7. évfolyam (2019) 2. szám 83–93. • DOI: 10.32561/nsz.2019.2.7

Dobák Imre[1]

OSINT – Gondolatok a kérdéskörhöz

OSINT – Thoughts on the Issue

Az OSINT mint hírszerzési ág napjainkra már széles körben kutatott, alkalmazása jelen van mind a gazdasági szereplők, mind a biztonságért felelős kormányzati szervek rendszerében. Számos alkalmazási előnnyel és korláttal rendelkezik, valamint a technológiai környezet jelentős hatást gyakorol az OSINT fejlődésére. Sajátos jellemzői rávilágítanak arra, hogy egyre összetettebb fejlődő területei a jövőben is meghatározóak maradnak.

Kulcsszavak: OSINT, hírszerzés, információgyűjtés, technológia, nemzetbiztonság

The OSINT as a branch of intelligence has been extensively researched nowadays, and its application is present in the sphere of both economic and government organisations responsible for security. It has many application advantages and limitations, and the technological environment has a significant impact on the development of OSINT. Its specific features highlight the fact that its more complex development areas will remain dominant in the future.

Keywords: OSINT, intelligence, information gathering, technology, national security

Jelen tanulmány az információgyűjtés egyik sajátos ágaként megjelenő nyílt forrásból történő információgyűjtés (OSINT – Open Source Intelligence) gyakran hangoztatott előnyei és hátrányai metszetében annak fejlődési kérdéseihez kíván gondolatokat megfogalmazni. A hírszerzési ág napjainkra már széles körben elterjedt, mind a gazdasági szereplők, mind a biztonságért felelős kormányzati szervek rendszerében. Mindazonáltal számos korlát és tisztán még nem látható fejlődési irány jellemzi a tevékenységet, amelyet közvetlenül befolyásol az infokommunikációs környezet rendkívül gyors fejlődése.

[1] Dr. Dobák Imre, Nemzeti Közszolgálati Egyetem. ORCID-azonosító: 0000-0002-9632-2914.

A fogalmi keret

Az angolszász rendszer hírszerzési ágai között megjelenő OSINT mint nyílt forrásból történő információgyűjtés fogalmának tudományos értékű tisztázására jelen tanulmány nem kíván részletesen kitérni, az általánosan ismert hazai és nemzetközi fogalmak néhány fő elemét azonban mindenképpen érdemes kiemelni. Ezek között jelenik meg a nyilvános forrásból történő *megszerezhetőség* elsődleges kritériuma, amely mellett az információgyűjtés összetett folyamatát (információk felkutatása, gyűjtése, szelektálása, elemzése-értékelése és felhasználása[2]), valamint egyes esetekben az információgyűjtés jogszerűségének kérdését szokták megemlíteni.[3]

Amíg Lévay definíciójában[4] megjelenik az információgyűjtés legális eszközökkel történő végzésének kérdése, a Vadász–Séllei szerzőpáros tanulmányában kiemeli, hogy az „angolszász szakirodalomban a jogszerűség általában kimarad, csak a mindenki számára történő elérhetőséget (publicly available) mint kritériumot adják meg”.[5] A kérdéskör hazai jogi oldalát tekintve Péterfalvy is rávilágít, hogy „a nyílt információgyűjtés nem egzakt jogi terminus abban az értelemben, hogy a jogforrásokban nem található olyan általános érvényű definíció, amely pontosan meghatározná a jelentését”.[6] Fenti megállapításokat elfogadva láthatóvá válik, hogy a két megközelítés (a nyílt forrású információgyűjtés jogi és hírszerzési célú OSINT-szakterminológia megközelítése) teljes egészében nincs átfedésben.

Amíg korábban a tevékenység elsősorban a különböző biztonsági szervekhez, titkosszolgálatokhoz kapcsolódott,[7] a század második felére a korábbi zárt állami jellegű felhasználásból kikerült a gazdasági, üzleti és egyéb szereplőkhöz. A kibertér térhódításával az információk tömeges jellegű, szabad elérhetősége biztosítottá vált, hiszen mint Szűts is megfogalmazza: „A mindenhol jelen lévő számítástechnika hatására az informatikai eszközök beépülnek környezetünkbe […] és ezzel együtt társadalmunkba is.”[8]

Nyílt jellege miatt az OSINT fejlődése rendkívül dinamikus és széles körű, egyedi és rendszerszintű információgyűjtési lehetőségei körül jelentős informatikai piacifejlesztői szegmens épült ki. Alkalmazási irányait, a világhálón keresztül elérhető adatok feldolgozhatóságának, felhasználásának témakörét szintén több tudományterület irányából, így például az informatika vagy akár a társadalomtudományok irányából kutatják. A témakörre is adaptálható Szűts informatika fejlődéséhez kapcsolódó megállapítása, miszerint a kutatók között „egyfajta felosztás alakult ki a munkát illetően: a hálózati kommunikációval foglalkozó mérnökök a jelenség technikai aspektusait vizsgálják, a kommunikációkutatók az információ átadásának folyamatát

