Az információgyűjtés területeinek evolúciója, a kibertér jelentősége

Dobák Imre

Bevezetés

A témakör a nemzetbiztonsághoz kapcsolódó információgyűjtés kibertérbe áthelyeződő területeinek ezredfordulót követő főbb változásait tekinti át az eltelt időszak jelentősebb nemzetközi „titkosszolgálati" fordulópontjai tükrében. A nemzetbiztonsági szolgálatok összetett feladatrendszerében alapelemként tekinthetünk az információk jelentőségére, amelyek megszerzése, elemzése, értékelése, illetve adott cél érdekében történő felhasználása nélkülözhetetlen módon részei a nemzetbiztonsági folyamatoknak. Az „információk" köré épülő egyes lépések (a megszerzéstől kezdve egészen a felhasználásig) önálló szakterületek kialakulását eredményezték, így gyakran találkozunk a szervezeteken belül adatszerző vagy akár értékelő-elemző, tájékoztató területekkel. Az információk központi szerepe ugyanakkor maga után vonja azt is, hogy a nemzetbiztonság számára releváns információk keletkezési formáiban, megszerzési lehetőségeiben bekövetkező külső változások közvetlenül érintik a szolgálatok működését.

A rendszerrel szemben elvárásként jelenik meg, hogy szükség esetén aktuális és hiteles információkkal rendelkezzen akár az egyén szintjétől kezdve, az átfogó stratégiai döntéseket igénylő eseményekig, folyamatokig. Mindezt alapvetően az előrejelzés céljával, szigorú jogszabályi kötöttségekkel, az adott országok határain kívülre (hírszerzés) vagy éppen a védelmi feladatkör (elhárítás) mentén befelé tekintve egy olyan környezetben, ahol a különböző technológiai platformokon napról napra szinte feldolgozhatatlan mennyiségű információ keletkezik. Kiemelten fontossá válik tehát az információszerzési formák és lehetőségek folyamatos kutatása, valamint a nemzetközi környezetben látható változások nyomon követése.

A nemzetbiztonsági szervezetek ezen információs igényeiket rendkívül szerteágazó módon elégítik ki, amelyek között a források típusát tekintve megjelennek a nyílt és nem nyílt források, az információk megszerzésének típusait illetően az együttműködések, valamint a sajátos egyedi és rendszerszintű titkosszolgálati megoldások, módszerek. Az angolszász terminológia hírszerzési ágait,

https://doi.org/10.36250/01005_07

információgyűjtési területeit[1] tekintve is jól látható a humán és a technikai jellegű irányok elkülönülése, amelyek mögött számos önálló szakmai részterület jött létre. Mivel részletes ismertetésük a szakirodalmak széles körében[2] elérhető, így ezektől eltekintünk, és a kategóriahatáraikon átnyúlva a kibertérben megjelenő információgyűjtés technikai és humán területeit ismertetjük. Hogy ezek milyen mértékben érintik az egyes országok nemzetbiztonsági szféráit, arra mindenképpen a politikai viszonyok, a nemzeti szabályozási környezet, valamint az eltérő gazdasági és technikai képességek gyakorolnak közvetlen hatást. Amíg egyes, technológiailag fejlett országok esetében a globális információszerzés képességei erősödtek fel (például Amerikai Egyesült Államok), addig más országok esetében emellett a belső megfigyelési rendszerek és megoldások váltak láthatóan hangsúlyossá (például Kína). Az itt megvalósuló folyamatok azonban – főként a technológiai környezet globalizálódásának köszönhetően – más országok gyakorlatára is minden bizonnyal hatással vannak, akár a magánszféra védelmének erősítése és a jogi környezet pontosítása, akár a kibertérből érkező veszélyek elleni védekezés fokozása terén.

Hatások – nemzetközi folyamatok

A technológiai fejlődés nemzetbiztonságra gyakorolt hatásait tekintve az információgyűjtés jövőbeli formáit befolyásoló tényezők között kell kiemelni a következőket:

- Az új technológiák exponenciális ütemben fejlődnek, amelyek azonban csak előremutató gondolkodás és stratégiák révén szolgálhatják a kívánt, így például a biztonsághoz kapcsolódó célokat.
- Egyre nő a digitális formában keletkező információk mennyisége, egyre fontosabbá válnak a nemzetbiztonsági szervezetek számára a pontos előrejelzést, megalapozott döntéseket támogató adatok.
- Az adatok felhasználásának üzleti, illetve állami lehetőségei általánosságban felvetették a magánszféra fokozott védelmének, és nemzetbiztonsági oldalról az információgyűjtés határainak a kérdéseit.

[1] Többek között: HUMINT, SIGINT, MASINT, GEOINT, CYBERINT, OSINT információgyűjtési-hírszerzési ágak.

[2] Dobák Imre (szerk.): *A nemzetbiztonság általános elmélete.* Budapest, Nemzeti Közszolgálati Egyetem, 2014.

- Habár számos információgyűjtési módszer a bűnügyi célú és a nemzetbiztonsági célú információgyűjtés (illetve törvényes ellenőrzés) megvalósítása során azonos, nem feledkezhetünk meg azok eltérő céljairól és azok sajátosságairól (például hírszerzés). Ezek elkülönülése a legtöbb országban nyomon követhető.
- Az utóbbi évtizedekben rendkívüli módon felértékelődött a kibertér szerepe és a közegben végzett információszerzés különböző megoldásai. Az információ- és kommunikációtechnológia fejlődése miatt az információgyűjtés, törvényes ellenőrzés irányai is a technológiai környezet felé fordultak.
- A nemzetbiztonsági szervezetek feladatrendszeréhez kapcsolódó biztonsági kihívások okai számos esetben távoli földrajzi, illetve joghatóságukon kívüli területekhez köthetők.

Társadalmunk működése során az általánosságban elterjedt infokommunikációs eszközökön keletkező információk önmagukban felvetik azok hasznosításának kérdéseit. Ezen adatok megállíthatatlanul, egyre nagyobb mennyiségben állnak rendelkezésre, amelyek feldolgozása, értékelése egyre inkább a figyelem előterébe kerül. A nemzetbiztonsági szolgálatok oldaláról is tagadhatatlanul megvan ez az érdeklődés, és – a gyakran hangoztatott megfigyelés társadalmának víziójától eltekintve – nem feledkezhetünk meg arról, hogy ezen adatok, meghatározott jogi szabályozás mentén, mindenképpen hozzájárulhatnak az adott ország biztonságához.

