NEMZETBIZTONSÁGI SZEMLE
7. évfolyam (2019) 2. szám 3–18. • DOI: 10.32561/nsz.2019.2.1

Solti István[1]

Az OSINT információgyűjtő eszközeiről

About the Information Gathering of OSINT

Az OSINT,[2] függetlenül attól, hogy katonai, polgári vagy üzleti hírszerzésről beszélünk, a mindennapi élet elismert és önálló része, amit valamennyi terület saját igényei szerint használ és alakít. Ebben a tanulmányban a szerző az OSINT hírszerzési ciklusának egyik szakaszát, az adatok és információk begyűjtési fázisát vizsgálja meg, mégpedig a nyílt információforrás és a nyílt információ dinamikáját veszi górcső alá. Ennek eredményeként kimutatja egyes információgyűjtő eszközökről, hogy az OSINT keretében felhasználhatók-e vagy sem, illetve meghatároz olyan magatartási formákat, amelyek az OSINT során nem alkalmazhatók.

Kulcsszavak: OSINT, nyílt információforrás, nemzetbiztonság, adatszerzés, információgyűjtés

The OSINT per se – regardless of whether it is military, civil or business intelligence – is authenticated as the part of life, which is used and formed by all the users according to their needs. In this essay the author scrutinises one part of the OSINT, namely the phase of collecting data and information, or in other words examines the dynamics of open information sources and open information. And as a result, the author presents whether certain information gathering means and methods are allowed or not to be used under OSINT and identifies such course of conducts which cannot be used thereunder.

Keywords: OSINT, open source information, national security, data acquisition, information gathering

[1] Dr. Solti István PhD, jogász. ORCID-azonosító: 0000-0003-4140-7782.

[2] A nyílt forrású információszerzés (Open Source Intelligence) hazai szakirodalom által is használt angol nyelvű rövidítése.

Bevezető

A nemzetbiztonsági és rendvédelmi célú információgyűjtéssel foglalkozó tudományos tevékenységet művelők közösségében általánosan elfogadott, hogy az OSINT az utóbbi évtizedekben a nemzetbiztonsági és a rendvédelmi szolgálatok egyre inkább nélkülözhetetlen információs eszközévé vált.[3] Elismert információgyűjtő eszköz, de túlmutat a hírszerzési, elhárítási, felderítési tevékenységeken, és a civil élet egyes területein is teret követelt magának.[4] Ezen véleményekkel e tanulmány szerzőjeként teljes egészében egyetértek. Tényként kezelem az OSINT kiemelt szerepét és szektorokon átívelő mivoltát. Viszont ehhez azt is szükséges hozzá tenni, hogy már koránt sincs ekkora egyetértés az OSINT lényegét érintő néhány alapvető kérdésben. Érzékelhetően nincs konszenzus például abban, hogy melyek azok az információgyűjtő eszközök, amelyek az OSINT keretein belül felhasználhatók, és melyek azok, amelyek ezeken a kereteken kívül vannak és más típusú információszerzés felségterületére tartoznak. Vagy ahogy Vida Csaba fogalmazott: „Megemlítendő, hogy az OSINT-tevékenység során is felmerülhetnek illegális vagy nem etikus, jogi következményekkel járó mozzanatok. Ilyen lehet például személyek profiljának az engedélyük nélküli feltörése, hozzáférési adataik megszerzése és felhasználása. Az OSINT-területen is figyelembe kell venni a szerzői jogi kérdéseket a megszerzett dokumentumok, fotók stb. felhasználása során."[5] Hogy e kérdésben mennyire eltérő, sőt esetleg egymásnak ellentmondó kutatói vélekedések vannak, elég megnézni a közelmúltban a témában megjelent hazai tanulmányokat, ahol találunk Vida véleményével ellentétes és ezzel egyetértő véleményeket is.[6]

Éppen ezért e tanulmányban arra teszek kísérletet, hogy bemutassam azokat a szempontokat és sarokpontokat, amelyek döntő jelentőséggel vannak az OSINT keretében végrehajtható információgyűjtés határainak meghatározásakor. Jelen keretek között azonban nem vállalkozom arra, hogy az OSINT-tevékenységet végző valamennyi terület (katonai hírszerzés és felderítés, polgári hírszerzés és elhárítás, rendészeti felderítés és bűnüldözési célú felderítés, civil és üzleti hírszerzés stb.)

---

3 Burke 2007

4 Az OSINT a 21. század első évtizedére túlmutat a hírszerzés keretein, és gyakorlatilag valamennyi ágazat (hírszerzés, elhárítás, bűnügyi felderítés, bűnmegelőzés) alkalmazott eszköze lett. Izsa Jenő az OSINT-tal kapcsolatban azt tartotta fontosnak kiemelni, hogy a nyílt forrású információszerzés mindenki számára szabadon elérhető forrásokat használ fel, ezért ez nem klasszikus hírszerzési tevékenység, az itt megjelenő információk szándékosan felkutatott, megkülönböztetett, azonosító adatokkal ellátott, megszűrt információk, amelyek további felhasználásra kerülnek. Izsa 2009, 49.

5 Vida 2013, 104.

6 Jellemző példaként két véleményt ismertetek. A *Hadmérnök* című folyóiratban jelent meg Deák Veronika tanulmánya 2018 szeptemberében, amelyben az OSINT-eszközök között sorolta fel a konspiratív környezettanulmányhoz, a konspiratív figyeléshez hasonló információgyűjtő eszközöket, legenda felhasználását, valamint többek között bemutatta a Shodan nevű kereső alkalmazást, amely „lehetővé teszi a felhasználók számára, hogy különböző szűrőket alkalmazva feltárják az Internethez csatlakozó eszközöket (pl. számítógépeket, okostelefonokat, tableteket, szervereket, webkamerákat és azok videóit stb.), illetve még akár azok tartalmát, részletes adatait, sebezhetőségeit is". Deák 2018, 399. Vida Csabával azonos nézetet képvisel Bányász Péter: „A felhasználók többsége kevésbé érzékeny az adat-és információbiztonságára, így a növekvő internethasználat következtében rengeteg információt gyűjthetünk össze a személyekről […] Fontos azonban hangsúlyozni a tanulmány elején említett kitételt: ez az eljárás nem képezi részét a nyílt forrású hírszerzésnek, hiszen a nyilvánosság elől védett információkhoz is hozzáfér." Bányász 2015, 30.

szempontjait megvizsgáljam, hanem csak két jellemző területre, a magánvállalatok által folytatott, valamint a nemzetbiztonsági és rendészeti szervek által folytatott tevékenységekre koncentrálok.