2 Lévay 2006.
3 Lásd többek között a *Nemzetbiztonsági Szemle* jelen 2019/2. számában megjelenő Szabó Károly: *Az OSINT – Gondolatok a tevékenységről és az alkalmazás közegéről*, vagy Solti István: *Az OSINT információgyűjtő eszközeiről* szóló tanulmányait.
4 Lévay 2006.
5 Vadász–Séllei 2017, 189.
6 Péterfalvy 2015, 17.
7 Schaurer–Störger 2010.
8 Szűts 2018, 53.

veszik górcső alá, míg a társadalomtudósok az egyénre és a közösségekre gyakorolt hatásokra kíváncsiak".[9]

Napjainkra az OSINT a köztudatban összeolvadt az interneten folytatott információszerzéssel, függetlenül annak egyedi vagy rendszerszintű megoldásaitól, témakörétől, vagy akár a megszerezhető adatok típusától, jellegétől. Az OSINT az elmúlt évtizedekben lényegében kinőtte a korábbi szűk fogalmi keretét, és kis jóindulattal szinte minden ide sorolható, ami nyílt forrásból elérhető és gyűjtője számára valamilyen relevanciával bír. A háttérben azonban a kibertér fejlődésével és a személyiségi jogok védelmével olyan szakmai viták is megfigyelhetők, mint az adatgyűjtési megoldások jogszerűsége, a nyílt információgyűjtés „határai", valamint a tömeges jellegű adatgyűjtések és feldolgozhatóság kérdése.

A kezdetben még a műsorszórásban megjelenő, majd később az interneten elérhető információk figyelése, monitorozása és az ott elhangzottak felhasználása egyre inkább nélkülözhetetlen információkat jelentett felhasználói számára. Az ICT[10]-környezet robbanásszerű fejlődésével azonban egyrészről átalakultak azon információs közegek, amelyek az OSINT számára a leginkább releváns forrásokat jelenthetik, másfelől átalakultak az információk megszerzésének és feldolgozásának módjai is. A felhasználói szokások változásával párhuzamosan így a nyílt információgyűjtés előterébe kerültek többek között a közösségi média különböző felületei, hiszen az itt megjelenő hírek számos esetben a biztonságra közvetlen hatást gyakorolnak (gondoljunk csak a terrorista hálózatok toborzó tevékenységére, vagy akár a nagyobb tömegek befolyásolásának szándékára).

Az OSINT jelene

Az OSINT mint sajátos hírszerzési ág, információgyűjtési terület jelenét tekintve mit is láthatunk?

- Az OSINT lehetőségeinek felhasználása érdekében számos alkalmazási területen saját információgyűjtő képességeket alakítottak ki, amelyek között a nemzetközi tevékenységek,[11] a kormányzati biztonsági szervek, az üzleti szféra, vagy akár a nem állami szereplők (NGO[12]) is megtalálhatók. Az OSINT-tevékenységek iránt jelentkező „megrendelői" igények kiszolgálására ugyanakkor számos olyan megoldás (például információbórkerek) is létrejött, amelyek internetre épülő adatgyűjtési megoldásaikkal, szolgáltatásaikkal, illetve szoftverfejlesztéseikkel tették professzionálissá a tevékenységet. Számos ország biztonsági szervei (rendőrség, nemzetbiztonsági szolgálatok) kezdték el az OSINT ellenőrzési és kutatási képességeit növelni, amelyek között megjelentek a nyílt interneten, a deep weben, a darkneten, valamint a közösségi oldalakon történő információgyűjtés lehetőségei. A megváltozott információmegosztási platformok folyamatosan alakították a kapcsolódó fejlesztések irányait is.

9 Szűts 2018, 127.
10 Information and Communications Technology.
11 Uri 2012.
12 Non-governmental organization – nem kormányzati szervezet, civil szervezet.