A hidegháborút követően a demokratikus társadalmakban is elfogadottá vált a nemzetbiztonsági célú információgyűjtés, így a titkos információgyűjtés szabályozott alkalmazása.[3] A társadalom oldaláról ugyanakkor felerősödtek a magánszféra védelmének kérdései és különösen 2001 után az „elektronikus lehallgatáshoz" kapcsolódó nemzetközi viták. Minderre a terrorizmus elleni küzdelem rendkívül széles körű amerikai megfigyelési tevékenysége hívta fel a figyelmet, és sokak szerint az orwelli[4] megfigyelés társadalma valósággá vált. Tény, hogy a kommunikáció „lehallgatása vagy nyomon követése intrusív

[3] A nemzeti jog lehetővé teheti szükséges és arányos intézkedésként például a nemzetbiztonság védelme érdekében, a közlések és az azokra vonatkozó forgalmi adatok érintett felhasználó hozzájárulása nélküli lehallgatását, elfogását.

[4] George Orwell 1949-ben írta az *1984* című regényét.

folyamat",[5] így szigorú jogi keretekkel kell szabályozni az alkalmazható megoldások körét és azok működtetésének rendszerét. A témakört elemző EU-tanulmány is rámutat arra, hogy habár a jog védi a magánjellegű kommunikációt, de meghatározott esetekben, többek között a nemzetbiztonsági fenyegetésekkel szemben a kormányok legálisan korlátozhatják a magánszférához való jogot.[6]

Az ezredfordulót követő terrortámadások ilyen rendkívüli események voltak, amivel ez a korlát jelentősen kitágult, nemcsak az érintettek körét illetően, hanem az alkalmazott módszereket tekintve is. Mivel a korábbi megoldások már nem voltak hatékonyak a terrorizmus elleni küzdelem feladataira, a történelem háborús időszakának példáihoz hasonlóan új (nemzet)biztonsági megoldásokat kerestek. Ennek széles példáit leginkább az Amerikai Egyesült Államok esetében láthatjuk, ahol a rendészeti, katonai jellegű intézkedések társadalom által is támogatott kiterjesztésén túl a nemzetbiztonsági szféra adatgyűjtési lehetőségei is kitágultak.

Titkos információgyűjtés a kibertérben

A technikai jellegű információgyűjtés, kommunikáció-ellenőrzés, vagy éppen adatok megszerzése és nemzetbiztonsági célú felhasználása ma már elfogadottnak tekinthető. Amíg ezek bűnüldözési célú igénybevétele alapvetően az adott ország saját területére összpontosít, addig a nemzetbiztonsági (hírszerzési), vagy éppen terrorelhárítási célok mentén teret nyerhetnek a más irányokban végzendő (titkos) információgyűjtési megoldások. Az elmúlt évtized amerikai titkosszolgálati botrányaival[7] számos ilyen kibertérhez köthető megfigyelési, információgyűjtési módszer került nyilvánosságra, amelyek alapján az alábbi információgyűjtési típusok kategorizálhatók.

[5] Institute for Human Rights and Business: *Lawful Interception and Government Access to User Data: Designing a Rights-Respecting Model.* (2016. január 15.) 6.

[6] Institute for Human Rights and Business (2016): i. m. 11.

[7] A legjelentősebb a 2013-ban kirobbant amerikai titkosszolgálati botrány. Kirobbanásának oka, hogy E. Snowden, az NSA amerikai nemzetbiztonsági ügynökséggel szerződésben lévő Booz Hamilton magánvállalat alkalmazottja – Glenn Greenwald, a *Guardian* újságírója segítségével – nyilvánosságra hozta, hogy az Egyesült Államok Nemzetbiztonsági Ügynöksége (NSA), amerikai állampolgárokat is érintve, az infokommunikációs technológiákhoz kapcsolódó új titkosszolgálati módszerekkel, globális szinten folytat telefon- és e-mail-ellenőrzéseket, és tömegesen szerez jogtalanul adatokat.

IKT-szolgáltatóval való együttműködés

A szolgáltatóval való együttműködés – mint a szükséges információkhoz való jutás egyik módja – széles körben alkalmazott megoldásként van jelen a nemzetbiztonsági szervek működése során. A technikai területeken főként azon infokommunikációs szolgáltatókkal való kapcsolatokat láthatjuk, amelyek rendszereiben a nemzetbiztonság számára releváns adatok keletkeznek. Ezen együttműködések vagy jogszabályi alapokon vagy egyéb sajátos érdekeltségi (például piaci) formában valósulhatnak meg. Az együttműködési hajlandóság kapcsán olyan kérdések emelhetők ki, mint az adott szolgáltató már ismertetett vásárlói bizalomvesztéstől való félelme, de nem feledkezhetünk meg a nemzeti szinteken túlmutató globális szolgáltatók alacsony együttműködési hajlandóságáról sem.

Jogszabályi kötelezettség esetén ezen együttműködőkre hárulhat a törvényes ellenőrzési feladatok alapján az elektronikus úton keletkezett információkhoz (közleményekhez) való hozzáférés biztosítása (akár egyedi módon, akár például monitoringfelületet kiépítve).

A szolgáltatói oldalon állnak rendelkezésre azok a metaadatokat (a kommunikációhoz kapcsolódó kísérő és forgalmazási adatok, helyadatok) tartalmazó adatbázisok is, amelyek adatai sajátos módon segíthetik a nemzetbiztonsági szervek tevékenységét. Ezen adatbázisokból a megfelelő jogszabályi engedélyek birtokában végzett egyedi adatkérések mind a bűnüldözésben, mind a nemzetbiztonsági területen nélkülözhetetlen és általános megoldásnak tekinthetők. Ilyen adatok jelennek meg például a mobiltelefonok földrajzi mozgása kapcsán, amelyek általános felhasználása már széles körben elterjedt a társadalomban is (például a térképes alkalmazások, közösségi közlekedés járműveinek nyomon követése), de az adatok nemzetbiztonsági szempontú feldolgozása akár az érintett személy mozgásaira, szokásaira vonatkozóan is információval szolgálhat.

