NEMZETBIZTONSÁGI SZEMLE
7. évfolyam (2019) 2. szám 50–67. • DOI: 10.32561/nsz.2019.2.5

Nyeste Péter[1] – Szendrei Ferenc[2]

Nyílt forrású információszerzés a bűnüldözésben

OSINT in Law Enforcement

A nyílt forrású információszerzés napjainkban nagyon fontos szerepet játszik a bűnüldöző hatóságok bűnmegelőzési és bűnüldözési tevékenységében. Ennek segítségével könnyebben feltérképezhetők a szervezett bűnözői tevékenységek, a bűnszervezetek felépítése, tagjai. Ugyanakkor a nyílt forrású információszerzés komoly segítséget tud nyújtani a már elkövetett bűncselekmények felderítésében és bizonyításában is. Írásunkban megvizsgáljuk a bűnüldözési célú nyílt forrású információszerzés jogi hátterét, módszertanának egyes kérdéseit és gyakorlati alkalmazását.

Kulcsszavak: bűnüldözési célú nyílt forrású információszerzés, szervezett bűnözés, bűnmegelőzés, OSINT-módszertan

Open Source Intelligence plays a very important role today in crime prevention and law enforcement. It helps to detect an organised criminal activity, the structure of criminal organisations and members. On the other hand, open source intelligence can hold a strong help for detecting and prove the crimes. In our paper, we will examine the legal background, practise and some methodology questions of the Criminal OSINT.

Keywords: criminal open source intelligence, organised crime, crime prevention, OSINT methodology

[1] Dr. Nyeste Péter egyetemi adjunktus, Nemzeti Közszolgálati Egyetem Rendészettudományi Kar Bűnüldözési és Gazdaságvédelmi Tanszék. ORCID-azonosító: 0000-0002-2440-6414.
[2] Dr. Szendrei Ferenc tanszékvezető egyetemi docens, Nemzeti Közszolgálati Egyetem Rendészettudományi Kar Bűnüldözési és Gazdaságvédelmi Tanszék. ORCID-azonosító: 0000-0002-7890-913x.

Bűnüldözési stratégiák és az információszerzés és -értékelés

A bűnüldöző hatóságok bűnüldözési feladatai hagyományosan hármas felosztásúak lehetnek. Ezek a *megelőzés, a bűncselekmények megakadályozása és az elkövetett bűncselekmények felderítése, bizonyítása*.

A bűncselekmények, illetve az életvitelszerűen folytatott bűnözői tevékenységek megelőzésének a *közösségi rendészet* szerint fontos eleme a közterületi rendészeti erők látható jelenléte, de „önmagában azonban a megnövelt rendőri jelenlét bűncselekmény-csökkentő hatása nem igazolható meggyőzően".[3] Egyes tanulmányok szerint „10%-os rendőrijelenlét-fokozásnak 3%-os bűncselekmény-csökkentő hatása lehet a kisebb értékű vagyon elleni és azokhoz kapcsolódó bűncselekményekre",[4] de az erőszakos bűncselekményekre gyakorolt hatása már nem egyértelműen kimutatható. Az eseményorientált, reaktív rendészet kritikájaként és alternatívájaként dolgozták ki az 1970-es években a problémaorientált rendészet modelljét, amelyet gyakran SARA-modellnek[5] is neveznek, amely a bűnüldözési probléma megvizsgálását, elemzését, az azokra való célzott reagálást, illetve az eredmény értékelését jelenti. Ez a rendészeti modell azonban olyan komoly elemzőkapacitást igényel, amely nem feltétlenül áll arányban az elvárt eredménnyel. A *hírszerzésalapú rendészet* közelebbről fókuszál a bűnüldözésre, valamint a büntető igazságszolgáltatás eszközeire és céljaira. A definíció szerint a hírszerzésalapú rendészet a bűnügyi hírszerző elemzés szigorú döntéshozatali eszközként való alkalmazása azzal a céllal, hogy hatékony rendészeti stratégiákon keresztül előmozdítsa a bűncselekmények számának csökkenését és a bűnmegelőzést.[6] *A hírszerzésalapú rendészetet* sikeresen alkalmazzák az előforduló főbb bűnügyi problémák ellen, de önmagában nem elég hatékony az új bűnelkövetési minták, folyamatok feltárásában és a válaszlépések megfogalmazásában.[7] A bűncselekmények egyre kifinomultabb, konspiráltabb, szervezettebb elkövetése, a határokon átnyúló szervezett bűnözés terjedése miatt már több nagy rendőrség döntött úgy, hogy a hírszerzésalapú megközelítést rendészeti stratégiájának meghatározó részévé teszi. Erre az egyik legjobb európai példa az angol National Intelligence Model (Nemzeti Hírszerzési Modell).[8] A NIM strukturális kialakításának célja, hogy a megfelelő, aktuális információkat megosszák a teljes rendszer különböző szintjein (helyi, teljes szervezeti, nemzetközi). A gyakorlatban azonban problémákat jelent, hogy mely információkat osszák meg a felsőbb szintek irányába; a releváns információkat inkább a felsőbb szintekről az alsóbb szervek irányába terjesztik, és kevés információt kapnak a helyi szintektől.[9]

Mindegyik stratégiai rendészeti modellről elmondható, hogy kiemelkedő szerepet tulajdonít a beszerzett információk értékelésének és elemzésének, függetlenül attól, hogy élőerősen vagy technikai úton szerezték meg a releváns információt.

---

3 Bradford 2011.
4 Levitt 1997.
5 SARA: Scanning – vizsgálódás, Analysing – elemzés, Responding – reagálás, Assessment – értékelés.
6 Ratcliffe 2008.
7 Maguire 2008.
8 Szendrei 2018.
9 Maguire–John 2003.

Az OSINT (Open Source Intelligence – nyilvános forrású információszerzés) eredetileg az amerikai titkosszolgálatok által kifejlesztett módszer, amely az internet terjedésével általánossá vált nemcsak a titkosszolgálatoknál, hanem az üzleti élettől a kormányzati tevékenységig széles spektrumon.[10] A nyílt hozzáférésű információk a minősített forrásokat nem tudják kiváltani, de kiegészíthetik, ellenőrzöttebbé tehetik a minősített és egyéb forrásokból szerzett információkat, illetve azok megfelelő értékelést és elemzést követően önmagukban is felhasználhatók.

Az OSINT az alább felsorolt modern információszerzési módszerek közé tartozik, amelyek többsége jellemzően a katonai, nemzetbiztonsági területen használatos, néhányat azonban már a bűnüldözés is átvett és eredményesen használ.

- *HUMINT (Human Intelligence)* – emberi erőforrással folytatott hírszerzés;
- *SIGINT (Signal Intelligence)* – rádióelektronikai felderítés;
- *COMINT* (*Communication Intelligence*) – rádiókommunikációs felderítés;
- *ELINT (Electronic Intelligence)* – rádiótechnikai felderítés;
- *TELINT (Telemetry Intelligence)* – a telemetriai felderítés;
- *RADINT (Radar-transmitted Intelligence)* – a radarkisugárzás-felderítés;
- *CYINT (Cyber Intelligence)* – a kiberhírszerzés;
- *IMINT (Imagery Intelligence)* – képi felderítés;
- *MASINT (Measurement and Signitures Intelligence)* – a mérési és jelmeghatározó hírszerzés;
- *GEOINT (Geospatial Intelligence)* – a geoinformációs felderítés;
- *TECHINT (Technical Intelligence)* – technikai adatszerzés;
- *OSINT (Open-Source Intelligence)* – nyílt forrású információszerzés;
- *SOCMINT (Social Media Intelligence)* – közösségi hálózatokból folytatott információszerzés.

