**HERÉDI ISTVÁN**

# A nyílt forrású adatgyűjtés szerepe a kiberbűncselekmények felderítésében [1]

## Bevezetés

A nyílt forrású adatgyűjtés a 21. század egyik legjelentősebb felderítési eszköze, melynek középpontjában az adat – a modern kor új vagyoneleme – áll. Az internet lakossági penetrációjának növekedésével, a legújabb szolgáltatások megjelenésével folyamatosan nő az aktív internet-felhasználók száma, miközben a digitalizáció korát élve szinte minden adatot elektronikus formában rögzítünk.

Az adat minden kétséget kizáróan vagyon, melynek védelmére külön tudományterület specializálódott. A tömeges online tartalomfogyasztás korszakában az interneten elérhető információk szerepe jelentősen felértékelődött, értéke pedig megtöbbszöröződött. A HubSpot felmérése alapján[2] a cégek 64%-a direkt marketing tekintetében elsődleges eszköznek tekinti a SEO-t, azaz a keresőoptimalizálást, a célzott megjelenítés pedig még ennél is népszerűbb. E tevékenység kizárólag szolgáltatói szintű adatgyűjtés felhasználásával valósulhat meg – a célcsoportról a lehető legtöbb információt kell beszereznie a szolgáltatónak, melyek alapján következtetni lehet a felhasználó érdeklődési körére, személyiségére, online aktivitására, szokásaira, társas kapcsolataira, betegségeire, illetve bármilyen egyéb jellemzőjére. Ez azonban csak úgy képzelhető el, ha a felhasználó is egyre több adatot oszt meg magáról akár tudatosan, akár a tudomása nélkül. A direkt marketing mind inkább arra sarkallja a szolgáltatót, hogy a felhasználókat minél több személyes adat megadására ösztönözze.

---

[1] A tanulmány a Rendőrség Tudományos Tanácsának 2021. évi pályázatán I. díjat elért pályamű szerkesztett változata.

[2] Forrás: https://www.hubspot.com/marketing-statistics
Letöltés ideje: 2021. 10. 17.

Naivitás lenne azt gondolni, hogy a személyes és kapcsolódási adatok online gyűjtése kizárólag marketingcélokat szolgál. Az viszont tény, hogy csak a Google anyavállalata, az Alphabet Inc. 154 milliárd USA dolláros bevételt generált hirdetésekből a 2020-as évben, miközben a cég piaci kapitalizációja 1,5 billió dollárra nőtt.[3]

Milyen adatok érhetők el az interneten? Mely adatok képviselnek ekkora piaci értéket? Amennyiben a kereső- illetve közösségimédia-óriások számára ennyire hatékonyan alkalmazható az adatok rendszerezett formában történő begyűjtése és elemzése, valamint célszemélyekhez, illetve célközösségekhez való társítása, akkor felhasználhatók-e ezek az adatok bármilyen formában a bűnügyi felderítés során?

A válasz kétségkívül: igen. A nemzeti titkosszolgálatok és rendvédelmi szervek munkájának középpontjában mindig is az adatok begyűjtése és rendszerezett formában történő feldolgozása állt. A lehetőségek tárháza az internetes közösségimédia-felületek, személyre szabott tartalomszolgáltatások, streaming- és blogoldalak, fórumok, azonnali üzenetküldő alkalmazások népszerűségének növekedésével csak tovább bővült.

A legtöbb rendészeti vagy állambiztonsági szerv ma már külön az online adatgyűjtésre szakosodott egységgel rendelkezik, melynek legfőbb feladata a nyílt forrásból beszerezhető információk felhasználásával a célszemély (vagy célobjektum) és környezetének tanulmányozása, a felderítési céloknak megfelelő profilalkotás.

A kiberbűncselekmények sajátos jellemzője, hogy legtöbbször információs rendszerekhez kötődnek, túlnyomó többségüket ma már az internet felhasználásával követik el. Az elkövetés körülményeiről, valamint az elkövetőről így nyilvánvalóan ugyanezen a felületen szerezhető be a legtöbb információ.

A nyílt forrású adatgyűjtés azonban nem kizárólagosan kiberbűncselekmények, hanem a klasszikus bűncselekményi kategóriák felderítése során

[3] Forrás: https://www.cnbc.com/2021/05/18/how-does-google-make-money-advertising-business-breakdown-.html.
Letöltés ideje: 2021. 10. 17.

is hatékonyan alkalmazható, hiszen az eljárással érintett személyek túlnyomó többsége maga is internet-felhasználó.

A Készenléti Rendőrség Nemzeti Nyomozó Iroda Kiberbűnözés Elleni Főosztályának munkája során előfordult,[4] hogy egy emberölés miatt ismeretlen tettes ellen indított eljárásban kizárólag a sértett feltételezett – ám nem az interneten használttal megegyező – személynevének ismeretében, csupán online adatgyűjtési módszerek alkalmazásával pontosan felderíthetővé váltak a bűncselekmény elkövetésének körülményei, így különösen a sértett és a feltételezett elkövető, valamint segítőjének kiléte, kapcsolatba kerülésük helyszíne, módja és körülbelüli időpontja, illetve közös ismeretségi körük.

Az online adatgyűjtés nem helyettesíti a klasszikus felderítési eszközöket, azonban hatékonyan egészíti ki azokat, így álláspontom szerint a bűnügyi felderítés során nélkülözhetetlen, mással nem pótolható eszközzé vált.

## A nyílt forrású adatgyűjtés (OSINT)

A bűnügyi felderítés egyik legfontosabb célja, hogy megbízható, időszerű és releváns információkat szolgáltasson az alapjául szolgáló eljárásban. Az online térben történő adatgyűjtés hatékonyan egészítheti ki a klasszikus felderítési eszközök sorát, hiszen gyakorlatilag korlátlan mennyiségű internetes forrásból szerezhetők be adatok.

A jól megtervezett, rendszerezett formában végrehajtott adatgyűjtés csökkentheti az egyéb adatszerzésre irányuló igényt, így kizárólag olyan adatokat kell beszerezni „klasszikus” felderítési eszközökkel, amelyekhez nyílt forrásokból nem lehet hozzáférni. Az eljárás eredményességének és időszerűségének biztosítása mellett az online felderítési módszerek alkalmazásával a rendelkezésre álló erők és eszközök is hatékonyabban használhatók fel, hiszen azokat a kibertérből is beszerezhető információk összegyűjtésének feladata már nem terheli.

[4] Forrás: http://www.police.hu/hu/hirek-es-informaciok/legfrissebb-hireink/bunugyek/megolte-feldarabolta-baratjat-a-rendorok-lezartak
Letöltés ideje: 2021. 10. 21.

Az online adatgyűjtés olyan képességgel ruházza fel a rendvédelmi szerveket, amely semmilyen más felderítési eszközzel nem pótolható, az információ időszerűsége és megbízhatósága pedig több forrásból, párhuzamosan is ellenőrizhető. A bűnözés elleni harcnak – így különösen a bűnügyi felderítésnek – elengedhetetlen és szerves részét kell, hogy képezze az az eljárási módszertan, amellyel az online megosztott információk beszerezhetők, rendszerezhetők, elemezhetők és összefüggéseiben megjeleníthetők.

A nyílt forrású adatgyűjtés, angol szavakkal Open Source Intelligence (a továbbiakban: OSINT), olyan adatok beszerzését és feldolgozását jelenti, amelyek nyílt forrásból bárki számára hozzáférhetők, tehát nyilvánosak. Az adatok forrásának felkutatása, begyűjtése és elemzése egy előre meghatározott cél érdekében történik azért, hogy választ találjunk valamilyen kérdésre.

A „nyílt forrás" további értelmezésre szorulhat: nem beszélhetünk nyílt forrásról akkor, ha egy olyan adatbázisból szerzünk adatokat, amelyhez kizárólagos vagy szervezeti szintű hozzáféréssel rendelkezünk (például lakcímnyilvántartás). Nyílt forrásról beszélünk azonban akkor, amikor egy regionális vagy hozzáférés-korlátozással ellátott adatbázishoz regisztrációval, vagy külföldi IP-cím használatával férünk hozzá (például kínai közösségi média).

Az adatgyűjtés offline és online környezetben is értelmezhető, de a jelenben az utóbbi jóval nagyobb relevanciával bír, hiszen a legtöbb publikus információ online felületekről szerezhető be.

A rendvédelmi szervek tekintetében az OSINT nem kizárólag önmagában kell, hogy az adatgyűjtés alapját képezze, hanem a beszerzett információkat a rendelkezésre álló más adatforrásokkal kiegészítve, egymással összefüggésben kell vizsgálni.

Az internet lakossági penetrációjának növekedésével[5] egyre népesebbé vált a különböző online tartalomszolgáltatások felhasználói tábora. Az on-

[5] A Statista adatai alapján 2021-ben 4,66 milliárd az aktív internet-felhasználók száma, ebből 4,2 milliárd fő aktív közösségimédia-felhasználó is.
Forrás: https://www.statista.com/statistics/617136/digital-population-worldwide/

line közösségek egyik fontos jellemzője, hogy a csoportképződések a megszokottól eltérő formát is ölthetnek, hiszen az online térben tetszőlegesen hozhatók létre avatárok.[6]

Könnyen elképzelhető, hogy egy közösség tagjait vizsgálva jelentős eltéréseket észlelünk – az idősebb és a fiatalabb korosztály, különböző nációk, kultúrák, vallások egyaránt képviseltethetik magukat –, a személyeket csupán az adott alkalmazás vagy szolgáltatás használata köti össze. Az adatgyűjtés kiemelkedően fontos eleme a releváns adatforrások felkutatása.

Az adat forrásai lehetnek a különböző online platformokon elérhető szolgáltatási felületek, így különösen: a tartalomszolgáltatók, a média, a keresőmotorok, a közösségimédia-felületek, nyilvántartások-adatbázisok, publikációk, az online kereskedelmi felületek és gyakorlatilag bármely internetes tartalom, ide értve az online szürke zónaként kezelt deep, illetve dark webet is.

Az elérhető adatok köre rendkívül változatos: többek között személyes adatok, gazdasági társaságok adatai, műszaki specifikációk, technológiai információk, dokumentumok, fájlok.

A bűnügyi felderítésben az online beszerezhető személyes adatok köre a leginkább hangsúlyos kategória, hiszen a személyekre és kapcsolataikra vonatkozó információk gyűjtése talán a legegyszerűbb, ugyanakkor gyakran ez az adattípus szolgáltatja a legtöbb hasznosítható információt is – különös tekintettel a közösségimédia-felületek népszerűségére. Fontos azonban nyomatékosítani, hogy a releváns adatok köre nem merül ki az alapvető személyes és kapcsolati információkban, hiszen sok esetben akár a célszemély hálózati kapcsolatára, online jelenlétére, felhasználási szokásaira tekintettel is lehetséges további adatokat gyűjteni.

