támaszkodik a technikai képességekre, ugyanakkor komoly negatívumokkal is számolni kell (Sano, 2015). Igaz, a technológia növelheti a hatékonyságot és a gyorsaságot, például az információk továbbításban, de ugyanakkor sérülékenységeket is okozhat. Gondoljunk csak a technikai úton továbbított üzenetek metaadataira, nyomaira, követhetőségére, melyek kiküszöbölésére Osama Bin Laden általánosan ismert technikai eszközhasználatot kerülő kommunikációs megoldásai állíthatók példaként. Az emberi tevékenységek virtuális térben történő megjelenésével, az internet és különösen a közösségi oldalak térhódításával fontossá váltak a HUMINT ismereteit sem nélkülöző, a kibertérre épülő OSINT egyes elemei is, a közösségi oldalak kapcsán megjelenő SOCMINT, vagy akár a nagyon divatos területeként fejlődő Social Engineering módszerei. Mindezek már a virtuális világ folyamataihoz kapcsolódnak, amelyek azonban nem választhatók el a fizikai dimenzió eseményeitől, és a két térben megjelenő információk

5 Over the Top: Egy olyan alkalmazás vagy szolgáltatás, amely lehetővé teszi egy infokommunikációs termék elérését az interneten keresztül, kikerülve a hagyományos terjesztést. Ilyenek lehetnek például a kommunikációs szolgáltatások, mint a Skype, Gmail, az egyéb alkalmazásszolgáltatások, mint a Facebook, LinkedIn, Twitter.

szükségszerűen kiegészítik egymást. Például azáltal, hogy a közösségi oldalakon egy fényképet teszünk közzé magunkról, akkor a virtuális térben megjelenő adatokat a valós, fizikai térben játszódó eseményhez, helyszínhez kapcsoljuk. A globális biztonságpolitikai színterére kitekintve – gondoljunk csak az arab tavasz eseményeire –, a biztonságot fenyegető, veszélyeztető események, megmozdulások nagy része a közösségi oldalakon szerveződött, de megemlíthetők akár az illegális migrációs útvonalakat formáló bejegyzések is. Az ezekhez hasonló tevékenységek már a virtuális-, kibertér befolyásolási célú felhasználását jelenthetik, egy a valós térben játszódó eseményre való hatásgyakorlás érdekében. Az ilyen törekvések megjelenésének, szándékos alkalmazásának észlelése és nyomonkövetése a biztonsági szervezetek számára is fontos, ahol a valós térben játszódó HUMINT és a virtuális térben végrehajtott digitális formában megjelenő HUMINT tevékenység értelemszerűen kiegészíthetik egymást, fokozva az információgyűjtés teljeskörűségét és hatékonyságát. A virtuális és a valós világban való megjelenés ugyanakkor ellentmondásokat is hordozhat magában, hiszen a felhasználók gyakran nem valós információkat osztanak meg magukról a kibertérben, például szándékosan fiktív adatokkal regisztrálnak a különböző alkalmazásokban. Ennek egy része mögött érthető módon saját személyes adataik védelme állhat, azonban a valótlan adatokból célirányosan felépített nacionálék, életvezetési legendák mások szándékos megtévesztésére, és bűnös tevékenység során az elkövetők személyazonosságának leplezésére is szolgálhatnak.

Az OSINT szempontrendszere

Az információs robbanás, a vele párhuzamosan bekövetkezett információs technológiai forradalom, valamint az internet gyors elterjedése magával hozta az OSINT, azaz a nyílt forrásból származó információszerzés eljárásainak és rendszerének folyamatos változását (Szabó, 2019, 69.). Napjainkban számos hazai és külföldi szakirodalom foglalkozik az OSINT témakörével, rávilágítva, hogy a nyílt információgyűjtés sajátos megoldásai lényegében mindenki számára rendelkezésre állhatnak, ugyanakkor az információk nyílt, profeszszionalizált megszerzése és felhasználása az állami, gazdasági, vagy akár a mindennapi életünket meghatározó döntések fontos elemeivé is váltak. Az elmúlt évek folyamatait tekintve jól látható, hogy a katonai és rendvédelmi jellegű hasznosulás mellett számos más alkalmazási területen is saját információgyűjtő jellegű képességeket alakítottak ki, amelyek között a nemzetközi

