



A nyílt forrású hírszerzés (OSINT) mint lehetőség a bűncselekmények felderítésében

A rendőrségen belüli önálló OSINT egység koncepciója

Open-source intelligence (OSINT) as an opportunity in the investigation of crimes

The concept of an independent OSINT-unit within the police

Márton Balázs

doktorandusz
Nemzeti Közszolgálati Egyetem,
Rendészettudományi Kar,
Rendészettudományi Doktori Iskola
marbal@t-online.hu



Absztrakt

Cél: A tanulmányban egy, a magyar rendőrség szervezetébe integrálható központi, nyílt forrású hírszerzési (OSINT) feladatokat ellátó egység előnyeit és létrehozatalának néhány súlyponti kérdését járja körül a szerző.

Módszertan: A szerző a bűncselekmények felderítésének rendészettudományi alapjait követően, az OSINT főbb, kurrens szakmai szabályainak megfelelően vizsgálja, hogy egy ilyen egység tevékenysége hogyan járulhatna hozzá a bűnfelderítéshez.

Megállapítások: Az információs társadalom kialakulása és a nagy fokú digitalizálódás okán a bűnfelderítésben egyre több lehetőséget hordoz a hírszerzésalapú rendészeti modell és azon belül is a nyílt forrású hírszerzés eszközeinek és módszereinek alkalmazása. A bűncselekményekhez valamilyen módon kötődő adathalmaz egyre nagyobb arányban vagy kizárólag a kibertérben lelhető fel. Jóllehet jelenleg a magyar rendőrség struktúrájában nem létezik olyan központi, szolgáltató jellegű egység, amelynek keretei között a professzionális és a szervezetszerű bűnfelderítési célú OSINT tevékenység ellátásához szükséges személyi és technikai feltételek összpontosulnának.

Érték: A tanulmány rávilágít, hogy napjainkban az OSINT mint a bűncselekmények felderítésében alkalmazott egyik módszer mennyiben jut egyre

kiemelkedőbb szerephez, és a rendőrség szervezetében miért volna indokolt önálló, szakmai alapon szervezett egység megszervezése. Emellett a rendőri állomány büntető feladatokat ellátó, potenciálisan az úgynevezett első lépcsős OSINT feladatokat végrehajtó tagjainak szakirányú felkészítésének fokozása is indokolt volna.

Kulcsszavak: nyílt forrású hírszerzés (OSINT), bűnüldözés, rendőrség, bűnügyi hírszerzés

Abstract

Aim: In the study the author elaborates the advantages of a central open-source intelligence (OSINT) unit to create within the organization of the Hungarian police and examines some essential points of its establishment.

Methodology: Following the basic police science of crime detection, the author examines how the activities of such a unit could contribute to crime detection, in accordance with the main OSINT disciplinary rules.

Findings: Due to the evolution of the information society and the massive impact of digitization, use of the method of intelligence-led policing including the tools and methods of OSINT provides broader range of opportunities in the criminal intelligence. A set of relevant data linked to the respective criminal offense can increasingly or exclusively be found in the cyberspace. However, there is currently no central service unit within the structure of the Hungarian police force that would provide the human and technical resources necessary for professional and organisational OSINT activities.

Value: The study shows that nowadays the OSINT, as one of the methods used in the criminal intelligence has an increasing role, moreover, it would be reasonable to organize an independent unit on a professional basis within the police organization. In addition, it would also be appropriate to increase the professional training of police officers performing crime detection tasks, potentially in the so-called first-stage OSINT tasks.

Keywords: open-source intelligence (OSINT), law enforcement, police, criminal intelligence

A bűncselekmények felderítésének jelentősége a bűnüldözésben

A bűnözés egy olyan társadalmi jelenség, amely különböző tudományágak rendszerén keresztül is vizsgálható. Érdeklődési körébe vonhatja a szociológia, a jogtudomány, de akár a közgazdaságtudomány is. A kriminalitás valamennyi fajtája beilleszthető egy olyan dialektikus rendszerbe, amelynek a „független változója” a társadalmi veszélyesség (Irk, 2014). Ahogyan Irk Ferenc arra rávilágít, a társadalmi veszélyesség a kriminológia és a büntetőjog közötti összekötő kapocs (Irk, 2014). Ebben a fogalomban fejeződik ki, hogy azért kriminalizálандók bizonyos cselekmények, mert azok veszélyeztetik a társadalom rendjét és működését. A társadalomra veszélyesség kérdésében az előzetes, absztrakt és általános döntéshozatal a jogalkotás felelőssége, amely a demokratikus jogállam és az alkotmányosság keretei között szabott, és az ezekkel átítatott büntető anyagi jogban ölt testet. A büntető jogalkotás hatásköre meghatározni, hogy mely cselekményeket tekinti a társadalomra veszélyesnek és különíti el, vagy ha úgy tetszik, az ultima ratio elve mentén emeli ki a morális tartalmat hordozó bűn halmazából akként, hogy azokat jogszabályi formába önti (Irk, 2014). A bűncselekmény fogalma ettől kezdve már tisztán jogtudományi szemszögből értelmezendő, a hatályos büntetőtörvény által meghatározott általános bűncselekmény-fogalom és a különös részi törvényi tényállásokban megtalálható, konkrét bűncselekményeknek minősített magatartások formájában.

A bűncselekmények alkalmasak arra, hogy mások személyét vagy jogait, illetve Magyarország Alaptörvénye szerinti társadalmi, gazdasági, állami rendjét sértsék vagy veszélyeztessék,¹ azaz a közrend, a közbiztonság és a jogrend szabályozott rendjére gyakorolnak olyan hatást, amelyet a többségi társadalom károsnak vél. Az európai jogfejlődés és a részét képező polgári jogállam kialakulásának eredményeként a bűncselekmények elleni fellépés – ideértve a fizikai erőszak legitim alkalmazásához való jogot – fokozatosan monopolizálódott az állam javára, egyes a jog által biztosított kivételekkel. A büntető igazságszolgáltatás állami feladattá vált, amelynek egyik sarokkövét a legalitás elve jelenti, ez pedig a büntető igény érvényesítésének kötelezettségét mondja ki, vagyis parancs az állami hatóságok számára, hogy alkalmazzák a büntető törvényeket (Bárd, 1986). A továbbiakban a bűnüldözésre mint kizárólagos állami feladatra tekintünk, nem foglalkozunk az alternatív igazságszolgáltatás vagy a komplexer rendészeti rendszer elemeivel.