A vizsgálat elvégzéséhez a fentieken túl további két alapvető szempontot tartok fontosnak kiemelni:

- Az OSINT mindig rendelkezni fog nemzeti jegyekkel, aminek következtében nemzeti szinten önállóan vizsgálható és vizsgálandó.
- Az OSINT önálló és kifejezett szabályozása[7] jellemzően nem történt meg sem demokratikus, sem egyéb berendezkedésű országok esetében. Ezzel párhuzamosan a demokratikus államok jogszabályi szinten kifejezetten szabályozzák az információgyűjtés titkos formáit, valamint a személyes adatok kezelésének lényeges területeit.

Az első szempontot azért fontos kiemelni, mert ennek következtében a témában Magyarországon kívül alkalmazott információszerzési eljárások automatikusan nem ültethetők át, minden esetben helye van a hazai alkalmazási környezethez való illesztésnek. A második említett szempont jelentősége pedig abban áll, hogy a titkos információgyűjtés (a továbbiakban: TIGY) és az információs önrendelkezéshez való jog magyar jogi szabályozása bizony az OSINT eszközrendszerének korlátait jelenthetik.

A rövid bevezető gondolatokat követően a keretek vizsgálatához az OSINT egyes fogalmi elemeit hívom segítségül. Ez esetben azonban nehézséget jelent, hogy egyelőre nem született meg a teljes nemzetbiztonsági és rendvédelmi szféra által elfogadott egységes meghatározás. Tekintettel viszont arra, hogy jelen tanulmánynak nem tárgya az OSINT jelentését önmagában vizsgálni, ezért több, köztük a magyar tudományos diskurzusban elfogadott jelentős nemzetközi szervezet által alkalmazott meghatározásokat és a hazai kutatók fogalmi meghatározásait veszem alapul.

Az OSINT információgyűjtő szakaszáról általában

A NATO OSINT Handbook[8] meghatározása szerint „az OSINT olyan információ, amelyet tudatosan megszereztek, kiválasztottak, kivonatoltak és felterjesztettek egy kiválasztott felhasználó körnek, általában a parancsnok és közvetlen beosztottja számára speciális kérdések megvizsgálása szempontjából. Az OSINT más szóval a hírszerzés bevált eljárási módszereit alkalmazza a sokféle nyílt forrású információ gyűjtése során, amely értesülések megszerzéséhez vezet”.[9]

---

7 Az önálló és kifejezett szabályozás hiányát azért tartom fontosnak hangsúlyozni, hiszen a jogállamok az információs önrendelkezéshez való jog alapjogként való elismerésével és szabályozásával közvetetten az OSINT-tevékenységre is hatással vannak.

8 A NATO OSINT-kézikönyv a nyilvánosság számára szabadon elérhető, 2001-ben publikált kiadvány, amelynek célja, hogy a nyílt forrású hírszerzés tárgyában alapvető oktatási segédlet legyen az egyesített és a szövetséges képzések alkalmával.

9 „OSINT is information that has been deliberately discovered, discriminated, distilled, and disseminated to a select audience, generally the commander and their immediate staff, in order to address a specific question. OSINT, in other words, applies the proven process of intelligence to the broad diversity of open sources of information, and creates intelligence.” NATO 2001, 2.

Az USA-ban a 2006. évi költségvetési évre kiadott Nemzeti Biztonsági Felhatalmazási Törvény szintén tartalmazott egy OSINT-meghatározást,[10] amelyet azt követően több dokumentum is irányadónak fogadott el. Irányadónak fogadta el a Nemzeti Hírszerző Igazgató által a nyílt forrású információszerzésről megjelentetett 301. számú direktíva,[11] vagy a *Második Generációs Nyílt Forrású Hírszerzés (OSINT) meghatározása a Védelmi Vállalkozások számára* című kiadvány.[12] E dokumentumok szerint az OSINT keretében kizárólag nyilvánosan elérhető információk gyűjthetők és hasznosíthatók, ahol a nyilvánosan elérhető információk alatt azok az információk értendők: „amihez bárki jogszerűen hozzáférhet akár kérés, vásárlás vagy egyszerű észlelés útján".[13]

A NATO-definíciótól eltérő terminológia található a témával foglalkozó Lévay Gábor és Vida Csaba magyar kutatók tanulmányaiban. A nyílt forrású információszerzés Lévay Gábor szerint: „A katonai felderítés és hírszerzés rendszerén kívül létező, a publikum (tehát minden egyén) számára nyilvánosan, legális eszközökkel megszerezhető, vagy korlátozott körben terjesztett, de nem minősített adatok szakmai szempontok alapján történő felkutatását, gyűjtését, szelektálását, elemzését-értékelését és felhasználását jelenti."[14] Tartalmi elemeit tekintve az OSINT hasonló meghatározását adja Vida Csaba is, aki szerint „az OSINT-tevékenység: az önálló nyílt adatszerző tevékenység valamely személy vagy szervezet által közzétett, nyilvánosan, legális eszközökkel megszerezhető vagy korlátozott körben terjesztett, de nem minősített adatoknak a hírszerzési igények kielégítésére, speciális módszertan alapján történő felkutatását, gyűjtését, szelektálását, értékelését és felhasználását jelenti".[15]

Ha a fent hivatkozott megfogalmazásokat egymással összevetjük, akkor az eltérő fogalmazásbeli különbségek mellett egy lényeges tartalmi különbséget fedezhetünk fel. Az USA-dokumentumok a hírszerző eljárások tárgyaként hangsúlyosan a *nyílt forrású információt* nevezik meg, függetlenül attól, hogy egyébként az információ maga képez-e bármilyen titkot, míg a nyílt információforrás Lévay és Vida szavai szerint: a közzétett, vagyis a publikum számára nyilvánosan, legális eszközökkel megszerezhető, vagy ugyan korlátozott körben terjesztett, de nem minősített információforrásokat jelenti. Az említett magyar elemzők ezzel az angolszász irodalomban alkalmazott kereteket valamelyest korlátozzák, hiszen nem elégednek meg a forrás nyilvános minőségével, hanem az információ nyílt jellegét is hangsúlyozzák. Vagyis az információ nem lehet *minősített.* De, hogy mégis mit tekinthetünk nyílt információforrásnak,

10 „Open-source intelligence (OSINT) is intelligence that is produced from publicly available information and is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement." National Defense Authorization Act for Fiscal Year 2006, 3411.