Az OSINT-információk forrásai a NATO[11] OSINT-kézikönyv[12] szerint:

- nyomtatott és elektronikus média;
- internet, deep web;[13]
- kereskedelmi (fizetős) online szolgáltatók tanulmányai, adattárai;
- „szürke irodalom", a szűk körben hozzáférhető, nyomtatott és digitális dokumentumok, tanulmányok;
- tudományos előadások, konferenciák;
- személyes tapasztalatok;
- kereskedelmi műholdak felvételei;
- tudományos szervezetek, egyetemek.

Robert D. Steele, az Open Source Solutions[14] (OSS.Net) vezérigazgatója szerint „minősített forrásokból a felhasználható információ 20%-a szerezhető meg, amire a költségek

[10] Bálint 2018, 139.
[11] NATO: North Atlantic Treaty Organisation – Észak-atlanti Szerződés Szervezete.
[12] *NATO OSINT Handbook* (2001).
[13] Deep Web: „a láthatatlan web" az internet keresőmotorok részére nem indexelt adatai, szolgáltatása.
[14] Open Source Solutions: nyílt forású megoldások.

95%-át kell áldozni […] nyílt forrásokból a felhasználható információ 80%-a származik, amihez a költségek 5%-át kell felhasználni".[15]

Ezek az adatok jól jelzik, hogy milyen fontos szerepet játszhatnak mind a megelőzés, mind a bűncselekmények utólagos felderítése és bizonyítása során a nyílt forrásokból elérhető információk beszerzése és azok szakszerű értékelése-elemzése.

A társadalomban robbanásszerűen lezajló információs forradalom és az Y, Z generációk szokásainak változása gyökeresen megváltoztatta az információkhoz való hozzájutás és az információk, adatok feldolgozásának módját. Manapság már csak felületesen olvasunk át nagy terjedelmű anyagokat, illetve sokkal gyakoribb a téma szerinti rövid tartalmak gyors áttekintése, váltogatása. Becslések szerint a világ rohamosan növekvő lakossága 28%-ának (több mint 2 milliárd embernek) közvetlen hozzáférése van a *World Wide Webhez,* és közel 5 milliárd ember mobiltelefonnal rendelkezik. Minden nap átlagosan 247 milliárd e-mailt küldenek el. Ez a százalékarány minden évben 24%-kal növekszik.[16]

A bűnügyi célú OSINT alkalmazása hatékonyan, célirányosan segítheti a bűnügyi hírszerzést és a bűnügyi nyomozást folytató felderítők, nyomozók, vezetők döntéseit a rendvédelmi szerveknél.

Jogi háttér

Az Európai Unió 2010-ben elfogadott *belső biztonsági stratégiája*[17] kihívásokat, alapelveket és iránymutatásokat fogalmazott meg. A stratégia alapján az elkövetkező években a következő legsürgetőbb kihívások megválaszolása áll az EU biztonsága, a hírszerző, elhárító, bűnüldöző szervezetek előtt: *embercsempészet, kábítószer- és lőfegyvercsempészet, pénzmosás, valamint illegális hulladékszállítás és -lerakás Európán belül és kívül, hamisított vagy veszélyes áruk értékesítése, terrorizmus, számítástechnikai bűnözés, határbiztonság.*

Ezek a cselekmények szervezett bűnözői csoportok működését feltételezik, amelyek elleni hatékony fellépésnek összehangoltnak, európai szintűnek kell lennie.

Az Európai Unió Belső Biztonsági Stratégiája által megfogalmazott főbb célkitűzések:

- nemzetközi bűnözői hálózatok felgöngyölítése;
- a terrorizmus, radikalizálódás és toborzás megelőzése;
- a virtuális tér biztonságának növelése a polgárok és vállalkozások számára;
- a biztonság megerősítése a határigazgatás útján;
- Európa válságokkal és katasztrófákkal szembeni ellenálló képességének javítása.

A stratégia szerint a *megelőzés és előrejelzés proaktív, hírszerzésen alapuló felderítést, megközelítést feltételez.*

A rendőrségi törvény 2018-ban hatályba lépett módosítása az úgynevezett *rendészeti célú titkos információgyűjtést* a büntetőeljárási törvény leplezett eszközeinek

[15] Kenedli 2013, 183–193.
[16] Rolington 2015.
[17] 5842/2/2010 tanácsi dokumentum: Az Európai Unió belső biztonsági stratégiája: Az európai biztonsági modell felé.

fogalmához igazítva határozta meg, és ez alapján olyan, a magánlakás sérthetetlenségéhez, valamint a magántitok, a levéltitok és a személyes adatok védelméhez fűződő alapvető jogok korlátozásával járó, a rendőrség által végzett különleges tevékenységként jellemzi, amelyet a rendőrség erre feljogosított szervei az érintett tudta nélkül végeznek. Amennyiben konkrét bűncselekményre vonatkozó információk merülnek fel, illetve a titkos információgyűjtés során végzett értékelő-elemző munka végtermékeként ilyen értékelt információ kerül előállításra, akkor azok további ellenőrzése már csak büntetőeljárási törvény által szabályozott keretek között kerülhet sor hagyományos vagy *leplezett eszközök*, nyomozási tevékenységek végrehajtásával.

A rendőrségi törvény a *bűnmegelőzési tevékenységet olyan bűnügyi hírszerző tevékenységként határozza meg*, amelynek tárgya nem egy adott bűncselekmény, hanem a Magyarország társadalmi rendjét veszélyeztető *bűnözés*. Az indokolás szerint a rendőrség információszerző, -értékelő, kockázatelemző tevékenységének eredményéhez tartozik a rendőrség intézkedési kötelezettsége is, amelynek része lehet egy adott bűncselekmény elkövetésének megakadályozása is. Definiálták a bűncselekmények megelőzését mint a titkos információgyűjtés egyik lehetséges célját, és az annak eléréséhez alkalmazható intézkedések meghatározására *lépcsőzetesen került sor.*

A törvényben elsőként egy általános bűnmegelőzési fogalom- és feladatrendszert határoztak meg, amely az úgynevezett értékelt-elemzett bűnüldözési információkon alapuló rendészet *(intelligence-led policing)* modelljének megfelelő működést feltételez.

A törvény szerint a rendőrség az alaptörvényben, az ágazati törvényben és törvény felhatalmazása alapján más jogszabályban meghatározott bűnmegelőzési, bűnüldözési, államigazgatási és rendészeti feladatkörében végzi a bűncselekmények megelőzését, amelynek során *figyelemmel kíséri Magyarország bűnügyi helyzetét, feltárja a bűncselekmények elkövetésének kockázatait, a bűncselekmények elkövetésére irányuló törekvéseket, továbbá megszerzi, elemzi, értékeli, ellenőrzi és továbbítja a bűnözéshez kapcsolódó, a bűncselekmények megelőzése, illetve megakadályozása céljából szükséges információkat.*

Ez az általános célú, ágazati bűnmegelőzési feladatrendszer jelenti a rendőrség stratégiai és taktikai[18] hírszerzésének alapját, amely nem kifejezetten csak bűnügyi irányultságú, hanem más szolgálati ágak információit is becsatornázza és egyben a hírigényeiket is kielégíti.

