HADMÉRNÖK

XII. Évfolyam 2. szám – 2017. június

TECHNIKAI TÍPUSÚ INFORMÁCIÓGYŰJTÉS A VÁLTOZÓ BIZTONSÁGI KIHÍVÁSOK TÜKRÉBEN

TECHNICAL INFORMATION GATHERING IN THE LIGHT OF CHANGING SECURITY CHALLENGES

DOBÁK Imre

(ORCID: 0000-0002-9632-2914)

dobak.imre@uni-nke.hu

Absztrakt

Az elmúlt években jelentős változások mentek végbe a tágan értelmezett európai biztonsági színtéren, amelyek közvetlenül hatottak a (nemzet)biztonsági gondolkodásra és az érintett szervek feladataira. Jelen tanulmány, a technikai vonatkozású titkos adatgyűjtés összetettségére, helyére, szerepére kíván rámutatni a változó biztonsági kihívások tükrében.
A mű a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosítószámú, „A jó kormányzást megalapozó közszolgálat-fejlesztés" elnevezésű kiemelt projekt keretében működtetett Zrínyi Miklós Habilitációs Program keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült.

Kulcsszavak: *titkos információgyűjtés, kommunikáció, nemzetbiztonság*

Abstract

In recent years, major changes have taken place in the European security arena that has had a direct impact on (national) security thinking and on the tasks of the national security services. The study intends to highlight the complexity, the place and the role of the technical type secret information gathering in the light of the changing security challenges.
The work was created in commission of the National University of Public Service under the priority project KÖFOP-2.1.2-VEKOP-15-2016-00001 titled „Public Service Development Establishing Good Governance" in the Miklós Zrínyi Habilitation Program.

Keywords: *secret information collection, communication, national security*

A kézirat benyújtásának dátuma (Date of the submission): 2017.05.07.
A kézirat elfogadásának dátuma (Date of the acceptance): 2017.05.21.

BEVEZETÉS

Az elmúlt években jelentős változások mentek végbe a tágan értelmezett európai biztonsági színtéren[1], amelyek közvetlenül hatottak a (nemzet)biztonsági gondolkodásra és az érintett szervek feladataira. Ezen változások talán a legjelentősebbeknek tekinthetőek a hidegháború befejezése óta, amely a nemzetbiztonsági, illetve titkos információgyűjtési képességekkel rendelkező biztonsági struktúrák szerepének felértékelődését eredményezték. Ennek hátterében több olyan markáns tényező is megfigyelhető, amelyekre az érintett országok rendszereik, jogszabályaik, illetve képességeik módosításával igyekeztek válaszolni.

Az egyik hatás a biztonságpolitikai veszélyek és kihívások, különösen a terrorizmus kapcsán figyelhető meg, amelyek mentén hirtelen *felerősödtek a hírszerzési, információgyűjtési igények*, valamint felértékelődtek a biztonsághoz kapcsolódó információk. A másik ilyen tényező a fejlődő technológiai környezet nyújtotta egyre *újabb információgyűjtő képességek megjelenésének és felhasználhatóságának határai* mentén kereshető, ahol a nemzetközi színtérre kitekintve a kibertér, a tömeges adatgyűjtés, az ún. metaadatok kérdésköreit, valamint az ezzel párhuzamosan jelenlévő társadalmi vitákat láthatjuk.

Jelen tanulmány, az elmúlt években a terrorizmus elleni küzdelem légkörében nemzetközi szinten felszínre került, technikai vonatkozású adatgyűjtés témakörét vizsgálva kíván rámutatni annak összetettségére, helyére, szerepére. Kérdésként jelenik meg, hogy a biztonsági környezet változása hogyan befolyásolta a titkos információgyűjtés „technikai vonatkozású" elemeit?

A téma vizsgálata szakirodalmi-, és egyéb relevanciával bíró hazai és nemzetközi publikus forrásokra támaszkodik, ahol főként az információgyűjtés jogi megközelítésével, valamint az egyre inkább meghatározó kibertér vizsgálatának kérdéseivel találkozhatunk. Nemzetközi kitekintéssel az 1980-1990-es évektől felerősödött „Surveillance (megfigyelés) Studies" mentén folytatott kutatások eredményeit láthatjuk [1; 179-194.o.], amelyek jól jelzik a kérdéskör a multidiszciplináris jelleget, hiszen részkérdései számos tudományterületet érintenek (többek között a műszaki-, a természet-, a társadalom-, vagy akár a bölcsészettudományok különböző területeit). A technikai típusú információgyűjtési tevékenységek[2] nagyságára, nincsenek átfogó, nemzetközi kutatási alapadatokat biztosító hivatalos statisztikák sem, és főként a nyilvánosságot kapott kérdéskörökre, a jogszabályok-, valamint a technológiai és a biztonsági környezet változásaihoz kapcsolódó információkra szorítkozhatunk. A tudományos források mellett jelentősnek tekinthető, hogy évek óta nemcsak a politikai és szakmai színtéren, de a médiákban is rendszeresen teret kapnak a technikai típusú információgyűjtési kérdések. Erre az amerikai titkosszolgálati megfigyelési botrány (2013) és hatásai, valamint az elmúlt időszak európai terrorcselekményei világítottak rá a legjobban, felvetve többek között

- a globális infokommunikációs szolgáltatók határokon átnyúló szerepét;

[1] Gondolok itt többek között az "arab tavasz" hatásaira, az Iszlám Állam megjelenésére, a bekövetkezett európai terrorcselekményekre, a 2015-ben kibontakozó tömeges migrációs hullámra, de ide sorolható a rendkívül összetett szíriai, vagy akár ukrajnai konfliktus is.

[2] Jelen tanulmány a technikai információgyűjtés kategóriájára a tágan értelmezett kommunikáció-ellenőrzéshez kapcsolódó információgyűjtés, illetve törvényes ellenőrzés oldaláról tekint, tudva azt, hogy a fogalom rendkívül széles módon értelmezhető. A titkosszolgálatokkal foglalkozó nemzetközi szakirodalmakban az "Intelligence" (hírszerzés) és az "Intel" tevékenységekhez sorolható technikai információgyűjtési ágakat láthatjuk, a vonatkozó jogszabályi megközelítések pedig az egyén magánszférájába beavatkozó titkos információgyűjtés kategóriája alatt tárgyalják.

- az állam oldaláról felmerülő technikai ellenőrzési lehetőségek jogszabályi kereteit;
- a biztonságpolitika és a diplomácia kérdéseit;
- az egyének magánszférájának sérülékenységét;
- a kibertér[3] jelentőségét.

TÖRTÉNETI ELŐZMÉNYEK

A humán, emberi tulajdonságokon és viselkedésen alapuló hírszerzés, információgyűjtés összetevői a történelemben visszatekintve nem új keletűek, mindez a technikai vonatkozású területekről azonban csak részben mondható el. Ezek fejlődése, *a titkos tevékenységek és szervezetrendszerek zártsága ellenére nem választható el a külső technológiai és társadalmi környezettől.* Kialakulásuknál a nem állami szférában is láthatunk történelmi előzményeket [12], annak különböző területei azonban alapvetően *az állam „biztonságért" felelős szervezeteinek tevékenysége mentén váltak meghatározóvá.* Az egyedi megoldások, és az azokon túllépő, rendszerszintű, állami információgyűjtési (felderítési) képességek különösen a világháborúk időszakában, mint kiemelt hírszerzési képességek indultak fejlődésnek. A kezdeti információgyűjtési formák mögött, az információkat megszerezni, meghallgatni, felhasználni vagy éppen biztonsági érdekekből cenzúrázni kívánók mellett már ekkor jelen voltak azon nagyobb távközlési/hírközlési szereplők, amelyek nemzeti és nemzetközi képességei értelemszerűen hatást gyakorolhattak pl. a cenzúra képességeire is.[4]

Konkrét előzményeket a technikai környezet 19. század végétől felgyorsuló fejlődésében kereshetünk, amikor is vezetékes távíró, majd a telefonok és telefonközpontok megjelenésével, vagy akár az első világháború időszakában a rádiózás kiteljesedésével párhuzamosan kialakult az információk megszerzésének, illetve ellenőrzésének lehetősége [6; 216.o.]. A korszak diplomáciai, politikai, katonai, bűnügyi feladatainak irányából jelentkező igények kiszolgálása *a szervezetszerű megoldások irányába mutattak*, formálva az ezt végző különböző állami szervezetek struktúráját is.