11 ODNI 2006, 8.

12 Williams–Blum 2018, 8.

13 „Open Source Information: Publicly available information that anyone can lawfully obtain by request, purchase, or observation." ODNI 2006, 8.

14 Lévay 2006, 6.

15 Vida 2013, 101.

arról a hivatkozott dokumentumokban csak általános felsorolásokat és szélesen értelmezhető megfogalmazásokat találhatunk.[16]

A nyílt információs források mint az OSINT forrásai

Az alábbiakban megvizsgálom azokat az információforrásokat, amelyek az OSINT esetében megjelennek, ehhez pedig a NATO kézikönyv felsorolását veszem alapul. A NATO kézikönyv nyílt információforrásként a következőket sorolja fel:[17]

- *Hagyományos média:* A sajtótermékeket, sugárzott televízió- és rádióadókat jelenti, függetlenül attól, hogy a média hozzáférése vezetékes vagy sem, fizetős vagy ingyenes, online elérhető vagy kizárólag hagyományos elérési módjai vannak. Ide sorolja a kézikönyv azon médiumok szolgáltatásait is, amelyek nemcsak saját készítésű híranyagokat szolgáltatnak, hanem más médiumok anyagaiból úgynevezett sajtószemléket készítenek. Mára a NATO-kézikönyv kiadásakor ismert hagyományos média jelentősen átalakult, lényegesen nagyobb súllyal vannak jelen az online térben elérhető médiatartalmak. Újabb platformok jöttek létre, mint például a blog, a vblog, a kép- és videómegosztók, illetve a közösségi média egyéb területei, amik az információforrás szintjén elmossák a határokat a média és az internet között. Viszont – bármelyik platformon is történik a médiamegjelenés – közös jellemzőjük, hogy akik közzéteszik, azok újságként, folyóiratként, televízióként, rádióként, illetve újságíróként, médiamunkásként határozzák meg magukat. Úgy vélem, hogy a hagyományos média termékeinek a felhasználása mélyebb értelmezésbeli kérdéseket nem vet fel. Ezen sajtótermékek egyértelműen a nyilvánosságnak szólnak még azokban az esetekben is, amikor a felhasználói kör valamilyen módon (például előfizetéshez kötött, szakmai szervezet tagjai számára elérhető stb.) korlátozott. Problémaként talán a ritka, néhány példányban létező sajtótermék legális módon történő megszerzése, valamint a zárt közösség számára biztosított tartalmak megszerzése jöhet elő, de ezeket a kérdéseket a következő forrásoknál részletesen tárgyalom.
- *Internet:* A kézikönyv keresőfelületként és elérési lehetőségként határozza meg. Az online közösségi média térhódításával napjainkra az OSINT számában és minőségében is jelentős információforrásokhoz jutott, elegendő, ha csak végigböngésszük az eszközök és erőforrások felsorolását tartalmazó kézikönyvet.[18]

---

16 „Open Source Data (OSD). Data is the raw print, broadcast, oral debriefing or other form of information from a primary source. It can be a photograph, a tape recording, a commercial satellite image, or a personal letter from an individual." ODNI 2006, 2. „Open Source Information (OSIF). OSIF is comprised of data that can be put together, generally by an editorial process that provides some filtering and validation as well as presentation management. OSIF is generic information that is usually widely disseminated. Newspapers, books, broadcast, and general daily reports are part of the OSIF world." NATO 2001, 2.

17 NATO 2001, 5–11.

18 Open Source Tools and Resources Handbook, 2018.

Az internet esetében fontos hangsúlyozni, hogy a nyilvános adatokon és tartalmakon túl számos olyan tartalom, adat és adatbázis érhető el, amelyeknél alapesetben nem, vagy csak pontosan meghatározott jogosulti kör számára biztosított a hozzáférés, illetve vannak olyan adatok, amelyek az online térben különböző technikák alkalmazásával elérhetők, de az adatok gazdái azokat nem a nyilvánosságnak szánják. Éppen ezért az internetnek mint OSINT-információforrásnak a használata már jóval több értelmezési kérdést vet fel. Például a) meg lehet-e támadni egy online adatbázist olyan adatokért, amelyek az általános felhasználók számára nem állnak rendelkezésre; b) már megszerzett hozzáférési jogosultsággal be lehet-e lépni valakinek a profiljába; vagy c) felhasználható-e egy álprofil adatok megszerzésére?

Ha ezeket a példákat mélyebben megvizsgáljuk, akkor az OSINT lehetséges információgyűjtő eszközeinek több korlátjára, így a médiánál felvetett problémára is magyarázatot kaphatunk.

a) A mindennapokban használt számítógépes alkalmazásoknak több-kevesebb biztonsági hibáik vannak. A biztonsági hibák egy részét már feltárták, egy másik részét majd csak később teszik meg, és minden bizonnyal lesznek olyan biztonsági hibák, amelyeket soha nem tárnak fel. A biztonsági hibák azt jelentik, hogy az alkalmazások, valamint az informatikai rendszerek által kezelt adatok a biztonsági hibát ismerők által elérhetők és megszerezhetők. A feltárt biztonsági hibák egy része nyilvánosan megismerhető, leírásuk elolvasható, hozzáértő által fel-, illetve kihasználható. Ezenkívül vannak olyan feltárt biztonsági hibák, amelyek nem kerülnek nyilvánosságra, csupán egy szűk kör ismeri és használja őket. A biztonsági hibák kihasználásával a hacker a megtámadott alkalmazás vagy számítógépes rendszer nem nyilvános területeihez fér hozzá, amelyekből akár személyes, akár szervezeti, akár az informatikai rendszerre vonatkozó belső adatokat szerezhet meg. Mindezt pedig egyébként *nyilvános* ismeretek birtokában teszi. Mindent összevetve azt mondhatjuk, hogy a hackingmódszerek[19] felhasználásával történő adatszerzés egy olyan célzott, előre eltervezett aktív és jogosulatlan tevékenység, ahol a hacker szándékoltan olyan adatokat szerez meg, amelyeket az adatgazda nem tárt a nyilvánosság elé. Hogy az ezúton történő adatszerzést besoroljuk, a vonatkozó EU-s és hazai jogszabályokat veszem alapul.

