NEMZETBIZTONSÁGI SZEMLE
7. évfolyam (2019) 2. szám 19–31. • DOI: 10.32561/nsz.2019.2.2

Csizner Zoltán[1]

Az OSINT határai

The Limits of OSINT

A nyílt forrású információgyűjtés korábban is hasznos segítséget jelentett, de ezt az informatikai forradalom, a világháló és a közösségi média térnyerése tovább fokozta. Ugyanakkor a lehetőség sok veszélyt és korlátot is hordoz magában, ami az alkalmazókban talán nem mindig tudatosul. Az alábbi pár gondolat figyelemfelhívás ezekre a veszélyekre és korlátokra, amelyek szem előtt tartása talán biztonságosabbá teheti a hírszerzés ezen szegmensét.

Kulcsszavak: OSINT, veszélyek és korlátok, felejtés joga, digitális lábnyom, jogszerűség

The open source intelligence gathering has been a useful tool earlier, but the information revolution, the world wide web and the social media made it more essential. Meanwhile this opportunity includes many dangers and limits which the users may not be aware of. These few thoughts below could contribute to the raising of the awareness of those dangers and limits; keeping them in mind should make this segment of the intelligence safer.

Keywords: OSINT, dangers and limits, the right to forget, digital footprint, legality

A nyílt forrású hírszerzés

Történelmi példák mutatják, hogy a köznapi ember számára is észlelhető, megismerhető adatok tudatos értelmezése és elemzése a politikai döntésekben – a múltban jellemzően a háborúkban – is hasznosíthatóvá válhatnak. A második világháborúban például német tudósok a londoni Big Ben harangjátékának élő közvetítéséből vontak le következtéseket az aktuális időjárási viszonyokról, amelyeket a Luftwaffe parancsnokai az angol főváros bombázásának tervezéséhez használtak fel.[2] Az persze már

[1] Csizner Zoltán r. ezredes, doktorandusz, a Terrorelhárítási Információs és Bűnügyi Elemző Központ főosztályvezetője. ORCID-azonosító: 0000-0002-1867-8560.

[2] Harari 2015, 354.

a módszer egyes korlátait (például megbízhatóság, ellenőrzésre szorultság) igazolja, hogy miután a brit hírszerzés erre rájött, felvételről kezdték sugározni a harangszót, és ezzel már dezinformálni tudták az ellenséget.

A nyílt forrású hírszerzés, az OSINT[3] fogalmi értelmezése szerint felölel minden elérhető nyílt forrást, így a médiaforrásokat (például újságok, magazinok, rádió- és televízióadások, számítástechnikai eszközökön megszerezhető adatok), közadatokat (például kormányzati jelentések, politikai nyilatkozatok, meghallgatások, törvénykezési viták), szakértői és kutatási adatokat (konferenciák, szakértői társaságok, tudományos folyóiratok).[4] Azonban a mai világban mégis az internet, pontosabban az azon futó világháló (www: World Wide Web) jelenti a legnagyobb forrást, és egyre ritkább a *Keselyű három napjá*ban[5] látott elemzési munkamódszer.

Ugyan pontos és mindenki által elfogadott meghatározása nincs az OSINT-nak, de az alábbi két idézet talán rávilágít a lényegre.

Az első Lévay Gábortól származik:[6] „Az OSINT a katonai felderítés és a hírszerzés rendszerén kívül létező, a publikum (tehát minden egyén) számára nyilvánosan, legális eszközökkel megszerezhető, vagy korlátozott körben terjesztett, de nem minősített adatok szakmai szempontok alapján történő felkutatását, gyűjtését, szelektálását, elemzését-értékelését és felhasználását jelenti…"

A másodikat az NSA[7] és a CIA[8] egykori igazgatójának, Michael Hayden nyugalmazott tábornoknak tulajdonítják: „A források nyilvánosak. Az érdeklődési körünk nem az. A szakmánkban nem mindig a titkos információk a legértékesebbek. Valójában, sokkal élvezetesebb megoldani egy problémát vagy megválaszolni egy nehéz kérdést olyan információk alapján, amit valaki meggondolatlanul nyilvánosan is hozzáférhetővé tett."

Az már csak a hírszerző társadalom leleményessége, hogy a nyílt forrású hírszerzést is tovább bontotta, és a hétköznapi tapasztalatok alapján megalkottak új – igaz, kevésbé tudományos – területeket is.

Így alakult ki többek között a PIZZINT, a pizzahírszerzés, amelynek alapját az USA-ban tevékenykedő szovjet hírszerzők megfigyelési eredményei jelentették. Ezek szerint ha a megszokottnál több pizzaszállító jelent meg a Fehér Ház, a Külügyminisztérium, a Védelmi Minisztérium vagy a CIA épületénél, akkor az valamilyen válsághelyzetet jelentett, ami miatt többen maradtak bent.

