Nemzetbiztonság a 21. század elején

Szemben a kihívásokkal

Szerkesztette
Dobák Imre

LUDOVIKA
EGYETEMI KIADÓ

Nemzetbiztonság a 21. század elején

Vákát

Nemzetbiztonság a 21. század elején

Szemben a kihívásokkal

Szerkesztő

Dobák Imre

LUDOVIKA
EGYETEMI KIADÓ
Budapest, 2022

A kutatás az Innovációs és Technológiai Minisztérium mint Támogató által
a TUDFO/51757-1/2019-ITM iktatószámon meghozott támogatói döntése alapján,
az NKFIH-830-8/2019. számú Megállapodásban foglaltak szerint, a 2019. évi Tématerületi
Kiválósági Program céljainak elérése érdekében költségvetési támogatásból valósult meg.

Szerzők
Bács Zoltán György
Csányi Csaba
Dobák Imre
Drusza Tamás
Mezei József
Regényi Kund Miklós

Szakmai lektor
Dr. Szabó Hedvig

A kézirat lezárva: 2020. június

Kiadja a Nemzeti Közszolgálati Egyetem
Ludovika Egyetemi Kiadó
A kiadásért felel: Deli Gergely rektor

Székhely: 1083 Budapest, Ludovika tér 2.
Kapcsolat: kiadvanyok@uni-nke.hu

Felelős szerkesztő: Karácsony Fanni
Olvasószerkesztő: Resofszki Ágnes
Korrektor: Tomka Eszter
Tördelőszerkesztő: Stubnya Tibor

Nyomdai kivitelezés: Pátria Nyomda Zrt.
Felelős vezető: Orgován Katalin vezérigazgató

DOI: https://doi.org/10.36250/00904_00

ISBN 978-963-531-637-3 (nyomtatott)
ISBN 978-963-531-638-0 (elektronikus PDF) | ISBN 978-963-531-639-7 (ePub)

Tartalom

Vákát

Előszó

Tisztelt Olvasó!

Ön a Nemzeti Közszolgálati Egyetem Nemzetbiztonsági Intézetének (NKE NBI) munkatársai által készített kiadványt tartja a kezében. A könyv a 21. század nemzetbiztonsági kihívásainak kérdéseire próbál választ adni. A szerzők között megtalálhatók a nemzetbiztonsági szolgálatok tagjai, írt a kiadványba jogász és terrorelhárítással foglalkozó szakember is. A mű lektora a Nemzetbiztonsági Szakszolgálat főigazgatója volt.

Az első fejezet a nemzetbiztonság 21. századi értelmezésével, annak változásaival és jellemzőivel foglalkozik. A második fejezet szerzői a nemzetbiztonság külső kapcsolatait elemzik, beleértve a biztonságpolitikai környezetet, a jelenkori terrorizmus hatásait, a technológiai környezet változásait és az új generációk nemzetbiztonsági munkába való bevonásának kérdéseit. A harmadik fejezet alkotói rendszerszintű válaszokat próbálnak megfogalmazni olyan területeken, mint a nemzetbiztonsági szervezetrendszer változásai, a kibertérben zajló küzdelem, a humán hírszerzés fontossága és az elemző, értékelő munka 21. századi kihívásai.

A negyedik fejezetben a nemzetbiztonsági kihívásokra adandó sajátos válaszokat fogalmazzák meg a szerzők. A fejezetben a felsőoktatás területén vizsgálják az együttműködés lehetséges formáit, foglalkoznak a biztonságtudatosság fontosságával. Szintén vizsgálják a nemzetbiztonság területére vonatkozó jogszabályok adta lehetőségeket, elsősorban a terrorizmussal, a kiberbiztonsággal, adatvédelemmel kapcsolatban. Ezenkívül részletezik az új technológiák és eljárások nemzetbiztonsági területre vonatkozó hatásait, beleértve a mesterséges intelligencia fejlődését és az automatizálásból adódó lehetőségeket.

A kiadvány alkotói hatalmas mennyiségű hazai és külföldi szakirodalmat dolgoztak fel a mű elkészítése során. A hivatkozott alkotások között közel 150 könyv, könyvfejezet, folyóiratcikk, számos jogszabály és internetes hivatkozás található.

Ajánlom a könyvet azoknak, akiket érdekel, hogyan is alakulnak a nemzetbiztonsággal kapcsolatos kérdések a 21. században, azoknak, akik a nemzetbiztonság területén dolgoznak, valamint a biztonság jelenlegi és jövőbeli kérdései iránt érdeklődőknek. Javaslom a kiadvány tanulmányozását az NKE NBI hallgatóinak.

Dr. Boda József nb. vezérőrnagy (ny.)

Vákát

A NEMZETBIZTONSÁG FOGALMI KERETE

Vákát

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/10.36250/00904_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.

Vákát

A KÜLSŐ KÖRNYEZET ÉS A NEMZETBIZTONSÁG KAPCSOLATA

Vákát

A külső biztonságpolitikai környezet és annak komplexitása

Bács Zoltán György

Minden társadalomban vannak és elkerülhetetlenek a belső érdekellentétekből, vélemény- és világnézeti, kulturális és vallási különbségekből, a társadalmi csoportok egyedei szocializációs hátteréből adódó súrlódások, esetleg konfliktusok. Ezeknek mint a belső nemzetbiztonsági környezet elemeinek figyelemmel kísérése, a veszélyes összefüggések és jelenségek feltárása, illetve részben kezelése – más államigazgatási szervek mellett – a nemzetbiztonsági struktúrák feladatkörébe tartozik. A nemzetbiztonsági környezet két ponton válik külsővé:

- amikor a nemzetbiztonsági helyzetünkre bármilyen hatást gyakorló, kihívást, kockázatot vagy fenyegetést jelentő események következnek be;
- amikor a magyarországi joghatósággal meghozott döntéseket más államok mint saját nemzetbiztonságukra nézve kihívást, kockázatot, illetve veszélyt jelentő tényezőt értékelik.

Mindkét esetben elengedhetetlen ezeknek a tényezőknek a feltárása, azonosítása, elemzése és értékelése ahhoz, hogy a megfelelő – szakmai vagy politikai szinten – döntést lehessen hozni.

Az összefüggések jellegéről

„Minden összefügg mindennel." A megállapítás irodalmi megerősítését Bulgakov *A Mester és Margarita* című művében[1] is megtaláljuk, de szívesen idézik az összeesküvés-elméletek hívei is. Az, hogy az események, azok ok-okozati összefüggéseinek kiterjedése az időben és a térben, vagyis az események a mérhető idő vonalán és földrajzilag is meghatározható helyen, egyre összetettebb, sokrétű és sokszintű kapcsolatban állnak, a globalizáció körülményei között nyilvánvaló. Ennek alapján célszerű megvizsgálni, melyek azok a nagyobb összefüggési hálózatok, amelyek hazánk nemzetbiztonsági helyzetére hatással vannak, vagy lehetnek.

[1] Lásd Mihail A. Bulgakov: *A Mester és Margarita.* (Ford. Szőllősy Klára.) Budapest, Európa, 2019.

https://doi.org/10.36250/00904_02

Ha a tényezőket egy amorf, fizikai paraméterekkel nem rendelkező, virtuális térbe helyezett mátrix hálózati elemeiként szemléljük, akkor az elemek közötti közvetlen és közvetett összefüggések, az azokból következő további események mint következmények idővonalra helyezve adhatnak képet az adott jelenség – gyakorlatilag bármelyik jelenség – okairól, előzményeiről, ezek időrendjéről, közvetlen vagy közvetett, tetszőleges irányú kihatásáról.

Figyelemre méltó, hogy bármelyik szintű, tehát globális, regionális, interregionális vagy helyi jelenség levezethető a felette álló szinteken végbement, összetett változások következményeként. A globális jelenségek pedig az alsóbb szinteken jelentkező, „utójelenségek" vagy „következményjelenségek" lépcsőzetes, szintenként felfelé haladó, kumulált hatásaként, valamint a jelenségeket kiváltó döntéshozatali tényezőknek a kumulált hatásra hozott válaszintézkedéseiből táplálkozva, körforgásszerűen alakulnak ki.

A nemzetbiztonsági környezetre ható tényezők

Klimatikus változások és hatásuk

Az utóbbi évtized meteorológiai adatai azt mutatják, hogy különböző okokra, így a szén-dioxid-kibocsátás növekedésére, illetve az üvegházhatás erősödésére visszavezethetően, folyamatos a Föld atmoszférájának, a világtengerek és beltengerek vizeinek felmelegedése. Ennek egyenes következménye a nagy tömegek számára alapvető ellátást biztosító haszonnövények termőterületének megváltozása, eltolódása épp a felmelegedés miatt. Tudományos vizsgálatok szerint „1992 és 2017 között 6400 milliárd tonna jég tűnt el. A mérések kezdetén még csak évi 81 milliárd tonna jég olvadt el, ami a 2010-es évekre évi 475 milliárd tonnára nőtt. Mindez elég volt ahhoz, hogy 17,8 milliméterrel megemelkedjen a globális tengerszint, ami több part menti áradást és eróziót okoz."[2] Sok növény hőtűrő képessége csak bizonyos területeken teszi lehetővé azok termelését, így a talaj nedvességtartalmának, összetételének, a környezet általános hőmérsékleti paramétereinek megváltozása alapvetően befolyásolja a haszonnövények termelését és az állattenyésztést. Az természetes, hogy amennyiben egy országban a klimatikus változások miatt élelmiszertermelési válság következik be, ennek kezelése

[2] Tóth Balázs: Hatszorosára gyorsult a jégtakarók olvadása. *Index,* 2020. március 12.

már nem pusztán gazdasági kihívás, hanem kifejezett nemzetbiztonsági kockázati tényező, amelynek kezelése komplex, nem csak gazdasági intézkedéseket igényel.

Ugyanilyen hatást vált ki, ha a tengerparti, sűrűn lakott városok egyes részei – elsősorban a gazdaságilag, politikailag és társadalmilag is folyamatos válságjelenségekkel, konfliktusokkal küzdő ázsiai és afrikai országokban – időközönként vagy folyamatosan víz alá kerülnek. Az elmúlt évek tapasztalatai azt mutatják, hogy a tengeri és folyami áradások intenzitása megnőtt, a korábban tapasztalt vízmennyiség többszöröse hosszan tartó, elhúzódó gazdasági, társadalmi veszélyhelyzetet okozott, az árvizek, cunamik, tornádók és hurrikánok halálos áldozatainak száma jelentősen megnőtt. Nyilvánvalóvá vált, hogy a korábbi időszakban érvényes építési előírások alapján épített szerkezetek, lakó- és kereskedelmi ingatlanok, közlekedési infrastrukturális létesítmények, védművek a megváltozott terhelést – szél- és víznyomást, statikai problémákat – már nem tudják elviselni.

Nem kell különösebben magyarázni, hogy a katasztrófa sújtotta területeken az államigazgatási intézmények működtetése is ellehetetlenülhet, azt csak a különleges jogrend körülményei és jogszabályi feltételei között lehet fenntartani. Bármilyen hasonló helyzet rendkívül súlyos biztonsági és nemzetbiztonsági, valamint rendészeti és rendvédelmi kihívás. Ennek oka, hogy ilyen helyzetekben bármilyen indíttatással fellépő, de az adott jogi igazgatási rendszert megkerülő vagy konkrétan az ellen fellépő, akár spontánul létrejövő csoport a helyzet miatt gyors radikalizációs folyamatot indíthat el, amelynek puszta megjelenése és tevékenysége is nemzetbiztonsági kihívás, illetve kockázat lehet. Az ilyen öntörvényű vagy öntörvényűnek látszó magatartás esetleg nehezen kezelhető és könnyen átcsaphat csoportos, szervezett vagy spontán erőszakcselekményekbe. Ezek célja, hogy az igazgatásban, ellátásban, szolgáltatásokban felmerülő nehézségeket, anomáliákat saját eszközökkel esetleg személy, személyek vagy csoportok elleni erőszakkal oldják meg. Az ilyen, régóta lappangó, mélyen gyökerező, összetett politikai, gazdasági és társadalmi aránytalanságok miatt felhalmozódott feszültségek esetében a közigazgatási, ellátási, szolgáltatási és rendvédelmi funkciók zavarai nem okai az erőszakos megnyilvánulásoknak, csak kiváltják azokat. Ez viszont már meghaladja a nemzetbiztonsági kockázat szintjét, ez már komoly veszély, hiszen a cselekmények célja a kormányozhatóság eszközeinek, a közigazgatási intézményeknek a támadása vagy rábírása bizonyos intézkedések megtételére vagy meg nem tételére az erőszakcselekmény vagy annak végrehajtásával történő fenyegetés hatására. Ezek a szavak már ismerősek: a terrorizmus szinte valamennyi meghatározásában megtalálhatók.

Társadalmi tényezők

Egyes régiókban, leginkább a migrációs célországokban mint befogadó államokban az aktív, munkaképes lakosság számának csökkenése, a társadalmak elöregedése egy sor hátrányos, tartós intézkedést tesz szükségessé. Ilyen például az öregségi-nyugdíj-korhatár hazánkban is előre látható kényszerű emelése, abból a célból, hogy a nemzeti összetermék, illetve a gazdasági fejlődés ne csak fenntartható, de folyamatosan növelhető is legyen. Ebben maguk az öregséginyugdíj-korhatárt elérők és a már nyugdíjas korúak is érdekeltek, mivel az ellátottak körének bővülése mellett a rendelkezésre álló nyugdíjalap változatlan vagy csökkenő nagysága esetén nyilvánvalóan az egy főre eső nyugdíj nagysága is csökken. A nemzeti össztermék előállításában részt vevő, egyre nagyobb és összetettebb szakképzettséget igénylő új munkavállalók munkába állítása – az igényelt felkészültség miatt is – folyamatosan akadozik.

Egyre gyakoribb, hogy a szakképzett munkaerő hiánya, a pótlás lassúsága, a szakképzettséggel szemben támasztott alapvető felkészültségi követelmények és a végzettség minőségi kritériumainak kényszerű csökkenését eredményezi, azzal a szándékkal, hogy az alacsonyabb kvalifikációjú munkavállalók képzését a munkavégzés mellett megoldják. A magas nemzeti össztermék alapján a korábban magas életszínvonalat, fejlett szociális hálót biztosító országok gazdasági eltartóképessége is csökken, ami a hátrányos helyzetű régiókból érkezők tömeges befogadása miatt újabb és intenzívebb társadalmi konfliktusokat gerjeszt. Ezek az újabb, vitára, súrlódásra alkalmat szolgáltató, potenciálisan konfliktusgerjesztő tényezők – amennyiben a csökkentésükre, megszüntetésükre szolgáló intézkedések késnek vagy elmaradnak – fokozatos radikalizálódáshoz vezethetnek.

Az eltérő kultúrájú csoportok eltérő társadalmi elfogadottsága miatt etnikai, vallási konfliktusok bontakozhatnak ki, amelyek csak súlyosbítják a többségi társadalom belső konfliktusait a befogadandókkal kapcsolatban. A helyzet még súlyosabb, ha a befogadó társadalmat is régebben gyökerező etnikai, vallási ellentétek osztják meg folyamatosan. A befogadásban reménykedők, menedéket keresők marginalizált helyzete, a felzárkózás objektív és szubjektív akadályai elősegíthetik a radikalizációt.[3] A marginalizálódás növekedése, az ebből adódó munkaerő-

[3] A felzárkózás objektív akadályaihoz sorolhatók például a megfelelő intézmények hiánya, az oktatók, nyelvet ismerő segítők hiánya, az anyagi-technikai háttér hiánya, a szükséges források hiánya, a meg nem kerülhető döntések elmaradása stb. Szubjektív akadály, ha a potenciális befogadó közeg, társadalmi réteg, csoport elutasítja a befogadandókat, illetve ha a befogadandók utasítják el a beilleszkedéshez szükséges magatartásformák elfogadását.

piaci leszakadás, ha csak kismértékben is, de a fejlődő társadalom színvonalához viszonyított életminőségben is megjelenő különbség egy újabb tényező, amely óhatatlanul erősítheti a radikalizálódást, illetve a bűnözés szervezett formáinak meghonosodását, ideértve a kábítószer-bűnözést, illetve a terrorizmussal szorosan együttműködő nemzetközi szervezett bűnözést is. Nem kell hosszan keresni az összefüggéseket, hogy a felsorolt tényezőknek milyen jelentőségük van a nemzetbiztonság szempontjából, illetve mekkora hatással vannak a külső környezet alakulására, következésképpen milyen új feladatokat jelentenek a nemzetbiztonsági struktúráknak.

Demográfiai tényezők

Ha az előbbiekben a klimatikus változások alapján mutattuk be a külső nemzetbiztonsági környezetben komplex kockázatok megjelenési lehetőségét, most egy másik, rendkívül komolyan veendő tényezőcsoportot vizsgálunk meg. Az úgynevezett jóléti társadalmak egyik jellegzetessége a munkaképes és gazdaságilag aktív lakosságcsoport csökkenése, a társadalom elöregedése. Ennek velejárója a társadalmi össztermék előállításában részt vevők számának csökkenése, amelyet a belső erőforrásokra támaszkodó innováció, valamint az egyre nagyobb szerephez jutó mesterséges intelligencia (MI) mellett a külső, nem az adott országban született munkaképes csoportok bevonásával, képzésével és integrálásával lehet ellensúlyozni. Amennyiben ez a folyamat harmonikus keretek között megy végbe, a társadalmi eltartóképesség egyensúlyban marad, sőt növekszik. A harmonikus körülmények fenntartása nemzeti biztonsági érdek.

Ezzel párhuzamosan, a klimatikus változásokkal is sújtott ázsiai, afrikai és latin-amerikai térségben relatív túlnépesedés tapasztalható, amely helyi gazdasági, társadalmi okainak vizsgálata nem témája jelen fejezetnek. A túlnépesedés relativitását az jelenti, hogy az érintett országok egy főre vetített társadalmi összterméke csökken, illetve nem követi, vagy csak lassan a népesség abszolút növekedését, ideértve a helyi gazdasági és kényszermigrációban részt vevőket is. A társadalmi eltartóképesség nyilvánvalóan csökken, az amúgy sem igazán fejlett ellátórendszerek és közintézmények – egészségügy, oktatás, élelmiszerellátás, szociális ellátás, közigazgatás – nem képesek megbirkózni az erőforrásaikat meghaladó igényekkel, elvárásokkal. A társadalmi eltartóképesség romlásával folyamatossá válik az egészségügyi ellátás romlása, a túlnépesedett és súlyosan veszélyeztetett térségekben az ellátás kritikus állapota, az akut betegségek

folyamatos jelenléte, esetenként járványok megjelenése és gyors terjedése, a gyermekhalandóság várható növekedése az egyes régiókban.

A fenti két alapjelenségből következően kialakul és a történelmet végigkíséri a gazdasági vagy megélhetési célú, politikailag alapjában véve közömbös migráció. A politikai közömbösség nem jelenti azt, hogy az önmagában politikailag semleges migráló csoport nem szolgálhatja más érdekcsoportok érdekeit pusztán helyzetével, illetve az ebből fakadó mozgásával. A migráló csoport, legyen az bármilyen származású vagy kulturális gyökerű, tetszőleges helyen szocializálódott entitás, megjelenése, tartózkodása egy vele nem azonos összetételű és eltérő szocializációjú közegben könnyen politikai viharok középpontjába sodorhatja a legjámborabb csoportot is. Ez a folyamat már alapesetben is nemzetbiztonsági kihívást, de inkább kockázatot hordozhat, vagyis a külső nemzetbiztonsági környezet elemzésénél és értékelésénél bármilyen csoport célirányos vagy áthaladó mozgását már a lehető legkorábban figyelemmel kell kísérni. A határokon kívüli információ megszerzésében, ellenőrzésében, az információs ciklus első szegmensében nagy szerep hárul a konzuli szolgálatra, illetve valamennyi, kapcsolati hálóval rendelkező külképviseleti szervre.

A gazdaságilag (és más szempontokból is) hátrányos vagy kritikus helyzetben lévő térségekből a természetes, gazdasági, megélhetési migráció célterülete a fejlett szociális hálóval és ellátórendszerekkel rendelkező jóléti társadalmak. Az a tény, hogy a beérkező csoportokból csak egy kisebb csoport jöhet számba mint potenciális munkaerő, komoly megterhelést jelent bármely ország szociális és ellátórendszerének, nem beszélve a társadalmi termelési folyamatból kimaradó csoportok okozta társadalmi feszültségről.

A potenciális befogadó országok irányába a kibocsátó országokból folyamatos, ám változó intenzitású migráció – legyen szó politikai, gazdasági, megélhetési, humanitárius vagy más okokra visszavezethető elvándorlásról – nagyon nehezen előzhető meg. A megelőzést alapvetően nehezíti, hogy a segítségnyújtásra kész országtól, országoktól távol éles társadalmi konfliktusokkal terhelt térségekben zajló folyamatos radikalizáció közepette kell a helyi körülményekhez nem mindig illeszkedő politikai, gazdasági, oktatási és társadalmi eszközökkel elősegíteni az olyan körülmények kialakítását, amely nem generálja, hanem inkább visszafogja a migrációs hajlamot. A kibocsátó országokban történő munkahelyteremtés és a létbiztonság kialakításának erőforrásigénye hosszú időszakra – esetleg évtizedekre is tehetően – rendkívül magas, rentabilitása negatív, az ott alkalmazott pénzügyi, gazdasági, ipari, oktatási, képzési és munkaerőpiaci befektetések hosszú ideig nem profitképesek. Ez önmagában is negatív hatást gyakorol több

potenciális befogadó, de segélynyújtásra képes és hajlandó ország gazdaságára, társadalmára, és ezen keresztül közvetlenül is visszahat a nemzetközi konfliktusmegelőző képességre.

Tekintettel arra, hogy a migrációs folyamat mint nemzetbiztonsági kockázat jelentős erőket köt le, így még a kibocsátó országban hozott megelőző intézkedések esetén is a teljes költséghez feltétlenül hozzá kell számítani a potenciális befogadó célországon belüli konfliktusmegelőzés és konfliktuskezelés primer és szekunder költségeit. Nyilvánvaló tehát, hogy a rövid idő alatt kifizetendő rendészeti, idegenrendészeti, nemzetbiztonsági szükségletek és költségek fedezése, illetve a hosszú távú megoldás érdekében mozgósítandó erőforrások jelentősen terhelik a társadalmi-gazdasági fejlődésre, fejlesztésre fordítható forrásokat, tehát hatása a társadalmi-gazdasági össztermék csökkenése, illetve a bővített újratermelésének, a GDP növekedésének akadályozása.

Gazdasági tényezők

A makrogazdasági, világgazdasági tényezők egy része folyamatosan a sajtó figyelmének központjában van. Ami viszont a makrogazdasági, világgazdasági tényezőkön kívül esik, az a mikrogazdasági szintje a gazdaságnak. Ez a szint, ahol a társadalmat alkotó rétegek és csoportok számára legfontosabb műveletek zajlanak: áruk cserélnek gazdát, szolgáltatásokat vesznek igénybe, banki műveleteket hajtanak végre. Ebből következően a mikrogazdasági szinten bekövetkező bármilyen változás, akár az árképzésben, akár az ár-érték arányban, akár az árak adótartalmában, a nemzetközi elszámolásokban és banki műveletekben használt árfolyamokban, azonnal jelentkezik a lakosság körében. Ez az a szféra, ahol a változásokra legérzékenyebb kis- és középvállalkozások működnek, amely közvetlen, szinte napi kapcsolatban van a lakosság széles rétegeivel, vagyis adott esetben hangulat-, illetve véleményformáló szerepet is betölthet.

A kis- és középvállalkozások kitettsége, sebezhetősége mind rendészeti, rendvédelmi, mind pedig nemzetbiztonsági szempontból nyilvánvaló. Könnyen beilleszkednek a lakossági környezetbe, ezért fontos szerepet játszhatnak a nemzetbiztonsági szempontból veszélyes kapcsolattartásban a bűnözői csoportok, a nemzetközi szervezett bűnözés és a terroristahálózatok hálózati személyei között. Szerepük a pénzmosásban, a terrorfinanszírozásban is megkerülhetetlen, tevékenységük során folyamatosan információhoz jutnak a megbízóik számára fontos körülményekről. Tevékenységük, mozgásuk, kapcsolatrendszerük legális

lábakon is áll. Az ilyen „kettős hátterű" (legális tevékenységet folytató, de bűnözői körökhöz kötődő) vállalkozások hatása a tevékenységi területükön hatással lehet az élet sok területére. A jogszerűen működő vállalkozások szakmai kamaráinak helyzetét és kapcsolatait felhasználva, érdekeiket szakpolitikai szinten is érvényesíthetik, sőt a lakossági kapcsolataik révén még az önkormányzati választásokra is hatással lehetnek.

Politikai tényezők

Ha a politikai tényezőket kezdjük elemezni, komoly kihívással találjuk szemben magunkat. A globalizációs folyamatok felgyorsították a különböző térségekben zajló politikai változások hatásainak terjedését más világrészekre és országcsoportokra. Ennek egyenes következménye a jobb, magasabb szintű és hatékonyabb nemzetközi együttműködés igénye. A 20. század utolsó évtizedei és a 21. század első két évtizede számos fájdalmas példával támasztotta alá a fenti kritériumoknak eleget tevő nemzetközi összefogás szükségességét – több más terület mellett – a terrorizmus elleni harcban.

A terrorizmus elleni harc

A nemzetbiztonság külső körülményei között a 20. század utolsó évtizedeitől kezdve növekvő szerepet játszott az iszlám dogmatikájával leplezett, de valójában politikai tartalmú és célú terrorizmus. Ennek az időszaknak a legjellemzőbb vonása a kíméletlen, lehetőleg tömeges halálos áldozatokkal járó, különböző módokon, eszközökkel és helyszíneken végrehajtott erőszakcselekmény. A terrorizmusellenes nemzetközi összefogásnak és koordinált harcnak köszönhetően a terrorizmus változásra kényszerült. Ezt az alábbi két szóval lehet jellemezni: taktikai paradigmaváltás és diverzifikáció.