A második világháború, amely rámutatott az új technológiák transzformatív erejére [5; 299.o.], majd az azt követő hidegháborús légkör – külső kényszerítő hatásként – tagadhatatlanul felgyorsította a katonai eszközrendszerek mellett a technikai hírszerzési, felderítési, titkos információgyűjtési területek megerősödését is. Példaként a hidegháború időszakának, a másik félről titkos módon, földrajzi határoktól függetlenül információkat gyűjteni kívánó titkosszolgálati együttműködései szolgálnak. A szembenálló felek nemzetközi technikai, ún. SIGINT[5] (rádióelektronikai felderítési) képességeinek kialakítása mind a korszak sajátosságai voltak.[6]

---

[3] Magyarország Nemzeti Kiberbiztonsági Stratégiájában [3] megfogalmazottak szerint *„A kibertér globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét jelenti."* Az információgyűjtés témaköre miatt érdemes A. Rolington hírszerzéssel foglalkozó munkában megjelent megfogalmazást is megemlíteni, amely szerint a kibertér *„az internetet, a közösségi hálózatokat, az adatgyűjtő programokat, a szoftveroperációkat és a felhő alapú szolgáltatásokat tartalmazza".* [2; 22.o.]

[4] A British Eastern Telegraph Company például világszinten meghatározó volt 19. század végén, amely lehetőséget teremtett a brit érdekek érvényesítésére is. [4; 197.o.]

[5] Signal Intelligence - *„A SIGINT kommunikációs felderítésre (Communication Intelligence – COMINT), vagy más néven rádiófelderítésre, amely a szembenálló fél kommunikációs rendszereinek lehallgatásával szerez információt; illetve elektronikai felderítésre (Electronic Intelligence – ELINT), vagy más néven rádiótechnikai felderítésre osztható, amely a kisugárzott elektromágneses jelek elemzéséből szolgáltat adatot*." [19; 96.o.]

[6] Ezek között jelentek meg a különböző nemzetközi technikai, szakmai kapcsolatok, továbbá a vezetékes és vezeték nélküli, titkosított, illetve nem titkosított kommunikáció felderítése, lehallgatása, a rejtjelzett

Amíg a hidegháború titkosszolgálati technikai megoldásai a nemzeti és az adott szövetségi szintű biztonsági érdeket támogatva, a nyilvánosság elől elzártan, a társadalom számára nem látható szabályozás mentén töltötték be szerepüket, addig a század vége ebben is változást hozott. A titkosszolgálatok *nyilvános szabályozásával párhuzamosan a (technikai) információgyűjtési módszerek bizonyos mértékig láthatóvá váltak,* és a kommunikáció-ellenőrzés, információgyűjtés szigorú jogszabályi keretek közé került. Jelentősége és indokoltsága a társadalom számára is elfogadottá vált, különösen az egyének biztonságát közvetlenül veszélyeztető tevékenységek (pl. bűncselekmények elkövetése, terrorizmus), valamint az adott ország érdekeit támogató nemzetbiztonsági tevékenységek (pl. hírszerzés, kémelhárítás) kapcsán. Ebben az időszakban váltak hangsúlyossá a magánszféra titkos információgyűjtéssel/megfigyeléssel szembeni védelmének kérdései is.

Napjainkra már általánosan megállapítható, hogy a demokratikus országokban a nemzetbiztonsági szolgálatok működését külső kontrollmechanizmusok felügyelik, valamint a technikai jellegű titkos információgyűjtés – nemcsak nemzetbiztonsági célokat szolgáló – kereteit nyílt jogszabályokban rendezték. A modern távközlési rendszereket érintő jogszerű, törvényesen engedélyezett lehallgatás kerete az EU Tanácsának [10] kapcsolódó állásfoglalásával az európai színtéren is már több mint 20 éve jelen van, kinyilvánítva, hogy a távközlési kommunikáció bizonyos körülmények közötti, jogilag szabályozott módon történő lehallgatása – különösen a nemzetbiztonság és súlyos bűncselekmények esetén – a nemzeti érdekek védelmének fontos eszköze.

A titkos információgyűjtés nyilvános jogi szabályozása mellett ma már egyes információgyűjtési feladatok technikai megvalósítására is nemzetközi szintű megoldások, akár szabványok [7][8] állnak rendelkezésre. A fejlődés azonban rendkívül dinamikus, így napjainkban a hagyományos hírközlés-ellenőrzésen túlmutatva az internet-technológiára épülő szolgáltatások jelentik a legnagyobb kihívást, ahol „*a törvényes ellenőrzést végző szervek több - jogi és technikai - problémával is szembesülnek*" [9; 137.o.]. A fejlődésre reagálva az ITU (Nemzetközi Távközlési Unió)[7] és az ETSI (Európai Távközlési Szabványügyi Intézet)[8] jelenleg is dolgozik a felhő alapú rendszerek törvényes ellenőrzésének szabványosításán. [9; 147.o.] (Az ETSI dokumentumai a távközlés jogszerű lehallgatása terén biztosítanak egységes értelmezést az együttműködésben érintett hálózatüzemeltetők, szolgáltatók, valamint a bűnüldöző, vagy akár nemzetbiztonsági szervek között.)

AZ INFORMÁCIÓGYŰJTÉS TECHNIKAI ASPEKTUSAI

Az elmúlt közel száz évet meghatározó „hagyományos kommunikációs" rendszerekhez köthető ellenőrzési igényeken túllépve, a 20. század végére a kibertérhez kapcsolódó információgyűjtési igények váltak meghatározóvá. Napjainkra mindez már potenciális információgyűjtési közegként van jelen, így az ellenőrzésben érintett szervek struktúrái is folyamatos változásokon mennek keresztül. Publikus forrásokból látható, hogy a *„kibertér, mint új konfliktusterület"* [5; 308.o.] kapcsán számos ország alakította ki, vagy éppen formálja azon képességeit, amely a kibertérben jelenlévő információk gazdasági-, politikai-, katonai hírszerzési, vagy éppen terrorelhárítási célból történő megszerzésére irányulnak. A titkos

közlemények megfejtésének feladatai. Említésre érdemesek a nyugati SIGINT együttműködések, az 1940-es évek közepétől meghatározó BRUSA, majd UKUSA együttműködés, amely a 20. század második felére megalapozta az Echelon, illetve az ún. Five Eyes együttműködést, de itt érdemes megemlíteni pl. a keleti blokk együttműködéseit is.

