Titkosszolgálatok fejlődése – technikai szemmel[1]

Dr. Boda József[2] – Dr. Dobák Imre[3]

Absztrakt: A tanulmány a biztonságpolitikai környezet változása és a technológiai fejlődés mentén fogalmaz meg gondolatokat a titkosszolgálatokra vonatkozóan. Röviden kitér többek között az információgyűjtés technicizálódása, a korszerű technológiák jelentősége, valamint az egyes információgyűjtési területek felértékelődésének kérdéseire.

Kulcsszavak: titkosszolgálat, nemzetbiztonsági szolgálat, hírszerzés, technológiai fejlődés

Abstract: The study formulates some ideas about the evolution of national security services in connection with the technological developments and also about the changes security environment. Briefly, it deals with the topics of technical aspects of information gathering, the importance of modern technologies and also with the appreciation of the various areas of information gathering.

Keywords: secret services, national security services, intelligence, technological development

[1] A tanulmány „A technikai-műszaki nemzetbiztonsági szolgálatok és feladatok jelentősége a 21. században" címmel A nemzetbiztonság technikai kihívásai a 21. században c. jegyzetben jelent meg. Budapest, NKE Szolgáltató Nonprofit Kft- 2015. 16-22.

[2] ORCID azonosító: 0000-0002-4010-896X

[3] ORCID azonosító: 0000-0002-9632-2914

Bevezető

Napjainkban a biztonságpolitikai, a hírközlési, az informatikai és a technikai-műszaki környezet robbanásszerű fejlődése, eljárásaiban és szervezetében modernizált, gyors alkalmazkodásra képes felderítést és elhárítást követel meg. Éppen ezért korunk nemzetbiztonsági szolgálatainak – ideértve a hazai nemzetbiztonsági szolgálatokat is – *nyitottnak kell lenniük a világ technikai változásaira*, és folyamatosan követni kell azokat, annak érdekében, hogy a hírszerzés, elhárítás hosszú távon az adott ország és szövetségesei biztonságának hatékony garanciája lehessen. Hazánknak és szövetségeseinek a megfelelő védelemhez magas szintű biztonsági kultúrával, biztonsági tudatossággal és etikával rendelkező humán erőforrásokkal, technikai eszközrendszerekkel, valamint megfelelő jogszabályi háttérrel kell rendelkeznie.

Az „elektronikus" úton továbbított információk megjelenési formái, határokat átívelő jellege alapvetően meghatározzák mindennapi életünket, amelyek értelemszerűen kihatnak a nemzetbiztonsági gondolkodásra is. A szélesebb körben, szabadon elérhető, nyílt forrású információk mellett – mint egyes, technológiailag fejlettebb nagyhatalmak esetében ennek példáját láthatjuk – a globális méretű hírközlési rendszerekhez köthető információgyűjtés irányába tettek lépéseket, más országok a szűkebb földrajzi környezetre összpontosító nemzetbiztonsági érdekek mentén látják el feladataikat. A technikai vonatkozású területek egyre erőteljesebb jelenléte azonban nemcsak a nagyobb, globális titkosszolgálati képességekkel rendelkező nemzeteket jellemzi, hanem általánosságban megfigyelhető a 21. század nemzetbiztonsági célú feladatrendszerei és szervezetei mentén.

A „technikai vonatkozású" titkosszolgálati elemek körét az egyik ilyen, a titkosszolgálati sajátosságokat is megjelenítő alábbi felosztás[4] segíthet értelmezni, amely alapján a titkosszolgálati technikai eszközrendszerek négy nagyobb csoportba sorolhatóak:

- Adatgyűjtéseket biztosító érzékelők (pl. optikai, elektronikai, vegyi, akusztikus, nukleáris, szeizmikus és térinformatikai);
- Különböző szenzoroknak helyet biztosító platformok (pl. ember vezette, valamint robotrepülőgépek, hajók, tengeralattjárók, és műholdak);
- Számítógépek, hálózatok és szoftverek (amelyek gyűjtik, összehasonlítják, és feldolgozzák az adatokat, valamint információkat biztosítanak);

[4] *Bruce BERKOWITZ: Perspective: The R&D Future of Intelligence, Issues in science and technology, Volume XXIV Issue 3, Spring 2008 http://issues.org/24-3/berkowitz-3/ (letöltve: 2015. 06.10.)*

- Különböző, hagyományosnak tekinthető titkosszolgálati technikai eszközök (pl. rejtett kommunikációs eszközök, miniatürizált kamerák, rejtett konténerek, zártechnikai eszközök, stb.).