A paradigmaváltás jelentősége abban áll, hogy a korábbi, erőszakra és megfélemlítésre alapozott, gyors, agresszív pozíciónyerési taktika helyett egyre nagyobb teret nyer a lassú, csendes területfoglalás. Ennek eszköze a terrorfinanszírozás diverzifikációja, vagyis az, hogy a terrorszervezet vagy -csoport működéséhez, befolyásának fenntartásához, a terrorcselekmények anyagi, technikai és logisztikai előkészítéséhez, valamint a támadások végrehajtásához szükséges anyagi, pénzügyi erőforrásokat egyre több, szerteágazó, nagyon gyakran legális vagy

legális vállalkozással fedett tevékenységből biztosítsák. A diverzifikáció színtere a gazdasági, pénzügyi, kereskedelmi, turisztikai és vendéglátási infrastruktúra, végrehajtói a vállalkozások, a pénzváltótól az emléktárgy- és régiségkereskedésen, élelmiszerüzleteken, szállodákon, utazási és szállítmányozási cégeken keresztül egészen a bankokig, a kulturális, sport-, közösségi és humanitárius szervezetekig. Ezek megjelenése és terjedése, legális vállalkozásokon és szervezeteken keresztül végrehajtott fokozatos és folyamatos behatolása nemcsak a jóléti társadalmakba, de néhány olyan országba is, ahol a gazdasági, társadalmi térnyerést követően jelentős politikai támogatásra is találhatnak, megnöveli a nemzetbiztonsági szervezetek amúgy sem kevés feladatát, hiszen a nemzetbiztonságra negatív hatással lévő szervezet harmadik, sőt negyedik országon keresztül, kívülről is utat találhatnak országunkba.

Belpolitikai tényezők

A politikai válaszokat és megoldásokat igénylő, előbb felsorolt globális klimatikus és társadalmi tényezők, valamint a később még említendő gazdasági tényezők többszörösen összetett, kumulált hatása folyamatos kihívást jelent a kormánynak. Nézzünk egy példát: a klimatikus viszonyok miatti termékszerkezet-változtatás ugyan csak lassan befolyásolja a mezőgazdasági termelést, de a termésátlagok változása, a várható termés és a fogyasztásra, vagyis a lakosság élelmiszerellátásának folyamatos biztosítására, valamint felhalmozásra szánt mennyiségek közötti arány azonnali intézkedéseket tehet szükségessé. Amennyiben a termés a szükségesnél több, úgy kínálatként jelenik meg a felesleg a nemzetközi piacon. Ha a termés szerényebb a vártnál, a hiányt behozatalból kell fedezni, ami a költségvetési előirányzatok átcsoportosításával, a szükséges pénzügyi fedezet megteremtését szolgáló pénzpiaci tevékenységgel is járhat. A fogyasztás növekedése, vagyis adott esetben a különböző okok miatt migráló csoportok ideiglenes vagy tartós befogadása olyan gazdasági erőforrásokat is igénybe vehet, amelyek miatt a lakosság tervezett életszínvonal-emelkedése is veszélybe kerülhet. Valamennyi gazdasági ágban a tervezett folyamatoktól való kényszerű eltérés, amelyet a leggyakrabban külső, általunk nem vagy nehezen befolyásolható tényezők váltanak ki, óhatatlanul a belpolitikai viták kiéleződéséhez vezet. Ezt a helyzetet tovább bonyolítja a politikai ellentét a befogadás vagy be nem fogadás kérdésében, a kulturális kompatibilitás, a vallási tolerancia vagy intolerancia, a szakképzett munkaerő pótlásának nehézségei az iparban, a termelő szférában, a szolgáltatások

sok területén, illetve az ehhez szükséges oktatási-képzési, felkészítési lehetőségek különböző gyengeségei.

Nem egyszerűsíti a helyzetet a más ágazatokban tapasztalható, foglalkoztatást nem találó, felesleges munkaerő okozta feszültség sem. Ezek a nehezen, csak hosszú idő alatt megoldható feladatok ismét csak a radikalizációs tendenciákat erősítik, táptalajt adva újabb szélsőséges nézeteket valló csoportok megjelenésének, a már meglévő csoportok további radikalizálódásához, összefonódásához, a radikalizáció esetleges átfordulásához erőszakcselekményekbe, illetve a társadalom perifériáján élő csoportok spontán vagy rosszabb esetben nemzetbiztonsági kockázatot vagy veszélyt jelentő csoportok által történő, indukált radikalizálásához. A társadalmi feszültségek, súrlódások, konfliktusok dinamikájának megértése, a várható komplex fejlődési irányok értékelése és az egyes lehetőségeket figyelembe vevő forgatókönyvek kidolgozásában való elengedhetetlen részvétel sok szempontból megköveteli a nemzetbiztonsági szervek gyorsabb reagálását, átfogóbb véleményalkotását. Az előbbi gondolatok nem fogják át a társadalmi tudatállapotra ható különböző tényezők valamennyi csoportját, de képet adnak az esetleg távolinak tűnő tényezők egymásra hatásáról, illetve egymásra épüléséről. Ennek a komplex és dinamikus erőviszonyrendszernek a rövid reakcióidejű figyelemmel kísérése, elemzése és értékelése talán korunk egyik legnagyobb szakmai kihívása.

Külpolitikai tényezők

A külpolitikai tényezők azok, amelyeken keresztül a nemzetbiztonság külső környezete a legláthatóbb módon érzékelhető. Hazánk esetében a globális erőviszonyokban tapasztalható bármely rezdülésnek, eltolódásnak komoly jelentősége van, hiszen nemcsak geopolitikai helyzetünk miatt, de kül- és gazdaságpolitikai kapcsolatrendszerünk miatt is a NATO-hoz, illetve az Európai Unióhoz fűződő legszorosabb kapcsolataink mellett jó kapcsolatokra, kiegyensúlyozott viszonyra törekszünk a politikailag és katonailag is szemben álló erőközpontokkal, illetve azok szövetségeseivel. Az elmúlt évtizedekben kialakított kapcsolatrendszerünk, elsősorban gazdasági és diplomáciai érdekeink kiterjednek több olyan országra is, ahol jelenleg hagyományos katonai műveletek folynak.

Ha a globális szembenállás mellett a regionális helyzetre fordítjuk figyelmünket, azonnal nyilvánvalóvá válik a globális ellentétek megjelenése regionális szinten. A vesztfáliai béke után kialakult, a mai geopolitikára is kiható államközi viszonyok során térségünk sajnálatosan mindig a régióközi, más szóval interregionális,

ütközőzónában volt. Térségünk bármely államának belpolitikai hullámzásait a világpolitikában meghatározó szerepet betöltő bármely szereplő – és itt már nemcsak az úgynevezett állami szereplőkre kell gondolni, de a terrort mint érdekérvényesítési eszközt alkalmazó nem állami szereplőkre is – igyekszik kihasználni, pozíciókat szerezni, illetve megszerzett pozícióit megerősíteni. Mindezt folyamatosan, egyes hazai társadalmi csoportok, egyesületek, közösségek körében végzett beépüléssel, támogatással, a kapcsolattartás – és mondjuk ki nyíltan –, a hálózatépítés új formáinak felhasználásával.

Ezeket a kihívásokat csak súlyosbítja a történelmileg megörökölt problémák egész sora, amely folyamatosan terhet jelent néhány szomszédos országgal fenntartott kapcsolatunkban. Ezeket a megoldatlan konfliktusokat bármilyen, fejlődésünkkel, biztonságunkkal ellentétes érdekből könnyű kihasználni, és a valós nemzeti, ezen belül a nemzeti biztonsági és nemzetbiztonsági érdekeink ellen felhasználni. Ebből is látható, hogy az európai térségnek az 1990-es években elkezdődött kitágulása, a gazdasági együttműködés majdnem három évtizedes magasabb szintje ellenére az ezekben rejlő politikai, társadalmi, kulturális lehetőségek kiaknázása még számos kívánnivalót hagy maga után.

A külső nemzetbiztonsági környezet komplexitásának vizsgálata során nem szabad figyelmen kívül hagyni azoknak az országoknak, illetve szervezeteknek a kommunikációs stratégiáját és taktikáját, amelyekkel érdekeink érvényesítése során interakcióba kerülünk. Ez az interakció részünkről lehet passzív, vagyis nem kezdeményezőként lépünk fel, de a másik fél kezdeményezésének célpontja vagyunk, kommunikációs stratégiája részben vagy egészében ránk is irányul. Az aktív interakció amikor mi lépünk fel kezdeményezőként egy kapcsolat kialakításában a másik féllel egyeztetett módon. Ekkor a kommunikációs stratégia kialakítása, az eszközök, módok, fórumok, a kifejezések megválasztása éppen a stratégiailag fontos kapcsolatok érdekét szolgálja a kölcsönösség alapján.

Az ellenséges kommunikációs stratégia forrásainak, eszköztárának, követőinek és továbbítóinak feltárása ugyanúgy a külső nemzetbiztonsági környezet stabilitásának fontos eleme, mint az előbbi bekezdésekben vázolt környezeti, demográfiai, politikai, gazdasági és társadalmi kihívások kezelése. Éppen ezek összefonódása teszi komplexszé a külső nemzetbiztonsági környezetet.

Viribus Unitis, avagy civil-professzionális konvergencia a 21. században

Bács Zoltán György

Nem, ezúttal nem I. Ferenc József osztrák császár és magyar király jelmondatának történelmi örökségéről vagy a Monarchia hasonló nevű csatahajójáról lesz szó. A latin kifejezés ma aktuálisabb, mint eddig bármikor. Jelentése „egyesült erővel" vagy „egységben az erő", az egyetlen észszerű, szakmailag, társadalmilag és politikailag is indokolt, megalapozott koncepcionális válasz a dinamikusan változó, felgyorsult, ezért szinte azonnali válaszokat igénylő, időszerű kihívásokra.

Milyen erőket kellene egyesíteni, és miért?

Egyedül nem megy. Voltak korok, amikor maga a társadalmi, gazdasági, politikai és ezzel egyetemben a védelmi, katonai fejlődés igényelte a teljesen elkülönített szakosodást, az egyes speciális, jól körülhatárolható feladatok rendszeres, ismert struktúrában történő végrehajtását. Példaként említhetők a termelési folyamatok, vagy a társadalom életében alapvető funkciók, mint a szintenként elkülönülő oktatás, az ellátás, a szolgáltatások és természetesen a védelem. Ezek között, ha volt is valamilyen átjárás, az rendkívül korlátozott volt, hiszen az elkülönülő területek más és más fizikai, szellemi és ismereti, valamint eszközhátteret igényeltek, és a tevékenységük helyszíne sem mindig volt azonos.

A funkcionális elkülönülésnek ez a rendszere leginkább a feudális hierarchián keresztül mutatható be, de különböző formáiban jelen volt és van az alkotmányos monarchiákban, az áldemokráciákban, az egyeduralmi, vezetőközpontú rendszerekben, így a fasizmusban, nácizmusban, kommunizmusban és minden olyan politikai, ideológiai rendszerben, ahol az abszolutizált, idealizált állam, illetve annak piedesztálra emelt, félistenként kötelezően tisztelt képviselői voltak az elkülönülésen alapuló rendszerek kedvezményezettjei. Ha a fenti helyzetleírás alapján valakinek a latin „Divide et Impera", vagyis az „oszd meg és uralkodj" elve és az erre épülő gyakorlat is eszébe jut, az nem a véletlen műve.

A merev funkcionális elkülönülés lebontása a társadalmi, gazdasági és tudományos fejlődés előrehaladtával egyre sürgetőbbé vált. Az alkalmazott tudományok mind gyorsabb felhasználása a termelés, fogyasztás, kommunikáció, oktatás,

https://doi.org/10.36250/00904_03

képzés és nevelés világában, illetve az alap- és alkalmazott kutatásoknak a gazdasági stratégiai fejlődésre gyakorolt hatása, vagyis az adott társadalom komplex fejlődése, a fenntartható fejlődés biztosításának igénye katalizálta a tudományterületek együttműködését.

A védelemmel kapcsolatos műszaki és egyéb kutatások a társadalomfejlődés extenzív időszakától – a gyarmatosítás korától gyakorlatilag napjainkig folyamatosan – prioritást élveztek és élveznek. Sok, ezen a területen megjelent újdonság, találmány, megoldás hosszabb-rövidebb idő után a védelmi felhasználás területéről átkerült a polgári alkalmazások közé. Gondoljunk csak a teflon és a titánium alkalmazására! Mindkettő hadiipari célú kutatás eredményeként lett a védelemtechnikai berendezések fontos alkotóeleme.

Az egyes tudományterületek és termelőbázisok merev elhatárolásának, illetve elkülönített irányításának egyik legjobb példája a szovjet hadiipari komplexum, a VPK[1] tevékenysége a hidegháború időszakában. Az 1960-as években a szovjet nemzeti össztermék éves növekedése 4-5% körül volt. Az 1970-es évek elejére ez először 4, majd 3% alá esett vissza, miközben a védelmi kiadások aránya az 1960-as években 12-13%-ról az 1970-es évek végére 13-14%-ra emelkedett.[2] Látható módon a hadiipari komplexum igényeinek kielégítése a szovjet termelési potenciál jelentős részét kötötte le úgy, hogy ebbe beletartozott az olyan polgári célú ipari létesítményekben a védelmi megrendelések teljesítésének ellenőrzése is, mint például egy csokoládégyár, textilgyár. Nagyon sok volt a többcélú termelést folytató üzemek száma is. Ezekben a polgári célú felhasználásra szánt termékek mellett az adott technológiával előállítható, védelmi célokat szolgáló termékeket is gyártottak. Arra is volt példa, hogy a polgári célú termelés mint fedőtevékenység szerepelt a VPK igényeit szolgáló termelés leplezésére. Ilyen volt például a Leningrádi Optikai és Mechanikai Gyár, ahol a filmfelvevők és más optikai eszközök, fényképezőgépek mellett a védelemben és az űrkutatásban, illetve a technikai felderítésben is használatos eszközöket is gyártottak. A védelmi célú berendezések beszerzése az 1970-es évek elején a teljes beszerzés mintegy harmadát tette ki, míg az évtized végére ennél magasabb arányt ért el.[3] A mereven elkülönített szakterületek koordinációja kormányzati szinten valósult meg: a szovjet kormány egyik elnökhelyettese volt felelős a hadiipari komplexumért. A szovjet tervutasításos

[1] Voenno-promislennij kompleksz *(Военно-промышленный комплекс).*

[2] Joint Economic Committee: *Soviet Economy in the 1980's: Problems and Prospects* Part 1. Washington, Joint Committee Print, 1983. 160.

[3] Joint Economic Committee (1983): i. m. 160.

gazdasági rendszer lényegéből adódóan a védelmi költségvetést névlegesen alacsonyan lehetett tartani, mivel a polgári ágazatok költségvetésének egy része is a védelmi célú feladatok teljesítésére szolgált.

Az alacsony katonai költségvetés másik oka a mesterséges árfolyam-szabályozás volt, amely alapján az átszámítások során az 1 dollár egyenlő 0,72 rubellel, ami irreális volt, de a statisztikai adatokban a valós különbséget nem lehetett érzékeltetni, ám a nemzetközi és hazai propagandában jól fel lehetett használni. Az alacsony nominálértékű katonai költségvetés harmadik pillére éppen maga az állami meghatározó szerepe, a tervutasításos rendszer volt. Ennek alapján a kijelölt termelőegységek a meghatározott mennyiséget, a meghatározott határidőre vagy előtte, az előre, a tervekben meghatározott áron (!) voltak kötelesek előállítani és leszállítani.

A szovjet rendszer gazdasági, politikai és ideológiai összeomlása rákényszerítette a védelemgazdaság és irányítás szereplőit, hogy az állami megrendelések és finanszírozás megszűntével először csak eseti, ad hoc jelleggel, később fokozatosan már projektek keretei között hangolják össze kutatási és fejlesztési, valamint tervezési és gyártási technológiai tevékenységüket. Ezzel párhuzamosan jelentősen felértékelődtek a tudományágak határterületein folyó kutatások. Ezek a határterületek egyre nagyobb jelentőségre tettek szert, mivel egyesítették magukban a több tudományágat is átfogó további fejlesztések lehetőségét a többcélú felhasználhatóságot, vagyis a piacképességet. A határterületek kutatásának további haszna is van: racionálisabbá, költséghatékonyabbá teszi a kutatásokat, és megmutatja az egyes eddig külön kezelt tudományágak közötti természetes egymásra épülést, összefonódást, a tudományterületeken is érzékelhető dinamikus komplexitást, a tudományágak és felhasználási területek komplementer jellegét, vagyis azt, hogy kiegészítik egymást.

A szovjet mentalitás ellenpontja természetesen az amerikai gondolkodásmód volt és maradt is. A tengerentúlon a kutatás és fejlesztés önmagában is a piaci törvények szerint folyt, vagyis a gyorsabb, hatékonyabb eredmények bármely területen piacképesebbek voltak a vetélytársaknál. Ennek megfelelően az új eredmények piaci értékesítése, illetve az ebből származó extraprofit volt a kutatások és fejlesztések célja, a további fejlesztések alapja is. A lehetséges külső piacokhoz, vagyis az ország határain túli eladásokhoz természetesen a belső mechanizmusokon, engedélyeztetési eljárásokon keresztül lehetett eljutni. Ezért is volt – és ma is egyszerűbb – az amerikai belső piacot megcélozni és az ott jelentkező igényeket, keresleti réseket kielégíteni. Ez egyaránt igaz a védelmi ipar és a polgári felhasználású termékek és technológiák, illetve a kettős felhasználhatóságú termékek és technológiák esetében. A védelmi termékek és technológiák esetében a piac nagyságát a védelmi

költségvetés különböző fejezetei határozzák meg, illetve a védelmi tárcához allokált egyéb feladatok, amelyekben más tárcák is részt vesznek. Ilyen például az űrkutatás.

Nyilvánvaló, hogy az egyre összetettebb, magasabb színvonalú, nagyobb anyagi és szellemi ráfordítást igénylő, de az aktuális környezetvédelmi, gazdaságossági és takarékossági előírásoknak is eleget tevő komplex rendszerek kidolgozása piaci alapon, vagyis több résztvevős versenyeztetés formájában lehet a leghatékonyabb, leggyorsabb és legtakarékosabb. Ennek több következménye is van. Az egyik, hogy a védelmi iparban meghonosodott technológiákat, és egyes, polgári célra is alkalmazható termékeket, nagyon gyorsan a nem katonai célú felhasználók számára is elérhetővé teszik. Itt talán elég csak a rendkívül nagy amerikai fegyverpiacra gondolni. Hány olyan kiegészítő található ma a sport- és fegyverboltok polcain, amely a katonai vagy rendvédelmi, esetleg a különleges erők eszköztárában jelent meg korábban? A másik következmény, hogy a hagyományos gyártmánytervezési, fejlesztési és kísérleti, valamint gyártási kapacitások központosítása helyett a célfeladatokat, az egyes fázisokat már egyre kevésbé az adott cégen belül hajtják végre, végzik el, hanem inkább projektrendszerben, a szakosodott vállalkozásokkal összefogva, koordináltan, szerződésekben rögzített feltételek mellett oldják meg. A projektet koordináló cég végzi a termék vagy technológia piacra vitelét, legyen szó akár védelmi, akár polgári célú technológiáról vagy termékről.

Van itt valami különleges, számunkra szokatlan. Észre kell venni, hogy a védelmi szükségletek kielégítésében nemcsak állami tulajdonban lévő vagy közvetlen állami irányítás alatt álló cégek vesznek részt, hanem beszállítóként minősített magáncégek is! Gondoljunk csak arra, hogy amikor Samuel Colt megalkotta a forgópisztolyát, azt mint magánszemély, mondhatni magánvállalkozó tette, és utána ajánlotta fel a hadseregnek. A helyzet mára abban változott, hogy a felhasználói oldal által meghatározott paraméterek alapján a potenciális beszállító a saját felelősségére és kockázatára kezd bele a megpályáztatott technológia vagy eszköz kifejlesztésébe, igyekezve jobb eredményeket elérni, mint a versenytársak. Ehhez akár konzorciumot is létrehozhat, hogy a technológia vagy eszköz előállításához szükséges részfeladatokat ezek végezzék el. Mi következik ebből:

- A kutatás és fejlesztés ideje a lehetőségek szerinti legrövidebb.
- Az erőforrások felhasználása megmarad az előírt keretek között, vagy azt csak az észszerűen indokolható mértékben lépi túl.
- A megrendelő igényei komplex módon teljesülnek.
- A nyertes beszállítói konzorcium jelentős piaci részesedéshez jut, és folyamatos profitot termel.

A kutatás, fejlesztés költségeit nem az állami költségvetés fedezi, hanem maga a versenyben részt vevő cég vagy cégcsoport. Az ilyen módon felépített védelmi költségvetés hatékonysága sokszorosan felülmúlja az állami költségvetésre támaszkodó védelmi kutatásokat és fejlesztéseket.

A fentiek alapján világos, hogy amit egyesíteni kell, azok a szellemi, technikai, tudományos és pénzügyi erőforrások, jöjjenek azok a polgári vagy a védelmi szférából. Egyesíteni és célorientált módon struktúrába kell foglalni ezeket az elemeket, minden esetben alárendelve a struktúra vertikális és horizontális szerkezetét a célfeladat jellegének. Ez a struktúra lehet egyedi, amely csak egy projektet szolgál ki, de lehet egy olyan struktúra is, amely több hasonló projektet vagy eltérő projekteket is képes akár párhuzamosan is kezelni. A siker lényege nem a struktúra nagysága, hanem a feladatmegoldás diverzifikálása, a részfeladatok helyes delegálása, átadása más, szakmailag hozzáértő egységnek, intézménynek. Csak a helyesen megszervezett munkafolyamatok hatékony koordinációja segíti elő a megrendelői oldalról meghatározott feltételek teljesítését.

Terrorizmus, aszimmetria és dinamizmus

A civil professzionális konvergenciának a 21. században különös jelentősége van. Az elmúlt évtizedek során globális fenyegetést jelentő politikai, gazdasági, társadalmi, kulturális és biztonsági-nemzetbiztonsági kockázati komplexum jelent meg, amely esetenként eltérő mértékben és formában, de a világ országainak nagy részét megérintette. Ez a terrorizmus. A terror eszközét céljaik megvalósítása érdekében alkalmazó terroristaszervezetek és -csoportok lételeme az aszimmetrikus módszer alkalmazása. Az aszimmetria mint a hadviselés egyik elterjedt formája évezredek óta ismert. A lényege az, hogy a várakozásoktól, számításoktól eltérő taktikai megoldásokkal kompenzálja, egyenlítse ki az egyik harcoló fél a jobb helyzetben lévő – jobban felszerelt, nagyobb élőerővel rendelkező – másik harcoló fél előnyét. Az aszimmetrikus megoldások tárháza rendkívül gazdag. Ezt az utat követik a terrorszervezetek és -csoportok is. Gyakran változtatják a támadások elkövetési módját, az eszközöket és természetesen a helyszíneket. Ez a dinamizmus komoly kihívást jelent a nemzetbiztonság és a közrendvédelem számára. Mivel nagy mobilitásuk, flexibilitásuk és jól felépített hálózatuk miatt előnyös helyzetben vannak, így a terrorellenes szervezetek és intézmények az esetek nagy többségében a beérkező információkra reagálva próbálják elejét venni a terrortámadásoknak, illetve

ha ilyen már bekövetkezett, igyekeznek mihamarabb kézre keríteni az elkövetőket és felderíteni a cselekmény és a tettesek hátterét.

A megelőzés, illetve a bekövetkezett cselekvésre való reagálás és a további ellenintézkedések egyik kritikus pontja épp a civil professzionális együttműködés, a polgári és szakmai intézmények tevékenységének egymást kiegészítő, egymásra épülő konvergenciája, az információmegosztást is beleértve. Nyilvánvaló, hogy a folyamatosan változó terroristamódszerek ellen változatlan, hagyományos módszerekkel csak korlátozott sikereket lehet elérni. Ezért szükség van az új helyzetben alkalmazható rendszabályok, protokollok szükség szerint aszimmetrikus, folyton a helyzet követelményeihez idomuló, dinamikus alkalmazására.

A terroristák aszimmetrikus módszereinek alkalmazása átfogja a terrorszervezet vagy terroristacsoport működésének számos területét, kezdve a toborzással, a művelet tervezésén, a finanszírozáson, az eszközbeszerzésen, a végrehajtók kiválogatásán, felkészítésén át egészen a célpontok kijelöléséig, a terrorcselekmény eszközeinek és a végrehajtás lehetséges alternatíváinak meghatározásáig. Ebből következik, hogy a dinamikus aszimmetria a terrorszervezetek sikereinek a kulcsa. Az aszimmetria dinamizmusa elengedhetetlen, hiszen a változó műveleti és hálózatfenntartási tényezőkkel elébe kell menni a terrorelhárító, a nemzetbiztonsági és a rendvédelmi szervek és intézmények lépéseinek. Ennek egyik, mára már nyilvánvaló útja a terrorizmus paradigmaváltása. Mit jelent ez a gyakorlatban?

Ahogy azt az elmúlt évtizedekben láttuk, a terroristaszervezetek a megfélemlítés, megtörés eszközével, a válogatás nélküli, tömeges erőszak alkalmazásával próbálták politikai céljaikat elérni. A nemzetközi koalíció és a terrorelhárítási szervek széles körű, hatékony összefogásának, együttműködésének és megelőző tevékenységének köszönhetően az elmúlt években, különösen az Iszlám Állam katonai szervezetének megtörése óta, csökkent az erőszakos terrorcselekmények száma. Ez nem jelenti a terrorizmus és a terror eszközét alkalmazó, politikailag motivált szervezetek és csoportok megszűnését, felszámolását. A dinamikus aszimmetria elvét a gyakorlatban alkalmazva, a változatlan stratégiai politikai célok elérésére a terrorszervezetek más taktikai megoldásokat kezdtek alkalmazni. Gazdasági, vállalkozási, nagy- és kiskereskedelmi, pénzügyi, kulturális, sport-, jótékonysági és oktatási fedőszerveket hoztak létre, amelyeken keresztül a vállalkozások közelében élő lakosságra célzott tevékenységet fejtenek ki. Meggyőző munkájukkal képesek befolyásolni az ott élők hangulatát, tekintélyre tesznek szert, és az önkormányzatokban is pozíciókat szereznek. Erre legjobb Libanon példája, ahol a 2018-as parlamenti választásokon a Hezbollah és szövetségesei a 128 parlamenti mandátumból 70-et

szereztek meg. Ez 54,68%-os többséget jelent.[4] Hasonló gondokkal küzd manapság a világ több, kormányzati, gazdasági és politikai hullámzásoknak kitett országa is, például Peru, Venezuela és Paraguay. Az ebből fakadó veszélyek kézenfekvők és magától értetődők.