Egyedi adatkérések esetén sajátos irányt jelent a globális infokommunikációs-technológiai nagyvállalatokkal való együttműködés igénye. A társadalom tagjai körében elterjedten használt IKT-eszközök és -alkalmazások kapcsán adott esetekben joggal merülhet fel – például terrorizmus, súlyos bűncselekmények elkövetése – az ezekre irányuló nemzetbiztonsági információs igény. Az államok joghatóságán kívüli üzleti szereplők felé támasztott biztonsági szervezetek kéréseinek kiszolgálása többnyire azonban a szolgáltató – kellően nem ismert – belső döntésén alapulnak.

Az egyedi kérésekkel szemben, az adatok tömeges, nemzetbiztonsági szolgálatokhoz történő „átemelésének", illetve „adatbázisok építésének" kérdése

azonban már vitatott megoldásként került nyilvánosságra. Utóbbi megoldás felvetette, hogy e teljes körű, strukturált adatbázisokból olyan összefüggések tárhatók fel, amelyek akár a kommunikáció-ellenőrzésnél is jelentősebb magánszféra-sérelmet okozhatnak.[8] A nyilvánosságra került amerikai gyakorlatban a megoldás Prism[9] néven vált ismertté, ahol az egyes internet-, illetve hírközlési szolgáltatók együttműködésbe történő szélesebb bevonására törekedtek, és az információgyűjtést azok beleegyezésével végezték (érintett volt többek között a Google, a Microsoft, a Yahoo, a Facebook, a Skype, az AT&T vagy akár a YouTube is). A nyilvánosságra került ellenőrzési programokból jól látható az adatgyűjtések volumene és jelentősége, amelyek tömeges adatbázisokká formálása a háttérben széles kapcsolatrendszert, lényegében a nemzetbiztonság, illetve az üzleti-szolgáltatói szféra nem nyilvános együttműködését igényelte.

2015-től a korábbi amerikai tömeges adatgyűjtés jogi keretei megváltoztak (a 2001-ben elfogadott Patriot Act törvénycsomagot felváltotta az úgynevezett Freedom Act törvény), lezárva ezzel a cél nélküli, készletező jellegű adatbázisok felhasználásának szakaszát.

Informatikai infrastruktúrán áthaladó kommunikáció ellenőrzése

Az Amerikai Egyesült Államok gyakorlatából nyilvánosságra került az úgynevezett *upstream* ellenőrzési forma, amely során belföldi és külföldi informatikai gerinchálózatok csomópontjain, elosztóin áthaladó telefon- és internetforgalmak ellenőrzését végzik el. A hazai szakirodalomban úgynevezett mély csomagelemzés (DPI) néven is jelölt módszer során az áthaladó adatforgalom minden csomagjának a tartalmát vizsgálat alá veszik, amely „hozzáférés azonban meglehetősen korlátozott, hiszen bár a nyíltan küldött adatok könnyen ellenőrizhetők, feldolgozhatók, a titkosított forgalmak esetében a titkosítást fel kell törni, ami időben hosszadalmas, nagy számítástechnikai eszközparkot igénybe vevő folyamat”.[10] Ebben az esetben is bizonyos mértékig jelen van a külső féllel való

[8] Glyn Moody: Revised Snooper’s Charter ignores key criticisms, widens police powers further. *Ars Technica,* 2016. március 2.

[9] Privacy and Civil Liberties Oversight Board: *Report on the Surveillance Program Operated Pursuant to Section 702 of the FISA* (2014. július 2.).

[10] Kovács Zoltán: Az alkalmazásszolgáltatók törvényes ellenőrzésének jövője – a technológiák konvergenciájának tükrében. *Nemzetbiztonsági Szemle,* 4. (2016), 1. 79–99.

együttműködés (például infrastruktúra-szolgáltató) jelenléte, hiszen a kommunikáció tranzit jelleggel a szolgáltató rendszerein halad keresztül.[11] A 2013-ban kirobbant botrány kapcsán külföldi nemzetbiztonsági partnerszolgálat közreműködésére is találunk nemzetközi példát (ilyen megoldást alkalmazott például a brit GCHQ technikai nemzetbiztonsági szolgálat Tempora néven, amely adatait megosztotta az amerikai NSA és a FiveEyes[12] együttműködés egyéb szolgálataival). A megoldás vitatott elemei közé tartozik az információk tömeges gyűjtése, valamint hogy az információgyűjtés technikai sajátosságából adódóan nem biztosítható, hogy kizárólag csak a célszemély kommunikációját ismerjék meg.[13] A megoldás alkalmazása vélhetően ott kerülhet előtérbe, ahol az együttműködés, illetve jogszabályi úton történő érdekérvényesítés nehezebben (például külföldi szolgáltató rendszerén áthaladó kommunikáció) valósulna meg (de az amerikai példa esetében gondolhatunk akár egyéb hírszerzési célokra is).[14]

Kibertérben megjelenő aktív eszközök, hackertechnikák alkalmazása

Az elmúlt évek már úgynevezett post-Snowden korszakában – a tömeges információgyűjtés vitatott formáinak alkalmazását követően – mind a nemzetbiztonsági és terrorelhárítási, mind a bűnüldözési célú titkos információgyűjtés során jogszerűen alkalmazható megoldásként kerültek előtérbe az úgynevezett hackingtechnikák. A gyűjtőkategória számos módszert takarhat,[15] mégis kategóriaként a tömeges jellegű megoldásoktól jól elkülöníthető információgyűjtési

[11] Privacy and Civil Liberties Oversight Board (2014): i. m. 35.

[12] Az Egyesült Királyság és az USA között 1946-ban megkötött technikai titkosszolgálati célú együttműködés (UKUSA), amelynek tagsága később Ausztráliával, Kanadával és Új-Zélanddal bővült (FVEY).