A legendák szerint hasonló ismeretek alapján jött létre a LAVINT (a mosdóhírszerzés), a RUMINT (a folyosói hírszerzés), valamint a DIVINT (az isteni hírszerzés).[9]

A 21. század technikai robbanása magában hordozta a keletkezett információ mennyiségének ugrásszerű fejlődését is. Soha nem látott mértékű személyes adat, ismeret, titok érhető el a hozzáértő számára a világhálón pár kattintással, rövid idő alatt. Egy amerikai tanulmány[10] szerint már 2012-ben is naponta 2,5 milliárd gigabyte (GB)

---

3 Open Sourche Intelligance – nyílt forrású hírszerzés.
4 Lowenthal 2017, 178.
5 James Grady (1949–) regényéből készült amerikai film, amelynek főhőse a CIA alkalmazásában naphosszat regényeket, cikkeket olvas és dolgoz fel az azokban található ötletek, információk felhasználhatósága érdekében.
6 Lévay 2006, 6.
7 National Security Agency – Nemzetbiztonsági Ügynökség (USA).
8 Central Intelligence Agency – Központi Hírszerzési Ügynökség (USA).
9 Lowenthal 2017, 179.
10 Monnappa 2019.

adat keletkezett. Az információ keletkezése soha nem látott módon gyorsul; 2020-ra az előrejelzések szerint minden másodpercben, személyenként 1,7 megabyte adatmennyiséget állítunk majd elő a Földön.

Ezzel párhuzamosan a tárolókapacitások növekedése, egyre olcsóbb elérhetőségük, az elemzési rendszerek és módszerek fejlődése megteremtette az igényt is az úgynevezett készletező adatgyűjtésre, azaz hogy konkrét cél nélkül, egy esetleges későbbi felhasználásra szerezzék be és tárolják az információkat. Ezt a fajta hírszerzési módszert tárta a világ elé 2013-ban Edward Snowden.[11] Ennek következtében a jelentősebb tartalomszolgáltatók az ügyfelek bizalmának visszanyeréséhez igyekeztek elzárkózni a hatóságokkal való együttműködéstől és minél több adatvédelmi garanciát beépíteni a működési rendjükbe.

A neten folyamatosan gyarapodó információhalmaz azonban továbbra is létezik, ami ezáltal felértékelődött, és nagy része könnyedén elérhető maradt. Mint minden területen, a keresés és kutatás emberi képességeinek korlátait itt is kitágítják speciális programok, applikációk és keresőmotorok, amelyek képesek könyvtárnyi dokumentumot a megadott keresési szempontok szerint a másodperc törtrésze alatt szelektálni, átvizsgálni.

Régi dilemma, hogy vajon az internethasználók tisztában vannak-e azzal, mennyire válnak sebezhetővé egy-egy bejegyzéssel, posztolással, vagy hogy mennyi információ válik ezáltal mások számára is hozzáférhetővé. A biztonságos-tudatos internetezésre szerencsére már fiatalkorban megkezdődik az oktatás, és egyre inkább válnak közismertté ezek a kockázatok. Azonban vajon az interneten kutakodók – akár laikusokról, akár hivatásszerű alkalmazókról beszélünk – ismerik-e a korlátokat és veszélyeket, tisztában vannak-e a jogi keretekkel? Hol a határ az interneten szabadon fellelhető adatok összegyűjtése és a hírszerzés vagy a jogi terminológia szerinti titkos információgyűjtés között? Milyen digitális lábnyomok árulkodnak az érdeklődésünk középpontjáról, vagy akár a magáról a kutakodást végző személyről? Valóban annyira mély a *deep web,* és annyira sötét a *darknet?* Az alábbiakban ezeket a kérdéseket próbálom megvilágítani.

A jogi korlát

A nyílt forrású információgyűjtés, hírszerzés fogalma mellett a jogi szabályozása sem egyértelmű és nem egységes. Az egyik elfogadott nézet szerint, ami az interneten fellelhető, annak a felhasználása nem ütközik semmilyen korlátba. Ez valószínűleg igaz, ha az információ megszerzéséhez nincs szükség valamilyen rendszerbe történő, engedélyhez kötött belépésre vagy esetleg jelszó alkalmazására, azaz az internet felszínen látható részéről, a *surface webről* beszélünk. De mi a helyzet, amikor valamely információ, adat megismerése feltételekhez kötött?

Az OSINT-tevékenységgel összefüggésben meg kell különböztetni a minden feltétel nélkül, bárki által megismerhető adatok megszerzését – ezt szokás passzív eljárásnak nevezni –, míg a csoportosítás másik fele az úgynevezett aktív információgyűjtés

[11] Edward Snowden (1983–) az NSA és a CIA volt alkalmazottja, a tömeges megfigyeléseket 2013-ban leleplező cikkek forrása; utóbbi időben az informatikai biztonság kérdéskörében nyilatkozik meg.

és hírszerzés, amely már valamilyen kiegészítő mozzanatot, tevékenységet igényel. Ez utóbbi esetben már nemcsak szemlélője, megfigyelője a hírszerző az eseményeknek, hanem valamilyen szinten beavatkozik a folyamatokba, ráhatással bír azokra. Ez a beavatkozás sok esetben külön engedélyhez vagy jogosultsághoz kötött, amelynek hiányában általában jogellenes az adat megszerzése. Az engedély és jogosultság származhat az adat birtokosától vagy az adatot kezelő szervezettől, informatikai rendszer üzemeltetőjétől, de szigorú feltételek mellett felhatalmazást adhat rá törvény is, mint például a titkos információgyűjtés vagy a leplezett eszközök alkalmazásának esetében.