Az állam büntető igényének érvényesítése a bűncselekmény és az elkövetője ismertté válásán mint esszenciális feltétel alapul, aminek elérése a bűnüldözés

1 2012. évi C. törvény a büntető törvénykönyvről, 4. §.

feladata. Finszter Géza meghatározása szerint a bűnüldözés szaknyelvi terminológia, amelynek szűkebb fogalma alatt értjük a bűnüldöző hatóságok minden olyan intézkedését, aminek célja a bűncselekmény elkövetésével gyanúsítható személyek kilétének megállapítására és az általuk elkövetett bűncselekmények felderítésére irányuló információszerző tevékenység annak érdekében, hogy az állam a büntetőigényét az igazságszolgáltatás útján érvényesíteni tudja (Finszter, 2018).

A bűnüldözési tevékenység része tehát a bűncselekmények felderítése (bűnfelderítés), amely megtörtént bűncselekményhez kapcsolódik, múltbeli eseményre vonatkozó adatok beszerzését célozza, idősíkban a bűncselekmény elkövetése után folytatják akkor is, ha még a bűncselekmény elkövetésének ténye sem ismert a hatóság előtt, hanem legfeljebb a gyanújának a fennállását kell megállapítani. Következésképpen a bűncselekmények felderítése mindenkor bűncselekménnyel összefüggésben történik, de irányulhat addig még látenciában maradt bűncselekményre, azaz a megbizonyosodásra, hogy valóban történt-e bűncselekmény, itt a bűnfelderítési gépezet beindulásának kezdőpontja a „gyanú gyanúja” (URL1). Illetőleg irányulhat már ismertté vált bűncselekményre, utóbbin belül annak elkövetőjére, vagy olyan körülményére, amelynek ismerete elengedhetetlen a kriminalisztika alapkérdéseinek² megválaszolásához (itt a kezdőpont a bűncselekmény gyanúja) (Lakatos, 2005).

A bűnfelderítéstől dogmatikailag el kell különíteni azt a bűnmegelőzési jellegű bűnüldözési tevékenységet, amelytől a hatóság olyan információk megszerzését várja, amelyek elemzése és értékelése révén feltárhatók a bűncselekmények elkövetésére irányuló törekvések, és lehetővé válik a bűncselekmények megelőzése, illetve megakadályozása.³ Ezek a hatósági aktusok olyan rendészeti információszerző tevékenységet feltételeznek, amelyek a közrend és a közbiztonság általános védelmét szolgálják, folyamatosan kutatva azon veszélyforrások, illetve körülmények után, amik bűncselekmények elkövetéséhez vezethetnek.

A bűnmegelőzési jellegű bűnüldözési tevékenység és a bűncselekmények felderítésének karakterisztikája rendészettudományi szempontból abban különbözik egymástól, hogy míg az előző proaktív, általános, tájékozódó és feltérképező jellegű rendészeti információgyűjtést feltételez, addig az utóbbi igazságszolgáltatási célú és a reaktív jelleg dominál benne. Jogi aspektusából az előző alapját a rendészeti ágazati jogszabályok adják, utóbbi többnyire a büntetőeljárásról szóló törvényben foglaltak szerint kell történnék.⁴

2 A kriminalisztika alapkérdései: Mi? Hol? Mikor? Hogyan? Kit? Kivel? Miért?

3 1994. évi XXXIV. törvény a Rendőrségről (Rtv.) 65. §.

4 Rtv. 63. § (4).

A bűnüldözés előzőekben bevezetett kétarcúsága tankönyvi pontossággal nem mindig választható szét a gyakorlatban. Sőt arra is akad példa (v.ö. „gyanú gyanúja”), hogy bár felmerül a bűncselekmény elkövetése, de annak gyanúja még nem áll fenn.

A bűnfelderítés vagy más szóval bűnügyi felderítés szoros rokonságban áll a bűnüldözési tevékenység hírszerzői jelleget magán viselő szektorával.

A hírszerzésalapú rendészet

A bűncselekmények felderítése érdekében igénybe vett eszközök és módszerek szerteágazók, ezek „független változója” az információ. Az információ, amelynek birtoklása szükséges a – büntetőeljárás esetén nyomozó hatóságként „viselkedő” – rendvédelmi szervnek ahhoz, hogy a bűncselekményt – vagy annak tényét és körülményeit – megállapítsa, illetve az elkövetőket azonosítsa. A bűncselekmények felderítése ezen aspektusából egy strukturált, tervezett és célzatos információgyűjtő tevékenység, amelyet egy elemző-értékelő fázis követ. E tekintetben a bűnüldözési célú felderítés a – többnyire a „hagyományos”, nemzetbiztonsági értelemben vett – hírszerzéssel rokonítható. Ez a rokonság idővel egy önálló rendészeti modell megszületését eredményezte, amire hírszerzésalapú rendészetként hivatkoznak, és amelynek lényege a proaktív természetű információgyűjtésben áll, amely a bűnügyi szolgálati ág mellett más területek (kiváltképpen a közrendvédelem) információigényét is képes lehet kielégíteni. A hírszerzésalapú rendészet (intelligence-led policing) leginkább abban különbözik a hagyományos értelemben vett hírszerzéstől, hogy míg az utóbbi célja a politikai, külpolitikai döntéshozatalhoz szükséges információk megszerzése, addig az előbbi az állam bűnüldözési feladatai teljesítéséhez nélkülözhetetlen információkra összpontosít. A hírszerzésalapú rendészetnek a magyar rendészettudomány képviselői között sincs egységes definíciója, de még elnevezése sem, például Korinek László az „adatfeldolgozás által vezérelt rendőrség” kifejezést használja rá, abban viszont konszenzus van, hogy a fogalom a bűnözés jellemzőiről felderített információkon alapuló rendészeti döntéshozatalt takar. A magunk részéről fontosnak tartjuk megjegyezni, hogy a hírszerzésalapú rendészetet nem tartjuk a reaktív rendészettel ellentétes fogalomnak. Álláspontunk szerint a bűncselekmény felderítése során (például a büntetőeljárás jog szabályai szerint folytatott nyomozásban) a rendvédelmi szerv igazságszolgáltatás előkészítése érdekében folytatott, hírszerzési jegyeket magán viselő információgyűjtő tevékenysége szintén a hírszerzésalapú rendészet körébe sorolandó, pedig erre – ahogy korábban már utaltunk rá – egyértelműen a reaktivitás