[13] Az ellenőrzés így lényegében egyfajta szűrő-kutató jelleget kap. Lásd Davis S. Kris: Trends and Predictions in Foreign Intelligence Surveillance: The FAA and Beyond. *Hoover Institution Essay, Aegis Paper Series,* (2016), 1601. 17.

[14] Az Egyesült Államok esetében lásd a FISA (Foreign Intelligence Surveillance Act, 1978) külföldi hírszerzési megfigyelési törvényt az elektronikus, külföldi hírszerzési célú megfigyelés szabályozására, a módosításáról szóló törvényt (FISA Amendments Act, 2008), valamint a Terrorist Surveillance Programot (TSP, 2001). Dobák Imre: Technikai típusú információgyűjtés a változó biztonsági kihívások tükrében. *Hadmérnök,* 12. (2017), 2. 235–249.

[15] 2017-ben a WikiLeaks több mint nyolcezer titkosított dokumentumot közölt többek között a CIA technikai hírszerzési megoldásairól, eszközeiről (köztük például okostévék mikrofonján keresztül történő lehallgatás).

formát jelent. Idesorolhatók az úgynevezett kémprogramok is, amelyek létrehozásának alapjait az internet szabad, nyílt forráskódú fejlesztéseket biztosító világa tette lehetővé. Sajátos, a kibertérben történő információgyűjtésre szakosodott állami, illetve nem állami üzleti szereplőkhöz, hackerekhez köthető üzleti szegmens foglalkozik a számítógépek webkameráin, mikrofonjain keresztül valós idejű megfigyelést, fájlok kinyerését biztosító programok létrehozásával, amelyek terjesztésére, exportjára azonban szigorú engedélyezési szabályok vonatkoznak.

A velük való együttműködés azonban – amellett, hogy akár hatékony, célirányos információgyűjtési megoldáshoz juttathat egy nemzetbiztonsági szolgálatot – magában hordozhatja a nemzetbiztonsággal fennálló kapcsolat nyilvánosságra kerülésének kockázatát is. Talán éppen ennek ellensúlyozására több ország is elkezdte saját, a kibertérben alkalmazható információgyűjtési és egyéb offenzív műveleti megoldásokat biztosító nemzeti/állami szintű struktúráinak és képességeinek a kialakítását.

Az egyedi megoldással (kémprogram) a célszemélyhez (illetve informatikai eszközéhez) kapcsolódó olyan ellenőrzési megoldás válik lehetővé, amely esetenként a földrajzi értelemben vett határokon átlépve[16] biztosíthatja a célszemély kommunikációjának ellenőrzését, megismerését. Németország esetében a hackingtechnikák például már közel tíz évvel ezelőtt megjelentek, de akkor még vitatott volt a használatuk. Ezt követően már nem külső forrásból, hanem saját fejlesztésekkel kívánták a megoldásokat biztosítani. A témakört vizsgáló átfogó anyag alapján[17] a német belügyminisztérium egy több száz fős szervezetet hozott létre (ZITiS), amely a német bűnüldözést támogatja a technikai készségek és a szakértelem biztosítása révén. A francia hatóságok hasonlóan saját eszközöket fejlesztettek ki a célszemély információihoz való távoli hozzáférés céljából, és Olaszország is a saját fejlesztői képességek irányába mozdult el. 2017-es törvénytervezetük például kimondja, hogy a megoldásokat a szférán belüli, nem külső szerződéses félnek kell működtetnie.

A nemzetbiztonsági információgyűjtés aktuális megoldásai kapcsán a hackingformák (akár külső együttműködői környezettel, akár belső állami

[16] Az Egyesült Államok esetében merült fel, hogy szövetségi bírók adjanak engedélyt az FBI számára a bíró illetékességi területén kívül található számítógépek távolról történő kutatására. Mark M. Lowenthal: *A titkoktól a politikai döntésig.* Budapest, Antall József Tudásközpont, 2017. 616.

[17] Mirja Gutheil et al.: *Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices*. Study for the LIBE Committee, European Union, 2017.

struktúrán belüli[18] végrehajtással történő) fejlődését, valamint a szolgáltatókkal való jogszabályi együttműködések erősítését és azok adattárolásra, illetve kérés esetén átadásra való kötelezésének jogszabályi megoldásait láthatjuk. Utóbbira talán a legszélsőségesebb megoldásként az orosz példa említhető, ahol mind a kommunikáció tartalmának fél évig, mind a metaadatoknak három évig történő tárolása a szolgáló kötelezettsége. Oroszország esetében a vonatkozó jogszabály továbbá előírja a titkosított kommunikáció során a dekódolásban való segítségnyújtást a titkosszolgálat számára.[19]

Aktív képességek

A kibertérben zajló, a társadalom számára is megismert jelentősebb kiberbiztonsági események jól jelzik, hogy napjaink különböző konfliktusaiban már kiemelt szerepet kapnak a kibertérhez köthető védelmi és támadó megoldások. Amíg az előbbi a kiberbiztonság rendkívül széles területét öleli fel, az offenzív megoldások már gyakran a hibrid hadviseléshez kapcsolódva akár a katonai információs műveleteken belül a kibertérben folyó műveletként,[20] akár a titkosszolgálatoknak tulajdonítva láthatók. Értelemszerűen az offenzív műveletek már túlmutathatnak az információgyűjtés szakmai területein is, hiszen gyakran a megszerzett információkra építve, békeidőben például aktív nemzetbiztonsági intézkedésként értelmezhetők, míg a hadviseléshez kapcsolódva akár az alkalmazás céljaiban (például katonai célok) és méreteiben (egyedi célok vagy például kiterjedt rendszerek) is elkülönülhetnek.

Amíg a kibertérben folytatható offenzív típusú műveletek (védelmi célból történő) állami alkalmazásának lehetősége jelenleg is szakértői viták tárgya, addig a kiberbiztonság a társadalom, a gazdasági szféra, valamint az állami szereplőket egyaránt érintő tevékenységként átfogó együttműködési és fejlesztési lehetőségeket teremtett. Mindkét területen jól látható, hogy számos ország az utóbbi öt-tíz évben már megkezdte ez irányú képességeinek kiépítését és a katonai-védelmi struktúrák, illetve a nemzetbiztonsági szervezetek égisze alatt a kapcsolódó eszköz- és módszerkészletek létrehozását. A vonatkozó struktúrák kialakítása

[18] Lásd Vault 7: CIA Hacking Tools Revealed. *WikiLeaks,* (é. n.).