szervezetek, az NGO[6]-k, a gazdasági élet szereplői vagy akár az egyes terrorszervezetek, mint például az Iszlám Állam is megtalálhatók (Solti, 2019, 4.). Ugyanitt érdemes hangsúlyozni, hogy a tevékenység nem pusztán adott információk nyílt elérését jelenti, hanem annál sokkal szélesebb körben (például adatok célirányos gyűjtése, elemzése, felhasználása) értelmezendő. Az OSINT során egyfajta alaptételként jelenik meg, hogy – a HUMINT területtel szemben – csak nyílt forrásokból elérhető információk szerezhetők meg. A források közé sorolhatók például a közösségi oldalakon nyíltan megosztott, az egyes felhasználókhoz és a velük kapcsolatba hozható személyekhez kötött információk is, felvetve azonban számos etikai és jogi kérdéskört is. Egy másik jelentős etikai és normatív kérdés az interneten nyíltan elérhető adatok tömeges jellegű megszerzésével és felhasználásával kapcsolatban jelenik meg, felhívva a figyelmet a mesterséges intelligenciát felhasználó keresőmotorok, algoritmusok, elemző-értékelő szoftverek alkalmazására. A nyílt forrásból történő információgyűjtés természetesen nem újkeletű (Regényi, 2019, 33.), azonban a rohamosan fejlődő infokommunikációs megoldások robbanásszerű változást eredményeztek annak jelentőségében. Egyfelől fejlődtek az információk megszerzésének és feldolgozásának platformjai, ezzel párhuzamosan pedig változtak azok a nyíltan hozzáférhető információs közegek is, amelyek az OSINT számára alapvető forrásokat jelentenek. (Az OSINT értelemszerűen túlmutat a hagyományos internetes keresőmotorokon és -eljárásokon, hiszen a kibertérben egy-egy információmegosztásra szolgáló új felület, szolgáltatás új OSINT eljárásokat is felszínre hozhat.) Értelemszerűen felmerül a kérdés, hogy pontosan hol is húzódhat az OSINT határa? Az OSINT kereteinek tisztázása során a források nyílt hozzáférhetőségét kell-e figyelembe venni, vagy azon módszerek sorolhatók ide, amelyek habár széles körben elérhetők, azonban mégis speciális ismereteket igényelnek. Az sem feltétlen biztos, hogy annak végrehajtója számára minden, az interneten megtalálható adat és a hozzáférés módja etikusnak, esetenként jogszerűnek tekinthető (gondoljunk csak egy adott internetes oldalon elérhető, jogszerűtlenül megszerzett és megosztott jelszavak megismerésére és felhasználására) (Bardóczi, 2018). Mindez már az OSINT-on túl, akár a hacker tevékenység irányába mutat. A témával foglalkozó egyik áttekintett szakirodalom példaként veti fel az interneten kiszivárogtatott állami szintű minősített adatok nyílt internetes felületen történő elérésének problematikáját (Hassan & Hijazi, 2018, 342.). Ezen etikai kérdéseket felszínre hozó adatgyűjtés (például a Cambridge Analytica tevékenysége) legyen az akár egy tudományos közegből kiinduló kutatás – amellett hogy

6 Non-Governmental Organization (civil szervezet).

az adatok nyílt forrásokból és jogszerűnek tűnő eljárások útján jelentek meg – már inkább az adatok sérülékenységére hívja fel a figyelmet. Gondoljunk az olyan kutatásokra, amelyek során végeredményként a különböző adatbázisokban elérhető egyedi adatok adatbázisszerű összevetése révén minőségileg új, az eredeti rendeltetési céljától eltérő adatkoncentráció jön létre. Ezek közé sorolhatók az egyes adathalmazokban megjelenő metaadatok, amelyek komplex elemzése és értelmezése, majd további adatbázisokkal történő kiegészítése akár szenzitív jellegű adathalmazok létrehozását is jelenthetik, például profilozás vagy kapcsolati hálók megalkotása során. Nemzetbiztonsági értelmezésben az információgyűjtő tevékenység titkosságának védelme szintén az OSINT egyfajta korlátjaként értelmezhető. A példa kedvéért: a hagyományos internetes keresőmotorok használata során a böngészési előzmények megőrzésre kerülnek, mindez azonban már rendszerszintű OSINT tevékenységeknél kerülendő azokon a területeken, ahol az információgyűjtés irányultságának nyilvánossága – például katonai, rendvédelmi, gazdasági irányultság során – nemkívánatos. Az információgyűjtés iránya mások számára is információt szolgáltathat a tevékenységet végző szervezet hírigényéről, amely csak széleskörű biztonsági előírások betartásával kerülhető el. Az OSINT sajátos kihívásaként jelenik meg az internetes felületekhez köthető egyre növekvő számú online dezinformáció terjedése – ezek egy része fake news, azaz álhír –, amelynek a közösségi hálózatok mindenképpen kedveznek. Az Európai Bizottság Álhírekkel és Dezinformációval Foglalkozó Magas Szintű Szakértői Munkacsoportjának (High-Level Expert Group on Fake News and Disinformation – HLEG) jelentése szerint a közösségi hálón megjelenő online dezinformáció *„olyan hamis, pontatlan vagy félrevezető információ, amelyet nyereségvágyból vagy szándékos károkozás elérése érdekében készítenek, tesznek közzé vagy terjesztenek. Ez a tevékenység fenyegetést jelenthet a demokratikus folyamatokra és értékekre, de akár a közélet egy specifikus részét is érintheti, mint például az egészségügy, tudomány, oktatás vagy gazdaság."* (EU Commission, 2018, 10.) A jelentés az online dezinformáció komplex halmazát jelöli meg komoly kockázatként, nem pedig kizárólag az álhíreket. A jelenség természetesen nem új, hiszen a dezinformációkkal történő megtévesztés, manipulálás a történelem számos jeles eseményénél megfigyelhető volt. A jelenség új lendületet a média, különösen a közösségi média kapcsolati hálózatainak terjeszkedése mentén kapott, közvetlenül elérve annak felhasználóit. A hiteles, ellenőrzött, aktuális információk felhasználásában érdekelt nemzetbiztonsági struktúrákban ezen dezinformációk és álhírek alapvetően az OSINT információgyűjtő tevékenysége során kerülhetnek felszínre, ahol elsődleges feladat az információk hitelességének megállapítása.