jellemző. A hírszerzésalapú rendszet erejét pontosan ebben a multifunkcionalitásban látjuk, azaz, hogy a modell a bűnüldözés proaktív bűnmegelőzési és reaktív bűnfelderítési szakaszában egyaránt alkalmazható.

A hírszerzésalapú rendszet forrásaira a katonai szakirodalomból átvett mozaikszavakkal utalunk. A teljesség igénye nélkül, létezik például humán forrás alapú hírszerzés (human intelligence, HUMINT), elektronikus jelátvitelen alapuló hírszerzés (signals intelligence, SIGINT), térinformatikai adatokon alapuló hírszerzés (geospatial intelligence, GEOINT), vagy nyílt forrású hírszerzés (open source intelligence, OSINT), stb.⁵ A források közötti hangsúlyok igazodnak a bűnügyi hírszerzés sajátosságaihoz, példának okáért a katonai felderítéshez képest kevésbé meghatározó a GEOINT, viszont a HUMINT és az OSINT kiemelt helyet foglalnak el a hírforrások között.

A nyílt forrású hírszerzésről általában

Az OSINT tevékenységet a közvélekedésben gyakran – és helytelenül – az információs társadalom felgyorsult evolúciójából fakadó aktuális trendekhez, így az internet egyre szélesebb körben való elterjedéséhez, a virtuális tér növekedéséhez, valamint a globalizáció és az interdependencia erősödéséhez kapcsolják. Az említett jelenségek kétségkívül hatékonyabbá és alkalmazhatóbbá teszik a nyílt forrású hírszerzést, mégis az OSINT fogalma sokkal korábbi történelmi időszakra vezethető vissza, és nem a világhálóhoz, hanem a hírszerzéshez mint politikai döntéstámogató módszer elterjedéséhez kapcsolódik. Az OSINT gyökerei az Amerikai Egyesült Államokban keresendők, a második világháború időszakában. A Princeton Egyetem egy kutatási kezdeményezéséből kiindulva, Roosevelt elnök 1941-ben pénzügyi forrást allokált annak érdekében, hogy a Szövetségi Kommunikációs Bizottságon (Federal Communication Commission) belül létrehozzanak egy külföldi médiamonitorozással foglalkozó részleget (Foreign Broadcast Monitoring Service). Később a részleget, ugyan már más elnevezéssel, az Amerikai Egyesült Államok Központi Hírszerző Ügynöksége (Central Intelligence Agency – CIA) szervezetébe integrálták (URL2). A részleg feladata a külföldi médiában megjelenő hírek és események nyomon követése, fordítása és az állami vezetők tájékoztatása volt. Az elmúlt több mint fél évszázadban komoly fejlődésen és számottevő átalakuláson ment keresztül az OSINT, igazodva a társadalmi és technológiai változásokhoz.

5 Dictionary of United States Military Terms for Joint Usage, Departments of the Army, Navy, and Air Force, Washington, D.C., May 1995.

A nyílt információ és a nyílt forrásból történő információgyűjtés fogalma egy gyűjtődefiníció. A fogalom meghatározás keretét a forrás típusa, hozzáféréseinek lehetőségei, az adat vagy információ megszerzésének módja adja. Ez alapján a nyílt információ és a nyílt források fogalmi elemei szűkebb értelemben véve (1) a nyilvánosság számára történő elérhetőség, vagyis a bárki, vagy – technikai és pénzügyi ráfordítás függvényében – korlátozott kör számára való hozzáférhetőség, valamint (2) a hírszerzés (bűnfelderítés) szakmai szempontjai szerinti jogszerű eszközökkel történő felkutatás, gyűjtés, strukturálás, elemzés és értékelés. A vonatkozó alapterminológia tágabb értelmezésében nyílt információgyűjtésnek tekinthető minden, ami nem tartozik a titkos információgyűjtés körébe. Fontos definícióformáló szempont, hogy a nyílt információgyűjtés azáltal válik információgyűjtő módszerré, hogy a nyilvánosan hozzáférhető információk megszerzése, elemzése és felhasználása célzottan, a bűnfelderítő (nyomozati) vagy hírszerző munka során, az ahhoz kapcsolódó eredmény elérése céljából történik.

Jelen tanulmány hipotézise a rendőrségen belül létrehozandó, központi, szolgáltató jellegű OSINT egység koncepciójának a szükségessége. Egy ilyen szervezeti egység létjogosultsága részben már az OSINT előnyeivel és hátrányaival kapcsolatos, megkövült tévhitek cáfolatából is levezethető. A következőkben néhány tévhitet vonunk vizsgálat alá.