Lényegében az internet az ott megtalálható nyílt adatoknak köszönhetően adott teret az új tevékenységek kialakulásának.[13]

- Előtérbe kerültek az OSINT módszereinek jogszerűségéhez, annak határaihoz köthető szakmai viták. Információs társadalmunkban joggal merülhet fel a kérdés, hogy pontosan hol is húzódhat a kibertérben folytatott OSINT-tevékenység határa, és elsődlegesen a nyíltan elérhető forrásokat kell tekintenünk, vagy akár azon módszereket, amelyek – habár széles körben elérhetőek – speciális ismereteket igényelnek. Az OSINT-jellegű kutakodás kapcsán szinte biztosan felmerül a kérdés, hogy annak végzője számára az interneten megtalálható minden megoldás etikusnak, esetenként jogszerűnek tekinthető-e.[14] Igaz, számos esetben maguk a módszerek is *nyíltan* elérhetők, mindez azonban nem jelenti egyértelműen, hogy azok alkalmazása minden felhasználó számára *legálisnak* tekinthető. A nyílt információk és források jelentőségét felismerve több kutatóintézet és egyetem is kutatási irányai közé emelte az OSINT-tevékenységet, amelyek arra is rávilágítottak, hogy a *nyílt* információgyűjtés képessége számtalan (például jogi, etikai, gazdasági, technológiai) korláttal rendelkezhet. Gyakran hangoztatott előnyei (például költséghatékonyság, aktualitás, biztonságos alkalmazás – kockázatmentes „kutakodás" lehetősége), valamint hátrányai (például információdömping, nyelvi képességek szükségessége, időtényező) mellett kiemelten fontos szemponttá vált az információk megbízhatóságának[15] kérdése.
- Az OSINT eszközei és módszerei nyilvánossága kapcsán szembesülhetünk az alkalmazott eszközök *átláthatóságának*[16] és az adatszerzés *mélységének* kérdésével. Fejlődő technológiai környezetünkben nap mint nap jelennek meg azon új megoldások, amelyeket például egy-egy közvetlenül nem értelmezhető információ megjelenítéséhez rutinszerűen felhasználunk.[17] Az eszköz *nyílt elérésénél* azonban már kérdésként merülhet fel, hogy mitől lesz az információ értelmezését segítő megoldás is nyílt egy olyan kibertérben, ahol számtalan forrásból akár a hackertechnikák szürke zónájához sorolható megoldások is szabadon elérhetők. Az OSINT kapcsán fontos hangsúlyozni, hogy az információ megszerzésére amellett, hogy a megjelenő információ nyíltan elérhető, csak passzív módon, legális eszközökkel kerülhet sor, egyéb megoldások már akár a hackingtevékenységek irányába mutathatnak. A biztonsági struktúrák,

---

13 https://homelandsecurityresearch.com/reports/osint-market-national-security-defense-homeland-security- private-sector-public-safety/ (A letöltés dátuma: 2019. 02. 10.)

14 A témával foglalkozó egyik áttekintett szakirodalom sajátos példaként veti fel például az interneten „kiszivárogtatott" állami szintű minősített információk nyílt internetes felületen történő elérésének problematikáját. Hassan–Hijazi 2018, 1.

15 A hiteles információkhoz történő hozzájutást segíthetik a professzionális OSINT-megoldások mellett a különböző állami és nem állami szereplők által kezelt adatbázisok (például tudományos adatbázisok). Ugyanezen kategóriába sorolhatók a gazdasági, pénzügyi élet területein alkalmazott megoldások (példaként a tőzsdei információk azonnali, illetve késleltetett elérése közti különbség említhető), amelyek a gyors gazdasági döntéseket segíthetik.

16 Wells 2016.

17 Gondoljunk egyszerűen egy olyan adatra, amely csak egy szabadon, bárki által letölthető nyílt programmal válik számunkra értelmezhetővé. Ebben az esetben mind a forrás, mind az annak értelmezéséhez szükséges megoldás nyíltan elérhető (eltekintve attól, hogy alkalmazása esetleg már speciális tudást feltételez).

nemzetbiztonsági szervezetek esetében azok állami célú feladatellátása és jogszabályi lehetőségei mentén azonban ezen eszközök és módszerek szélesebb körben értelmezhetők.