A hazai büntető törvénykönyv[12] (Btk.) a XLIII. fejezetében külön tárgyalja az informatikai rendszerek védelmét, illetve szankcionálja ezek megsértését. A 423. § szerint két évig terjedő szabadságvesztéssel büntetendő az, aki információs rendszerbe az annak védelmét biztosító technikai intézkedés megsértésével vagy kijátszásával jogosulatlanul belép, vagy a belépési jogosultsága kereteit túllépve vagy azt megsértve bent marad. Ugyancsak szabadságvesztéssel büntetendő többek között az is, aki ehhez jelszót, programot készít, forgalmaz, hozzáférhetővé tesz.

A 422. §-ban a személyes adat, magántitok, gazdasági titok vagy üzleti titok jogosulatlan megismerésének egyes elkövetési magatartásait szintén szabadságvesztéssel rendeli büntetni a Btk., így például az elektronikus hírközlő hálózat – ideértve az információs rendszert is – útján másnak továbbított vagy azon tárolt adatok kifürkészését, és az észleltek technikai eszközzel történő rögzítését is.

A Btk. értelmezi is az információs rendszer fogalmát: a 459. § (1) bekezdésének 15. pontja szerint az az adatok automatikus feldolgozását, kezelését, tárolását, továbbítását biztosító berendezés, vagy az egymással kapcsolatban lévő ilyen berendezések összessége.

Azonban a jogi korlátok a passzív kutatás esetében is fennállhatnak, ha az elérhető tartalom megtekintése, megszerzése (letöltése) vagy birtoklása már önmagában is bűncselekmény. Ilyen például a Btk. 204. §-ban nevesített gyermekpornográfia körébe tartozó adat (például fénykép, videó), de egyes államokban a terrorizmushoz köthető információk, tartalmak is ebbe a kategóriába tartoznak. Legutóbb az Egyesült Királyság döntött úgy, hogy a 2019. évi Terrorizmus Elleni és Határvédelmi Törvény[13] szerint a terrorista propagandatartalmak megtekintése akár 15 évig terjedő szabadságvesztéssel lesz büntethető.

Amennyiben ezen tartalmak megtekintésére, indokolt letöltésére a nyomozó hatóság részéről az eljárási szabályok betartása mellett büntetőeljárásban kerül sor, nem merülhet fel a felelősségre vonás kérdése. De ha ezt konspiráltan, leplezetten kell végrehajtani, már nem ennyire egyértelmű a helyzet. Ekkor már felmerülhet fedett nyomozó igénybevételének és előzetes ügyészi engedély szükségességének a kérdése.

További érdekes kérdést feszegetett Gál István László egyetemi docens 2014-ben *Az OSINT (Open Source Intelligence), mint a kémkedés lehetséges elkövetési magatartása*[14] című szakmai cikkében. A levezetett gondolatmenete szerint a kémkedés elméleti

12 2012. évi C. törvény.

13 Counter-Terrorism and Border Security Act 2019. Elérhető: www.independent.co.uk/news/uk/home-news/terrorist-propaganda-law-thought-crime-click-link-online-prison-a8866061.html (A letöltés dátuma: 2019. 04. 29.)

14 Gál 2014.

lehetősége ugyan felmerülhet a nyílt forrásból megszerezhető adatok összegyűjtése és elemzése során, de annak társadalomra veszélyessége, illetve a bizonyíthatósága eléggé kérdéses marad. Gyakorlatban is reálisnak tűnő büntetőjogi felelősségre vonást a szerző csak olyan lebukott és tényleges kémtevékenységet folytató hírszerző esetén lát, akinél a minősített adatok átadása helyett csak azt lehetne bizonyítani, hogy rendszeres kapcsolattartás mellett egy idegen szervezet részére folyamatosan adott át nyílt forrásból származó, de általa megszűrt, elemzett információkat.

A megismert adatok további felhasználása is felvethet jogi kérdéseket. A közösségi médiából kinyert fényképekkel, adatokkal érintett egyén személyiségi jogai vagy a szerzői jogok védelme sem hagyható figyelmen kívül. Ez még akkor is igaz, ha a közösségi oldalon posztoló saját döntése alapján osztja meg adatait, képeit.

Akár aktív, akár passzív információszerzés végrehajtására kerül sor, a számítógépet használónak pontosan kell ismernie azokat a határokat, amelyek átlépése büntetőjogi felelősségre vonást eredményezhet. És ezeket a határokat meg kell tartani még akkor is, ha informatikai ismereteiben bízva biztos abban, hogy őt lehetetlen azonosítani.

A megbízhatósági korlát, az ellenőrzés igénye

A nyílt forrású információgyűjtés egyik legnagyobb hátránya, hogy nem tekinthető megbízható, ellenőrzött forrásnak. Ennek okai többrétűek. Egyrészt az adatokat elhelyezőket nem kötelezi semmiféle szabály a hitelességre. Elég csak arra gondolni, hogy a közösségi oldalak profiljain mennyi negatív tulajdonság található. Valóban ennyire makulátlanok a felhasználók, vagy – finoman fogalmazva – csak szűrten tájékoztatják egyéniségükről a többieket? A fiktív identitások, a valótlan életutak és állítások nem meglepők a világhálón. Ugyancsak nem biztos, hogy egy-egy fénykép tényleg ott készült, ahol állítják, és még hosszan folytatható a bizonytalanságok sora. A digitális és a virtuális identitások gyorsan cserélhetők és szinte ellenőrizhetetlenek.