Először is árnyalni szükséges azt a szakmai körökben elterjedt vélekedést, miszerint az internetes források jellegéből, többrétegű felépítéséből, dinamikusan növekvő, ugyanakkor – gyakran egyoldalú szándékkal megvalósuló – archiváló természetéből adódóan, a nyílt forrásokból kinyerhető adatok forrásmennyisége és az azokból származó információtömeg tekintetében előnyként értékelhető a nagy volumenű adatmennyiség. Ugyanis a források és az információk értékelése során az elemzés többletfeladatokat ró az elemzőkre, és kritikai gondolkodást igénylő kihívások elé állítja őket. Az elemzés során az adatáramlás növekvő mennyisége, sebessége és sokfélesége egyszerre jelent kihívást és lehetőséget, attól függően, hogy milyen infrastruktúra áll rendelkezésre az adatzajból az információs zaj, majd utóbbiból az adatok és információk kinyerésére.

Másodsor az a megállapítás, miszerint a nyílt forrásokból megszerezhető adatok kinyerésének költségvonzata alacsony, tehát az OSINT alkalmazásának egyik előnye, hogy gyors és költséghatékony módja az információk megszerzésének csak részben igaz. Egy ütőképes, technológiai, módszertani lépéselőnyt felmutatni tudó központi szolgáltató OSINT egység fejlett információtechnológiai infrastruktúrájához széles spektrumú, előfizetéshez kötött adatbázisok (például céginformációk, egyéb adatbázisok), az üzleti szférában elérhető, magasán képzett informatikai, adatelemzői, pszichológusi, közösségi médiaelemzői

szaktudás, valamint sokrétű nyelvismereti kapacitás, ezek megszerzéséhez és integrálásához pedig jelentős anyagi erőforrások kellenek.

Harmadszor azt a paradigmát, amely a különböző hírszerzési módszerekkel megszerzett információk arányára vonatkozik és amely szerint a megszerzett információk közel kilencven százaléka nyílt forrásból származik, napjainkra meghaladta a nyílt információgyűjtés kiemelt jelentőségének bizonyítottsága. A nyílt és humán forrásból származó információknak diffúz módon kell egy komplex információs elegyet alkotniuk, amelynek metszéspontjai az információk hitelességének, valóságának, megbízhatóságának kölcsönös ellenőrzése, kiegészítése.

Negyedszer az általános vélekedés szerint alacsony a rizikó, a nyílt internetes forrásokból történő információgyűjtés kockázatok nélküli, mivel alapértelmezetten anonim. Ezt azonban ellensúlyozza az az információbiztonsági megfontolás, miszerint az online kutatás során mindig hagyunk nyomot magunk után. Ezért különösen fontos, hogy megfelelő biztonsági környezetet, úgynevezett „online higiénia” teremtünk a nyílt információgyűjtés technikai előfeltételeként annak érdekében, hogy tevékenységünk, beleértve az azt végrehajtó személyt és szervezetet, ne legyen visszakövethető. Ez a követelmény a jelenlegi rendvédelmi IT⁶ infrastruktúra keretében a területi és központi szervek eltérő tárgybeli infrastrukturális feltételeinél fogva korlátozottan valósítható meg.

Speciális OSINT eszkörendszer, technikák, adat- és információforrások

Az OSINT eszkörendszer fontos kritériumai (1) a biztonságos használatot megalapozó környezet, (2) az online higiénia megteremtése, valamint (3) az eszkörendszer diverzifikált megvalósítása a gyártó, a beépített keresési, elemzési, monitoring funkciók, az elemzési eredmény, valamint a manuális és szoftveres eszközök kombinálhatóságának, egymással történő kiegészíthetőségének lehetősége tekintetében.

Számos manuális OSINT eszközt összegző gyűjtés, lista létezik statikus és dinamikus webes felületek formájában. Ezek gyorsan változnak és olykor kérészerűek, ennél fogva nem lehet célunk a hiánytalan összegyűjtésük. Sokkal fontosabb egy kategorizált, az információszerzési feladathoz igazodó, funkciók és források szerinti struktúrában gyűjtött naprakész eszköztár kialakítása, folyamatos karbantartása, továbbá új lehetőségek felkutatása az OSINT-tal foglalkozó

6 IT, Information Technology, magyarul információtechnológia vagy információs technológia.

szakmai felületeken található blogok és megosztott tartalmak nyomon követése. Az eszköztár dinamikus változóiban rejlő kitettség mérsékelhető az egy-egy funkcióra rendszeresített minél több eszköz, saját fejlesztésű szoftveres megoldások beépítésével, a harmadik fél által működtetett félig automatizált online megoldások kiiktatásával.

Az OSINT leggyakrabban a célszemély közösségi oldalainak, posztjainak, online jelenlétéből levonható pszichológiai jegyeinek, ismerősi körének, családi kapcsolatainak, érdeklődési körének, a hozzá köthető telefonszámok és e-mail címek, valamint a jelenlegi és korábbi tartózkodási helyeinek beazonosítására irányul. Ezen információk megszerzéséhez az elemző számos, a kutatást megkönnyítő ingyenes és fizetős eszközök tárházából válogathat, azonban ezek hatékonysága egyenesen arányos a célszemélyek által hátrahagyott digitális lábnyomok minőségével és mennyiségével. Az OSINT elemző számára az az ideális, ha a célszemély minél több információt oszt meg önmagáról, minél több helyre regisztrál, használja e-mail címét, telefonszámát. Bizonyos esetekben azonban elegendő csupán egy információmozaik az elemző számára ahhoz, hogy egy OSINT munkafolyamat megfelelő minőségű és mennyiségű információt eredményezzen.

A nyilvánosan elérhető információk forrásának és az OSINT technikáknak a köre rendkívüli ütemben bővül, azonban hasznosíthatósága ezzel egyenes arányban nem nő, amennyiben nincsenek kidolgozott eljárások a keletkezett információk valóságtartalmának, valamint a forrásoknak az értékelésére. A megfelelő ellenőrzési folyamatok nélkül az elemzett eredmény kockázatokat rejt magában. Az ellenőrzési mechanizmus keretében szükséges tehát a források hitelességének vizsgálata, az információk ellenőrzése, elemzési protokollok kialakítása.