Ezt követően az adott információ akár más hírszerzési információkkal összevetve válhat értékes, ellenőrzött részinformációvá. Napjaink online hírfolyamában az azonos témakörben megjelenő, eltérő tartamú hírek közül azonban gyakran rendkívül nehéz kiszűrni a valóságosat. Az elmúlt években az online források mindenki számára elérhető értékelő, elemző eljárásai ugyanakkor sajátos fejlődési irányokat is létrehoznak. A nyíltan hozzáférhető adatforrások, valamint az OSINT szabadon megszerezhető szoftveres eszközei lehetővé tették például, hogy adott események nyílt forrású feldolgozását bárki elvégezhesse és színvonalas elemzéseket készítsen (Jasikevicius, 2015). Ennek korlátját a jelentősebb képességű, mélyebb információk kinyerésére és komplexebb elemzések elvégzésre képes szoftverek fizetős változatai, valamint a professzionális szakmai hozzáértés hiánya jelenthetik.

A SOCMINT szempontrendszere

A közösségi oldalakhoz köthető fiatal információgyűjtési terület a SOCMINT. Eredményes alkalmazásához a nemzetbiztonsági és egyéb biztonsági szervezetek esetében már nélkülözhetetlen a hagyományos HUMINT alapú szakmai ismeretek és információk bizonyos szintű megléte, hiszen az információgyűjtés iránya alapvetően a biztonságot negatívan befolyásoló személyekre, közösségekre irányul. A témakört vizsgáló tanulmányt idézve *„A SOCMINT és a HUMINT integrálása elengedhetetlen a terrorizmus fenyegetéseinek azonosításához, megakadályozásához és megelőzéséhez. A technológia szerepe elengedhetetlen az aggodalomra okot adó viselkedés összegyűjtéséhez, összekapcsolásához és előrejelzéséhez."* (Lombardi, Rosenblum & Burato, 2015).

A SOCMINT – habár már évek óta jelen van a szakirodalmakban – terminológiai határai még mindig nem letisztultak (Antonius & Rich, 2013). Alapesetben a tevékenység, az információgyűjtés hagyományos elemeinek a közösségi média felületeihez kapcsolódó folyamatait takarja. Természetesen metodikai módszerei a közösségi oldalak fejlődésével párhuzamosan változnak. Az egyes tevékenységek elhatárolását tekintve emelhető ki példaként Erdész Viktor kategorizálása, aki szerint *„a SOCMINT-ot megkülönbözteti a klasszikus OSINT-tevékenységtől, hogy az érdemi információ kinyeréséhez, felhasználónévhez kötött online profil szükséges",* azonban mint írja *„az adatszerzők fő szabály szerint nem lépnek interakcióba a közösségi médiában. Erre már – indokolt esetben – a virtuális HUMINT-tevékenység során kerül sor."* (Erdész, 2018).