A közösségimédia-felületek az egyik legnépszerűbb platformját jelentik a célszemélyek közötti kapcsolattartásnak. A technológia fejlődésével e fe-

Letöltés ideje: 2021. 10. 17.

[6] Az avatár szót használja az internetes közösség az online személyiségek, profilok megjelölésére.

lületek száma folyamatosan nő és dinamikusan változik. A P2P-technológia, a felhőszolgáltatások, de akár még az online játékok is teret adhatnak a kommunikációnak, a csoportképzésnek, az információk megosztásának.

A 2015-ös párizsi terrortámadások következményeként került előtérbe, hogy a támadás elkövetői a Playstation 4 játékkonzol online képességeit használták fel az egymással való kommunikációra.[7] A nemzetközi bűnügyi felderítésben pedig arra is volt már példa, hogy egy kábítószer adás-vételi ügylet ellenértékének megfizetésére egy népszerű online játék virtuális pénznemében került sor.[8]

Általánosságban kijelenthető, hogy annál több információ szerezhető be egy entitásról, minél nagyobb az online aktivitása – entitás alatt személyeket, gazdasági társaságokat, földrajzi helyeket, eszközöket, illetve bármely olyan jelenséget érthetünk, amely az adatgyűjtés szempontjából releváns. Nem kizárt azonban, hogy olyan személyről szerezzünk online információkat, aki egyébként nem internet-felhasználó. Erre kitűnő példák idősebb személyek tekintetében az online elérhető keresztelési anyakönyv-adatbázisok, vagy a közösségimédia-felületeken megosztott képeket érintő bejelölések.

Az online elérhető információk tekintetében minden esetben figyelembe kell vennünk, hogy az adatgyűjtés tárgya személyes adat – sok esetben különleges személyes adat –, magán-, gazdasági, üzleti vagy banki titok, sőt, akár minősített adat is lehet.

A rendvédelmi szervek számára rendkívül hangsúlyos, hogy az adatgyűjtés során mindig a hatályos jogszabályi rendelkezésekre – különös tekintettel az adatvédelmi szabályokra – figyelemmel járjanak el, még akkor is, ha a beszerzett adatok nyíltan elérhetők a világhálón, hiszen csak így biztosítható az információk bizonyítékként történő felhasználása is.

---

[7] Forrás: https://www.forbes.com/sites/insertcoin/2015/11/14/why-the-paris-isis-terrorists-used-ps4-to-plan-attacks/?sh=53e32e137055
Letöltés ideje: 2021. 10. 17.

[8] Forrás: https://www.tripwire.com/state-of-security/featured/hackers-automate-the-laundering-of-money-via-clash-of-clans/
Letöltés ideje: 2021. 10. 17.

Az adatgyűjtés tárgya tekintetében megkülönböztethetjük

- a tájékozódó célú adatgyűjtést – mely esetben nem áll rendelkezésre elegendő információ ahhoz, hogy egy bizonyos entitás tekintetében folytassuk az adatok rendszerezett gyűjtését, vagy kifejezetten monitorozó jelleggel kívánunk adatokat gyűjteni, illetve
- a célzott adatgyűjtést, melynek keretében a tevékenység egy konkrét entitást érintően történik.

Fontos kiemelni, hogy a felderítéshez hasonlóan az adatgyűjtés esetében is megkülönböztethetjük a proaktív, illetve a reaktív kategóriákat.[9] Előbbit információvezérelt adatgyűjtésnek tekinthetjük. A cél a minél szélesebb spektrumban történő adatgyűjtés- és elemzés, majd ez alapján az értékelő jelentés összeállítása. Utóbbi esetben jellemzően egy már folyamatban lévő felderítésből származó adatok mentén folyik az adatgyűjtés, melynek célja a verziók felállítása, megdöntése vagy megerősítése.

Az adatgyűjtés módja tekintetében

- passzív adatgyűjtésről beszélünk, ha nem végzünk olyan tevékenységet, amelyet a célszemély bármilyen módon észlelhet, míg
- aktív adatgyűjtésről beszélünk akkor, ha olyan interakcióra is szükség van, amelyről a célszemély is tudomást szerezhet, például egy zárt közösségimédia-profil *„bejelölése”* vagy követése.

Az adatgyűjtés akkor hatékony, ha gondosan megtervezett, egymást logikai sorrendben követő lépésekből áll. Minden felderítés egyedi, azonban a rendelkezésre álló eszköztár a legtöbb esetben adott, így a folyamat tervezhető. Az egyes lépések, adatgyűjtési formák szükség esetén – például a rendelkezésre álló szűk időkeret miatt – mellőzhetők. Azonban a tervszerűség nem csupán a hatékonyságot szolgálja, hanem egyben garantálja,

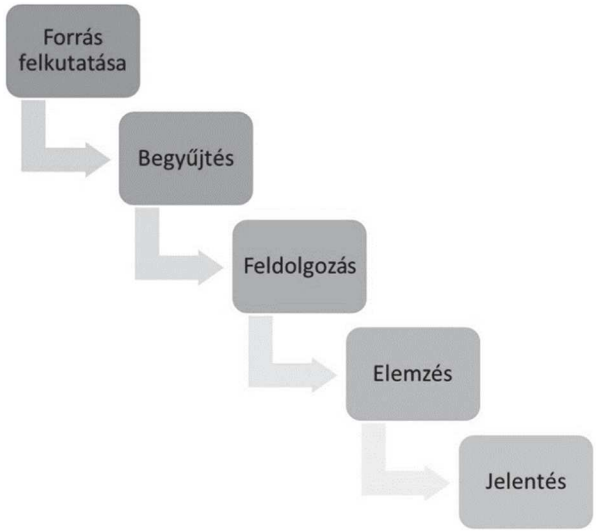
[9] Rogers C, Lewis R (szerk.): Introduction to police work. Routledge, London. 2013. 10. 8. fejezet

hogy a rendelkezésre álló információkat validált formában és a maguk teljességében lehessen összegyűjteni és bemutatni.

Az adatgyűjtés tervezése során meg kell határozni, hogy mi az adatgyűjtés tárgya, célja, milyen eredmények várhatók tőle, és milyen keretek között végezhető az online felderítés. Az egymásra épülő folyamatokat az adatgyűjtés ciklusa szemlélteti.

## Az adatgyűjtés ciklusa

Tervezhető folyamatként az online adatgyűjtés is egymásra épülő folyamatok ciklusaként jellemezhető, melyben az egyes elemek az adatszerzés egy-egy részmozzanatának végrehajtását jelölik. Az adatgyűjtési ciklus az 1. ábrával szemléltethető.

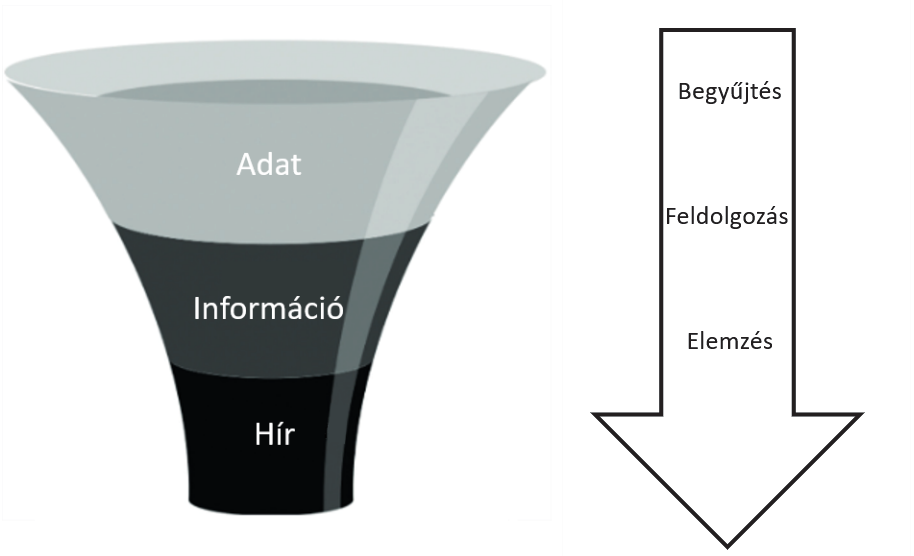



6. számú ábra
Az adatgyűjtés ciklusa

A forrás felkutatása az online felderítés szükségképpeni első eleme, melynek keretében azon szolgáltatások, illetve felületek körét kell megha-

tározni, ahonnan várhatóan releváns adat szerezhető be. A lehetséges források köre szinte sosem teljes az adatgyűjtés kezdetén, hiszen az online felderítés során – a ciklus későbbi elemeinek részét képező tevékenységek végrehajtásakor – további adatforrások merülhetnek fel, melyek tekintetében újra le kell folytatni a teljes ciklusnak megfelelő adatgyűjtést.

Az adat begyűjtése, feldolgozása és elemzése egy tölcsér modellel szemléltethető, mely az adat információvá, majd hírszerzési értesüléssé (a továbbiakban: hír) alakulásának folyamatát írja le. Ezt a modellt láthatjuk a 2. ábrán.




2. számú ábra:
A tölcsér modell

Az adat bármilyen olyan tény, ismeret, jelenség, amelyet valamilyen formában megőriztek, rögzítettek.[10] Az információ valamely entitásra vonatkozó, rendszer szerint gyűjtött adatok összessége, míg a hír ezen információ elemzéséből fakadó konklúzió.[11]

A NATO OSINT kézikönyve[12] a nyílt forrásból beszerzett adatok tekintetében egy újabb kategóriát is nevesít: a validált nyílt forrású hírt. Ez olyan elemzett információt jelent, amelynek igazságához a bizonyosság nagy foka társítható.

A kibertérben az adatok jellemzően nagy mennyiségben – sokszor ömlesztve – állnak rendelkezésre. Ezeknek a begyűjtése történhet manuálisan – online kereséssel, illetve dokumentálással – vagy automatikusan, különféle eszközök, szoftverek felhasználásával. Mivel az interneten elérhető adatok könnyen megváltoztathatók, a felkutatás után haladéktalanul intézkedni kell az adatok begyűjtéséről is.

A feldolgozás során az önmagukban reprezentált adatok egy előre meghatározott rendszer alapján összeállításra kerülnek, melyekből az elemzés során következtetések vonhatók le, majd egymás viszonylatában vizsgálva – és validálva – azokat, hírértékkel rendelkező információk keletkeznek.

A feldolgozás közben az adat mindaddig megőrzi e minőségét, amíg abból hírértékkel rendelkező, releváns információt nem tudunk kinyerni. Így a tölcsér ábrás hasonlattal élve az adat a tölcsér száján helyezkedik el, a tölcsérből pedig csak hírértékkel bíró információ juthat ki.

Ha az adatból az adatgyűjtés befejezéséig nem vonható le értékelhető következtetés, úgy önmagában nem képvisel felderítési értéket, ezért nem szükséges megjeleníteni a vizsgálati jelentésben.