A digitális személyazonosság – amit egy-egy közösségi oldalon vagy más fórumoknál alkalmazunk – egy tudatosan felépített információhalmaz (adatok, fényképek, vélemények), amely alapján az online világban egy képet tudnak rólunk alkotni. A valóságos, fizikai profilunkkal szemben azonban ennek megváltoztatása vagy törlése csak pillanatok műve. Igaz, a profillal végzett tevékenységek nagy része a törléstől függetlenül hagy maga után nyomokat, amelyek a hozzáértők számára észlelhetők lesznek később is.

A virtuális identitás, az *avatár* már egy játékfelületre célzatosan létrehozott személyiség, amelyben már a valóság látszatát sem kell kelteni.

Mindkét esetben megnyílik annak a lehetősége, hogy egy képzelt, fiktív személyiség mögé rejtőzve tegyünk meg olyan dolgokat, amiket a valóságos világban nem tudunk vagy nem merünk.

A bizonytalanság másik fő tényezője az időbeliség. A fellelhető adatok valóságtartalma mellett fontos bizonytalansági tényező a valós információk aktualitása is. Sokan kevésbé rossznak gondolják, ha valami olyat állítanak, ami valamikor igaz volt, függetlenül attól, hogy már nem az. Ilyen például a jól fizető munkahelyek megjelölése, a divatos hobbik (például golfozás, repülés, vadászat, vitorlázás) vagy akár a drága környéken bérelt korábbi lakás megjelölése.

Ezek mellett – mivel az internet nem selejtez – nagyon fontos az információ értékelése során a letöltés, hozzáférés dátumát, illetve a keletkezés és feltöltés időpontját is figyelni, ellenőrizni, ami sok téves megállapítástól és felesleges munkától óvhat meg.

A tudatos félrevezetés mellett a felületes vagy el nem végzett ellenőrzés is eredményezhet súlyos hibákat. Erre volt jellemző példa a 2015-ös bostoni terrorcselekménnyel kapcsolatos sajtóhiba. 2015. április 15-én a Bostonban megrendezett maratoni futás befutójánál két, szemeteskukákba rejtett pokolgéppel megöltek 3 embert, és közel 150 személyt megsebesítettek a később azonosított, csecsen származású Carnajev testvérek. Az egyik legnagyobb tévétársaság, a CNN már nem sokkal a merényletet követően a Twitterből kinyert adatok felületes feldolgozása után hírül adta, hogy az elkövető színes bőrű, és a letartóztatásáról is beszámolt. Később ez valótlannak bizonyult, és a csatorna magyarázkodásra kényszerült.[15] Ez a baklövés mind a tévétársaság elismertségét és hitelességét, mind pedig a nyílt forrású hírszerzés megbecsülését visszavetette.

A fenti bizonytalanságok ellenére a megszerezhető információk nagyban tudnak segíteni; lehetőséget adnak az ellenőrzésre, azok megerősítésére vagy cáfolatára, irányt mutatva ezzel az elemzőnek és hírszerzőnek. Az egyik legnagyobb hiba, ha a nyílt forrású kutatás során beszerzett adatokat mindenféle értékelés, ellenőrzés nélkül tényként fogadjuk el.

Az időbeli korlát, a felejtés jogának kérdése

Az informatikai fejlődés egyik melléktermékeként az az adathalmaz, amely évről évre gyűlik a szerverek memóriájában. Egy kitöltött adatlap, egy munkahelyi önéletrajz, egy kiposztolt esemény évek után is elérhető. Már a volt barátnővel készült és a közösségi oldalra kiposztolt nyaralási fotó is kellemetlen perceket okozhat egy új kapcsolatban, nem beszélve a korábbi munkahelynek megadott bizalmas adatokról. Az aktuális hírekben szereplő személyek és események az idő múlásával már érdektelenné válhatnak, a róluk szóló híradások azonban továbbra is elérhetők maradnak. Az évekkel ezelőtti állapotok elérhetősége sokak szerint alapvető jogokat sért, de az információs rendszerek halmazában szinte lehetetlen selejtezni.

Az áttörést az Európai Unióban Mario Costeja González spanyol állampolgár 2010-ben benyújtott panasza jelentette. Ebben azt sérelmezte, hogy a Google keresőmotorja a nevére indított lekérdezés eredményeként a *La Vanguardia* nevű, nagy példányszámú spanyol újság többéves közleményét is feladta találatként, amelyben az akkori társadalombiztosítási tartozás miatt elárverezett házával kapcsolatban nevesítették őt. A több fórumot megjárt bírósági perben végül az Európai Bíróság kimondta,[16] hogy a magánszemélyek jogosultak név alapján a Google-hoz hasonló keresőmotoroktól a lekérdezésekre kapott találatok eltávolítását kérni.

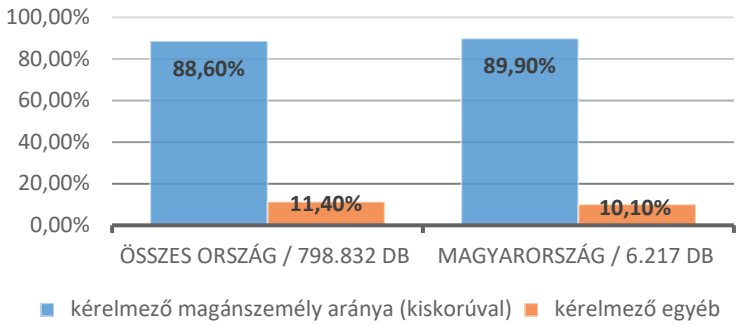
[15] Brogen 2015.