Abban a szakértők egyetértenek, hogy nem húzható egyenlőség az OSINT és a SOCMINT terület között. Amíg az OSINT tevékenység általánosságban a nyilvánosan, bárki által jogszerűen hozzáférhető információs forrásokat és azok megszerzéséhez szükséges eljárásokat jelöli, addig a SOCMINT esetében a nézőpontok megoszlanak. Egyes szerzők a SOCMINT-ot az OSINT részeként értelmezik, annak egyik sajátos irányaként, amely a közösségi oldalakhoz kapcsolódik. Amíg az OSINT értelemszerűen nem szűkíthető le a kibertérre, addig a SOCMINT kizárólag ezekre irányul. Mások arra hívják fel a figyelmet, hogy a SOCMINT a nyilvánosság számára korlátozottan hozzáférhető információkat is magában foglalja, vagyis értelmezhető nyílt és zárt irányultsága is (Antonius & Rich, 2013, 45.). Ebben a megközelítésben azonban, véleményünk szerint, a SOCMINT nem lehet kizárólag az OSINT részterülete, ahol a nyílt forrás megléte egyfajta alapfeltételként értelmezhető. Ebben az esetben, ha az köthető emberi közreműködéshez, akkor nemzetbiztonsági vonatkozásban a tevékenység jellege már a kibertérben végzett CYBER-HUMINT irányába mozdul el, hiszen a HUMINT fogalomkörében a zárt rendszereken tárolt, korlátozottan hozzáférhető, védett információk megszerzése érdekében alkalmazott titkos információgyűjtő eszközök is értelmezhetők. (Természetesen, csak ha azt jogszabályban erre kifejezetten feljogosított információgyűjtő szervezet végzi, a normatív garanciális elemek betartása mellett.) A fentiek jól jelzik, hogy az éles határ vagy akár a tiszta definíció tekintetében a források sem egységesek, s e mögött a kibertérben megjelenő nyílt és nem nyílt források közötti szürke zóna kérdésköre található. A titkos információgyűjtő tevékenység végrehajtására feljogosított szervezetek számára a fenti határok jelentősége kettős. Egyrészről a jogszabályok által deklarált felhatalmazási jogosítványaik, illetve a nemzetbiztonsági érdekek érvényre juttatása a minél részletesebb, pontosabb, releváns információk megszerzését teszik szükségessé, így nem állnak meg a nyílt, de zártabb felületeken megjelenő információk határnál, másrészről azonban ennek a határnak az átlépése már jogszabályban meghatározott engedélyeket és szakmai szempontok alkalmazását igényelheti. Példaként említhető, hogy a passzív jellegű, nyílt információgyűjtés területén túllépve, akár az (etikus) hacker technikák aktív alkalmazásával vagy akár a műveleti célú online HUMINT tevékenységgel, már nemcsak a zártabb közösségből történő információszerzésre nyílik lehetőségük, hanem az események részesei, akár formálói (befolyásolói) is lehetnek az érintett szervezetek. Ennek követelményei között pedig már fontossá válik a tevékenység valós céljának és a végrehajtói állomány kilétének rejtése, vagy akár az online kommunikáció során az adott ügynek megfelelő azonnali döntés jelentősége. Ebben az esetben a közösségi

felületen való aktív jelenlét szükséges, amely révén az OSINT-al szemben egy sokkal mélyebb – a hagyományos HUMINT területéhez hasonló – betekintést nyerhet alkalmazója egy adott közösség, csoport (például szervezett bűnözői kör) működésébe. Lehetővé válhat akár egy csoporton belüli hierarchikus viszonyok feltárása, rejtett szándékok megelőző jellegű felderítése (például terrorcselekmény előkészülete), valamint a csoport tagjai belső személyiségi jegyeinek mélyebb megismerése is. A CYBER-HUMINT fogalma alatt, álláspontunk szerint, egyszerűen a HUMINT módszerek kibertérben történő megjelenését és alkalmazását érthetjük, így az információgyűjtés során lényegében lehetővé válik, hogy közvetlen fizikai kapcsolat nélkül, a kapcsolattartás online térbe terelésével, a tevékenységet végzők humán forrásokat foglalkoztathassanak, akár távoli földrajzi térségekben is. Mindezen lehetőségek jelentősen csökkenthetik a humán hírszerzési tevékenység kockázatait is. Az alkalmazás környezetétől függően (például közösségi oldalak) lehetővé válhat mind a forrás, mind a célszemély vagy célobjektum mélyebb megismerése, tevékenységének nyomon követése, a szándékok feltárása. A tevékenység hatékony végrehajtásához ugyanakkor a HUMINT ismeretek mellett a különböző – aktív és passzív – támadó jellegű informatikai eljárások és egyéb, korunk információtechnológiai környezetéhez igazodó technikai képességek is szükségesek. Talán ez lehet az oka annak, hogy a kibertérhez kapcsolódó nemzetbiztonsági irányultságú HUMINT területeken a fiatalabb generációk dominanciája várható, hiszen a technológiai környezetből érkező információk értelmezése, a kapcsolódó ICT (Information and Communication Technology – Információ- és kommunikációtechnológia) megoldások alkalmazása számukra magától értetődőbb, mint az idősebb generációk számára. A CIA (Central Intelligence Agency – Központi Hírszerző Ügynökség) egyik korábbi vezető munkatársa, John Sano tanulmányában kitér rá, hogy mindez lényegében egy digitális szakadék, amely megkülönbözteti a tisztek jelenlegi generációját elődeiktől, ahol az előbbiek digitális bennszülöttek, míg az utóbbiak a digitális bevándorlók. Mindez – mint megfogalmazza – nem csupán annyit jelent, hogy a fiatal generáció többet töltött a televízió vagy a számítógép előtt, mint könyvek olvasásával, hanem más gondolkodási mintákat is magában foglal (Sano, 2015).