A paradigmaváltás mellett, azt kiegészítve érzékelhető a terrorfinanszírozás diverzifikációja is. Erre a legjobb lehetőséget a fent felsorolt – vállalkozási, nagy- és kiskereskedelmi, pénzügyi, kulturális, sport-, jótékonysági és oktatási – területeken megszerzett pénzügyi eszközök, illetve a hagyományosnak számító pénzmosás kínálja. Ez a fajta diverzifikáció vagy „több lábon állás" kiegészíti a hagyományos, bűncselekményekből származó forrásokat. A kábítószer-bűnözésben való részvétel, az illegális műkincs-kereskedelem, a zsarolás, kényszerítés, védelmi pénz szedése ugyanúgy jellemző bevételi forrás napjainkban is. Ezzel elérkeztünk egy másik, egyre inkább előtérbe kerülő és egyre nagyobb szerepet játszó tényezőhöz, a konvergencia gyakorlatához.

Konvergencia a fenyegetések oldaláról

Mi mivel konvergál, mi mihez közelít? A határon átnyúló kapcsolatrendszerek, különös tekintettel a nemzetközi szervezett bűnözésre, ezen belül a kábítószer-bűncselekményekre, ember, fegyver és egyéb árucikkek csempészésére, továbbá a terrorizmusra, alapvető jellegzetesség a komplexitás, az egyes cselekvési mozzanatok egymásra épüléséből, kellő időzítéséből kialakuló, horizontálisan és vertikálisan is strukturált együttműködés. A gazdasági együttműködést érintően már írtam, a munkafázisok elkülönülése és azok összehangolása a megoldandó feladatok bonyolultságának növekedéséből fakadó, természetes folyamat. Nincs ez máshogy a szervezett bűnözés és a terrorizmus világában sem.

A taktikai érdekazonosság, az anyagi előnyök, illetve a terrorizmus esetében a politikai szándékok érvényesítéséhez szükséges eszközök megszerzése a különböző bűncselekményfajtákra szakosodott csoportok, szervezetek között „természetes", esetleg stratégiai együttműködést indít el. Így a bűncselekményfajták egymást kiegészítve közös célok mentén valósulnak meg. Mivel a szervezeti háttér leggyakrabban változatlanul elkülönül, nem olvad egybe, vagyis nem jön létre a bűnszervezetek között egyesülés, fúzió, hanem csak egymás felé tartva közelednek

[4] Tom Perry: Factbox: Hezbollah and Allies Gain Sway in Lebanon Parliament. *Reuters,* 2018. május 22.

egymáshoz, ezért beszélhetünk konvergenciáról, a bűnszervezetek funkcionális konvergenciájáról.

A terrorizmus mint a jelenkori szervezett, politikai indíttatású, de gyakran vallási, ideológiai téveszmékkel leplezett bűncselekmények sajátos fajtája különleges helyet foglal el a konvergencia szempontjából is. Ahogy az előbb már látható volt, a taktikai együttműködés a terrorcselekmények előkészítésében más bűnszervezetekkel a terrorszervezeteknél folyamatosan alkalmazott eljárás. Ugyanakkor van egy rendkívül sajátos terület, a nemzetközi szervezett bűnözés egyik különösen veszélyes ága, ahol az ágazati, stratégiai konvergencia megfigyelhető. Ez pedig a nemzetközi kábítószer-bűnözés és a terrorfinanszírozás. Ebben az esetben a terrorcselekmények és a szervezet finanszírozásához szükséges anyagi-pénzügyi háttér megteremtése az a stratégiai érdek, amely folyamatos és tartós kapcsolat kiépítését teszi szükségessé. Ennek következménye, hogy a terrorszervezetek jelentős része részt vesz a kábítószer-termelésben, -terjesztésben, védi a termőterületeket és feldolgozóüzemeket. Itt természetesen mindenkinek a Kolumbiai Forradalmi Fegyveres Erők és a perui Fényes Ösvény jut eszébe először, de érdemes figyelembe venni, hogy legnagyobb részben a Hezbollah áll a közel-keleti Captagon-ipar, vagyis az amfetamin- és metamfetamin-gyártás mögött.[5]

A kábítószer további feldolgozása, finomítása és a felvevő piacra történő továbbítása és terjesztése már az erre „szakosodott" kábítószer-bűnözői szervezett csoportok feladata. Ha az összképet tekintjük, észre kell venni a konvergencia szintjeinek egymásra épülését. Először az egymást kiegészítő bűncselekményfajták elkövető szervezetei konvergálnak, majd a határok különböző oldalain tevékenykedő komplex bűnelkövetői szindikátusok között is kialakul ilyen együttműködés, végül látható a nemzetközi szervezett bűnözés és a terrorizmus konvergenciája is.

A konvergenciának létezik egy másik strukturált területe is. Ennek alapját már az előbbiekben érintettük. Ebben a rendszerben a terrorszervezetek helyi szinten létrehozott fedővállalkozásai, pénzmosodái, vallási-kulturális iskolái, sportegyesületei és segélycsoportjai a lakosság leginkább szükséget szenvedő szociálisan sérülékeny rétegeire hatva közelednek a helyi politikai, gazdasági, kulturális, sport- és érdekképviseleti szervezetekhez. Céljuk a hatalmi szervekbe való beépülés és befolyásszerzés. Mindezt a meglévő jogi keretek és lehetőségek kihasználásával teszik, a jogszerűen működő vállalkozások és szervezetek látszatát fenntartva, miközben

[5] Anne Barker: Captagon: Evidence Paris Attackers Used 'Jihadist's Drug' Favoured by Islamic State Fighters. *ABC News,* 2015. november 25.

valójában a háttérben meghúzódó terrorszervezet konvergál észrevétlenül a helyi hatalom irányába.

Konvergencia a fenyegetések kezelésének oldaláról: az állami és nem állami szereplők együttműködése

Az aszimmetrikus kihívások aszimmetrikus reagálást követelnek, amelyek szintén konvergálnak. A különböző illetékes szervezetek és intézmények által saját hatáskörükben, de egymás közt egyeztetett módon meghozott aszimmetrikus válaszintézkedések egy részét, annak érdekében, hogy a kiváltó cselekmény felderítése és vizsgálata a legeredményesebb legyen, nem feltétlenül azonnal a kiváltó cselekmény bekövetkezése után azonnal foganatosítják, sőt!

Az aszimmetrikus reagálás nem csupán egy esemény bekövetkezte után alkalmazható. Létjogosultsága van a megelőzésben is, amikor egy cselekmény előkészítésére vonatkozó információra kell dinamikusan, adaptív módon, vagyis a beérkezett információ sajátosságaihoz alkalmazkodva, az aszimmetria elvének alkalmazásával reagálni a cselekmény megelőzése és a körülmények felderítése érdekében. Egyszerűbben: ott, akkor, úgy és olyan eszközökkel kell megakadályozni a cselekmény elkövetését, amely a terroristák számára a lehető legkevésbé kiszámítható. Ezek jellegzetességei mindig folyamatosan, dinamikusan változnak, ezeket változtatni kell. Épp ez az aszimmetrikus reagálás lényege.

A szervezett bűnözés, kábítószer-bűnözés és terrorizmusellenes fellépés nem az erre hivatott és létrehozott rendvédelmi és terrorelhárító szervezetekkel és szolgálatokkal kezdődik, hanem az egyes állampolgárral. Vagyis, ha egy lehetséges és kívánatos konvergens rendszerben gondolkozunk, akkor először a társadalmilag veszélyes cselekmények üldözésére hivatott szervezeteket kell közelíteni az állampolgárhoz, a szolgálati érdekek határáig ki kell lépni a szofisztikált elzártságból, a szakmai elefántcsonttoronyból, meg kell szólítani az állampolgárt, hogy az kezdje el interaktívan támogatni a hatósági feladatok ellátását. Konvergencia? Igen, az! Az állampolgár és az ő védelmére hivatott intézmény közötti érdekazonosság alapján itt egyfajta társadalmi konvergenciáról beszélhetünk. Ennek a konvergenciának a feltételei, módja, lehetőségei, területei és határai több külön tanulmány tárgyát is képezhetik.

Az érdekazonosság és a közös célok nyilvánvalóan megvannak a különböző nemzetbiztonsági, rendvédelmi és terrorelhárító szolgálatok között is. Ennek alapján – félretéve a hagyományos szakmai szervezeti rivalizálást – létrejönnek,

Magyarországon már létre is jöttek, a szakmai konvergencia feltételei, aminek a szervezeti megjelenítése a Terrorelhárítási Információs és Bűnügyi Elemző Központ. A nemzetközi terminológia még fúziós központok néven is ismeri ezeket a konvergenciára épülő, a hatékony információmegosztást elősegítő szervezeteket. Csak nézzük vissza, mi áll a korábbi, a gazdasági célokat követő konvergenciáról írott részben! A kettőt összehasonlítva láthatóvá válik a konvergenciamodell, amely a többszintű, magasan strukturált, egymásra épülő feladatok ellátását fogja át.

A konvergens struktúráknak itt még messze nincs vége. Ha szakmai intézmények és szervezetek konvergenciáját nézzük, nem hagyhatjuk figyelmen kívül a szervezetek hatékony működését elősegítő tudományos és műszaki bázist sem. A nemzetbiztonsági és terrorelhárítási tevékenység olyan komplex feladat, amelynek technikai hátterét folyamatosan fejleszteni kell. Az állami részről rendelkezésre álló források messze nem elégségesek, hiszen a „sötét oldal" az állami költségvetés jogszerű keretei nélkül képes nagy összegeket és erőforrásokat fordítani a saját eszközeinek fejlesztésére, a legújabb tudományos eredmények azonnali alkalmazására. Ha nem nézünk mást, mint az informatikai alkalmazásokat, amelyeket a nemzetközi szervezett bűnözői csoportok, a kábítószer-bűnözők és a terroristahálózatok anyagi-pénzügyi eszközök mozgatásához, termékek és szolgáltatások beszerzéséhez, manipulatív célú kommunikációjukhoz vagy más célokra is alkalmaznak, láthatjuk, hogy azok között saját fejlesztésű szoftverek is szép számmal találhatók.

A fentiekből is látszik, hogy a dinamikusan fejlődő bűnözői „háttériparral és szolgáltatási szférával" csak a tudományos és technikai terület valamennyi szférájára kiterjedő, összehangolt kutatói-fejlesztői-alkalmazói együttműködéssel lehet szembeszállni. Ehhez egy új, sajátos „konvergens" tudatot kell meghonosítani. Ennek alapja a civil és a nemzetbiztonsági, rendvédelmi, terrorelhárítási és katonai struktúrák, valamint az ezen a területen tudományos fejlesztésekkel és alkalmazások használatával foglalkozó, nemzetbiztonsági szempontból akkreditált intézetek, laboratóriumok közötti összehangolt munkamegosztás, a szakmai nemzetbiztonsági szervezetek irányítása és ellenőrzése mellett. Ez a fajta civil – nem civil együttműködés egyaránt ki kell hogy terjedjen a műszaki és a humán tudományterületre, az alapkutatásokra és az alkalmazott tudományok kutatására is. Át kell hogy fogja az elméleti és a gyakorlati területet, továbbá az úgynevezett gyakorlat-elméleti kutatásokat is, hiszen ezek dinamikus egysége, komplementer jellege és folyamatos fejlődése, fejlesztése teszi lehetővé a 21. századi nemzetbiztonsági, védelmi, terrorelhárítási és rendvédelmi kihívásokkal szembeni folyamatosan magas színvonalú fellépést, a nemzeti gazdasági, társadalmi, kulturális és polgári célú tudományos kutatások fejődési feltételeinek maradéktalan biztosítását.

Társadalom – technológiai környezet – nemzetbiztonság

Dobák Imre

A „nemzetbiztonság” működésének közege

Napjainkban a nemzetbiztonsági szolgálatok egy rendkívül összetett, dinamikusan változó világban látják el feladataikat. Működésüket számos külső tényező befolyásolja, amelyek az alábbi irányokból érkezhetnek:[1]

- a *társadalom irányából* (például érdekek módosulása, elvárások változása);
- az *állam irányából* (például állami berendezkedés, politikai rendszer, szabályozás változása);
- a *gazdaság irányából* (például erőforrások rendelkezésre állása, költségvetés kérdései);
- a *biztonságpolitika irányából* (például együttműködések, rendkívüli események bekövetkezése, biztonsági veszélyek jellemzőinek változása – például új terroristamódszerek, migráció tömeges jellege);
- valamint a fejlődő technológiai környezet irányából.

Értelemszerűen e tényezők teljességgel nem választhatók el egymástól, amelyek összetettségére a „társadalom”, a „gazdasági szereplők”, és a „nemzetbiztonsági” szféra háromszöge mentén felállítható alábbi modellel kívánunk rávilágítani. Segítségével reményeink szerint áttekinthetőbbé válnak az egymásra gyakorolt hatások, illetve az ott megjelenő, gyakran ütköző érdekek. Ebben a háromszögben:

- A *társadalom* tagjainak alapvető érdeke, hogy szabadon, határoktól és egyéb korlátoktól függetlenül kommunikáljanak, személyes adataikat szabadon védjék (akár titkosítási megoldásokat használjanak), és magánszférájukat az állam tiszteletben tartsa. A gazdasági szereplők felé ugyanakkor az egyének széles körben önként adnak felhatalmazást adataik „gyűjtésére-tárolására”, hiszen ezen adatokkal személyre

[1] Dobák Imre: Technológiai fejlődés – titkosszolgálatok. In Fekete Károly (szerk.): *Kommunikáció.* Budapest, Nemzeti Közszolgálati Egyetem, 2013. 66.

https://doi.org/10.36250/00904_04

szabottabb szolgáltatásokat kapnak, életüket megkönnyítő megoldásokhoz juthatnak. Társadalmi elvárásként jelenik meg részükről, hogy az erre a célra létrehozott biztonsági és nemzetbiztonsági szervek (nemzetbiztonság) biztonságukat garantálják.

– A *gazdasági szereplők* kategóriájához jelen modell főként az infokommunikációs és online kereskedelmi tevékenységek területén globális piacokat szerző és lényegében jelentős gazdasági és egyben politikai szereplőkké váló nagyvállalati szereplőket sorolja (például Apple, Microsoft, Google, Facebook vagy akár az Amazon). E nagyvállalatok érdekei között (legyenek azok akár nemzeti, akár globális szintű szereplők) jelennek meg, hogy a társadalom tagjainak igényeit kiszolgálva üzleti alapon biztosítsák az információs technológiákhoz és a kommunikációhoz való hozzáférés lehetőségét. Mindez sajátos viszonyrendszert eredményez a nemzetbiztonsági struktúrák irányába is, hiszen a nemzetbiztonsággal való túlzott együttműködésük felboríthatja a társadalom irányába meglévő, termékeik, szolgáltatásaik szempontjából fontos bizalmi viszonyt (és úgynevezett bizalmi deficit alakulhat ki).[2] A globális infokommunikációs szereplők esetében további jellemzőként merül fel, hogy rendkívüli, akár adott országok politikai folyamataira hatást gyakorló technológiai képességekkel rendelkeznek.
– A *nemzetbiztonsági* szféra ebben a köztes viszonyrendszerben látja el feladatát, ahol a működése mentén a társadalom érdekében végzett összetett nemzetbiztonsági feladatokat, a nemzetbiztonsági érdekek érvényesítését és közvetve az állampolgárok védelmét kell keresni. Ugyanakkor a korábbi hidegháborús viszonyokkal szemben a veszélyeket gyakran már nem egy jól látható másik fél, hanem a társadalom tagjai között meghúzódó nem békés célú egyének (bűnözők, terroristák, hackerek) is jelenthetik, akik tevékenységének felderítése sajátos (egyes esetekben a magánszféra sérülését okozó) eszközöket igényelhet. A gazdasági szereplők egyrészről együttműködési szükségletet (például hírközlési adatok beszerzése egy hírközlési szolgáltatótól), másrészről együttműködési lehetőségeket (például fejlesztések) jelentenek. Az együttműködés tartalmát és formáit a nemzetbiztonsági tevékenység érzékenysége miatt

[2] Példaként az Apple vagy akár a BlackBerry mobiltelefonok említhetők, amelyekről elterjedt, hogy nagyobb biztonságot jelenthetnek felhasználóik számára, így a vállalatok széles együttműködése a nemzetbiztonsági szférával minden bizonnyal csökkentené a termékeik iránti keresletet.

ugyanakkor a nemzetbiztonsági szféra is sajátos fenntartással kezeli. Számos ország esetében látható például a biztonsági magánvállalati szereplők fokozott szerepvállalása, de itt említhető akár egy külföldi kommunikációs szolgáltató állami kommunikáció biztosításába történő bevonásának vitatott kérdése is. Az együttműködéstől való teljes elzárkózás esetén a nemzetbiztonsági szolgálatok eszközrendszerei, megoldásai „elavulhatnak", és előtérbe kerülhet az úgynevezett *„going dark"* jelensége,[3] amely (a fejlett titkosítások szabad használata és elterjedése kapcsán jelent meg, és) egyfajta „képességvesztést" jelez a technológiailag fejlettebb környezettel szemben. A demokratikus államok nemzetbiztonsági rendszerei oldaláról így egy, az állam, a társadalom és tagjainak védelme érdekében működő olyan rendszer működtetése a cél, amely az egyének magánszférájának a lehető legkisebb sérülését okozza, ugyanakkor a külső környezet kihívásaira reagálva, a hírszerzés és a nemzetbiztonság egyéb területei szempontjából a legnagyobb hatékonyságot biztosíthatja. Ezt a hatékonyságot a képességeik és az ezek működésének kereteit biztosító jogszabályi környezet hangolásával igyekeznek elérni.

A viszonyrendszer működése

Az infokommunikáció 21. századi globális szereplői sajátos helyzetük, kutatási és termelési erőforrásaik révén szinte szabadon formálhatják a technológiai trendeket. Közös jellemzőjük, hogy túlnyomó többségük olyan technikai profilú vállalat, amely egy korábban nem létező piaci szegmensben jött létre az elmúlt 20 év során. Igazi erőforrásaik és jelentőségük magukban a „szolgáltatásaik" használatában, és a nagy mennyiségű adatok „kezelésében" rejlik. Ilyenek például az internetes keresők vagy akár a közösségi oldalak, ahol az információk kezelése, hozzáférések biztosítása a működés lényegét alkotják. Szolgáltatásaik lényegében kikerülik az adott állami szereplőket, aminek eredményeként e globális nagy nemzetközi cégek tevékenysége – az általuk szolgáltatott, a társadalom életét pozitívan támogató tagadhatatlan megoldások és fejlesztések mellett – akár az egyes államokra is közvetlen hatással lehetnek. A „digitális kapitalizmus" profitorientált nagyvállalataival szemben természetesen sajátos

[3] Peter Swire – Kenesa Ahmad: Encryption and Globalization. *The Columbia Science & Technology Law Review,* 23. (2012), Spring 464.

válaszok születnek, amelyek mentén a *szabályozás* és használat, valamint a *tiltás* folyamatos váltakozásait figyelhetjük meg.

Szabályozás

Idesorolhatók az Európai Unió szintjén megjelenő, globális szolgáltatókkal szembeni büntetések és a monopolhelyzettel kapcsolatos vizsgálatok. Ki kell emelni az állampolgárok személyi adatai fokozottabb védelmének területét, amelyre jó példa az EU általános adatvédelmi rendeletének (GDPR)[4] 2018 óta történő kötelező alkalmazása,[5] valamint az állampolgárok személyes adatainak EU-n kívüli fél részére történő átadási kereteinek újraszabályozása. Az Európai Unióból az Amerikai Egyesült Államok felé – adott feltételek megléte esetén – történő személyes adatok továbbítására az Európai Bizottság 2000-ben elfogadott határozata (Biztonságos Kikötő Adatvédelmi Alapelvek – úgynevezett „Safe Harbor Privacy Principles") adott lehetőséget, amelyet az Európai Bíróság 2015-ben érvénytelenített,[6] majd 2016-ban már amerikai kormánygaranciákkal új megállapodást (EU–USA Adatvédelmi Pajzs – *Privacy Shield*) hoztak létre.[7] Az infokommunikációs megoldásokhoz köthető adatvédelmi igények a nagy globális infokommunikációs szolgáltatóktól is számos lépés megtételét követelték. Előtérbe került a felhasználók megfelelő tájékoztatásának követelménye az adataik felhasználásáról, kezeléséről és őrzéséről.

[4] General Data Protection Regulation – 2016-ban hatályba lépett, 2018-tól alkalmazott európai szintű általános adatvédelmi rendelet a természetes személyek személyes adatainak kezeléséről, védelméről.

[5] Az Európai Unióban kialakítandó adatvédelmi egyezmények gondolata már az évtized elején felmerült, felvetve egy egységes elveken alapuló európai szabályozás szükségességét, ahelyett, hogy azokat eltérő módon nemzeti szinteken szabályozták volna.

[6] A személyes adatok védelme kapcsán gyakran idézett példa a Schrems-ügy, amelyet egy osztrák állampolgár indított Facebook-adatainak Egyesült Államokban lévő szerverekre történő továbbítása kapcsán, hivatkozva arra, hogy – a 2013-ban kirobbant amerikai titkosszolgálati megfigyelési botrány információinak a fényében – adatai nincsenek biztonságban. Mivel az EUB „az olyan szabályozást, amely hatóságok számára lehetővé teszi, hogy általános jelleggel hozzáférjenek az elektronikus kommunikációk tartalmához, a magánélet tiszteletben tartásához való, alapvető jogot sértőnek találta", így érvénytelenítette a határozatot. A példát lásd Európai Unió Alapjogi Ügynöksége – Európa Tanács: *Európai adatvédelmi jogi kézikönyv* 2018. évi kiadás, Luxembourg, Az Európai Unió Kiadóhivatala, 2019. 49.

[7] Európai Unió Alapjogi Ügynöksége – Európa Tanács (2019): i. m. 49.

Nemzetbiztonsági vonatkozásban az Európai Parlament LIBE Bizottsága[8] által az amerikai Nemzetbiztonsági Ügynökség (NSA) titkos adatgyűjtése és uniós állampolgárokat érintő tömeges elektronikus megfigyelése kapcsán 2013–2014 között lefolytatott vizsgálat[9] említendő, amelynek eredményeként még inkább hangsúlyossá vált az adatbiztonság és a személyes adatok védelme, mind a szabályzás szükségességének, mind a biztonság fokozására szolgáló technikai képességek megteremtése terén.

Széles körben terjedtek el a végpont–végpont közötti titkosítási megoldások, amelyek azonban a nemzetbiztonsági és egyéb bűnüldöző szervek számára is megnehezítették a szükséges információkhoz való hozzájutást. A titkosítások alkalmazásának sajátos paradoxona, hogy az egyre erősebb titkosítás nélkülözhetetlen a biztonság növelése érdekében akár az egyének szintjén, akár az állami rendszereknél, emellett azonban fontos azt is biztosítani, hogy az arra jogosult bűnüldözési, illetve nemzetbiztonsági szervek meghatározott feladataik mentén (például terrorizmus elleni küzdelem) hozzáférjenek a számukra szükséges és engedélyezett adatokhoz. A legismertebb, a médiában megjelent nemzetközi példaként a 2016-os FBI[10] vs. Apple[11] eljárás emelhető ki. Ennek során egy San Bernardinói terrorcselekményt követően az FBI bírósági eljárásban kérte az Apple közreműködését, egy, a rendszerében alkalmazott titkosítási funkció dekódolási módszerének általános átadására. A nemzetbiztonsági érdek versus személyes adatok precedensjellegű eljárás hatalmas nemzetközi visszhangot keltett, amely végén az FBI mégis külső közreműködéssel, egyedi hackereljárással szerezte meg az eszközről a kívánt adatokat.

Hasonló helyzetet láthatunk a Google-höz hasonló, az oroszországi internetes keresések túlnyomó részét uraló Yandex keresőszolgáltató elleni orosz állami fellépés esetében is. A korábban még együttműködőnek[12] tekintett szolgáltatót 2019-ben rendszerének állami blokkolásával fenyegették, mivel nem volt hajlandó átadni titkosítási kulcsait az orosz titkosszolgálatoknak, annak ellenére,

[8] Committee on Civil Liberties, Justice and Home Affairs – Állampolgári Jogi, Bel- és Igazságügyi Bizottság.

[9] Claude Moraes*: Working Document 1 on the US and EU Surveillance Programmes and Their Impact on EU Citizens Fundamental Rights.* Committee on Civil Liberties, Justice and Home Affairs, 2013.

[10] Federal Bureau of Investigation, Szövetségi Nyomozó Iroda.

[11] The Apple-F.B.I. Case. *The New York Times,* (2016).

[12] Ekaterina Drobinina: Russian Search-Engine Yandex Passed Information to FSB. *BBC News,* 2011. május 3.

hogy erre az orosz törvények kötelezték. A Yandex esetében ez szintén azt jelenthette volna, hogy állami oldalról általános lehetőség nyílna a személyes kommunikáció átfogó, rendszerszintű megfigyelésére. A kérést a szolgáltató már az internet szabadsága ellen vívott lépésként értékelte, és nem tett eleget az orosz titkosszolgálat kérésének.[13]

A legtöbb országban azonban a tiltás, korlátozás helyett, illetve mellett az állam önmaga is előszeretettel használja hivatalos információmegosztásra a globális infokommunikációs szereplők szolgáltatásait. Ilyenek a közösségi felületek, amelyek milliárdos felhasználói közössége lehetőséget nyújt az állami szféra számára az állampolgárok csoportos, de akár egyéni megszólítására is. Ma már általánosnak tekinthető, hogy a kor kihívásaira reagálva és a választók, állampolgárok széles körét elérve a politikusok a korábbi állami internetes oldalak mellett a nagyobb közösségi oldalakon (Facebook, Twitter) tesznek közzé hivatalos üzeneteket. Számos kutatás vizsgálta az amerikai elnökválasztások sorából Barack Obama korábbi amerikai elnök 2008-as választási kampányát, amely során már több mint 100 főt alkalmaztak digitális jelenlétének biztosítására, de ő használta először (a 2011-es előválasztások során) a YouTube-ot választási üzenetének közzétételére.[14] Donald Trump 2016-os választási kampányánál szintén jelentős szerepet kaptak a közösségi csatornák, ahol azonban már – mint arra a 2018-ban Facebook – Cambridge Analytica-botrány felhívta a figyelmet – a közösségi oldalakon keresztül történő célzott politikai befolyásolás és a személyes adatok helytelen kezelésének problémái is felszínre kerültek.[15]

Tiltás

Általánosan ismert Kína és a nagy keresőóriás Google viszonya, ahonnan a vállalat szolgáltatásával már tíz éve kivonult, mivel az állam a keresések cenzúrázását

[13] Fred Weir: Russian Internet Giant Yandex Takes Rare Stand Against State Snooping. *The Christian Science Monitor,* 2019. június 14.