- Gyakran hangoztatott szempont az OSINT költséghatékonysága, amely a többi információgyűjtési terület forrásigényét feltételezve valóban egyértelműnek tűnik, hiszen relatíve kis költséggel rendkívül nagy számú információt érhetünk el.[18] A megfelelő, professzionális szakmai képesség (idesorolva az OSINT professzionális informatikai megoldásait és a szükséges szakértői, elemzői bázist) kialakítása azonban akár már jelentősebb forrásokat igényelhet. Ennek eleme a hozzáértő, egyre inkább az informatikai megoldások iránt nyitott szakmai állomány alkalmazása, amely a magas szintű OSINT-képesség működtetésének egyik kulcstényezője. Itt természetesen az alapszintű OSINT-tevékenységen túlmutató ismeretek megszerzése (idesorolva a lehetséges ágazati jellegű ismereteket, például üzleti, gazdasági, rendvédelmi ismeretek) azonban időt, felkészülést és nem utolsósorban a változások folyamatos nyomon követését igénylik. Szót kell ejteni a speciális tudásra és képességekre épülő információbrókerekről is, akik már adott anyagi ellenszolgáltatásért biztosíthatják az információmegrendelő számára azon szükséges információkat, amelyek megszerzésére az adott félnek sem szakmai képessége, sem eszközrendszere nem áll rendelkezésre. Ugyanide sorolhatók egyes fizetős adatbázisok változatai is, ahol az alapvetően nyíltan elérhető adatok mentén az anyagi korlátok megléte szabhat gátat az információk elérésének. Azt gondolhatnánk, hogy ezek forrásigénye elhanyagolható, azonban ha csak a jelentősebb nemzetközi tudományos adatbázisok jogszerű, folyamatos online elérésére gondolunk, akár jelentős költségek is felmerülhetnek. Ennek egyszerűbb példái azon tőzsdei mozgásokat megjelenítő megoldások is, amelyeknek például csak időben késleltetett változatai érhetők el ingyenesen.
- Az idővel való versengés az OSINT egyik legfontosabb elemévé vált, amely az egyéb szempontoknak történő megfelelés (például hitelesség, ellenőrzöttség) esetén a gyors döntéshozatal nélkülözhetetlen tényezője. A globális média korában az úgynevezett CNN-effektust szokták említeni, hiszen a média is a rendkívül gyors, aktuális információk megszerzésében és közzétételében érdekelt. Mint Botz 2000-ben közzétett írásában kifejti, „az OSINT […] részben a hírszerzés válasza a »CNN-effektusra«, azaz a professzionális hírszolgáltatók versenyére, amely nemcsak a közvélemény, hanem a döntéshozók kegyeinek megnyeréséért is folyik”.[19] Véleményem szerint máig igaznak tekinthetők megállapításai, miszerint a mérleg a hírszerzés oldalára dől, amely „szakmai kvalitásai alapján megbízhatóbb, tárgyilagosabb, tényszerűbb, mélyebbre hatoló, jobban a felhasználói igényekhez igazított, rendszerezőbb, szakszerűbb és vezethetőbb, mint a szenzációhajhász, manipuláló és manipulálható média”.[20]

[18] Bányász 2015, 24.
[19] Botz 2000, 27.
[20] Botz 2000, 27.

- Az OSINT-források mentén szembesülhetünk az álhírek/információk[21] jelenségével, „az online hamis hírek előrejelzett növekedésével”.[22] Mindez hamar a kutatók látókörébe került, amely az OSINT oldaláról az egyes adatok, illetve információk hitelességének kérdését és a mögöttes vélt vagy valós megtévesztési szándékokat vetheti fel. Nemzetbiztonsági szempontból a propaganda, szándékos megtévesztés, információs műveletek digitális formáinak korszakában mindennek rendkívüli jelentősége van. A történelem korábbi példáihoz viszonyítva az eltérés talán csak annyi, hogy napjaink megtévesztési műveleteinek elsődleges színterei az elektronikus média különböző megjelenési formáira tevődtek át. A digitális közösségi média térhódításával, az egyének által generálható hírek gyors terjedésével hatásuk fokozottan jelenik meg, és ellenőrzöttség hiányában rendkívül gyorsan válhatnak akár a hitelesnek vélt források részeivé is. A biztonságot befolyásoló, az adott állam szuverenitását, működésének megzavarását okozó hatásuk miatt jelentőségük és ezáltal kiszűrésük feladata vitathatatlan. (A közösségi oldalakon és egyéb internetes médiafelületeken megjelenő hatalmas információmennyiségből a felhasználók számára szinte lehetetlen a hamis hírek kiszűrése, amely még az információgyűjtésre, elemzésre-értékelésre szakosodott szerveket is komoly feladat elé állíthatja.)
- Előremutató kérdésként jelenik meg az interneten nyíltan elérhető adatok tömeges jellegű kereshetőségének, megszerzésének, feldolgozhatóságának problematikája, amely lehetőségét szintén a fejlődő technológiai környezet hozta létre. Gondoljunk csak a napjainkban már globálisan elterjedt üzleti célú adatgyűjtésre (például trendelemzés), amelyek akár életvitelünkbe, szokásainkba, érdeklődési körünkbe is betekintést engedhet. A közösségi oldalakhoz köthető az elmúlt években kirobbant, már említett adatvédelmi botrány (Cambridge Analytica[23]) is, amely jól jelzi, hogy a nyílt információgyűjtés határán létrehozhatók olyan személyes jellegű adathalmazok, metaadatok, amelyek tömeges feldolgozása már szenzitív kumulált adathalmazként értelmezhetőek.[24] Végeredményként a különböző adatbázisokban elérhető egyedi adatok összevetése révén akár minőségileg új, az eredeti rendeltetési céljától eltérő adatkoncentráció jöhet létre. Az adatbázisokban történő keresés kapcsán érdekes gondolatot vet fel a Vadász–Séllei szerzőpáros is, miszerint nehéz a valóságban pontos határt vonni a nyílt forrású információkeresés és