[19] Ronald Bailey: Is Russia's Surveillance State Being Modelled on the West? New Russian anti-encryption and data retention laws look sadly familiar. *Reason,* 2016. július 22.

[20] Haig Zsolt et al.: *Elektronikai hadviselés.* Budapest, Nemzeti Közszolgálati Egyetem, 2014. 27.

(akár katonai, akár nemzetbiztonsági) több országban is illetékességi és irányítási kérdéseket vetett fel. Alapvetően annak kapcsán, hogy a kibertérben végzendő (titkos) műveletek egyes elemei a hadviselés részeként, a biztonsági szféra új elemeként vagy a nemzetbiztonsági tevékenység részeként értelmezhetők. A nemzetközi terroristaellenes műveletek fényében a határ még nehezebben húzható meg.

Alkalmazásuk szintjei is akár az adott egyéni szinttől kezdve (például online tevékenységének korlátozása), a biztonságot fenyegető veszélyekre történő válaszadáson át (például terrorizmus során az online formában történő toborzás vagy akár a terrorizmus finanszírozásának megakadályozása), egészen az államok–államok közötti, fizikai értelemben vett jelentős pusztítást és várhatóan áldozatokat okozó (például elektromos hálózatok leállítása) tevékenységekig húzódhat.

A formálódó új nemzeti szintű képességek valós súlyát rendkívül nehéz megítélni. Az egyes kormányzati nyilatkozatok mögött akár a korábbi hidegháborús stratégiákból ismert elrettentés kibertérre átformált gyakorlata, akár a képességek túlzott előrejelzése is állhat. Tényként kezelhető ugyanakkor, hogy az offenzív területek valós súlyát a legtöbb állam próbálja titokban tartani, mondván, hogy csak akkor fogják alkalmazni azokat, ha valóban szükség lesz rá. Nagy-Britannia például 2018 végén 500 fős, a Védelmi Minisztérium és a GCHQ nemzetbiztonsági szolgálat állományából álló kibertámadási egységgel történő bővítésre készült, hogy szembenézzenek az Oroszország, Észak-Korea és Irán irányából jelentkező fenyegetésekkel. A feladat összetett titkosszolgálati és katonai hadviselési jellegét jól mutatja a nemzetbiztonsági és védelmi minisztériumi együttműködés szükségessége.[21]

HUMINT a kibertérben

A technológiai fejlődés, a kibertér növekvő szerepe a humán jellegű titkosszolgálati tevékenységekre is folyamatosan hatást gyakorol. Gyakran hangzik el, hogy a humán jellegű információgyűjtési módszerek a történelem folyamán változatlanok maradtak, hiszen azok többsége magukhoz az emberi tulajdonságokhoz és viselkedés sajátosságaihoz kapcsolódnak, míg a technikai eszközökkel

[21] David Bond: Britain preparing to launch new cyber warfare unit. *Financial Times,* 2018. szeptember 21.

végzett információgyűjtési módszerek egy folyamatosan változó és fejlődő kört takarnak. A megállapítások azonban csak részben tekinthetők igaznak, hiszen az új technológiák megjelenésével számos olyan információgyűjtési forma is kialakult (illetve átalakult) a kibertérben, amelyek a hagyományos humán jellegű titkosszolgálati elveket és módszereket tükrözik vissza.

A kibertérhez köthető HUMINT kérdésköre az ezredfordulót követően jelent meg, fogalmi kategóriája pontos határokkal még nem lezárt, nemzetközi szakirodalma is viszonylag még szűkösnek tekinthető. Megjelenésével gyakran az online HUMINT, CYBERHUMINT címszavak mentén találkozhatunk, amely lényegében az emberi erőforrásokra építő humán hírszerzés, illetve információgyűjtés egyes szakmai ismereteinek, valamint a kibertérhez kapcsolódó informatikai ismeretek és szakértelem koncentrációját jelenti. (Belső tartalmát tekintve számos értelmezéssel találkozhatunk, ahol a fontos választóvonalat a nyílt és azon túlmutató tevékenységek elválasztóvonalai, határai képezik.) Alapkérdésként merül fel, hogy a századunk fejlett infokommunikációs felületeihez köthető humán vonatkozású titkosszolgálati módszerek, azok alkalmazási metodikái újnak tekinthetők-e, vagy csak a régi módszerek korszakunkhoz igazodó megjelenését, leképeződését láthatjuk.

A 20. század második felében a hidegháborús zártság révén a közvetlen, emberi erőforráshoz köthető titkosszolgálati módszerek (például titkos kapcsolatok, ügynökök alkalmazása) talán minden más eszköznél fontosabbnak bizonyultak. Szakmatörténeti szemmel vizsgálva, az úgynevezett hálózatok alkalmazása a titkos információgyűjtés irányaitól (belföld, külföld, elhárítás, hírszerzés) függetlenül mindenütt jelen voltak, legyenek azok akár a katonai célú információgyűjtés feladatai vagy akár a biztonságpolitikai, gazdasági célú titkosszolgálati munka területei. Az ősi emberi tulajdonságokhoz és személyes kapcsolatokhoz köthető viselkedés sajátosságai miatt talán nem csodálkozhatunk azon, ha az ügynökök, informátorok, rezidensek, titkos találkozási helyek vagy akár a megszerzett információk személyes és személytelen titkos továbbítási módszereivel a titkosszolgálatok történetében országoktól függetlenül egyaránt találkozhatunk. Ezen módszerek a vasfüggöny ellenére keleten és nyugaton szinte párhuzamosan, egymás módszereit továbbfejlesztve, az információk megszerzésére való törekvés (hírszerzés) és az annak megakadályozására irányuló feladatok (elhárítás) légkörében formálódtak. Hátrányai közül a kapcsolat, az együttműködő biztonságának közvetlen fizikai veszélye emelhető ki, amely egyben indokolta a nagyfokú konspirációt és az információk forrásainak kiemelt védelmét.