[14] Contentgroup: Social media on the campaign trail: Barack Obama and Donald Trump. (2017).

[15] Az évekig húzódó (2015–2019) Cambridge Analytica adatelemző cég botránya, amely során 87 millió amerikai Facebook-profilját használta fel egy profilozásra, elemzésre alkalmas szoftver létrehozásához, amely eredményeként például személyre szabott politikai hirdetésekkel befolyásolni lehetett amerikai szavazókat a 2016-os amerikai elnökválasztási kampány alatt. Lásd Kurt Wagner: Facebook Says Cambridge Analytica may have had Data from as Many as 87 Million People. *Vox,* 2018. április 4.

várta el. A piaci érdekek mentén igaz, az elmúlt években ismét felmerült a kínai állam számára hozzáférést biztosító keresőmotor *(Dragonfly)* fejlesztésével a piacra történő visszatérése, hiszen így egy több mint egymilliárdos ország piaci szegmense maradt meg a kínai IKT-szektor számára. Oroszországban hasonló piaci és a nemzetbiztonsági érdekek találkozását láthatjuk. 2019-ben a hatóságok felszólították a Google-t, hogy állítsák le a cég tulajdonában lévő YouTube-on közzétett és „Oroszországban törvényellenesnek minősített tömegmegmozdulások hirdetését", és felmerült a keresőmotor elérésének blokkolása is. Ugyanakkor az Apple – vélhetően szintén piaci megfontolások miatt – lépéseket tett arra, hogy a nemzeti szintű elvárásoknak megfelelve Kína, valamint Oroszország esetében is biztosítsa, hogy az adott országok határain belül tárolja a honos állampolgárok adatait.[16] Oroszország esetében terrorizmusellenes törvény (Jarovaja tv.) alapján így együttműködési kötelezettsége jelenik meg a biztonsági szolgálatok irányába is.

A kommunikáció szabadsága és az állami szintű megfigyelési lehetőségek körüli vitákhoz sorolható az orosz VKontakt közösségi oldal korábbi példája, amely sikertelenül próbált meg ellenállni az orosz állami elvárásoknak, vagy akár a blokkolással fenyegetett Telegram üzenetküldő elterjedt alkalmazása, amely titkosítást alkalmazva biztosítana védelmet felhasználói kommunikációja számára.[17]

Idesorolhatók azon gyakorlatok is, amikor egyes államok a nemzeti szintű biztonsági érdekeik kapcsán bizonyos infokommunikációs területeken a függetlenségre való törekvés útját választják. A kiberbiztonság szempontjait tekintve ezek főként az államigazgatás területén figyelhetők meg, így például saját hírközlési és adatátviteli rendszerek, illetve zárt kommunikációs szolgáltatások kiépítése és az azokra való áttérés (nemzeti szintű mobiltelefon- vagy akár levelezési szolgáltatások kialakítása). Franciaországban például a külföldi titkosszolgálati megfigyeléseket elkerülendő a BlackBerry okostelefon internetezésre való tiltása az államigazgatásban már 2007-ben megjelent, de a 2013-as amerikai titkosszolgálati botrány után a francia kormányzat érzékeny területein az általánosan használt mobiltelefonok helyett a francia Thales hadiipari cég mobiltelefonjának (Teorem) használatát írták elő.[18] Az amerikai haditengerészet pedig 2019 végén a rendkívül gyors ütemben terjedő (a kínai ByteDance tulajdonában álló) TikTok

[16] Amy Mackinnon: How Russia is Strong-Arming Apple. *Foreign Policy,* 2019. január 31.
[17] Domokos Erika: Oroszország letilt egy üzenetküldő szolgáltatást. *Napi.hu,* 2018. április 13.
[18] MTI: Hadat üzent a Gmail-nek a francia kormány. *Napi.hu,* 2013. szeptember 13.

mint közösségimédia-alkalmazás letöltését és használatát tiltotta be kiberbiztonsági okokból a kormány által biztosított okostelefonokon és táblagépeken.[19]

A kínai példa

A kínai példa annak sajátosságai és a megfigyelés általános jellege miatt mindenképpen áttekintésre érdemes. Kína napjainkra széles körű megfigyelési technológiai eszközrendszereket épített ki az országban, amelyek szintje a világon addig sehol nem látott méreteket öltött, és amely fejlett technológiákkal rendkívül széles körben (az emberek mozgásától kezdve egyéb elektronikus kommunikációjukig) megfigyelhetik tevékenységüket. Nemzetközi szakirodalmi források több mint 200 millió biztonsági kamerát említenek, amely szám 2022-re várhatóan 213%-kal, 626 millióra fog emelkedni. Ezek egyéb IKT-megoldásokkal, arcfelismeréssel, az egyén mozgásának nyomon követésével, egyéb adatbázisokban tárolt személyes adatokkal történő összevetésével és a mesterségesintelligencia-alkalmazásokkal együtt már a társadalom mindennapjainak átfogó elemzését biztosíthatják, elősegítve a kínai „társadalmi érdemeken alapuló kívánt viselkedés elfogadását ösztönző" társadalmi pontrendszer bevezetését.[20]

A kínai „megfigyelési technológia" exportja a 2008-as pekingi olimpia után kezdődött, amely óta Kína 54 országba exportálta a magánéletre hatást gyakorló megfigyelőrendszereit.[21] Míg a szakirodalmi források alapvetően a „tekintélyelvű" kormányok működéséhez kapcsolják a széles körű, a társadalom tagjait érintő megfigyelési alkalmazásokat, mindezek egy-egy kiemelt biztonsági kihívás kapcsán (például terrorizmus, bűncselekmények, sportrendezvények) jelen vannak a világ demokratikus állami berendezkedésű régióiban, nagyvárosaiban is (például London). E képességek az „okos város" technológiái mentén is várhatóan megjelennek, így kiemelten fontossá válik az adatok tárolásának és felhasználhatósága szabályozásának változó technológiai környezethez történő igazítása.

[19] Dalvin Brown: The U.S. Navy Banned TikTok from Government-Issued Smartphones over Cybersecurity Concerns. *USA Today,* 2019. december 23.

[20] Tenzin Dalha: Beijing's Export of Surveillance Technology. *Modern Diplomacy,* 2020. január 7.

[21] Dalha (2020): i. m.

Dobák Imre

A kutatás, fejlesztés és innováció átrendeződése nemzetbiztonsági szemmel

A 21. századi nemzetbiztonsági struktúrák – amelyekkel szemben társadalmi és „szakmai" elvárás, hogy korszerű megoldásokkal, rendkívül képzett állománnyal és megfelelő reagálási lehetőségekkel rendelkezzenek – eszközei, megoldásai, személyi utánpótlásuk jelentős része is ebben a „megoszthatatlan" környezetben fejlődnek. Más ágazatoktól eltérően céljaikat nem a profitorientáltság, hanem az állam biztonsági igényeinek kielégítéséhez való hozzájárulás, az abban történő részvétel határozza meg.

A múlt század keleti–nyugati szembenállásának időszakában a különböző technológiák fejlesztésénél és felhasználásánál az egyes államok törekedtek a nemzeti, illetve szövetségesnek tekintett országok különböző szektoraiban létrehozott technikai megoldások alkalmazására, így széles kapcsolatokat építettek ki a külső, tudományos kutatóintézeti és együttműködő vállalati környezet irányába. Ennek az időszaknak a fejlesztési sajátosságaira többek között az alábbiak voltak jellemzők:

- a hidegháborús szembenálláshoz igazodó rendkívüli technológiai verseny;
- a technikai rendszerek létrehozása történelmileg vagy az állami oldalon történt, vagy azok fejlesztése, beszerzése sajátos zárt kapcsolatot igényelt a nemzeti iparral, amelyet a titoktartás jellemzett;
- az ipari, technológiai, gazdasági jellegű hírszerzés kiemelt jelentősége;
- a nemzeti szinteken rendelkezésre álló K+F képességek és kapacitások felhasználása, a nemzeti szintű (állami) „külső" kutatóintézetek, egyetemek nem nyilvános módon történő bevonása;
- a szövetségesi rendszerben partnerként megjelenő országokkal való technikai, technológiai, tudományos együttműködések és tapasztalatcserék.

Globális információs társadalmunkban mindennek szempontjai azonban átalakultak. Napjainkban a technológiai fejlesztések és a K+F eredmények túlnyomó része már az állami szférán kívül, a piaci, vállalati szférában keletkezik, és számos területen a korábbi elzártság már nem megvalósítható. Ennek okai között jelennek meg, hogy a 21. századi korszerű elektronikus információmegosztási formák, a tudomány új eredményeihez való globális hozzáférés, a fejlesztési képességek és központok decentralizálódása, valamint az internetre és az informatikára épülő szabad fejlesztési lehetőségek rendkívüli módon átalakították

a kutatás-fejlesztés és innováció (K+F+I) rendszerét, amely napjainkra a fejlődés egyik legmeghatározóbb területévé vált.

Amíg az új technológiák előnyei egyértelműnek tűnnek, addig nemzetbiztonsági szempontból azok megjelenése kapcsán gondoljunk egyszerűen a magánszférában vagy akár másik országban fejlesztett olyan megoldásokra, amelyek (állami szférába történő) beáramlása azonban kockázatokat is rejthet magában.[22] A Kadtke–Warton szerzőpáros a technológiai nagyhatalom Egyesült Államok esetében fogalmazza meg, hogy „számos tényező miatt az új technológiák következő generációja valószínűleg az Egyesült Államokon kívül kerül forgalomba és gyártásra, ami stratégiai és hosszú távú veszélyt jelent".[23]

Minderre talán a legjobb példa, a világunkra mindenképpen hatást gyakorló 5G technológia bevezetése,[24] amely már önmagában is – mint az egyes nemzeteken túlmutató és globális vállalati szereplők részvételével zajló – technológiai rivalizálás színtere. A hagyományosnak tekinthető kommunikációs megoldásokkal szemben szakértők hívják fel a figyelmet arra, hogy az 5G kiépülése várhatóan alapjaiban fogja megváltoztatni társadalmunk számos szegmensét. Eszközök tömegei fognak valós időben kommunikálni egymással és az IoT- (*Internet of Things,* dolgok internete) megoldások, az internetre csatlakozó szenzorok milliói várhatóan életünk több területét is a technikai adatok által vezérelt irányba mozdítják el. Tovább fejlődnek a tömeges adatok feldolgozásának újszerű megoldásai, és ezzel párhuzamosan a mesterséges intelligencia alkalmazásai.[25]

Az 5G politikai jelentősége is vitathatatlan, gondoljunk csak a technológiai élmezőnybe tartozás gazdasági, társadalomfejlődési és biztonsági hatásaira. Számos ország (például Kína, Dél-Korea, Japán és több EU-tagország) már kijelölte a rendszer működéséhez szükséges frekvenciaspektrumot, és jelenleg már a hálózatok kiépítése, a regionális szolgáltatásindítás, valamint az infra-

[22] A piaci, nemzetgazdasági, valamint nemzetbiztonsági kérdéskörök találkozásánál számos olyan nemzetközi példa látható, amelyek jól jelzik ezen kérdéskörök összetettségét. 2018-tól zajló gazdasági háborúvá növekvő folyamat része a kínai Huawei mobilkommunikációs óriáscég nemzetbiztonsági kockázatra való hivatkozással, Egyesült Államokból történő kitiltásának kérdése.

[23] James Kadtke – John Wharton: Technology and National Security: The United States at a Critical Crossroads. *Defense Horizons,* 2018. március 1.

[24] Az 5G-szabvány végleges változatának jóváhagyását 2020 elejére tervezte a Nemzetközi Távközlési Unió (ITU).

[25] Andrej Kadomtsev: 5G: A new stage in civilization development amid global competition. *Modern Diplomacy,* 2019. december 26.

struktúra technológiai – gazdasági szempontrendszerei körül folynak a gyakran „gazdasági csatározásokba" torkolló nemzetközi viták.[26]

A kérdéskör összetettségét, jövőbe mutató gazdasági és nem utolsósorban társadalmi súlyát jelzik az egyes országok eltérő álláspontjai is. Míg Kína ellenőrzi a „világ 5G-szabadalmainak több mint egyharmadát, és a meglehetősen korlátozott számú potenciális fejlesztői és gyártói kört",[27] az európai országok többsége támogatja annak bevezetését, az Egyesült Államok esetében pedig a kínai technológiai kiszolgáltatottságtól tartva, a technológiai lemaradás behozatalához való időnyerés vagy akár egy későbbi technológiai piaci pozíciószerzés előkészítése sejthető.

A technológiai-gazdasági fölényért vívott küzdelemben kiemelten fontos nemzetbiztonsági kérdésként merül fel, hogy lehet-e, és ha igen, milyen mértékben egy adott társadalom működését alapjaiban meghatározó technológiai infrastruktúrát, a felhasználók életének szinte minden területére kiterjedő adatokat egy másik országnak vagy akár multinacionális nagyvállalati szereplőnek kiszolgáltatni. Mennyiben veszélyeztetheti ez az adott nemzet és a társadalom szuverenitását, vagy pedig ennek ellenoldalaként a korszerű megoldások hiányában a technológiai elszigetelődés és a gazdasági-társadalmi lemaradás veszélye fenyegethet. A jövőben minden bizonnyal egyre gyakrabban találkozunk majd az új technológia biztonságra gyakorolt kérdései körül felmerülő dilemmákkal.

Anélkül, hogy a biztonságra, védelemre és a hadviselésre a jövőben hatást gyakorló egyéb technológiákat felsorolnánk jelen fejezetben, megállapítható, hogy egyre fontosabbá válik a különböző technológiák folyamatos monitorozása, és annak megállapítása, hogy azok a jövőben kulcsfontosságúnak tekinthetők-e, hogyan befolyásolják egy adott nemzet védelmi képességeit, biztonsága növelésének lehetőségeit, valamint a nemzeti ipar szintjén rendelkezésre állnak-e annak fejlesztési képességei.[28]

[26] Lásd: az Egyesült Államok és Kína között kirobbant gazdasági háború, a kínai Huawei cég térhódítása.

[27] Kadomtsev (2019): i. m.

[28] Quentin Ladetto: *Defence Future Technologies, Emerging Technology Trends 2015.* (DEFTECH) Federal Department of Defence, Civil Protection and Sport DDPS Armasuisse Science and Technology, 2016.

Nemzetbiztonság és a kiszervezés

A nemzetbiztonsági rendszer működésének sajátosságai, annak központi és kritikus elemei, valamint a döntéseket segítő feladatrendszere miatt általánosságban megfogalmazható, hogy annak ellátása elválaszthatatlan állami feladat. Mint Finszter Géza is kifejti tanulmányában:

> „A nemzetbiztonság nem privatizálható. Ennek oka egyfelől a fenyegetések súlyosságában, másfelől az elhárításukra alkalmas eszközök jogkorlátozó természetében található. Ezek együtt államigazgatási felhatalmazást és felelősséget igényelnek. Alkotmányos rendszerekben ez a sajátos erőszak-monopólium is a jog uralma alatt áll, és gyakorlása nem korlátlan."[29]

Fentiek ellenére a nemzetbiztonság és az üzleti alapon működő magánszektor témakörét vizsgálva, bizonyos területeken mégis találkozhatunk az úgynevezett *outsourcing,* vagyis adott feladatok üzleti alapon történő kiszervezésének gyakorlatával. A jelenség kapcsán a nemzetközi szakirodalmak is alapvetően annak alkotmányossági problémájára hívják fel a figyelmet, annak az elvi kérdésére, hogy – akár az ellenőrzési funkció megtartásával is – az állam „erőszak-monopóliumához" tartozó tevékenységek kiadhatók-e egyáltalán külső együttműködő partner számára?

A biztonságért felelős ágazatok szélesebb körét tekintve a kiszervezés általánosan elfogadott jelenség, gondoljunk csak a rendészeti tevékenység bizonyos területeire (például őrző-védő cégek), hiszen „a közbiztonság nem csupán állami szolgáltatás, hanem megvásárolható áru".[30] Mindezt erősíti, hogy a biztonság olyan közös társadalmi érdek, ahol a feladatok nemcsak adott állami szervek, hanem a magánszféra és az egyének közös munkáját is szükségessé tehetik, ezzel azonban sajátos piaci lehetőségek jönnek létre. Mint Balogh László Levente megfogalmazza tanulmányában, az erőszak-privatizáció „egy egyre dinamikusabban fejlődő erőszakpiac kialakulását, és az erőszak bizonyos formáinak magánkézben való összpontosulását jelenti".[31] Az erőszak-privatizáció folyamatának irányai kapcsán, tanulmányában[32] alulról felfelé irányuló *(bottom-up),* és felülről lefelé irányuló *(top-down)* formákat különböztet meg, ahol formai értelemben

[29] Finszter (2019): i. m. 105.
[30] Finszter (2019): i. m. 101.
[31] Balogh László Levente: Állam és erőszak. *Politikatudományi Szemle,* 20. (2011), 1. 119–132.
[32] Balogh (2011): i. m. 130.

a „felülről lefelé irányuló" formához – ahol a gazdasági kiadások csökkentése és a hatékonyság növelésének egyéb indokai kereshetők – sorolja a biztonsági szektor önálló gazdasági ágazattá válását. Ennek értelmében a nemzetbiztonság egyes elemei is ehhez a formához sorolhatók, bár azon véleményeknek is helye lehet, hogy a rendkívül érzékeny nemzetbiztonság semmilyen területen nem szervezhető ki.

A gyakorlatban, napjaink összetett feladatrendszerei alapján a pontos választóvonal rendkívül nehezen határozható meg, ugyanakkor a nemzetközi példák kapcsán az is látható, hogy a hatékonyság növelése érdekében a nemzetbiztonsági szféra is gyakran fordul a számára megbízhatónak vélt külső vállalati feleknél meglévő képességek felé. Ez az együttműködés azonban még nem feltétlen jelenti az adott tevékenység kiszervezését, gyakran csak a nemzetbiztonsági célú feladatok, illetve az információgyűjtést segítő folyamatok elengedhetetlen, illetve azt hatékonyan támogatni tudó nemzetbiztonsági kapcsolatrendszereinek működtetését jelentik. Látható, hogy vannak olyan területek (például fejlesztési, informatikai, logisztikai, képzési területek adott részei), amelyek bizonyos elemeiben akár leválaszthatók is lehetnek a nemzetbiztonsági feladatkör központi elemétől, és amelyekre a struktúra, hasonlóan más állami szervekhez, egyszerűen piaci megrendelőként tekinthet. Az ezeken a területeken igénybe vett szolgáltatás/termék alapvetően nem különbözik egy civil szereplőnek nyújtottól, ráadásul e képesség kiépítése, fenntartása akár rendkívüli erőfeszítéseket is okozhat az adott szervezet számára (gondoljunk csak a piaci alapon működő informatikai fejlesztésekre, amelyekre az amerikai titkosszolgálati botrány is ráirányította a figyelmet).

Az együttműködés két fő formáját tekintve (lásd Pap András László munkájában[33] „diszpozitív" és „kógens" típusok), megjelennek a jogszabályi kötelezettségen alapuló együttműködési formák, illetve az adott fél önkéntes (alapvetően piaci alapú) együttműködésének lehetősége. Az első esetben gondolhatunk például a pénzintézeteket, postai vagy akár infokommunikációs szolgáltatókat együttműködésre kötelező jogszabályokra. A második (piaci alapon kialakuló együttműködési) forma kapcsán az adatfeldolgozás vagy akár a kutatás-fejlesztés területén megvalósuló együttműködések, kutatási célú kapcsolatok említhetők. E kapcsolatoknak létezhet egy, a partnerség jegyeit mutató (közös munkán és érdekeltségen alapuló) formája és egy mélyebb, az egész

[33] Pap András László: *A megfigyelés társadalmának proliferációjától az etnikai profilalkotáson át az állami felelősség kiszervezéséig.* Budapest, L'Harmattan, 2012. 40–41.

tevékenységet kiszervező formája. Adott területeken megtalálható az úgynevezett PPP *(Public-Private Partnership)* a köz- és magánszféra közötti partnerségi típus is, amely alkalmazásának megítélése szintén vitatottnak tekinthető, hiszen akár ütköző érdekek, így a „biztonsági ügynökségek biztonságot maximalizáló logikája és a magánvállalatok profitmaximalizáló logikája”[34] találkozhat. Az aggodalmak kapcsán a magánszektor szereplőinek „elszámoltathatósága, felügyelete és legitimitása” is felmerülhet.[35]

Tényként állapítható meg, hogy a különböző szintű együttműködések jelentősége napjainkban egyre inkább felértékelődik, hiszen a nemzetbiztonsági szervezetek sem tudják leválasztani tevékenységüket, képességeik fejlesztését a külső, rendkívüli ütemben fejlődő környezettől. Idesorolhatók a titkosszolgálati technológiák „kereskedelmi piacán” megjelenő vállalkozásokkal fenntartott, eszközrendszerek beszerzésére, akár a sajátos tudásbázist igénylő szoftverek és megoldások fejlesztésére irányuló együttműködések. Jelen vannak a nagy mennyiségű adatok feldolgozására szakosodott privát cégek, amelyek például az internet és a közösségi felületekhez kapcsolódó fejlesztéseikkel, termékeikkel kínálhatnak egyedi megoldásokat felhasználóik számára (például kémszoftverek alkalmazása). Itt értelmezhetők a nyílt forrású információgyűjtés (OSINT) üzleti alapon működő célirányos termékei, amelyeket mind az állami, mind a piaci szektor előszeretettel alkalmaz, vagy akár az úgynevezett adatbróker cégek, amelyek a különböző helyeken keletkező adatok megszerzésével, akár azok elemzésével-értékelésével kapcsolódhatnak a biztonsági szervek munkájához. Ennek gyakorlatát főként az amúgy is elterjedt nemzetbiztonsági kiszervezési megoldásokkal érintett országokban (például Amerikai Egyesült Államok) láthatjuk.

Habár a piaci alapon működő együttműködés formáihoz sorolható, mégis talán attól elkülönülten érdemes megemlíteni a nemzetbiztonságot közvetlenül befolyásoló fegyveres konfliktusokban a hírszerzéssel-felderítéssel, őrzéssel-védelemmel, logisztikai feladatokkal foglalkozó magáncégek, katonai magánvállalatok igénybevételének rendkívül vitatott, sokszor botrányoktól kísért nemzetközi példáit. Alkalmazásuk során gyakran az állami és gazdasági szereplők egybeeső kormányzati és üzleti érdekei (például olajipari érdekeltségek védelme a konfliktustérségben) és nem utolsósorban szerződéses viszonyuk (így elszámoltathatóságuk korlátja)

[34] Oldrich Bures – Helena Carrapico: Private Security beyond Private Military and Security Companies: Exploring Diversity within Private-Public Collaborations and its Consequences for Security Governance. *Crime, Law and Social Change,* 67, (2017), 3. 229–243.

[35] Bures–Carrapico (2017): i. m. 237.

jelenik meg. Alkalmazásukra és azok mértékére számos nemzetközi példát láthatunk,[36] jelentősége a hibrid hadviselés kapcsán vélhetően a későbbiekben is erősödni fog.

Nemzetbiztonsági értelemben sajátos állami és vállalati együttműködésként jelentkezik a fedőtevékenységre használt üzleti-gazdasági környezet kialakítása, illetve nemzetbiztonsági feladatokba történő bevonása. Ugyanakkor ezek nem sorolhatók a hagyományos értelemben vett kiszervezés kategóriájához, hiszen mögöttük valójában nemzetbiztonsági szervek állnak, és a működtetés okait, formáját is a nemzetbiztonsági érdekek mentén kell keresnünk. A szolgálatok számára feladatként, a civil piaci szereplőkkel azonos gazdasági környezetben működő, azonban ellenérdekelt nemzetbiztonsági kötődésű vállalatok kiszűrése jelentheti, hiszen a velük való esetleges együttműködés már biztonsági kockázatot hordozhat magában. 2020 elején került nyilvánosságra, hogy a semlegesség szimbólumaként megjelenő Svájcban, a világ egyik vezető rejtjelező eszközök gyártásával foglalkozó vállalata (Crypto AG.) 2018-ig, közel 50 éven keresztül az Egyesült Államok hírszerzésének (CIA) a tulajdonában volt.[37] A külföldi kormányoknak rejtjelező eszközöket biztosító vállalaton keresztül így az amerikai fél számára hozzáférés nyílhatott mások féltve őrzött titkaihoz. A megoldás – ha talán nem is ilyen eredményességgel – jelen lehet más országok gyakorlatában is, így biztonsági szempontból a nemzetbiztonsági ágazatban általánosságban a nemzeti, állami vállalatokkal való együttműködést preferálják.

Összességében a kiszervezés tevékenysége kapcsán számos olyan kérdés merülhet fel, amelyek befolyásolhatják a nemzetbiztonsági gondolkodás és felhasználás jövőbeli alakulását. Ezek között vethetők fel az alábbi teoretikus kérdések:

– Melyek azok a szolgálatok működéséhez kapcsolódó területek, amelyek a „nemzetbiztonság" sérelme nélkül kiszervezhetők egy piaci alapú környezetbe, és milyen mértékben? (Itt érdemes hangsúlyozni, hogy egy

[36] Az Amerikai Egyesült Államok példáját kiemelve, a katonai magánvállalatok és magán hírszerző cégek alkalmazása nem történeti előzmények nélkül való. A II. világháború időszakában a hírszerzés és információgyűjtés területén például a Pond (1942–1955) [lásd Mark Stout: The Pond: Running Agents for State, War, and the CIA. The Hazards of Private Spy Operations. Studies in Intelligence, 48. (2004), 3. 69–82.] nevű szervezet vált ismertté, majd 50 évvel később az Eric Prince által alapított, külföldi katonai konfliktusokban sajátos szerepet betöltő Blackwater szervezete került vitatott tevékenységével a nyilvánosság középpontjába.