[7] International Telecommunication Union

[8] European Telecommunications Standards Institute

információgyűjtés, a gyakran vitatott tömeges adatgyűjtések lehetősége, valamint az ún. metaadatok kérdésköre mentén kapott szélesebb publicitást és jelenik meg a nemzetközi szakirodalmakban. Igazi választóvonalat a 2013-ban kirobbant amerikai, tömeges megfigyelési botrány jelentett [11; 129-130.o.], így korunk viszonyait már a „Snowden utáni korszak" részeként tárgyalják.

Az *„internet-technológiára épülő szolgáltatások […] törvényes ellenőrzése* (jelenleg azonban) *minden ország nemzetbiztonsági és rendvédelmi szervét kihívások elé állítja."*[9] Ezen szolgáltatások törvényes ellenőrzése kapcsán, a témakörrel foglalkozó tudományos értekezés [9; p.148] négyféle ellenőrzési modellt kategorizál, amely nemzetközi értelmezésben is jól jelzi az információgyűjtésben, ellenőrzésben érintett szervek képességeinek lehetséges fejlődési irányait. Ezen módszerek között jelennek meg:

- az ún. aktív ellenőrző eszköz alkalmazása (más néven „online házkutatás")[9];
- a közbeékelődéses ellenőrzés végrehajtása[10];
- az ún. „mély csomagvizsgálat" módszere[11];
- valamint a kommunikációs szolgáltatóval való együttműködés lehetősége.

A hagyományos hírközlés-, vagy akár internet-technológiára épülő szolgáltatások törvényes ellenőrzési feladatainál *alapvetően a szolgáltatói együttműködések tekinthetőek meghatározónak*, utalva a már említett szabványokra, eljárásrendekre, amelyek biztosíthatják az állam és szolgáltatói szektor közötti szükséges és elégséges mértékű együttműködési felületet. Érdemes hangsúlyozni azonban, hogy a jelzett modelleken túl rendszeresen kerülnek nyilvánosságra új és újabb, a kiberteret érintő hírszerzési lehetőségeket felvillantó kiszivárogtatások[12], amelyek jól mutatják, hogy *a technológiai fejlődéssel az ismertetett kategóriák egyáltalán nem tekinthetőek lezártnak*.

Az egyedi típusú ellenőrzési megoldások mellett a tömeges típusú ellenőrzésre lehetőséget teremtő formák *a nemzetbiztonsági és terrorelhárítási célú információgyűjtés mentén váltak meghatározóvá*, amelyeket a szakirodalmak az ún. upstream és downstream módszer megnevezés alatt tárgyalnak. Ezek lényegében a már ismertetett felosztás [9; pp. 169-170] alapján a szolgáltatóval való együttműködés lehetőségeként, valamint az ún. „csomagvizsgálati" megoldásként értelmezhetők, amelyek előnyei a passzív, kommunikációt nem befolyásoló ellenőrzési sajátosságaikban, a tömeges információgyűjtés lehetőségében, valamint az érintett szervek oldaláról történő távoli, biztonságos alkalmazásukban mutatkozhatnak meg.[13]

[9] Lényegében egyedi megoldásként a célszemélyek számítógépeire juttatott kémprogram / ellenőrző szoftver alkalmazását takarja.

[10] A kommunikációs csatornába beállva és a másik félnek adva ki magát, a kommunikáció lényegében áthalad az ellenőrzést végző eszközén.

[11] Az egyes adatcsomagok tartalmi vizsgálata, és ennek során az ellenőrzéssel érintett csomagok kiválasztása.

[12] A Wikileaks folyamatosan teszi közzé az amerikai CIA (Külföldi Hírszerző Ügynökség) hírszerzési megoldásait tárgyaló dokumentumokat, így 2017-ben többek között az okostévék mikrofonján keresztül történő lehallgatásról, kémprogramokról szóló hírek jelentek meg. [23] (Megj.: A CIA feladata a külföldön történő hírszerzési tevékenység, amely során az FBI-hoz, valamint az NSA-hoz hasonlóan alkalmaz technikai információgyűjtő megoldásokat és eszközöket.)

[13] Lásd az internet-technológiára épülő szolgáltatások törvényes ellenőrzésére jelenleg rendelkezésre álló módszerek előnyeit, és hátrányait összefoglaló táblázatot [9, pp. 169-170]

Tömeges adatgyűjtés, metaadatok, titkosítás

Az elmúlt években a technikai információgyűjtés problematikáját leginkább az alcímben szereplő három kifejezés jellemezte, amelyek egyben jól mutatják a biztonságért dolgozó (nemzet)biztonsági szféra, a társadalom civil szereplői, és a profitorientált vállalati környezet találkozásánál felmerülő kritikus pontokat. A témakört vizsgáló tanulmányok is többek között az adatgyűjtések tömeges jellegét, a belföldi-külföldi információgyűjtés problémáját, a nemzetbiztonsági-bűnügyi információgyűjtés összetett jellegét, valamint az információgyűjtéssel szembeni társadalmi érzékenys*ég* kérdéseit vetik fel.

A *tömeges adatgyűjtés* kapcsán, az amerikai gyakorlatot vizsgáló 2014-ben készült PCLOB jelentés [13] részletesen ismerteti a külföldi hírszerzési célú technikai információgyűjtés két fő típusát („downstream" és "upstream" adatgyűjtés). A dokumentum alapján a „downstream" megoldás az egyes szolgáltatók (pl. internetszolgáltató vagy más hírközlési szolgáltatók) bevonására és a rendszerükben megjelenő adatokra összpontosít. A folyamatban az érintett kormányzat küldi meg a szükséges azonosítót (pl. e-mail cím) az elektronikus kommunikációs szolgáltatónak és ezt követően egyfajta szolgáltatói közreműködéssel történhet az információgyűjtés.[14] Az "upstream" megoldás pedig a nemzetközi szinten jelentősebb gerinchálózati csomópontokon, létesítményeken átmenő kommunikáció ellenőrzésére irányul, amely már felöleli a telefon és az internetkommunikáció ellenőrzését is.[15] A jelzett forrás az NSA[16] downstream és upstream megoldásainak arányát tekintve megjegyzi, hogy *„mintegy 90 százaléka az NSA tevékenységének downstream, és kevesebb, mint 10 százaléka tekinthető upstream megoldásnak"*. [14; 16.o.][13; 33.o.]

Az upstream megoldás vitatott kérdései egyfelől az adatok tömeges rögzítéséből, másfelől abból adódhat, hogy a tömeges adathalmazból (metaadat és tartalom) csak valamilyen szűréssel, vagy más eljárással lehet kiválasztani az érdeklődésre számot tartó kommunikációt. Az upstream kérdése így igazából már *a korszak egyfajta korlátjaként jelentkezik,* hiszen (a tömeges adatgyűjtés vitatott kérdésén túl) felmerül, hogy létezik-e olyan technológiai megoldás, amely „csak" a célzott adatok kiválasztását biztosítja. Mint Kris 2016-os írásában [14; 17.o.] kifejti az NSA nem tudja elkerülni, hogy egyéb kommunikációkat is megszerezzen, azaz szűrő kutató felderítést folytasson.