[21] Gyakran használt kifejezés az úgynevezett „fake news”, amely kapcsán a szakirodalmak bővelkednek a meghatározásokban, ezek közös elemeként jelenik meg, miszerint olyan valótlan információkról beszélhetünk, amelyekkel egy adott cél érdekében egyéneket, vagy szélesebb közösségeket kívánnak megtéveszteni. Irányait tekintve a politikai jellegű álhírektől kezdve, a gazdasági-üzleti irányokig számtalan megoldásával találkozhatunk.

[22] Hassan–Hijazi 2018.

[23] Lásd: www.europarl.europa.eu/news/hu/headlines/society/20181005STO15108/facebook-botrany-tobbet-kell-tenni-az-adatvedelmi-torveny-ervenyre-juttatasaert (A letöltés dátuma: 2019. 02. 10.)

[24] Szinte közhelynek tekinthető, hogy a kibertér össztettsége révén a legkörültekintőbb akarattal is mindenki olyan digitális nyomokat hagy maga után, amelyek nyílt elérése révén információk keletkeznek életére, szokásaira, preferenciáira nézve. Ezek tudatos felhasználása, amellett, hogy névtelenül lecsupaszítva az üzleti célú felhasználást segíthetik, a politika oldalán akár befolyásolási lehetőségeket is megalapozhatnak az egy adott csoport irányába (profilozás lehetősége, kapcsolati hálók).

a tágabban értelmezhető *információkeresés* között. A témakör hazai kereteit vizsgáló szaktanulmány fontos megállapítást tesz: „Ismereteink szerint a nyílt forrású adatok keresése nem kell, hogy célhoz kötötten történjen. Más szavakkal: nem tiltott a tömeges információkeresés (bulk search).”[25]

- Az OSINT üzleti-vállalati és kormányzati megoldásainak fejlesztése ma már önálló piaci szegmensként jelenik meg. Mint a Market Research Future ötéves (2018–2023) OSINT piaci előrejelzéséről szóló tájékoztatójában rámutat, a globális OSINT piaca folyamatosan – a 2017-es 2865,9 millió dollárról 2023 végére várhatóan 7047,7 millió dollárra – növekszik.[26] A kutatási jelentésről szóló rövid ismertetőben hangsúlyozzák, hogy számos OSINT technikai megoldás és irány jelent meg (big data adatszoftverek, videóelemzés, szövegelemzés, vizualizációs megoldások, kiberbiztonság, webelemzés, közösségi médiaelemzés), amelyek egyre bővülő piaccá növik ki magukat,[27] és ahol technológiai szempontból a kiberbiztonság tekinthető a vezető szegmensnek. Egy másik, a témával foglalkozó előrejelzés[28] szintén a globális szintű nyílt forráskódú hírszerzési piac növekedését – 2018 és 2026 között várhatóan 23,7%-kal – vetíti előre. „A globális OSINT-piac élvonalában Észak-Amerika van. […] A piac növekedése nagyrészt a felhőtechnológia és az IoT[29] egyre növekvő elfogadásából származik a régióban.” [30] Növekszik a Webint[31] és a Social Media Monitoring piaca is,[32] hiszen ezen források a nyílt adatokra alapozva szinte azonnal adatokat szolgáltathatnak, a kormányzati vagy akár gazdasági szereplők számára.

A jövő kérdései

- Az OSINT-megoldások számos előnnyel és hátránnyal rendelkeznek, amelyek közül leginkább a dinamikusan változó ICT-környezetben történő szabad fejlődés lehetősége emelhető ki. Mindez előrevetíti az alapvetően nyíltként aposztrofált OSINT folyamatosan változó sajátosságait: információtechnológiai környezet fejlődése, a mesterséges intelligencia egyre szélesebb körben történő alkalmazása, vagy akár az adat és szövegbányászati technológiák, vagyis maga az információk elérésének sajátos formái. A fejlődés mögött a szabad fejlesztési lehetőségek, az egyre bővülő, nyíltan, digitális formában elérhető szabad források, valamint az OSINT-képességek iránti jelentős piaci kereslet

---

25 Vadász–Séllei 2017, 189.

26 www.marketresearchfuture.com/press-release/open-source-intelligence-market (A letöltés dátuma: 2019. 02. 10.) (Megj.: jelen tanulmány szerzőjének a teljes előrejelzés tanulmányozására nem nyílt lehetősége.)