Fenti elemek az egyes országok katonai és (nemzet)biztonsági szervezeteiben eltérő szinten vannak jelen, azoknak alapvetően a technológiai képességeik, a gazdasági lehetőségeik és a politikai szándékaik szabhatnak határt. Általánosan megfogalmazható azonban, hogy napjainkra már a titkosszolgálati szervezetrendszerek szerves elemévé váltak:

- a különböző technikai jellegű forrásokra épülő nyílt és titkos információszerző területek;
- a technikai megoldásokkal támogatott információ-feldolgozó (elemző, értékelő) szakterületek;
- a technikai fejlesztési területek;
- (műszaki - technikai) szakértői funkciók;
- valamint a technikai- és információbiztonságért felelős szervezeti elemek.

Ezek, egyes esetekben egy-egy nagyobb szervezeten belül, más esetekben sajátos nemzeti tagoltság mentén, szervezetek között megosztva jelennek meg. További jellemzőként figyelhető meg a nemzetbiztonsági mellett a katonai, rendészeti, bűnügyi célú technikai vonatkozású információs igény, amely kiszolgálására nemzetközi szinten szintén többfajta strukturális megoldás látható. Mindezek mögött legerősebben két formáló tényező különböztethető meg, így az *infokommunikációs környezet fejlődése*, valamint *a biztonsági környezet változása*, egyes veszélyek szintjének jelentős megemelkedése.

Hatásaikra a nemzetbiztonsági szolgálatok esetében az alábbi néhány sajátossággal kívánunk rávilágítani.

A biztonsági környezet változása

Amíg korábban jól körülhatárolható ellenfél és alapvetően katonai fenyegetések határozták meg a titkosszolgálati feladatrendszereket, addig a biztonsági környezet változásával napjainkban jelentős módosulás következett be a célokban. A hírszerző szervezetek feladatköre kitágult, a veszélyek gyakran előre nem meghatározhatók, illetve távoli földrajzi térségben kereshetők. *Jelen vannak a társadalom tagjai között elvegyülő, szándékaikat rejtő, a nemzet biztonságát veszélyeztető személyek és csoportok is*, akik a békés célokra szánt technikai eszközöket szintén felhasználják. A veszélyek felderítése és elhárítása, a szükséges információk (technikai) eszközrendszerekkel történő beszerzése azonban összetett, a technikai és humán titkosszolgálati munka fokozott együttműködését követeli meg a nemzetbiztonsági szervezetektől.

A biztonságpolitikai viszonyokat tekintve jól látható, hogy a különböző veszélyek, kihívások és fenyegetések mentén számos infokommunikációs megoldás van jelen, formálva ezen biztonságpolitikai veszélyek súlyát, vagy akár (el)terjedését is. Mindezek közül a térségünket is súlyozottan érintő tömeges, illetve illegális migráció, a kapcsolódó embercsempészet, a terrorizmus felerősödése, a szervezett bűnözés, a kábítószer-kereskedelem vagy akár a gazdasági-pénzügyi válságok különböző megjelenési formái említhetők. Gondoljunk csak napjaink déli irányú tömeges méretű migrációs nyomására, amely mögött például megtalálhatjuk az embercsempész hálózatok által az interneten folytatott tudatos befolyásoló tevékenységet. Idesorolhatók az internetes közösségi oldalaknak a terrorizmus terjedésére, a terroristák toborzására, valamint a nyilvánosság befolyásolására gyakorolt hatása is. Hasonlóképpen jelen vannak a technikai eszközrendszerek a terrorizmushoz kapcsolódó hackertámadások, vagy akár az illegális pénzügyi – gazdasági tevékenységeik mentén. Mindezek rendkívül jól jelzik az infokommunikációs hálózatok és megoldások nemzeti határokat túllépő „hatásait", közvetetten befolyásolva az egymástól távoli térségek biztonsági helyzetét is.