A *metaadatok* az egyes szolgáltatások, kommunikációs csatornák felhasználása során, nem közlemény (pl. beszéd) típusú adatként jelennek meg. Fajtái az elektronikus hírközlési megoldásokhoz kapcsolódóan sokfélék lehetnek, így ide sorolhatóak például a technikai, a forgalmazási és előfizetői adatok (helyszín, hálózat, szolgáltató stb.) [15; 54.o.]. Jelentős részük kapcsolódik az eszközök mobilitásához (pl. mobiltelefon, mobilinternet), és magához a szolgáltatásokhoz, így főként az érintett kommunikációs szolgáltatók rendszereiben állnak rendelkezésre. A kérdést itt is az adatok *tömeges gyűjtése, tárolása és „feldolgozhatósága*" vetette fel, hiszen elemzés és értékelés nélkül ezen adatok alapvetően csak adathalmaznak tekinthetőek, amelyek *gyűjtésére és monitorozására a technológiai fejlődés teremtette meg a*

[14] A 2014-es dokumentum [13] alapján az Egyesült Államokban az NSA minden „downstream" által gyűjtött adatot megkap, a CIA és az FBI pedig egy részét. Az "upstream" adatgyűjtésből származó adatokat az amerikai gyakorlatban kizárólag az NSA kapja meg, sem a CIA-nak, sem az FBI-nak nincs hozzáférése.

[15] Ebben az esetben is vannak azonban együttműködő felek, csak például nem internetszolgáltató, hanem azon adott infrastruktúra szolgáltatója, amelyen a kommunikáció tranzit jelleggel keresztülhalad, A folyamatot részletesen leíró dokumentum alapján, ebben az esetben az információgyűjtés nem a „helyi" pl. telefonszolgáltatónál jelenik meg, amely akár olyan „külföldi" érdekeltségű szolgáltató is lehet, amely felé a kormányzat nehezebben érvényesítheti igényét. Lásd: [13; 35.o.].

[16] National Security Agency - Nemzetbiztonsági Ügynökség, Az Egyesült Államok kommunikációs hírszerzéssel foglalkozó szervezete.

lehetőséget. Elemezve és értékelve ezen adatok köre az egyén jogainak bizonyos mértékű sérülését is okozhatják, hiszen részletes információkat is kaphat annak elemzője az érintett szokásairól, viselkedéséről. G. Moody veti fel írásában [16], hogy a metaadatok tárolása bizonyos esetekben még jelentősebb, mint magának a kommunikációnak a tárolása, hiszen a metaadatok elemzése – mint számítógéppel olvasható adatok feldolgozása – könnyebb lehet, mint egy strukturálatlan tartalmú közleményé. Más forrás ezzel szemben azt hangsúlyozza, hogy jelenleg nem ismertek olyan technikai eljárások, amelyek kiválthatnák a tömeges (meta)adatok jelentőségét, bár a magánszféra védelmének növelése érdekében dolgoznak annak célzottabbá tételén.[17] A jogvédőkkel szemben jelen vannak azon érvek is, amelyek a terrorizmus elleni hatékonyabb fellépés miatt pártolják az adatgyűjtések szélesebb körű engedélyezését[17], valamint gondoljunk arra, hogy a vállalati / szolgáltatói szféra oldalán az állami szereplőknél akár jelentősebb mennyiségű adathalmaz keletkezhet, amelyek célzott állami felhasználása segítheti a biztonság növelését. Az elmúlt évek európai terrorcselekményei is arra világítottak rá, hogy a metaadatok körébe sorolható adatok mind a nemzetbiztonsági,[18] mind a bűnüldöző hatóságokat hatékonyan támogathatják feladataik végrehajtásában. A 2016-ban európai színtéren megjelent terrorellenes törvénycsomagokban már fontos elemként jelentek meg a biztonsági szféra képességeinek növelését szolgáló internetes metaadatok elérésének és felhasználásának lehetőségei. [29][34]

Éles viták formálódtak az infokommunikáció során szabadon alkalmazható titkosítások kérdésében is, amelyek nem állami szereplők körében történő alkalmazása – a világháborúk, majd a hidegháborúk időszakának állami / katonai titkosított kommunikációitól elvonatkoztatva – a század utolsó negyedére[19], a technológiai fejlődéssel és a szabadon hozzáférhető fejlesztői és felhasználói környezettel párhuzamosan erősödött fel. A 21. század elejére a törvényes ellenőrzési, valamint információgyűjtési feladatokat ellátó állami szervek már növekvő szintű és változatos titkosítást alkalmazó technikai környezettel szembesültek, ahol a piaci, hírközlési, szolgáltatói szereplők egyre inkább vonakodtak a kormányzatok titkos információgyűjtést érintő kéréseinek támogatásában. Globális szolgáltatók sorra jelentették be titkosítások alkalmazását, amelyet például az Egyesült Államok bűnüldöző szerve (FBI) már 2014-ben aggasztónak talált[20], félve attól, hogy a megnövekedő szintű titkosítás eredményeként képtelen lesz hozzáférni a nyomozásaihoz szükséges adatokhoz. (A szakirodalmak példaként általánosan az FBI-Apple közötti vitát említik, amikor is az FBI

[17] Így például a 2015-ös San Bernardino-i terrorcselekmény miatt bírálták a metaadatok gyűjtésének 2015-ös Freedom Act-beli korlátozását [18]

[18] Az Egyesült Királyságban például a nemzetbiztonsági szféra esetében is jelen van a „tömeges adatok" (bulk data) felhasználása, amelyek felölelik mind a tömeges személyi vonatkozású adatállományokat (ún. bulk personal data - BPD), mind a tömeges kommunikációs (meta)adatokat (nem közlemény típusú). Mint az MI5 honlapján megjelenik a tömeges kommunikációs adatok használata a szervezet számára alapvető fontosságú nyomozati eszköz, amely szerepet kapott minden nagyobb terrorizmusellenes műveletben az elmúlt évtizedben. Jelentősége a 2001-es amerikai, majd a 2005-ben történt londoni terrorcselekmények után nőt meg. forrás: https://www.mi5.gov.uk/bulk-data

[19] A határokon átnyúló titkosított elektronikus kommunikáció már a 19. század végén megfigyelhető volt, amely elsődlegesen az államok üzenetváltásainak titkosságát szolgálta (pl. diplomáciai üzenetek, vagy akár a gyarmatok irányába megjelenő táviratok), majd a gazdasági szereplők kommunikációja mentén is terjedni kezdtek a sajátos információvédelmet jelentő megoldások. Az egyre „szabadabban" terjedő titkosítás már akkor sértette az állam sajátos érdekérvényesítési igényét, így korlátozására, tiltására már a 20. század első felében találhatunk példákat.

[20] Példaként az Apple és a Google említhető, amelyek már 2014 végén bejelentették, hogy fokozott biztonsági megoldásokat, automatikus titkosítást vezetnek be a termékeiknél a magánélet védelmére és az adatok biztonsága miatt.

bírósághoz fordult egy bűncselekménnyel kapcsolatba hozható mobiltelefon titkosított adatainak nyílt hozzáférése érdekében.)

Az Egyesült Államokban már korábban megjelent azon társadalmi-szakmai vita, miszerint az államnak van-e joga arra, hogy "kivételes hozzáférést" kapjon a titkosított kommunikációhoz és adatokhoz azért, hogy végrehajtsa feladatát [14; 26.o.]. Európában a figyelem azonban csak a párizsi terrorcselekményeket (2015) követően irányult a kérdésre, felvetve, hogy a titkosított kommunikáció különösen alkalmas lehet a terroristák közötti információk hatóságok előli elrejtésére.[21]

Tényként kezelhető, hogy a titkosítások fejlődésével egyre nagyobb nyomás nehezedik az érintett állami szervekre, és amíg a fejlett titkosszolgálatok hírszerzési igényeik mentén sajátos információgyűjtési megoldásokat fejlesztettek ki (az ismertetett upstream és downstream megoldások), addig a bűncselekmények felderítéséhez kapcsolódó lehetőségek gyakran a nemzeti határokon kívüli szolgáltatóktól való adatok beszerzésének bizonytalan kikényszerítése felé mutattak. A szolgáltatók számára a (nemzet)biztonsági együttműködések és kérések kiszolgálása a piaci pozícióvesztés félelmét vethetik fel[22], mondván, hogy a felhasználók nem fogják használni az adott technológiát, ha nem bíznak annak biztonságosságában (technológia bizalmi deficit [14; 6.o.],[30]).