---

[10] Verók Attila: Bevezetés a könyvtár- és információtudományba. Eszterházy Károly Főiskola. 2011.
Forrás: https://regi.tankonyvtar.hu/hu/tartalom/tamop425/0005_02_bev_konyvtar_es_-inftudomany_scorm_02/231_az_adat_s_az_informci_fogalma.html
Letöltés ideje: 2021. 09. 09.

[11] Negyedik kategóriaként érdemes lehet megkülönböztetni a *validált hír* fogalmát is: olyan hír, amelyhez nagyfokú bizonyosság köthető. A bizonyosság fokát az adatgyűjtésről készült jelentés összefoglalójában érdemes megjeleníteni, ezáltal is megkönnyítve az olvasóban – legtöbbször a vezetőben – kialakuló értékítéletet.

[12] NATO OSINT Handbook. SACLANT Intelligence Branch, Norfolk, VA. 2001. 3. o.

Az elemzés-értékelés külön fázisát képviseli a kapcsolatelemzés, amely a beszerzett információk közti kapcsolat alapján levonható következtetések felállításának leghatékonyabb módja. Attól, hogy valamely adat önmagában – legalább is látszólag – nem képvisel értéket, más adatokkal összevetve hasznos információkkal szolgálhat.

Az OSINT folyamatában tehát

- a forrás felderítése során azt kell megtudnunk, hol kereshetjük az adatokat;
- a feldolgozás során megállapítjuk, hogy a fellelt adatok mit jelentenek;
- az elemzés során kigyűjtjük a releváns információkat;
- majd a jelentésben prezentáljuk a célszemély profilját és/vagy az értékelt információkat.

Mind a feldolgozás, mind pedig az elemzés végrehajtható manuálisan, illetve automatikus eszközök, szoftverek segítségével.

Az adatgyűjtési ciklus befejező eleme az elvégzett tevékenység, illetve a beszerzett információk dokumentálása. Az írásos jelentés összeállításának alapelve, hogy abból az adatgyűjtés célja, a releváns adatok beszerzésének forrása, az elemzés eredménye, valamint a beszerzett hírszerzési információk hitelessége kiolvasható legyen.

Különbséget kell tenni ugyanakkor a belső használatra készült dokumentáció, illetve a mások számára készült – sokszor publikus – jelentés között.

A dokumentáció az adatgyűjtés folyamán a felderítést végző személyek által vezetett „naplószerű” feljegyzés, amely alapján bárki által visszakövethető, azonosítható és – az adatok rendelkezésre állása esetén – reprodukálható az adatgyűjtési ciklus minden eleme.

A jelentés ezzel szemben egy jóval szűkszavúbb dokumentumot jelent, hiszen azt bizonyos esetekben bárki megismerheti, így abban a pontos metodikai és technikai eljárások prezentálása nem csak szükségtelen, de célszerűtlen is.

## Az adatgyűjtés végrehajtása

Annak ellenére, hogy egy viszonylag könnyen leírható folyamatként jellemezhető, az adatgyűjtésnek mégis vannak alapvető feltételei, melyeket minden esetben szem előtt kell tartani.

Alapfeltétel, hogy olyan személy végezze az adatgyűjtést, aki ismeri annak célját, és tisztában van az adatgyűjtés tervében foglaltakkal. Alapvetően bárki gyűjthet adatokat az interneten, a legtöbbször azonban az információs igény mellett felmerül az adatgyűjtő szerv konspirációs igénye is, mely jellemzően nem kevésbé hangsúlyos. A tervezés nélkül végzett adatgyűjtést sokkal inkább adatömlesztésnek tekinthetjük, hiszen a releváns adatok és az azok közötti kapcsolat megállapítása nehézkes, sok esetben lehetetlen feladat. A tervnek természetesen nem szükséges minden esetben egy részletesen kidolgozott, specifikus tervnek lennie, hiszen a monitorozó adatgyűjtések jellegükben nagyon hasonlóak. Ebben az esetben elegendő egy típusterv alkalmazása, aminek betartásához – és az adatgyűjtő személyekkel történő ismertetéséhez – minden esetben ragaszkodni kell.

A típustervek előállításával biztosítható az is, hogy az adatgyűjtési ciklus minden eleme ugyanabban a formában reprodukálható, vagy a ciklus megszakadásakor hiánytalanul folytatható legyen.

Az OSINT során alapvető feltétel, hogy a beszerzett információk közül semmi sem vehető biztosra, csupán megfelelő bizonyossággal állítható annak valószínűsége. Az online térben megjelenített információkból levont következtetések minden esetben az objektivitás talaján kell, hogy álljanak. Akkor is, ha látszólag minden adat egy bizonyos verzió megalapozottságára utal. Kategorikus kijelentéseket csak közismert tények vonatkozásában célszerű tenni.

A verziók felállítása a sikeres felderítés egyik alapkövetelménye, melynek során bármennyire is szeretne objektív maradni az adatgyűjtést végző személy, mégis ki kell választania egy kezdeti hipotézist, melynek mentén az adatok begyűjtése el tud indulni. Az adatok begyűjtésének célja a legtöbb esetben éppen annak a megállapítása, hogy a kezdeti hipotézis igaz vagy hamis. Az információgyűjtés során arra kell választ találni, hogy mi

a legracionálisabb magyarázata annak, hogy a beszerzett adatok egy bizonyos irányba korrelálnak.

Ideális esetben az adatgyűjtés kezdetekor elegendő információnak kell rendelkezésre állnia ahhoz, hogy egy megfelelően megalapozott hipotézis mentén induljon meg a munka, és ennek megfelelően közvetlenül a releváns források kerüljenek kiaknázásra. Ez természetesen az esetek többségében nem így van, hiszen töredékinformációkból kell egy előzetes – lokalizáló – adatgyűjtéssel beszerezni azokat az adatokat, amelyek egyáltalán megalapozhatják azt, hogy egy kiinduló hipotézis felállítható legyen. A szubjektum, illetve a szakmai hozzáértés szerepének addicionális hatása talán ebben a szakaszban érzékelhető a legjobban. A kiinduló hipotézis felállításához megfelelő szakértelem szükséges azon a területen, amelyen az adatgyűjtés végrehajtásra kerül, hiszen annak hiányában nem lehet értékítéletet alkotni a tények hitelességével és a verziók életszerűségével kapcsolatban.

Az egyén értékítéletének objektivitást torzító hatása úgy küszöbölhető ki, hogy az adatgyűjtést több személy végzi, illetve a validálás során megjelölésre kerülnek a kérdéses információk hitelességét erősítő és azokat gyengítő állítások is. Ha a beszerzett információk korrelációja harmadik személy számára is elfogadható bizonyossággal állítható értékelést tartalmaz, akkor az adatgyűjtés sikeresnek tekinthető. Ha a kezdeti hipotézis az adatgyűjtés során nem nyer megerősítést, akkor új hipotézis felállítása szükséges.

Ha a nyílt forrású adatok begyűjtésére és az értékelő jelentés elkészítésére olyan eljárásban kerül sor, amelyben lehetőség van az adatok korlátozott hozzáférésű adatbázisokból származó információkkal történő összevetésére is, úgy ezek tekintetében szükséges lehet egy szintetizáló jelentés elkészítése is. A két jelentés a felderítő szerv igénye szerint egyetlen dokumentumba is összevonható, ez esetben azonban nem kizárólagosan nyílt forrású adatgyűjtésről készült jelentésről beszélünk.

Az adatgyűjtést végző személy vagy szervezet az adatok összegyűjtése során rendkívül nagy mennyiségű információt is feldolgozhat, így tisztában kell lenni azzal a jogszabályi környezettel is, ami lehetővé teszi az adatok

begyűjtését és feldolgozását. A beszerzett adatok kezelése meg kell, hogy feleljen a jogszabályok által támasztott követelményeknek. És ha az adatgyűjtés eredménye valamely eljárásban felhasználásra kerül, különös tekintettel kell eljárni az adatok validálása és az eszközök konspirációja terén is.

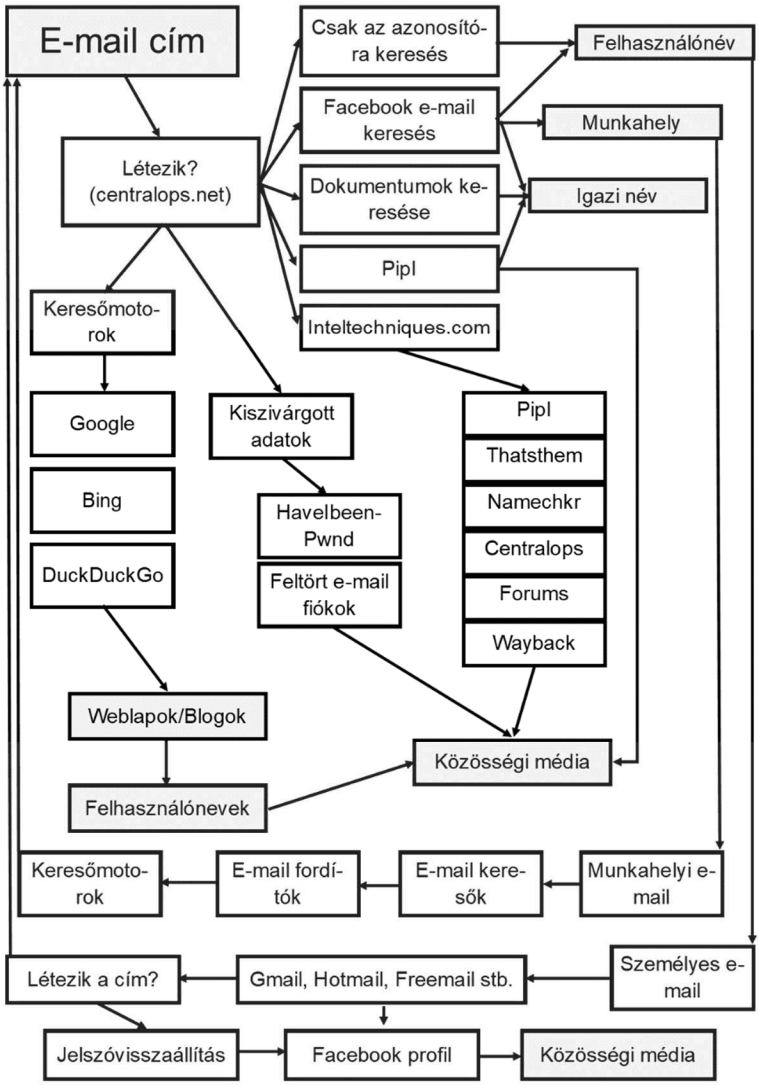
Az online kutatás hatékonyabbá tétele érdekében információszerzési modellek állíthatók fel,[13] amelyeket követve a különböző forrásokból indulva előre meghatározott tevékenységi folyamatként írható le az adatgyűjtés, így annak eredménye is minden esetben azonos kell, hogy legyen.

