A nemzetbiztonság 21. századi értelmezése és jellemzői

Dobák Imre

Bevezető

A 21. századi biztonsági struktúrák szerves részét alkotják a nyilvánosság nagymértékű kizárásával működő nemzetbiztonsági szolgálatok. Sajátos rendeltetésük, feladataik hatékony végrehajtása a zártságuk mellett ugyanakkor feltételezi, hogy a külső környezetben végbemenő változásokra folyamatosan reagáló, azokat lekövető képességekkel és megoldásokkal rendelkezzenek. A megállapítás országoktól és a (nemzet)biztonsági szolgálatok típusától függetlenül igaznak tekinthető.

Nagyobb történelmi távlatba helyezve a századunk elejére jellemző nemzetbiztonsági gondolkodást a későbbiekben vélhetően egy átmeneti korszakként fogják értelmezni. Történhet mindez azért, mert a 20. század világháborúival, majd hidegháborúival szemben az ezredfordulóra számos, a Földünk és a rajta élő társadalom biztonságát befolyásoló tényező jelentősen átalakult. A bipoláris világrend helyébe a folyamatosan formálódó multipoláris világrend lépett, ahol a korábbi – túlsúlyosan – katonai tényezők mellett a biztonság egyéb elemei is szerepet kaptak. Gondoljunk egyszerűen a globalizáció megállíthatatlan jelenségére, a gazdasági egymásrautaltságra, de megemlíthetjük a kibertér vagy akár a technológiai környezet addig nem látott fejlődési ütemét. A változások és az ezredfordulót követően „kitáguló" biztonságpolitikai problémák (fegyveres konfliktusok, humanitárius vészhelyzetek, tömeges illegális migráció, terrorizmus felerősödése, környezeti és egészségügyi veszélyek) napjainkra szintén visszafordíthatatlanul befolyásolják az egyes nemzetek biztonságát. A múlt századdal szemben ezek azonban már nem egy jól látható másik féltől származnak, hanem főként az összetett nemzetközi politikai, gazdasági, társadalmi és technológiai kérdéskörök mentén formálódnak, amelyekre az egyes államoknak és azok (nemzet)biztonsági rendszereinek ma még csak részben állnak rendelkezésére a megfelelő kezelési technikák.

https://doi.org/10.36250/01005_01

A 20. század hidegháborús időszakában a titkosszolgálatok[1] meghatározó szerepet töltöttek be a szemben álló felek egymás elleni, háttérben folytatott küzdelmében. Sajátos szervezetrendszerek alakultak ki, amelyek működésének mélyebb megismerése egészen a bipoláris világrend felbomlásáig kevéssé volt ismert. Ma már nem titok a nemzetbiztonsági szervezetek létezése, működésük főbb kereteit nyílt jogszabályok rendezik, és a nyílt tudományos gondolkodásban is sajátos szakmai-tudományos elméletek alakultak ki a nemzetbiztonsági témakörök vizsgálatára. Mint Jávor Endre tanulmányában megfogalmazza:

> „A nemzetbiztonsági tevékenységnek a társadalmon belül kettős funkciója volt és van. Egyrészt van egy hatalmi, másrészt egy szolgáltató funkciója, melyek közül a hidegháborút megelőző időszakban a hatalmi funkció volt domináns […] [Napjainkban pedig] tendenciájában előtérbe kerül a nemzetbiztonsági tevékenység szolgáltató funkciója."[2]

A múlt század vége összességében a nemzetbiztonsági rendszerek számára is egy átalakulási, helykeresési időszakot biztosított, amely során szerepük és feladataik módosultak, a hidegháborús ellenfél hiányából adódó kezdeti bizonytalanságtól kezdve egészen a terrorizmus elleni küzdelem felértékelődéséig. Az egymás elleni, korábban politikai, ideológiai alapokon nyugvó, globális fegyverkezési versenyt ösztönző szembenállást felváltották a nemzeti, illetve szövetségi tagságokból adódó érdekek, amelyek közvetlenül hatottak a szolgálatok működésére. A hidegháború lezárásának változó nemzetbiztonsági irányát jól jellemzi az amerikai James Woolsey 1993-ban tett legendássá vált mondása, miszerint: „Megöltünk egy nagy sárkányt. De most olyan dzsungelben élünk, amely tele van különféle mérgező kígyókkal. És sok szempontból a sárkányt könnyebben lehetett nyomon követni."[3]

Térségünkben felszámolták az állambiztonsági struktúrákat és a demokratikus jogállami normák mentén a nemzetbiztonsági szolgálatok a működésükbe mélyebb betekintést biztosító jogszabályi kereteket kaptak. Mindez nemcsak hazánkban, hanem régiónk országaiban szinte párhuzamosan zajlott le. Az addig

[1] A „titkosszolgálat" kifejezést gyűjtőfogalomként használták, napjainkban, általánosságban a nemzetbiztonsági, illetve hírszerző és biztonsági szolgálatok elnevezés alkalmazott.

[2] Jávor Endre: A hír, az adat, az információ és a dokumentáció fogalma, helye, szerepe a döntéshozatalban. *Nemzetbiztonsági Szemle,* 5. (2017), 3. 57–58.