Az Európai Parlament és a Tanács által *Az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról* címmel kiadott 2013 / 40 / EU irányelv határozottan kijelenti, hogy az egyes információs rendszerekhez való jogosulatlan hozzáférés az EU területén bűncselekménynek minősül, és a tagállamok ennek megfelelően kötelesek jogrendszerüket kialakítani.[20] E szemléletet követi a magyar Büntető Törvénykönyv is, amely szerint bűncselekményt követ el az, aki információs rendszerbe az információs rendszer védelmét biztosító technikai intézkedés megsértésével vagy kijátszásával belép.[21] Amellett, hogy a magyar jog a jogosulatlan belépést általánosságban tiltja, vannak olyan pontosan meghatározott állami szervezetek, amelyek számára törvényi felhatalmazással, TIGY keretében lehetővé

[19] Hackingmódszereknek azokat az alkalmazott támadási technikákat nevezhetjük, amelyek segítségével a hacker megtalálja és kihasználja az informatikai ezközök és rendszerek sebezhetőségét.

[20] 2013/40/EU irányelv (8) pont.

[21] Btk. 422. §.

is teszi azt.[22] Tekintettel az OSINT és a TIGY viszonyára, fogalmilag kizárt, hogy mind a két információszerző mód alkalmazza ugyanazt az információszerző eszközt, amiből pedig az következik, hogy az OSINT során nem használható hackingmódszereket alkalmazó eszköz.

A jogi környezet alapján tehát azt láthatjuk, hogy az EU-ban – és így Magyarországon is – az információs rendszerekbe történő jogosulatlan behatolás az állam által üldözendő magatartásnak minősül. Legálisan ilyen tevékenységet kizárólag az erre direkt felhatalmazott szervezetek, külön felhatalmazás alapján, TIGY keretében folytathatnak.

b) Ismeretlenek online elérhetővé tettek egy adatbázist, amely sok millió felhasználó e-mail-hozzáférési adatait tartalmazza. A listában lévő belépési adatokkal az érintett tudta és beleegyezése nélkül bárkinek a személyes postafiókjába be lehet lépni és a levelezését meg lehet szerezni. Sőt, vannak olyan szolgáltatók (mint például a Google), akiknél a levelezésen túlmenően sokkal többféle információ (saját készítésű képek és videók, hónapokra visszamenőleg tartózkodási adatok, véletlenszerűen rögzített hanganyagok, levelezési és címlisták, egyéb, a felhőszolgáltatásba feltöltött dokumentumok, naptárbejegyzések stb.) található egyetlen fiókba történő belépésnél. A felhozott példa esetében nem is csak egy, hanem két adatszerzéssel kapcsolatos kérdés is felmerül:

1. Vajon harmadik személy által nyilvánosságra hozott személyes adat (hiszen a hozzáférési adat személyes adatnak minősül) bárki által jogszerűen megszerezhető és kezelhető?
2. Vajon a megszerzett hozzáférési adat felhasználható információszerzésre az OSINT keretében?

Az első kérdésre adandó válasznál jelen tanulmány keretei között nem kívánom valamennyi lehetséges esetet önállóan megvizsgálni, csupán két alapesetet – magántársaságot, illetve állami hírszerző, elhárító és felderítő szervet – vizsgálom meg.

Az Alaptörvény II. cikke szerint az emberi méltóság sérthetetlen, ezért alkotmányos szinten védelem illeti meg az egyén magán- és családi életét, a személyes kapcsolatrendszerét, az otthonát és jó hírnevét.

A védelmi rendszer legfelső szintjén nemzetközi egyezmények (például Európai Unió Alapjogi Kartája) állnak, nemzeti szinten az Alaptörvény, az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (Infotv.), valamint egyes ágazati törvények adatkezelési rendelkezései találhatók. A személyes adatok védelmét biztosító többszintű rendszer megfelel a törvényesség és a hátrányos megkülönböztetés kívánalmainak, szem előtt tartja a szükségesség és az arányosság követelményeit, illetve biztosítja a bírósághoz és más független szervhez történő fordulás lehetőségét.

A legmagasabb szinten az Alaptörvény kimondja a személy beazonosítására alkalmas és személyiségéhez tapadó adatok nyilvánosságának általános tilalmát. Eszerint személyes adataival mindenki maga rendelkezik, és alapvetően maga dönt

[22] Nbtv., Rtv., Be., NAV tv. Ütv.

azok megismerhetőségéről, vagy jogszabály rendelkezhet egyes személyes adatok mások által történő kezeléséről. Az Alaptörvény rendelkezéseit részletezve az Infotv. megadja a különböző típusú személyes adatok meghatározását, definiálja és részletezi az adatkezelés szabályait és deklarálja az alapelveit. Ezenkívül meghatározza, hogy milyen felhatalmazással kezelhető személyes adat: személyes adatot kezelni kizárólag az érintett hozzájárulása, törvény vagy helyi önkormányzati rendelet felhatalmazása, az érintett hozzájárulását átmenetileg pótló törvényi felhatalmazás vagy az érintett vélelmezett hozzájárulása alapján lehet.

Tekintettel arra, hogy magántársaságok esetében a személyes adatok kezelésének egyik jogalapja sem áll rendelkezésre az OSINT égisze alatt, ezért már a személyes adatok kezelésének eddig bemutatott legalapvetőbb ismérvei alapján is megállapítható, hogy egy hozzáférési jogosultságot megszerző magánszemély jogszerűen nem kezelheti, vagyis még csak nem is rögzítheti és semmilyen formában nem használhatja fel azt, így be sem léphet vele más személyes fiókjába.

Második alapesetben az OSINT-tevékenységet végző állami hírszerző, elhárító és felderítő szerveket vizsgálom, amihez a tevékenységüket szabályozó törvényeket kell alapul venni. Hiszen, ha a rájuk vonatkozó ágazati törvény tevékenységük végzéséhez felhatalmazza a hatóságokat harmadik személy személyes adatainak kezelésére, akkor a hozzáférési adatokat megszerezhetik és kezelhetik. A nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény (Nbtv.) az adatkezelés szabályai között felhatalmazza a magyar szolgálatokat a személyes adatok kezelésére, és meghatározza az adatok beszerzésének módjait is.[23] Eszerint a szolgálatok adatokat szerezhetnek be nyílt forrásból történő adatgyűjtéssel. Ebből pedig az következik, hogy a szolgálatok az interneten talált hozzáférési jogosultságokat rögzíthetik és kezelhetik. Viszont az nem következik, hogy OSINT keretében további információgyűjtésre használhatnák fel, éppen ellenkezőleg. Az Nbtv. későbbi rendelkezéseiből ugyanis az olvasható ki, hogy kizárólag TIGY során léphetnek be vele felhasználói fiókba és használhatják információszerzésre, mivel az Nbtv. külső engedélyhez kötött TIGY keretében jogosítja fel a szolgálatokat arra, hogy információs rendszerben kezelt adatokat titokban megismerjenek és az ott észlelteket technikai eszközzel rögzítsék.[24]