A nyílt forrású hírszerzés alkalmazhatósága a bűnfelderítésben

A bűnüldöző szervek és a nemzetbiztonsági szolgálatok újfajta kihívásokkal néznek szembe a technológiai változásoknak köszönhetően. A hagyományos bűncselekmények és a nemzetbiztonságot érintő jelenségek már egyre nagyobb arányban jelennek meg az online térben is, így az ellenük irányuló szakmai munka is módosult a 21. században (Nouh, Nurs, Webb & Goldsmith, 2019). A bevett nyomozati eszközök a kibertérben nem működnek, és az újfajta feladatok, így az OSINT sikerességét is nagyban befolyásolja a célszemélyek tudatos internethasználata. A kibertérre és a személyes adatok védelmére irányuló felhasználói tudatosság ismerete elengedhetetlen a bűnfelderítési feladatok

végrehajtása során, mivel ez határozza meg az információgyűjtési lehetőségeket és a felderítő tevékenység irányvonalait. A terrorizmushoz köthető online tudatosság például már a 2010-es évek elején felmerült a szakirodalmi kutatásokban (Jenkins, 2011).

Az OSINT előnyeit a bűnüldöző szervek is felismerték, a módszer térnyerése a bűncselekmények felderítése érdekében folytatott hírszerzésen alapuló rendszeti eljárásokban is tetten érhető. Az OSINT bűnüldöző szerveknél történő alkalmazásával kapcsolatban egyes amerikai egyesült államokbeli szakértők rámutatnak, hogy a módszer terjedésének üteme a benne rejlő potenciálhoz képest jóval visszafogottabb. Ennek egyik okát a túlzott adatmennyiséghez viszonyított korlátozott kapacitások rendelkezésre állásában, egyes alapvető jogokkal kapcsolatos bizonytalanságokban és az elemzési képességek hiányában látják (URL3). Ezeket a megállapításokat a magyar bűnüldöző szervek vonatkozásában is helytállónak tartjuk.

A jogi bizonytalanság abból fakad, hogy az OSINT szabályozása nem egységes és egyértelmű. A módszernek relatíve kevés, alapvetően az adatvédelmi szabályokra kiterjedő jogi korlátai vannak, azonban tekintve, hogy az adatgyűjtés közhatalmi szerv működése körében és kifejezetten bűnfelderítési céllal folyik, ezért több jogszabályban foglalt előírásnak is meg kell felelnie. A bűnfelderítés során tisztában kell lennünk azzal, hogy amennyiben az ügyben büntetőeljárás van folyamatban, akkor a nyílt forrású hírszerzésnek és az abból kinyert és később bizonyítékként felhasználni tervezett információk rögzítésének is meg kell felelniük a büntetőeljárásról szóló törvény mindenkor hatályos rendelkezéseinek. Az adatok kezelésére vonatkozó törvényi rendelkezések és a belső közjogi szervezetszabályozó eszközök iránymutatásai sem hagyhatók figyelmen kívül (Koops, 2013).

A bűnüldöző szerveknél az állomány mindazon tagjai alkalmazzák az OSINT módszereket, akiknek a bűncselekmények felderítése vagy az abban való részvétel szükségyszerűen a feladatát képezi (vizsgálók, nyomozók, felderítők, egyéb szolgálati ágak és szolgálatok képviselői, területi és központi szervek alkalmazottai). Ez általában alap- és felhasználói szintű és nem professzionális keretek között történik, de sok esetben célravezető módszerekre épül (például kapcsolatrendszer feltérképezése közösségi médiafelületek alapján). Azonban az OSINT speciális ága, a közösségi médiafelületekről történő információgyűjtés (social media intelligence, SOCMINT) területén a bűnüldöző felhasználók gyakran szembesülnek a szolgáltatók konstans adatvédelmi célú defenzív törekvéseivel és a manuális OSINT eszközök lehetőségeinek, a keletkező adatmennyiség strukturált, automatizált adatfeldolgozó módszereket igénylő korlátaival. Ezekre a kihívásokra is megoldást jelenthetne egy olyan szervezeti egység, amelynek

állománya naprakész módon, készségszinten mozog a dinamikusan változó manuális és szoftveres OSINT eszközök és a „módszertani trükkök” világában.

Javaslatként és egyben előremutató szervezetfejlesztési célként fogalmazódik meg egy kifejezetten erre a célra létrehozandó szervezeti egység koncepciója, amelynek speciálisan felkészített állománya által megvalósítható a professzionális szintű, megfelelő technikai eszközökkel végrehajtott OSINT tevékenység. A továbbiakban felvázoljuk e szervezeti egység elméleti modelljét, a modell konkrét, aktuális szervezeti struktúrába illesztése nélkül.

A magyar rendőrség szervezetén belüli OSINT egység koncepciója

Jelenleg nem létezik egy olyan koncepciózus szolgáltató funkciót betöltő szervezeti egység – sem az emberi erőforrás állományt, sem az eszközrendszert tekintve –, amely a területi és a központi szervek számára egyaránt, az azok rendelkezésére álló eltérő információtechnológiai háttértől függetlenül, valamilyen mértékben túlmutat a felkérő szervek nyílt információgyűjtési lehetőségein. A modell felállítását megelőzően többek között azt szükséges tisztázni, hogy a bűnügyi szolgálati ág mely részterületeit, feladatait tudja lefedni, kiváltani a nyilvánosan hozzáférhető információk. Továbbá ezek az információk hogyan integrálhatók az egyes szolgálati ágak, szolgálatok munkafolyamataiba oly módon, hogy az operatív forrásból származó adatokat kiegészítsék, azaz hozzáadott értéket teremtsen gyűjtésük, elemzésük, felhasználásuk. A magyar rendőrség szervezetén belül létrehozandó OSINT egység jelen tanulmányban megjelenített modellje kidolgozásának első lépéseként meg kell határoznunk azokat a szolgálati ágakat és szolgálatokat, amelyek feladatrendszere indokolja az OSINT támogató tevékenység centralizált formában történő létrehozását. Ezek a belső bűnmegelőzési és bűnfelderítési, a bűnügyi, a terrorelhárítási szolgálati ág, továbbá a repülőtéri rendőri, az ügyeleti, valamint a tanúvédelmi szolgálat.