[37] Imogen Foulkes: Swiss Crypto AG spying scandal shakes reputation for neutrality. *BBC News,* 2020. február 16.

adott terület teljes kiszervezése a képességvesztés elkerülése érdekében akár kényszerű folyamatos együttműködésre ítélheti a szervezeteket.)
- Milyen formáló (káros vissza)hatása lehet a kiszervezésnek (például fejlesztés) a nemzetbiztonság központi folyamataira?
- Mennyire tekinthető megbízhatónak az adott együttműködő fél által biztosított információ (adatbrókerek jelenléte), és ez torzíthatja-e a nemzetbiztonsági szolgálat döntés-előkészítési tevékenységét?
- Mennyire és hogyan biztosítható a nemzetbiztonsági és információgyűjtési érdekek hosszú távú védelme?
- A korábban szervezeten belül végzett folyamatok külső együttműködő környezetbe helyezése hogyan befolyásolhatja az állomány elvándorlását? (Különösen érintett az IT-szektor, ahol a magasabb fizetések hatása nemzetközi példák alapján is jól látható.)[38]

A nemzetközi szakirodalom alapján elmondható, hogy az ezredfordulót követően a terrorizmus elleni küzdelem felerősödésével a kiszervezés súlya felerősödött, bár a 2013-ban kirobbant amerikai megfigyelési botrány rávilágított a megoldás sérülékenységére is. Amellett, hogy a gyakorlat segítheti adott területeken a gazdaságosabb működést, akár a külső környezethez igazodó innovatív ismeretek becsatornázását, számos biztonsági kockázatot hordoz magában. Sérülhet a nemzetbiztonsági tevékenységek irányainak, képességeinek titkossága, de a profitorientált üzleti szemlélet torzíthatja is a nemzetbiztonsági feladatok ellátását. Az érintett piaci szereplők egy idő után a nyereségük növelése érdekében a folyamatokat befolyásoló politikai szereplők számukra kedvező döntése érdekében lobbitevékenységeket kezdhetnek.[39] Rendkívül szélsőséges esetben egyes döntések is piacorientálttá válhatnak, „miközben az állam egyedülálló legitimációjának köszönhetően a politikai döntések sohasem követhetik kizárólag a magánhaszon elveit".[40]

[38] Adott feladatok (például K+F) kiszervezése esetén gyakran a korábban állami szférában dolgozó alkalmazottak már a profitorientált vállalati környezetben, sajátos jogviszonyban (például szerződéssel) végzik el a korábban még az állami szférában teljesített feladatokat.

[39] A biztonság szélesebb területei kapcsán lásd Bures–Carrapico (2017): i. m. 239.

[40] Balogh (2011): i. m. 131.

Új generációk hatása a nemzetbiztonsági gondolkodásra

Drusza Tamás

A változás természetének változása

Természetes, hogy a dolgok változnak körülöttünk, mi pedig igyekszünk alkalmazkodni a változásokhoz, ezt hívhatjuk fejlődésnek is. Az életünk utóbbi időszaka abból a szempontból hozott újdonságot, hogy a változások sebessége „hirtelen" felgyorsult. E szokatlanul gyors változás kiindulópontja a robbanásszerű technológiai fejlődés volt. A változás egyensúlytalanságokat eredményezett a mindennapokban, mert sem az emberek, sem az intézmények nem voltak felkészülve rá. A szervezeteknek évtizedes szervezeti kultúrát, az embereknek évtizedes szokásokat kellene átalakítani nagyon rövid idő alatt. Erre senki nincs felkészülve, így a folyamatot rengeteg konfliktus kíséri. Azonban már az is kevés, ha próbálunk viszonylag időben reagálni, mert mire ezt megtesszük, a körülmények tovább változnak. Így mindennapi gondolkodásunk részévé kell tenni egy új szemléletet, amit proaktivitásnak lehet nevezni. Ennek lényege, hogy nem a megtörtént változásra reagálunk, hanem a várható, de még be nem következett változásra készülünk fel.

Ebből fakadóan az ehhez hasonló képzési anyagok szemléletének, belső arányának is igazodnia kell a változásokhoz. A múltról csak a jelen és a jövő megértéséhez szükséges mértékig kell szólnia. A jelenről olyan mértékig, hogy megalapozott kijelentéseket tehessünk a jövővel kapcsolatosan. A jövőnek pedig az eddigiekhez képest jelentős mértékben megnövekedett terjedelemben kell megjelennie. E fejezet megírásával ezt a szemléletet kívánjuk erősíteni, amely révén jobban megérthetők a jövő kihívásai, problémái, hogy még bekövetkezésük előtt fel lehessen rájuk készülni.

E fejezet célja, hogy megvizsgálja, hogy a generációváltás felgyorsulása és az újabb – elsősorban az Y és Z generációk eltérő – jellemzői milyen módon hathatnak a nemzetbiztonsági szervezetrendszerre. Bár a titokzatosság kevés információt enged láttatni, azért az bizonyos, hogy ezek a szervezetek is szembesülnek a generációs kihívással. Magyarország érdekeinek érvényesítése szempontjából fontos, hogy az ezen munkálkodó szervezetek milyen képességekkel rendelkeznek, hogyan tudnak alkalmazkodni a változó környezeti feltételekhez.

https://doi.org/10.36250/00904_05

Az új generációk a titkosszolgálatoknál is másként viszonyulnak ugyanazon helyzetekhez, problémákhoz, másképp élik az életüket, dolgoznak, kommunikálnak, eltérő elvárásaik és céljaik vannak, amelyeket új módokon érvényesítenek és valósítanak meg.[1] Ez a körülmény nemzetbiztonsági szervezetek esetében is megteremti az igényt új megoldások iránt. Ezek kimunkálásához azonban új szemlélet is szükségeltetik, ami csak nagyon ritkán adódik a régi tapasztalatokból.

A generációs attitűd változása

A társadalmi generációváltás folyamata egyidős az emberiséggel, ugyanakkor csak az utóbbi évtizedekben indultak meg az ezzel kapcsolatos intenzív kutatások. Biológiai értelmezésben az azonos korúakra használhatjuk a generáció kifejezést, illetve a szülők és gyerekeik közötti átlagos életkori különbséget is jelentheti. Manapság azonban gyakorlati jelentősége sokkal inkább a szociológiai értelemben vett generációnak van. Ez olyan személyek csoportja, akik azon a történelmi időn és téren osztoznak, amely kollektív személyiséget biztosít nekik.[2] A kollektív személyiség következménye pedig a hasonló attitűd,[3] azaz az érzelmek, a tudás és az ezekből fakadó cselekvések hasonlósága.[4]

A generációváltás korábban egy lassú, kiszámítható folyamat volt.[5] Ennek során az idősebb személyek átadták tudásukat és tapasztalataikat a fiatalabbaknak, akik ezt saját tapasztalataikkal formálták, bővítették. E folyamat során az újabb nemzedékek világról alkotott elképzelései lassan, de folyamatosan változtak, és mikor már kellően nagymértékben tértek el a korábbi korosztályok nézőpontjától, akkor újszerű gondolkodásmódok alakultak ki, amelyek újszerű cselekvésekhez vezettek, és ekkor megtörtént egy új szociológiai generáció

[1] Cortney Weinbaum – Richard Girven – Jenny Oberholtzer: *The Millennial Generation – Implications for the Intelligence and Policy Communities.* Santa Monica, Rand Corporation, 2016. 6.

[2] Buda András: Generációk, társadalmi csoportok a 21. században. *Magyar Tudomány,* 180. (2019), 1. 120–129.

[3] Az attitűd fogalmával kapcsolatosan. Csepeli György: *Szociálpszichológia.* Budapest, Osiris, 2001. 123.

[4] A hasonlóság nem jelent egyformaságot. Jelent viszont jól azonosítható közös pontokat, mintázatokat, trendeket.

[5] Besenyei Lajos: A generációváltás forradalma. *Opus et Educatio,* 3. (2016), 4. 375.

megjelenése. Az utóbbi évtizedekben azonban radikális változások történtek ebben a folyamatban.

Az első különbség a generációváltás sebességének „hirtelen" megnövekedése. A korábbi történelmi korszakokban évszázadok, de legalábbis emberöltők kellettek ahhoz, hogy az egymást követő biológiai nemzedékek attitűdjében lényeges változás álljon be. Ennek főleg az volt az oka, hogy a világ változása lassú, az új tudás terjedésének sebessége igen alacsony volt. A 21. század egyik nagy változása, hogy az egyén életében bekövetkező újszerű életesemények száma nő,[6] illetve az új technológiák révén az ismeretek szinte azonnal megoszthatóvá váltak bárkivel. A gyorsuló világhoz gyorsuló alkalmazkodás szükséges, ami gyorsuló attitűdváltozásban, azaz gyorsuló generációváltásban fejeződik ki. A Z generáció kifutási ideje a várakozások szerint körülbelül szűk 15 év, míg a 21. század korábbi generációi esetében ez még 20–30 év is lehetett, korábban pedig ennél is lényegesen több. (Érdekes megjegyezni, hogy a nemzedékváltás, azaz a biológiai értelemben vett generációváltás még lassult is azzal, hogy egyre nő az az életkor, amelyben a nők gyermeket vállalnak.) A sebességből (és a növekvő átlagos élettartamból) fakad, hogy egy adott társadalomban a korábbi két-három helyett öt-hat generáció[7] (azaz kollektív attitűd) van jelen egyidejűleg, míg a munkaerőpiacon a jellemző egy-két generáció helyett immár három-négy[8] generáció van jelen.

A generációváltás másik fontos jellemzője a térbeli kiterjedtsége: az újabb generációk már globálisnak tekinthetők. A ma emberének horizontját jelentősen kitágította a helyváltoztatási lehetőségek bővülése és a virtuális tér jelentette lehetőségek. Ebből fakad, hogy a földrajzi távolság már egyre kevésbé jelent szükségszerűen különböző attitűdöt, ennek formálásában bármely fontos esemény szerepet játszhat, lokációtól függetlenül. Végül talán a legfontosabb újdonság a generációs attitűd változásának módjában lelhető fel. A szocializáció folyamatában megszokott rend a feje tetejére állt. Korábban a fiatalabb generációk

[6] Meretei Barbara: Generációs különbségek a munkahelyeken. *Vezetéstudomány,* 48. (2017), 10. 10.

[7] Törőcsik Mária – Szűcs Krisztián – Kehl Dániel: Generációs gondolkodás – A Z és az Y generáció életstílus csoportjai. *Marketing & Management,* (2014), 2. klsz. 3–15.

[8] A generációk időbeni elhelyezését illetően a kutatók sem egységesek. Egy születési év alapján gyakran alkalmazott felosztás a következő: Veteránok (–1945), baby boomer (1945–1965), X generáció (1965–1980), Y generáció (1980–1995), Z generáció (1995–2010). Ez a felosztás többek között azt is mutatja, hogy egy generáció kifutási ideje az utóbbi egy évszázadban csökkenő tendenciát mutatott, így egy adott időszakban a munkaerőpiacon jelen lévő generációk száma is növekedett.

tudásuk túlnyomó részét az idősebbektől szerezték, azt saját tapasztalataikkal kis részben kiegészítették. A felgyorsult fejlődés azonban azt eredményezte, hogy a digitális generációk már tudásuk jelentős részét nem az idősebbektől, hanem saját korosztályuktól szerzik meg.[9] A szocializáció folyamatának megfordulása mára azt is eredményezte, hogy fontos dolgokat az idősebb generációk tanulnak a fiatalabbaktól. A fordított szocializáció jelensége olyan eddig nem ismert helyzeteket teremtett, amelyben a társadalom hagyományos működési mechanizmusai közül számos egyszerűen már nem működőképes. Mindez a fiatalabb generációkban kialakította azt az érzést, hogy ők már fiatalon többet tudnak, és ezért „értékesebbek", mint az idősebbek. A felnövő korosztály számára – szemben a korábbi generációkkal – a kor így ma már önmagában kevéssé hordoz értéket. Ez együtt járt az idősebbek iránt tanúsított tisztelet csökkenésével. Másrészt ugyanakkor az új világ egyes jelenségeinek nehezebb megértése az idősebb korosztályban előhívott egyfajta kisebbségi érzést. Ezek az új érzések vezettek oda, hogy a jelenlegi multigenerációs társadalmunkban a generációs konfliktuspotenciál nagyobb, mint a korábbi időszakokban volt. Mindez szükségszerűen erősebb ott, ahol több generáció folyamatos interakciója elkerülhetetlen. Tipikusan ebbe a körbe tartoznak például az államigazgatási szervezetek, így a nemzetbiztonsági érdekek érvényesítésért felelős szervezetek is.

A Z generáció

Manapság az úgynevezett Z generáció képviseli a várható változás világát a legjobban. Tagjai egy megváltozott és gyorsan átalakuló világhoz próbálnak alkalmazkodni, ez irányú kompetenciáikat fejlesztik. Ezt a „régi", most még a többséget alkotó világ persze saját szempontjából furcsának találja, olykor „rossz" irányként értékeli. Egy évtized múlva azonban a társadalom jelentős és aktív részét már az újak fogják alkotni, és így komoly befolyásuk lesz a világra. A probléma megértése szempontjából nem az egyes életkori csoportok a fontosak, hanem az a tendencia, amit a generációváltozás jelensége mutat.

A Z generáció napjainkban kezd kilépni a munkaerőpiacra, így a világra gyakorolt befolyása a közeli jövőben drasztikusan növekedni fog. Ezen okoknál fogva érdemes alaposabban szemügyre venni e csoport jellegzetességeit. A Z generáció legfőbb jellemzője, hogy nagyrészt már nagyon fiatalon találkoztak a digitális

[9] Besenyei (2016): i. m. 374.

technológiákkal, aminek révén ők a világ első globális bennszülött[10] nemzedéke. Számukra az információ gyors megszerzése, megosztása a természetes állapot, a világ bármely pontján is éljenek, azonos eseményeket tudnak meghatározónak tekinteni. Mindezekből fakadóan közös attitűdjük is különbözik a korábbi generációkétól. A kutatások alapján az alábbi közös jellemzőkkel írhatók le e generáció tagjai:[11]

- sokkal fontosabb számukra a hitelesség, ez a tekintély első számú forrása. A pozícióból fakadó tekintélyt kevésre értékelik;
- kevésbé szabálykövetők, kritizálnak, megkérdőjeleznek, újraértékelnek;
- fontos számukra az élmény, a megélés, „csak azt hiszik el, amit látnak";
- gyorsabb az életritmusuk, elutasítják azt, ami ezt megpróbálja „feleslegesen" lassítani;
- bátrak és kezdeményezők, bíznak önmagukban;
- természetesnek veszik a változást, nem félnek tőle, sőt igénylik a változatosságot;
- kevésbé lojálisak, mint a korábbi generációk;
- inkább okosak, mint bölcsek, azaz a tudást fontosabbnak tartják a tapasztalatnál;
- pragmatikusak, azt becsülik meg, aminek gyakorlati haszna van.

A fenti felsorolás persze közel sem jelenti azt, hogy az adott generáció minden tagját minden fenti tulajdonság ugyanolyan mértékben jellemzi. Azért tartottuk fontosnak alaposabban bemutatni a Z generációt, mert ez a generáció mutatja a legnagyobb eltéréseket a társadalom gerincét alkotó baby boom és X generációktól, de még az Y generációtól is.

A generációs felosztás tudományos háttere folyamatosan fejlődik, az egyes vizsgálatok egyre pontosabbak, ezekre alapozva lehet a gyakorlati teendőket megfogalmazni. Lássuk, hogy az új generációk által képviselt gondolkodás hogyan hat és fog hatni a nemzetbiztonsági gondolkodásra és működésre.

[10] Buda (2019): i. m.

[11] Pál Eszter – Törőcsik Mária: *Irodalmi áttekintés a Z generációról.* Pécs, Pécsi Tudományegyetem, 2013; Törőcsik–Szűcs–Kehl (2014): i. m.

A nemzetbiztonsági tevékenység érintettjei

Ahhoz, hogy vizsgálhassuk az emberi viselkedés változásának nemzetbiztonsági gondolkodásra gyakorolt hatását egy olyan módszert alkalmazunk, amellyel számba vehetjük e két tényező kapcsolódási pontjait. Remekül alkalmazható e célra az úgynevezett érintetti (más néven: *stakeholder*) elemzés.[12] Ez a vezetéstudományi elemzési eszköz onnan kapta a nevét, hogy minden olyan csoportot igyekszik azonosítani, amelyet valamilyen formában érint a szervezet működése, illetve amelyek kölcsönösen befolyással vannak egymásra. Az elemzés során nemcsak felsoroljuk az érintetteket, hanem jellemezzük is azokat, külön kitérve az adott csoport céljaira, a tagokat a csoporthoz való tartozásból fakadóan jellemző közös attitűdjére, mint a viselkedésüket jól leíró tényezőkre. Ebből következően meg tudjuk határozni, hogy a szervezet milyen célokat és mi módon kövessen.[13] Elemzésünk során a nemzetbiztonsági feladatot ellátó szervezeteket egyetlen rendszerként fogjuk kezelni. Ezt azért tehetjük meg, mert az egyes szervezetek szorosan együtt dolgoznak, és így érintettjeik között jelentős átfedések találhatók.

Belső érintettek

Azokat a személyeket nevezzük belső érintetteknek, akik valamilyen jogviszony keretében a szervezethez tartoznak, annak részei. A nemzetbiztonsági szolgálatok esetében az alábbi két fő csoport azonosítható:

- A legnagyobb csoport a *munkatársaké,* ezen belül két további csoportot különböztethetünk meg.
  - *Műveleti állomány:* A műveleti állomány sajátossága, hogy személyes kompetenciáikat tekintve több szempontból válogatott csoportról van szó. Ebből fakadóan elvárásaik is különböznek az átlag munkavállalóétól. Hatványozottan jellemző, hogy nemcsak munkahelyet keresnek, hanem kihívást jelentő feladatokat is. Az újabb generációk érkezésével számítani kell továbbá arra, hogy számukra egyre fontosabb a munka és a magánélet egyensúlya. Így a hagyományos karrier-

[12] Chikán Attila: *Vállalatgazdaságtan*. Budapest, Aula, 2008. 22–27.
[13] Chikán (2008): i. m. 23.

és munkafelfogás e csoportok tagjainak kevésbé elfogadható.[14] Fontosabb még számukra az objektív teljesítményértékelés, az önállóság, kevésbé tűrik a szoros irányítást.
E jellemzők figyelmen kívül hagyása, magasabb mobilitásuk okán, az új generációk tagjai esetében a korábbiakhoz képest rövid idő alatt a szervezet elhagyásához vezet. Ez, figyelembe véve, hogy a titkosszolgálatok műveleti munkatársainak képzése rendkívül sokba kerül, illetve hogy munkájuk során számos érzékeny adat birtokába jutnak, veszteséget jelent a szolgálatoknak. A rendszernek ebből fakadóan elemi érdeke a fluktuáció alacsonyan tartása.

- *Támogató állomány:* Ebbe a csoportba tartoznak azok a munkatársak, akiknek elsődleges feladata a műveleti munka támogatása. Jellemzően informatikai, pénzügyi, HR- és jogi szakemberekről van szó. A csoport fontosságát az adja, hogy szaktudásuk révén e csoport tagjaiért is erős verseny folyik a munkaerőpiacon.

– A szervezetben *vezető beosztást betöltők:* Jóllehet a vezetők is a szervezet munkatársai, de mivel a beosztottakhoz képest eltérő feladat-, felelősségi és hatáskörrel rendelkeznek, amit a nemzetbiztonsági tevékenység specialitása és a hivatásos jogállás csak erősít, így célszerű külön kezelni őket. Mivel a jogszabályok általában elég lassan és pontatlanul követik a működési környezet változásait, ez a csoport két irányból is „nyomásnak" van kitéve: egyszerre kellene megfelelnie a szigorú jogi szabályozóknak és alkalmazkodnia a gyors környezeti változásokhoz. Mindezt nehezíti, hogy a korábbi hivatásos szolgálati szervezeti kultúrát a pozícióból fakadó tekintély és a feltétlen engedelmesség jellemezte, míg az újabb generációk számára ezek nem maguktól értetődők. Emellett vezetőként és beosztottként is sokkal gyakorlatiasabbak, így nemcsak az utasítás tartalma, de indoka is a korábbiaknál fontosabb számukra. Mindezek eredményeként a jövőben egyre inkább számítani lehet a gyors ütemben elavuló szabályozók és a cselekedetek növekvő arányú összeütközésére, valamint a generációs konfliktusok szaporodására.

A munkatársi és vezetői állományban várhatóan gyorsan fog növekedni az újabb generációkba tartozók száma, ebből fakadóan pedig a generációs kihívások aránya is. Ennek főbb formái vélhetően az alábbiak lesznek:

[14] Weinbaum–Girven–Oberholtzer (2016): i. m. 27.

- a hierarchikus működéssel való azonosulás csökkenő mértéke;
- a „lojalitás" csökkenő mértéke, azaz a leszerelések aránya növekvő tendenciát fog mutatni;
- a szervezeti konfliktusok növekvő aránya. A generációs konfliktus egyik eredője a tudás és a tapasztalat fontosságának eltérő megítélése. A hivatásos szolgálatot teljesítő szervezetekben a munkatapasztalat általában magasabbra értékelt, mint a szaktudás. A nemzetbiztonsági rendszerben általában nincs előírt végzettségi kritérium, mivel a tevékenység multidiszciplinárisnak mondható. Ebből fakadóan a munka- és szervezeti tapasztalatnak a hétköznapi működésben és a javadalmazási rendszerben is komoly szerepe van. Ezzel szemben az újabb generációk számára már fontosabb a szaktudás. Egyrészt ők maguk is a legújabb tudással vannak felvértezve, másrészt a folyamatos tanulás is az életük természetes része. Így szakmai tapasztalat helyett, illetve mellett egyre többre értékelik a tudást, az előbbi helyett az utóbbi válik a tekintély forrásává.

Külső érintettek

A külső érintettek azok, akik valamilyen formában kapcsolatban állnak a nemzetbiztonsági szervezetrendszerrel, de nem részei annak.

- *Ellenérdekelt személyek, szervezetek:* A nemzetbiztonsági szervezetek szempontjából legfontosabb személyi körben természetszerűleg egyre nagyobb lesz az új generációs személyek aránya. Ennek legfontosabb következménye az lesz, hogy a célszemélyi viselkedésminták is át fognak alakulni, ami lényegi hatással lehet a nemzetbiztonsági érdekeket veszélyeztető magatartásformákra, valamint a konspirációs eszközökre és módszerekre. A fiatalabb korosztály sokkal képzettebb és fogékonyabb az újszerű informatikai eszközök és szoftverek alkalmazását illetően, így újszerű módokon és gyakrabban alkalmazza ezeket. Viselkedésük, cselekedeteik jelentősen különböznek az eddig megszokottaktól, így fokozott figyelmet kell fordítani ezek megismerésére, megértésére.
- *Politikai irányítók és ellenőrzők:* A politikai irányítást és ellenőrzést végző csoportok tagjai jellemzően az idősebb, baby boom vagy X generációból tevődtek össze. Több érv szól azonban amellett, hogy ez az állapot a jövőben változhat. Egyrészt a politika is reagálni fog arra, hogy az új generációk egyre nagyobb hányada válik választókorúvá. Másrészt

megjelentek már olyan politikai erők, amelyek tagjai kései Y, illetve akár Z generációs politikusok. Így nem kizárható, hogy a fiatal korosztály akár már a következő évtizedben politikai irányító, ellenőrző szerepbe kerülhet.[15]

– *Információfelhasználók:* Azok a személyek tartoznak ebbe a csoportba, akik a nemzetbiztonsági szervezetektől kapott információkat felhasználják. A felgyorsult világban fontos előnyt jelent az információhoz jutás sebessége. Ezt az igényt csak erősíteni fogja, hogy az információt felhasználók között is egyre nagyobb arányban találhatunk majd új (Y, de akár Z) generációs személyeket.
– *Titkos együttműködők:* Ők azok, akik valamilyen formában segítik a nemzetbiztonsági szolgálatok tevékenységét. A titkos együttműködők között is egyre nagyobb arányban találhatók majd újabb generációs személyek. Az USA-ban folytatott kutatások azt mutatják, hogy az Y generáció tagjai alapvetően kevésbé bíznak az állami intézményekben, így bizalmuk csak fokozott erőfeszítések és új megközelítések révén nyerhető el.[16] Ez várhatóan az őket követő generáció tagjainál sem lesz másképpen.
– *Állományba jelentkezők:* A nemzetbiztonsági szolgálatok számára is létfontosságú az utánpótlás megszervezése. Régen úgy válogathattak a jelentkezők között, hogy a jelentkezők alapvetően tudtak és akartak is alkalmazkodni a szervezetek értékrendjéhez, szervezeti kultúrájához. Ezt a folyamatot azonban az utóbbi időben mindkét oldalról kihívás érte. Nemcsak a jelentkezők száma esett vissza, de a jelentkezők egyre kevésbé illeszkednek bele a szervezeti önképbe, és csökkenő mértékben hajlandók alkalmazkodni a nemzetbiztonsági szervezetek írott és íratlan szabályaihoz, szokásaihoz. A régi kiválasztási szemlélet így problémát okozhat azzal, hogy az értékes embereket is kiszűrheti pusztán a régi szervezeti kultúrához való gyengébb illeszkedése okán.[17]
– *Védett intézmények munkatársai:* A védett intézmények munkatársai egyszerre alanyai és partnerei a nemzetbiztonsági rendszer működésének. Együttműködésük, bizalmuk akkor szerezhető és tartható meg,

[15] A folyamat az USA-ban is megfigyelhető: Weinbaum–Girven–Oberholtzer (2016): i. m. 4.
[16] Weinbaum–Girven–Oberholtzer (2016): i. m. 14–15.
[17] Hasonló kihívásokkal szembesülhet az USA hírszerző közössége: Weinbaum–Girven–Oberholtzer (2016): i. m. 29–30, 39.

ha a szolgálatok képesek professzionális módon, az új generációk változó igényeihez alkalmazkodva ellátni a védelmi tevékenységet.