Már ekkor megtalálhatjuk azokat a pszichológiai háttérismereteket, amelyekkel ma az interneten például a piaci célzatú információgyűjtés, a befolyásolás vagy akár a vásárlói szokások megismerése és profilozás kapcsán találkozunk. A szocialista állambiztonságban mindezt az úgynevezett „operatív pszichológia", lényegében a pszichológiai ismeretek és módszerek állambiztonság területén történő alkalmazásának témaköre fedte le. Jelentősége a humán típusú operatív tevékenységek (így például a lehetséges ügynökök tanulmányozása, beszervezése, majd foglalkoztatása) során mutatkozhatott meg, de a befolyásolás, megygyőzés, megtévesztés vagy akár az operatív játszmák szintén a pszichológia területéről merítettek.[22] Mint Révész Béla megfogalmazza:

> „[N]em csak a diktatúrák állambiztonsági szerveinél, de a demokráciák nemzetvédelmi szolgálatainál is megtalálható a komplex operatív módszerek körében – a dezinformáció, a csapda, az intézkedés, valamint a kombináció mellett – az operatív játszma, amely továbbra sem nélkülözheti az operatív pszichológia alkalmazott ismeretanyagát."[23]

Amellett, hogy a humán titkosszolgálati területek (például megfigyelés, titkos kapcsolatok) hagyományos megoldásai napjainkban is meghatározók, a technológiai környezet fejlődésének köszönhetően azok bizonyos területei már leképeződtek az elektronikus-információs felületeken, illetve igénybe veszik a technikai eszközrendszerek támogatását. A hatalmas változást jól szemlélteti, hogy amíg a közvetlen emberi erőforrással végzett figyelési tevékenységek a 20. század közepén még csak fényképezőgépekkel, kamerákkal és gépjárművekkel egészülhettek ki, addig a század végére már a technikai információgyűjtés ágazataihoz sorolható drónokról, összetett kamerarendszerekről, valamint automatikus arcfelismerési megoldásokról beszélhetünk.

Példaként a témakört vizsgáló egyik 2019-es tanulmány[24] adatai említhetők, amely szerint a világ megfigyelőkamerákkal legjobban kiépített első 20 városából kilenc Kínában található, ahol az előrejelzések szerint 2022-re minden két emberre egy megfigyelőkamera fog jutni. A nagyobb európai városokat tekintve a listában London a 6. helyen áll több mint 627 ezer, Moszkva a 18. helyet 146 ezer, Berlin pedig a 19. helyet foglalja el közel 40 ezer, megfigyelést lehetővé tevő kamerájával. De gondolhatunk az elektronikus rendszerekben hagyott

[22] Révész Béla: Állambiztonság és pszichológia. *Beszélő,* 10. (2005), 5. 48–62.
[23] Révész (2005): i. m.
[24] Paul Bischoff: The word's most-surveilled cities. *Comparitech,* 2019.

nyomok (földrajzi helyzet, telefonok azonosítói, biometrikus azonosítók) jelentőségére is, vagy akár a vizuális megfigyelés korszerű technikai megoldásaira.

A közösségi oldalak jelentősége

A társadalomban zajló kommunikációs szokások változását jól jelzik a nagyobb közösségi médiumok felhasználóinak statisztikai adatai. Az internetezők közül összességében 3,3 milliárd fő tekinthető – többségében mobileszközeiket felhasználva – aktív közösségimédia-felhasználónak,[25] ahol a legnagyobb szereplő, a Facebook esetében például tíz év alatt megtízszereződött a felhasználóinak száma, és napjainkra már közel 2,5 milliárdos körrel büszkélkedhet.[26]

A közösségi oldalak mentén az elmúlt években sajátos, a társadalomban általánosan használt „információmegismerési" megoldások alakultak ki, hiszen ezek a felületek rendeltetésükből adódóan a felhasználók által önkéntesen közzétett, rendkívüli mennyiségű, többségében nyíltan megismerhető adatot koncentrálnak. Az információgyűjtés szakmai kategóriáit tekintve ezen oldalak nyílt adatainak felhasználása az úgynevezett OSINT (nyílt forrásból történő információgyűjtés) nagyobb szakmai kategóriájaként értelmezhető, amelyen „belül mintegy leágazásként […] a SOCMINT (Social Media Intelligence)"[27] területe öleli fel a közösségi média oldalairól történő információgyűjtést. A közösségi oldalak működésének és céljainak sajátosságaiból adódóan a passzív jellegű SOCMINT nyílt információgyűjtése azonban már olyan (fedő)profilokat igényelhet, amelyek ezt az adatgyűjtést lényegében megalapozzák.

Mindezen túlmutatva (és ezáltal már elkülönülve az OSINT-tevékenységtől) bizonyos folyamatok személyes közreműködést, kommunikációt, aktivitást is igényelhetnek a felhasználó irányába, amelyek nemzetbiztonsági értelmezésben már az online HUMINT (CYBINT) témaköréhez sorolhatók. Mivel ebben az esetben a felhasználókhoz köthető nem nyilvános adatok lényegében offenzív módon történő megszerzéséről beszélhetünk,[28] így annak jellege miatt

[25] Lenyűgöző közösségi média statisztikák I. rész. *Szubjektív,* (2018. szeptember 12.).

[26] 2019. 3. negyedév, forrás: Number Of Monthly Active Facebook Users Worldwide as of 1st Quarter 2020. *Statista,* (2021).

[27] Szabó (2019): i. m. 71.