A Social Engineering szempontrendszere

A fenti témakörhöz gyakran sorolt Social Engineering az ember befolyásolására, manipulálására alapozza módszereit, lényegében emberek hackelése-

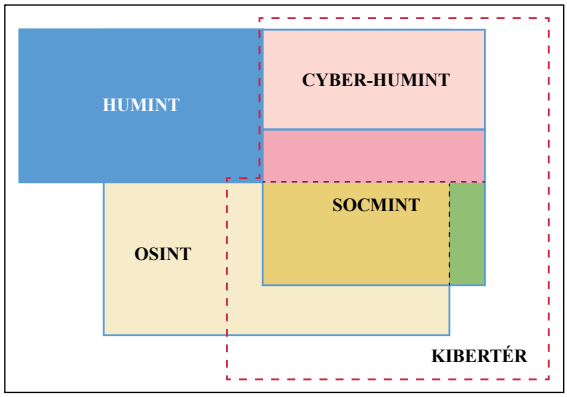
ként is jellemzik. Elsődleges alkalmazói a különböző bűnelkövetői csoportok, azonban bizonyos elemei természetesen alkalmazhatók szabályozott, jogszerűen kifejtett tevékenység részeként is. Harl szerint az SE nem más, mint az emberi tényező kihasználható tulajdonságaira, az emberi hiszékenységre építő támadási forma, olyan technikák és módszerek összessége, amely az emberek befolyásolására, manipulálására alapozva teszi lehetővé bizalmas információk megszerzését, vagy éppen kártékony programok terjedését és működését (Harl, 1997). Az SE műveletek kivitelezése alapvetően kétfajta módszertani csoport megkülönböztetésével valósulhat meg, amely szerint elhatárolhatók egymástól a humán és az infokommunikációs (technikai) csatornákon keresztül végrehajtott SE módszerek (Guenther, 2001). A tevékenység során megjelennek a HUMINT és az OSINT egyes elemei is, amely módszerek a nemzetbiztonsági szervezetek eszközkészletében is jelen vannak. Jelentősége a kibertérhez köthetően értékelődött fel, ahol a kibertámadások kb. 80%-a SE támadással kezdődik (Capano, 2019), amelyeknek számos formája ismert (a célirányos e-mailektől kezdve egészen a közvetlen emberi kommunikációt igénylő formákig). Capano szerint az SE támadások lehetnek emberi vagy számítógépes alapú támadások, ahol az emberi alapú támadások szükségessé teszik, hogy a támadó – valós személyazonosságát rejtve – kapcsolatba lépjen az áldozattal az információk megszerzése érdekében, így alapesetben korlátozott a támadás kiterjedése. Az informatikai alapú támadások során azonban nagyon rövid idő alatt a megtámadott áldozatok halmaza rendkívül nagyra, akár több ezer fős felhasználói körre is duzzadhat. Erre példaként az adathalász e-mailek említhetők, amely az internethasználat során az egyik legismertebb és leggyakoribb megtévesztési technika. Írásában Capano kitér a támadások közvetlen (személyes kapcsolatot, vagy csak kommunikációt igénylő, például telefonhívás), illetve közvetett (például az adathalászat) kategorizálásra is. Adathalászat során a támadók infokommunikációs csatornán (e-mail, hanghívás, üzenet) is felvehetik a manipulálni kívánt személlyel a kapcsolatot, melyben például egy hamisított weboldal megnyitására ösztönzik. Ezek a weblapok megjelenésükben rendkívül hasonlítanak az eredeti oldalra, azonban van néhány eltérés, például az URL-címben, amelyeket megvizsgálva felfedhető a támadás. A támadás során beszerezhető adatok köre lehet például: felhasználónevek, jelszavak, bankkártya szám, PIN-kód, születési hely, születési idő, anyja neve, lakcím, tartózkodási hely, okmányszámok, munkahely neve, munkahely címe, gépjármű adatok, pénzügyi információk stb. (EC-Council, 2011, 22.). Az adathasználat módszereinek humán és informatikai felosztása rávilágít arra, hogy az SE napjainkra számos módszert felölelő széles kategóriává fejlődött, ahol alapelemei a HUMINT területéről