TERRORIZMUS ELLENI KÜZDELEM, TECHNIKAI INFORMÁCIÓGYŰJTÉS, A KÉRDÉSKÖR ÖSSZETETTSÉGE

Az utóbbi húsz évben a nyugati fejlett országok területén elkövetett terrorcselekményekkel párhuzamosan tanúi lehettünk a technológia környezet megállíthatatlan fejlődésének, robbant ki az amerikai adatgyűjtési botrány, és kerültek nyilvánosságra a titkosszolgálatok működését is érintő WikiLeaks dokumentumok. Együttes hatásaik felerősítették a technikai információgyűjtés körüli nyilvános és szakmai vitákat, amelyek közvetve befolyásolták – különösen a terrorizmus légkörében – a biztonság növelésére tett állami lépéseket.

Napjainkban a legtöbb európai ország törekszik arra, hogy az információgyűjtés során *elkülönítse a bűnügyi célt és a titkosszolgálati célt* [20; 139.o.], amely az alapjogokba beavatkozó eszközök és módszerek kapcsán kihat ezen tevékenységek engedélyezési megoldásaira is. Amíg az előzőnél bírói engedélyhez kötöttséggel, addig a titkosszolgálati (nemzetbiztonsági) szervezeteknél és célnál már ettől eltérő engedélyezési formákkal is találkozhatunk. A titkos információgyűjtés céljai között pedig nemzetbiztonsági, terrorelhárítási, rendészeti és bűnüldözési célokat láthatunk [21; 8.o.], ahol a nemzetbiztonsági célnál jelenik meg a külföldi irányultságú (technikai) információgyűjtés, a terrorelhárítási cél pedig, a terrorizmus elleni küzdelem komplexitása (rendőri, katonai, titkosszolgálati elemek, határon belüli és kívüli információk jelentősége) miatt formálja kiemelten a titkos információgyűjtés kérdéseit. Mint Finszter 2016-os tanulmányában megfogalmazza *„a terrorelhárítási célú felderítés egyik formája beilleszthető a bűnüldözési célú titkos információgyűjtés körébe, a másik lehetséges forma viszont a nemzetbiztonsági*

[21] A titkosított kommunikációs megoldások alkalmazását – az áttekintett források szerint – a 2015-ös párizsi események nyomozásának későbbi adatai nem támasztották alá (az elkövetők eldobható telefonokat használtak és nyílt SMS kommunikációt folytattak).

[22] A viták főként a nagyobb szolgáltatók (pl. Google) esetei kapcsán kerültek nyilvánosságra, amelyek mögött az adott „vásárlói bizalmat” megtartani szándékozó szolgáltatók és a biztonsági szervek együttműködési mélységének kérdésköre áll, ahol az állami információs igénnyel szemben, egyes nagyvállalatok globális jelentőségüknél, a társadalom mindennapi életére gyakorolt hatásuknál fogva egyre gyakrabban fejezik ki ellenvetésüket.

célú felderítés jegyeit ölti magára" [21; 21.o.]. Sajátossága abból is adódik, hogy a terrorcselekmények megelőzése érdekében a felderítést és elhárítást szolgáló információgyűjtés az összbiztonsági struktúra számos elemére feladatrendszert ró. Az információgyűjtés jelentőségére utal A. Rollington megfogalmazása, miszerint egy *„tragédia után azonnal a megelőzés elmaradását vizsgálják, hogy megállapítsák: a hírszerzés miért nem jelezte előre a tragédia esetleges bekövetkezését."* [2; 164.o.]

A terrorizmus elleni küzdelem során a technikai jellegű információgyűjtésben alapvetően azon kommunikációs csatornák és formák ellenőrzése lehet meghatározó, amelyet a társadalom békés tagjai között meghúzódó terroristák is használhatnak (így pl. a mobiltelefonok, valamint az internet-alapú szolgáltatások). A terrorizmus sajátosságai miatt változnak a SIGINT-ként kategorizált olyan „hagyományos" információgyűjtési megoldások[23] is, amelyek a hidegháborús szembenállásra még jellemzőek voltak, hiszen – mint Mark M. Löwenthal megfogalmazza – a *„SIGINT-et úgy fejlesztették ki, hogy a Szovjetuniót és más országokat érintő információgyűjtésre legyen alkalmas"* [22; 158.o.]. Az információgyűjtés problematikája itt éppen abban rejlik, hogy a terroristák által használt kommunikációs csatornák tisztán nem különíthetőek el a társadalom békés tagjai által használt platformoktól.

Nemzetközi kitekintéssel, az elmúlt időszakban mind az Egyesült Államok, mind több európai ország módosította a titkos információgyűjtést tárgyaló jogszabályi kereteit, elősegítve ezzel, hogy (nemzet)biztonsági szerveik hatékonyabban férhessenek hozzá a terrorfenyegetettséggel kapcsolatos információkhoz.

Az Egyesült Államok esetében – ahol a külföldi célú információgyűjtő tevékenységet a FISA[24] törvény (1978) alapján lehetett végrehajtani – a folyamat 2001-ig[25] tekint vissza, amikor is az elnök engedélyezte az NSA számára, hogy elnöki engedéllyel ellenőrizzenek olyan, az országba befelé és kifelé irányuló olyan kommunikációkat, ahol az egyik fél a terrorizmussal kapcsolatba hozható. [14; 3.o.]. A felhatalmazás érintette a tömeges, kommunikációs tartalommal (közleménnyel) nem rendelkező információk (metaadatok) gyűjtését is. Az elnöki engedély alapján végzett lehetőség (kommunikációs tartalmak és metaadatok tömeges gyűjtése) együttesen a Terrorist Surveillance Program (TSP) néven vált ismerté. 2005-ben jogi vita kezdődött a kérdéses információgyűjtési megoldások bírói, vagy bírósági engedélyhez kötöttségének hiányáról, majd magát a FISA módosításáról szóló törvényt (FISA Amendments Act) jelentős vita után 2008 júliusában fogadta el a Kongresszus és írta alá az elnök. A törvény *„lehetővé teszi az amerikai célpontokat érintő, egy hétig tartó, végzés nélküli, rendkívüli lehallgatást abban az esetben, ha erősen megalapozott annak feltételezése, hogy a célpont terrorizmushoz köthető. Hasonlóan egyhetes időszak vonatkozik a külföldi célpontokra."* [22; 161.o.] A külföldi hírszerzési célú megfigyelés azon személyekre irányulhat, akik nem amerikai állampolgárok, és akik az Egyesült Államok területén kívül vannak.[26] Továbbá az adatgyűjtésnek a FISA-ban meghatározott külföldi

[23] Pl. a rövidhullámú sávtartományban végzett rádiókommunikáció-ellenőrzés

[24] A Foreign Intelligence Surveillance Act-ot (FISA – külföldi hírszerzési megfigyelési törvény) 1978-ban léptették életbe az Egyesült Államokban az elektronikus külföldi hírszerzési célú megfigyelés szabályozására, a megfigyelések során kötelezővé téve a bírói engedélyt [22; 378.o.].