Együttműködési felületek jelentőségének felértékelődése

Korunkban már mind a technikai, mind egyéb szakmai feladatok terén már nehezen elképzelhető, hogy a nemzetbiztonsági szolgálatok széles körű együttműködési felületek és kapcsolatok nélkül hatékonyan hajtsák végre feladataikat. Itt kell megemlíteni egyrészről a titkos információgyűjtés ellátásához, az infokommunikációs környezet fejlődéséhez kapcsolódó hírközlési és infokommunikációs szolgáltatókkal való együttműködéseket, de itt jelennek meg a műszaki-tudományos, ipari együttműködési felületek is, amelyek többek között a fejlesztések és az eszközrendszerek kialakítása terén kaphatnak különös jelentőséget. Másrészről pedig nagy szükség van a biztonsági környezet változására (pl. terrorizmus) reagáló nemzeti és gyakran nemzetközi szintérre kiszélesedő szakmai együttműködésekre és információcserét biztosító kapcsolatokra.

Korszerű technológiák és a fejlesztés jelentősége

A nemzetbiztonsági szolgálatok feladata, hogy jogszabályi felhatalmazásuk, feladatrendszerük, valamint képességeik és lehetőségeik mentén – a folyamatosan változó technikai környezet figyelembevételével – hatékonyan reagáljanak a különböző veszélyekre, valamint titkos (és nyílt) információgyűjtő tevékenységükkel biztosítsák a szükséges információk megszerzését. Ennek megvalósítása azonban csak a technikai környezet sajátos jellemzőinek és változásainak figyelembevételével, hosszú távú stratégiai elképzelések mentén lehetséges. Amíg az illegális tevékenységek mentén rövid időn belül megjelennek a legkorszerűbb eszközök, illetve a résztvevői kör felhasználja a tevékenységéhez szükséges új és újabb infokommunikációs alkalmazásokat, addig a nemzet biztonságáért dolgozó szerveze-

teknek mindezek törvényes ellenőrzési képességeinek megteremtésére tudatosan, hosszú távú kitekintéssel kell felkészülni. A nemzetközi színtérre kitekintve mindehhez:

- a technikai környezet változásaira, új technológiák megjelenésére reagálni képes hatékony nemzetbiztonsági-technikai szervezetrendszer;
- megfelelő anyagi források, és kapcsolatrendszer;
- hatékony jogszabályi környezet;
- valamint képzett humánerőforrás szükséges.

A titkos információgyűjtés technicizálódása

Általánosságban megfogalmazható, hogy a különböző hírszerzési (titkosszolgálati) célú technológiák alapvetően nem különböznek a külső „civil" környezetben alkalmazott technológiáktól. Azok fejlődésétől nem elválaszthatóak, az eltérések igazán rendeltetésükben és sajátos alkalmazásaikban kereshetőek. Egyes esetekben azok fejlesztése – a várható alkalmazás érdekében – elzártan, a titkosszolgálati érdekek mentén történik, más esetekben a külső környezetben fejlesztett eszközök és megoldások adaptálása figyelhető meg. Jellemzőik a speciális szaktudás, a titkosszolgálati szempontok érvényesítése, és a célok elérését biztosító fejlesztési irányok zárt meghatározása.