Az egység kialakításának előkészítő lépéseként az OSINT-ot mint szolgáltatást igénybe vevők vonatkozásában szükség van az OSINT szolgáltatás szempontjából releváns szakterületi igények felmérésére, a munkafolyamatok beazonosítására, mert ezekre történik majd az OSINT szolgáltatás ráépítése. Ezenfelül elkerülhetetlen a felkérők igényeihez igazodó adatbázisok, információforrások, specializált OSINT munkafolyamatok, előfizetések, eszközrendszer, IT-infrastruktúra, személyi állomány összetételének megtervezése és kialakítása. Mindezek felmérésének módja a következő kérdésekre kiterjedő, félig strukturált interjú felvétele az érintett szolgálati ágak, szolgálatok, szervezeti egységek képviselőivel:

- Mely munkafolyamatok során válik szükségessé a nyílt internetes forrásokban történő kutatás? Melyek a leggyakoribb kiinduló adatok, adattípusok, azonosítók, amelyekre OSINT végrehajtása szükséges?
- Milyen adatbázisok, információforrások, előfizetések, eszközrendszer, IT-infrastruktúra állnak rendelkezésre?
- Jelenleg mely tipikus munkafolyamatok, nyílt információgyűjtési igények vonatkozásában valósul meg az úgynevezett „sajáterős (elsőlépcsős) OSINT”? Van-e igény szakmai támogatásra az elsődleges, saját erőből végrehajtható OSINT feladatokban?
- Milyen informatikai fejlesztés, képzési módszer, képzési forma lenne szükséges a sajáterős OSINT feladatok végrehajtásához?
- Az együttműködés során a büntetőrendészeti munkát támogató nyílt információgyűjtés protokolljának kialakításához melyek a súlyponti szakmai irányelvek, szükségletek?

A kérdésekre adott válaszok értékelése és az azok mentén lefolytatott egyeztető folyamat során fontos az alábbiakat figyelembe venni.

Az érintett szervezeti egységeknél tipikus büntetőrendészeti célokhoz szükséges az egyes OSINT technikákat hozzárendelni, beazonosítani azokat a karakterisztikus indító adatokat, entitásokat (lead), amelyekre építve kidolgozhatók a szakterület-specifikus munkafolyamatok. Ennek példaként említhető a (cél)körözési szakterület esetében a célszemélyhez online jelenlét társítása, egyedi azonosítók feltárása, a családtagokon keresztüli beazonosítás lehetőségeinek vizsgálata, a vonatkozó adatbázisok mozgósítása, enumerációs technikák alkalmazása.

Kulcsfontosságú a rendelkezésre álló minden lehetséges adatforrás fúziójának megvalósítása az adatgyűjtő és -elemző folyamat során, amely a minősített információkat tartalmazó adatvagyonon túl a közhiteles adatbázisokat, a felszíni web (általános keresési lehetőségek az internet legfelső rétegében), a deep web (regisztrációhoz és/vagy előfizetéshez kötött adatbázisok, források) és a dark web (speciális keresőeszközökkel, böngészővel elérhető, az internet legmélyebb rétegében megtalálható információk tárháza) forrásrétegeit is magában foglalja.

Az adott szervezeti egység humán erőforrásának tekintetében az OSINT képességek felmérését követően meghatározandó azon OSINT alapképzési tematika, amelynek elsajátításával a felkérő szervezeti egységek optimális eredményességgel képesek elvégezni az úgynevezett sajáterős OSINT kutatást, elsősorban manuális és félig automatizált szoftveres részmegoldások igénybevételeivel. A haladó képzés keretében ismereteket kapnak a résztvevők egyrészt a haladó OSINT technikákról, eszközökről, mikro-OSINT fókuszú, azaz az entitásokra koncentráló, egyedi azonosítókra lefolytatott nyílt információgyűjtés

eszközrendszeréről, másrészt az általuk végrehajtott elsődleges OSINT kutatás lehetőségeinek kimerítésén túl a központi OSINT egység szolgáltatásainak köréről, mindezt az adott szervezeti egység ügýtípusaihoz igazítva.

A javasolt protokoll első lépése az ügygazdával történő egyeztetés a szükséges kutatási irányokról, a kérdéses háttérinformációk tisztázása, továbbá annak összehangolása, hogy a felkérőnek milyen információra lenne szüksége, mi segítené a munkáját (életút, közeli ismerősök, családtagok, érdeklődési körei, fellelhető egyedi azonosítók, közösségi média elérhetőségek). Szükség van a kutatást segítő egyéb információk, egyedi azonosítók bekérésére (releváns műveleti információk, telefonszám, e-mail cím, általuk kikutatott OSINT információk begyűjtése, így például a közösségi média elérhetőségek, kapcsolati kör stb.). Az egyeztetés részét képezi az anyag elkészítési határidejének tisztázása, valamint szükség esetén az OSINT szolgáltatások szóban történő ismertetése. Nélkülözhetetlen eleme a protokollnak a teljes adatvagyonban történő előzménykutatás, az előfizetett adatbázisokban, közhiteles adatbázisokban történő ellenőrzés, az adat- és információhalmaz vizualizációja, egyéb elemzési módszerek alkalmazása.