[16] Európai Bíróság C-131/12. számú ítélete. Elérhető: http://curia.europa.eu/juris/liste.jsf?num=C-131/12&language=HU (A letöltés dátuma: 2019. 04. 29.)

A keresőmotornak eleget kell tennie ennek akkor, ha a kérdéses linkek „nem megfelelők, nem vagy már nem relevánsak, illetve túlzók". Az eltávolításhoz a keresőmotor üzemeltetője jogosult figyelembe venni a kérelmező személy esetleges közéleti szerepét is.

A Google már az ítélet hatálybalépése előtt megkezdte a kérelmek befogadását, amelyek teljesítését és elutasítását folyamatosan közzéteszi.[17] Ezekből megállapíthatók a beérkezett kérelmek statisztikai adatai (összesítve, illetve országokra bontva), így többek között az összes kérelem száma, a kérelmezők jellege (magánszemély, egyéb személy), az eltávolításra kérelmezett URL-ek[18] száma, illetve a kérelmek elintézési módja (teljesítve vagy elutasítva).

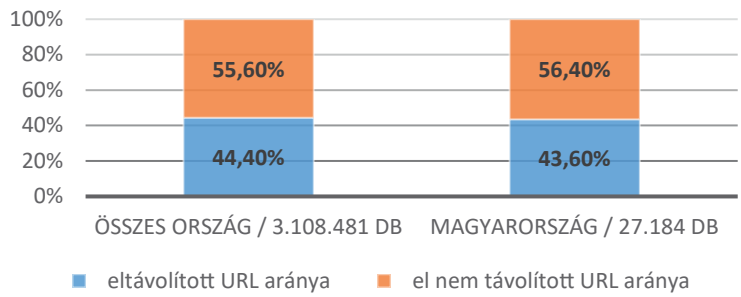
A 2014. május 28. és 2019. április 29. közötti időszak adatait az alábbi diagramok ábrázolják:



1. ábra

A beérkezett kérelmek eloszlása

Forrás: transparencyreport.google.com



2. ábra

Az eltávolításra kérelmezett URL-ek elintézési módja

Forrás: transparencyreport.google.com

[17] Elérhető: https://transparencyreport.google.com/eu-privacy/overview 2014. 05. 28. – 2019. 04. 29. közötti adatok. (A letöltés dátuma: 2019. 04. 29.)

[18] Uniform Resource Locator – Egységes Erőforráshely.

A statisztikai adatok szerint Magyarországon a kérelmeket benyújtók megoszlási aránya, illetve a kérelmezett intézkedések teljesítésének aránya megegyezik az összesített adatokkal.

A fentiekben említett ítélet, illetve az időközben hatályba lépett GDPR[19] hatására várhatóan az interneten egyre szűkül majd a korlátlan ideig fellelhető adatok, információk köre. Ez a tény szűkíti majd a nyílt forrású hírszerzés, kutatás forrásbázisát, de nem feltétlenül jelenti a hatékonyság csökkenését.

Biztonsági korlátok, a digitális lábnyomok veszélyei

Az általánosan elfogadott meghatározás szerint a digitális lábnyom fogalma azokra a jelekre, nyomokra vonatkozik, amelyek a felhasználó online jelenléte után maradnak, és amelyekből következtetni lehet a tevékenységére. Minden aktivitásunk, és sokszor a passzív jelenlétünk és megfigyelésünk is kitörölhetetlen nyomot hagy az informatikai rendszerekben.

Ebből adódóan a nyílt forrású kutatás kétélű fegyver is lehet. Hiszen ha a kutatás célszemélye kellő szakértelemmel és megfelelő technikai eszközökkel rendelkezik, úgy könnyen azonosíthatja az utána érdeklődőket. A kereséshez, kutatáshoz használt keresőszavak vagy az alkalmazott informatikai eszköz és hálózat azonosítói (mint például az IP-cím vagy -tartomány, a DNS,[20] a domain vagy nickname, mobileszközök IMEI-száma) könnyen elárulhatják az érdeklődőt. Sok esetben ez természetesen nem jelent konkrét dekonspirációs veszélyt, de adott körülmények között már maga az érdeklődés tényének felismerése, az érdeklődő szervezet azonosítása, esetleg a nagyobb számú vagy huzamosabb időn át tartó lekérdezések elemzése értékes információkkal szolgálhat a célszemélyi kör számára.

Ezt minden körülmények között mérlegelni kell, és szükség esetén meg kell teremteni a fedésnek, a lekérdezések leplezésének technikai feltételeit a biztonságos kutatáshoz.

A szakértelem hiányának korlátai, a végrehajtás központosításának kérdése

Szintén régi dilemma, hogy vajon a nyílt forrású információszerzést központosítva, egy erre kijelölt olyan speciális szervezetnek kell-e végrehajtani, ahol mind a technikai feltétel és a humán szakértelem jelen van, avagy minden ilyen irányú igényt ki lehet elégíteni a tényleges felhasználás szintjén. Mivel mindkét álláspont mellett és ellen is lehet érveket felsorakoztatni, az igazság szerintem valahol a két szélsőséges vélemény között van.