Történetileg az elmúlt évszázadra érdemes visszatekinteni, amikor is a világháborúk időszakával párhuzamosan felerősödött a titkosszolgálati technikai képességek jelentősége. Az Egyesült Államok által vezérelt nemzetközi SIGINT együttműködés, a szövetségi keretekben történő technikai vonatkozású információcsere, vagy akár a Varsói Szerződés megalakulását követően formálódó, a szocialista tábort jellemző nemzetközi technikai együttműködési felületek mutatják a hidegháború időszakának határokon átnyúló technikai információgyűjtési feladatát. Létrejöttek azon közismert nemzeti szolgálatok[5], amelyek feladatrendszerében már megtalálhatjuk a technikai titkosszolgálati elemeket is. Ezek fejlődése a hidegháború végét követően azonban nem szakadt meg, tehát a 21. század titkosszolgálati eszközrendszerei és képességei nem előzmények nélküliek. Ezt követően a megváltozott biztonsági környezet, valamint a párhuzamosan felgyorsuló technikai fejlődés hatásait figyelhetjük meg a nemzetbiztonsági szervezetek feladatrendszere mentén is. Az ezredfordulót megelőzően a korábbi szembenállásra jellemző struktúrák átalakultak, és lassan helyet vívtak ki maguknak az új típusú kihívásokra reagáló szervezeti elemek. Ezt az időszakot a technikai eszköz-

[5] *Többek között: 1952 / National Security Agency – NSA, 1954 / Komityet Goszudarsztvennoj Bezopasznosztyi - KGB, 1946 (1919) - Government Communications Headquarters – GCHQ, 1956 / Bundesnachrichtendienst – BND, 1982 / Direction générale de la sécurité extérieure - DGSE*

parkok megújítása, a korábbi stratégiák újragondolása, valamint a nemzeti és nemzetközi együttműködések mentén az új képességek keresése jellemezték.

Napjainkban, a külső környezet (biztonsági, illetve technikai) változásaira az érintett nemzetbiztonsági szolgálatok a jog által szabályozott módon a nyílt és a titkos információgyűjtő képességeikkel, azok folyamatos fejlesztésével reagálhatnak. Az elmúlt évek széles körben ismertté vált nemzetközi adatgyűjtési botrányaitól[6] eltekintve, jól jellemzik az információgyűjtés technicizálódásának jelentőségét az ezredfordulót követően felszínre kerülő szabályozási kérdések körüli viták. Ennek gyakran említett példája a 2001. szeptember 11-ei terrortámadás és hatásaként megjelenő Patriot Act, vagy akár a Londonban 2012-ben megrendezett nyári olimpiai játékokat megelőzően, a brit Kormányzati Kommunikációs Parancsnokság (GCHQ - Government Communication Headquarters) technikai ellenőrzési lehetőségeinek kiterjesztése is.

A nyílt forrású információgyűjtés felértékelődése

A megváltozott biztonsági környezetben felerősödő, majd 2001-ben kicsúcsosodó terrorizmus elleni küzdelem világított rá a társadalom oldaláról jelentkező alapjogok védelmének és az információgyűjtés határainak kérdésére, valamint az információk határokon átnyúló hatásaira. Mindez már a globális méretű internethasználat korszakában történt, ahol egyre erőteljesebben jelentek meg az infokommunikációs eszközök illegális, illetve bűnös tevékenységekre felhasználhatóságának kérdései. A szolgálatok hamar felismerték, hogy rendkívül értékes részinformációkat nyerhetnek a különböző nyíltan elérhető technikai forrásokból, így az internet, mint forrás jelentősége felértékelődött a nemzetbiztonsági/biztonsági szervezetek számára. Az egyes országok nemzetbiztonsági struktúráiban fokozatosan teret nyertek a technikai alapokon nyugvó, nyílt információk gyűjtését biztosító (OSINT) képességek és szervezeti elemek, amelyek sajátos szakmaiság mentén egyre kifinomultabb megoldásokkal törekszenek a számukra értékes információk gyűjtésére, elemzésére, értékelésére.