A legegyszerűbben folyamatábrák felhasználásával lehetséges célirányos és tervezett adatgyűjtést végezni. A folyamatábra a felderítési vonatkozások és körülmények függvényében egyedileg alakítható ki – de természetesen léteznek általános érvényű munkafolyamatok is.

A 3. ábra[14] az e-mailek tekintetében végezhető adatgyűjtés gyakorlati algoritmusát ábrázolja. A vázlat megértéséhez természetesen szükséges az alapvető keresési lehetőségek ismerete is, azonban itt sokkal inkább a keresési folyamat szemléltetése a hangsúlyos, mellyel a keresés minden esetben egy mechanikus folyamat részét fogja képezni, így a hiba kockázata minimálisra csökkenthető.

[13] Staniforth, Andrew: Police Use of Open Source Intelligence: The Longer Arm of Law. In: B. Akhgar et al. (eds.): Open Source Intelligence Investigation. Springer International Publishing AG. 2016. 28. o.

[14] Bazzell, Michael: Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information 6th edition. 2017. 445. o.




**3. számú ábra**
**E-mailek tekintetében végezhető adatgyűjtés gyakorlati algoritmusa**

Különösen fontos a beszerzett adatok tekintetében az egységes validálási eljárás bevezetése, valamint az információértékelés uniformitásának biztosítása is. A felderítési munka tekintetében meg kell állapítani az alábbiakat.

**A forrás megbízhatósága**[15]

| | Értékelés | Leírás |
|---|---|---|
| **A** | Megbízható | Nem kétséges a forrás hitelessége, illetve megbízhatósága. |
| **B** | Általában megbízható | Csak kevés kétely fér a megbízhatóságához, korábban főként megbízható információ származott innen. |
| **C** | Elég megbízható | Kétséges a megbízhatósága. Származott már belőle megbízható információ. |
| **D** | Nem mindig megbízható | Jelentős kétségek merülnek fel, de származott már belőle megbízható információ. |
| **E** | Nem megbízható | Nem származott belőle még megbízható információ, nem megbízható. |
| **F** | Nem lehet eldönteni | Nincs elég információ a besoroláshoz. |

[15] Forrás: https://www.first.org/global/sigs/cti/curriculum/source-evaluation
Letöltés ideje: 2021. 09. 17.

**Az információ megbízhatósága**[16]

| | Értékelés | Leírás |
|---|---|---|
| **1** | Megerősített | Logikus, konzisztens, más releváns információkkal, valamint más forrásból is megerősített. |
| **2** | Valószínűleg igaz | Logikus, konzisztens más releváns információkkal, de nem megerősített. |
| **3** | Lehet, hogy igaz | Valamennyire logikus, más releváns információkkal egybevág, nem megerősített. |
| **4** | Kétséges, hogy igaz | Nem logikus, de lehetséges, nincs más információ ezt érintően, nem megerősített. |
| **5** | Valószínűtlen | Nem logikus, más információval ellentétes. |
| **6** | Nem lehet eldönteni | Nincs elég információ a besoroláshoz. |

Az adatgyűjtés szempontjából alapvető követelmények tehát a következőkben foglalhatók össze:

- Az adatgyűjtésnek törvényesnek kell lennie, azt kizárólag célhoz kötötten, a szükséges és arányos mértékben kell végrehajtani.
- Az adatgyűjtés előfeltételeit a humán és az eszköz oldalon egyaránt biztosítani kell.
- Az információs és a konspirációs igény közötti egyensúly csak meghatározott esetekben, előre tervezett módon borítható fel.
- Az adatgyűjtés során beszerzett információkat objektíven kell megítélni és validálni, azokat megbízhatóság szerint értékelni kell.

[16] Forrás: https://www.first.org/global/sigs/cti/curriculum/source-evaluation
Letöltés ideje: 2021. 09. 17.

– A kezdeti hipotézisből kiindulva verziókat kell felállítani a beszerzett információk alapján, az adatgyűjtésnek pedig a legvalószínűbb verzió(ka)t kell az értékelésben tartalmaznia.
– Az adatgyűjtési ciklust megfelelően felkészített állománnyal, tervezett és dokumentált módon kell végrehajtani.

## Az internetről beszerezhető adatok

A nyílt forrású adatgyűjtés alapját az internetről beszerezhető adatok jelentik, melyek az OSINT-ciklusban történő feldolgozást követően válnak hírszerzési értékkel bíró információvá. Az adatok bűnügyi felderítési célból történő összegyűjtésének tekintetében fontos hangsúlyozni, hogy az adatgyűjtés az eljárás sikerének biztosítása érdekében, célhoz kötötten, szükséges és arányos mértékben kell, hogy történjen. Az nem vezethet nagy mennyiségű személyes adat önkényes „letárolásához".

Az interneten elérhető adatok köre minden személyre vonatkoztatva más és más. Jellemzően a célszemély internetes aktivitásával arányosan nő az online térből beszerezhető információk mennyisége.

Az internetes aktivitás nem csupán aktív szolgáltatás-felhasználást jelent, hiszen egy egyszerű böngészési folyamat is nyomot hagy maga után.[17] Az online adatgyűjtés során ezért minden esetben úgy kell eljárni, hogy a lehető legtöbb információt szerezzük be a célszemélyről, és mindeközben a legkevesebb információt hagyjuk hátra saját tevékenységünkről.

Az adatgyűjtés célja nem egyszerűen információk beszerzése, hanem a releváns adatforrások felkutatása. Gyakorlatilag a kutatás a nyílt forrású adatgyűjtés lelke, amelynek során beazonosításra kerülnek az adatgyűjtés célja szempontjából releváns források, az ezekből származó információkkal pedig megválaszolhatók a feltett kérdések.

[17] Amennyiben az adatgyűjtéssel érintett személy hozzáfér a felkeresett webszerver adminisztrátori felületéhez, akkor arról is értesülhet, hogy számára ismeretlen személy – esetlegesen hatósági IP-cím tartományba tartozó eszközről – látogatta az érintett webhelyet, melynek azonosítását követően a webhelyen – vagy akár más weblapokon – végzett tevékenysége is megismerhető.

A Statista, valamint a Nemzetközi Távközlési Unió (a továbbiakban: ITU) statisztikája[18] alapján 2021-ben 4,66 milliárd volt az aktív internet-felhasználók száma, melyből 4,2 milliárd fő egyben rendszeresen jelen volt valamely közösségimédia-felületen is.[19] Csak a Facebook felhasználói közössége megközelíti a 2,89 milliárd főt[20], mely szám annak tekintetében igazán nagy, hogy például az ázsiai vagy orosz felhasználók jelentős része alapvetően más – regionális – közösségi felületet használ.

Az aktív internet-felhasználók egy-egy böngészési munkamenet során rengeteg online információt hagynak maguk után a kibertérben, melyek nem csupán személyükre, hanem hálózati kapcsolatukra, internetezésre használt eszközeikre, társadalmi kapcsolataikra, érdeklődési köreikre, online aktivitásukra és rengeteg egyéb más tulajdonságukra utaló adatot is hordozhatnak.

Az adatok forrásuk helyén strukturált, illetve strukturálatlan formában egyaránt fellelhetők. A strukturált formában megtalálható adatok jellemzően olyan adatbázisokból származnak, amelyek elemei valamilyen szabály alapján épülnek egymás köré. Ilyen például egy relációs adatbázis. A strukturálatlan adatok ezzel szemben nem rendelkeznek olyan egyértelmű összefüggésekkel, amelyek alapján kétséget kizáróan és azonnal kikövetkeztethető lenne az adatok közötti kapcsolat.

Az adatgyűjtés tervezésekor meghatározható, hogy annak célja tekintetében vélhetően mely forrásokból lehet a legtöbb – releváns – adatot beszerezni. A lehetséges források köre rendkívül sokszínű. A korábban már említetteknek megfelelően az adatok forrásai lehetnek a különböző online platformokon elérhető szolgáltatási felületek, így különösen: a tartalom-

[18] Forrás: https://www.google.com/search?client=firefox-b-d&q=international+telecommunication+union
Letöltés ideje: 2021. 10. 17.

[19] Forrás: https://www.statista.com/statistics/617136/digital-population-worldwide/
Letöltés ideje: 2021. 10. 17.

[20] Forrás: https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/
Letöltés ideje: 2021. 10. 17.

szolgáltatók, a média, a keresőmotorok, a közösségimédia-felületek, a nyilvántartások-adatbázisok, a publikációk, az online kereskedelmi felületek és gyakorlatilag bármely internetes tartalom – ide értve az internet *„szürke zónáját”*, a deep és a dark webet is.

Az adatok formájukat tekintve lehetnek adatbázisok, szabadszöveges tartalmak, képek, hanganyagok, videók, API-lekérések[21], dokumentumok, illetve egyéb fájlok.

Beszerzésük tekintetében automatizált folyamatok részeként vagy manuálisan gyűjthetők, mely metódusok a képzeletbeli skála két végpontján helyezkednek el, így azok szintetizálása is elképzelhető. Az automatizált begyűjtési forma az adatgyűjtések kezdetére jellemző, míg a jóval időigényesebb manuális vizsgálat általában az adatgyűjtés ciklusának későbbi fázisaiban hangsúlyos.

Az adatforrások rendkívül változatosak, gyakorlatilag bármilyen internetes tartalom potenciálisan releváns információt rejthet. Az adatok beszerzése leggyakrabban mégis közösségimédia-felületeken vagy a keresőmotorok által beindexált és hivatkozott tartalomszolgáltatói felületeken történik meg.

**Keresőmotorok**

A keresőmotorok segítségével hatékonyan szűrhetők a felszíni interneten elhelyezett tartalmak, a helyes keresőkifejezés alkalmazásával célzottan – kizárólag az adatgyűjtés szempontjából releváns találatokat megjelenítve – lehet böngészni a találati listát.

Az ilyen szolgáltatások nagy előnye, hogy egy előre felépített adatbázisból, az úgynevezett *„index-állományból”* dolgoznak, így a találatok megjelenítése gyakorlatilag azonnal megtörténik. Fontos azonban, hogy a keresőrobotok is csak bizonyos időközönként keresik fel a beindexálandó

[21] Az API vagy magyarul alkalmazásprogramozási felület egy program vagy szolgáltatás más programok által felhasználható részeinek összessége.

oldalakat, így elképzelhető, hogy egy relatíve friss tartalom nem fog szerepelni a találati listában. A weboldalak üzemeltetői meg is tilthatják a keresőrobotoknak azt, hogy az oldal egészét vagy annak egy részét beolvassák. Ezt egy egyszerű szövegfájl – a robots.txt – web gyökérkönyvtárban történő elhelyezésével tehetik meg, amely szintén árulkodó lehet a keresők elől elrejteni kívánt könyvtárak tekintetében.