Az általános bűnmegelőzés célrendszerében alkalmazható intézkedéseken túl szűkített feltételek fennállása esetén vehetők igénybe a titkos információgyűjtés ágazati törvényben szabályozott, bírói engedélyhez nem kötött lehetőségei.

A törvény 65. § (1) bekezdésében szereplő normatív szempontrendszer rögzíti, hogy bűncselekmény elkövetésének megelőzése céljából csak akkor folytatható titkos információgyűjtés, ha *megalapozottan feltehető,* hogy attól a bűnözésre vonatkozó olyan információk megszerzése várható, amelyek elemzése és értékelése révén feltárhatók a bűncselekmények elkövetésére irányuló törekvések, és lehetővé válik a bűncselekmények megelőzése, illetve megakadályozása.

[18] Nyeste 2013.

Ezzel a titkos információgyűjtés egyszerűbb, a jogkorlátozásra kevésbé alkalmas eszközei is csak indokolás alapján működtethetők.

A legsúlyosabb jogkorlátozó, bírói engedélyhez kötött titkos információgyűjtési lehetőségeket csak a szervezett bűnözéssel szembeni fellépés során engedi meg a törvény bűnmegelőzési céllal.

A jogalkotó elképzelései alapján a jogalkalmazó szervek pontosan definiált bűnmegelőzési célokból folytathatnak titkos információgyűjtő tevékenységet. A bűnmegelőzési tevékenység mint a rendészet egyik jövőbeli stratégiai célja, detektálja a bűncselekményeket kiváltó okokat, deviáns magatartásokat, a bűnözés állapotát monitorozza, amelynek során egy fontossági sorrend alapján feladatrendszert állítanak fel, tevékenységük célpontjait, irányait meghatározzák. Ebben komoly szerepet játszhat a rendőrség nyílt forrású információszerzési tevékenysége. A rendőrségi törvény alapján folytatott nyílt forrású információszerzés céljai lehetnek többek között a szervezett bűnözői csoportok, terrorista csoportok feltérképezése, a csoport tevékenységében fontosabb szerepet játszó személyek beazonosítása, kapcsolatrendszerük feltárása, tartózkodási helyük megállapítása, elérhetőségeik, kommunikációs eszközeik, csatornáik feltárása. A rendvédelmi szervek (és a titkosszolgálatok) által folytatott bűnöző szervezetek felépítésének megismerésére és azok bomlasztására irányuló titkos információgyűjtő tevékenység az Európai Unióban már régóta elfogadott és alkalmazott tevékenység.[19]

Svédországban 2009 óta egy integrált megközelítést[20] alkalmaznak a szervezett bűnözés megelőzése és az ellene való fellépés érdekében, amelynek módszertana az úgynevezett bűnügyi arborisztikus módszer,[21] amely a kertészetben alkalmazott metszési módszerek ellentéteként fogható fel, mivel a bűnügyi fakertészeti módszer lényege nem a gyenge részek eltávolítása, hanem éppen ellenkezőleg, a bűnözői szervezet kulcsfontosságú személyei ellen irányul. A módszertan lényege szerint a bűnözői csoportok felépítését, kapcsolatrendszerét kell tanulmányozni elsősorban, a belső magot alkotó stratégiai fontosságú személyeket kell beazonosítani (képességeik és fontosságuk alapján) és „kimetszeni" a bűnözői hálózatból, ezzel elérhető a bűnözői csoportok meggyengítése és végső soron felszámolása. A módszer alkalmas stratégiai és taktikai célok segítésére egyaránt. A módszer alkalmazásának elsődleges céljai:

- a „rejtőzködő" stratégiai fontosságú személyek beazonosítása, az információgyűjtés és -elemzés számára egy közös struktúra megalkotása, a belső magot alkotó stratégiai személyek képességeinek a feltérképezése, az eddig ismeretlen bűnöző személyek gyorsabb beazonosítása telefonlehallgatás, helyiséglehallgatás, megfigyelés segítségével;
- az együttműködő személyek kiválasztásánál stratégiai információk nyújtása az információk forrásainak az értékeléséhez, továbbá segítséget jelent az együttműködők információkhoz való hozzáférési lehetőségeinek értékelésénél;
- objektív alapokat teremt a döntések és a fontossági sorrendek felállításakor, összekapcsolja a stratégiai elképzeléseket a műveleti munkával, a kiválasztott

[19] Nyeste 2012, 28.
[20] Balláné Füszter – Szendrei szerk. 2011, 133.
[21] Nilval–Mattson 2016, 83.

személyek ellen irányuló intézkedések hatásának előrejelzését segíti, valamint a visszacsatolást segíti a strukturált felépítésű jelentések és a beavatkozással kapcsolatos hatások értékelése.

A rendőrségi törvény a bűnmegelőzési célból végezhető bírói engedélyhez nem kötött titkos információgyűjtés eszközeinek sorában nevesíti az elektronikus hírközlési eszközön vagy információs rendszeren folytatott kommunikáció tényének a megállapításához, az elektronikus hírközlési eszköz vagy információs rendszer azonosításához, illetve hollétének megállapításához szükséges adatok megszerezését, amelyek alkalmazására sor kerülhet a nyílt forrású információszerzés adatainak értékelése alapján is. Az ilyen információszerzés végrehajtása a rendőrségi törvényben meghatározott bármelyik bűnüldözési feladatot elősegítheti, az információk ellenőrzöttebbé tételével, megalapozásával, kiegészítő információk beszerzésével. Ez a tevékenység végezhető akár az általános bűnüldözési feladatok ellátása során, vagy a törvényben nevesített titkos információgyűjtési célokból, mint személybiztosítás, létesítményvédelem, fedett nyomozó védelmét szolgáló, tanúvédelmi tevékenység, vagy akár a körözési munka elősegítése is.

A konkrét bűncselekmények felderítését és bizonyítását is nagymértékben elősegítheti a nyílt forrású információszerzés, támogatja az elkövetett cselekmény elkövetési helyének, módjának megállapítását, a cselekménnyel összefüggésbe hozható helyek felkutatását, az elkövetéshez használt eszközök felderítését, a lehetséges motivációk, az elkövetést lehetővé tevő körülmények megállapítását, bizonyítékok beszerezhetőségét.

A nyílt forrású információszerzés mellett számos egyéb felderítési lehetőség áll a bűnüldöző hatóságok rendelkezésére, amellyel a beszerzett információkat ellenőrizhetik, kiegészíthetik azokat. A bűnüldöző hatóságok adatszerző tevékenységet folytathatnak a büntetőeljárás szabályai szerint, de konspirált módon titkos megfigyelést vagy a büntetőeljárásban rejtett figyelést folytathatnak, konspirált módon koncentrált adatgyűjtést végezhetnek környezettanulmány formájában, vagy együttműködő személyeket, fedett nyomozót alkalmazhatnak, vagy amennyiben feltételei adottak, lehallgatást végezhetnek a célszeméllyel, büntetőeljárásban gyanúsítottal szemben.