– *Társszolgálatok:* A nemzetbiztonsági rendszer egyik jellegzetessége, hogy szervezetei az újszerű kihívások és fenyegetések elleni küzdelem élvonalában vannak. Ebből fakadóan jogos elvárás velük szemben, hogy mintaként szolgáljanak a környezeti kihívásokhoz történő rugalmas és gyors alkalmazkodás tekintetében. Élen kell járniuk az új jelenségek (például ipari forradalom 4.0, generációs problémák stb.) okozta új problémák megismerésében, megértésében, új eszközök és módszerek alkalmazásában. Ennek elmaradása a szolgálatok tekintélyének csökkenéséhez vezethet, ami negatív hatással van az együttműködés hatékonyságára.
– *Partnerszolgálatok:* A külföldi partnerszolgálatok együttműködése nélkül a nemzetbiztonsági szolgálatok működése sokkal kevésbé lenne eredményes, ezért nagyon fontos a velük való jó, kölcsönös bizalmon alapuló kapcsolat kiépítése. Azt megállapíthatjuk, hogy a generációs változások számukra is hasonló kihívást jelent, mint a magyar szolgálatok számára. A különböző partnerszolgálatok különböző mértékben alkalmazkodhatnak, de azt elmondhatjuk, hogy ha a magyar szolgálatok lemaradásba kerülnek a folyamat során, az negatívan hathat a partnerszolgálatokkal való kapcsolataikra is.
– *A társadalom egésze:* A nemzetbiztonsági szervezetek egyik jellegzetessége, hogy közvetve a teljes társadalom érintettje a működésnek. A nemzetbiztonsági szolgálatok működésének sikerei, kudarcai az egész társadalom biztonságérzetére hatással lehetnek. Az emberek szolgálatokhoz való viszonya a titkosság okán nagyobb érzelmi telítettségű, így az ezekkel kapcsolatos hírek jelentős hatással lehetnek a közvéleményre. Ezektől a szervezetektől a társadalom tagjai biztonságot, kiszámíthatóságot és támogatást várnak, és ezt a lehető legnagyobb mértékben érzékelni, tapasztalni szeretnék, ezt azonban a szervezetek teljes titkolózása jelentős mértékben akadályozza. Az újabb generációk némileg bizalmatlanabbak, így csak nyitott, partneri jellegű kommunikációval nyerhető el a bizalmuk.

A fentiek alapján jól látszik, hogy a nemzetbiztonsági szervezetek társadalmi (emberi) környezete radikális átalakuláson megy keresztül. A szervezeteknek erre a jelenségre válaszokat kell találni és adni, ennek elmaradása ugyanis komoly szervezeti és ebből fakadó biztonsági válságokhoz vezethet.

A nemzetbiztonsági szervezetek alkalmazkodási folyamata

Az alkalmazkodás azt jelenti, hogy az adott szervezet az új körülményekhez igazítja működését. A nemzetbiztonsági szolgálatok ugyanakkor nincsenek könnyű helyzetben, mert a hasonlóan erős hagyományokkal és szervezeti kultúrával[18] rendelkező szervezetekben a változás sokkal nehezebben megy végbe, mint mondjuk egy versenyszférához tartozó hasonló méretű szervezetben.

Ennek alapvetően három oka van.

- A nemzetbiztonsági rendszer működését viszonylag részletesen szabályozzák a jogszabályok, így azok változásának elmaradása lassíthatja az igazodás ütemét.
- A szervezeti működést parancsok szabályozzák. A rendszer változásának mértékét, irányát és sebességét az utasítások tartalma és kibocsátásuk időzítése határozza meg, nem pedig a változáshoz történő automatikus igazodás szükségessége.
- A szolgálatok szervezeti kultúrájának egyik központi értéke az állandóság, kiszámíthatóság, ami általában is erősíti a változással szembeni ellenállás képességét.

Az előző fejezetben vázolt kihívások kezelése érdekében, figyelembe véve az új korosztályok jellemzőit, az alábbi területeket fontos kiemelt figyelemmel kezelni a generációs kihívások hatékony kezelése érdekében.

- *Munkatevékenységek, folyamatok:* Csökkenteni célszerű azon tevékenységek arányát, amelyek a feltétlenül szükségesnél és célszerűnél nagyobb mértékű adminisztrációt jelentenek, vagy amelyek csak a régi szokások és szabályzók alapján vannak előírva, miközben funkciójukat már elvesztették.
- *Információkezelés:* Tekintettel arra, hogy a nemzetbiztonsági szolgálatok fő feladata az információk megszerzése és értelmezése, ez kulcsfontosságú terület. A változékony környezethez való igazodás igényli az információáramlás és -értelmezés sebességének növelését. A hagyományos szervezeti folyamatok és keretek között ez még a modern informatikai eszközökkel is korlátozottan lehetséges, így szükséges új megoldások kigondolása.

[18] Zalai-Göbölös Noémi*:* A Z és az alfa generációk jövője a nemzetbiztonsági szolgálatoknál. *Belügyi Szemle,* 66. (2018), 2. 46.

– *Munkavállalói korlátozások:* Még a szolgálatok speciális világában is csökkenteni célszerű azon munkatársakra vonatkozó szabályozói korlátozások számát, amelyek a változó világban már nem rendelkeznek funkcióval, vagy azt nem tudják hatékonyan betölteni. A feltétlenül szükséges korlátozásokat úgy kell átalakítani, hogy a legkisebb kellemetlenséget okozzák a munkatársak számára. Emellett fontos, hogy a korlátozások valamilyen módon ellentételezve legyenek, például magasabb fizetéssel vagy izgalmas, motiváló munkafeladatokkal.
– *Belső szabályozók:* A gyorsan változó világban a nagy terjedelmű és bonyolult szabályzók egyértelműen a rugalmas alkalmazkodás akadályai. Célszerű e szabályzók terjedelmét és összetettségét a feltétlenül szükséges minimumra csökkenteni, emellett célszerű a változtatásuk módját is jelentősen leegyszerűsíteni. Ez lehetséges például protokoll-jellegű előírások alkalmazásával, amelyek megváltoztatása alacsonyabb hierarchiai szinteken lehetséges.
– *Teljesítményértékelés:* Az államigazgatási, ezen belül is a biztonságért felelős szervezetek egyik legnehezebb kérdése a munkavállalói teljesítmény objektív, differenciált értékelése, amely azonban az újabb generációk egyik legfontosabb elvárása. Ezen ellentmondás feloldása érdekében a jövőben egyre inkább szükség lesz új értékelési módszerekre a jelenleg a hivatásos szolgálatban alkalmazott, inkább szubjektívnek mondható – a vezetői megítélésen alapuló – eszközök kiváltására.
– *Vezetői kiválasztás és felkészítés:* A változó világ egyik nagy problémája, hogy a vezetés egyre összetettebb tevékenység, amit a Z generáció megjelenése csak bonyolítani fog. A nemzetbiztonsági vezetőket érő fentebb említett, a jogi szabályozók állandóságából és a gyorsan változó környezetből fakadó kettős „nyomás" miatt a vezetőkiválasztásnál a hierarchiába való illeszkedés mellett a jövőorientált vezetésre való alkalmasság vizsgálatának is döntő szemponttá kell válnia. Emellett célszerű a vezetéssel kapcsolatos készségeket és képességek erősítését már a vezetővé válás előtt megkezdeni, és a vezetői munka során folyamatosan fenntartani.
– *Munkatársak bevonása, részvétel bátorítása:* Az utasítás-központú, erősen centralizált, bürokratizált szervezetek működési hatékonyságán jelentős mértékben javítani lehet azon kompetenciák, kreatív emberi erőforrások kihasználásával, amelyek az új problémákra új megoldásokat nyújthatnak. Az alkalmazkodási folyamat egyik pillére lehet a munkatársak új módokon történő bevonása a szervezeti működés fejlesztésébe,

döntések előkészítésébe, amire az újabb generációk egyébként is nagyobb igényt mutatnak.

– *Szakmai módszertan:* Az emberi viselkedés változása igényli a titkos információgyűjtő eszközök és módszerek felülvizsgálatát, tudatos és folyamatos fejlesztését. E tekintetben is fontos a 7. pontban említett bevonás. Szükség lehet továbbá újszerű műveleti szemlélet kialakítására.
– *Képzés:* A módszertanok felülvizsgálatát követően az új módszereket be kell építeni a munkatársi kompetenciastruktúrába. Az új generációk tanulási módszere – az eltérő tanulási szocializáció miatt – különböző. Szívesebben tanulnak saját felfedezés, illetve rövid, de intenzív kurzusok révén, mint hosszú, száraz elméleti képzéseken.[19] E körülményekből fakadóan megfontolandó a képzési rendszer radikális átalakítása.
– *Toborzás, kiválasztás:* A toborzás kiválasztási rendszerének kialakításánál egyensúlyba kell hozni a szervezethez való illeszkedés szempontjait és a jövő kihívásainak kezeléséhez szükséges kompetenciákat, hogy a szolgálatok ne veszítsék el a minőségi emberi erőforrás bevonásának lehetőségét.[20]

Új gondolkodásmód, azaz új értékek és szervezeti kultúra

A fenti intézkedések megvalósítása akkor lehet eredményes, ha a szervezetek gondolkodásmódja, azaz értékrendje és szervezeti kultúrája is fejlődik, alkalmazkodik a változó körülményekhez.[21] Ennek egy formája a szervezeti kultúra fejlesztése az alkalmazkodást segítő értékek megerősítése révén. Ilyen értékek lehetnek példának okáért az alábbiak:

– *Humánközpontúság:* Az új generációk számára a személyből fakadó tekintély értékesebb. A biztonsági szervezeteket jellemző szabály- és hierarchia-központú kultúrát – ha a szervezetek eredményes működését fent kívánjuk tartani – humán központú kultúrává célszerű alakítani, ahol – az esetek nagyon szűk körét leszámítva – az emberekre gyakorolt hatás fontos szempont. Az alaptevékenység bizonyos szigorú szegmenseit

[19] Weinbaum–Girven–Oberholtzer (2016): i. m. 32.
[20] Weinbaum–Girven–Oberholtzer (2016): i. m. 32.
[21] Drusza Tamás: A szervezeti kultúra jelentősége a generációs kihívás és a nemzetbiztonsági szolgálatok fejlesztése szempontjából. *Nemzetbiztonsági Szemle,* 6. (2018), 2. 69–89.

leszámítva az embert kell a szervezeti működés középpontjába helyezni, elősegítve ezzel a szervezeti célokkal való azonosulást, amely fontos feltétele a belső motiváció kialakulásának és fennmaradásának.
- *Nyitottság:* Bár a nemzetbiztonsági szervezetek lételeme a titkos működés, az új generációs munkavállalók a szervezeten belül egyre jobban fogják igényelni a széles körű kommunikációt, a szervezet egészét érintő döntéshozatalra való rálátást.
- *Innovativitás:* A szervezeti változás elengedhetetlen új ötletek nélkül, új megoldások alkotása viszont kreativitást igényel. A kreativitás viszont jellegéből adódóan olyan készség, amelyet nem lehet utasításra aktiválni, sőt a tudományos kutatások szerint a külső motiváció inkább negatív hatással van rá.[22] A kreativitás jobbító alkalmazásának feltétele az innovatív szemlélet értékként való elismerése, az ilyen magatartásformák jutalmazása, ösztönzése.
- *Rugalmasság:* Az újabb generáció számára a változásokhoz való gyors alkalmazkodás természetes jelenség, így a szervezeteknek a minél gyorsabb reagálást és az állandó változtatásra való készséget is értékrendszerük központjába kell helyezniük.

Összegzés

A generációs probléma egyes szektorokra gyakorolt hatásának vizsgálata során gyakran felbukkan az a vélekedés, hogy az új generációk nem fognak tudni igazodni a meglevő szervezeti keretekhez. Ez az értelmezés azonban komoly csapdát rejt a szervezetek – köztük a nemzetbiztonsági szolgálatok – számára is. A helyzetet ugyanis inkább fordítva célszerű értelmezni. A szervezetekre az jelenti a legnagyobb veszélyt, ha nem fognak tudni igazodni a gyors ütemű generációs változáshoz. Az új generációk törvényszerű érkezését megváltoztathatatlan külső adottságként, egyben a szervezeti gazdagodás lehetőségeként célszerű értelmezni. Ebből fakadóan nem az újonnan érkezők megváltoztatására kell törekedni, hanem fokozatosan, de mégis gyorsuló ütemben alkalmazkodni kell hozzájuk. Minél késedelmesebb és pontatlanabb ez az alkalmazkodás, annál nagyobb veszélyt, veszteséget jelent a nemzetbiztonsági szervezeteknek és velük együtt az adott nemzetnek.

[22] Daniel H. Pink: *Motiváció 3.0.* Budapest, HVG Könyvek, 2016. 61.

Vákát

RENDSZERSZINTŰ VÁLASZOK ÉS FOLYAMATOK

Vákát

A szervezetrendszerek módosítása, strukturális válaszok

Mezei József

Bevezetés

A nyugati típusú demokráciákban a 21. század kezdetére létrejöttek és kvázi állandósultak azok a szervezeti keretek, amelyek e társadalmi berendezkedésekben a nemzetbiztonsági tevékenység végrehajtásához elengedhetetlenek, illetve megerősödtek az érintett szervezetek közötti együttműködési mechanizmusok. A szakterülettel foglalkozó kutatók közül néhányan a nemzetbiztonsági tevékenységben érintett, illetve azzal szorosan összefüggő szervezetek összességét mint nemzetbiztonsági szervezetrendszert definiálják. E felfogás szerint ebbe beletartoznak – többek között a hírszerző, elhárító, adatszerző, adatvédelmi feladatokat ellátó – nemzetbiztonsági szolgálatok és e szolgálatok irányítói. Idesorolandók továbbá a nemzetbiztonsági szolgálatokat ellenőrző szervezetek, amelyek a szolgálatok működését, különböző szempontok szerint – anyagi, törvényességi, szakmai és a legújabb területként adatvédelmi – vizsgálják. Végül, de nem utolsósorban a nemzetbiztonsági szervezetrendszer elemei a szolgálatok közötti koordinációért felelős, azt végrehajtó szervezetek.[1] Jelen fejezetben mi is ezt a megközelítést alkalmazzuk.

Számos, a rendszer működése szempontjából releváns tényező hat a szervezetrendszer elemeire, így a szervezetrendszerre is. Ezek közül néhánnyal számolni lehet minden szervezetrendszernél (például elvárások a kormányzat részéről), azonban vannak olyanok is, amelyek csak egyes országok, országcsoportok speciális jellemzői (például politikai rendszer típusa). Ezek a tényezők nemcsak térben, de hatásuk időbeni terjedelmében is eltérők lehetnek. Vannak, amelyek rövid távon, eseményszerűen vannak jelen (például egy terrorcselekmény), de vannak olyanok is, amelyek hosszabb időn keresztül fejtik ki hatásukat (például technológiai változások). Olyan is előfordul azonban, amely ciklikusan

[1] Lásd Béres János (szerk.): *Külföldi nemzetbiztonsági szolgálatok.* Budapest, Zrínyi, 2018. 10.

https://doi.org/10.36250/00904_06

ismétlődik (például a választások).[2] E hatások közül néhánynak olyan jelentősége van, hogy változást generálhat akár a szervezetrendszer összetételében vagy a működési mechanizmusokban. E körülményekre tekintettel a nemzetbiztonsági szervezetrendszer nem egy állandó, a hírszerző tevékenység megjelenésétől kezdve a mai formájában jelen lévő képződmény. A történelem folyamán a tevékenységet befolyásoló körülmények hatására – ha nem is minden időszakban egyforma ütemben –, de időről időre változott és változik most is. Legrégebbi tagja a hírszerző/elhárító tevékenységet folytató szolgálat, jelenlegi legfiatalabb elemét pedig a 21. század elején megjelent, adatkezelést ellenőrző szervezetek alkotják.

A környezetnek, illetve a rendszer elemeinek a szervezetrendszerre kifejtett hatása gyakran összetett, előfordul, hogy az egyes hatások egymásra épülnek, vagy több szempontból is figyelembe kell venni őket. (Ilyen például a technikai fejlődés, amely egyik oldalról hatékonyabbá teheti a szolgálatok munkáját, másik oldalról viszont az új technológiák terroristák általi alkalmazása kihívásként jelentkezik.) Megfigyelhető az is, hogy a rendszerre ható körülmények, a rendszerre gyakorolt hatásuk nagyságát illetően országonként jelentős eltéréseket mutatnak, illetve ebből is adódóan a rendszer változásának dinamikája is sok esetben különbözik az egyes országokban. Ezek következménye, hogy a nemzetbiztonsági szervezetrendszerek megjelenési formájában, működési mechanizmusaiban az egyes országok tekintetében megfigyelhetők kisebb-nagyobb különbségek.[3]

Ilyen lényegi különbségeket láthatunk a több nemzetbiztonsági szolgálattal rendelkező országok esetén az információtovábbítás kapcsán abban, hogy a megszerzett információk milyen úton jutnak el a döntéshozókhoz. Ezt a szempontot is figyelembe véve a napjainkban megtalálható alrendszereket három strukturális modellbe/típusba sorolja a hazai szakirodalom. Ezek a konkuráló/

[2] Példaként említhető Lengyelország, ahol a 2001-es országgyűlési választásokat követően a baloldali kormány feloszlatta az 1991-ben polgári területen létrehozott Államvédelmi Hivatalt, és létrehozott egy hírszerző és egy elhárító szolgálatot. A 2005-ös választáson sikeres jobboldali kormány 2006-ban felszámolta a katonai területen működő Katonai Információs Szolgálatot, és létrehozott egy hírszerző és egy elhárító szolgálatot.

[3] Vegyük például a nemzetbiztonsági szerveztrendszeren belül a nemzetbiztonsági szolgálatokat, illetve azoknak is a számát. Európában két – lélekszámát, területét, gazdasági erejét összevetve – hasonló adottságokkal rendelkező országot nézve láthatjuk, hogy míg az Egyesült Királyságban jelenleg kilenc önálló nemzetbiztonsági szolgálat működik, addig a Német Szövetségi Köztársaságnak szövetségi szinten három nemzetbiztonsági szolgálata van.

versengő; a szektorra épülő; és a kooperatív/együttműködő.[4] A számtalan változás, átszervezés, korrekció következtében egyes országokban e három modell elemei egy szervezetrendszeren belül párhuzamosan vannak jelen. A három modell mindegyikének vannak előnyei és hátrányai, így nem lehet azt mondani, hogy bámelyik hatékonyabb lenne a másiknál. Mindazonáltal a későbbiekben bemutatott példák segítenek megérteni, hogy a világban bekövetkezett változások hatására miért az együttműködő modell lett az, amellyel „az elmúlt két évtizedben az euroatlanti térség államainak egyre bővülő körénél találkozhatunk".[5]

Jelen fejezetben összefoglaljuk, hogy a 21. század eddig eltelt időszakában megjelenő új körülmények eredményeként hogyan, milyen formában módosult a szervezetrendszer, vagyis hogy egy adott kihívásra milyen strukturális válaszok születtek. Fontos látni, hogy a szervezetrendszerre számtalan körülmény gyakorol hatást, azonban ezek közül csak kevés olyan van, amely a szervezetrendszer strukturális felépítését is képes befolyásolni. Első lépésként áttekintjük a szervezetrendszer változásával kapcsolatos általános ismereteket, azon belül kiemelten, hogy milyen jellegű szerkezeti változások történhetnek, illetve ezek mögött milyen okok, milyen közvetett és közvetlen hatások állhatnak.

A nemzetbiztonsági szervezetrendszer

A nemzetbiztonsági szervezetrendszer módosulása kapcsán többféle változásról beszélhetünk. Előfordulhat valamely, meglévő funkció/feladat vagy szervezet megszűnése;[6] új feladat kapcsán egy új szervezet létrehozása;[7] szervezetek

[4] Héjja István: Nemzetbiztonsági szervezeti modellek. In Dobák Imre: *A nemzetbiztonság általános elmélete.* Budapest, Nemzeti Közszolgálati Egyetem, 2014. 63.

[5] Urbán Attila: A koordinációs folyamatok intézményi hátterének evolúciója a magyar nemzetbiztonsági igazgatásban. *Nemzetbiztonsági Szemle,* 8. (2020), 1. 8.

[6] A lengyel Katonai Információs Szolgálatot 2006-ban felszámolták, és létrehoztak helyette egy hírszerző és egy elhárító szolgálatot.

[7] Lengyelországban 2006-ban egy új típusú kihívás kezelése érdekében létrehoztak egy teljesen új szervezetet, a Központi Korrupcióellenes Irodát.

összevonása,[8] meglévő szervezetből egy új szervezet megalakítása,[9] valamint a változtatások hatására a nemzetbiztonsági struktúra megváltozása. Gyakran előfordul, hogy ezek a változások összefüggenek és párhuzamosan történnek. Ahogy a példákból látszik, a 21. század eddig eltelt rövid időszakában is találhatunk minden változásra egy-egy esetet, ennek ellenére összességében ebben az időszakban leginkább a nemzetbiztonsági szervezetrendszer bővülését lehetett megfigyelni.[10] Jellemzően új funkciók/feladatok jelentek meg, illetve ezzel összefüggésben új szervezetek jöttek létre, és/vagy kapcsolódtak a nemzetbiztonsági tevékenységhez.

A szervezetrendszer legmeghatározóbb elemei maguk a nemzetbiztonsági szolgálatok, minden más elem ehhez, illetve az általuk végzett feladatokhoz köthető, ahhoz csatlakozik és hat rá – irányítja, koordinálja –, vagy vizsgálja azt előre meghatározott céllal, szigorúan szabályozott módon. A nemzetbiztonsági szolgálatok a kormány, a politikai vezetés által kitűzött célok elérését támogatják. A „nyugati típusú demokráciák" kormányai folyamatosan értékelik a biztonsági környezetüket, a biztonságot fenyegető kockázatokat és azok kezelését jellemzően jogi formában, esetleg politikai nyilatkozatként hosszú távon, folyamatosan ellátandó feladatként jelenítik meg egyes állami szervek, köztük a nemzetbiztonsági szolgálatok számára. A kormányok ezzel összefüggő stratégiai tervező tevékenysége eredményeként előálló dokumentumok (például nemzeti biztonsági stratégia) alapvető fontosságúak a szervezetrendszer

[8] 2005-ben a cseh Katonai Hírszerző Szolgálat és a Katonai Védelmi Hírszerzés összevonásával hozták létre a Katonai Hírszerzést, Csehország jelenlegi egyetlen katonai szolgálatát, míg 2013-ban Szlovákiában történt meg ugyanez.

[9] 1992-ben a Komityet Goszudarsztvennoj Bezopasznosztyi (KGB) ukrajnai szervezetéből megalakult az Ukrán Biztonsági Szolgálat. 2004-ben vált ki belőle a Hírszerző Főcsoportfőnökség, amelyből létrejött a Külső Hírszerző Szolgálat.

[10] Amennyiben egy kis kitekintést teszünk e téren, és kicsit visszatekintünk a 20. századra is, akkor látható, hogy a szervezetrendszeren belül, a titkosszolgálatok vonatkozásában a bővülés oka, hogy fő tevékenységük, működési területeik és a hírszerzési módszerek szerint specializálódtak. A katonai titkosszolgálatok mellett megjelentek a polgári szolgálatok, illetve a hírszerzést és elhárítást is folytató szervezetek szétváltak, megjelentek az önálló hírszerző és elhárító szolgálatok. A hírszerzés módszere szerinti specializáció egyik egyértelmű példája pedig az Amerikai Egyesült Államok hírszerző közösségének meghatározó tagja, az NSA létrehozása, amelyet az addig főleg humán hírszerzést folytató szervezetektől eltérően kimondottan a jelhírszerzési feladatok ellátására hoztak létre. Ez a változás természetszerű, hisz egyrészt a nemzetbiztonsági szervezetrendszer fő elemei a titkosszolgálatok, illetve az elmúlt évszázad kezdetétől beszélhetünk igazán a titkosszolgálati szervezetek állandósult jelenlétéről.

változása tekintetében, mivel a struktúra megváltoztatásának legfőbb motivációja a biztonsági kihívásokból levezetett feladatok eredményes végrehajtása. A fentiek alapján a rendszert érintő strukturális változások mögött a legtöbb esetben a végrehajtó hatalom áll.

Emellett azonban a nemzetbiztonsági szervezetrendszerben jelen van a másik két hatalmi ág is, így ezek is előidézhetnek változásokat, illetve a hatalmon lévő kormány támogatottságának függvényében néhány, a kormány által javasolt, elképzelt változás csak a törvényhozói hatalmi ág támogatásával valósulhat meg. A hatalmi ágak tehát egyrészt azok, amelyek közvetlenül gyakorolhatnak hatást a nemzetbiztonsági szervezetrendszerre, beleértve annak megváltoztatását is. Ezek mögött számos, eltérő területről származó tényező figyelhető meg. E területek közül meghatározók: a politika;[11] a gazdaság;[12] a társadalom és a technológia.[13] Ezeken belül is több olyan részterület találhatunk, amelyek képesek közvetlenül vagy közvetetten hatni a nemzetbiztonsági szervezetrendszer tagjaira, és befolyásolni tudják azok működését, tevékenységét. Ezen túlmenően a nemzetbiztonsági szervezetrendszer strukturális változása maga is előidézhet további szerkezeti változást. A nemzetbiztonsági szervezetrendszerre ható körülmények közül azok, amelyek elég jelentősek ahhoz, hogy változásokat indukáljanak, előfordul, hogy összetetten jelentkeznek, továbbá, hogy a szervezetrendszer több elemére is jelentős hatást gyakorolnak.

[11] A politikai tényezők közül példaként említhető egy ország politikai berendezkedésében történt változás. Egy ilyen tényező jelentős hatással lehet a nemzetbiztonsági szervezetrendszerre, illetve annak megváltozására, amelyet egyértelműen szemléltetnek a posztkommunista, kelet-közép-európai országokban 1990 környékén lezajlott rendszerváltások következményei az állambiztonsági struktúrákra. Magyarország esetében az addig – a katonai hírszerzést leszámítva – a Belügyminisztérium keretében működő állambiztonsági szerv, a III. Főcsoportfőnökség megszűnt, helyette három új szervezet jött létre, továbbá alapjaiban változott meg a szolgálatok irányítása.

[12] Több esetben a nemzetbiztonsági szolgálatok összevonása mögött gazdasági okok húzódtak meg. Börcsök András – Vida Csaba: A nemzetbiztonsági szolgálatok rendszere (Nemzetközi gyakorlat a nemzetbiztonsági rendszer kialakítására). *Nemzetbiztonsági Szemle,* 2. (2014), 1. 63–100.