A pontosabb szűréshez bővített keresési lehetőségek is rendelkezésre állnak, melyeket úgynevezett *„keresési előtagok”* alkalmazásával lehet elérni. A Google esetében a legalapvetőbb előtagokat tekintve

– konkrét kifejezésekre, szóösszetételekre lehet keresni az idézőjel,
– szavakat lehet kizárni a találati listából negatív előtag,
– adott domain-re irányítható a keresés a site: előtag,
– az URL-ben lehetséges keresni az inurl: előtag,
– fájlokra lehet keresni a filetype: előtag

alkalmazásával.[22]

A keresőmotorok a beindexált tartalmak indexálás pillanatában történő állapotának megtekintését is lehetővé teszik az úgynevezett cache-elt verzió megjelenítésével. A Google esetében erre a találati listaelem hivatkozási sora mellett megjelenő lefelé mutató nyíl kiválasztásával nyílik lehetőség. A tárolt verzió egyfajta webarchívumként is szolgál, hiszen az időközben megváltozott tartalom is a korábbi, eredeti formájában tekinthető így meg. Elképzelhető tehát, hogy egy – az adatgyűjtés szempontjából releváns – bejegyzést időközben eltávolítottak, az ilyen pszeudo-archív tartalmak között azonban továbbra is elérhető.

Nem csupán szöveges tartalmak, hanem akár képek, hálózatra csatlakoztatott eszközök, szolgáltatások, forráskódok keresésére is lehetőség van.

[22] A Google-keresési kifejezések teljes listája a Google hivatalos weboldalán érhető el a https://support.google.com/websearch/answer/2466433 hivatkozási címen.
Letöltés ideje: 2021. 09. 17.

A kép alapján történő keresést többek között a Google képkeresőjével vagy a TinEye nevű szolgáltatással érdemes végrehajtani. A kép-visszakeresés nem eredményezhet arcfelismerést, hiszen az a személyes adatok védelme szempontjából aggályos lenne. A keresés színtelítettség, kontúrok, hisztogram-hasonlóság és egyéb tulajdonságok alapján történik, így a legtöbb esetben nem csak azonos, hanem hasonló találatokat is eredményez.

Az OSINT tevékenység során különös figyelemmel kell eljárni az olyan szolgáltatások használatakor, mely esetekben tartalommegosztás történik egy harmadik féllel – jelen esetben a keresőszolgáltatóval. A keresőmezőbe bevitt, vagy a képkeresőbe feltöltött adatok az érintett szolgáltató rendelkezésére állnak, azokat üzleti vagy marketingcélokra is felhasználhatja, így minősített, érzékeny vagy jogszabályba ütköző tartalmak megosztása kifejezetten tilos.

A „szokványos" keresőszolgáltatások mellett speciális keresők is használhatók az adatgyűjtés során, melyek segítségével hálózati eszközöket és szolgáltatásokat, programkódokat, videókat lehetséges megkeresni. Ezek közül kiemelkedik a Shodan nevű platform, mely a hálózatra kapcsolt eszközök, szolgáltatások és azok jellemzői tekintetében nyújt keresési lehetőségeket.

**Közösségimédia-felületek**

A közösségimédia-felületek alapvetően szociális kapcsolatépítés céljából jöttek létre, mára azonban szinte egy „kisebb internetté" nőtték ki magukat az interneten belül. A piacot jelenleg kis számú óriás uralja, bár léteznek kisebb felhasználói bázissal rendelkező tematikus vagy regionális közösségimédia-felületek is.

Egyes felmérések szerint[23] az aktív internet-felhasználók 93%-a egyben közösségimédia-felhasználó is, így azok üzemeltetői rendkívül robosztus

[23] Forrás: https://backlinko.com/social-media-users
Letöltés ideje: 2021. 10. 21.

adatbázissal rendelkeznek, melyekből nem csupán a célszemélyre vagy entitásra, hanem annak kapcsolataira vonatkozó információk is kinyerhetők. Mivel alapvető céljuk a kapcsolatépítés, illetve a felhasználói interakciók kiváltása, ezért jellemzően relációs adatbázisként kezelhetők, az abból fellelt adatokból pedig kapcsolati ábrák is építhetők.

A passzív profilok tekintetében is lehetőség nyílik további adatok beszerzésére, hiszen a szolgáltatások alapvető célja a felhasználói interakciók kiváltása. Annak hiányában a tartalomszolgáltató el is távolíthatja az adott profilt. Ennek felhasználásával egy entitás tekintetében nem kizárólag saját profiljáról, hanem kapcsolatain keresztül is végezhető adatgyűjtés, teljesen passzív – valós – felhasználó kizárólag passzív ismerősökkel pedig saját tapasztalatom szerint nem létezik – hiszen értelmét vesztené a felület közösségi jellege. Így valamilyen mennyiségű adat jellemzően az aktivitással látszólag nem rendelkező profilokról is begyűjthető.

Külön említést érdemel a közösségimédia-felületen jelen nem lévő személyek esete. Ha egy entitás nem szerepel a felhasználói adatbázisban, azonban valamely ismerőse – például egy csoportképen – megjelölte az adott személyt, úgy a szolgáltató maga alkotja meg profilját – csupán közvetlen hivatkozás nélkül. Annak ellenére, hogy az adott profil vagy adatlap nem létezik, az entitás elnevezése alapján kereshetővé válik, és a vele kapcsolatos említések, bejelölések megjeleníthetővé válnak.

Fontos jellemzője az ilyen szolgáltatásoknak, hogy általában okoseszközre telepíthető alkalmazásból is elérhetők, így pedig a megosztásokkal kapcsolatban akár készülékazonosítók vagy geolokációs koordináták is beszerezhetők. Az azonnali üzenetküldési funkcióval rendelkező szolgáltatások esetében lehetőség nyílik arra is, hogy az okoseszköz névjegyzékét szinkronizálva az adott felületen használt telefonszámokra keressünk.

A közösségimédia-felületeken tett interakciók számát kapcsolati fokként használva súlyozott gráfok állíthatók elő az egymással vélt vagy valós kapcsolatban álló személyekről.

## Egyéb tartalomszolgáltatók

Az egyéb adatforrásokat tekintve rendkívül hosszú lista állítható fel arra vonatkozóan, hogy milyen adat jellemzően milyen forrásból szerezhető be. A keresőmotorok, illetve a közösségimédia-felületek képezik a legnagyobb adatforrást, azonban a célszemély internetes aktivitásával arányosan nő azoknak a felületeknek a száma, ahonnan az adatgyűjtés szempontjából releváns adat szerezhető be.

Minél több szolgáltatást, minél több online platformot használ a célszemély vagy annak környezete, annál több forrást kell felkutatni is. A potenciális adatforrások meghatározása minden esetben az OSINT tervezési folyamatának része, és különböző korú, nemzetiségű, foglalkozású, illetve érdeklődési körű személyek esetében más és más.

A felderítő szerv feladata többek között egy olyan adatbázis működtetése, amely a különböző potenciális adatforrások listáját tartalmazza, de online keresésekkel is felkutathatók újabb források.

Az adatgyűjtések során hasznos lehet többek között az adatbázisok, interneten megosztott fájlok, dokumentumok, képek – és azok metaadatainak – vizsgálata, hálózati eszköz vagy szolgáltatásokat indexáló felületek ellenőrzése.

Ha a célszemély saját maga is üzemeltet valamilyen tartalomszolgáltatást, vagy épp egy hálózati infrastruktúrával kapcsolatban kell adatot gyűjteni, úgy ezek járulékos információként szintén felhasználhatók. Kiemelendő, hogy az adatgyűjtés nem csupán szöveges és grafikus tartalmak felkutatására kell, hogy irányuljon. Sok esetben a metaadatokból, kapcsolati információkból, szerverarchitektúrával kapcsolatos információkból vonható le olyan következtetés, amely az adatgyűjtés kezdeti hipotézisét vagy a felállított verziók valamelyikét igazolja/erősíti, vagy éppen cáfolja/gyengíti.

Külön említést érdemelnek az internetes archívumok, mint például a Wayback Machine. Ezek a szolgáltatások különféle weboldalak pillanatképét tárolják el, mintegy könyvtárat készítve az internet éppen aktuális álla-

potáról. Az érintett weboldal látogatottságával arányban áll a készített pillanatképek száma, azonban bármely oldalról kérelmezhető mentés közvetlenül a szolgáltatásban vagy az azzal kompatibilis böngésző-bővítményeken keresztül. Az archívum vizsgálatával korábban törölt adatok megtekintésére is lehetőség nyílik.

## Nyílt forrású adatgyűjtés a rendvédelmi szervek aspektusában

A rendvédelmi szervek alapvető feladatai közé tartozik a közrend, közbiztonság védelme, a bűncselekmények elkövetésének megelőzése és felderítése, mely tevékenységek elképzelhetetlenek időszerű és releváns információk beszerzése nélkül. Ezért e szervek feladata a beszerzési folyamat megtervezése, az adatok begyűjtése, feldolgozása és értékelése.

E szervek adatgyűjtésük során a jogszabályi keretek által meghatározott eszközökön túl mindig is használtak fel nyílt forrásokat. Azonban míg korábban ez főként helyi vagy regionális szintre összpontosult, a globális hálózatokkal összekapcsolt világban a felderítés már nem csupán lokális keretek között zajlik, hiszen a bűncselekmények elkövetői is transznacionális dimenzióban tevékenykednek.

A bűnüldöző szervek számára kiemelt lehetőséget teremt az internet, mint potenciális, nyílt felderítési adatok forrása. Jelentősége nem csupán abban áll, hogy nagy mennyiségű adat szerezhető be, hanem abban is, hogy relatíve alacsony ráfordítással olyan adatok is beszerezhetők, amelyek leplezett eszközök alkalmazásával sem kerülnének a felderítő szerv birtokába.

A felderítés hatékonysága abban mérhető, hogy a beszerzett információkat milyen mértékben képes feldolgozni az adatgyűjtést végző szerv. Előnyös helyzetet jelent számukra, hogy a nyílt forrásból beszerzett adatokat a rendelkezésükre álló közhiteles adatbázisokban – például személyek nyilvántartása – ellenőrizni tudják, így az adatgyűjtés eredménye pontosabban validálható.

## OSINT a bűnügyi felderítésben

A bűnügyi felderítésnek rendkívül hasznos eszköze lehet a nyílt internetes forrásokból származó információk begyűjtése, melyeket a rendőrségi adatbázisokból származó adatokkal kiegészítve egy átfogó környezettanulmánynak megfelelő minőségű profil állítható fel a célszemélyről.

Míg a hivatalos nyilvántartások, rendőrségi adatbázisok egy viszonylag statikus adattartalommal rendelkeznek, melyek csak a hatósági érintkezések során frissülnek, addig a nyílt interneten olyan dinamikusan változó tartalmakat lehet begyűjteni, amelyeket a célszemély vagy közvetlen környezete oszt meg, illetve az általuk végzett interakciók révén válnak elérhetővé. Az interakciók alatt nem feltétlenül aktív tartalommegosztást kell érteni, hiszen önmagában egy okoseszköz vagy valamely szolgáltatás használata is keletkeztet információkat. Valamint elképzelhető, hogy nem is közvetlenül a célszemély, hanem annak környezete oszt meg számunkra értékelhető, hasznos információt.