[28] Erdész Viktor: A SOCMINT helye, szerepe az összadatforrású hírszerzésben, *Felderítő Szemle,* (2018), 4. 27–40.

a megfelelő engedélyezés folyamata és egyéb nemzetbiztonsági szempontok figyelembevétele is fontossá válik. Egyetértve Erdész megfogalmazásával, „a SOCMINT, az OSINT […] területei és a CYBINT között félúton helyezkedik el abban a tekintetben, hogy a nyilvánosan megosztott információk megszerzésére szakosodik ugyan, de a fedőprofilok használatával megtéveszti a közösségimédia-vállalatokat, valamint a célszemélyeket és csoportokat".[29]

Az emberi erőforrásból végzett információgyűjtés kibertérhez kapcsolódó megoldásai számos előnnyel és hátránnyal is rendelkeznek. Ezek közül – a technikai területekkel szemben – talán kiemelhető, hogy a megszerzendő információk nem strukturáltak,[30] ezért emberi közreműködést igényelnek, egy-egy információgyűjtési folyamat során jelen van az azonnali reagálás (aktív kapcsolat) igénye (játszma), rendelkezésre áll a megtévesztés lehetősége. A hagyományos HUMINT-ismeretek[31] így a kibertérben végezve is értelmezhetők, amelyek hatékony alkalmazásához a szakmai és technikai felkészültségen túl a biztonságos működési környezet kialakítása, valamint az információk megjelenítését, feldolgozását, adatok elemzését, vizualizálását biztosító technikai megoldások szükségesek. Gondoljunk a tevékenység végzéséhez szükséges konspirációt biztosító felhasználói profilokra és azok folyamatos működtetésére, aktivitásuk fenntartására, amelyek önmagukban azonban még nem jelentik az online HUMINT tevékenységét, csak a kereteket teremthetik meg annak végzéséhez.

A köztudatban az infokommunikációs platformokon végzett HUMINT-tevékenység gyakran mosódik össze a social engineering tevékenységgel is.[32] Az átfedéseket vizsgálva a social engineering módszerek használatával az emberi tulajdonságokat kihasználó különböző manipulációs, befolyásolási, megtévesztési technikák és annak egyre bővülő támadási célú formái során juthatunk el a kívánt információ megszerzéséig. A social engineering esetében nem hírszerzési területről, ágról beszélhetünk, hanem a módszerek egyfajta gyűjtőkategóriájáról, amelynek egyes elemei – mivel a humán oldalról jelentkező sérülékenységre épít – a hagyományos titkosszolgálati HUMINT-területeken is megtalálhatók, valamint alkalmazása sem kizárólag a kibertérhez kapcsolódik. Módszereinek

[29] Erdész (2018): i. m.

[30] Luc Pigeon – Clark J. Beamish – Michel Zybala*: HUMINT Communication Information Systems for Complex Warfare.* Defence Research and Development Canada Valcartier (QUEBEC), 2002.

[31] A témakörben lásd Regényi Kund (szerk.): *Információszerzés kapcsolati forrásai.* Budapest, Nemzeti Közszolgálati Egyetem. 2019.

[32] Amit Steinhart: *The Future is Behind Us? The Human Factor in Cyber Intelligence: Correlations Between Cyber-HUMINT and Hackers' Social Engineering* (é. n.).

tartalmában a befolyásolás, rábeszélés eszközeit[33] kell keresni, amellyel az ember mint célpont megtévesztő lehet. Alapesetben az alkalmazója és az „áldozat" között valamilyen interakció valósul meg, de számos esetben erre nem kerül sor, és a megtévesztés más úton zajlik.

A social engineering során az emberi „célpont" csak egy köztes kapocs a támadó és az adott védendő rendszerinformáció között. Habár lehetnek módszerbeli átfedések a szintén pszichológiai elemeket és a hagyományos HUMINT metodikáját alkalmazó eddig vizsgált online HUMINT-tevékenységgel, utóbbi az emberre mint információforrásra tekint.[34]

A social engineering kibertérben megjelenő módszerei között megtalálhatók a humán, valamint a hackertechnikákhoz sorolható technikai megoldások, így ismeretei is gyakran a két terület szakmaiságát ötvözik. Ennek arányait az alkalmazó informatikai, kommunikációs és személyes képességei, ismeretei befolyásolhatják, de tipizálhatók annak főbb, bár rendkívül gyors ütemben bővülő módszerei is.[35] Az idesorolható módszerek az egyes szakirodalmakban gyakran eltérnek, és egyéb technikai jellegű támadási technikákat is idesorolnak. Nemzetbiztonsági értelemben ezek bizonyos elemei a hagyományos titkosszolgálati módszerek között ismert és ott jogszerűen alkalmazott megoldások (például fiktív adatok felhasználása, ürügyek és legendák alkalmazása, kapcsolatépítési szándék), míg a social engineering során azok illegális célját kell feltételezni, így a kategória a kiberbiztonság, a védekezés oldaláról kap különös jelentőséget. Amíg a hagyományos „Intel" területek esetében rendszerszintű szabályzatokkal, doktrínákkal találkozhatunk, addig az online HUMINT esetében a fogalmi letisztulást vélhetően tovább nehezíti, hogy amíg a hagyományos Intel területek

[33] Kevin D. Mitnick – William L. Simon: *Art Of Deception: Controlling the Human Element of Security.* Hoboken, John Wiley & Sons, 2003.

[34] Cyber-HUMINT: https://wikivisually.com/search

[35] Tóth Tamás: Egyes Social Engineering módszerek elhatárolása és rendszerezése. *Szakmai Szemle,* 18. (2020), 1. 87–110. kategorizálása alapján idesorolható módszerek: idegen identitás felhasználása, segítség kérésére módszerek: help desk kihasználása, third party authorization (harmadik fél felhatalmazása), piggybacking (más jogosultságának felhasználása), tailgating (szoros követés), hamis bizalomkeltés; segítség nyújtására módszerek: reverse social engineering, quid pro quo (valamit valamiért módszer), shoulder surfing (képernyő jogosulatlan megtekintése) módszer, dumpster diving (információk felkutatása a hulladékban) módszer. IT-alapú módszerek: álweboldalak, adathalászat (phishing [e-mail-alapú adathalász módszer], vishing [hangalapú adathalász módszer], smishing [rövid üzenetalapú adathalász módszer], pharming [DNS-eltérítés-alapú adathalász módszer], KRACK [Key Reinstallation Attack]), nyílt internethálózatok manipulálása, kártékony programok, baiting (adathordozók szétszórása).

az adatok forrása mentén épülnek fel, addig a kibertérben végzett HUMINT-tevékenység valójában az alkalmazott módszer kategóriáját jelöli.