A nyilvánosan hozzáférhető adatok felkérő számára történő hasznos OSINT terméké alakításához multidiszciplináris megközelítés mellett, több készséget és szakértelmet ötvöző humánerőforrás-bázisra van szükség. Optimális esetben egy OSINT szervezeti egységben helyet kapnak bűnügyi/operatív elemzők, nyomozók, felderítők, informatikusok, közösségi média szakemberek, adatelemzők, pszichológusok, nyelvészek, speciális és kevésbé speciális nyelvtudással rendelkezők. A pszichológusok és a nyelvészek szaktudása értékes a szleng, az egyes csoportok, közösségek által használt speciális nyelvezet, az idegen nyelvű információk felkutatásához, elemzéséhez. Ők azok, akik tisztában vannak azzal a tágabb kulturális, földrajzi, politikai és társadalmi környezettel, amely vonatkozásában a konkrét felkérés megfogalmazódik. A humán erőforrás emberi oldala és készségei tekintetében megfogalmazódó követelményeknél a kreativitást, kitartást, monotonitástűrést, precizitást, analitikai képességet, a döntési heurisztikák kiszűrésének képességét, az erre vonatkozó hatékony önreflexiót, a csapat egészét tekintve pedig a tapasztalatok és készségek sokféleségét érdemes kiemelni. A szervezeti egység említett szakértői tehát feltárják a releváns adatforrásokat, összegyűjtik azokból az adatokat, az információkat elemzik, értékelik, végül vizualizálják az eredményt. Az egyes szakértői feladatkörök között vannak átfedések, amelyek szükségessé teszik a projektalapú, az adott feladatra létrehozott ad hoc munkaszervezési keretet. A cél saját eszköztárat felépíteni képes, a digitális lábnyomokat felkutatni és olvasni tudó, innovatív szemléletű elemzők szinergikus csapatának kiképzése, majd folyamatos továbbképzése. Ennek szellemében fontos leszámolni azzal a téves elképzeléssel, miszerint az

OSINT tevékenységet egy szervezeten belül egy korlátozott létszámú, valós eredményeket felmutatni nem tudó néhány ember végzi.

A képzés fontossága

A nyílt információgyűjtésben és elemzésben rejlő lehetőségek optimális kihasználásának érdekében az OSINT képzési rendszerének makro (temakutatásra fókuszáló) és mikro (entitáskutatásra fókuszáló) tématerületeken történő intézményi szintű fejlesztése szükséges. Ahhoz, hogy a nyílt forrású technikákban rejlő lehetőségek kiaknázhatók legyenek, a képzés professzionális megközelítésére van szükség. A képzés tematikáját az adott felhasználói közeg IT-kompetenciaszintjének, előzetes tudásszintjének, infrastrukturális korlátainak figyelembevételével szükséges meghatározni. Azonban az alábbi fő tematikai irányok megalapozzák az alap, majd a haladó OSINT szaktudás elsajátítását:

- speciális tartalomtípusok keresése: dokumentumkeresés, kutatói és tudományos adatbázisok, FTP⁷ keresőeszközök és források;
- kép- és videókereső, elemző, azonosító módszerek, fordított képkereső, videókereső módszerek, metaadatok kinyerése, videómegosztó platformokról történő információgyűjtés, videók letöltése, elemzése, szerkesztése, hitelesség és valóságellenőrzés;
- valós személyekre vonatkozó OSINT, felhasználói azonosítók alapján történő személyazonosítás;
- speciális közösségi médiakutatás eszközei (SOCMINT);
- személyekhez kapcsolódó entitásokra vonatkozó nyílt információgyűjtő tevékenység (e-mail cím, telefonszám, kiszivárogtatott adatbázisok, archivált tartalmak);
- weboldalak, metaadatok elemzése;
- szervezetekre, cégekre vonatkozó információgyűjtés;
- tartalomellenőrzés és hitelesítés (közösségi médiatartalmak validálása, alprofilok, botok kiszűrése, azonosítása, közösségimédia-bejegyzések elemzése, képek és videók elemzése, tényellenőrző eszközök alkalmazása);
- speciális nyelvtudást helyettesítő eszközök alkalmazása (fordítóprogramok, OCR⁸ lehetőségek, szöveg/hang extraktálása);
- országspecifikus, közösségspecifikus, szubkultúraspecifikus eszközrendszer kialakítása;

7 FTP, File Transfer Protocol, magyarul fájl átviteli protokoll.

8 OCR, optical character recognition, magyarul optikai karakterfelismerés.

- térképes alkalmazások;
- a dark webről történő információgyűjtés eszközei.

A centralizált OSINT egység küldetése kell legyen a szakterületi tudásbázis működtetése, amelynek keretében az együttműködők igényeihez igazítva, a folyamatos fejlődésüket elősegítve, tudásmegosztást valósít meg az OSINT területén. Fontos a felkérő szervezeti egységek olyan irányú oktatása, amely képessé teszi őket az OSINT szakértőkkel való együttműködésre, releváns kérdések megfogalmazására, a szolgáltatott információk integrálására.

Összegzés, a javaslatok összefoglalása

Jelen tanulmányunkban a bűnfelderítési tevékenység meghatározását és rendszertudományi alapjainak lefektetését követően, a bűnüldözési módszerek közül kiemeltük a hírszerzésalapú rendszert. A hírszerzésalapú rendszert egyik speciális formája a nyílt forrású hírszerzés (információgyűjtés), amelynek bűnfelderítés során való alkalmazhatóságához nem fér kétség. A magyar rendőrség jelenlegi szervezetéből ugyanakkor hiányzik a professzionális OSINT tevékenység ellátására alkalmas központosított egység. A nyílt információgyűjtő és elemző munkát a jelenlegi szervezeti keretek között széttöredezetté, kapacitáshiány, a szervezeti egységek ezirányú igényeinek tekintetében hiátus jellemzi. Az ebből adódó kihívás megoldására került kidolgozásra a központosított OSINT szervezeti egység létrehozásának gondolata.