[3] James Woolsey 1993 februárjában, az USA Szenátusának Hírszerző Bizottsága előtt, a CIA igazgatói kijelöléséhez kapcsolódó meghallgatáson tett kijelentése. J. J. Green: The Fog of Espionage. Part 3: 'A Bewildering Variety of Poisonous Snakes'. *Wtop News,* 2019. szeptember 27. (szerzői fordítás).

csak szűk kör számára megismerhető jogszabályi háttér nyílt formába öntésével lehetővé vált a társadalom számára is a szolgálatok rendeltetésének, működésének adott szintig történő megismerése. A szükséges fékek és ellensúlyok rendszerét beépítve társadalmi támogatottságon és elfogadáson alapuló nemzetbiztonsági rendszerek jöhettek létre, illetve a korábbi hidegháborús titkosszolgálati szervezetek több-kevesebb sajátosságot megtartva átalakultak.

Századunk ennek az átmeneti időszaknak a folytatásaként újabb kihívásokkal vette kezdetét, amelyek közül a legjelentősebbnek a nemzetbiztonsági kérdéskörökre tartósan hatást gyakorló, 2001-ben bekövetkezett amerikai egyesült államokbeli terrortámadás tekinthető, amely új szervezeteket, jogszabályokat és széles nemzetközi kapcsolatrendszereket keltett életre. A változásokhoz igazodva, a hidegháborút követően egyszer már megújult nemzetbiztonsági irányok, feladatok és az ezek végrehajtását biztosító szervezeti struktúrák újabb, mélyreható változásokon estek át. A terrorizmus elleni küzdelemhez igazodó fúziós jellegű, valamint a kibertér kihívásaira összpontosító szervezeti modellek működése azonban gyakran eltér a korábban ismert megoldásoktól, illetve a nemzetközi környezetben is jól láthatók ezek még letisztulatlan folyamatai.

Jelentős hatásként értelmezhető, hogy a nemzetbiztonsági rendszerek egyre több, nélkülözhetetlen szálon kapcsolódnak az állam és a társadalom egyéb szektoraihoz, a biztonságot befolyásoló tényezők jelentős arányban már nem az államok közigazgatási határain belül keletkeznek, továbbá a korábbi határok szigorú elválasztó szerepe is leértékelődött. Az infokommunikációs megoldások robbanásszerű fejlődése – annak az államra és a társadalomra gyakorolt tagadhatatlan pozitív hatásai mellett – ugyanakkor közelebb is hozta a biztonságot fenyegető kihívásokat, gyakran felvetve a nemzetközi szabályozási kérdések fontosságát.

A modern társadalmak egyre sebezhetőbbé váltak, és rendkívüli jelentőséget kapott a kölcsönös függőség kérdése. Mindezek a széles körben elterjedő IKT- (Információs és Kommunikációs Technológiák) megoldásoknak köszönhetők, amelyek fejlődése az utóbbi 40 évben gyorsult fel.[4] Az egyes technológiák kapcsán több fordulópont is megfigyelhető, hiszen a jelzett időszak alatt az analóg eszközöktől eljutottunk a jövőnket bizonyosan meghatározó felhőalapú információtárolásig, az IoT- (*Internet of Things,* dolgok internete) megoldásokig,

[4] Hiroshi Nishimura – Emiko Kanoshima – Kazuhiro Kono: Advancement in Science and Technology and Human Societies. In Seiji Abe – Mamoru Ozawa – Yoshiaki Kawata (szerk.): *Science of Societal Safety Living at Times of Risks and Disasters.* Springer, 2019. 23.

amelyek az internetre kapcsolódva lényegében szinte önállóan cserélhetnek információkat. Mindezek mögött már a hétköznapi ember számára rendkívül összetett metodikai, információs és technológiai kapcsolatok húzódnak meg.

A nemzetbiztonság értelmezése

A nemzetbiztonság tudományos jellegű megközelítése és kérdéseinek vizsgálata köré napjainkra egyre több szakirodalom és elmélet társul.[5] Az információgyűjtés fejlődő területei esetében a *„surveillance studies"* kategóriája főként a megfigyelés és a szabadságjogok közötti kérdések vizsgálatát öleli fel, míg a „titkosszolgálatok" esetében a nemzetbiztonsági rendszerek működését (például stratégiák, struktúrák, együttműködések, információcsere, felügyelet kérdései) és a jelentősebb biztonsági fenyegetések vizsgálatát az *„intelligence studies"* néven kategorizálható terület mentén láthatjuk.

Fogalmi megközelítésben a nyugati szakirodalmakban elterjedt a *„national security intelligence"* fogalma, amely jelentése körül a szakértők sem egységesek. Loch K. Johnson megfogalmazását tekintve az eltérés az *„intelligence"* szűkebb és tágabb értelmezése körül jelentkezik. Szűkebb értelmezésben a titkosszolgálatok információgyűjtő és -elemző tevékenységére (vagyis az információra) utal, tágabb értelmezésben a három elsődleges hírszerzési tevékenységet, az információgyűjtést és -elemzést, a fedett akciókat és az elhárítást foglalja magában.[6] Ugyancsak Johnson felosztását tekintve az „intelligence" folyamatként is tekinthető, ahol a legelterjedtebb tevékenység az információgyűjtés és -elemzés. Spracher az „intelligence" kategóriájára egy másik megközelítésben olyan áruként vagy eszközként is tekint, amelyre minden nemzetnek szüksége van a túléléshez, ahol a hírszerzés hagyományos iránya mellett van egyik másik terület, a „rendészeti hírszerzés", amelyet „belbiztonsági hírszerzésnek" is nevezhetnek.[7] A hírszerzés harmadik területeként az üzleti hírszerzést[8] jelöli meg, mint amely nem az állami struktúra része.