A bűnügyi felderítés jellemzően a hivatali munkavégzéshez köthető, azonban a büntetőeljárás eljárási cselekményeiként végzett tevékenységeket el kell határolni a nyílt forrású adatgyűjtéstől. Mint hogy minden online tevékenység nyomot hagy maga után, így a felderítő szervek tagjai által végzett keresések is visszakövethetők, az adatgyűjtés alapvetői szabályainak be nem tartása esetén pedig ezek az adatok közvetlenül is köthetők az adott hatósághoz.

Tegyük fel, hogy az adatgyűjtést végző személy értesül a célszemélyhez (és egyben az elkövetéshez) köthető webhely elérhetőségéről. Az adott szolgáltatáshoz az irodájában lévő számítógép felhasználásával csatlakozik, amelynek internetkapcsolatát valamely állami szolgáltató biztosítja, a címtérből pedig az is megállapítható, hogy az adott IP-cím melyik szervhez köthető. Ha a célszemély hozzáfér a beazonosított webhely naplófájlaihoz, úgy könnyedén azonosítani tudja az adatgyűjtéshez használt munkamenetet, ezáltal pedig tudomást szerezhet arról is, hogy valaki kutat utána. Ezt elkerülendő az adatgyűjtést végző személynek lepleznie kell személyazonosságát és egyben hálózati kapcsolatát is.

A leplezett adatgyűjtés végrehajtásához a rendvédelmi szerveknek is különböző avatárokkal kell rendelkezniük az interneten, melyek profiljainak karbantartása is szükséges a dekonspiráció elkerülése végett. Gyakori hiba, hogy a felderítő szerv létrehoz ugyan egy internetes profilt, de azon tartalmakat nem oszt meg, csak kevés és véletlenszerűen kiválasztott ismerőst gyűjt, és azokkal nem végez semmilyen interakciót. Egy, az adatgyűjtésben jártas személy számára könnyű feladat a passzív, csupán hírszerzésre használt profilok azonosítása.

## Kiberbűncselekmények felderítése

A kiberbűncselekményeket alapvetően az alapján kategorizálhatjuk, hogy az információs rendszer az elkövetés tárgya vagy annak eszköze.
Az angol nyelvű szakirodalom[24] az úgynevezett *„cyber dependent crime”* kifejezést használja azon kiberbűncselekményekre, amelyek során valamely információs rendszert ér támadás. Kizárólag a kibertérben követhetők el azok a cselekmények, amelyek elkövetési magatartása kifejezetten valamely információs rendszert érinti – az elkövetés során az információs rendszer bizalmassága, sértetlensége vagy rendelkezésre állása sérül. Ilyen bűncselekmények jellemzően a túlterheléses támadások, a rosszindulatú kódok alkalmazása vagy a rendszerfeltörések.

Az úgynevezett *„cyber enabled”* vagy kibertérben is elkövethető bűncselekményi kategória esetében ezzel szemben olyan – „klasszikus” módszerekkel is elkövethető – bűncselekményekről beszélünk, amelyekhez a kibertér egy újfajta elkövetési eszközként szolgál. Ilyen lehet például egy online csalás, melynek tevékenységi folyamata, a tévedésbe ejtés, megvalósulhatna akár egy telefonhívással vagy személyes kapcsolatfelvétellel is, az elkövető azonban ehelyett a kibertérben fejti ki az elkövetési magatartást, ez elkövetés eszköze pedig az általa használt információs rendszer.

[24] EUROPOL: Internet Organised Crime Threat Assessment (IOCTA) 2017., The Hague, 2017. 18. o.

A bűnügyi felderítés alapelvei a kibertérben is változatlanok, ugyanúgy a kriminalisztika hét alapvető kérdésére keressük a választ, melyek: mi, hol, mikor, hogyan, ki, kivel, miért?

A klasszikus bűncselekmények felderítéséhez képest alapvető eltérés, hogy az elsődleges intézkedések túlnyomó részét a kibertérben kell végrehajtani. Az információs rendszerek közötti tájékozódást elsősorban az online adatgyűjtés teszi lehetővé. Az elsődlegesen beszerzett adatok jellemzően

- név(töredék),
- felhasználónév vagy felhasználó azonosító,
- e-mail cím,
- IP-cím,
- domain-név, illetve
- telefonszám.

**Név, felhasználónév**

A nevek illetve felhasználónevek ellenőrzése online adatbázisokban, a tartalomszolgáltatók felületén megjelenített elemekben, illetve a közösségimédia-felületeken történő kereséssel történhet. A tájékozódó célú adatgyűjtés során azt szükséges megállapítani, hogy

- az adott név valós – mely esetben a keresőmotorok használatával érdemes célzott keresést végrehajtani általános információk beszerzése végett, majd a rendelkezésre álló adatbázisokban (például felhasználó-adatbázisok, archívumok, közösségimédia-felhasználói adatbázisok) végzett keresés eredményeként a lehető legtöbb adatforrás felderítése mellett konkrét célszemélyre kell szűkíteni az adatgyűjtést;
- vagy kitalált név – mely esetben azt kell megállapítani, hogy honnan eredeztethető az adott névhasználat.

## E-mail cím

Az e-mailek feladójával kapcsolatos adatgyűjtések elengedhetetlen eleme az e-mail fejlécének[25] vizsgálata. A fejléc nélkül nem vonhatók le érdemi következtetések az e-mail feladójának személyére, valamint az elektronikus üzenet kézbesítéséhez használt infrastruktúrára vonatkozólag. Az e-mail eredeti formájának megtekintésére a legtöbb szolgáltató lehetőséget biztosít, így a törzs mellett láthatóvá válnak a fejlécben tárolt adatok is. A fejléc vizsgálatához ingyenesen hozzáférhető szoftverek is rendelkezésre állnak, ilyen többek között az MxToolbox[26], illetve a Google Admin Toolbox.[27]

Az e-mailek felhasználásával elkövetett bűncselekmények felderítésének elengedhetetlen mozzanata az eredeti elektronikus üzenet beszerzése. A leggyakrabban használt e-mail kliensek esetében a Beállítások vagy az Üzenet menüponton keresztül lehet elérni az eredeti e-mailt, majd azt adott fájlformátumban le kell menteni, vagy egyszerű szövegként ki kell másolni a teljes tartalmat.

Egyes esetekben nem kerülhető el az üzenet fejlécmezőinek manuális vizsgálata, mivel az automatizált szoftverek sem képesek minden információt maradéktalanul megjeleníteni. A fejlécmezőkből megállapíthatjuk: a feladáshoz használt eredeti e-mail fiókot, a kézbesítési láncot – így a küldéshez használt hálózati infrastruktúra IP-címeit is, az esetleges átirányításokat, késleltetéseket, eltérő időzóna-beállításokat, a küldéshez használt szolgáltatást, és ennek függvényében számos egyéb, járulékos adatot, melyek információval szolgálhatnak az üzenet megküldésével kapcsolatban.

[25] Az e-mail fejléce az elektronikus üzenet kézbesítéséhez elengedhetetlen információkat tartalmazza, melyet az RFC2822 szabvány fektetett le elsőként.
Forrás: https://datatracker.ietf.org/doc/html/rfc2822
[26] Forrás: https://mxtoolbox.com/EmailHeaders.aspx
Letöltés ideje: 2021. 10. 17.
[27] Forrás: https://toolbox.googleapps.com/apps/messageheader/
Letöltés ideje: 2021. 10. 21.

Az egyes fejlécmezők leírása az Internet Engineering Task Force RFC2822-es számú szabványában található meg.

**Domain-név**

A kibertérben elkövetett bűncselekmények felderítésének egyik legfontosabb eleme az elkövetőkhöz köthető hálózati azonosító, az IP-cím beszerzése. Az online adatgyűjtés célja leggyakrabban a célszemély azonosságának és hálózati kapcsolatának felderítése.

Az internetezésre használt eszközök egymás között az úgynevezett Internet-protokoll (vagy röviden: IP) felhasználásával kommunikálnak. Egy hálózati eszköz megcímzéséhez elengedhetetlenül szükséges egy IP-cím, amelyet az internet-szolgáltató bocsát a felhasználó rendelkezésére, és az eszközei ennek segítségével szólíthatók meg.

Ha az adott IP-címen valamilyen szolgáltatás – például weblap – üzemel, akkor a könnyebb megjegyezhetőség érdekében az üzemeltető egy domain-nevet is vásárol, amellyel az adott hálózati címen elérhető kiszolgáló ugyanúgy megcímezhető, mint a numerikus IP-címmel. A domain-neveket domain-szolgáltatók bocsátják a felhasználók rendelkezésére.

Az IP-címekkel és domainekkel kapcsolatos adatgyűjtést elsősorban az úgynevezett WHOIS-adatbázisokban kezdhetjük. Ezek az adatbázisok az IP-címek kiosztásáért felelős szervezetektől és a domain-regisztrátoroktól kapott információkból épülnek fel. Egy domain tekintetében ellenőrizhetjük, hogy az adott nevet melyik szolgáltatónál regisztrálták, mikor került sor erre, illetve meddig érvényes a regisztráció. A domain-tulajdonossal kapcsolatos további információk ezt követően a domain-regisztrátortól szerezhetők be.

Fontos, hogy az Európai Unió Általános Adatvédelmi Rendelete (a továbbiakban: GDPR) hatályba lépését követően a természetes személy domain-regisztrálók adatai nem jeleníthetők meg a publikusan elérhető WHOIS-adatbázisokban, azok kizárólag az adott regisztrátor megkeresésével szerezhetők be.

A domain-nevek kapcsán érdemes szót ejteni a host-nevekről is, amelyek különböző szolgáltatásokat címezhetnek meg egy adott hálózati infrastruktúrán belül. A host-név jellemzően a domain-névből és a szolgáltatás megnevezéséből (vagy annak azonosítójából) épül fel. Ennek megfelelően a levelezőszerver host-neve általában így néz ki: mail.domain.hu.

A kiberbűncselekmények elkövetői jellemzően figyelmen kívül hagyják azt a tényt, hogy a DNS[28]-információkból nem csupán az elsődleges hostra, hanem egyéb kiszolgálókra – például a már fentiekben is említett levelezőszerverre – vonatkozóan is érhető el információ. Elképzelhető, hogy a célszemély egy anonimitást biztosító úgynevezett reverse-proxy[29] felhasználásával kívánja elrejteni a szolgáltatást üzemeltető szerver valós IP-címét, azonban megfeledkezik az ugyanehhez a domainhez köthető levelezőszerver címének átirányításáról, így ennek adatai alapján a tényleges hálózati szolgáltató sok esetben megállapítható.