[19] General Data Protection Rules – Általános Adatvédelmi Szabályzat; az Európai Parlament és a Tanács (EU) 2016/679 számú, 2018. május 25-én hatályba lépett adatvédelmi rendelete.

[20] Domain Name System – az internetes tartománynevek rendszere.

Nem lehet azt elvárni, hogy egy egyszerű háttérelemzéshez minden olyan adatot, amely az interneten vagy más nyílt forrásból fellelhető, egy másik szervezettől kelljen megkérni. Sok kérdés egy egyszerű Google kereséssel megválaszolható, de az összetettebb kérdésekre is könnyen gyűjthet le adatokat egy rövid képzésen átesett felhasználó.

Ugyanakkor az a mélységű keresés, kutatás és információgyűjtés, amely már speciális programokat és kellő rutint igényel, nem várható el olyan felhasználótól, aki csak ritkán és korlátozott technikai feltételekkel felvértezve kényszerül erre. Különösen igaz ez akkor, ha már az információszerzés tényét is leplezni szeretnénk. Sem a szervezett kiberbűnözésben érintett célszemély, sem egy kiképzett hírszerző ellenőrzése, kapcsolatrendszerének felkutatása nem végezhető el biztonságosan megfelelő fedés, speciális képzettség, hardverek és szoftverek nélkül.

Ez a kérdés az USA hírszerző közösségében is hangsúlyos. Az OSINT-ot egy kicsit szakmán kívülinek érzik. Ezen elterjedt – álláspontom szerint tévedésen alapuló – előítélet egyik magyarázata, hogy a titkosszolgálatok fő feladata a titkok felkutatása, amihez kevésbé illenek a mindenki által hozzáférhető, nyílt adatok. Míg a többi *-INT* (például HUMINT,[21] SIGINT,[22] GEOINT[23]) identitását és szakmaiságát a rendelkezésükre álló specialisták jelentik, addig az OSINT-hoz mindenki ért egy kicsit.

Az USA 2004. hírszerzési törvénye[24] már választás elé állította a DNI-t[25] abban a kérdésben, hogy szükségesnek tartja-e egy központosított speciális egység felállítását. A WMD Bizottság[26] a CIA-n belül javasolta egy Open Source Center[27] (OSC) létrehozását, amely javaslat végrehajtását az USA elnöke szintén a DNI-ra delegálta. Végül a DNI egy CIA-irodát, a Foreign Broadcast Information Service-t[28] (FBIS) nevezett ki OSC-nek, míg irányító végrehajtója a CIA lett.

2015-ben az OSC-ből Open Sourche Enterprise[29] (OSE) lett, és a részleges függetlenségét elveszítve a CIA újonnan létrehozott *Directorate of Digital Innovation*[30] (DDI) alá integrálták be. Az elképzelések szerint az OSE lehetőséget biztosítana a szakértők képzésére, fejlesztésekre, amelyek nélkül az OSINT nem tudna lépést tartani a kihívásokkal. A szakemberek véleménye szerint az OSINT önálló hírszerzési elismertsége most a DDI kezében van, és kérdés, hogy a korábbi előítéleteket mennyire lesz képes kioltani.[31]

Hazánkban is 2015-ben merült fel először a nyílt forrású kutatással, hírszerzéssel foglalkozó speciális egység felállításának igénye. A terrorizmus jelentette fenyegetés hatására először a Szervezett Bűnözés Elleni Központ (SZBKK) keretében osztály

21 Human intelligence – humán (élőerős) hírszerzés.
22 Signals intelligence – jelhírszerzés.
23 Geospatial intelligence – térinformatikai hírszerzés.
24 IRTPA of 2004: Intelligence Reform and Terrorism Prevention Act of 2004 – Hírszerzési reform és a terrorizmusmegelőzési törvény.
25 Director of National Intelligence – nemzeti hírszerzési igazgató.
26 Weapons of Mass Destruction; 2005-ben felállított bizottság az USA tömegpusztító fegyvereket érintő hírszerzési lehetőségeiről.
27 Nyílt Forrású Központ.
28 Külföldi Hírközlési Információs Szolgálat.
29 Nyílt Forrású Vállalkozás.
30 Digitális Innovációs Igazgatóság.
31 Lowenthal 2017, 181.

jogállással kezdett működni, majd a jogutódként 2016 júliusában életre hívott Terrorelhárítási Információs és Bűnügyi Elemző Központ (TIBEK) szervezetéhez került, ahol később főosztállyá bővült. Az Nbtv. alapján a TIBEK „nyílt információgyűjtést és feldolgozást végző szolgáltató és támogató szervet működtet".[32] Ugyan az Nbtv. szerint az egység feladata szolgáltatás nyújtása, de az jól érzékelhető Magyarországon is, hogy az összes igényt nem képes egy szakegység kielégíteni, nélkülözhetetlen a közvetlen végrehajtók általi nyílt forrású kutatás és hírszerzés.