[5] A témakör hazánkban is ismert alapvető irodalma közé sorolják Sherman Kent, Roy Godson, Loch K. Johnson, vagy például Mark Lowenthal műveit.

[6] Loch K. Johnson: *National Security Intelligence, Secret Operations in Defense of the Democracies.* Second edition, Malden, John Wiley & Sons, Polity Press, 2017.

[7] William C. Spracher: *National Security Intelligence Professional Education: A Map of U.S. Civilian University Programs and Competencies.* Dissertation. 2009. 14–15.

[8] *Competitive intelligence,* illetve *business intelligence* néven jelöli a területet.

Érdemes néhány szót ejteni a nemzetbiztonsági rendszer kategóriájáról is, amely napjainkra a hagyományosan idesorolt hírszerzési és elhárítási („titkosszolgálati") funkciójú szolgálatok összeségén kívül már jóval szélesebb értelmezést nyert. Mint Finszter Géza megfogalmazza tanulmányában:

> „A nemzetbiztonság a köznyugalomhoz hasonlóan egyensúlyi állapot. Egyetlen országnak sincs lehetősége a fenyegetések felszámolására, minthogy azok többsége szuverenitásának hatókörén kívül keletkezik. Amire lehetőség nyílik, az a veszélyek időben történő felismerése és a gyors reagálás."[9]

Mindez sajátos feladatrendszert és a külvilág számára számos elemében nem látható képességeket, vagyis titkos megoldásokat és eljárásokat igényel. Szükségszerű jogállami fékeket a demokratikus normáknak megfelelő jogszabályok és a működés kellően kialakított ellenőrzési rendszerei jelenhetnek.

A szolgálatok fő feladatai az adott ország szuverenitásának védelme mellett gyakran eltérő nemzeti érdekek mentén keresendők, ahol az információk védelme vagy éppen megszerzése, elemzése és értékelése, majd a döntési szintekre való gyors eljuttatása kulcsfontosságú. Fentiek a nemzetbiztonsági szolgálatok szintjén túlmutató „nemzetbiztonsági rendszerek" működését igénylik, hiszen a biztonságot fenyegető tényezők számos irányból és formában jelentkezhetnek. Ennek megfelelően szoros kapcsolatrendszerek és együttműködések alakultak ki a biztonsági-rendvédelmi szervek egyéb ágaival, de idesorolhatók az adott nemzetbiztonsági struktúra irányítói, koordinálói, valamint az ellenőrzésében érintett elemei is.

A nemzetközi színtérre kitekintve országonként gyakran eltérő nemzetbiztonsági rendszermodellekkel találkozhatunk, hiszen nincs általánosan „elfogadott" megoldás arra nézve, hogy egy ország hány szolgálattal és milyen irányítási rendszerrel biztosíthatja hatékonyan a tágan értelmezett nemzetbiztonságát. Az azonban megfogalmazható, hogy a nyílt alapjogszabályi környezet, a demokratikus jogállami működés normái, a nemzetközi viszonyok érzékenysége, valamint a magánszférába történő beavatkozás korlátai kereteket szabnak ezen szervezetek működésének. Látható továbbá, hogy a nemzetbiztonsághoz sorolt „szolgálatok" az adott ország biztonsági struktúráinak részeként a nemzetbiztonsági érdekek mentén, nyílt és titkos eszközökkel, módszerekkel, belföldön és külföldön végzik tevékenységeiket. Mindez jól jelzi a terület érzékenységét is, hiszen:

– a mögöttes nemzetbiztonsági érdekek alapvetően nem nyilvánosak;

[9] Finszter Géza: Állambiztonság – nemzetbiztonság. *Nemzetbiztonsági Szemle,* 7. (2019), 3. 105.

- az alkalmazható eszközök és módszerek teljes részletességgel nem publikusak;
- belföldi irányban a társadalmi érzékenység és az állampolgárok magánszférájának kiemelt védelme, külföldi irányban a diplomáciai viszonyok és a nemzetközi kapcsolatok válnak meghatározóvá;
- a hagyományosan nemzeti szintű szolgálatok bizonyos területeken (például terrorizmus elleni küzdelem) akár a szövetségi tagságokon túlmutató együttműködésekben is érintettek lehetnek.

Fontos szempont továbbá, hogy a különböző országok nemzetbiztonsági szolgálatainak struktúrája és működése gyakran nem vizsgálható egyazon síkon. Eltérő történeti, politikai, gazdasági, biztonságpolitikai sajátosságokkal rendelkeznek, valamint eltérő érdekek mentén fejlődtek és fejlődnek napjainkban is. A tevékenység megítélése szempontjából talán az egyik legfontosabb mögöttes tényező mégis az adott állam politikai berendezkedése és működése. Amíg egyes országokban a „titkosszolgálati" tevékenység gyakran állambiztonsági céllal működik, addig a demokratikus berendezkedésű államokban azok működése mögött széles nemzeti alapokon nyugvó érdekeket és értékeket kereshetünk.