## IP-cím

Egy IP-cím tekintetében megtudhatjuk, hogy mely szolgáltatónak bocsátották azt rendelkezésére, ennek megkeresésével pedig további információkat szerezhetünk be az IP-címet az adott időpillanatban használó előfizetőre vonatkozólag.

A szolgáltatók más internet-szolgáltatóknak is tovább oszthatják a rendelkezésükre álló IP-címeket vagy címtartományokat. Célszerű tehát mindig az IP-címet még tartalmazó legkisebb címtérhez társított szolgáltató

[28] A DNS (Domain Name System) az internetes címzésekért felelős rendszer elnevezése, amely gyakorlatilag az egyes IP-címek domain-nevekkel való megcímzését teszi lehetővé.
[29] A reverse-proxy szolgáltatás a proxy szolgáltatás fordítottja: itt nem a felhasználó kapcsolódik egy közbenső kiszolgálón keresztül a világhálóra, hanem az adott szolgáltatás (például weboldal) érhető el egy közbenső kiszolgálón keresztül. Az egyik legnagyobb reverse-proxy szolgáltató a Cloudflare, amely céget jellemzően – tévesen – tárhelyszolgáltatóként azonosítják a felderítők, holott a társaság nem kínál ilyen jellegű szolgáltatást. Reverse-proxy szolgáltató esetében arra vonatkozólag kell megkeresni a szolgáltatót, hogy az adott IP-címen és domainen elérhető szolgáltatás átirányítását mely felhasználójuk részére biztosítják.

megkeresése, mellyel az előfizetőre vonatkozó információk beszerzése lerövidíthető. Ellenkező esetben a nagyobb címtér szolgáltatója csak arról fogja tájékoztatni a hatóságot, hogy az adott IP-címet tovább osztotta, így az előfizető kilétéről nem tud adatot szolgáltatni.

Az IPv4-címtér kimerülése miatt elképzelhető, hogy egy IP-címet a szolgáltató adott időpontban több előfizető részére is kioszt – ez az úgynevezett szolgáltató szintű címfordítás (angolul: NAT, Network Address Translation). Ebben az esetben a szolgáltató egy több előfizetőt tartalmazó listát bocsát a hatóság rendelkezésére, amely jellemzően a kapcsolódási időpontok kezdeti és befejező időbélyegzőjét is tartalmazza. Minél több IP-cím – kapcsolódási időpont pár áll a hatóság rendelkezésére, annál nagyobb az esélye, hogy a listák összefésülését követően az előfizetők száma kellően leszűkíthető. Az előfizetők közül a célszemély azonosítása sok esetben OSINT-módszerekkel is lehetséges.

**Telefonszám**

A telefonszámok tekintetében is léteznek az interneten elérhető robosztus adatbázisok, például online telefonkönyvek. A GDPR hatályba lépése óta azonban a személyes adatok internetes megjelenítése jelentős pénzbüntetést vonhat maga után, márpedig a rendelet értelmezésében a telefonszám is személyes adatnak minősül. A központi telefonszám-adatbázisok feltöltöttsége így a felhasználók hozzájárulásának függvénye.

Az okoseszközök alkalmazásával, különös tekintettel az okostelefonokra, azonban rendkívüli módon megnőtt az érdeklődés az azonnali üzenetküldő szolgáltatások iránt. Mindemellett pedig számos egyéb alkalmazás is lehetőséget teremt az ismerőseinkkel történő kapcsolatfelvételre (például egy játék keretében) a telefonon tárolt címjegyzékhez történő hozzáféréssel.

Az ilyen alkalmazások jellemzően közösségimédia-felületként is szolgálnak, így elengedhetetlen egy mögöttes felhasználói adatbázis felépítése. Ha egy ismeretlen hívószámot elmentünk az okostelefon memóriájába, úgy

az eszközre telepített szolgáltatásokban kereshetővé válik a számot használó felhasználó – amennyiben van ilyen. Ezzel a módszerrel hatékonyan kereshetők hívószám-tulajdonosok a különféle azonnali üzenetküldő szolgáltatásokban, így különösen a Messengeren, a Viberen, a Whatsappon, a Signalon vagy a Telegramon.

## Az adatgyűjtéssel kapcsolatos kihívások

A felderítési kihívásokat aszerint célszerű csoportosítani, hogy azok a felderítést végző szerv személyi állományához, technikai felszereltségéhez, a jogszabályi környezethez vagy a technológiai korlátokhoz kapcsolódnake.

### *A végrehajtó állomány*

A felderítés kezdeti szakaszában a legnagyobb kihívást az információhiány kiküszöbölése jelenti. Az adatgyűjtést végző személy a legtöbb esetben csak hiányos vagy töredékinformációkkal rendelkezik, aminek enyhítésére manuális keresések végrehajtására törekszik, amelyek gyorsan, nagy mennyiségű adatot szolgáltathatnak. A tervezés nélkül végrehajtott adatgyűjtés azonban könnyen félrevezetheti a végrehajtó állományt, hiszen a különböző forrásokból beszerzett információk látszólagos korrelációja mentén végzett adatgyűjtés eredménye nehezen validálható, az ez alapján végzett eljárási cselekmények pedig nem kellően megalapozottak, és gyéren dokumentáltak.

A felderítésre rendelkezésre álló idő az a faktor, amely a legtöbb esetben megnehezíti a beszerzett adatok validálását, azonban akár az orvostudományban, az adatgyűjtés végrehajtása tekintetében is alkalmazható a *„triage”*, mint eszköz, a legrelevánsabb információk gyors begyűjtésére. A gyorsaság azonban soha nem mehet a dokumentáció – közvetett módon a hitelesség –, a törvényesség, illetve a szakszerűség rovására. Ilyen esetekben – például élet- vagy kárveszély esetén – a lehetséges források közül csupán azokat kell figyelembe venni, amelyek a keresett adat beszerzését

leginkább valószínűsítik. A későbbi azonosítás, illetve kiegészítő adatgyűjtés elvégzése végett azonban az így végrehajtott tevékenységet is dokumentálni kell. Amennyiben nincs lehetőség írásos dokumentáció készítésére, úgy képernyőfelvétellel kell rögzíteni az elvégzett cselekményeket.

Az ember, mint validálást és értékelést végző személy, jellemzően nem hagyható ki az adatgyűjtésből, az automatizált eszközök azonban gyorsabbá és kényelmesebbé teszik nagy mennyiségű adat begyűjtését. Fontos azonban tekintettel lenni arra, hogy egyetlen jól megalkotott automatizmus sem képes az adatgyűjtést és annak célját jól ismerő személlyel azonos értékítélet megalkotására, ezért a különböző OSINT célszoftverek alkalmazása mellett nem mellőzhető az ember által végzett hitelesítési folyamat.

A kapacitásbővítés és a folyamatos képzés az adatgyűjtés elengedhetetlenül szükséges eleme. A technológia fejlődésével – és sok esetben változásával – újabb és újabb ismeretek megszerzése szükséges ahhoz, hogy a rendelkezésre álló információforrások kiaknázhatók maradjanak, vagy azzá váljanak. Az állomány részére lehetőséget kell biztosítani az ismeretek elsajátítására, valamint célszerű kialakítani egy olyan szakmai segítséget nyújtó hálózatot, mely közvetlenül támogatja a felderítő állományt.

***Az adatgyűjtést végző szerv technikai felszereltsége***

Az adatgyűjtések hatékonysága az állomány felkészültségének és eszközállományának függvénye, melyek közvetlen kapcsolatban vannak egymással. Kisebb szaktudással rendelkező állomány is végezhet hatékony adatgyűjtést megfelelő szoftverek alkalmazásával, ezek beszerzési és üzemeltetési költsége azonban jellemzően meghaladja egy átlagos rendvédelmi szerv költségkeretét. Az erre adott reakció általában a végrehajtó állomány számának növelése, melyhez azonban sok esetben nem társul a korábbiakban említett képzési program kidolgozása.

Az OSINT alapelveinek figyelembevételével végzett adatgyűjtés és a megfelelő anonimitás biztosítása csak speciális eszközök alkalmazásával lehetséges, arra a rendvédelmi szervek által hivatali munkára használt eszközök nem alkalmasak.

A technikai feltételek megteremtése az adatgyűjtést végző egység munkájának megalapozása, mely nélkül nem várható el a célzott eredmény biztosítása. A minimálisan szükséges eszközpark a rendvédelmi szervhez nem köthető – virtuális gép futtatásához elegendő számítási teljesítménnyel, térhellyel és memóriával rendelkező – számítógépből, internetkapcsolatból, valamint a feldolgozást segítő irodai és elemző-értékelő szoftverekből, grafikus alkalmazásokból, a hálózati kapcsolat elfedését biztosító VPN-kliensből és az ezekhez tartozó perifériákból áll.

A felszereltségi szint emelésével az adatgyűjtés hatékonysága is növelhető. A kriptovaluta-tranzakciók hatékony nyomon követése elképzelhetetlen blokklánc-elemző szoftverek nélkül, jelenleg azonban legjobb tudomásom szerint egyetlen ilyen eszköz sem áll a rendőrség rendelkezésére.

### *Technológiai korlátok*

Az adatgyűjtés esetében sokszor az alkalmazott technológia korlátai jelentik a kihívást. Az internet sötét oldalaként jellemzett deep, illetve dark weben végzett adatgyűjtés, valamint az innen származó információkkal kapcsolatban végzett felszíni internetes keresés csupán egy a sok közül.

A deep web az internet azon részét képezi, melyet nem indexáltak a keresőrobotok, valamint azok a tartalmak, szolgáltatások is ide tartoznak, amelyek csak valamilyen korlátozással – például felhasználónév és jelszó, vállalati vagy intranetes hálózat alkalmazásával – érhetők el. Egyes becslések szerint a deep web jelenleg az internetes tartalmak több mint 90%-át teszi ki.[30]

A dark web ezzel szemben egy újabb, kisebb szeletét képezi az internetnek – gyakorlatilag egy hálózat a hálózatban, melynek szolgáltatásai csak a hálózatra jellemző speciális célszoftver segítségével érhetők el.

A deep web tekintetében az adott információ hozzáférhetősége korlátozott, míg a dark web esetében a hálózat anonimitásának kiküszöbölése okozhat nehézséget.

---

[30] Forrás: https://www.csoonline.com/article/3249765/what-is-the-dark-web-how-to-access-it-and-what-youll-find.html
Letöltés ideje: 2021. 10. 17.

Az avatar-menedzsment, azaz a felderítő által használt online identitások naprakészen tartása, illetve létrehozása is kihívást jelent, hiszen a legtöbb szolgáltató jellemzően aktívan monitorozza platformját a hamis, vagy nem használt profilok kiszűrése érdekében. Az adatgyűjtést végzőnek tehát nem csupán aktív és eltérő identitásokkal rendelkező online avatárokat kell létrehoznia, hanem azokat karban is kell tartania, ez a feladat pedig egy széles spektrumban tevékenykedő felderítő szerv esetében nem elhanyagolható kapacitást köt le.