[13] A technikai, technológiai fejlődés is olyan tényező, amely változást eredményezhet a nemzetbiztonsági szervezetrendszerben. Ez a változás többrétű lehet. Amennyiben csak a nemzetbiztonsági szolgálatokat tekintjük, ez kiválthatja új szervezetek létrehozását, amelyre példa a már korábban említett NSA, vagy az USA-ban 1961-ben létrehozott Nemzeti Felderítő Iroda, amely a műholdakkal folytatott képi hírszerzésért felel.

A nemzetbiztonsági szervezetrendszert érintő változások a 21. században

A következőkben tárgyalt események, változások, jelenségek az élet számos területére gyakoroltak hatást, és a biztonságot érintően is széles körben voltak relevánsak, azonban mi itt csak szűken a nemzetbiztonsági szervezetrendszert érintő változásokat tekintjük át.

Terrorcselekmények

Sajnos az új évszázad nem is kezdődhetett volna rosszabbul a nyugati világban nemzetbiztonsági szempontól annál, mint ami történt. Mind az USA-ban, mind Európában új típusú, a polgári lakosságot célzó, súlyos, számos emberáldozatot követelő terrortámadásokra került sor. Már az első évben történt olyan esemény, amelynek jelentős hatása volt a nemzetbiztonsági szervezetrendszerekre. 2001. szeptember 11-én az al-Káida 19 tagja eltérített négy repülőgépet, amelyekkel támadásokat hajtottak végre ikonikus, illetve a biztonság szempontjából kritikus épületek ellen.[14] A támadások következtében a támadókkal együtt 2996 ember vesztette életét, de ezen túlmenően is számos, jelentős közvetett és közvetlen negatív hatása volt a támadásnak. Ez a támadás az al-Káida részéről nem volt előzmény nélküli,[15] azonban annak súlyossága, az áldozatok nagy száma, valamint az, hogy azt az USA területén követték el, sokkolta a társadalmat és a politikai vezetőket egyaránt. A történtek, azok nemzetbiztonsági szempontú kivizsgálása, illetve a következmények nagy nyilvánosságot kaptak. Érdemes ezeket kicsit részletesebben áttekinteni, mert egyrészt ezen eseményeken keresztül bepillantást nyerhetünk egy gazdasági, katonai és politikai téren is kiemelkedő ország nemzetbiztonsági szervezetrendszere megváltozásának folyamatába, másrészt mivel hasonló változások ezt követően Európában is megtörténtek, összehasonlítási alapot adnak.

A támadást követően az USA-ban két bizottságot is életre hívtak, hogy az eseményeket kivizsgálják. Az egyik a 2002 elején felállított, úgynevezett Közös Bizottság volt, amelybe a Szenátus és a Fehér Ház jelölt nemzetbiztonsági szakembereket. A bizottság a nemzetbiztonsági szervek által elkövetett hibák, hiányosságok feltárásával foglalkozott. 2002. decemberi jelentésükben számos

[14] FBI: *9/11 Investigation* (é. n.).

[15] FBI: *East African Embassy Bombings* (é. n.); FBI: *USS Cole Bombing* (é. n.).

kritikát megfogalmaztak azokkal a biztonsági szolgálatokkal szemben, amelyeknek terrorelhárítási feladataik voltak.[16] A másik, a 2002 novemberében a Fehér Ház és a Kongresszus által életre hívott „9/11 Bizottság" volt. E második testület amellett, hogy teljeskörűen fel kívánta tárni a támadás körülményeit, felhatalmazást kapott arra is, hogy ajánlásokat fogalmazzon meg a jövőben esetlegesen bekövetkező támadások megelőzése érdekében.[17] 2004. július 22-én e bizottság közzétette jelentését.[18] Ebben számos területet érintően állapított meg hiányosságot és fogalmazott meg ajánlást, közöttük a nemzetbiztonsági szervezetrendszer kapcsán is. Ezek közül néhány lényegi megállapítás:

1. Hiányosságok, problémák:
   - a CIA-nek képességbeli hiányosságai voltak a terrorelhárítási tevékenységében;
   - az FBI hiányossága a hírszerzésben, a stratégiai értékelésben, a rendelkezésre álló információk és a fenyegetések összevetése, valamint az információmegosztás terén;
   - együttműködési problémák az ügynökségek között;
   - a Központi Hírszerzés Igazgatójának[19] korlátozott hatalma a hírszerző közösség irányítása tekintetében;
   - a hírszerző szolgálatok elavult struktúrákkal működtek, a szervezetek között bürokratikus rivalizálás volt;
   - túlzott titkosítás, ami hátráltatta a szolgálatok felügyeletét, az információmegosztást.

Érdekes megjegyzése a jelentésnek, hogy a szeptember 11-i támadást követően a közös munka ugyan javult, a szolgálatok aktivitása is jelentősen nőtt, viszont a koordinációs problémák is megsokszorozódtak.

[16] *Report of the U.S. Senate Select Committee on Intelligence and U.S. House Permanent Select Comittee on Intelligence* (2002).
[17] *National Commission on Terrorist Attacks Upon the United States* (2004).
[18] *National Commission on Terrorist Attacks Upon the United States* (2004): i. m.
[19] Ebben az időben a CIA igazgatója látta el ezt a feladatkört.

2. Javaslatok:
   - új Nemzeti Hírszerzési Igazgató (*Director of National Intelligence,* DNI) pozíció létrehozása (ennek a pozíciónak a létrehozását már a Közös Bizottság is javasolta);
   - Nemzeti Terrorizmusellenes Központ (*National Counterterrorism Center,* NCTC) létrehozása;
   - új, a kormányzaton belüli, határokon átívelő információmegosztó rendszerek létrehozása;
   - a kongresszusi felügyelet egységesítése és megerősítése a minőség és az elszámoltathatóság javítása érdekében;
   - az FBI és a hazai biztonsági szervezetek megerősítése.

A támadás és az azt követő vizsgálatok eredményeként elfogadták a 2004. évi hírszerzési reformról és a terrorizmus megelőzéséről szóló törvényt. A törvénnyel jelentősen módosult az Amerikai Egyesült Államok nemzetbiztonsági szervezetrendszere. Többek között létrehozták a Nemzeti Hírszerzési Igazgató (DNI) pozíciót. Az ezt betöltő személy az elnök fő hírszerző tanácsadója és a hírszerző közösség vezetője lett. Feladata a hírszerzési közösséget alkotó 16 ügynökség szorosabb koordinációjának és integrációjának megteremtése. Létrehozták a Nemzeti Terrorizmus Elleni Központot (NCTC), amely elemzi és összesíti a terrorizmussal kapcsolatos valamennyi hírszerzési információt.[20] Ezen túlmenően erőfeszítéseket tettek a hírszerző közösség tagjai közötti információmegosztás fejlesztésére is.[21]

A vizsgálatok több olyan problémát is feltártak, amelyek vélelmezhetően más demokratikus országok nemzetbiztonsági szolgálatainak működésében is alapvető hiányosságként jelen lehettek. Ilyen például a párhuzamosságokból, a szolgálatok egymással történő „versenyeztetéséből" adódó rivalizálás jelensége, valamint az érdemi koordináció és információcsere hiánya. A működés jellegéből adódóan vélelmezhető, hogy ezek a problémák a nemzetbiztonsági elhárító tevékenység más területein is jelen vannak, csak a terrorcselekmények azok, amelyek megnyilvánulási formájuknál fogva jelentős társadalmi figyelmet kapnak. A feltárt probléma súlyosságát, valamint az Egyesült Államok kormánya által arra adott válaszok helyességét támasztja alá, hogy ebben az időszakban

[20] The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA): *Justice Information Sharing* (2004).

[21] Office of the Director of National Intelligence: *About the ISE* (é. n.).

több nyugati típusú demokráciában is hasonló döntéseket hoztak. Figyelmet érdemel, hogy a 2001. szeptemberi terrortámadást követően három év telt el addig, amíg a szükséges, a feltárt hiányosságok kiküszöbölését biztosító változtatásokat eredményező döntéseket meghozták.

Az Amerikai Egyesült Államokban történtek Európa országaira is komoly hatással voltak, amit a 2004-es és 2005-ös sajnálatos események tovább erősítettek. 2004. március 11-én tíz robbantásos merénylet történt Madridban, amelyeknek következtében 191 ember veszítette életét. A támadást az al-Káida vállalta magára. 2005. július 7-én Londonban, a tömegközlekedési rendszereket érintően hajtottak végre robbantásos merényleteket. Négy pokolgépet robbantottak fel, közülük hármat a földalatti-hálózat egy-egy forgalmas állomásán, egyet pedig egy városi buszon. A támadásnak 56 halálos áldozata volt. A támadások az al-Káida hálózatához voltak köthetők. 2005. július 21-én újabb négy támadást kíséreltek meg Londonban ugyanilyen helyszíneken, de ebben az esetben a detonátorok nem működtek.

E támadásokra válaszul Európa több országában is megváltozott a nemzetbiztonsági szervezetrendszer. Például az Egyesült Királyságban 2003-ban új szervezetként létrehozták a Belső Biztonsági Szolgálat (*Security Service,* a volt MI5) keretében az Egyesített Terrorizmuselemző Központot (*Joint Terrorism Analysis Center,* JTAC),[22] míg a Német Szövetségi Köztársaságban 2004-ben a Szövetségi Alkotmányvédelmi Hivatalon belül a Közös Terrorelhárító Központot.[23] Ezen elemző-, értékelő-, tájékoztató-központok azon túlmenően, hogy hatékonyabbá tették az információfeldolgozást, abban is előrelépést jelentettek, hogy munkatársaik az adott országban terrorelhárítással foglalkozó szervezetek állományából kerültek ki, ami további segítséget jelentett a szervezetek közötti együttműködés, információmegosztás és koordináció területein. A 2000-es években további európai országokban is megalakítottak a terrorelhárítás hatékonyságának növelése

[22] Security Service MI5: *Joint Terrorism Analysis Centre* (é. n.).

[23] Gemeinsames Terrorismusabwehrzentrum (GTAZ – Joint Counter-Terrorism Centre). Verfassungsschutz.de. (2020).

érdekében koordinációs, illetve elemző-értékelő – egyes szakirodalmakban fúziós központnak nevezett – szervezeteket.[24]

A 21. század elején elkövetett terrortámadások rávilágítottak a terrorelhárítás hírszerzési kudarcára, a rendvédelmi szervek közötti koordináció komoly problémáira, és igazolták a nemzetközi együttműködés hiányosságait. Emellett megerősítették, hogy a terrorizmusra globális kihívásként kell tekinteni. Az események hatására azonban megtörténtek azok a változások a nemzetbiztonsági szervezetrendszerekben mind szervezetileg, mind a működési mechanizmusokat érintően, amelyek növelték a nemzetbiztonsági szolgálatok ez irányú tevékenységének hatékonyságát. Volt még egy újszerű kezdeményezés a nemzetbiztonsági szolgálatok részéről a terrorprevenció érdekében, ez pedig a biztonságtudatosítás megjelenése. A témakör jelentősége okán ezzel külön fejezetben foglalkozunk.

A támadások óta eltelt időben a nyugati demokráciákban a muszlim terrorizmus elkövetésének kockázata nem csökkent, amit az elmúlt években Európában elkövetett újabb terrorcselekmények egyértelműen alátámasztanak.[25] Ez alapján kijelenthető, hogy sajnálatosan e terrorcselekmények kiváltó okai napjainkra sem szűntek meg, továbbá az eddig megtett megelőző intézkedések nem elegendők, azokat fokozni kell. A problémakört tovább szélesíti, hogy a technológia is rohamosan fejlődik, aminek eredményeit a terrorszervezetek is kihasználják. Ezek alapján fel kell rá készülni, hogy a terrorizmusra a következő évtizedekben is egy olyan kockázati tényezőként kell tekinteni, amely komoly hatással lehet a nemzetbiztonsági szervezetrendszerekre.

[24] Az Oroszországi Föderációban a Szövetségi Biztonsági Szolgálat (FSZB) vezetőjének irányítása alatt 2006-ban hozták létre a Nemzeti Terrorellenes Bizottságot, míg Svédországban, 2005-ben a szolgálatok koordinációjáért felelős szervezetet, a Terrorelhárítási és Együttműködési Tanácsot, amelyet a Polgári Nemzetbiztonsági Szolgálat főigazgatója elnököl. Hazánkban 2003-ban hozták létre a Nemzetbiztonsági Hivatal keretében a Terrorellenes Koordinációs Bizottságot (TKB), amely a nemzetbiztonsági és rendőri szervek által begyűjtött, terrorszempontból releváns információkat elemezte, értékelte, kormányzati tájékoztatókat készített, továbbá összehangolta az érintett szervezetek műveleti tevékenységét. 2010-ben került sor arra, hogy a terrorelhárítási feladatok komplex kezelésére megalapítottak egy új, önálló rendőri szervet, a Terrorelhárítási Központot (TEK), amely a TKB irányítását is átvette. Ezt követően, 2016-ban létrehozták a Terrorelhárítási Információs és Bűnügyi Elemző Központot (TIBEK), amely információfúziós és információmegosztó központként funkcionál, állománya pedig hasonlóan a nyugat-európai példákhoz a rendészeti, nemzetbiztonsági szervek munkatársaiból tevődik össze.

[25] 2015 Charlie Hebdo Attacks Fast Facts *CNN,* (2020. december 18.); Terrorist drives Truck Through a Bastille Day Celebration. *History,* (2016. július 14.).

Információrobbanás

Évtizedek óta exponenciálisan nő a világon az újonnan keletkezett információk mennyisége. Ennek elsődleges feltétele az információ kezelésének (rögzítése, tárolása, feldolgozása) módszereiben bekövetkezett ugrásszerű technológiai fejlődés, amely alapvetően az informatikai eszközök, rendszerek megjelenésének, folyamatos fejlesztésének köszönhető. Az infokommunikációs rendszerekben folytatott információgyűjtésnek számos előnye van. Az adatok gyorsan, olcsón, távolságtól, időtől függetlenül, nagy mennyiségben folyamatosan elérhetők. Természetesen vannak hátrányai is, amelyek közül komoly problémaként jelentkezik, hogy az adatok olyan nagy tömegben állnak rendelkezésre, hogy nehéz megtalálni a releváns adatokat, továbbá az adatok lehetnek hiányosak, hibásak, vagy akár szándékosan torzítottak.

A releváns információk megszerzését célzó információgyűjtés a nemzetbiztonsági szolgálatok fő feladata, így minden, ami ezzel összefügg, az jelentősen befolyásolja a nemzetbiztonsági szolgálatok működését. A nemzetbiztonsági munkában nagyon régóta, a modern szolgálatok megjelenése óta élnek a nyílt forrásokból beszerezhető információk összegyűjtésének lehetőségével.[26] A szakterminológia ezt a hírszerzési módszert az OSINT mozaikszóval jelöli, és szakértői vélemények szerint a „szolgálatok tevékenységében növekvő szerepe van a nyílt forrásból származó információszerzésnek".[27] „Napjainkra az OSINT a köztudatban összeolvadt az interneten folytatott információszerzéssel",[28] ennek ellenére ez valójában a nyíltan, bárki számára elérhető adatforrások, adatbázisok teljes körét lefedi.

Az említett változások eredményeként az OSINT a 21. századra a nemzetbiztonsági tevékenység meghatározó módszerévé vált, több területen is jelentős segítséget ad a nemzetbiztonsági szervezetek számára feladataik eredményes végrehajtásához. Ennek megfelelően az elmúlt években több országban is történtek lépések azzal a céllal, hogy az OSINT-tevékenységet valamilyen módon, akár új szervezetek létrehozásával is fejlesszék. 2005. november 1-jén a CIA (*Central Intelligence Agency,* Központi Hírszerző Ügynökség) infrastrukturális

[26] Regényi Kund Miklós: OSINT a második generációs internetet megelőző korokban. *Nemzetbiztonsági Szemle,* 7. (2019), 2. 32–37.

[27] Béres János: A hírszerzés feladatrendszere. In Dobák Imre (szerk.): *A nemzetbiztonság általános elmélete.* Budapest, Nemzeti Közszolgálati Egyetem 2014. 123.

[28] Dobák Imre: OSINT – Gondolatok a kérdéskörhöz. *Nemzetbiztonsági szemle,* 7. (2019), 2. 85.

és személyi bázisán a DNI létrehozta az Open Source Centert (OSC), amelynek feladata a nyílt – nyomtatott, sugárzott és online – forrásokból származó információk gyűjtése, elemzése, illetve tájékoztatók készítése lett.[29]

Németországban 2007-ben hozták létre a Szövetségi Alkotmányvédelmi Hivatal által működtetett Egyesített Internetközpontot (*Gemeinsames Internetzentrum,* GIZ), amely elsődlegesen az interneten megtalálható, szélsőséges iszlám tartalmak és kommunikáció megfigyelését, elemzését, értékelését végzi a szélsőséges terroristaszervezetek időben történő azonosítása érdekében.[30] Magyarországon ez idáig a nemzetbiztonsági szolgálatok saját maguk folytatták nyílt forrásokból az információk gyűjtését.[31] A 2016-ban létrehozott TIBEK feladatkörében azonban már dedikáltan megjelenik az OSINT mint olyan tevékenység, amelyet a nemzetbiztonsági szolgálat szolgáltatásként nyújt, hiszen a nemzetbiztonsági törvény szerint „nyílt információgyűjtést és feldolgozást végző szolgáltató és támogató szervet működtet".[32]

Az információrobbanásként meghatározott jelenség a közeljövőben biztosan tovább folytatódik, és így egyre szélesebb körben, egyre nagyobb adatbázisok állnak majd rendelkezésre, ha csak az internetet mint a legnagyobb és legdinamikusabban növekvő adatbázist vizsgáljuk. Az OSINT jelentőségének további növekedését nagyban segítheti a technológia fejlődése, amellyel az OSINT több részfeladata (keresés, elemzés, értékelés) automatizálhatóvá tehető. Ahogyan a példákból látható, néhány országban már most is tettek konkrét lépéseket arra, hogy külön szervezeteket hozzanak létre erre a feladatra. Ezek a változások a nemzetbiztonsági szervezetrendszer tekintetében aktuálisan még nem jelentősek, de mégis nagy valószínűséggel kijelenthető, hogy az OSINT a jövőben jelentősen felértékelődik, és további, erre specializált feladatkörű szervezetek megjelenésére lehet számítani. Ennek kapcsán megemlíthetők az elmúlt években létrejött információfúziós központok is, hiszen ezek a helyek a titkosszolgálati információk feldolgozása kapcsán OSINT-központként is tevékenykednek, ha a nevükben nem is viselik ezt. Az újabb szervezetek létrehozásán túl elképzelhető az adatbázisokban történő adatkeresési, feldolgozási tevékenységek bizonyos adatkörönként történő specializációja is, hiszen könnyen belátható, hogy egy

[29] Establishment of the DNI Open Source Center. *ODNI News Release,* (2005. november 8.).

[30] Gemeinsames Internetzentrum (GIZ – Joint Internet Centre). *Verfassungsschutz.de* (2020).

[31] Szabó Károly: Az OSINT – Gondolatok a tevékenységről és az alkalmazás közegéről. *Nemzetbiztonsági Szemle,* 7. (2019), 2. 68–82.

[32] 1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról.

gazdasági szektor és mondjuk a közösségi média adatsorai között a feldolgozás tekintetében jelentős különbségek vannak.

Biztonságtudatosság fokozása

A 21. század egyik jelentős változása a nemzetbiztonság területén a biztonságtudatossági programok megjelenése. Korábban is voltak korlátozott mértékben ehhez hasonló kezdeményezések, azonban ilyen széles körű alkalmazására eddig nem volt példa. Az ok, hogy hangsúlyosan a terrorelhárítás, a kémelhárítás és ezzel összefüggésben az információbiztonság területén rövid idő alatt olyan jelentős változások történtek, amelyek korábban elképzelhetetlen mértékben kiszélesítették e kockázatoknak kitett személyi kört. Ezen új típusú kihívásokra a nemzetbiztonsági szolgálatok meglévő eszközei nem kínáltak hatékony megoldást, ezért vált szükségessé egy új módszer bevezetése, a biztonságtudatosítás. A lényege, hogy a nemzetbiztonsági szolgálatok széles körben, előzetesen adnak át információkat a lehetséges kockázatokról, illetve készítik fel az embereket a kockázatok észlelésére, elkerülésére, illetve a bekövetkezés esetén tanúsítani szükséges magatartásra. A körülmények ily módon történt megváltozása következtében nemcsak a nemzetbiztonsági szolgálatok szándéka volt a biztonságtudatosság elterjesztése, arra a társadalom is nyitott volt, illetve bizonyos mértékig el is várta azt. A témakört itt nem fejtjük ki, azzal egy későbbi fejezetben részletesen foglalkozunk, azonban a nemzetbiztonsági szervezetrendszer változása kapcsán is érdemel figyelmet.

Annak ellenére, hogy nem találni rá példát, hogy erre a tevékenységre létrehoztak volna külön szervezeteket, tehát módosult volna a szervezetrendszer, a hatása kicsit mégis ahhoz hasonló. Ennek alapja, hogy egyrészt a társadalom jelentős hányadát vonják be a szolgálatok ezekbe a projektekbe. Igaz, hogy ezzel az elsődleges cél a prevenció, vagyis a kockázatok bekövetkezésének megelőzése, azonban ennek során a nemzetbiztonsági szolgálat a társadalmat mint információforrást is hozzákapcsolja a szolgálathoz, amely viszont egy olyan jelentős tényező, amely akár jelentősen növelheti az elhárító tevékenység hatékonyságát. Másrészt vannak olyan országok, ahol nem vagy nem csak a nemzetbiztonsági szolgálat hajt végre nemzetbiztonsági kockázatokkal összefüggő biztonságtudatossági programokat, hanem más szervezetek is.[33]

[33] Counter Terrorism Policing: www.counterterrorism.police.uk/

Az előzők alapján felvetődik a jövőre vonatkozóan egy lényegi kérdés. Megjelenik-e a feladatok kiszervezése a nemzetbiztonsági szolgálatok területén? Amennyiben igen, akkor mikor és milyen feladatokat érint majd ez? A kérdés nem utópisztikus, sőt a feladatok kiszervezése már el is kezdődött, ha az átlagemberek számára ez még talán nem is olyan látványos. Gondoljunk csak egyrészt az USA egyes szervezetei által alkalmazott katonai biztonsági magánvállalatokra például Irakban, amelyek hírszerzési tevékenységeket is ellátnak,[34] vagy a 2013-ban „Snowden-ügyként" elhíresült eseményekre, amelyek kapcsán Snowden azt nyilatkozza, hogy a CIA és az NSA szerződéses partnereinél, gazdasági társaságoknál nemzetbiztonsági szolgálati tevékenységeket végzett.[35] A kérdés tehát igazából az, hogy a továbbiakban milyen területeken és milyen mélységben vesznek részt „civil" cégek a nemzetbiztonsági szolgálati tevékenységben úgy, hogy az a társadalom szélesebb rétegei számára is nyilvánvaló legyen?

Együttműködések szerepe

A nemzetbiztonsági szolgálatok feladatköre még országhatáron belül is nagyon gyakran átfedést mutat úgy, hogy a rendelkezésre álló eszközök és módszerek általában azonosak. A versengő struktúrák esetében maga ez a helyzet alkalmas arra, hogy a nemzetbiztonsági szolgálatok között rivalizálás alakuljon ki, de előfordul az is, hogy a kormányzat szándékosan versenyezteti egymással a szolgálatokat. A rivalizálásnak viszont az lehet a következménye, hogy a szolgálatok a gyakorlatban nem, vagy csak minimális hatékonysággal működnek együtt egymással, hiába írják elő ezt akár különböző szintű szabályzók, ami jelentősen növelheti valamely nemzetbiztonsági kockázat bekövetkezését. A versengő struktúrákban az egyes szolgálatok azt szeretnék elérni, hogy egy-egy probléma kapcsán az ő megoldásuk, az ő sikerük legyen az, amelyik eljut a döntéshozók elé.

A nemzetbiztonsági szolgálatok közötti együttműködés alapja az információmegosztás, ezért e problémakör kezelésének egyik lehetséges módja olyan szervezetek létrehozása, amelyek felé a nemzetbiztonsági, valamint más szervezeteknek adattovábbítási kötelezettségeik vannak. Ilyenek az elmúlt időszakban

[34] Varga Krisztián: Katonai biztonsági magánvállalatok amerikai alkalmazása Irakban. *Nemzet és Biztonság,* 2. (2009), 3. 57–69.

[35] Glenn Greenwald: *A Snowden-ügy: korunk legnagyobb nemzetbiztonsági botránya*. Budapest, HVG, 2014.

egyre nagyobb számban létrehozott fúziós központok. Ezek a szervezetek sok esetben a nemzetbiztonsági szervezetrendszerek új elemeként jelennek meg. Az a szakmai elképzelés, hogy ezekben a szervezetekben a nemzetbiztonsági szolgálatok, illetve az adott témakör szerint releváns rendvédelmi szervek delegálnak munkatársat, több szempontból is pozitív. Egyrészt elősegíti a különböző szervezetektől származó információk egységes értékelését, másrészt a szolgálatok közötti együttműködésre is pozitív hatással lehet.

A rivalizálás kiküszöbölésének másik megoldása lehet, ha koordinációs szervezeteket hoznak létre az érintett nemzetbiztonsági szolgálatok, rendvédelmi szervek, illetve az irányításukért felelős személyek, szervezetek bevonásával. Az együttműködés „kikényszerítése" jelenleg annyira fontos a legkritikusabb terrorelhárítás területén a döntéshozók részéről, hogy találkozunk olyan megoldásokkal, ahol a döntéshozói akarat eredményeként az együttműködés több szinten is (operatív, műveleti vezetői szint, irányítói szint)[36] jelen van.