Az egyszerűen csak eltérő elnevezésnek vélt szóhasználat (állambiztonság vagy nemzetbiztonság) mögött így rendkívül fontos, alapvető különbségek húzódnak meg.[10] Ezen rendeltetésbeli különbségek kihatnak a különböző új típusú kihívások kezelésének megoldásaira is, aminek alátámasztására példaként említhető a társadalmak mindennapjait átszövő kibertér megközelítése. Amíg a demokratikus társadalmakban a kibertér szabad felhasználásának, a magánszféra védelmének szempontjait láthatjuk, addig ennek ellenpólusaként más országoknál akár az internet és a szabad kommunikáció átfogó korlátozásának, vagy éppen a tömeges, rendszerszintű megfigyelésnek a gyakorlatát tapasztalhatjuk. Míg az autokratikus társadalmakban ritkán kap teret a titkosszolgálatok működésével szembeni társadalmi kritika, addig a demokratikus berendezkedésű országok esetében a nemzetbiztonsági szolgálatok működését a társadalom érdeklődő figyelemmel kíséri, és érzékenyen reagál a működési keretek esetleges kiterjesztésére.

Általánosságban megfogalmazható az is, hogy rendkívüli eseményeket (idesorolhatók akár a 2001-ben az Amerikai Egyesült Államokban [Egyesült Államok, USA], illetve a később Nyugat-Európában elkövetett terrorcselekmények)

[10] Részletesen lásd Finszter (2019): i. m. 9.

követően felértékelődik a nemzetbiztonsági ágazat szerepe, amely a létszámbővítésen és a technikai képességnövelésen túl a társadalmi érzékenységet már befolyásoló titkosszolgálati módszerek kiterjesztésének is teret engedhet.[11] A terrorizmus elleni küzdelem jogszabályainak módosításával, így például korábban elképzelhetetlennek tűnő megfigyelési lehetőségek (telefon-ellenőrzés, metaadatok tömeges feldolgozása, kamerarendszerek telepítése) széles társadalmi rétegek számára váltak elfogadhatóvá. A rendkívüli események „aktív" időszakának lecsengését követően a társadalom biztonságérzete azonban ismét „átalakul", és az állampolgárok egyéni szabadságjogainak fokozott védelme válik újra hangsúlyossá. Mindennek lényege talán abban összegezhető, hogy senki nem szeretne az orwelli megfigyelés társadalmában élni, de konfliktushelyzet esetén a közösség biztonsága érdekében elfogadja bizonyos jogainak időszakos korlátozását. Hasonló a külföld-belföld nemzetbiztonsági viszonylatának megítélése is, ahol az országhatárokon túlmutató nemzetbiztonsági tevékenység (külföldön végzett hírszerzés) azok irányaitól, céljaitól és gyakran az alkalmazott eszközök mélységétől függetlenül elfogadottabbak lehetnek az állampolgárok számára. Vagyis az esetleges szabadságjogokat érintő, magánszférát korlátozó „belső biztonság" nemzetbiztonsági kérdései és annak társadalmi megítélése érzékenyebb, mint a közös, nemzeti biztonsági érdekek mentén jobban akceptálható külső irányú titkosszolgálati funkció.

Jellemzők és tendenciák

A hírszerzés és elhárítás hagyományos megközelítését tekintve a hidegháború időszakában a jól látható külső és vélt vagy valós belső veszélyek felderítése, elhárítása képezte a „titkosszolgálatok" meghatározó alapfeladatát. A korszak lezárultával azonban – a könyv egyéb fejezeteiben részletesen ismertetett új veszélyek, kihívások, valamint megváltozott külső környezet mentén – a hírszerzés és elhárítás tevékenysége és rendszerei is alkalmazkodtak a megváltozott körülményekhez. Az alábbiakban ezeknek, az eltelt évtizedekhez köthető, egymáshoz kapcsolódó *főbb jellemzőknek* az áttekintésével kívánunk hozzájárulni

[11] Mint arra több szerző is felhívta a figyelmet, már az ezredfordulót követően rövid időn belül komoly aggodalmak merültek fel az amerikai közvéleményben a hírszerző közösség adatokhoz való hozzáférésével és azok használatával kapcsolatban, annak ellenére, hogy azok hírszerzési forrásként potenciális értéket képviselnek.

napjaink nemzetbiztonsági rendszereinek, a hírszerzés vagy akár elhárítás kérdéskörének teljesebb megértéséhez.