A szakirodalmakban gyakran említett tételként jelenik meg, hogy a hírszerző, illetve nemzetbiztonsági szolgálatok tevékenységéhez szükséges adatok, illetve információk túlnyomó része nyíltan, nyílt forrásból elérhető. Egyes becslések ennek arányát 80-90% közöttire is teszik. A pontos arányok értelemszerűen meg-

[6] *Így például a WikiLeaks, vagy az E. Snowden nevéhez köthető 2013-ban kirobbant lehallgatási botrány. A technikai eszközrendszerek adta információgyűjtések alkalmazása számos konfliktust okoztak a szövetségesek között is, ide sorolva az amerikai hatóságok által végzett szövetségeseket érintő lehallgatásokat (a német kancellár, vagy akár a 2006-2012 közötti időszakban a francia államfők beszélhetéseinek lehallgatása.) (forrás: http://www.parameter.sk/rovat/kulfold/2015/06/24/titkos-adatgyujtes-parizs-nem-turi-el-biztonsagat-megkerdo jelezo, letöltve: 2015. június 25.)*

határozhatatlanok, elfogadva, hogy a titkosszolgálatok tevékenységéhez szükséges adatok nagyobb arányban vannak jelen nyíltan elérhető módon, a titkos információgyűjtés pedig egy speciális eszközöket és módszereket igénylő tevékenységi kört ölel fel. Utóbbinál jelennek meg a demokratikus társadalmakban azon eszközök és módszerek, amelyek az érintett személyek alapjogainak sérülését okozhatják, így ezek kizárólag szigorú törvényi szabályozás mentén alkalmazhatóak. A két „kategória" között a technológiák fejlődésével, azonban *egyre összetettebb ún. szürke zóna körvonalazódik*, amely szaktudás és technikai képesség birtokában teret adhat akár illegális adathalászok számára is.

Technikai adatgyűjtés – társadalmi érzékenység

A 20. század utolsó harmadában szemtanúi lehettünk a nyilvános jogi kereteket öltő titkosszolgálati szabályozások megjelenésének, a demokratikus társadalmakra jellemző külső kontrollrendszer erősödésének, valamint a titkos információgyűjtés és a társadalom „viszonya" egyfajta rendezésének. Azzal együtt, hogy ma már az állami feladatok rendszerében elismerten helye van az alapjogokba, a magánszférába különböző mértékig beavatkozó, szabályozott információgyűjtésnek, a „társadalom oldaláról" mégis gyakran merül fel a titkos információgyűjtés mértékének és lehetőségeinek kérdése. Érthető módon szükséges, hogy ennek megfelelő jogi és szakmai keretei legyenek, amelyek mentén az érintett szervezetrendszerek a demokratikus normáknak megfelelően működhetnek és végezhetik tevékenységüket. Sajátos jelenségként figyelhető meg a nyílt és titkos információszerzés közötti határokat érintő társadalmi érzékenység időszakos eltolódása is. *A határok elmozdulásának egy-egy jelentősebb, a biztonságot negatívan befolyásoló esemény bekövetkezésekor lehetünk tanúi.* Ekkor kerülnek előtérbe a társadalom (és az állam) oldaláról megjelenő fokozottabb biztonsági igények, és felértékelődik a nyílt és titkos információgyűjtés határán mozgó, főként valamilyen technikai úton megszerzendő információ lehetősége, amelyek akár formáló tényezőként is kihathatnak az érintett szervezetek tevékenységére és struktúrájára is.

Kitekintés

A jövőt illetően valószínű, hogy a titkosszolgálatok technikai vonatkozású szegmenseit a már említett két tényező, így a biztonság oldaláról jelentkező fenyegetések változása, valamint a technikai környezet fejlődése formálja majd a továbbiakban is. A fenyegetések terén a már most is látható hangsúlyeltolódások új hírszerzési célokat, és ezek mentén új és újabb információgyűjtési megoldásokat eredményeznek majd. Itt kap egyértelmű szerepet a technológiai fölény kérdése, amely a korszerű, határokon átnyúló, globális méretű információgyűjtési képesség mentén megjósolhatatlan előnyöket biztosíthat az ezekkel rendelkező országoknak. Mindezek mögött új alkalmazási elvek, módszerek jöttek és jönnek létre,