Az alkalmazható *OSINT-eszközök:*

- innovatív adatbányászati és adatelemzési módszerek,
- intelligens nyelvészeti alapokra épülő keresési módszer,
- intelligens keresőmotorok,
- tematikus leválogató rendszer (például RSS-csatornák figyelésének automatizálása),
- közösségi oldalak figyelése (például flashmobok azonnali kockázati értékelése),
- honlapok forráskódjának értékelése, rejtett tartalmak megjelenítése,
- domain search, whois tools (a honlap domain-előfizetőjéhez kapcsolható adatok kinyerése),
- magyar és nemzetközi sajtófigyelés.

Fontosabb OSINT-területek:

- internetes hírek,
- szürke irodalom,
- közösségi háló,

- hagyományos média,
- nyílt adattárak,
- nyilvántartások (például Céginfo, Takarnet).[22]

Becslések alapján a világhálón 15 milliárd és 1 trillió közötti oldal található. A legtöbb népszerű és leggyakrabban alkalmazott keresőprogram – mint a Google – a teljes webadatok tartalmának csak a 3–4%-át fésüli át, mivel azok csak a megszerkesztett weboldalakat figyelik. A fennmaradó tartalom (96–97%) a világháló mélyebb részéhez, a deep webhez tartozik, ahol a webtartalom csak adatokat és nem szerkesztett oldalakat tartalmaz. Utóbbiak csak meta-keresőprogramokkal, kulcsszavakra történő kereséssel érhetőek el (például Chunkit, Kayak, DeeperWeb, Dogpile, MetaLib).

Több tagállam, ország felismerve a nemzetbiztonsági szolgálatok és a rendvédelmi szervek információi megosztásának egyre égetőbb szükségességét, valamint a koncentrált információszerzés előnyeit, úgynevezett fúziós központokat hozott létre az információk összegyűjtése, elemzése, értékelése érdekében. A Nemzeti Biztonsági Stratégia[23] megfogalmazza, hogy minden kormányzati intézmény feladata, hogy saját szakterületén folyamatosan értékelje a nemzeti és nemzetközi biztonság és fenyegetettség elemeit, és megtegye a szükséges lépéseket azok kezelésére és elhárítására. A stratégia külön kiemeli a nemzetbiztonsági szolgálatok és a bűnügyi hírszerzés biztonságpolitikai stratégiai feladatait.

A stratégiai hírszerzési és elhárítási célok eléréséhez szükséges, hogy rendelkezésre álljanak a terrorizmusra, a szervezett bűnözésre, az egyéb illegális tevékenységek jelentette aszimmetrikus fenyegetésekre, más globális, regionális és belső kihívásokra vonatkozó információk. A Nemzeti Biztonsági Stratégia meghatározza, hogy a Magyarországot érintő biztonsági kihívásoknak megfelelően – a hazai szervek koordinált tevékenysége mellett – szorosabb együttműködést kell kialakítani és fenntartani a szövetséges államok hírszerző és elhárító szervezeteivel, valamint az egyes kérdésekben hasonló biztonságpolitikai célokat követő más államok szolgálataival. A stratégia meghatározza, hogy a nemzetközi kapcsolatokat is fel kell használni *az új bűnügyi trendek feltérképezésére, az új bűnözési jelenségek megismerésére, a legjobb gyakorlatok átvételére.*

A fenti alapdokumentumok egy folyamatos, átfogó, koordinált stratégiai tervezést és annak részeként megjelenő hírszerzési képességet fogalmaznak meg a nemzetbiztonság és a bűnüldözés területén is.

A nemzetbiztonsági és bűnüldözési felderítési információk megosztási csatornájaként 2001. január 1-jei hatállyal létrejött a Szervezett Bűnözés Elleni Koordinációs Központot (SZBKK). A központ alapfeladata volt a szervezett bűnözés megelőzésének, megszakításának, felderítésének elősegítése a *nemzetbiztonságok és a rendvédelmi* szervek által szolgáltatott adatok gyűjtése, feldolgozása, elemzése és a szolgáltató szervezetek részére történő visszacsatolás által, valamint a szervezett bűnözés elleni fellépéshez szükséges kormányzati döntések információs igényének a kielégítése. Majd 2011-ben a Nemzeti Információs és Bűnügyi Elemző Központról szóló

[22] Bálint 2018, 139.
[23] A kormány 1035/2012. (II. 21.) Korm. határozata Magyarország Nemzeti Biztonsági Stratégiájáról.

törvénytervezet[24] sikertelen benyújtását követően 2016. július 15-i hatállyal létrejött egy új polgári nemzetbiztonsági szolgálat, a Terrorelhárítási Információs és Bűnügyi Elemző Központ (TIBEK) a SZBKK jogutódjaként.

A központ új feladatává vált a légitársaságok által továbbított utasnyilvántartási adatok kezelése, valamint elemzése és értékelése, összhangban az uniós adatvédelmi előírásokkal. Továbbá a TIBEK feladata a nemzetbiztonságot, bűnüldözést, közbiztonságot vagy más alapvető biztonsági érdeket sértő adatok feldolgozásának, elemzésének eredményeként a lehető legátfogóbb kép összeállítása az ország terror-, illetve esetleges más fenyegetettségéről, a belső biztonsági helyzetről, a közbiztonság állapotáról. Minderről tájékoztató rendszert működtet, értékelő jelentéseket készít, és azokat a miniszter útján eljuttatja a kormánynak.

A TIBEK az együttműködő szervek nyomozási és felderítő tevékenységét a *titkos információgyűjtések és a büntetőeljárások kezdeti stádiumától taktikai szinten támogatni tudja, valamint eljárást kezdeményező indító jelzéseket, elemzéseket adhat, készíthet*.

A TIBEK információfúziós és elemző-értékelő tevékenységével a bűnüldözési hírszerzési és speciális, leplezett nyomozási feladatokat is egyaránt segíteni tudja. Továbbá a kiemelt bűncselekményi körbe tartozókon túl feldolgoz olyan bűncselekményeket is, ahol az elkövető személye vagy a bűncselekmény társadalomra veszélyessége, illetve a cselekmény gyakori ismétlődése miatt az azokkal összefüggő adatok elemzése, értékelése indokolttá válik. Ezzel a tevékenységgel nemcsak a speciális, leplezett nyomozási tevékenységeket igénylő bűncselekményeket, hanem az egyszerűbben felderíthető, de komolyabb elemzést igénylő ügyek felderítését is segíteni tudja.

A *Terrorelhárítási Információs és Bűnügyi Elemző Központ* folyamatosan vizsgálja Magyarország *biztonsági és bűnügyi helyzetét*, elemzi Magyarország nemzetbiztonsági, bűnügyi és terrorfenyegetettségi helyzetét.

A Terrorelhárítási Információs és Bűnügyi Elemző Központ támogató, koordinációs elemző-értékelő tevékenysége során elemző, tájékoztató és koordinációs tevékenysége kiterjed az együttműködő szervek hatáskörébe és illetékességébe utalt valamennyi információra. *Nyílt információgyűjtést és -feldolgozást végző szolgáltató és támogató szervet működtet (OSINT-központ).*

Ezzel a feladattal létrejött a központi bűnügyi OSINT szervezeti eleme, jelenleg főosztályi szervezeti formával végzi feladatait, nyújtja szolgáltatásait.

„A hazai és külföldi blogok, hírforrások figyelése, értékelése és elemzése révén a központi OSINT képes kiszűrni például:

– A legújabb dizájnerdrogok fejlesztésének várható irányait (kockázatos vegyületek), a terjesztői online hálózatokat, a célközeget, a terjesztés lehetséges online vagy valós helyszíneit (chat, blog).