Nemzetközi szakirodalmak alapján látható, hogy a titkosszolgálatok és mellettük az üzleti célú hírszerzéssel foglalkozó magánszervezetek jelentős forrásokat fordítanak a kibertérben végzett információgyűjtésre.[36] Ennek során azonban „úgy tűnik, hogy különösen a titkosszolgálati információgyűjtés területén figyelmen kívül marad sok olyan hagyományos készség, amelyeket a nemzeti hírszerző szervezetek több mint egy évszázados tapasztalata alapján értek el".[37]

A hírszerzési célú online tevékenység kérdéseiben a szakirodalmak érthető módon kevés részismeretet tartalmaznak, hiszen azok – az állami célú hírszerzési tevékenységeken túlmutatva – különböző illegális tevékenységek részeként, így például az ipari kémkedés területein (vagy akár egy szemben álló fél esetében) is felhasználhatóvá válhatnak. A témakör a kiberbiztonság területén is előtérbe kerül, hiszen a külső támadók elleni védekezés nyíltan, jogszerűen végezhető és kutatandó terület. Ehhez azonban a szükséges infokommunikációs, informatikai szakértelmen túl értelemszerűen ismerni kell azokat a technikákat,[38] amelyek akár a káros programok, vagy akár a befolyásolás és manipuláció segítségével kívánnak a támadói oldalról eljutni a kívánt információhoz.

Az online HUMINT élesen nem lehatárolt kategóriáját tekintve összességében megfogalmazható, hogy:

- Forrásai humán jellegűek, emberi interakciót igényelnek a kibertérben.
- Főként az egyének által kibertérben használt applikációkhoz, közösségimédia-felületekhez kapcsolódhat alkalmazásuk, ahol a hagyományos HUMINT-hoz hasonló folyamatok végrehajthatók. Egyes szakértők azt is megfogalmazzák, hogy habár a hagyományos HUMINT hasznossága csökken, a szociális média miatt az online HUMINT szerepe növekszik.[39]
- Megvalósítását tekintve alapvetően aktív jellegű tevékenység, a passzív elemek például a közösségi oldalakhoz kapcsolódó információgyűjtés során a SOCMINT-hoz sorolhatók. Amíg az első esetben a hagyományos HUMINT-hoz hasonlóan egyének közötti interakciók jelennek meg,

[36] Steinhart (é. n.): i. m. 164.

[37] Steinhart (é. n.): i. m. 164.

[38] Deák Veronika: Social engineering alapú információszerzés a kibertérben megvalósuló lélektani műveletek során. *Hadtudományi Szemle,* 12. (2019), 3. 95–111.

[39] Matthew Harris: The Limit of Intelligence Gathering: Gianni Vattimo and the Need to Monitor 'Violent' Thinkers. In Jai Galliott – Warren Reed (szerk.): *Ethics and the Future of Spying, Technology, National Security and Intelligence Collection.* Routledge, 2016. 28.

addig utóbbinál például a közösségi hálózat zárt csoportjában való passzív jelenlét (SOCMINT) említhető, de idesorolhatjuk a bűnüldözési, illetve a nemzetbiztonsági munka során is alkalmazható profilozást, amelynek számos hagyományos módszere ismert,[40] és amelynek köre a 21. századi korszerű technológiák elterjedt társadalmi használatával új lehetőségekkel bővült.

– Alkalmazásuk során a konspiráció széles körű, mind a feladat célja, mind az alkalmazó személye (például információgyűjtő személy) konspirált, a tevékenységnek részei lehetnek a megtévesztés, a befolyásolás. Példaként a brit GCHQ nemzetbiztonsági szolgálat említhető, ahol Glenn Greenwald[41] szerint társadalomtudósokból (pszichológusok) álló csoportot is igénybe vesznek, hogy kidolgozzák az online HUMINT, a befolyásolás és a megtévesztés technikáit.[42]
– Megoldásai mindenképpen túlmutatnak az OSINT-tevékenységen.[43] Amíg a kibertérben végzett nyílt információgyűjtésnek a források elérhetősége, valamint a jogszabályi környezet határt szabhat (például üzleti célú adatgyűjtés), addig például a hírszerzési célú CYBERHUMINT alkalmazási határait (hasonlóan a HUMINT hagyományos területéhez) az egyes nemzeti szabályozási környezetben kell keresni. A témakörben elérhető nemzetközi forrásokat tekintve kiemelhető a nyilvánosságra került brit JTRIG *(Joint Threat Research and Intelligence Groups)* dokumentuma,[44] amely alapján a tevékenység céljai olyan egyének, csoportok, állami szereplők lehetnek, akik bűnügyi, nemzetbiztonsági, vagy egyéb védelmi szempontból fenyegetést jelentenek. Speciális technikák állhatnak rendelkezésre lejáratásra, megzavarásra, bomlasztásra, olyan elemeket alkalmazva, mint például:
  • meggyőző üzeneteket tartalmazó videók feltöltése;

[40] Általános szakaszai és módszerei kapcsán lásd példaként M. Tóth Balázs – Pap András László: *A hatékonyság mítosza. Az etnikai profilalkotás alkotmányos és rendészeti kérdőjelei.* Budapest, L'Harmattan, 2012. 32; 228–229.

[41] Greenwald (2014): i. m. 193.

[42] The Art of Deception. Edwardsnowden.com, (é. n.)

[43] Az OSINT kérdéseit részletesen lásd Kenedli Tamás: A nyílt forrású információszerzés (OSINT). In Dobák Imre (szerk.): *A nemzetbiztonság általános elmélete.* Budapest, Nemzeti Közszolgálati Egyetem, 2014.

[44] Mandeep K. Dhami: Behavioural Science Support for JTRIG'S (Joint Threat Research and Intelligence Groups) Effects and Online HUMINT Operations. 2011. *The Intercept,* 2015. június 22.

  - online közösségi oldalakon álnevek, profilok készítése;
  - blog és fórumtagságok elérése, ahol adott témákban diskurzusok indíthatók;
  - hamis üzenetek és e-mailek küldése vagy akár hamis kereskedelmi oldalak kialakítása.
- Nemzetbiztonsági célú alkalmazása során elhárulhatnak az akadályok a nagyobb adatbázisokhoz (akár például állami szinten működtetett adatbázisokhoz) való hozzáférés, így a tevékenység egyéb oldalú támogatásának és az adatok összevetésének lehetősége előtt.