[25] 2001-ig ha a *„SIGINT-célpont az Egyesült Államokban tartózkodott, nyomon követése az FBI, nem pedig az NSA hatásköre volt"*, akiknek erre bírói engedélyt kellett beszereznie. [22; 160.o.]

[26] A FISA 702 szakasza lehetővé teszi az ún. azonosító („szelektor" pl. e-mail cím, telefonszám) alapján történő adatgyűjtést. Ha az adott azonosító amerikai személyé, vagy az Egyesült Államok területén található személyé, az azonosítót nem lehet a törvény 702 szakasza alapján ellenőrzésre kijelölni. (Az USA esetében fontos megjegyezni, hogy a hírszerzési cél során megjelenik az amerikai állampolgárok védelmének hangsúlyossága,

hírszerzési célú információ megszerzésére kell irányulnia, amelyhez a FISA Bíróság döntése szükséges.

A 2013-ban nyilvánosságra került adatgyűjtési gyakorlat kapcsán két program került a nemzetközi figyelem középpontjába. Az egyik program alapján[27] az NSA belföldi telefon metaadatokat gyűjtött tömegesen, a másik programban[28] az amerikai kormányzat külföldi elektronikus, internetes kommunikációs tartalmakat gyűjtőtt, ahol azok érintettjei az Egyesült Államok területén kívül tartózkodó nem amerikai személyek voltak. [25] A megfigyelési programot vizsgáló 2014-es amerikai jelentésből [13] kitűnik, hogy a külföldi hírszerzési célú információgyűjtés kérdésköre rendkívül komplex, sok szervezetet érintett, és a gyűjtött információk típusa, célja is sokrétű volt. Átfogóan már az anyag bevezetőjében megfogalmazzák azonban, hogy azok az információk, amelyeket a program gyűjt értékesek és hatékonyak a nemzet biztonságának szempontjából. Az amerikai és brit[29] gyakorlatot érintő botrány kirobbanását követően az EU is vizsgálta a tömeges megfigyelések kérdéskörét, felvetve többek között, hogy azok célzott, vagy tömeges adatgyűjtések, mi történik a hírszerző szolgálatok által összegyűjtött tömeges adatokkal [27; 39.o.], valamint kifejezte fenntartásait[30] a *tömeges típusú* csúcstechnológiájú adatgyűjtési megoldásokkal szemben.

A technikai típusú titkos információgyűjtés amerikai gyakorlatában az utóbbi években is történtek olyan változások, amelyek nemzetközi szinten nyilvánosságot kaptak. Ilyen változás volt például, hogy *„a szövetségi bírók engedélyt adjanak a bíró illetékességi területén kívül található számítógépek távolról történő kutatására."* [22; 139.o.]. A módosítás lehetővé teszi, hogy az FBI távoli (akár az USA területén kívüli) számítógépekbe is betekintést nyerhessen. [32]. Az új amerikai kormányzat részéről 2016-ban jelentek meg olyan elképzelések, hogy az Egyesült Királyság példáján ismét kiszélesítsék az információgyűjtés kereteit, annak érdekében, hogy hatékonyabban tudjanak fellépni a terrorizmussal szemben. A brit és orosz megoldásokhoz hasonlóan olyan javaslatok jelentek meg, hogy törvényben kötelezzék az internetes cégeket, infokommunikációs szolgáltatókat arra, hogy szükség esetén biztosítsanak hozzáférést a titkosított kommunikációhoz. Az amerikai titkosszolgálati képességekre vonatkozóan pedig a WikiLeaks szivárogtatott ki (újabb) anyagokat 2017-ben, amely dokumentumok a CIA[31] egyes technikai információgyűjtő képességeit (pl. okostévék mikrofonján keresztül történő lehallgatás) tárták a nyilvánosság elé.[32]

így elkülöníthető a „non-US" személyek külföldi kommunikációját érintő kérdéskör. - Non-U.S. person: olyan személy, aki nem amerikai állampolgár és jogszerűen nem állandó lakosa az Egyesült Államoknak.)

[27] A PATRIOT ACT 215 szakaszára való hivatkozással

[28] A Foreign Intelligence Surveillance Act "FISA" 702 szakaszára való hivatkozással

[29] Nagy-Britannia esetében a GCHQ szervezete volt érintett az adatgyűjtési botrányban. (GCHQ - Government Communications Headquarters, többek között SIGINT tevékenységet végző brit nemzetbiztonsági szolgálat. Összetett feladatrendszerével 1946 óta segíti a brit kormány és szövetségesei katonai, diplomáciai és bűnüldöző szerveinek tevékenységét.

[30] A témakörrel foglalkozó 2013-as EU tanulmány alapján a terrorizmus és a szervezett bűnözés elleni küzdelemben részt vevő legtöbb európai szolgálat a metaadatok széles körű gyűjtését használta, hogy megtalálja a gyanúsítottak tevékenységeinek kapcsolódási pontjait a nyomozások során. Ebben az esetben, még akkor is, ha nagy mennyiségű gyűjtés történik, az célzott megfigyelésként értelmezhető. Az NSA vizsgált adatgyűjtése azonban a különböző megfigyelési programokon keresztül ettől jelentősen eltért, hiszen akár az amerikai társaságok javára az európai vállalatokkal szembeni kémtevékenységekre is utalhatnak, valamint az európai állampolgárok adatai saját államuk tudta nélkül kerülhettek az NSA-hoz. [27; 39.o.]

[31] A Központi Hírszerző Ügynökség (CIA) feladata külföldön történő hírszerzési tevékenység, amely során az FBI-hoz, valamint az NSA-hoz hasonlóan alkalmaz technikai információgyűjtő megoldásokat és eszközöket.

[32] A WikiLeaks több mint nyolcezer titkosított dokumentumot közölt többek között a CIA technikai hírszerzési megoldásairól, eszközeiről, valamint szélesebb hozzáférést adott az érintett cégeknek, hogy elzárhassák ezen technikai információgyűjtési megoldások lehetőségét. [23]

Az Egyesült Királyságban már 2015 végén felmerült, hogy több jogkört kapjanak a titkosszolgálatok a terrorizmus elleni küzdelem érdekében.[24] Széles szakmai vita előzte meg [35] az ún. Investigatory Powers Act törvénytervezetét [34], amely többek között a telefon és internetszolgáltatókat célozta meg, megfogalmazva a böngészési előzmények és személyes üzenetek tárolásának kötelezettségét, hogy azokhoz kérés esetén az érintett szolgálatok hozzáférhessenek. Az ellenzők mindezt támadták annak rendkívül széles körű jogosítványai miatt. A kormányzat azonban kitartott elképzelései mellett (2016 végén elfogadták a törvényt), mondván a terrorizmus fenyegetése közepette kötelességük, hogy biztosítsák a hatáskörét azon szerveknek, akiknek a biztonság szavatolása a feladatuk.[28] *„A jogszabály alapjaiban változtatja meg az Egyesült Királyság kiber-megfigyelési, engedélyezési és adattárolási gyakorlatát. Az online adatgyűjtést eddig ugyanis egy kétlépcsős jóváhagyási folyamat előzte meg, melyben a belügyminiszteri mellett külön bírói engedély is szükségeltetett a titkos adatgyűjtés lefolytatásához. […] a törvény azonban kiveszi ezeket a fékeket a rendszerből, melynek eredményeképp a nyomozóhatóságok mindenféle korlátozás nélkül gyűjthetnek bizonyos online adatokat.”*[26]

Oroszország esetében is fordulópontot jelentett a 2016-os év az internet-technológiára épülő információgyűjtés terén, amelyet az orosz utasszállító ellen 2015 végén Egyiptomban elkövetett terrorcselekmény válthatott ki. Médiaforrások alapján, a 2016 közepén elfogadott terrorizmus elleni törvény (ún. Yarovaya Law) értelmében *„kötelezik az orosz telekommunikációs és internet szolgáltatókat, hogy fél évig tárolják a telefonbeszélgetéseket, a szöveges üzeneteket, a videókat és képeket, három évig pedig a telefonhívások metaadatait*. [29]. Felléptek a titkosított kommunikációkkal szemben is, így az érintett szolgáltatók ilyen alkalmazás esetén kötelesek segíteni az erre jogosult Szövetségi Biztonsági Szolgálatot (FSZB[33]) a titkosítások dekódolásában.