– A radikalizálódás folyamatában a kockázati szintekben történő változásokat, csoportképződési kezdeményezéseket.

– Vagyonvisszaszerző tevékenysége során olyan, már látókörbe került szervezett bűnözői csoportok vagyoni helyzetének változását, amelyek kivonni igyekeznek a bűnös profitot a hatóságok látóköréből.

[24] T/5004. törvényjavaslat egyes rendvédelmi tárgyú törvények módosításáról, valamint az azzal összefüggő további törvénymódosításokról.

– A hazai és külföldi bűnszervezetek közötti kapcsolatokat, a bűnelkövetésből származó pénzek mozgását.

– A központi OSINT egyik feladata a külföldi törvényhozás azon szegmensét érintő változások figyelése, amely hatással van a magyar társadalmat veszélyeztető bűncselekmények megjelenésére."[25]

Magyarország nemzetbiztonsági, *terrorfenyegetettségi és bűnügyi helyzetével*, ezek meghatározott elemeivel, konkrét kockázatokkal vagy bűncselekményekkel kapcsolatos *tájékoztató jelentéseket, háttér- és kockázatelemzéseket készít az együttműködő szervek* részére a hatáskörükbe tartozó feladatok törvényes, szakszerű és eredményes ellátásának elősegítése céljából.

Feltárja az együttműködő szervek által folytatott *párhuzamos adatkezeléseket,* különösen a több együttműködő szerv által ugyanazon bűncselekmény, személy vagy egyéb tárgykör vonatkozásában párhuzamosan folytatott titkos információgyűjtéseket, illetve az ugyanazon bűncselekmény miatt párhuzamosan folytatott nyomozásokat, és ezekről tájékoztatja az érintett együttműködő szerveket.

- *Figyelemmel kíséri a bűnszervezetek és terrorszervezetek*, valamint *a szervezett bűnözői és terrorista csoportok tevékenységét,* az ilyen szervezetek és csoportok egymáshoz való viszonyát, kapcsolatait; jogsértő módon szerzett vagyonuk, illetve az ilyen vagyon jogsértő eredetének leplezésére irányuló törekvéseik és az ilyen célt *szolgáló vállalkozásaik elemzésével segítséget nyújt az ellenük való fellépéshez*.
- A Terrorelhárítási Információs és Bűnügyi Elemző Központ ellátja az *utasadat-információs egység feladatait.*

Az OSINT módszertana[26]

Az OSINT hírszerzési ciklus módszertana a szakirodalom alapján négy elemre osztható: az információk begyűjtése, feldolgozása, szövegösszefüggésbe helyezése, osztályozása és megosztása.

Az első szakaszban történik *a potenciálisan hasznos, releváns információtartalmak beazonosítása és azok begyűjtése.* Ez a szakasz erőteljes számítástechnikai támogatást igényel. A hírszerzési igényeknek megfelelő információk prioritási sorrendjének megfelelő információk kinyerése, leválogatása történik. A modern demokratikus társadalmakban a szolgáltatók által tárolt személyes adatokhoz való hozzáférés számos jogi akadályba ütközik, ezért azok összegyűjtése még bűnügyi célú felhasználás esetén is időigényes vagy nem lehetséges.

A hírszerzési ciklus második fázisa az összegyűjtött adatok *feldolgozása*, azok értékelése, az elemzés számára hasznosíthatóvá tétele. Ennek két eleme van: az információk, adatok *lefordítása és azok összesítése*. Ezek nem feltétlenül kell, hogy kövessék egymást, de segítséget nyújthatnak ebben a fázisban. Az *összesítés* kritikus pontja

[25] Bálint 2018, 253.
[26] Williams–Blum 2018.

a ciklusnak, mivel itt csökkentik az adattartalom méretét, és a fordított tartalmakat egybeillesztik.

A számítógépes szakembereknek nehézséget okozhat annak pontos megállapítása, hogy melyik adatbázisokból gyűjtötték össze a kinyert, összesített adatokat, hogy azok tartalmát hitelesíteni tudják, és megfelelő szövegösszefüggésbe helyezik. Az elemzés a következő fázis, amely során meg kell állapítani a kinyert információ helyességét, valós értékét. Az elemzésnek három szakasza van: hitelesítés, hitelesség értékelése, szövegösszefüggésbe helyezés.

Az *OSINT-termék megosztása* a végző fázisa a ciklusnak. Itt már gyakran a beszerzett és elemzett információk a többlettartalom miatt belső felhasználású vagy minősített információknak minősülnek és az arra jogosult személyek részére továbbíthatóak.

Az OSINT-metodika eszközei: *a lexikális elemzés, hálózatelemzés, térinformatikai elemzés,* illetve ezek kombinációi.[27]

A lexikális elemzés a nyílt forrású elemzés legerőteljesebb eszköze, amely során a különböző forrású és nagy mennyiségű szöveges tartalmak egyidejű elemzése történhet. Az alapszintű lexikális elemzés megmutatja a keresőmotorokon leggyakrabban használt kifejezéseket, legtöbbet keresett tartalmakat.

A közösségihálózat-elemzés segítségével felderíthetjük a személyek kapcsolatrendszerét, a hálózatelemzés a csomópontokra összpontosít, a külső és belső körök, kapcsolatrendszerek feltárására. A csomópontok közötti kapcsolatok száma, az interakciók sűrűsége a személyek fontosságát, információszerzési lehetőségeit határozhatja meg. Ennek segítségével megállapíthatók a kulcsfontosságú személyek és a lehetséges támadási pontok.

Térinformatikai elemzés az új közösségimédia-platformokra alapozott, a használók eszközeinek, terminéladatoknak felhasználásával kinyert térinformatikai elemzés – kombinálva az előbbi lehetőségekkel – gazdagabb képet tud nyújtani a célszemélyről, az elkövetőről, és bizonyítékként is felhasználhatók a kinyert adatok.

Bűnügyi OSINT a gyakorlatban

Az OSINT alkalmazási lehetőségei gyakorlatilag bármilyen bűnügyi rendőri tevékenységben tetten érhetők. Segítheti, illetve eredményei felhasználhatók lehetnek bármelyik büntetőeljárásban, illetve titkos információgyűjtésben, ugyanakkor speciális elemző-értékelő feladatként is megjelenhet, ahol a már összegyűjtött információk további feldolgozása is megtörténik.

A rendőrség keretein belül az alábbi szervezeti egységeknél találhatunk feladatszerűen OSINT-tal foglalkozó munkatársakat:

- ORFK Bűnügyi Főigazgatóság Bűnügyi Elemző-értékelő Főosztály
- ORFK Készenléti Rendőrség Nemzeti Nyomozó Iroda Kiberbűnözés Elleni Főosztály
- ORFK Készenléti Rendőrség Nemzeti Nyomozó Iroda Vagyonvisszaszerzési Hivatal

[27] Nyeste 2019.

A Bűnügyi Elemző-értékelő Főosztály esetében a vezetői döntéseket előkészítő elemzésekhez, a bűnügyi-közbiztonsági helyzet felméréséről szóló jelentésekhez, a bűnügyi munkához, kiemelten a büntetőeljárásokhoz kapcsolódó elemző-értékelő tevékenységhez használhatják fel a nyílt forrásból származó információkat.