származnak, míg technikai kötődésű területeinek nagy része tíz évvel ezelőtt még csak a hackertechnikák gyűjtőfogalma alatt jelentek meg (Capano, 2019). A szakirodalmakban az SE számos fogalmával találkozhatunk (Hadnagy, 2011; Mitnick, 2003, 191–193.), amelyek közös jellemzőjeként látható, hogy annak alkalmazója az emberi hiszékenységet kihasználva, megtévesztéssel, rábeszéléssel, befolyásolással kíván olyan információhoz jutni, amely segítheti egy adott informatikai rendszer elleni támadó szándékát. Az ilyen jellegű befolyásolási eljárás nem feltétlenül a kibertérben megy végbe, hanem a fizikai dimenzióban megjelenő, hagyományos közvetlen emberi kontaktusok során is megvalósulhat. Az alkalmazható, emberi sérülékenységet (például manipulálhatóságot, naivitás, nem megfelelő biztonságtudatos magatartást stb.) kihasználó megoldások így rendkívül sokfélék lehetnek, felölelhetik a személyes kontaktust igénylő és a technikai eszközök tárházát is. Ugyanakkor nem szabad megfeledkeznünk arról, hogy a megtévesztés, befolyásolás érdekében alkalmazott módszerek többsége már túlmutat a másik fél hagyományos – akár pszichológiai ismereteket igénylő – tanulmányozásának körén, és az illegális tevékenységek halmazába sorolható. Legjobb példaként a személyiség-, identitáslopás különböző, humán és technikai elemeit ötvöző megoldásai említhetők, e körben jellemző a személyes adatok jogosulatlan megszerzése és felhasználása, például bankkártya adatokkal összekötve, illegális anyagi haszonszerzés céljából (Sörös & Váczi, 2013, 11–12.). Az SE tevékenység elhagyhatatlan eleme az előzetes, tanulmányozó jellegű információgyűjtés, hiszen a támadó ennek során igyekszik feltérképezni a másik fél gyenge pontjait, a sérülékenység lehetséges területeit. A tanulmányozás forrásai között jelennek meg a nyíltan hozzáférhető internetes tartalmak, amelyek köre az adott céltól függően eltérő mélységű lehet. Ennek jellemző területei például a közösségi oldalak, ahol az egyes felhasználók eltérő mélységben, a veszélyt gyakran nem érzékelve tesznek közzé magukról szenzitív adatokat. Jelen lehetnek azok a már nyílt forrásokon túlmutató adattárak is, amelyek megszerzése már legális eszközökkel nem biztosítható, illetve az ott elérhető információk, annak tulajdonosának belegyezése nélkül jogszerűen nem is használhatók fel. Például gondoljunk egy zárt közösségi csoporton belül megjelenő, adott körnek szánt bizalmasabb információkra. A SE tevékenységet tekintve egyre nélkülözhetetlenebb módon vannak jelen azok a technikai eszközök is, amelyek a megtévesztést, befolyásolást elősegíthetik (például proxy szerverek, feltöltős SIM kártyák). Az ide sorolható eszközökkel lényegében annak alkalmazója azonosíthatatlan maradhat. A professzionális SE támadás kivitelezése során számolni kell a humán és az informatikai rendszer együttes alkalmazásával (Tóth, 2020, 87.).