Németországban 2017. januárjától teszi lehetővé törvénymódosítás, hogy a Német Szövetségi Hírszerző Szolgálat (BND[34]) adatokat szerezhessen a belföldi és külföldi kommunikációs forgalomból, és azokat hat hónapig tárolhassa. [33] A kritikák az NSA adatgyűjtési lehetőségeihez hasonlítják a változást, amely jól jelzi a kibertérhez kapcsolódó információgyűjtő képességek növelésének szándékát.

KÖVETKEZTETÉSEK

Az ezredfordulót követően átalakuló biztonságpolitikai környezet és különösen a terrorizmus térnyerése nemzetközi kitekintéssel a biztonsági, nemzetbiztonsági szolgálatok tevékenységének és képességeinek újragondolását tették szükségessé. Amíg a globális hírszerzési képességeket kiépítő Egyesült Államokban mindez, már a 2001-ben bekövetkezett terrortámadással kezdetét vette, addig Európában az elmúlt évek terrorcselekményei adtak jelentős lendületet az információgyűjtési és elemzési képességek átértékelésének. 2013 után a terrorizmus erősödő jelensége kapcsán a vezető európai államok növelték technikai megfigyelési képességeiket [14; 11.o.], majd 2015-ben és 2016-ban további lépeseket tettek ezen az úton. [29][33][34] A változások a minél hatékonyabb (így az internet alapú szolgáltatások ellenőrizhetősége, és a metaadatok hatékony felhasználhatósága) irányába mutattak.

[33] Federalnaja Szluzsba Bezopasznosztyi Rosszijszkoj Federacii – Oroszország nemzetbiztonsági (belbiztonsági és kémelhárítással foglalkozó) szolgálata

[34] Bundesnachrichtendienst – Németország nemzetbiztonsági (szövetségi hírszerző) szolgálata

A 2013-ban kirobbant amerikai titkosszolgálati botrány rendkívül jól jelezte a fejlett országok titkos információgyűjtő technikai megoldásainak fölényét. Az eset rávilágított a kibertér jelentőségére, a (globális) szolgáltatók szerepére, valamint az állampolgárokat védő és a (nemzet)biztonsági érdekeket is biztosító, jogszabályi megoldások szükségességére. Az azóta eltelt időszak eseményei megerősítették azt is, hogy az életünk elválaszthatatlan részét képező kibertér, amellett, hogy számos illegális tevékenységnek, így a terrorizmusnak is teret adhat, globális szinten egyre inkább a hírszerzési célú információgyűjtés, és egyéb titkosszolgálati tevékenységek kiemelkedő platformja. Itt jelenik meg *„a technológiai fölény kérdése, amely a korszerű, határokon átnyúló, globális méretű információgyűjtési képesség mentén megjósolhatatlan előnyöket biztosíthat az ezekkel rendelkező országoknak”*.[31; 23.o]

A rendkívüli technikai fejlődés légkörében az új internet alapú szolgáltatásokat, alkalmazásokat kidolgozó szolgáltatói szféra és az ehhez kapcsolódó információgyűjtés igényével jelentkező nemzetbiztonsági, bűnügyi szervezetek „versenyfutása” „kényszerű egymásra utaltsága” a jövőben is folytatódni fog. Amíg az érintett szolgálatok fejlesztésekkel, együttműködésekkel, vagy éppen a szolgáltatókat kötelező törvényi előírásokkal kívánják hatékonyságukat, így közvetve a társadalom biztonságát növelni, addig a szolgáltatói szféra szereplői piaci érdekeik szem előtt tartásával, globális szereplőként gyakran vonakodva vesznek részt a folyamatban. A civil, piaci szereplők jelentősége azonban egyre vitathatatlanabb, így tanulmányok hívják fel a figyelmet arra, hogy az üzleti alapokon nyugvó „nem titkosszolgálati célú” technikai megoldások és fejlesztések számos területen tágítani fogják a biztonság szolgálatába állítható információforrások[35] körét.

A nyílt jogszabályi keretekkel működő, információgyűjtést végző (nemzet)biztonsági szervek oldaláról a jövőben is fontos a társadalom bizalma, valamint azon egyensúly megtartása, hogy a fejlődő infokommunikációs környezet közepette biztosítva legyen a törvénytisztelő állampolgárok jogainak védelme, ugyanakkor az érintett nemzetbiztonsági és bűnüldöző szervek számára rendelkezésre álljanak a feladataik ellátáshoz szükséges felderítési képességek.

FELHASZNÁLT IRODALOM

[1] MURAKAMI WOOD, D.: *The ‘surveillance society’, Questions of History, Place and Culture*, European Journal of Criminology, Volume 6(2), European Society of Criminology and SAGE Publications, DOI:10.1177/1477370808100545, 2009. p. 179-194.

[2] ROLINGTON A.: *Hírszerzés a 21. században, a mozaikmódszer*, Antall József Tudásközpont, 2014. ISBN 978-963-87486-3-8,

[3] *Magyarország Nemzeti Kiberbiztonsági Stratégiája (1139/2013. (III.21.) Korm. határozat 1. sz. mell.* http://www.kozlonyok.hu/nkonline/MKPDF/hiteles/MK13047.pdf (letöltve: 2017.05.06.)

[4] HILLS, J.: What’s new? War, censorship and global transmission, From the the Telegraph to the Internet, The International Communication Gazette, 2006 Sage

[35] *Ide sorolhatók például a civil fejlesztői környezet informatikai megoldásai, a kamerarendszerek, amelyek akár gyorsabb, értékesebb információkat biztosíthatnak a hagyományos „titkos” információgyűjtési képességeknél.*

publications, London, Thousand Oaks & New Delhi 1748-0485 VOL 68(3): 195–216 DOI: 10.1177/1748048506063761

[5] DANNREUTHER R.*: Nemzetközi Biztonság*, Antall József Tudásközpont, 2016, ISBN 978 615 5559 20 4. 395.o.

[6] KOVÁCS L.: *Az elektronikai hadviselés jelene és lehetséges jövője*, Hadmérnök 2017/1. szám, http://www.hadmernok.hu/171_17_kovacs.pdf (letöltve: 2017.04.26)

[7] *ETSI TS 101 331 V1.3.1 (2009-10) - Lawful Interception (LI); Requirements of Law Enforcement Agencies* http://www.etsi.org/deliver/etsi_ts/133100_133199/133106/09.00.00_60/ts_133106v090000p.pdf (letöltve: 2017.03.19.)

[8] *ETSI TS 133 106 V9.0.0 (2010-02) Universal Mobile Telecommunications System (UMTS); LTE; Lawful interception requirements* http://www.etsi.org/deliver/etsi_ts/101300_101399/101331/01.03.01_60/ts_101331v010301p.pdf (letöltve: 2017.03.19.)