A másik két egység ennél speciálisabb feladatként végez OSINT-ot:

- A Kiberbűnözés Elleni Főosztály a hatáskörébe tartozó bűncselekmények felderítése és nyomozása során szükségszerűen használja az internet adta lehetőségeket, így a nyílt forrású információszerzést is. Ugyanakkor a szakterületen meglévő speciális ismereteiknek köszönhetően sok esetben más szervek felkérése, megkeresése alapján szolgáltatnak OSINT-tal beszerzett információkat.
- A Vagyonvisszaszerzési Hivatal saját eljárásaiban, illetve más szervek felkérésére is végez nyílt forrású információszerzést a bűncselekményekből származó vagy igazolatlan eredetű vagyon feltárása és végső soron elvonása érdekében.

Természetesen a fentiek nem jelentik azt, hogy ezeken kívül, más egységeknél vagy gyakorlatilag akár a teljes bűnügyi rendőrségnél ne beszélhetnénk nyílt forrású információszerző tevékenységről. Saját ügyeiben, saját keretei között, saját ismereteinek megfelelően minden nyomozó és vizsgáló, tudatosan vagy kevésbé tudatosan, de használja az OSINT lehetőségeit.

Ugyanakkor azzal is tisztában kell lennünk, hogy bár legtöbben és leggyakrabban az internettel és a közösségi oldalakon történő kutatással azonosítják az OSINT-ot, valójában számos más, korábban kifejtett OSINT-megoldás, -módszer és lehetőség is létezik.

Másrészről azt is látni kell, hogy önmagában az OSINT sem old meg minden problémát, nem helyettesíthet más felderítési módszereket, információgyűjtő tevékenységeket, annak ellenére, hogy információs társadalmunkban szinte alapelvárás, hogy valaki a virtuális térben is létezzen, folyamatosan jelen legyen ezeken az oldalakon, posztoljon, blogoljon, fényképeket töltsön fel.

Látnunk kell azt is, hogy ezek a közösségi hálók sem változatlanok, sőt az is folyamatosan változik, hogy éppen mi számít trendinek, mit használ a többség. Természetesen nyelvi és földrajzi jellemzők alapján is lehet sorrendeket és kedvenceket találni, ami nálunk a Facebook, az Oroszországban a VK, Kínában a RenRen, a Sina Weibo, QZone, és ezek csak a legnagyobbak, ezeken kívül több mint 250 olyan közösségi (szociális) oldal működik, amelynek több százezer tagja, követője van, amelyek között vannak egészen speciálisak is, gondoljunk csak például arra, hogy az FBI most kezdte el használni azokat a DNS-adatbázisokat a nyomozásaihoz, amelyeket családkutató és egyéb célokból hoztak létre, és gyakorlatilag bárki által hozzáférhetők.

Milyen felderítési célok elérésére, milyen információs igény kielégítésére lehet alkalmas az OSINT?

A célszemély beazonosítása: az eljárások kezdeti szakaszában viszonylag kevés információ áll a nyomozó hatóság rendelkezésére, általában nem rendelkeznek a célszemély pontos személyi adataival. Ami rendelkezésre áll, azok jellemzően nevek, lakcímek, IP-címek, domainnevek, telefonszámok, felhasználónevek és e-mail-címek ömlesztve. Ebben az esetben segítséget jelenthetnek azok a netes oldalak vagy szoftverek, amelyek ilyen töredékadatokból is képesek teljes személyiséget összeállítani azáltal, hogy végigböngészik az internetet és összekapcsolják az ott feltalálható töredékinformációkat. Eljuthatunk a célszemély valamely közösségi oldalához, ahol nagy valószínűséggel találunk róla fényképet, illetve további adatokra is szert tehetünk.

Ilyen oldalak például:

- numberingplans.com – telefonszám alapján,
- imei.info – IMEIszám alapján,
- sync.me – telefonszám alapján,
- sudo app – valódi személy keresése,
- pointofmail.com – e-mail-alapú keresés,
- pipl.com – név-, e-mail-, felhasználónév-, telefonszám-alapú keresés.

A célszemély életvitelszerű tartózkodási helyének megállapítása: amennyiben a célszemély, elkövető lakóhelye, tartózkodási helye ismeretlen, közösségi oldalakon találhatunk olyan fényképeket, bejegyzéseket, amelyekből következtethetünk valamilyen földrajzi helyre, címre. Egy lakás teraszán pózoló és a kilátásban gyönyörködő célszemélyről készült fénykép segíthet a cím meghatározásában. Egy eseményről szóló bejegyzés, például egy vendéglátóhelyről szóló értékelés szintén segíthet valamely cím beazonosításában, és más, akár leplezett eszközök alkalmazásával a célszemély tartózkodási helyének megállapításában. Ugyanakkor egy célszemély által használt IP-cím azonosítása is közelebb vihet minket a kívánt lakóhely azonosításához (például iplogger.com – IP-cím keresése).

A célszemély családi körülményeinek, kapcsolatrendszerének feltérképezése: a célszemély életkörülményeinek teljes körű feltérképezéséhez elengedhetetlen, hogy családi körülményeit és egyéb kapcsolatait is megismerjük. Ez később akár tettestársak, orgazdák és egyéb, a bűncselekmény elkövetésében közreműködő személyek azonosításához is vezethet. A közösségi hálókon megjelenő képek, a különböző családi eseményeket megörökítő fényképek, a haveri bulikon, kocsmázáson, fesztiválokon készített fényképek, a sporteseményeken, koncerteken, nyaraláson, vagy akár horgászat közben készített képek valóságos aranybányát jelentenek egy jószemű OSINT-elemzőnek. Természetesen a fényképeken lévők beazonosítása rengeteg időt és energiát igényel, vagy további OSINT-lehetőségek felhasználásával, vagy egyéb rendelkezésre álló nyilvántartások igénybevételével, illetve más eszközök segítségével beszerzett információk is szükségesek a kérdéses személyek azonosításához.

A célszemély munkahelyének, munkakörének megállapítása: feltéve, hogy célszemélyünk dolgozik valahol, és más rendelkezésünkre álló adatbázisok (például

a NAV nyilvántartásai) nem hoztak eredményt, ismét fordulhatunk a nyílt források segítségével összegyűjthető információkhoz. A fentiekben említett kapcsolatrendszer feltérképezése is hozhat valamiféle munkahelyi, munkatársi információkat, a közös munkahelyi összetartásokon, továbbképzéseken készült képek, a munkahelyen pózolós fényképek közelebb vihetnek a szükséges információk megszerzéséhez. Ugyanakkor a különböző internetes oldalakon tett bejegyzések, like-ok szintén utalhatnak valamiféle foglalkozásra, munkahelyre.