Mindezek szellemében az állapítható meg, hogy Magyarországon alapesetben felhasználói adatok nem használhatók fel további információszerzésre OSINT keretében, hiszen a példánkban az e-mail-fiókba történő belépéskor és a levelezési adatok megismerésekor már hiányzik a nyílt forrású információgyűjtés alapvető feltétele: a nyílt információforrás. Azzal, hogy a szolgálat nyílt forrásból szerezte meg a hozzáférési jogosultságot, csupán az információhoz való hozzáférés egyik lehetséges módja nyílt meg előtte, a forrás minősítése nem változott, az továbbra is zárt maradt. Ennek következtében azok a szervek, amelyek TIGY végrehajtására törvényi felhatalmazás hiányában nem jogosultak, vagy ugyan jogosultak, de az adott ügyben nem folytatnak jogszerűen TIGY-t, nem léphetnek be az e-mail-fiókba és nem ismerhetik meg annak tartalmát. Viszont azok a TIGY végrehajtására felhatalmazott szervek, amelyek adott

[23] Nbtv. 38. §.
[24] Nbtv. 56. § e) pont.

esetben jogosultak az információs rendszerben kezelt adatokat titkosan megismerni, TIGY keretében elvégezhetik az adatgyűjtést.

c) A harmadik példánkban az információgyűjtéssel érintett személy Facebookon folytatott tevékenységét szeretné valamely szerv figyelemmel kísérni. Az érintett a Facebookon a mindenki számára nyilvános felület mellett általa létrehozott privát helyszíneket is használ. Kérdés, vajon meddig terjednek az OSINT lehetőségei: csak a nyilvános felületeken megadott információk begyűjtésére, vagy valamennyi felület információinak megszerzésére. Ennek érdekében vajon létrehozható egy álprofil és hozzá kapcsolódó legenda, akinek jelentkezését az érintett elfogadja a privát helyszínekre is?

Megítélésem szerint a b) pontnál bemutatott jogi környezet ebben az esetben is meglehetősen pontos utasítást ad arra, hogy közösségi felületeken meddig folytatható a nyílt forrású információgyűjtés, és mi az, ami már a TIGY területére tartozik. Az előző példában bemutatott okfejtéshez képest ez esetben az a lényeges különbség, hogy az Nbtv. egy másik jogszabályi rendelkezése alapján lehet álprofil és legenda alkalmazásával információhoz jutni. Míg az előzőnél egy külsőengedély-köteles titkos információszerző eszköz alkalmazása történik, addig a mostani példa esetében egy külső engedélyhez nem kötött titkos információgyűjtő eszköz felhasználására kerül sor.[25]

Mindezek következtében egyetértek Vida Csaba azon megállapításával, miszerint: „A közösségi oldalak a nyílt információszerzés új, de a kiberadatszerzéssel határos területe, mert abban az esetben, ha a hírszerzés már megtévesztő, esetenként legendával alátámasztó megtévesztő információkkal folytat keresést, akkor az már nem nyílt, hanem műveleti adatszerzés."[26]

A fent bemutatott három eset alapján összefoglaltan az állapítható meg, hogy az internet alapvető OSINT-forrásként való megjelölése nem vitatható, azonban az online térben automatikusan nem alkalmazható minden információgyűjtő eszköz az OSINT során. Nem tartoznak az OSINT területére azok az információgyűjtő tevékenységek, amelyeknél

- hackingeszközök felhasználásával,
- megszerzett jogosultságok felhasználásával vagy
- szándékolt, az érintett megtévesztését célzó magatartás tanúsításával történik információszerzés.

- *Az online kereskedelmi szolgáltatók:* Kereskedelmi alapon nyújtanak online válogatott és rendszerezett tartalmakat az előfizetőik számára. Az online kereskedelmi szolgáltatóknak számos formája létezik, a NATO-kézikönyv több fontos szolgáltató felhasználási lehetőségeit is leírja.[27] Lényeges ismertetőjük, hogy az általuk létrehozott tartalmakat és adatbázisokat ellenszolgáltatás fejében biztosítják

[25] Nbtv. 54. § (1) A titkos információgyűjtés keretében a nemzetbiztonsági szolgálatok
a) […]
b) a nemzetbiztonsági jelleg leplezésével információt gyűjthetnek.

[26] Vida 2013, 107.

[27] Vida 2013, 6–9.

partnereik számára. A szolgáltatás nem feltétlenül működik online, előfordulhat, hogy digitális adathordozón vagy egyéb elektronikus módon és úton juttatják el az információkat az ügyfeleik részére.

Ahogy Lévay Gábor bemutatja, ebbe a körbe olyan szolgáltatók tartoznak, amelyek jellemzően egy-egy szakterületre szakosodtak. A szakterületek rendkívül széles skálán mozoghatnak, kezdve a biztonságpolitikától a gazdasági és pénzügyi elemzéseken át egészen az energiabiztonságig. Termékeik mögött az adott témában komoly szakmai ismeret és tevékenység húzódik. Példaként a Stratfor[28] és a Jane's[29] cégeket említi, amelyek szolgáltatásai között szerepel komplett értékelések-elemzések és prognózisok készítése, jól strukturált kereshető adatbázisok biztosítása.[30]

Önmagában az online kereskedelmi szolgáltatók OSINT-információs forrásként történő felhasználása alapvető információszerző módszertani kérdést nem vet fel, csupán egyetlen esetben merülhet fel a hovatartozás kérdése. Akkor, ha egy szolgálat HUMINT keretében álcázott személy útján, az online kereskedelmi szolgáltatót a partner személyében megtévesztve szerzi meg a terméket. Ezt az esetet azonban később, az interjúztatás témakörében részletezem.