Prioritások változása

A 20. század végén még helyüket kereső titkosszolgálatok az ezredfordulót követően egy rendkívül összetett jelenséggel, a terrorizmussal szembesültek, amely rövid időn belül szinte országoktól függetlenül a biztonságot veszélyeztető elemek ranglistájának első helyére került. Ezzel lényegében egy közös „ellenségkép" jött létre, amely sajátos fejlődést indított el a biztonsági-védelmi szférában. Akár a térségünk szempontjából meghatározó NATO-, illetve EU-tagországokat, de akár Oroszország vagy Kína példáját is megemlíthetjük, ahol a terrorizmus elleni küzdelem közvetlenül hatott mind a rendészeti, a katonai és kiemelten a nemzetbiztonsági gondolkodásra. Ha csak vázlatosan is tekintünk az elmúlt 30 év jelentősebb, nemzetbiztonsági struktúra- és feladatváltozásokat eredményező fordulópontjaira, megtalálhatjuk a terrorcselekmények közvetett hatásait. A 2001. szeptemberi Amerikai Egyesült Államok elleni terrortámadás alapjaiban formálta át az amerikai titkosszolgálatok információgyűjtési rendszerét, de idesorolhatók az Európai Unió több országában, továbbá Oroszországban és Törökországban elkövetett jelentősebb terrortámadások vagy akár az Iszlám Állam elleni küzdelem közös célja. A 2015-től tömegessé váló Európába irányuló illegális migráció szintén újabb prioritásváltozást jelentett a nemzetbiztonsági rendszerekre, amelyeket a jogszabályokban és a szervezeti változásokban is nyomon követhetünk.

Nem feledkezhetünk meg a nemzeti szintű nemzetbiztonsági érdekek érvényesítésének szándékáról és annak eltérő képességeiről sem, hiszen a dinamikusan változó nemzetközi nagyhatalmi erőegyensúly és az egyes államok regionális és világgazdasági szereplővé válásának céljai mögött joggal feltételezhetjük[12] a nemzetbiztonsági szolgálatok munkáját is.

[12] Ma már szakértők hívják fel arra a figyelmet, hogy például a 2016-os amerikai választásokba történt feltételezett orosz beavatkozás lehetősége kapcsán a korábbi hidegháborús ellenféllel szembeni nemzetbiztonsági figyelemcsökkenés hiba volt az Amerikai Egyesült Államok részéről. 2019 szeptemberében R. James Woolsey a már korábban idézett, a Szovjetunió felbomlását követően tett mondását kiegészítve jelentette ki: „Úgy tűnik, hogy a sárkányt mégsem ölték meg […] Sebesült és dühös." (szerzői fordítás) Green (2019): i. m.

Kooperáció

Globalizálódó világunkban a (nemzet)biztonság szükségszerű együttműködésre kényszerül az őt körülvevő, rá hatást gyakorló környezettel. Szervezetei, képességei, nyílt és titkos módszerei, a működés jogszabályi keretei, valamint kapcsolatrendszere a külső környezetben végbemenő változásokra reagálnak. A biztonság területén látható egymásrautaltság felvetette a nemzeteken túlmutató közös gondolkodás, az együttműködés és az információk megosztásának szükségességét. Gondolhatunk itt a már évtizedek óta meglévő, eltérő tagságot felölelő titkosszolgálati együttműködési formákra (például a Five Eyes[13] együttműködés, Berni Klub[14]), de idesorolhatók az elmúlt évtizedekben létrejött intézményesített együttműködési formák. Ezek egy része a terrorizmushoz kapcsolódó információmegosztást szolgálja, elfogadva azt, hogy az együttműködésekben érintett nemzetek egyéb hírszerzési területei a tagállami szuverenitás, a nemzeti érdekek érvényesítése és védelme érdekében működnek.

Az együttműködés jelentősége tehát vitathatatlan, de értelemszerűen korlátozott, hiszen a nemzeti hírszerzés területén keletkező információk alkalmasak lehetnek az adott ország érdekével ellentétes befolyás vagy előny megszerzésére, továbbá a nemzetbiztonság hatékonysága az alkalmazott módszereik, forrásaik kikerülésével csökkenhet.

Az együttműködések a nem biztonsági jellegű szervezetek, így a piaci szféra egyéb szereplői irányába is teret nyertek. Példaként az infokommunikációs területek mögött meghúzódó vállalati környezet emelhető ki, hiszen a korszerű technológiák és megoldások fejlődése megállíthatatlanul folytatódik. Szinte naponta szembesülünk új és újabb eszközökkel, megoldásokkal, amelyek már komplex módon integrálják a korábbi kommunikációs platformok széles eszköztárát, és átfogó módon képesek többek között az információk létrehozására, továbbítására, értelmezésére és feldolgozására. A változások már közvetlenül hatnak a nemzetbiztonsági szolgálatokra is, hiszen a munkájukhoz elengedhetetlen információk jelentős része ebből a „technológiaorientált" környezetből származik, így e kapcsolatrendszerek is nélkülözhetetlen módon beépültek a szolgálatok eszköztárába.

[13] Az Amerikai Egyesült Államok, az Egyesült Királyság, Ausztrália, Kanada és Új-Zéland részvételével megvalósuló technikai jellegű hírszerzési együttműködés.

[14] 1971-ben létrehozott, az Európai Unió, Norvégia és Svájc biztonsági és hírszerző szolgálatai vezetőinek részvételével megvalósuló informális titkosszolgálati fórum.