[9] KOVÁCS Z.: *Az infokommunikációs rendszerek nemzetbiztonsági kihívásai*, PhD értekezés, NKE KMDI, Budapest 2015.

[10] *COUNCIL RESOLUTION, of 17 January 1995 on the lawful interception of telecommunications (96/C 329/01), Official Journal of the European Communities C 329, 4.11.1996. Volume 39, ISSN 0378-6986* http://eur-lex.europa.eu/legal-content/EN/TXT/ PDF/?uri=OJ:C:1996:329:FULL&from=EN (letöltve: 2017.03.19.)

[11] GREENWALD, G.: *A Snowden-ügy, Korunk legnagyobb nemzetbiztonsági botrány*a (magyar kiadás) HVG könyvek 2014, ISBN 978-963-304-183-3

[12] SEGRAVE, K.: *Wiretapping and Electronic Surveillance in America, 1862-1920*, McFarland, 2014, ISBN 1476617406, 232. https://books.google.hu/books?id=he5ZBAAAQBAJ&printsec=frontcover&hl=hu&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false (letöltve: 2017.02.05.)

[13] *Privacy and Civil Liberties Oversight Board: Report on the Surveillance Program Operated Pusuant to Section 702 of the FISA*, https://www.pclob.gov/library/702-report.pdf (letöltve: 2017.05.01.) July 2, 2014

[14] KRIS, D. S. (2016). *Trends and predictions in foreign intelligence surveillance: The FAA and beyond*. Journal of National Security Law & Policy, 8(3), 1-42. https://search.proquest.com/docview/1831706283?accountid=42933

[15] LOIDEAIN, N. Ni: *EU Law and Mass Internet Metadata Surveillance in the Post-Snowden Era*, Media and Communication (ISSN: 2183-2439) 2015, Volume 3, Issue 2, Pages 53-62 Doi: 10.17645/mac.v3i2.297

[16] MOODY, G.: *2/3/2016, Revised Snooper's Charter ignores key criticisms, widens police powers further*, http://arstechnica.co.uk/tech-policy/2016/03/revised-snoopers-charter-ignores-key-criticisms-widens-police-powers-further/ (letöltve: 2017.04.25.)

[17] *National Academies Report on Bulk Intelligence Collection, Schneier on Security,* https://www.schneier.com/blog/archives/2015/02/national_academ.html (letöltve: 2017.03.20.)

[18] GOLDMAN, A. – BERMAN, M. – ACHENBACH, J.: *FBI says San Bernardino attacks considered act of terrorism; shooter pledged allegiance to Islamic State leader*, The Washington Post, December 4, 2015, https://www.washingtonpost.com/news/post-

nation/wp/2015/12/04/san-bernardino-attackers-tried-to-cover-their-tracks-official-says/?utm_term=.b6bfb0d960a3 (letöltve: 2017.04.20.)

[19] HAIG Zs.– KOVÁCS L. – VÁNYA L. – VASS S.: *Elektronikai hadviselés, Elektronikai hadviselés,* Nemzeti Közszolgálati Egyetem, Budapest, 2014, ISBN 978-615-5305-87-0, 271.

[20] SIEVERT, R. (2016). *The foreign intelligence surveillance act of 1978 compared with the law of electronic surveillance in europe.* American Journal of Criminal Law, 43(2), 125-155. https://search.proquest.com/docview/1833946813?accountid=42933

[21] FINSZTER G.: *Bűnüldözés és jogállam*, Ügyészségi Szemle 2016/1 6-28. o. http://ugyeszsegiszemle.hu/hu/201601/ujsag#undefined (letöltve: 2017.04.02.)

[22] LOWENTHAL, M. M.: *Hírszerzés, A titoktól a politikai döntésig*, Antall József Tudásközpont 2017. ISBN 978-615-5559-21-1. 616.o.

[23] VAULT, https://wikileaks.org/-Leaks-.html (letöltve: 2017.04.30.)

[24] MOODY, G. - *17/11/2016, Why the Investigatory Powers Act is a privacy disaster waiting to happen,* http://arstechnica.co.uk/tech-policy/2016/11/investigatory-powers-act-privacy-disaster-waiting-to-happen/ (letöltve: 2017.04.25.)

[25] BERGEN, P. – STERMAN, P. – SCHNEIDER, E. – CAHALL, B.: *Do NSA's Bulk Surveillance Programs Stop Terrorists?, New America Foundation,* 2014. https://na-production.s3.amazonaws.com/documents/do-nsas-bulk-surveillance-programs-stop-terrorists (letöltve: 2017.05.01.)

[26] VARGA Á.: *Közeleg 1984? – Az Egyesült Királyság bemutatta a biztonsági hivatalok és a titkosszolgálatok új megfigyelési jogszabályát, 2016.11.23.* http://mtmi.hu/cikk/975/Kozeleg_1984__Az_Egyesult_Kiralysag_bemutatta_a_biztonsagi_hivatalok_es_a_titkosszolgalatok_uj_megfigyelesi_jogszabalyat (letöltve: 2017.02.10.)

[27] *National Programmes for mass surveillance of personal data in EU member states and their compatibility with EU law, Study, Directorate General for Internal Policies,* Policy Department C: Citizens' Rights and Consitutional Affairs, 2013 http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493032/IPOL-LIBE_ET(2013)493032_EN.pdf (letöltve: 2017.05.01.)

[28] GRIFFIN, A.: *Snoopers' Charter: Theresa May to push huge new spying powers through Parliament, despite major report concluding they are not needed, 11 June 2015* http://www.independent.co.uk/life-style/gadgets-and-tech/news/snoopers-charter-theresa-may-to-push-huge-new-spying-powers-through-parliament-despite-major-report-10313042.html (letöltve: 2017.02.10.)

[29] BAILEY, R.: *Is Russia's Surveillance State Being Modelled on the West?, New Russian anti-encryption and data retention laws look sadly familiar. Jul. 22, 2016, reason.com,* https://reason.com/archives/2016/07/22/is-russias-surveillance-state-being-mode/print (letöltve: 2017.04.30)

[30] SMITH, B.: *Unfinished Business on Government Surveillance Reform, THE OFFICIAL MICROSOFT BLOG (June 4, 2014),* https://blogs.microsoft.com/firehose/2014/06/04/microsoft-general-counsel-us-government-needs-to-address-technology-trust-deficit/#sm.0002zabmb9llejf117u1wz6afeswb

[31] BODA J. – DOBÁK I.: *Titkosszolgálatok fejlődése – technikai szemmel,* NKE Nemzetbiztonsági Szemle 2016/4. szám, 17-25.o.

[32] VOLZ, D.: *FBI to gain expanded hacking powers as Senate effort to block fails* http://www.reuters.com/article/us-usa-cyber-congress-idUSKBN13P2ER (letöltve: 2017.05.01.)

[33] BERTA S.: *NSA-szintű jogokat kapott a német titkosszolgálat, 2017.01.04.* https://sg.hu/cikkek/it-tech/123068/nsa-szintu-jogokat-kapott-a-nemet-titkosszolgalat (letöltve: 2017.04.28.)

[34] *Investigatory Powers Bill*, https://www.publications.parliament.uk/pa/bills/lbill/2016-2017/0066/17066.pdf (letöltve: 2017.04.25.)

[35] *Joint Committee on the Draft Investigatory Powers Bill Written evidence, 1532 p.* http://www.parliament.uk/documents/joint-committees/draft-investigatory-powers-bill/written-evidence-draft-investigatory-powers-committee.pdf (letöltve: 2017.05.01.)