A kutatható terület korlátai, a darknet kérdése

Az Europol évente elkészülő, a szervezett bűnözés aktuális helyzetét értékelő jelentésében[33] kiemelt hangsúlyt fektet a kiberbűnözés veszélyeire és kihívásaira. Ezek között is elsődleges helyen szerepel a darkneten elérhető illegális áruk és szolgáltatások kereskedelme (lőfegyver, kábítószer, új típusú pszichoaktív anyagok), de emellett az illegális fizetési műveletek (kriptovaluták használata, terrorizmus finanszírozása, pénzmosás) is előkelő helyet foglalnak el a veszélyeztetettségi skálán.

Először is kicsit pontosítani kell magát deep web és a darknet fogalmát. Abban megyezenek, hogy egyik területét sem képesek a hagyományos keresőmotorok (például Google, Bing, Yahoo!) keresni. A deep web legális és jellemzően legális tevékenységre használatos, míg a darknet megalkotásának a célja is az illegális kereskedelem, tevékenység leplezése volt.

Egyes becslések szerint a deep web terjedelme mintegy ötszázszorosa a felszíni (nyílt, mindenki által látható) felületnek, azaz a surface webnek. Ebbe beletartoznak többek között a regisztrációhoz kötött fiókok, levelezőrendszerek, netbankos oldalak, szakmai vagy tudományos portálok, de akár a személyes adatokat is tartalmazó felületek is.

A darknet – amelynek terjedelmére becslések sem születtek – használatához már speciális böngészők szükségesek, és az ott található oldalak sem a hagyományos elnevezésekkel, azaz URL-ekkel rendelkeznek. A legismertebb böngészők a TOR,[34] az I2P és a Freenet, amelyek alkalmazása gyakorlatilag ellehetetleníti mind a felhasználó, mind a felkeresett oldal azonosítását.[35]

A darknet egyik legismertebb kereskedőfelülete a 2011-ben létrejött Silk Road (Selyemút) volt a 2013-ban történt felszámolásáig. Egy 2013-ban készült tanulmány[36] szerint a Silk Roadon keresztül értékesített kábítószer értéke az USA-ban megközelítőleg 23 millió dollár volt évente, míg az egész éves kábítószer-forgalom becsült éves mértéke 300 milliárd dollár. Ez ugyan nem tűnt nagymértékű részesedésnek, de a bitcoin és az illegális piactér kombinálása dinamikus fejlődést prognosztizált.

32 Nbtv. 8/A. § (3) bekezdés d) pont.
33 SOCTA: Serious and Organised Crime Threat Assessment – súlyos és szervezett bűnözés fenyegetettségi értékelés.
34 The Onion Router – Hagyma Elosztó.
35 Ciancaglini et al. 2013.
36 Martin 2014, 351–367.

A felfelé ívelő karriernek az FBI[37] 2013. októberi akciója vetett véget. Eljárás alá vonták az üzemeltetéssel vádolt *Dread Pirate Roberts* néven ismert Ross Ulbrichtot, akit 2015-ben többek között pénzmosásért, szervezett bűnözésben való részvételért és kábítószer-kereskedelemért első fokon kétszeres életfogytig tartó szabadságvesztésre ítéltek. 2017 júniusában az ítélet elleni fellebbezését elutasította San Franciscóban a Másodfokú Fellebbviteli Bíróság, így reálisan élete végéig börtönben marad a most 35 éves férfi.

Hasonló forgalmú, közismert darknetes kereskedőfelület volt a 2017 júliusában szinte egyidőben felszámolt *Hansa* és az *AlphaBay*, míg 2019. május elején Németországban szüntették be a *Wall Street Market* nevű, hasonlóan aktív portált az azt üzemeltető három személy elfogásával együtt.

Hiú ábránd lenne azt gondolni, hogy ezekkel az intézkedésekkel megszűnt a darknet illegális kereskedelme. Az illegális árukra – különösen a kábítószerre – az igények nem csökkenek, így a folyamatos megújulás sem maradhatott el. 2013. novemberétől 2014. márciusáig a Silk Road 2.0-n lehetett kábítószert vásárolni,[38] majd 2017 májusában már a Silk Road 3.0 elindulásáról adtak hírt,[39] de aktuálisan a Silk Road 3.1 érhető el. Az egyszerű kereséssel könnyen megtalálhatók az internet nyílt felületén üzemelő azon honlapok, ahol az aktuális kereskedőfelületek hirdetik. Ilyen például a *darkwebnews.com/dark-web-market-list* is, amelyen a piactér aktuális állapota (online/offline), illetve az egyes marketek eléréséhez szükséges információk is megtalálhatók.

Az extraprofit, az illegális áruk és szolgáltatások iránti kereslet és a kriptovaluták elterjedése biztosítja a folytonosságot, amellyel szemben az egyik fellépési lehetőség lehet a nyílt forrású hírszerzés.

Összegzés

Ugyan megbecsülhetetlen mennyiségű értékes információ található olyan tárgyiasult adathordozókon, mint a könyvek vagy újságok, azonban a mai világban a nyílt forrású hírszerzés legnagyobb forrása a digitális alapú világháló. Ennek alkalmazása azonban sok esetben olyan korlátot állít a felhasználók elé, amelyek ismeretének vagy betartásának hiánya téves vagy jogszerűen fel nem használható adatokat eredményez.