A kibertér meghatározó szerepe

Az internet térhódítása alapvető gazdasági, társadalmi változásokat eredményezett, életünk számos része költözött át a korábban ismeretlen virtuális térbe. Annak gondolatát követve, hogy a nemzetbiztonsági szolgálatok feladatrendszere és lehetőségei elválaszthatatlanok az információ- és kommunikációtechnológiai változásoktól, mindez a nemzetbiztonsági szféra oldaláról különös jelentőséget kap. Egyrészről a rendszerek védelme (kiberbiztonság), másrészről a sajátos információgyűjtési, törvényes ellenőrzési képességek (például lehallgatás) biztosítása terén. Az infokommunikációs felületeken habár továbbra is meghatározó az elektronikus úton továbbított szóbeli kommunikáció (például telefonbeszélgetések), egyre inkább átveszik a szerepet az üzenetek továbbításának fejlődő új megoldásai. A változások közvetlenül érintik a nemzetbiztonság információgyűjtési területeit, hiszen a kibertér olyan közeggé vált, ahol a globális IKT-környezetnek köszönhetően informatikai programokkal megvalósítható a másokról (egyének, csoportok, országok) történő információk megszerzése. A határok IKT-környezetben történő „elmosódásával" ugyanakkor adataink, rendszereink az idegen állami és nem állami szereplők irányából érkező támadásokkal szemben egyre inkább védelmet igényelnek (kiberbiztonság).

Az elmúlt évek e témakörrel foglalkozó szakirodalmai is kiemelik, hogy az ezredforduló óta bekövetkezett robbanásszerű technikai-technológiai változások egyre több kihívás elé állítják a nemzetbiztonságért felelős szerveket. Hatásuk mind a hagyományos értelemben vett elhárítás, mind a hírszerzés oldalán érezhető. Az elhárítás oldalán új védelmi (kiberbiztonsági) koncepciók születését láthattuk, valamint a nemzetbiztonsági szervezeteken túlmutató, az állam és a társadalom egyéb szereplőit is felölelő, széles körű kiberbiztonsági jogszabályok és stratégiák készültek. Mindezek jól jelzik a biztonsági szempontok nemzetközi szintű együttműködéseket igénylő kialakításának szükségességét, a kibertérből érkező támadások elleni közös fellépés igényét. Az elmúlt években a NATO vagy akár az EU szintjén átfogó előírások, követendő irányelvek és a közös erőfeszítéseket támogató szervezetek jöttek létre.

A kibertér nemzetbiztonsági megközelítését tovább nehezíti, hogy napjainkra a kibertérben is leképeződtek azok a „biztonságot fenyegető" területek, amelyek hagyományos értelemben is megtalálhatók a társadalomban, illetve a biztonságpolitikai környezetben. Gondoljunk egyszerűen a bűnözés kibertérben megjelenő formáira, az ipari kémkedésre, a terroristaszervezetek jelenlétére és toborzótevékenységére, a nemzetközi szintű, embercsempészethez köthető

szervezett bűnözői körök tevékenységére, de idesorolhatók az állami szereplők által támogatott kibertámadások, illetve hírszerzési tevékenységek. Ezen elemek – ahogy a társadalom működésének hagyományos színterén – gyakran szorosan kapcsolódnak egymáshoz, így elválasztásuk alapvetően nem a kibertérben jelentkező eszközök típusában, hanem azok alkalmazásának céljaiban (például katonai, nemzetbiztonsági, bűnözői, terrorizmushoz köthető) keresendők.

Új nemzetbiztonsági struktúrák

A szervezeti változások ok-okozati tényezőként a nemzetbiztonság esetében is gyakran valamilyen rendszert érő hatás eredményeként kerülnek előtérbe. Az elmúlt évtizedeket tekintve a feladatok prioritásváltozása kapcsán kiemelhető a terrorizmus elleni küzdelem, amely önmagában is új szervezetek létrehozását eredményezte. További megoldandó feladatot a táguló információs közegből egyre nagyobb számban érkező adatok, információk elemzése és értékelése jelentett, amelyre a választ a fúziós szervezeti forma adhatta. Létrehozásuk az összetett biztonsági problémák kezelését támogató, katonai, civil, nemzetbiztonsági és rendészeti jellegű látásmód koncentrációjaként is értelmezhető. Már egy évtizede a NATO hírszerzési struktúrájában is nyomon követhető a polgári és katonai nemzetbiztonsági gondolkodás közeledése. Mint később még kitérünk rá, 2006-ban létrehozták a Hírszerzési Fúziós Központot (*NATO Intelligence Fusion Center,* NIFC),[15] majd 2017-ben a NATO hírszerzésének legjelentősebb reformjaként felállították a katonai és polgári hírszerzési területének, illetve a NATO Biztonsági Irodájának (*NATO Office of Security,* NOS) a bevonásával a NATO Közös Hírszerző és Biztonsági Osztályát (*Joint Intelligence and Security Division,* JISD).[16]

[15] Lásd Kis-Benedek József: A nemzetbiztonsági szolgálatok nemzetközi együttműködése. *Hadtudomány,* 23. (2013), 1–2. 110.

[16] Arndt Freytag von Loringhoven: Adapting NATO Intelligence in Support of "One NATO". *NATO Review,* 2017. szeptember 8; Arndt Freytag von Loringhoven: A new era for NATO intelligence. *NATO Review,* 2019. október 29.