A célszemély vagyoni helyzetének feltérképezése: a büntetőeljárás egyik legfontosabb feladata, hogy megállapítsa a bűnös tevékenységből származó vagyon nagyságát, meghatározza annak pontos helyét, és ezáltal elősegítse annak későbbi elvonását, a vagyoni reparációt. Az elkövetők oldaláról ezzel szemben természetes törekvésként jelentkezik, hogy a bűncselekményből származó vagyonukat, pénzüket elrejtsék, azokat más forrásból származónak vagy más személyhez tartozónak tüntessék fel, ugyanakkor él bennük az az igény is, hogy vagyoni helyzetüket másoknak is megmutassák, ezáltal is hangsúlyozva társadalmi pozíciójukat, összeköttetéseiket, magas életszínvonalukat. A célszemély közösségi oldalain megjelenő ingatlanokról, gépjárművekről, hajókról, magánrepülős utakról, nyaralásokról, költséges hobbikról szóló, azokat bemutató fényképek nyújthatnak segítséget egy vagyoni háttérnyomozáshoz. Ennek legjellemzőbb példája talán a dél-amerikai drogkereskedőkről készült, az interneten fellelhető fényképek, ahol rengeteg ékszerrel, (arany)fegyverekkel, egzotikus állatokkal, nagy teljesítményű autókkal, hajókkal, repülőkkel szerepelnek a különböző bandák tagjai. A napjainkban divatos kriptovaluták, illetve bizonyos pénzügyi aktivitás is nyomon követhető az OSINT lehetőségeivel.

A célszemély szabadidős tevékenységének, nézeteinek felderítése: a kapcsolatrendszer feltérképezésének részeként juthatunk ilyen információk birtokába is. A hobbija, szabadidős tevékenysége utalhat vagyoni helyzetére, adhat egyfajta kapcsolati hálót. A célszemély nézeteinek, esetlegesen szélsőséges vallási vagy politikai hitvallásának megismerése is fontos feladat lehet, különösen bizonyos speciális felderítési területeken (lásd: terrorelhárítás). Ezekre utalhatnak a célszemély által kedvelt oldalak, ezeken az oldalakon vagy egyéb blogokon tett bejegyzések, amelyeket leginkább a különböző speciális keresőmotorok használatával, illetve a lexikális elemzés módszerével ismerhetők meg. Adott esetben bizonyos zárt csoportokba bejutás, az ott zajló kommunikáció megismerése vagy speciális leplezett eszközök, fedett nyomozó felhasználását, vagy valamiféle pszeudoszemélyiség létrehozását és felhasználását igényelheti a felderítő szervektől.

A *célszemély speciális ismereteinek, az általa használt eszközök körének megállapítása:* bizonyos speciális ismereteket feltételező és speciális eszközigényű bűncselekmények nyomozása során fontos lehet annak bizonyítása, hogy az elkövető (gyanúsított) rendelkezik a szükséges ismeretekkel, és rendelkezésére álltak a megfelelő eszközök is az elkövetéshez. Ez eredhet egyrészt a már feltárt munkaköréből, foglalkozásából, de más webes információkból, adatokból is, például a célszemély a műhelyében készült fényképen látható, és a háttérben az adott eszköz is a képre került.

Az érintett helyiség felderítése, alkalmazható technológiák meghatározása: egy házkutatás vagy valamely más nyomozási cselekmény előkészítése során, vagy

a titkos kutatást, illetve a hely titkos megfigyelését megelőzően fontos lehet, hogy előzetesen információkkal rendelkezzünk az adott helyről. Ebben segítségünkre lehetnek az adott helyiségről készült és a közösségi oldalakra feltöltött fényképek, lakáshirdetések, az ezekben megjelenő alaprajzok, a kivitelező által közzétett alaprajzok, látványtervek, fényképek.

Az elkövetett cselekmény elkövetési módjának megállapítása: Magyarországon talán még nem jellemző, hogy az elkövetők az elkövetésről töltsenek fel képeket, videókat a közösségi hálóra, de egyes (mexikói) kábítószerkartelleknél már láthattunk ilyet, amikor elsősorban megfélemlítési célból tettek fel fényképeket az általuk elkövetett emberölésekről (kivégzésekről), vagy akár a terrorszervezetek kivégzéseiről a videómegosztó oldalakra felkerült videók esetében.

A cselekménnyel összefüggésbe hozható helyek felkutatása, az elkövetéshez használt eszközök felderítése: elsősorban ismeretlen bűncselekmény-helyszínek és elkövetési eszközök beazonosításához nyújthat segítséget az OSINT. Például van egy minden jel szerint emberölésbe torkolló eltűnési ügy, ahol már a gyanúsított is a hatóságok látókörébe került, azonban nincs meg a holttest. Az OSINT segíthet a gyanúsítotthoz kötődő helyek beazonosításában, azoknak a helyeknek a megállapításban, ahol a kérdéses időszakban megfordult, ahol fényképet készített, ahonnan bejelentkezett valamilyen internetes fórumra vagy csoportba, ahol bármilyen helymeghatározáshoz kapcsolódó tevékenységet végzett.

A lehetséges motivációk megállapítása, az elkövetést lehetővé tevő körülmények megállapítása: amennyiben az OSINT nyújtotta információhalmaz alapján képesek vagyunk egy viszonylag pontos képet és jellemrajzot felállítani a célszemélyünkről, akkor a nézetei, megnyilvánulásai mellett motivációira, szándékaira is tehetünk megállapításokat, vonhatunk le következtetéseket. Az elkövetést lehetővé tévő körülmények feltérképezésében sokat segíthetnek azok a közösségi oldalak, amelyek egy adott lakókörnyezet információival, visszásságaival foglalkoznak, a tagok folyamatos bejegyzésekben jelzik a rendellenességeket, hiányosságokat, amelyeket bűnügyi szempontból elemezve feltárhatjuk a bűncselekmények elkövetéséhez vezető lehetőségeket.

Az online térben végzett OSINT információforrásait tekintve általában mindenkinek a *közösségi oldalak* ugranak be, azonban ennél sokkal szélesebb a paletta, sokkal több lehetőséggel tud dolgozni, aki nyílt forrású információkat keres.

Keresőmotorok (Google, Google+, Google képkeresés, Google Reverse Image Search, Graph Search, Creepy stb.), amelyek címszavakra egyszerű és összetett keresésekre képesek, illetve képesek adatok alapján képet, vagy fordítva, kép alapján adatokat keresni. Ugyanakkor ezek csak a legismertebb, a többség által használt keresőmotorok, egy komoly titkosszolgálati vagy bűnügyi elemző ezeknél sokkal hatékonyabb lehetőségekkel is rendelkezik.

Közösségi média (Facebook, Instagram, Twitter, LinkedIn, üzenetküldő szolgáltatások): az internethasználók közel fele rendelkezik Facebook-profillal, amelyek a fentebb tárgyaltak szerint rengeteg lehetőséget adnak az OSINT-tevékenységre.

E-mail- és/vagy telefonszám-adatbázisok (Numberingplans.com, Imei.info, Sync.me, mobilszolgáltatók weboldalai): a nevéből adódóan e-mail-címek használóit

tudja beazonosítani vagy éppen telefonszámok előfizetőjét vagy használóját lehet megállapítani.

IP vagy domain keresése (WHOIS-adatbázisok, Centralops.net): a célszemélyünk által használt IP-címet és az alapján valamilyen tartózkodási helyet tud produkálni, illetve az általa használt domainnév alapján a domainszolgáltatótól a regisztráció során közölt adatok kinyerhetők. Az IP-cím megállapítása során problémás lehet, hogy a célszemély interakciójára van szükség, vagy le kell töltenie, vagy meg kell nyitnia valamit, ezáltal esetleg az OSINT-ot végző lelepleződhet.