ideértve mind az információgyűjtés, mind az információk elemzésének és értékelésének kiemelten fontos területeit is. Mint A. Rolington megfogalmazta *„a kommunikációs forradalom mélyen érintette a hírszerzési ciklus tradicionális elemeit…”*[7]. A tömeges méretekben rendelkezésre álló információk megszerzése, feldolgozása, és elemzése pedig újfajta megközelítések megjelenését vetítik előre, amelyek kihathatnak az érintett nemzetbiztonsági szervezetek struktúráira is. A jövőben *a technikai jellegű „elemek” a szűken értelmezett nemzetbiztonsági szervezetrendszereken túlmutatva, a biztonságért felelős egyéb szervezetek (pl. rendvédelmi) munkája mentén is egyre inkább meghatározóbbá válhatnak.*

Ma már számos ország hadseregében, nemzetvédelmi és nemzetbiztonsági szervezeteinél kibervédelemmel foglalkozó katonai és polgári szervezetek működnek, jelezve a kibertér irányából jelentkező kihívásokat, a kiberbűnözés és a kiberterrorizmus térhódítását. Ennek jelentősége pedig állami szinten is kiemelten fontossá vált, hiszen szinte minden korszerű technikai eszközrendszer informatikai alapú, beleértve a honvédelemmel, a kritikus infrastruktúrákkal, a rendvédelemmel, és a nemzetbiztonsági szolgálatokkal kapcsolatos rendszereket és hálózatokat is.

Még nagyobb jelentőséget kapnak majd a K+F tevékenységek, valamint az ezekre épülő kapcsolatok, amelyek megalapozhatják az adott szervezetek további képességeinek fejlődését. Amíg egy zártnak tekinthető titkosszolgálati szféra egyfajta hátrányban lehet szakmai elszigeteltsége, nyíltan felvállalható szakmai kapcsolatrendszerei hiánya miatt, addig a civil szférában értelemszerűen nagyobb számban jelen lévő tudósok és kutatók szabadabb tudományos mozgástérrel rendelkeznek. Az érintett nemzetbiztonsági szolgálatoknál így előtérbe kerülhet a K+F tevékenységet folytató szervezetekkel való szorosabb kapcsolatok kialakítása, a külső környezetben folyó kutatások munkatársaikkal történő megismertetése, a tudományos (különösen technikai területeken) történő képzések és új tudományos eredmények létrehozásának ösztönzése.[8]

---

[7] *Alfred ROLINGTON: Hírszerzés a 21. században – a mozaikmódszer, Antall József Tudásközpont, 2015. ISBN 978-963-87486-3-8. p.13. A szerző a tradicionális hírszerzési ciklus és tervezési modell kiváltásának szükségességére hívja fel a figyelmet és javasolja a hírszerző szolgálatok, rendfenntartó szervek, valamint kereskedelmi szervezetek számára korszerű, az infokommunikációs környezetnek megfelelő modellek megalkotását.*

[8] *Bruce BERKOWITZ: Perspective: The R&D Future of Intelligence, Issues in science and technology, Volume XXIV Issue 3, Spring 2008 http://issues.org/24-3/berkowitz-3/ (letöltve: 2015. 06.10.)*

Felhasznált irodalom:

- BERKOWITZ, Bruce: Perspective: The R&D Future of Intelligence, Issues in science and technology, Volume XXIV Issue 3, Spring 2008 http://issues.org/24-3/berkowitz-3/ (letöltve: 2015. 06.10.)
- FLURI, Philipp – JOHNSON, Anders B. – BORN, Hans: A biztonsági és védelmi szektor parlamenti felügyelete (IPU-DCAF kézikönyv), Budapest, 2004, ISBN 963 214 458 9
- HAIG Zsolt: Információ, társadalom, biztonság, NKE Szolgáltató Kft, 2015, ISBN 978-615-5527-08-1
- ROLINGTON, Alfred: Hírszerzés a 21. században – a mozaikmódszer, Antall József Tudásközpont, 2015. ISBN 978-963-87486-3-8