Konklúziók

A kutatási eredmények alapján megállapítható, hogy a HUMINT, az OSINT és a SOCMINT módszerek – kibertérhez köthető – elhatárolhatósága mellett is számos átfedés látható, mivel azok végrehajtását általánosan jellemzi a komplex, az egyes információgyűjtő módszerek fúzionalizált alkalmazása. Amíg az OSINT tevékenység általánosságban a nyílt forrású információk megszerzéséhez szükséges eljárásokat jelöli, addig a SOCMINT-ot a szakirodalom egy része az OSINT részhalmazaként értelmezi, amely a közösségi oldalakhoz kapcsolódik. Értelemszerűen az OSINT forrásoldala nem szűkíthető le a kibertérre, a SOCMINT azonban kizárólag ezekre irányul. A szakirodalmi források másik köre arra hívja fel a figyelmet, hogy a SOCMINT a nyilvánosság számára korlátozottan hozzáférhető információkat is magában foglalhatja, vagyis értelmezhető nyílt és zárt irányultsága is. Véleményünk szerint a SOCMINT nem kizárólag az OSINT részterülete, ahol a nyílt forrás megléte egyfajta alapfeltételként értelmezhető, hanem az összadatforrású információgyűjtés egy lehetséges ága, melynek az OSINT-tal csak kapcsolódási pontjai (halmazuniói) vannak, a közösségi oldalakon elérhető, nyíltan hozzáférhető információk vonatkozásában. A SOCMINT-nak a közösségi oldalak nem nyilvánosan hozzáférhető tartalmait megszerző irányultsága már a kibertérben végzett CYBER-HUMINT irányába mozdul el abban az esetben, ha a releváns információk megszerzéséhez valamilyen emberi tevékenység is társul, hiszen a HUMINT fogalomkörében a nyilvánosan nem hozzáférhető információk megszerzése érdekében jogszerűen alkalmazott titkos információgyűjtő eszközök is értelmezhetők. Fontos megjegyezni, hogy a SOCMINT tekintetében csak akkor beszélhetünk közös metszéspontról a HUMINT vonatkozásában, ha az információgyűjtés emberi tevékenységhez kötött. Az egyes tevékenységek elhatárolását a forrásoldal irányából érdemes megközelíteni. Meg kell vizsgálni, hogy a releváns információ, illetve adat jogszerűen, nyíltan hozzáférhető – például a közösségi hálón –, és annak megismerése, kezelése nem ütközik normatívába (OSINT U SOCMINT). Vagy az érdemi információk megszerzése érdekében a lehetséges irány – a jogszabályi garanciáknak való megfelelés mellett – a zárt, a nyilvánosság számára nem, vagy csak korlátozottan hozzáférhető forrásokból történő információgyűjtés (HUMINT U SOCMINT).

A jövőre kitekintve már most látható, hogy az emberi viselkedés és kapcsolattartás virtuális platformokon megjelenő digitalizált adatai a humán és a technikai alapú ismereteket igénylő új információgyűjtő megoldáso-



1. számú ábra: Az információgyűjtő területek lehetséges kapcsolódásának elvi vázlata.
Forrás: A szerzők saját szerkesztése

kat eredményeznek. Gondoljunk a globális kiterjedésű közösségi oldalak elterjedésére, adathalmazainak létrejöttére, amelyeken keresztül az emberi viselkedés addig soha nem látott formában, rendszerszintű eljárásokkal vált megismerhetővé. A jövőben várhatóan nemcsak az egyén, hanem a csoportokhoz köthető viselkedésminták, folyamatok modellezésének fejlődése várható, melyek amellett, hogy hozzájárulhatnak a biztonság növeléséhez, ugyanakkor a mérleg másik oldalán akár lehetővé is tehetik, hogy egyes társadalmi csoportokat befolyásoljanak, manipuláljanak. Mindezek sokoldalú kihívást jelentenek a biztonságért felelős szervezetek számára. A Global Trends 2012-ben készített, 2030-ig szóló előrejelzése szerint a közösségi média működése és szabályozása, a kiberbiztonság mellett kiemelt jelentőségű területé fog válni. A növekedés jelentős kihívásokat jelent mind a kormányok, mind a társadalom tagjai számára, melyeknek új módszereket kell találniuk a megjelenő ICT technológiák előnyeinek kiaknázására, miközben az e technológiák jelentette új fenyegetésekre megfelelő válaszokat is kell alkotniuk, például az információgyűjtés hatékonyságának optimalizálása során. Mindezen változásoknak már most is a részesei, szemtanúi vagyunk (Global Trends 2030, 2012). Számos, a fejlett a titkos információgyűjtést letetővé tevő technológia alkalmazása terén meghatározónak tekinthető ország (többek között Nagy Britannia, az Orosz Föderáció, Kínai Népköztársaság, Ausztrália, Izrael és az USA) esetében a technológiák hangsúlyos jelenléte látható, amely közvetlenül befolyásolhatja a kibertében végezhető HUMINT fejlődését is, míg egyéb, technológiailag fejletlenebb országok esetében ez a folyamat lassabban megy végbe. A jövőt azonban láthatóan nem a humán vagy a technikai terület kizárólagossága jelenti. Elkerülhetet-

lennek tűnik a hagyományos HUMINT módszerek és a technológia alapú információgyűjtő eljárások fúziója, és olyan szakmai képességek kialakulása valószínűsíthető, ahol a technológiai jellegű, szaktechnikai tudás és a humán alapú információgyűjtéshez szükséges ismeretek koncentráltan lesznek jelen.

Felhasznált irodalom

Antonius, N. & Rich, L. (2013). Discovering collection and analysis techniques for social media to improve public safety. *The International Technology Management Review*, *3*(1), 42–53.