- *A szürke irodalom:* Olyan nyílt információkat tartalmazó dokumentumokat takar, amelyek egy jól meghatározott szűk kör számára készülnek, a széles nyilvánosság felé nem feltétlenül publikálják őket. Ide sorolhatók az akadémiai értekezések, disszertációk, bizottsági beszámolók, konferenciaanyagok, technikai jelentések és technikai szabványok, vitairatok, előnyomatok, kormányzati beszámolók, hírlevelek, üzleti vagy piaci előrejelzések, kutatási beszámolók, fordítások, úti beszámolók, munkaanyagok stb. A legtöbb szürke irodalom kategóriájába tartozó információgyártó szervezet a nemzeti kormányok és kormányzati szervek, a politikai pártok, a kutatóintézetek, egyetemek, akadémiák, valamint a kereskedelmi társaságok.[31]

  Az előző ponthoz képest a szürke irodalom esetében azt lehet mondani, hogy az információ előállításának és publikálásának módja okán már több módszertani kérdés vethető fel. Elsősorban az, hogy van-e a publikált terméknek nyilvános elérési módja, vagy csupán jól körülhatárolt felhasználói kör számára publikált. Utóbbi esetben ugyanis a kereskedelmi szolgáltatóknál is megemlített probléma merül fel, amelyet a későbbiekben fogok tárgyalni. Másodsorban a dokumentum minőségi problematikáját is meg kell vizsgálni, hiszen az így készült tartalmak egy jelentős része valamilyen – még akkor is, ha ez egyébként nincs a tartalmon egyértelműen feltüntetve – titkot képezhet vagy védendő személyes adatot tartalmazhat. A titok kérdéskörét szintén e tanulmány későbbi részében vizsgálom meg.

---

28 A Stratfor egy amerikai geopolitikai magán hírszerző platform és kiadó, amelyet 1996-ban alapítottak meg Austinban. Elérhető: www.stratfor.com/ (A letöltés dátuma: 2019. 04. 02.)

29 A Jane's Information Group egy katonai, repülési és közlekedési témákra szakosodott brit kiadó. Elérhető: www.janes.com/ (A letöltés dátuma: 2019. 04. 02.)

30 Lévay 2004, 54.

31 Lévay 2004, 55.

- *A szakértők és megfigyelők:* A szakértők és megfigyelők esetében az OSINT-irodalom több forrást is megjelöl, úgymint a szakértők és megfigyelők személyes tapasztalatai alapján készített leírásokat, beszámolókat és a tapasztalásaikról szóló személyes interjúkat. Mindezek a források addig nem is vetnek fel problémát, amíg nyilvános forrásból elérhetők, viszont amint már valamilyen, az előzőkénél is említett korlátozás áll fenn, akkor az ott felvetett módszertani probléma itt is jelentkezik. Sőt, külön szükséges kiemelni az interjúztatás kérdését, hiszen egészen más megvilágításban jön elő a nemzetbiztonsági hírszerző, elhárító és felderítő szolgálat, és egészen másként a gazdasági társaságok esetében.

  Az utóbbi megteheti, hogy nyíltan, magát megnevezve, akár a célját is felfedve megkeresi a szakértőt és átveszi vagy megveszi a tapasztalatait. A nemzetbiztonsági szolgálatok esetében azonban a szakértő interjúztatása valamilyen szervezeti kapcsolat nélkül meglehetősen valószínűtlen, ezért az információgyűjtés könnyedén átcsúszhat a leplezett vagy titkos oldalra. Mindez abból következik, hogy egy nemzetbiztonsági szolgálat többféleképpen építhet ki kapcsolatot olyan személlyel, aki nem érintettje a vizsgált eseménynek, hanem csak szakismerete okán bír értékes tudással. Megtörténhet, hogy a kapcsolatfelvételnél a szolgálat:
  - titkolja kilétét és titkolja célját,
  - titkolja kilétét, de nem titkolja célját,
  - nem titkolja kilétét, de titkolja célját,
  - nem titkolja kilétét és nem titkolja célját.

  Megítélésem szerint az első két esetben bármilyen kapcsolaton keresztül is történik az interjú elkészítése, nem beszélhetünk OSINT-ról. A szolgálat ugyanis leplezi nemzetbiztonsági jellegét, ami az Nbtv. 54. § (1) bekezdés b) pontja értelmében külső engedélyhez nem kötött titkos információgyűjtő eszköz. A harmadik esetben az ügynökség szintén alkalmaz valamilyen legendát, amivel megtéveszti és tévedésben tartja az interjúalanyt, ráadásul a szolgálat felvilágosítást kér, ami pedig az a) bekezdés értelmében minősül külső engedélyhez nem kötött titkos információgyűjtésnek. Valószínűleg ebben az esetben jogosan felvethető, hogy a hatályos törvényi rendelkezések helyesen sorolják-e ezen tevékenységet a TIGY keretében alkalmazható információgyűjtő eszközök közé, hiszen a mindennapi élethez szorosan kapcsolódó, számtalanszor előforduló természetes viselkedési formáról van szó. A negyedik esetben sem egyértelmű, hogy nyílt forrású információszerzésről beszélhetünk-e. Ebben a szituációban fontos szempont az interjúalany és az ügynökség viszonya. Amennyiben kettőjük között bármilyen szervezetszerű kapcsolat áll fenn, vagyis az interjúalany az ügynökség valamilyen rendű kapcsolata, akkor az egyértelműen a TIGY körébe tartozik.[32] Ha viszont az alannyal semmilyen szervezetszerű kapcsolat nem áll fenn, az interjúztató személyével és céljával sincs tévedésben, akkor is ott van a felvilágosításkérést TIGY-nek minősítő törvényi szakasz. Ebben az esetben az információgyűjtés minősítését már az döntheti el, hogy az interjúztatás tényéről harmadik személy tudomást szerezhet-e, vagy az interjúalany köteles azt titokban tartani.

[32] Nbtv. 54. § (1) bekezdés c) pont.

Az interjúztatás apropóján leírtak alapján a magyar nemzetbiztonsági szolgálatok és a források kapcsolatainál eddig felvetett problémákra együttesen vonható le következtetés. Mégpedig az, hogy az információforrással legenda felhasználásával való személyes kapcsolat kialakítása és valakinek az interjúztatása az Nbtv. hatálya alá tartozó szervek esetében egy-két egyedi kivételtől eltekintve TIGY keretében alkalmazható információgyűjtő eszköz.

- *A kereskedelmi műholdak felvételei:* Mára a katonai műholdak mellett egyre több kereskedelmi műhold is működik, amelyek felvételei bárki számára elérhetőek, aki megfizeti. E tekintetben a nemzetbiztonsági szolgálatok esetében ismét a hogyanra adott válasz lehet a vízválasztó.