Egy centrális szolgáltató OSINT egység keretében lennének kialakíthatók és megtervezhetők az optimális, a felkérő szervezeti egységek operatív igényeihez is igazodó technikai feltételek úgynevezett izolált munkafelületek formájában (például VPN⁹ szolgáltatás, virtuális gép használata, ingyenes, böngészőn keresztül elérhető eszközök). A legnagyobb hatékonysággal egy, az elemző szakterülethez rendelt, azon belül létrehozott centralizált OSINT egység lenne képes a teljes bűnüldözési intézményrendszer kiszolgálására hadrendbe állítani:

- az óriási adatmennyiségből történő szűrést, az ehhez optimalizált, folyamatosan karbantartott és aktualizált manuális és szoftveres OSINT eszköztárat, költséghatékony módon hosszú távon fenntartható sajtó- és adatbázis előfizetéseket;
- a felkérő szervek és szervezeti egységek sokszínűségéhez igazodó, a rendvédelmi szakmai háttérrel, valamint jelenleg csak az üzleti szférában jellemző

9 VPN, virtual private network, magyarul virtuális magánhálózat.

adatelemzői, közösségi média és marketing elemzői készségekkel rendelkező humán erőforrásbázist;

- a bűnfelderítői (bűnügyi hírszerzői, operatív) munkát tervezetten előfeldolgozással és utánkövetéssel, szoros, napi szintű, folyamatos elemzői közreműködést, a bűnüldözési igényekhez igazodó stratégiai gondolkodást megvalósító, szolgáltató szemléletű szervezeti koncepciót; valamint
- stabil, hosszútávon fenntartható információtechnológiai feltétel- és keretrendszert, segítve a releváns információ beszerzésének, az adatmennyiség feldolgozásának modernizálását.

A nyilvánosan elérhető adatok tekintetében fontos annak megválaszolása és kidolgozása, hogy ezek a források mely bűnfelderítési területeket tudják segíteni, és hogyan lehet az OSINT-ot az információszerzés folyamatába integrálni úgy, hogy a minősített információkkal együtt, vagy azok ellenőrzéseként hozzáadott értéket teremtsen. A bűncselekmények felderítése során a rétegzett – egyes büntetőeljárás szakaszokhoz igazodó – „OSINT eredmény személet” lehetővé teszi az információgyűjtési célok, specifikus részfolyamatok, az információgyűjtési források, nyelvi, eszköz- és rendszerbeli szükségletek, a közösségi média-használatból eredő sajátosságok beazonosítását, az adat- és információgyűjtés módszertanának elsődleges megtervezését. Bizonyos esetekben a nyilvánosan elérhető információk gyűjtése és elemzése hasznosabb lehet az így megszerzett ismeretek első rétegének kialakításában, értve ezalatt a „gyanú gyanújától” az elkövető azonosításáig terjedő időszakot. A magas színvonalú OSINT hatékony felhasználásával célzottabb módon bővíthetők a bűnfelderítő munka során keletkezett hiányos ismeretek.

Hangsúlyozzuk, hogy a technológiai versenyképesség fenntartása nagymértékben függ az elemzési eszközökre és adatforrásokra fordított pénzügyi források mértékétől, azonban az OSINT infrastruktúrába történő befektetés arányban áll annak egyre növekvő értékével. Az általunk felvázolt modell megvalósításával egy helyen összpontosulhatnak a költséges technikai eszközök, fizetős adatbázisok felhasználási lehetőségei; egyedi technikai előny, ezáltal prompt reagálási képesség és fokozott hatékonyság érhető el a modern bűnüldözési kihívások közepette.

Felhasznált irodalom

- Bárd K. (1986). Legalitás és bűnüldözés. *Jogtudományi Közlöny*, 41(9), 402–409.
- Finszter G. (2018). *Rendészettan*. Dialóg Campus Kiadó.

- Irk F. (2014). Deviancia, bűn, bűncselekmény, makrokriminalitás. *Jogtudományi Közlöny*, 69(4), 180–186.
- Jenkins, B. (2011). *Stray Dogs and Virtual Armies. Radicalization and Recruitment to Jihadist Terrorism in the United States Since 9/11*. Rand Corporation.
- Koops, B. (2013). Police investigations in Internet open sources: Procedural-law issues. *Computer Law & Security Review*, 29(6), 654–665. <https://doi.org/10.1016/j.clsr.2013.09.004>
- Lakatos J. (2005). *Kriminalisztikai alapismeretek jegyzet*. Rendőrtisztí Főiskola.
- Nouh, M., Nurs, J., Webb, H. & Goldsmith, M. (2019). *Cybercrime Investigators are Users Too! Understanding the Socio-Technical Challenges Faced by Law Enforcement*. Network and Distributed System Security Symposium Conference. <https://doi.org/10.14722/usec.2019.23032>

A cikkben található online hivatkozások

URL1: *Leplezett eszközök és titkos információgyűjtés, avagy az új büntetőeljárás törvény margójára*. <https://ujbtk.hu/dr-barandy-gergely-dr-enyedi-krisztian-leplezett-eszkozok-es-titkos-informaciogyujtes-avagy-az-uj-buntetoeljarasi-torveny-margojara/>

URL2: *Foreign Broadcast Information Service History, Part1: 1941-1947*. <https://www.cia.gov/readingroom/collection/foreign-broadcast-information-service-history-part-1-1941-1947>

URL3: *3 roadblocks for using OSINT in law enforcement*. <https://www.authentic8.com/blog/3-roadblocks-using-osint-law-enforcement>

Alkalmazott jogszabályok

2017. évi XC. törvény a büntetőeljárásról

2012. évi C. törvény a Büntető Törvénykönyvről

1994. évi XXXIV. törvény a Rendőrségről

Dictionary of United States Military Terms for Joint Usage, Departments of the Army, Navy, and Air Force, Washington, D.C., May 1995.

A cikk APA szabály szerinti hivatkozása

Márton B. (2023). A nyílt forrású hírszerzés (OSINT) mint lehetőség a bűncselekmények felderítésében – A rendőrségen belüli önálló OSINT egység koncepciója. *Belügyi Szemle*, 71(8), 1419–1435. <https://doi.org/10.38146/BSZ.2023.8.5>