A nemzetbiztonság humán és technikai területeinek egyensúly(talanság)a

A szakirodalmakban gyakran előtérbe kerül azon elméleti kérdésfelvetés, miszerint a humán vagy technikai nemzetbiztonsági területek lesznek a jövőben meghatározók. Igaz, számtalan megközelítéssel találkozhatunk, de fontos hangsúlyozni, hogy szerepük mindig a külső környezetben zajló biztonságpolitikai folyamatok sajátosságai mentén értelmezhetők. Amíg például a technikai úton történő információgyűjtés elsődlegességére a 2013-as[17] és 2017-es[18] botrányok, addig a tömeges illegális migráció jelensége az emberi tényező, valamint az IKT-megoldások komplex formáló hatásaira hívták fel a figyelmet, és a technikai területek mellett a humán képességek nagyarányú fejlesztését gyorsították fel. Ebben a tekintetben még a terrorizmus jelenségénél sem húzható éles határvonal, hiszen amíg az al-Káida a technikai jellegű kommunikációs csatornák helyett az információtovábbítás emberi elemeire helyezte a hangsúlyt, addig az Iszlám Állam esetében kiemelt szerepet kaptak az internet biztosította lehetőségek. Egyes prioritássá váló biztonságpolitikai veszélyek tehát sajátosságukból adódóan befolyásolják a kérdéskört, gondoljunk csak a Covid–19-világjárvány azonnali hatására, az emberek közötti kontaktusok számának csökkenésére *(social distancing)* és a kommunikáció kibertérbe és egyéb elektronikus platformokra történő áthelyeződésére. Anélkül, hogy bármelyik mentén is állást kellene foglalnunk, bátran állíthatjuk, hogy mindkét területnek a jövőben is helye lesz a szervezetek képességei és alkalmazott módszerei között, amelyek azonban csak egymást támogatva, kiegészítve lehetnek sikeresek.

Nem hagyhatjuk ugyanakkor figyelmen kívül a kibertér rendkívül meghatározó, átfogó jelentőségét, amely a jövőben szinte minden, így a humán típusú nemzetbiztonsági tevékenységekhez kapcsolódó gondolkodást is alapvető módon fogja befolyásolni. Igaz, számos humán jellegű titkosszolgálati módszer napjainkban és a történelemben visszatekintve ugyanazon emberi tulajdonságokon alapul, azonban ahogy a társadalom tagjai közötti kapcsolatok áttevődnek a kibertér világába, ugyanúgy megjelennek az ehhez köthető titkosszolgálati megoldások is. A fejlődés,

[17] Az E. Snowden nevéhez kapcsolódó, Amerikai Egyesült Államok Nemzetbiztonsági Ügynöksége (*National Security Agency,* NSA) által végzett globális információgyűjtési programok titkos dokumentumainak nyilvánosságra hozatala.

[18] A 2010-ben a WikiLeaks oldalon (Bradley Manning közlegény) tettek közzé több százezer titkos dokumentumot, majd a 2013-ban kirobbant „Snowden-botrány" után 2017 márciusában a WikiLeaksen újabb jelentős kiszivárogtatás történt.

illetve a külső környezethez való igazodás tehát minden területen – legyen az a hírszerzés vagy akár az elhárítás hagyományos területe – megállíthatatlan, és folyamatosan módosulni fog a nemzetbiztonsági szolgálatok által alkalmazható technikai és humán információgyűjtési megoldások köre. Ezek struktúrák és jogszabályok általi lekövetése már napjainkban is számos ponton látható.

Tömeges adathalmazok megjelenése

A társadalom információs térben folytatott növekvő aktivitása kapcsán napról napra hatalmas adatmennyiségek halmozódnak fel akár az üzleti, akár az állami szférában. Ezen adatok lehetővé teszik, hogy azokat célirányosan felhasználva társadalmunkat jobbá tevő új megoldások jöhessenek létre. Századunkra az információk megszerzéséhez köthető „titkosszolgálati privilégium" is megszűnt, hiszen a technikai fejlődés eredményeként lehetővé vált az információkhoz való szabad hozzáférés. Korábban nem látott tevékenységeket „digitalizáltak", és az így születő adatbázisok lehetővé teszik azok strukturált felhasználását. Olyan adathalmazok jöttek létre, amelyeken keresztül addig soha nem látott mértékben az egyénekhez és társadalmi csoportokhoz köthető viselkedésminták, folyamatok modellezése vált lehetővé. Igaz ez a piaci szereplőkre, akik például az internetes kereséseinkhez kapcsolódóan üzleti információs igényeiket elégítik ki, de igaz olyan megoldásokra is, ahol az adatokra épülő alkalmazásokkal mindennapjaink válnak egyszerűbbé (például tömegközlekedés, parkolás, útvonaltervezés, kamerarendszerek), vagy éppen biztonságunk növelését szolgálják.[19] Az interneten végzett keresések például közvetve információkkal szolgálnak az egyén szokásaira, életvitelére vonatkozóan, de politikai irányultságát is jelezhetik, magában hordozva annak befolyásolási lehetőségét[20] is.