Adatbázisok (Haveibeenpwned.com, Pastebin.com, Shodan.io): ezekből rengeteggel találkozhatunk és rengeteget használhatunk az interneten, van, amelyik bankszámla-információk után keres, van, amelyik nagyobb mennyiségű szöveget képes bizonyos szempontok szerint elemezni, van, amelyik több ezer webkamera képét tudja a gépünkre hozni.

Tartalomszolgáltatók (Wayback-archívumok, weboldalak archív oldalai, Google Cache): archivált oldalakon, archivált tartalmakban történik a keresés valamely kulcsszóra.

Az online térben végzett OSINT-adatgyűjtés megvalósulhat aktív vagy passzív formában is.

- Passzív adatgyűjtés: semmilyen kontakt nincs a célszemély profiljával.
- Aktív adatgyűjtés: bármilyen kapcsolati pont kihasználása (amelyről a célszemély is értesül).

Az online térben végzett OSINT-tevékenységünk során tekinttel kell lennünk arra, hogy minden online keresés, illetve egyéb tevékenység nyomot hagy maga után, tehát nemcsak az a feladatunk, hogy rábukkanjunk a célszemélyünk nyomaira, hanem az is, hogy saját nyomainkat minél jobban igyekezzünk eltüntetni.

Néhány taktikai jó tanács:

- Olyan eszközöket, illetve kapcsolatot használjunk, ami nem köthető a nyomozó hatósághoz, illetve a személyünkhöz!
- Mindig figyeljünk a dekonspiráció veszélyére!
- Amelyik interakció eredményében nem vagyunk biztosak, azt ne hajtsuk végre (például bejelölés, meghívás, „elfelejtett jelszó")!
- Maradjunk rejtve!
- Alakítsunk ki külön felhasználói környezetet, használjunk másik számítógépet, akár virtuális gépet (VMWare, VirtualBox), válasszuk külön a munkameneteket, használjunk más böngészőt, mint általában, kapcsoljuk be az inkognitómódot, vagy válasszunk privát böngészést!
- Igyekezzünk a kapcsolataink elfedésére, használjunk fedett fiókokat, azonosítókat, e-mail-címeket, telefonszámokat!
- VPN-kliens alkalmazása (Opera-VPN).

A cél a lehető legtöbb információ beszerzése a lehető legkevesebb nyom hátrahagyása mellett. Ennek érdekében gyakran kell a számítógépen kívül további feltételeket is biztosítani (VPN-kapcsolat, e-mail-címek, telefonszámok, felhasználói fiókok, feltöltőkártyás internet).

Külön problémát jelenthet a darkneten való információgyűjtés. Darknetnek vagy deep webnek nevezzük azokat a rejtett hálózatokat, amelyek csak speciális célszoftverekkel érhetők el és a normál keresőmotorok számára láthatatlanok.

Arányaiban az internet körülbelül 80%-a ebbe a kategóriába tartozik, ami miatt mégis megkerülhetetlen az internet ezen része, hogy a bűnözők felismerték ennek előnyeit, és kommunikációs csatornának használják, gyakorlatilag bármilyen illegális dolog adásvételének (fegyver, kábítószer) platformot biztosít, a pedofil hálózatok gyűjtőhelye, illetve a kriptovaluták forgalmazásának a terepe.

Természetesen azért itt is megvannak azok a speciális keresőmotorok és egyéb lehetőségek, amelyek által bizonyos információk kinyerhetők (célszoftverek: például Tor, I2P, Freenet, Deepdotweb.com, Reddit, GRAMS).

Összegezve, az OSINT lehetőséget ad a bűnös tevékenységek feltérképezésére, szervezett bűnözői csoportok beazonosítására, bomlasztására, bűncselekmények megelőzésére, korábban elkövetett cselekménnyel kapcsolatos információk beszerzésére, bővítésére, a célszemély kilétének megállapítására, a célszeméllyel kapcsolatos adatok bővítésére, a bűncselekmény elkövetési módjának megállapítására, tanulmányozására.

Felhasznált irodalom

Balláné Füszter Erzsébet – Szendrei Ferenc szerk. (2011): *A szervezett bűnözés kézikönyve: Kiegészítő megközelítések és intézkedések a szervezett bűnözés megelőzése és az ellene való küzdelem érdekében – Összeállítás az EU tagállamainak jó gyakorlataiból.* Budapest, Rendőrtiszti Főiskola.

Bálint László (2018): Terrorelhárítási Információs és Bűnügyi Elemző Központ. In Resperger István szerk.: *A nemzetbiztonság elmélete a közszolgálatban.* Budapest, Dialóg Campus.

Bradford, Ben (2011): *Police numbers and crime rates – a rapid evidence review.* London, HMIC.

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

Kenedli Tamás (2013): *A nemzetbiztonság általános elmélete*. Egyetemi jegyzet. 183–193.

Levitt, S. (1997): Using Electoral Cycles in Police Hiring to Estimate the Effect of Police on Crime. *The American Economic Review,* Vol. 87, No. 3. 270–290.

Maguire, Mike (2008): Criminal investigation and crime control. In Newburn, T. ed.: *Handbook of Policing.* Cullompton, Willan.

Maguire, Mike – John, Tim (2003): Rolling out The National Intelligence Model: Key Challenges. In Bullock, Karen – Tilley, Nick eds.: *Crime reduction and problem-oriented policing.* Cullompton, Willan.

NATO OSINT Handbook (2001). Saclant, Norfolk.

Nilval, Kim – Mattson, Fredrik (2016): The Criminal Arboristic Perspective – A method to combat Organised Crime. In Töttel, Ursula – Bulanova-Hristova, Gergana – Flach, Gerhard eds.: *Research Conferences on Organised Crime at the Bundeskriminalamt in Germany Vol. III.* Bumdeskriminalamt, Wiesbaden. 83.

Nyeste Péter (2013): A Nemzetbiztonsági célú stratégiai felderítés/elhárítás és a bűnügyi célú startégiai hírszerzés összehasonlítása, kiemelten a szervezett bűnözés elleni fellépés területén. *Felderítő Szemle,* 12. évf. 1. sz. 100–119.

Nyeste Péter (2012): A bűnügyi hírszerzés. *Magyar Rendészet,* 12. évf. 4. sz. 28.

Nyeste Péter (2019): A bűnügyi OSINT. In Szendrei Ferenc szerk.: *A bűnügyi hírszerzés kézikönyve.* Budapest–Pécs, Dialóg Campus.

Ratcliffe, Jerry H. (2008): *Intelligence-led Policing.* Cullompton, Willan Publishing.

Rolington, Alfred (2015): *Hírszerzés a 21. században – A mozaikmódszer.* Budapest, Antall József Tudásközpont.

Szendrei, Ferenc (2018): Az európai bűnügyi hírszerzési modell előzményei Angliában. In Dobák Imre – Hautzinger Zoltán szerk.: *Szakmaiság, szerénység, szorgalom. Ünnepi kötet a 65 éves Boda József tiszteletére.* Budapest–Pécs, Dialóg Campus. 613–627.

Jogforrások

5842/2/2010 tanácsi dokumentum: Az Európai Unió belső biztonsági stratégiája: Az európai biztonsági modell felé.

A Kormány 1035/2012. (II. 21.) Korm. határozata Magyarország Nemzeti Biztonsági Stratégiájáról.

T/5004. törvényjavaslat egyes rendvédelmi tárgyú törvények módosításáról, valamint az azzal összefüggő további törvénymódosításokról.