27 www.marketresearchfuture.com/press-release/open-source-intelligence-market (A letöltés dátuma: 2019. 02. 10.)

28 www.businesswire.com/news/home/20181214005137/en/2018-Open-Source-Intelligence-Market-Global-Analysis (A letöltés dátuma: 2019. 02. 10.)

29 Internet of Things – „dolgok internete”.

30 *Open Source Intelligence (OSINT) Market Research Report – Global Forecast to 2023*, 2018.

31 Web Intelligence.

32 https://homelandsecurityresearch.com/reports/osint-market-national-security-defense-homeland-security-private-sector-public-safety/ (A letöltés dátuma: 2019. 02. 10.)

húzódik meg.[33] Mindez érthető, hiszen a gazdasági élet szereplői jelentős arányban fektetnek be olyan OSINT-képességekbe, amelyekkel hatékonyságukat növelhetik, piaci szerepüket erősíthetik. Vezető szerepet a belbiztonsági szegmens tölt be, míg a katonai és védelmi terület várhatóan a leggyorsabban növekvő szegmens lesz.[34]

- Az adatvédelmi és etikai kérdésekhez fontos megemlíteni, hogy a nyílt forrásokból származó adatok összegyűjtése a jövőben is felszínen tartja az adatvédelmi és jogi kérdéseket.[35] Ennek egyik elemének tekinthető a GDPR általános adatvédelmi rendelet, amely a személyes adatok mentén érinti a kérdéskört. A sokféle nyílt formában elérhető adat „kategóriájában" azonban talán kevésbé tudatosulnak az egyes metaadatként megjelenő, anonim adatokat tartalmazó adathalmazok, amelyek meghatározott szempontú feldolgozást követően akár „értékes" részelemeket is tartalmazhatnak.
- A jövőben a rohamosan fejlődő technikai képességek mentén az OSINT és az azon túlmutató képességek között továbbra is meghatározó marad az a „szürke zóna", amely megfelelő szaktudás és technikai képesség birtokában túlmutathat a nyílt források legális felhasználásának lehetőségén.[36]
- Az álhírek kapcsán felértékelődő kérdés lesz, hogy hogyan lehet kiszűrni a téves/hamis információkat, azok típusától, illetve megjelenési platformjától függetlenül. Az álhírek kapcsán a témakörben áttekintett több forrás is felhívja a figyelmet a hitelesség biztosításának nehézségére, ahol az információmennyiség nagyságrendjéből és összetettségéből adódóan a humán elemzési tényezők mellett különös jelentőségek kaphatnak a jövőben a *mesterséges intelligencia* képességei. A hatalmas mennyiségű, internetes felületen elérhető adathalmazok gépi keresésének, ellenőrzésének során nagyobb valószínűséggel derülhet fény az egyes álhírek ellentmondásaira, segítve ezzel a hitelesség megállapítását.[37] Ugyanakkor szakértők fontosnak tartják[38] a szabadság és emberi jogok, valamint a társadalmat érintő fenyegetések egyensúlya mentén a big data elemzésekhez kapcsolódó OSINT-tevékenység további vizsgálatainak szükségességét is.
- A technológiai környezet fejlődésével, az egyre mélyebb informatikai és adatbázisfeldolgozói ismereteket igénylő OSINT-tevékenység mentén bizonyos szakmai ágak jelentős fejlődés előtt állnak (így például az adatfeldolgozás, -értékelés, -elemzés területei). Mindez azonban a nemzetbiztonsági szervezetek humán erőforrásának fejlesztési igényét is előrevetíti, hiszen „a hírszerzői lehetőségek kihasználását illetően számos szakértő azon a véleményen van, hogy a szolgálatok a megfelelő képzettség hiányában nem képesek az ipar

33 *Open Source Intelligence (OSINT) Market Research Report – Global Forecast to 2023,* 2018.
34 *Open Source Intelligence (OSINT) Market Research Report – Global Forecast to 2023,* 2018.
35 Gibson 2016.
36 Boda–Dobák 2015.
37 www.cobwebs.com/fake-news-challenges-for-osint/ (A letöltés dátuma: 2019. 02. 10.)
38 Staniforth 2016.