Azani, E. (2018). Global Jihad – The Shift from Hierarchal Terrorist Organizations to Decentralized Systems. https://www.ict.org.il/images/Global%20Jihad%20%E2%80%93%20The%20Shift%20from%20Hierarchal.pdf

Bardóczi Á. (2018). *Nyílt-forrású információszerzés – kémek, kurvák, gengszterek, OSINT*. NetAcademia LLC.

Capano, D. E. (2019). *The human asset in cybersecurity*. https://www.controleng.com/articles/the-human-asset-in-cybersecurity/

Crosston, M. & Valli, F. (2017). An Intelligence Civil War: "HUMINT'" Vs. "TECHINT". *Cyber, Intelligence, and Security*, *1*(1), 67–82.

Erdész V. (2018). A SOCMINT helye, szerepe az összadatforrású hírszerzésben. *Felderítő Szemle*, *17*(4), 27–40.

EC-Council (2011). *Penetration Testing: Procedures & Methodologies, Cengage Learning*

EU Commission (2018). *A multi-dimensional approach to disinformation*

Fialka Gy. (2018). Emlékek az operatív technika világából - A titkos információgyűjtés technikai támogató rendszere. In Dobák I. & Hautzinger Z. (Szerk.), *Szakmaiság, szerénység, szorgalom* (pp. 197–202.). Dialóg Campus

Guenther, M. (2001). *Social Engineering – Security Awareness Series*. Előadás

Hadnagy C. (2011). *Social Engineering: The Art Of Human Hacking*. Wiley Publishing Inc.

Mitnick, K. D. (2003). *Art Of Deception: Controlling The Human Element of Security*. Wiley Publishing Inc.

Hassan, N. A. & Hijazi, R. (2018). *Open Source Intelligence Methods and Tools: A Practical Guide to Online Intelligence*. Apress. https://doi.org/10.1007/978-1-4842-3213-2

Harl, G. (1997). *People Hacking - The Psychology of Social Engineering*. Text of Harl's Talk at Access All Areas III, March 7, 1997.

Jasikevicius, Z. (2015). Exploring the VW scandal with graph analysis. https://linkurio.us/blog/exploring-the-vw-scandal-with-graph-analysis/

Johnson, L. K. (Eds.) (2010), *The Oxford Handbook of National Security Intelligence*. Oxford University Press. https://doi.org/10.1093/oxfordhb/9780195375886.001.0001

Károly L., Drusza T., Regényi K. & Laufer B. (2019). *Információszerzés kapcsolati forrásai*. Nemzeti Közszolgálati Egyetem

Kovács Z. (2015). *Az infokommunikációs rendszerek nemzetbiztonsági kihívásai.* Doktori értekezés. Nemzeti Közszolgálati Egyetem, Katonai Műszaki Doktori Iskola

Lombardi, M., Rosenblum, T. & Burato, A. (2015). *From SOCMINT to Digital Humint: re-frame the use of social media within the Intelligence Cycle*. Fondazione de Gasperi

NATO Standardization Office (2019). *NATO Glossary of Terms and Definitions AAP-06*.

Omand, D., Bartlett, J. & Miller, C. (2012). Introducing Social Media Intelligence (SOCMINT). *Intelligence and National Security*, *27*(6), 801–823. https://doi.org/10.1080/02684527.2012.716965

Regényi K. (2019). OSINT a második generációs internetet megelőző korokban. *Nemzetbiztonsági Szemle*, *7*(2), 32–37. https://doi.org/10.32561/nsz.2019.2.3

Sano, J. (2015). The Changing Shape of HUMINT. The Intelligencer: Journal of U.S. *Intelligence Studies, 21*(3), 77–80.

Sörös T. & Váczi D. (2013). *Social engineering a biztonságtechnika tükrében – Avagy a modern támadók nem símaszkot, hanem álarcot viselnek*. XXXI. Országos Tudományos Diákköri Konferencia

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

Solti I. (2019). Az OSINT információgyűjtő eszközeiről. *Nemzetbiztonsági Szemle, 7*(2), 3–18. https://doi.org/10.32561/nsz.2019.2.1

Tóth T. (2019). General Description of Social Engineering and Its Place In Information Warfare. *National Security Review*, *5*(1), 42–55.

Tóth T. (2020). Az egyes Social Engineering módszerek elhatárolása és rendszerezése. *Szakmai Szemle, 18*(1), 87–110.

Twitchell, D. P. (2006). Social engineering in information assurance curricula. *InfoSecCD, 3*, 191–193. https://doi.org/10.1145/1231047.1231062

A cikk APA szabály szerinti hivatkozása

Dobák I. & Tóth T. (2020). Régi módszerek a kibertérben? (CYBER-HUMINT, OSINT, SOCMINT, Social Engineering). *Belügyi Szemle*, *69*(2), 195-212. https://doi.org/10.38146/BSZ.2021.2.2