A NATO-kézikönyvben felsorolt OSINT-forrásokat a tudomány magyar művelői továbbiakkal egészítik ki. Forrásnak minősítik a nyomtatott kiadványokat, az oktatási intézményeket, az újságírókat, a nyelviskolákat, az üzleti életet, a nemzetközi szervezeteket, a nem kormányzati szervezeteket és a már említett közösségi oldalakat,[33] valamint ezeken is túlmenően a helyszíni előadásokat, konferenciákat, a tudományos kutatószervezeteket, a könyvtárakat és az információbrókereket.[34] Ezek számbavétele során azt láthatjuk, hogy az alkalmazható információszerző eszközök meghatározása a fenti forrásoknál bemutatott elhatárolásokkal analóg módon tehető meg. Valamennyiüknél megtalálhatók azok a produktumok és termékek, amelyek – legyen az akár valamelyest korlátozott is – a nyilvánosságra hozás szándékával, vagy a nyilvánosság számára készülnek. Azonban szinte mindegyik esetében lehet olyan produktumokat említeni, amikor az információhoz való hozzájutás módja miatt nem lehet egyértelműen kijelenteni, hogy ezektől a forrásoktól minden megszerezhető OSINT során. Például ezen területek online elérhető adatait csak addig a pontig tekinthetjük az OSINT számára felhasználhatónak, ameddig az valóban legális eszközökkel történik. Vagyis – ahogy azt az internetnél bemutattam – az online térben ez azt jelenti, hogy a világhálóra a nyilvánosságra hozás szándékával feltett információk begyűjtése érdekében bármilyen eszköz, szolgáltatás, keresőmotor stb. felhasználható. Mindaddig, amíg a szolgálatok nem alkalmaznak megtévesztést, kerülik a hackingeszközöket és – új szempontként említem – tiszteletben tartják a szerzői jogokat. Ezen forrásoknál is érvényes, hogy egy megtévesztéssel megszerzett hozzáférési jogosultsággal folytatott információgyűjtés már a titkos kategóriába tartozik, hasonlóan a malware-rel történő adatlopáshoz.

A nyílt információ mint az OSINT-tevékenység kizárólagos tárgya

Az OSINT fogalmának második lényeges ismérve a forrás mellett a hazai tudományos diskurzusban a nyílt információ. Azért tartom lényegesnek ennek hangsúlyozását, mert az angolszász irodalom ezzel szemben megelégszik azzal, hogy az információ nyílt forrásból származzon. Ahogy viszont az OSINT jellemzőinek bemutatásakor is

[33] Vida 2013, 105.
[34] Lévay 2004.

kiemeltem, a hazai meghatározás azt is kiköti, hogy az információ nem lehet minősített adat. Ebben a fejezetben azt fogom megvizsgálni, hogy ennek a fogalmi elemnek a hazai OSINT esetében valóban van-e relevanciája, vagy esetleg elhagyható lenne.

A minősített adat fogalmát jelenleg a minősített adat védelméről szóló 2009. évi CLV. törvény határozza meg. A törvény a minősített adat két formáját ismeri. Nemzeti minősített adatnak tekintendő a minősítői joggal rendelkező személy által beminősített adat. A minősítés szükséges feltétele, hogy a minősítő a minősített adat adathordozóját a törvényben előírt alaki kellékekkel lássa el. Ezenkívül a törvény ismeri a külföldi minősített adatot, amely alatt az EU valamennyi intézménye és szerve, továbbá az EU képviseletében eljáró tagállam, a külföldi részes fél vagy nemzetközi szervezet által készített és törvényben kihirdetett nemzetközi szerződés vagy megállapodás alapján átadott olyan adatot értünk, amelyhez történő hozzáférést az EU intézményei és szervei, az EU képviseletében eljáró tagállam, más állam vagy külföldi részes fél, illetve nemzetközi szervezet minősítés keretében korlátozza.

Mint látható, a minősített adat alatt viszonylag jól körülhatárolt adathalmazt értünk, amelyet vagy erre feljogosított magyar szervek, vagy külföldi államok – jellemzően, de nem kizárólag EU- és NATO-tagállamok – szervei láttak el minősítéssel. A minősített adatot csak az szerezheti és ismerheti meg, akinek erre a minősítő vagy törvény felhatalmazást ad. A hazai jog a minősített adat jogosulatlan kezelését és megszerzését szankcionálja, jogosulatlan kezelését szabálysértésnek,[35] míg jogosulatlan megszerzését és felhasználását bűncselekménynek minősíti.[36]

Tekintettel arra, hogy a minősítő nagy eséllyel nem biztosít megismerési jogosultságot az OSINT-tevékenységet végző magántársaságoknak, illetve törvényi szinten sem lehető fel erre vonatkozó felhatalmazás, továbbá még az Nbtv. sem tartalmaz a nemzetbiztonsági szolgálatoknak szóló, erre vonatkozó általános felhatalmazó rendelkezéseket, ezért minősített adat bárki által történő megszerzése, még ha az nyílt forrásból is történik meg, jogszerűtlen magatartásnak minősül. Ehhez azonban azt is fontos hozzátenni, hogy az állítás csak abban az esetben igaz, ha az adat adathordozóján egyértelműen megtalálhatók a minősítés alaki kellékei. Ezek hiányában, ami azért például egy digitális adathordozón fellelhető adat esetében korántsem elképzelhetetlen, nem derülhet ki egy adatról, hogy az minősített-e vagy sem.

De vajon mi a helyzet azokkal a *minősített adatokkal,* amelyeket a magyar jog nem ismer el minősített adatnak, és így megszerzését, felhasználását és kezelését nem szabályozza és nem is szankcionálja? A kérdésben a válasz is megtalálható. Mivel a magyar jog nem ismeri el minősített adatnak, ezért a hatálya alá tartozó személyek és szervezetek tekintetében sem minősül minősített adatnak. Ennek következtében jogi védelemben nem részesül, vagyis bárki által szabadon gyűjthető. Viszont, ha ez kiderül, akkor azért az adatforrás országát a későbbiekben érdemes elkerülni, hiszen nagy valószínűséggel az adat a hazaihoz hasonló szintű védettséget élvezett az adott államban.

A minősített adatokon kívül vannak olyan adatok, amelyek valamilyen széles körben elfogadott társadalmi norma alapján bizalmasnak vagy titkosnak számítanak.