által kínált új technikai lehetőségeket felhasználni, például az elemzés, az események követése és a kommunikáció területén".[39]

- A szabadon elérhető szoftverek, valamint azok nyílt környezetben történő fejlesztésének lehetősége a jövőben még inkább lehetővé teszik, hogy a nyíltan elérhető adathalmazok vagy akár adott események OSINT-feldolgozását szabadon bárki elvégezhesse és elemzéseket készítsen.[40] A biztonságért felelős területeken vélhetően erősödni fog az OSINT azon előnye is, miszerint „szabadon hozzáférhető adatok miatt az együttműködés lehetőségét biztosítja külső szakértőkkel".[41]
- Mint Akhgar kifejti a tanulmányában,[42] a big data és az OSINT, illetve a tömeges adatállományok elemzési képessége, a jövőben egyedülálló lehetőséget biztosítanak a biztonsági szolgálatoknak a különböző veszélyek feltárására. Nemzetbiztonsági szempontból a fő cél, hogy az OSINT-megoldások járuljanak hozzá, segítsék a bűnüldöző szervek és a biztonsági szolgálatok információgyűjtési képességeit, támogassák a különböző információkon alapuló döntéshozatalt.[43] Szakértői tanulmány szerzője[44] hívja fel a figyelmet a big data alkalmazásának gondos mérlegelésére és fokozatosságára, hiszen ellenkező esetben (például túlterjeszkedve) az állam és polgárai közötti kapcsolat megromlásához vezethet. Mindez kétségtelenül megköveteli a meglévő hírszerzési modellek, a kapcsolódó rendszerek és folyamatok áttekintését.[45]
- Összességében a kibertérhez köthető nyílt forrásokból történő információgyűjtés jelentősége a jövőben még inkább meghatározó lesz, ide sorolva a 21. század nemzetbiztonsági célú feladatrendszereit és szervezeteit is, ahol a szolgálatok „sajátos szakmaiság mentén egyre kifinomultabb megoldásokkal törekszenek a számukra értékes információk gyűjtésére, elemzésére, értékelésére".[46] Tendenciaként egyrészről a személyiségi jogok további védelme kerülhet előtérbe, másrészről a metaadatként értelmezhető részadatok tömeges, akár mesterséges intelligenciával támogatott feldolgozása nyithat új, eddig ismeretlen területeket. Mint Nihad A. Hassan és Rami Hijazi kifejti könyvében, a jövőben elterjedő IoT-eszközökből származó hatalmas mennyiségű metaadatok bonyolult analitikai megoldásokat igényelnek majd, és „a mesterséges intelligencia és a gépi tanulási technológiák fejlődése ismét átalakítja az OSINT-ot az elkövetkező években".[47]

---

39 Kis-Benedek 2013, 109.

40 www.datasciencecentral.com/profiles/blogs/exploring-the-vw-scandal-with-graph-analysis (A letöltés dátuma: 2019. 02. 10.)

41 Bányász 2012, 157.

42 Akhgar 2016.

43 Az OSINT vs. nemzetbiztosági szervezetek relációban nem feledkezhetünk meg arról sem, hogy az OSINT megközelítése kettős, hiszen egyrészről az információgyűjtési lehetőségek maximális kihasználásában, másrészről a hozzájuk kapcsolható információk védelmében vagy éppen megfelelő alakításában érdekeltek.

44 Staniforth 2016, 18.

45 Staniforth 2016.

46 Boda–Dobák 2015, 22.

47 Hassan–Hijazi 2018, 342.

Felhasznált irodalom

Akhgar, Babak – Bayerl, P. Saskia – Sampson, Fraser eds. (2016): *Open Source Intelligence Investigation, From Strategy to Implementation*. Springer. DOI: https://doi.org/10.1007/978-3-319-47671-1

Bányász Péter (2015): A közösségi média, mint a nyílt forrású információszerzés fontos területe. *Nemzetbiztonsági Szemle,* 3. évf. 2. sz. 21–36.

Bányász Péter (2012): A közösségi média szerepe a 21. század hadseregeiben. *Hadtudomány,* 22. évf. 1–2. sz. 152–161.

Boda József – Dobák Imre (2015): A technikai-műszaki nemzetbiztonsági szolgálatok és feladatok jelentősége a 21. században In: *A nemzetbiztonság technikai kihívásai a 21. században.* Budapest, NKE Szolgáltató Nonprofit Kft. 16–22.

Botz László (2000): A Katonai Felderítő Hivatal feladatai a NATO-csatlakozás után. *Külpolitika,* 6. évf. 1–2. sz. 22–36.

David, Robert – Vivas, Steele (2004): *Special Operation Forces Open Source Intelligence (OSINT) Handbook.* Oakton. OSS International Press.

Gibson, Helen (2016): Acquisition and Preparation of Data for OSINT Investigations. In Akhgar, Babak – Bayerl, P. Saskia – Sampson, Fraser eds.: *Open Source Intelligence Investigation, Advanced Sciences and Technologies for Security Applications*. Springer International Publishing AG. DOI: https://doi.org/10.1007/978-3-319-47671-1_6

Hassan, Nihad A. – Hijazi, Rami (2018): *Open Source Intelligence Methods and Tools, A Practical Guide to Online Intelligence*. Berkeley, Apress Media. DOI: https://doi.org/10.1007/978-1-4842-3213-2

Kis-Benedek József (2013): A nemzetbiztonsági szolgálatok együttműködése. *Hadtudomány,* 23. évf. 1–2. sz. 100–114.