[19] Ilyen megoldásként értelmezhető például a Covid–19-járvány kapcsán a fertőzöttek mozgását és kapcsolatait feltérképező alkalmazás kidolgozása, például Csehországban, Izraelben, míg hazánkban vagy akár Tajvanon a karanténkötelezettség betartásának ellenőrzéséhez használják a rendelkezésre álló helymeghatározási adatokat.

[20] A technikai rendszerek széles körű alkalmazása kapcsán fontos megjegyezni, hogy a felhasználók adataikat önmaguk szolgáltatják ki a sajátos bizalommal felruházott globális infokommunikációs szolgáltatók felé. Azzal, hogy az egyének önmaguk tudatosan tesznek ki adatokat, osztják meg geolokációs helyzetüket (vagy éppen az egyes alkalmazások szereznek meg róluk – akár tudtuk nélkül – lényegtelennek tűnő információkat), lehetővé teszik, hogy felállítható legyen egy adott személy személyiségi profilja, megállapítható legyen érdeklődési köre, vásárlási szokásai, sőt politikai preferenciái.

Az adatok tömeges megjelenése kapcsán egyre fontosabbá válik azok elemzésének gyors képessége, ahol a mesterséges intelligencia rohamosan terjedő alkalmazásaival találkozhatunk. Széles körűvé váltak az anonimizált, tömeges adatokban rejlő kutatási lehetőségek,[21] és a jövőben ezek várhatóan új és újabb eredményeket jelenthetnek a biztonság különböző területein (így a kiberbiztonság vagy akár a bűnüldözés területén, ahol már vannak olyan országok, amelyek az adatok online feldolgozásával próbálják meg előre jelezni egy-egy bűncselekmény területi esélyét). A technológiai fejlődés révén keletkező adattömegek már eddig is új kutatási irányokat alapoztak meg az adattudományok területein, különös tekintettel az információk feldolgozhatóságára, értelmezhetőségére és felhasználhatóságára.

Nemzetbiztonsági értelmezésben mivel a megszerzett információk valamely magasabb szintű döntés nélkülözhetetlen kezdeti elemét jelentik, így az érintett biztonsági szervezetek az információforrások lehető legszélesebb körét használják. Az úgynevezett összadatforrású információgyűjtés[22] megközelítésétől elvonatkoztatva, a „titkos információgyűjtés" útján szerzett információk vagy akár a nyílt forrásból származó információk mellett a jövőben előremutató lehetőséget hordozhat a nagy mennyiségű, akár személyes jellegű elemektől lecsupaszított információk feldolgozása. Hívószóként talán a strukturált adatok automatizált feldolgozhatósága, az adatok között meghúzódó rejtett kapcsolatok és összefüggések feltárása, vagy akár az adatok nagy tömegéhez kapcsolódó egyfajta előrejelző képesség víziója merülhet fel. Mindez azonban újfajta megközelítést kíván, hiszen Galántai Zoltán hasonlatával élve „a hagyományos és a big datán alapuló megközelítés közötti különbség a vadászok és halászok közötti különbség. Az előbbiek megtehetik, hogy egy konkrét vadra mennek, míg az utóbbiak kivetik a hálójukat, és aztán nincs más dolguk, mint várni, hogy mi akad bele."[23]

Társadalomtudományi értelemben – idesorolva a nemzetbiztonság tudományterület számos elemét – a nemzetközi színtérre kitekintve azt látjuk, hogy az országok egyre inkább figyelembe veszik azokat az „adatosítható" elemeket, amelyeknek nemzetbiztonsági vonatkozásuk lehet. Amíg a külső gazdasági

[21] Az adatokhoz való kutatási hozzáférések országonként jelentős eltéréseket mutatnak, így főként az Egyesült Államokban egyszerűbben elérhető adatkörnyezet okán az amerikai kutatások túlsúlyával találkozhatunk. A lehetőségek bővítése minden bizonnyal a biztonsági területen számos hasznosítható új tudományos eredményt hozhatna.

[22] *All Source Intelligence* – az összes rendelkezésre álló információforrásra épülő (teljes spektrumú) hírszerzés.

[23] Galántai Zoltán: Big data, tudomány, kauzalitás. *Információs Társadalom,* 16. (2016), 2. 38.

környezetben már általánosan elterjedtek a különböző formában és rendszerekben keletkező személyes adatokat nem tartalmazó, metaadatokat felhasználó megoldások, addig a biztonság területein ezek felhasználása minden bizonnyal még jelentős fejlődés előtt áll. Amíg az első esetben az adatok valamely üzleti szereplő rendszerében keletkeznek, és felhasználásuk gyakran nehezen ellenőrizhető, addig a demokratikus államok nemzetbiztonsági szférája esetében – amellett, hogy ezen adatok általánosságban nem saját rendszereikben keletkeznek, és a tevékenység ellenőrizhetősége is biztosítható lehet – a kérdéskör még nem letisztázott. Az adathalmazok (nemzet)biztonsági célú tömeges kutathatósága és prognosztizációs felhasználhatósága is vitákat generálhat, felvetve a megfigyelés társadalmának víziójától való félelmet. Megfelelő technológiák (például mesterséges intelligencia) segítségével azonban ezek egy része minden bizonnyal a biztonság szolgálatába állítható.