A kriptovaluták és általában a decentralizált fizetési rendszerek megjelenésével ugyancsak technikai kihívást jelent az ezeken végrehajtott tranzakciók követése és a tranzakcióban részt vevő felek azonosítása. Mivel nincs olyan központi szerv, akit meg lehetne keresni a blokklánc-tranzakciók vonatkozásában, a hatóságok saját – és különböző gazdasági társaságok által kínált szoftverek – elemzési kapacitásuk korlátai között képesek csak a fizetési műveletek követésére, illetve azonosítására. Ugyancsak a tranzakció-analízishez köthető, de nem technikai jellegű kihívás a szolgáltatók válaszadási, illetve együttműködési hajlandósága. A blokklánc-technológián alapuló fizetési szolgáltatások „gyenge pontja" az a tranzakció, amely egy a hatóságokkal együttműködő szolgáltató irányában megy végbe. Ebben az esetben az adott társaság megkereshető, és ha rendelkezik az érintett címhez vagy tranzakció-azonosítóhoz köthető ügyféladatokkal, azt a hatóság rendelkezésére bocsáthatja.

***Jogszabályi korlátok***

A szabályozási környezet közvetlen hatással van a felderítést végző szerv munkájára. A monitorozó jellegű adatgyűjtés automatizált eszközök alkalmazásával például könnyen eredményezheti nagy számú irreleváns személyes adat letárolását, melynek megfelelő kezeléséről az adatgyűjtést végző szervezetnek kell gondoskodnia.

Léteznek olyan aktív adatgyűjtő módszerek, amelyek nagy számú kérést küldenek a kiszolgáló szerver irányába, és az ezekre adott válaszokból szolgáltatnak releváns információt például az adott kiszolgáló technikai jellem-

zőiről. Ilyen adatok begyűjtése nyílt forrásból ingyenesen elérhető eszközök segítségével is egyszerűen lehetséges, alkalmazásuk azonban könnyen eredményezheti az érintett információs rendszer működésének akadályozását, mely a legtöbb állam jogrendje szerint bűncselekmény.

Természetesen nem csak a szerver túlterhelésével ütközhetünk jogszabályi korlátokba, hiszen egyes esetekben bizonyos információkhoz való egyszerű hozzáférés – például egy keresőmotor által beindexált intranetes tartalomszolgáltatás felkeresése, majd ott történő kutatás – is bűncselekmény elkövetését eredményezheti.

## A nyílt forrásból beszerzett adatok felhasználása a felderítésben

Az adatgyűjtés tervezésekor meghatározott szempontok szerint a konspirációs és információs igény közötti egyensúly fenntartásával a kiberfelderítés célja a jogszabályi keretek között a lehető legtöbb információ beszerzése a dekonspiráció lehetőségének legkisebb foka mellett.

A nyílt forrásból beszerzett információk önmagukban is szolgálhatnak bizonyító erővel, ugyanakkor könnyen elképzelhető, hogy akár az adatgyűjtés folyamán, akár annak befejezését követően szolgáltatói megkeresések kiküldése vagy nemzetközi jogsegély teljesítése válik szükségessé.

Ahhoz, hogy az internetről beszerzett információk bizonyítékként felhasználhatók legyenek, gondoskodni kell az adatgyűjtés megfelelő dokumentálásáról, valamint az adatgyűjtésről szóló jelentés előállításáról is. A jelentésből kiolvasható kell, hogy legyen az adatgyűjtés célja, a beszerzett információk és azok forrása. Az alkalmazott eszközöket csak abban az esetben szükséges szerepeltetni, ha az a bizonyíték előállításának folyamatában elengedhetetlen szerepet töltött be, és ez az információ mással nem pótolható. Ebben az esetben figyelemmel kell lenni arra, hogy az alkalmazott módszert lehetőleg ne dekonspiráljuk.

Akár az automatikus eszközök által szolgáltatott, akár pedig a manuálisan végrehajtott adatgyűjtés során beszerzett információk tekintetében is tisztában kell, hogy legyen az adatokat beszerző személy az adatgyűjtés

mechanizmusával is. Önmagában az a tény, hogy egy szoftver használatával egy, a célszemélyre vonatkozó információt sikerült beszerezni, önmagában nem rendelkezik bizonyító erővel, csak ha pontosan leírható az a mechanizmus, amellyel a szoftver az érintett adatot szolgáltatta. Ettől az eljárási rendtől eltérően beszerzett információk csupán operatív értesülésként használhatók fel a különböző verziók felállításakor.

A beszerzett információk szervezeten kívüli felhasználása esetén különös óvatossággal kell eljárni, hiszen amennyiben az eljárás alapján feltehető, hogy a megkeresendő szolgáltató is érintett lehet a bűncselekmény elkövetésében, vagy a célszemély hozzáférhet ezen szolgáltató adataihoz, úgy az adatgyűjtés egésze dekonspirálódhat a szolgáltató megkeresésével. Ugyanez igaz azokra az iratokra is, amelyek az eljárás anyagát képezik, azonban azokból közvetlen vagy közvetett módon a felhasznált eszközökre vagy módszerekre utaló következtetések vonhatók le.

A nyílt forrásból beszerzett adatok megerősítéseként, vagy azoknak konkrét személyhez köthetőségének megállapítása végett a rendvédelmi szervek jellemzően további megkeresésekkel élnek az egyes szolgáltatók irányába. Az internetes tartalomszolgáltatók megszokott üzleti gyakorlata az, hogy a rendvédelmi megkereséssel érintett felhasználót értesítik a megkeresés tényéről, így ennek mellőzését kifejezetten kérni kell a címzett szolgáltatótól a neki címzett adatkérésben.

Az aktív adatgyűjtő eszköz alkalmazásának tervezésekor számolni kell azzal, hogy az így beszerzett adat nem tehető a nyomozati iratok részévé, csak operatív információként használható fel. Ha az adatgyűjtéshez használt eszközt az OSINT-dokumentációban a felderítő szerv megjeleníti, úgy a nyomozati iratok megismerésekor egyértelművé válhat a célszemély számára is az információ forrása, ami annak jövőbeli alkalmazását lehetetlenítheti el.

A felderítő szervnek kell megállapítania a konspirációs, illetve információs érdek közötti viszonyt, azonban e szerveknek minden esetben arra tekintettel kell eljárniuk, hogy egy eszköz dekonspirálásával nem csak a saját eljárásukban, hanem nemzeti vagy akár nemzetközi szinten is ellehetetleníthetik annak későbbi alkalmazását. Ilyen esetekben az aktív felderítési

módszerekkel beszerzett információ mentén tovább folytatva az adatgyűjtést, azt kell megállapítani, hogy mely forrásból lehetett volna még az adott információt beszerezni, ha az eszköz nem állt volna a felderítő szerv rendelkezésére.

A felderítő szerv a nyílt forrásból származó információkat az adatgyűjtés végeztével általában szintetizálni kívánja az egyéb módon beszerzett információkkal. Álláspontom szerint a nyílt forrásból beszerzett adatokat – azaz a nyílt forrású adatgyűjtésről készült jelentést – külön dokumentumban kell megjeleníteni, a más adatokkal való esetleges összevetésről pedig külön feljegyzést kell készíteni. Az adatgyűjtés dokumentációját nem célszerű az iratanyag részévé tenni, azonban a maradványiratok között az esetleges későbbi reprodukció lehetősége miatt elhelyezhető.

## Konklúzió

A nyílt forrású adatgyűjtés a rendvédelmi szervek számára újfajta felderítési eszközként szolgál, amelynek megfelelő kiaknázása és a klasszikus felderítési eszközökkel párhuzamosan történő alkalmazása rendkívül hasznos, mással nem pótolható információforrásként szolgálhat az alapeljárásban vagy a tájékozódó célú adatgyűjtés során.

Az online szolgáltatások népszerűségének növekedésével, valamint a platformok azon gyakorlatával, hogy még több adat és tartalom megosztására ösztönzik a felhasználókat, egyre több információ érhető el a kibertérben, sőt bizonyos információk kizárólag innen szerezhetők be.

Az információs társadalom korában a rendvédelmi szervek nem engedhetik meg maguknak, hogy felderítéseiket ne egészítsék ki a kibertérből származó nyílt információkkal, melyek beszerzése és feldolgozása ciklikus folyamatként írható le, így hatékonyan, egyszerűen és könnyen elsajátítható módon alkalmazhatók bármely eljárásban.

A nyílt forrásból beszerzett adatok nem csupán operatív értesülésként, hanem akár bizonyítékként is felhasználhatók, amennyiben azok begyűjtése törvényes, szakszerű és mindenekelőtt megfelelően dokumentált mó-

don történt. Az adatgyűjtés tervezett végrehajtása megalapozhatja egy kezdeti hipotézis felállítását, segítségül szolgálhat a rendvédelmi szervek közbiztonsági célú monitorozó tevékenysége során, az eljárásokban verziókat igazolhat vagy éppen cáfolhat meg, a beszerzett adatok pedig a hatóságok számára hozzáférhető adatokkal kiegészítve pontos és időszerű profilok felállítását teszik lehetővé.

Bár a folyamat egyszerű, az információk gyűjtéséhez pedig nincs szükség különleges szakértelemre, mégis hangsúlyos szerepet kell, hogy kapjon a rendvédelmi szervek állományának oktatása. Ennek során az adatgyűjtéseket végző állomány megismerkedhet a nyílt információgyűjtés elméleti alapjaival, a felmerülő adatforrások kiaknázásnak lehetőségével, valamint olyan metodikai és technikai eljárásokat sajátíthat el, amelyekkel hatékony és szakszerű módon végezheti tevékenységét.

Az adatok forrásai, valamint az alkalmazható módszerek – így az adatgyűjtés metodikája – is folyamatosan változik. Amely adatforrás ma kiaknázatlan, elképzelhető, hogy a közeljövőben a legrelevánsabb információkat fogja szolgáltatni. Ez azonban fordítva is igaz: elképzelhető, hogy a ma aktívan és hatékonyan használt eszközök a jövőben már nem lesznek elérhetők, ezért folyamatosan figyelemmel kell kísérni az online térben zajló folyamatokat.

A nyílt forrású adatgyűjtés lényege tehát nem csupán az adatok beszerzése, hanem a források ismerete, felderítése, valamint az OSINT-ciklust követve az elemző-értékelő folyamat végrehajtását követően a reprezentáns irat megfelelő szakmai színvonalon történő elkészítése, mely biztosítja a rendvédelmi szervek eljárásaiban történő – akár bizonyítékként való – felhasználás lehetőségét is.

Végül kiemelendő, hogy az OSINT nem csupán a kiberbűncselekmények felderítésében alkalmazott eszköz, hanem bármilyen olyan esetben sikerrel alkalmazható, amely online vetülettel rendelkezik. E kategória pedig 2022-ben gyakorlatilag minden jelenséget magába foglal.