35 Szabstv. 206. §.
36 Btk. 265. §.

„[Minden] olyan ismeret, ami csak egy adott személyi kör számára áll rendelkezésre, és amit azok, akik a birtokában vannak, igyekeznek kisajátítani, mások számára hozzáférhetetlenné tenni (különböző titokvédelmi rendszabályok alkalmazásával). Az információt birtokló, azt a saját érdekében felhasználni kívánó csoport szempontjából a »kívülállók« illetéktelennek számítanak, nem jogosultak az adott információ megismerésére és felhasználására."[37] Ide tartozónak tekinthetjük például a foglalkozásokból eredő titkokat (ügyvédi, üzleti, orvosi és gyónási titok stb.), valamint az egyes emberi viszonyokból eredő titkokat (hitéletbeli, biztosítási, szerződési, üzleti titok stb.). Titkosnak tekinthetők továbbá a személyes adat és a különleges adat, amelyek közvetlen jogi védelem alatt állnak. A titok alapból feltételezi, hogy nyílt forráson nem található meg, vagyis csak illegális eszközökkel beszerezhető. A titok viszont csak addig lesz titok, amíg azt birtokosa direkt akarattal vagy egyszerűen csak hanyagságból nem teszi illetéktelenek számára elérhetővé. Ha valaki például a betegségével kapcsolatos adatokat kiteszi egy közösségi oldal mindenki által elérhető felületére, vagy nyilvános blogon tesz fel egy bizalmas szerződésével kapcsolatos konkrét kérdést, vagy gazdasági társaság bizalmas üzleti szerződést tesz elérhetővé honlapján, akkor az így megadott információk az OSINT szempontjából nyílttá válnak és az OSINT tárgyai lehetnek.

Összefoglaló gondolatok

Az OSINT információszerző szakaszával kapcsolatban az eddig kifejtettek alapján összegzésképpen azt mondhatjuk, hogy önmagában nem elegendő az OSINT alá sorolni az információforrást, mert a forrás általános megnevezése alapján nem feltétlenül dönthető el, hogy az adott adat az alkalmazni kívánt információszerző eszközzel valóban megszerezhető-e OSINT-tevékenység keretében, vagy sem, az eldöntéséhez az alkalmazni kívánt információgyűjtő eszköz besorolására is szükség van. Ráadásul mindez az OSINT-tevékenységet végzők szintjén is eltérő lehet, más szempontokat kell figyelembe venni egy magántársaság esetében és megint más szempontokat egy rendvédelmi szerv esetében.

További lényeges megállapítás, hogy az OSINT információszerző eljárásoknak nem kizárólagos feltétele a megszerezni kívánt információ nyílt minősége, jogos a Vida Csabánál és Lévay Gábornál tett szigorítás, mert a nemzeti és bizonyos külföldi minősített adatok nem képezik OSINT-információszerzés tárgyát. Ezzel párhuzamosan fogalmi szinten további korlátozást is indokoltnak tartok, hiszen személyes adatoknál az OSINT-tevékenységet végzőkre vonatkozó jogi szabályozás egyértelműen szűkíti a gyűjtési lehetőségeket, míg a titkok és a hazai jog által nem védett minősített adatok esetében a forrás határozza meg ezt.

[37] Rácz 2010, 6.

Felhasznált irodalom

Bányász Péter (2015): A közösségi média, mint a nyílt forrású információszerzés fontos területe. *Nemzetbiztonsági Szemle,* 3. évf. 2. sz. 21–36. Elérhető: https://folyoiratok.uni-nke.hu/online-egyetemi-folyoiratok/nemzetbiztonsagi-szemle/korabbi-szamaink/20152-szam (A letöltés dátuma: 2019. 04. 25.)

Burke, Cody (2007): *Freeing knowledge, telling secrets: Open source intelligence and development.* CEWCES Research Papers. No. 13. Bond University. Elérhető: https://pure.bond.edu.au/ws/portalfiles/portal/28737919/Freeing_knowledge_telling_secrets.pdf (A letöltés dátuma: 2019. 02. 20.)

Deák Veronika (2018): A nyílt forrású információszerzés szerepe a kibertámadások végrehajtása során. *Hadmérnök,* 13. évf. 3. sz. 391–402. Elérhető: www.hadmernok.hu/183_29_deak.pdf (A letöltés dátuma: 2019. 04. 25.)

Izsa Jenő (2009): *Nemzetbiztonsági Alapismeretek (A Titkosszolgálatok Működése).* Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem.

Lévay Gábor (2004): A nyílt források felhasználásának lehetőségei a hírszerző munkában. *Felderítő Szemle,* 3. évf. 3. sz. 48–65.

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

NATO Open Source Intelligence Handbook (2001). Elérhető: www.oss.net/dynamaster/file_archive/030201/ca5fb66734f540fbb4f8f6ef759b258c/NATO%20OSINT%20-Handbook%20v1.2%20-%20Jan%202002.pdf (A letöltés dátuma: 2018. 09. 07.)

ODNI (2006): *Intelligence Community Directive Number 301.* Washington, D. C., Office of Director of National Inteligence. Elérhető: www.hsdl.org/?abstract&did=469452 (A letöltés dátuma: 2019. 04. 10.)

Open Source Tools and Resources Handbook 2018 (2018). Elérhető: www.i-intelligence.eu/osint-tools-and-resources-handbook-2018/ (A letöltés dátuma: 2019. 04. 23.)

Rácz Lajos (2010): A titkos információszerzés néhány elméleti kérdése. *Szakmai Szemle,* 3. sz. 5–32.

Vida Csaba (2013): Nyílt forrású adatszerzés (OSINT). In Kobolka István szerk.: *Nemzetbiztonsági Alapismeretek.* Budapest, Nemzeti Közszolgálati Egyetem. 101–109.

Williams, Heather J. – Blum, Ilana (2018): *Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise.* Santa Monica, Rand Corporation. DOI: https://doi.org/10.7249/RR1964

Jogforrások

1995. évi CXXV. törvény a nemzetbiztonságról

2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról

2012. évi C. törvény a Büntető Törvénykönyvről

2012. évi II. törvény a szabálysértésekről, a szabálysértési eljárásról és a szabálysértési nyilvántartási rendszerről

Európai Parlament és a Tanács 2013/40/EU irányelve az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról. Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32013L0040&from=EN (A letöltés dátuma: 2019. 04. 02.)

National Defense Authorization Act for Fiscal Year 2006, Public Law 109–163, Department of Defense Strategy for Open-Source Intelligence, January 6, 2006.