Ennek elkerülése, megelőzése érdekében szükséges lenne a nyílt forrású információgyűjtést végrehajtók számára szervezett oktatást – a módszertan, a gyakorlati fogások, illetve az informatikai rendszerek és eszközök alkalmazási ismeretei mellett – a kockázati tényezőkre és korlátokra is kiterjeszteni.

[37] Federal Bureau of Investigation – Szövetségi Nyomozó Iroda (USA).
[38] Osborne 2019.
[39] Richard 2017.

Alkalmazott rövidítések

- Btk.: a Büntető Törvénykönyvről szóló 2012. évi C. törvény
- CIA: Central Intelligence Agency – Központi Hírszerző Ügynökség (USA)
- DDI: Directorate of Digital Innovation – Digitális Innovációs Igazgatóság (CIA)
- DNI: Director of National Intelligence – nemzeti hírszerzési igazgató (USA)
- FBI: Federal Bureau of Investigation – Szövetségi Nyomozó Iroda (USA)
- GDPR: General Data Protection Rules – Általános Adatvédelmi Szabályzat; az Európai Parlament és a Tanács (EU) 2016/679 számú, 2018. május 25-én hatályba lépett adatvédelmi rendelete
- GEOINT: Geospatial intelligence – térinformatikai hírszerzés
- HUMINT: Human intelligence – humán (élőerős) hírszerzés
- IRTPA: Intelligence Reform and Terrorism Prevention Act of 2004 – Hírszerzési reform és terrorizmusmegelőzési törvény (USA)
- Nbtv.: a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény
- NSA: National Security Agency – Nemzetbiztonsági Ügynökség (USA)
- OSC: Open Source Center – Nyílt Forrású Központ (USA)
- OSE: Open Source Enterprise – Nyílt Forrású Vállalkozás (USA)
- OSINT: Open Intelligence – nyílt forrású hírszerzés
- SIGINT: Signals Intelligence – jelhírszerzés
- SOCTA: Serious and Organised Crime Threat Assessment – súlyos és szervezett bűnözés fenyegetettségi értékelés
- SZBKK: Szervezett Bűnözés Elleni Koordinációs Központ
- TIBEK: Terrorelhárítási Információs és Bűnügyi Elemző Központ
- WMD: Weapons of Mass Destruction – tömegpusztító fegyverek

Felhasznált irodalom

Brogen, Mary Kate (2015): How Twitter is Changing Narrative Storytelling: A Case Study of the Boston Marathon Bombings. *Elon Journal of Undergraduate Research in Communications,* Vol. 6, No. 1. Elérhető: www.inquiriesjournal.com/articles/1135/how-twitter-is-changing-narrative-storytelling-a-case-study-of-the-boston-marathon-bombings (A letöltés dátuma: 2019. 05. 04.)

Gál István László (2014): Az OSINT (Open Source Intelligence) mint a kémkedés lehetséges elkövetési magatartása. *JURA,* 20. évf. 1. sz. 51–55. Elérhető: https://jura.ajk.pte.hu/JURA_2014_1.pdf (A letöltés dátuma: 2019. 04. 29.)

Harari, Yuval Noah (2015): *Sapiens: A Brief History of Humankind.* New York, Harper.

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

Lowenthal, Mark L. (2017): *Hírszerzés. A titoktól a politikai döntésig.* Budapest, Antal József Tudásközpont.

Martin, James (2014): Lost on the Silk Road: online drug distribution and the 'cryptomarket'. *Criminology & Criminal Justice,* Vol. 14, No. 3. 351–367. DOI: https://doi.org/10.1177/1748895813505234

Jogforrások

1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról
2012. évi C. törvény a Büntető Törvénykönyvről
Counter-Terrorism and Border Security Act 2019. Elérhető: www.independent.co.uk/news/uk/home-news/terrorist-propaganda-law-thought-crime-click-link-online-prison-a8866061.html (A letöltés dátuma: 2019. 04. 29.)
Európai Bíróság C-131/12. számú ítélete. Elérhető: http://curia.europa.eu/juris/liste.jsf?num=C-131/12&language=HU (A letöltés dátuma: 2019. 04. 29.)
IRTPA of 2004: Intelligence Reform and Terrorism Prevention Act of 2004

Internetes források

Ciancaglini, Vincenzo – Balduzzi, Marco – Goncharov, Max – McArdle, Robert (2013): *Deepweb and Cybercrime. It's Not All About TOR.* Elérhető: www.trendmicro.ie/media/wp/deepweb-and-cybercrime-whitepaper-en.pdf (A letöltés dátuma: 2019. 05. 05.)
Osborne, Charlie (2019): *Failed student jailed for Silk Road, dark web drug profiteering.* Elérhető: www.zdnet.com/article/failed-student-jailed-for-silk-road-dark-web-drug-profiteering/ (A letöltés dátuma: 2019. 05. 05.)
Richard (2017): *Silk Road 3.0 Back From The Dead.* Elérhető: https://darkwebnews.com/darknet-markets/silkroad-3-back/ (A letöltés dátuma: 2019. 05. 05.)
Monnappa, Avantika (2019): *Data Science vs. Big Data vs. Data Analytics.* Elérhető: www.simplilearn.com/data-science-vs-big-data-vs-data-analytics-article (A letöltés dátuma: 2019. 01. 19.)
https://transparencyreport.google.com/eu-privacy/overview (A letöltés dátuma: 2019. 04. 29.)