Kleinsmith, Erik (2016): *Fake News and Data Mining: Mapping Today's Media for Intel Analysis*, December 13, 2016. Elérhető: https://inhomelandsecurity.com/fake-news-data-mining-intel/

Lévay Gábor (2006): *OSINT (Open Source Intelligence) – Nyílt információs hírszerzés.* Egyetemi jegyzet. Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem.

McKeown, Sean – Maxwell, David – Azzopardi, Leif (2014): *Investigating People: A Qualitative Analysis of the Search Behaviours of Open-Source Intelligence Analysts*. Regensburg, Germany. DOI: https://doi.org/10.1145/2637002.2637023

Péterfalvy Attila (2015): Néhány gondolat a nyílt információgyűjtés és a személyes adatok védelmének összefüggéseiről. In: *A nyílt információgyűjtés fejlődő területei*. Nemzetközi Tudományos-Szakmai Konferencia Tanulmánykötet. Budapest, Belügyi Tudományos Tanács.

Schaurer, Florian – Störger, Jan (2010): *The evolution of Open Source Intelligence.* OSINT Report 3/2010, International Relations and Security Network (ISN), ETH Zurich. Elérhető: www.research-collection.ethz.ch/bitstream/handle/20.500.11850/25221/eth-2238-01.pdf (A letöltés dátuma: 2019. 02. 10.) DOI: https://doi.org/10.3929/ethz-a-006251404

Staniforth, Andrew (2016): *Open Source Intelligence and the Protection of National Security.* In Akhgar, Babak – Bayerl, P. Saskia – Sampson, Fraser eds.: *Open Source Intelligence Investigation.* Advanced Sciences and Technologies for Security Applications. Springer International Publishing AG. DOI: https://doi.org/10.1007/978-3-319-47671-1_2

Szűts Zoltán (2018): *Online – Az internetes kommunikáció és média története, elmélete és jelenségei.* Budapest, Wolters Kluwer Hungary.

Vadász Pál – Séllei Márton (2017): Az információkeresés magyar jogi környezete. *Hadtudomány,* 27. évf. 1–2. sz. 178–191. DOI: https://doi.org/10.17047/HADTUD.2017.27.1-2.178

Uri László (2012): *A rendőri tanácsadó misszió és a nyílt forrású információgyűjtés.* Elérhető: http://mhtt.eu/hadtudomany/2012/2012_elektronikus/2012_e_Uri_Laszlo.pdf (A letöltés dátuma: 2019. 02. 10.)

Wells, Douglas (2016): Taking Stock of Subjective Narratives Surrounding Modern OSINT. In Akhgar, Babak – Bayerl, P. Saskia – Sampson, Fraser eds.: *Open Source Intelligence Investigation. Advanced Sciences and Technologies for Security Applications.* Springer International Publishing AG. DOI: https://doi.org/10.1007/978-3-319-47671-1_5

Internetes források

Fake News Challenges for OSINT (2018). Elérhető: www.cobwebs.com/fake-news-challenges-for-osint/ (A letöltés dátuma: 2019. 02. 10.)

https://homelandsecurityresearch.com/reports/osint-market-national-security-defense-homeland-security-private-sector-public-safety/ (A letöltés dátuma: 2019. 02. 10.)

Open Source Intelligence (OSINT) Market Research Report – Global Forecast to 2023 (2018). Elérhető: www.marketresearchfuture.com/reports/open-source-intelligence-market-4545 (A letöltés dátuma: 2019. 02. 10.)

The 2018 Open Source Intelligence Market: Global Analysis & Forecast Through 2016–2026 (2018). Elérhető: www.businesswire.com/news/home/20181214005137/en/2018-Open-Source-Intelligence-Market-Global-Analysis (A letöltés dátuma: 2019. 02. 10.)

www.datasciencecentral.com/profiles/blogs/exploring-the-vw-scandal-with-graph-analysis (A letöltés dátuma: 2019. 02. 10.)

www.europarl.europa.eu/news/hu/headlines/society/20181005STO15108/facebook-botrany-tobbet-kell-tenni-az-adatvedelmi-torveny-ervenyre-juttatasaert (A letöltés dátuma: 2019. 02. 10.)

www.marketresearchfuture.com/press-release/open-source-intelligence-market (A letöltés dátuma: 2019. 02. 10.)