Az együttműködésre vonatkozó törekvés nemcsak az egyes államok nemzetbiztonsági szervezetei szintjén jelent meg ilyen markánsan a 21. század elején, hanem ezzel párhuzamosan az olyan nemzetközi szervezetekben is, mint például a nyugati demokráciák biztonsága szempontjából meghatározó NATO *(North Atlantic Treaty Organization)* és az Európai Unió (EU). A NATO-nak nincs önálló hírszerzése békeidőben, a tagállamoktól származó információkat használják fel tevékenységük során. A közel 30 tagállam érintettsége okán, valamint a megváltozott biztonsági környezet kihívásainak való megfelelés érdekében a NATO-ban döntés született arról, hogy fokozni kell a tagországok hírszerző szervezetei közötti együttműködést, az információmegosztást. E cél érdekében több konkrét lépés is született az elmúlt időszakban. 2006-ban létrehozták a NATO Hírszerzési Fúziós Központját (*Intelligence Fusion Centre,* NIFC), amely nem a NATO szervezetének része, de feladata a NATO műveleteinek hírszerzési támogatása a szervezet munkájában részt vevő tagállamok együttműködése eredményeként. A kooperáció fokozásának következő lépéseként 2010-ben átszervezték a korábbi hírszerző struktúrát, és létrehozták a Polgári Hírszerző Bizottságot

[36] Nagyon jó példa erre a magyar terrorelhárítás területe. Az irányító szintű koordináló szerv a Nemzetbiztonsági Kabinet. A nemzetbiztonsági szolgálatok vezetőinek feladatorientált koordinációs szintje a Kabinet mellett működő Terrorellenes Koordinációs Bizottság, míg a konkrét információcsere szintjét a Terrorelhárítási Információs és Bűnügyi Elemző Központ képviseli. Ez a fajta mélységben tagolt koordináció több ország nemzetbiztonsági szervezetrendszerében is megtalálható (USA, Egyesült Királyság, Németország).

(*Civilian Intelligence Committee,* CIC), valamint a Katonai Hírszerző Bizottságot (*Military Intelligence Committee,* MIC), amely szervezetek keretet biztosítanak a tagországok hírszerző szervezetei koordinációs mechanizmusainak. A CIC az első szervezet, amelynek segítségével a polgári titkosszolgálatokat be tudták vonni a NATO tevékenységébe. Fő feladata az Észak-atlanti Tanács közvetlen tájékoztatása hírszerzési kérdésekben, továbbá tanácsadás a kémkedéssel, a terrorizmussal, illetve egyéb fenyegetésekkel kapcsolatban, amelyek érinthetik a Szövetséget.[37] Az együttműködés további előmozdítása érdekében 2017-ben újabb lépésre került sor, amikor is létrehozták a Közös Hírszerző és Biztonsági Osztályt (*Joint Intelligence and Security Division,* JISD) a NATO főhadiszállásán, Brüsszelben. Ezt a lépést egyesek a legfontosabb reformnak tartják a NATO hírszerzési együttműködésének történetében.[38] Ahogy e rövid összefoglalóból kitűnik, a NATO a 21. század eddigi, kezdeti szakaszában komoly lépéseket tett a hírszerzés területén a tagállami együttműködések fokozására.

Az EU, hasonlóan a NATO-hoz, nem rendelkezik önálló, hírszerzést folytató hírszerző szervezettel. Első hírszerző szolgálata az 1999-ben létrehozott Helyzetelemző Központ volt (*European Union Situation Centre,* SITCEN), amely a tagországok hírszerző információit dolgozta fel, elemezte, és készített belőlük tájékoztatókat az EU vezetői részére. 2012-ben a SITCEN-t az Európai Külügyi Szolgálat (EKSZ) szervezetébe integrálták, annak egyik igazgatósága lett. Nevét Hírszerző és Helyzetelemző Központra (European Union Intelligence and Situation Centre, INTCEN) módosították, és közvetlenül az EU hírszerzéséért is felelős főképviselő irányítása alá került.[39] A szervezet elemzéssel és értékeléssel foglalkozó munkatársait a tagállamok nemzetbiztonsági szolgálataitól vezénylik, és OSINT-képességekkel is rendelkezik. Az EU az INTCEN mellett a katonai vonalon is rendelkezik hírszerzési szervezettel. Az EKSZ megalakítását követő átszervezés során került a Katonai Törzs, illetve azon belül a Hírszerző Igazgatóság (*Military Staff Intelligence Directorate,* MS INT DIR) az EKSZ szervezetébe. Működése az INTCEN-éhez hasonló. Ahogy látható, a 21. század eleje hírszerzési szempontból az EU számára is meghatározó időszak volt. Hasonlóan a tagállamokhoz, az EU-n belül is létrehozták azokat az információs központo-

[37] NATO: Civilian Intelligence Committee (CIC) (2011. november 16.).

[38] Loringhoven (2017): i. m. 16.

[39] Beke József: Az Európai Unió hírszerző képességének technikai támogatása. *Nemzetbiztonsági Szemle,* 6. (2018), 2. 56–68.

kat, amelyek megadták a tagországok közötti együttműködés kereteit, és amelyek kialakítási, működési elvei a tagországok közötti együttműködést ösztönzik.

Századunkban már eddig is számos olyan változás történt a világban, aminek eredményeként szervezeti változásokat figyelhettünk meg a nemzetbiztonsági szervezetrendszerben, azonban ezek leginkább a nemzetbiztonsági szolgálatokhoz, valamint a koordinációs szervezetekhez kötődtek. A változások egyáltalán nem érintették a nemzetbiztonsági szervezetrendszerek ellenőrzési alrendszerét. Ez annak köszönhető, hogy napjainkra a demokratikus országokban a nemzetbiztonsági szolgálatok tevékenységének ellenőrzése érdekében már létrejöttek azok a szervezetek és kialakultak azok az ellenőrzési mechanizmusok a hatalmi ágak, illetve a civil társadalom oldaláról, amelyek segítségével fel lehet tárni a nemzetbiztonsági szolgálatok esetleges jogszerűtől eltérő működését.

A 21. század eddig eltelt időszakát a nemzetbiztonsági szolgálati tevékenység tekintetében egyik oldalról a jelentős, új típusú kihívásokkal, míg másik oldalát a biztonságtudatosítással és az együttműködéssel lehetne leginkább jellemezni. A 21. század elejére egyrészt az informatika robbanásszerű fejlődésének hatására jelentős, új típusú kihívások jelentek meg a kémelhárítás, az információs és az informatikai rendszerek biztonsága területein. Másodsorban a terrortámadások a mindennapjaink részévé váltak úgy, hogy a 2000-es évek elején elkövetett terrortámadásokat követően már történtek változások az elhárító tevékenység hatékonyabbá tétele érdekében, de ennek ellenére tíz évre rá Európának mégis újabb támadásokat kellett elszenvedni.

E kihívásokra jelentett részben megoldást a biztonságtudatossági programok bevezetése, amely ilyen megvalósításban mint új prevenciós módszer szinte berobbant a szolgálatok világába. A terrorkockázatok kapcsán pedig egyértelműen megfogalmazódott, hogy a nemzetbiztonsági szolgálatok közötti együttműködést erősíteni, ennek részeként az érdemi információk megosztását pedig fokozni kell. A terrorkockázatok csökkentése érdekében egyes országokban önálló terrorelhárítási szervezeteket hoztak létre, az együttműködéseket pedig különböző koordinációs szervezeteken keresztül fokozták. E második megoldás részeként jelentős számban jöttek létre egyes országokban, de nemzetközi szervezeteken belül is információfúziós központok, amelyek az alapfunkciójukon (információfeldolgozás, tájékoztatás) túl hatékony segítséget jelenthetnek az együttműködések fokozásán keresztül is a nemzetbiztonsági kockázatok felderítésében, elhárításában.

Az információs csatornák alapján felállítható három modell (versengő, ágazati, együttműködő) tekintetében elmondható, hogy az elmúlt időszakban

a kooperációt erősítő megoldások (a szervezetrendszer több szintjén megjelenő koordináló szervezetek, fúziós központok) előretörésének hatására a kooperáló modellek felé látható elmozdulás. Azt, hogy mit hoz a század további része, a szervezetrendszerre ható tényezők számossága, folyamatos változása miatt nehéz megjósolni. A változás dinamikája és az érintett területek sokasága alapján azonban rövid időn belül jelentős változásokra kell felkészülni. A kockázatok sokszorozódása, a határon átnyúló jellege, súlyossága okán tovább kell erősíteni az országokon belüli, illetve a nemzetközi együttműködéseket. A big data-jelenség miatt az OSINT jelentős felértékelődése, specializálódása várható. A technológiai robbanás, a kibertér jelentőségének folyamatos növekedése következtében egyrészt további, új típusú nemzetbiztonsági szintű kockázatok megjelenése várható, másrészt rövid időn belül széles körben jelenhetnek meg a szervezetrendszerekben az önálló jelhírszerző szolgálatok.

Az információgyűjtés területeinek evolúciója, a kibertér jelentősége

Dobák Imre

Bevezetés

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

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

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

https://doi.org/10.36250/00904_07

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

Hatások – nemzetközi folyamatok

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

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

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

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

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

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

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

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

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

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

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

Titkos információgyűjtés a kibertérben

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

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

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

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

IKT-szolgáltatóval való együttműködés

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

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

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

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

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

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

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

Informatikai infrastruktúrán áthaladó kommunikáció ellenőrzése

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

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

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

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

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

Kibertérben megjelenő aktív eszközök, hackertechnikák alkalmazása

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

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

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

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

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

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

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

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

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

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

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

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

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

Aktív képességek

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

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

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

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

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

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

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

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

HUMINT a kibertérben

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

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

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

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

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

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

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

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

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

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

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

A közösségi oldalak jelentősége

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

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

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

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

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

[27] Szabó (2019): i. m. 71.

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

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

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

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

[29] Erdész (2018): i. m.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[36] Steinhart (é. n.): i. m. 164.

[37] Steinhart (é. n.): i. m. 164.

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

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

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

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

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

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

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

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

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

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

A HUMINT reneszánsza

Regényi Kund Miklós – Drusza Tamás

Bevezetés

A 21. század második évtizedének végén a HUMINT, azaz az emberi erőforrásokból való információgyűjtés egyértelműen reneszánszát éli Európában (jelen fejezetben Európa alatt az Európai Unió országait értjük). Ebben az alfejezetben ehhez a reneszánszhoz vezető utat törekszünk bemutatni, azaz bemutatjuk a HUMINT születését, meggyőződésünk szerint első virágzását, szakmai álláspontunk szerint átmeneti háttérbe szorulását, mai helyzetét, azaz újjászületését, illetve lehetséges fejlődését a közelebbi jövőben. Tesszük ezt úgy, hogy tisztában vagyunk azzal: vannak országok és szolgálatok, ahol nem beszélhetünk reneszánszról, hiszen ott a HUMINT mindvégig megőrizte kitüntetett szerepét a titkos felderítés ágazatai között. A nyílt forrásokra támaszkodó kutató szempontjából sajnálatos, hogy ezek az országok a titkosságra vonatkozó hagyományokat is őrzik, így megnevezni is csak feltételes módban lehet őket, de aligha téved nagyot, aki az Egyesült Királyságra és Oroszországra gondol. Percepciónk az akadémiai kutatóé, nem egy konkrét rendvédelmi szerv gyakorló felderítőjéé. Gondolatainkat az érdeklődő laikus és szakmai közönségnek szánjuk. Örülnénk, ha a leírtak gondolkodást, vitát és reflexiót váltanának ki az akadémiai világban és a titkosszolgálatok világában egyaránt.

És kezdetben volt a HUMINT

Nem egyszerű feladat a titkos felderítésről és annak legrégibb ágáról, az emberi erővel folytatott, közkeletűbb nevén az ügynöki munka gyökereiről írni.[1] A titkos tevékenységekről jellegük miatt eleve kevesebb információ marad fent, ez az írásbeliséget megelőző korokról fokozottan igaz. Ha az emberi erővel folytatott titkos felderítés természetét szeretnénk megérteni, akkor nem elsősorban

[1] Az alfejezethez felhasznált irodalom: Boda József – Regényi Kund (szerk.): *A hírszerzés története az ókortól napjainkig.* Budapest, Dialóg Campus, 2019; Pilch Jenő: *A hírszerzés és kémkedés története* I–III. Budapest, Franklin Társulat, 1936; Jeffrey Burds: *The Second Oldest Profession: A World History of Espionage.* Boston, Recorded Books, 2011.

https://doi.org/10.36250/00904_08

a régi források, hanem emberi természetünk, viselkedésünk elemzésén keresztül vezet az út.

Az emberi erővel folytatott hírszerzésről[2] szóló fejezet elejére feltétlenül kívánkozik a szokásos közhely: a kémkedés egyike a legősibb mesterségeknek, és ez nem véletlen. Minden élőlény igyekszik megtudni, milyen lehetőségeket vagy veszélyeket rejt rá nézve a környezete, így a környezet kikémlelése egy teljesen természetes cselekvés, amelyet az életösztön vezérel. Az ember azonban az állatokhoz képest ezt is magasabb szintre emelte azzal, hogy nem várva be a veszély megjelenését tudatosan törekedett annak saját területén való felderítésére. További előrelépést jelentett, mikor már nem maga kémlelte ki a veszélyt, hanem másokat bízott meg ezzel. Ehhez már szükség volt valamiféle összetettebb kommunikációra, amellyel a „feladatot" meg lehetett fogalmazni, és a megszerzett ismereteket át lehetett adni.

Más kérdés, hogy ez a kezdetekben még egyáltalán nem jelentette a mai értelemben vett hivatást. A kémkedés fejlődésének folyamata – illetve az azt alkalmazó államokkal, szervezetekkel együtt – aztán időről időre egyre fejlettebb formákat öltött, míg végül eljutottunk a mai nemzetbiztonsági szolgálatok által alkalmazott professzionális HUMINT-módszerekig. Nézzük röviden e folyamat kezdeti szakaszait. Ebben a fejezetben megállapításainkat illetően kizárólag a logikai elemzés eszközére tudunk hagyatkozni, mert ezekről az időkről nem állnak rendelkezésünkre írott források.

Természetes, hogy már az őskor vándorló embercsoportjainak fel kellett deríteniük, hogy hol tudnak megfelelő életfeltételeket találni, hova költözzenek a kimerülő területről, vagy a változó időjárás hatására. Ahogy az emberi közösségek egyre nagyobbak és fejlettebbek lettek, a túlélés érdekében egyre tudatosabban törekedhettek a természeti erőforrások megszerzésére. Azok a területek voltak értékesek számukra, amelyek több élelmet és biztonságot, jobb életfeltételeket kínáltak. Egy idő után azonban e területekért is megindult a küzdelem, különösen akkor, ha könnyebbnek tűnt megszerezni egy másik csoport területét, mint keresni egy hasonlót. Ekkor az emberi erőforrással folytatott hírszerzés már túlment a terület felderítésén, meg kellett ismerni az ellenérdekelt felet is.

Ez a folyamat folytatódott az ember letelepedése után is. Érdekes módon az emberi közösségek letelepedése máig vita tárgya, a legújabb nézetek szerint

[2] Az emberi erőforrásból való információszerzés tárgyában két monografikus jellegű művet említhetünk: Regényi (szerk.) (2019): i. m. 163; Dobák Imre – Regényi Kund (szerk.): *Szakmatörténeti szemelvények*. Budapest, Nemzetbiztonsági Szakszolgálat, 2014.

a mezőgazdaság kialakulása nem oka, hanem következménye volt e folyamatnak. De a tény az, hogy a letelepedés az i. e. 5000. év környékén magával hozta az államok kialakulását, amelyek igyekeztek egyre nagyobb területekre kiterjeszteni hatalmukat. A fegyveres konfliktusok így egyre gyakrabban robbantak ki, amelyeket egyre modernebb fegyverekkel vívtak, ami újfajta kémkedési formákat honosított meg. A jobb eszközökkel és fegyverekkel rendelkező csoportoktól meg kell tudni, hogyan készítik azokat. A ma ipari kémkedésnek nevezett tevékenység egyik első megjelenése lehetett körülbelül i. e. 3000–5000 évvel a fémmegmunkálási technikák riválisoktól történő megszerzése. A fém bányászata, ötvözése és megmunkálása már olyan összetett munkafolyamat, amely nehezebben kikísérletezhető, mint például a kőből való pattintás vagy a fából való faragás.

A fenti gondolatmenetből is látszik a korabeli nagyobb embercsoportok, törzsek, később pedig államok közötti rivalizálás leggyakoribb formája egy másik ősi viselkedésforma, a fizikai küzdelem, azaz a háborúskodás volt. Ebből fakadhatott Pilch Jenő – az első komoly összefoglaló mű szerzőjének gondolata is, aki szerint e korai időszakban a kémkedés és felderítés még nem választódott szét jelentősen.[3] Különösen fontos lehetett a kémkedés alkalmazása a gyengébb fél számára. Néhány jó kémet alkalmazva kikémlelni az ellenség gyenge pontjait vagy megvesztegetni az ellenség egy fontos vezetőjét még mindig lényegesen olcsóbb volt, mint fegyvereket gyártani és katonákat felszerelni.

Azt már az ókorban is felismerték, hogy a titkos módon, kémek révén megszerzett információk a hadviselés fontos támaszai. A kémkedés első írásos említése is ezt támasztja alá. Az Ótestamentum szerint az (i. e. 1500 körül) Jerikót ostromló izraeliták kémek révén tudták meg a város gyenge pontjait, és ők segítettek annak elfoglalásában is.[4] Az i. e. 4–3. században Szun-ce által írt, *A hadviselés törvényei* című munka, illetve a Flavius Vegetius Renatus az i. e. 400 körül kiadott műve is, amely utóbbi a korábbi évszázadok római katonai íróinak alapján készült[5] szintén ezt a nézetet támasztják alá. A titkos információgyűjtés elsődleges célja tehát a katonai összecsapásokra való felkészülés volt, és ez tulajdonképpen a 20. századig így is maradt. Nem kell azonban mondani, hogy a módszerek és az eszközök sokat változtak. Az írások sokszorosításának technikáját megelőzően az információgyűjtés egyetlen lehetséges és kézenfekvő eszköze az ember volt. Nézzük, hogyan működhetett a középkorig a titkos információgyűjtés.

[3] Pilch (1936): i. m. 177.
[4] Burds (2011): i. m. 11–12.
[5] Pilch (1936): i. m. 12–13.

Fontos kiindulópont, hogy ekkor az információgyűjtés csak akkor lehetett sikeres, ha az azt végző személy személyesen vagy egy vele együttműködő helyben élő személy révén látta, hallotta az adott dolgot. Ehhez azonban az adott helyre kellett utaznia. Ebből következett, hogy kémszolgálatra elsősorban azok a személyek voltak alkalmasak, akik hivatásukból adódóan eljuthattak a célterületre. Ezek elsősorban:

– kereskedők;
– követek;
– egyházi személyek.

Ezek a személyek azonban a kor adottságai miatt gyakran alkalmaztak helyi segítőket, azaz a mai értelmezés alapján rezidentúrákat építettek ki, amelyek összegyűjtötték számukra a híreket. Természetesen ezek nem azok a nagyon alaposan szervezett és fenntartott hálózatok voltak, mint manapság. Az persze valószínű, hogy a fenti személyek rendszeresen foglalkoztak kémkedéssel, azonban az, hogy azt kinek a javára végezték, gyakran változhatott. Annak kémkedtek, akinek hatalma volt felettük, aki többet fizetett, vagy akinek a politikájával jobban tudtak azonosulni. E dolgok természetéből fakadóan az ugyanazon kémkedésre szakosodott személy „megrendelője" valószínűleg gyakran változott, különösen a kereskedők esetében.

Adódik a kérdés, hogy kik voltak azok, akik az embereket kémkedésre alkalmazták. Mivel a modern szolgálatok csak a 19. század „termékei", valaki másnak kellett alkalmazni a kémeket. Értelemszerűen a két legfontosabb információfelhasználó központ az uralkodó és a hadsereg volt, de feltehetően – főleg a középkortól kezdődően – a magánszféra szereplői, azaz eleinte egyházi és világi földesurak, majd termelő és pénzügyi vállalkozások, magándetektív-irodák (például Pinkerton), hírügynökségek is alkalmaztak embereket információszerzésre.

A HUMINT első virágkora

Ebben a fejezetben arra keressük a választ, hogy mikor volt, és főleg miért volt a HUMINT virágkora. A HUMINT virágkora Európában és Észak-Amerikában a titkosszolgálatok archaikus, klasszikus és modern korszakára egyaránt kiterjed, azaz, hogy régebbre ne menjünk vissza, kiterjedt a 17. századtól a hosszú 19. század végéig, azaz az I. világháborúig.

Ez alatt a hosszú idő alatt vitathatatlanul a HUMINT volt az uralkodó titkos felderítési eszköze. Ha ennek a jelenségnek az okait keressük, túl egyszerű lenne azt állítani, hogy hiszen nem volt más: egy titkosszolgálat mindig is arra törekedett és napjainkban is arra törekszik, hogy az adott társadalmi viszonyok között alkalmazható leghatékonyabb titkos felderítési eszközöket minél szélesebb körben használja. Vizsgáljuk meg tehát, melyek voltak azok a körülmények, amelyek a HUMINT alkalmazása mellett szóltak.

Elsősorban és mindenekelőtt: a korban az emberi tevékenység volt a meghatározó. Bármit előállítani, legyen az szellemi vagy anyagi érték, csupán az emberek voltak képesek. Nyilván a korszak vége felé haladva egyre több géppel találkozhatunk, de az ember szerepe továbbra is nagyon széles körű maradt. Gondoljunk csak arra, hogy aki tehette, háztartásában is például cselédeket alkalmazott olyan feladatokra, amelyeket manapság gépek látnak el. Nem volt ez másként a titkos felderítés vonatkozásában sem: a szükséges információkat kézenfekvő és egyszerű volt más emberektől megkérdezni.

Másodsorban a korabeli viszonyok megkönnyítették az emberek bármilyen munkára, adott esetben titkos felderítési feladatra való igénybevételét. A korban a társadalomnak meglehetősen hierarchikus felépítése volt. Aki a társadalmi piramis magasabb fokán helyezkedett el, viszonylag könnyen rákényszeríthette akaratát az alatta állóra, akár kényszerrel, akár – és ez volt a leggyakoribb – a hagyomány okán, akár pedig pénzzel vagy más juttatással. Magyarul, ha egy „úr" kért valamit egy „szolgától", akkor arra jó esélye volt, hogy kérése teljesülni fog. Ha pedig ezért fizetett is valamit, az az alárendeltnek tiszta nyereség volt. Ez a fajta munkára való megbízás vagy felkérés meglehetősen kevés formasággal járt, elég volt hozzá a szóbeli megállapodás, esetleg egy kézfogás, nem kellett hozzá részletes munkaszerződés. Jól látható, hogy ezek a faktorok a HUMINT-ot segítették.

Ugyancsak segítette a HUMINT-ot, hogy a korszakban, különösen annak vége felé, megjelent egy nagyon erős rendezőelv, amely nagymértékben segítette a titkos felderítésre az emberi erőforrások megnyerését: a nemzeti eszmére, a nacionalizmusra gondolok. A nemzeti eszme a korban mindent átfogó hivatkozási alap volt. A haza, a nemzet szolgálatának önnönmagában nagyon erős és nagyon pozitív tartalma, értéke volt. Paradox, de előfordult, hogy bűnözők is örömmel vállalták a haza, a nemzet szolgálatát (nyilván büntetésük elengedése vagy enyhítése fejében). Hasonló paradoxon, hogy a korszak végén, a 19. és 20. században a nemzeti eszme mellett annak logikai ellenpárja, tagadása, azaz az internacionalizmus is komoly meggyőző erővel rendelkezett.

A korban a titkosság szerepe is más volt, mint amit a 21. században megszoktunk. A munkaerőről mondottak erre az esetre is alkalmazhatók: a társadalmi piramis magasabb fokán állóknak kvázi joguk volt az alattuk állók titkaira. Másrészt az azonos szociális státuszban levők között a bizalom is erősebb volt. Titkok elmondása becsületszóra tett ígéret fejében, miszerint azt senkinek nem adja tovább, előfordult. A társadalmi piramis alacsonyabb fokán állók viszont azzal segíthettek magukon, hogy mintegy észrevétlenként (cselédként, kocsisként, inasként) számos titkos cselekménynek lehettek szem- és fültanúi. Nyilvánvaló, hogy ez a hozzáállás a titkos felderítők dolgát ugyancsak megkönnyítheti.

A HUMINT-ot segítette, hogy a végrehajtók autonómiája nagyobb volt, mint manapság. Könnyen elképzelhető, hogy egy vitorlás hajó kapitánya lényegében teljes egészében magára volt hagyatva, és külső erő, ellenőrzés, kialakult forgatókönyv, eljárásrend cselekedeteit viszonylag sok áttételen keresztül befolyásolta csupán. A feladat végrehajtásának záloga ebben a helyzetben a sokéves gyakorlat, a gyakorlaton alapuló kiválasztás, a közös cél és nem utolsósorban a parancsnokokba vetett bizalom volt. Újabb körülményként kell megemlítenünk a népesség nyilvántartásának, anyakönyvezésének máról visszatekintve meglehetősen csökevényes voltát. Az emberek anyakönyvezésére (születésük, haláluk, házasságkötésük, együttesen személyazonosságuk nyilvántartására) a korszaknak a végéig az egyes egyházközségek vállalkoztak. Állami, központi nyilvántartás csak az államigazgatás forradalmát követően, a tömeghadseregek igényeinek kielégítése céljából a 19. század végén jelent meg. Ilyen körülmények között a legenda biztosítása egyszerűbb feladat volt.

A korszakban egyfelől a titkosszolgálat és a hadsereg, másfelől a nemzetbiztonság és a mai szóval rendőrségként emlegetett rendészeti szervek között a kapcsolat szoros volt. Ez azt jelenti, hogy belföldön a nemzetbiztonság rendelkezésére állt a büntetőeljárás eszköztára: a büntetéstől való eltekintés, a nyomozás során tett vallomások, vagy a nyomozás során akár kényszerrel kicsikart vallomások egyaránt. Hasonló volt a helyzet például a hadifoglyok kihallgatása során is. Itt kell aláhúzni a fizikai kényszer nem túl dicsőséges, de kétségtelen meglévő szerepét a HUMINT ezen korszakában.

Végül, de nem utolsósorban beszélnünk kell a fizikai veszély szerepéről. A HUMINT egyik legfőbb hátránya, hogy a kapcsolatnak, vagy a szolgálat szakembereinek fizikai veszélyt kell vállalnia, még hogyha ennek a mértéke változó is. A vizsgált korszakban az emberélet jelentősége és a fizikai veszélynek a súlya teljesen más volt. Az a fajta fájdalommentességre, sérülésmentességre, kockázatmentességre törekvő attitűd, amely napjainkat jellemzi, a korszakban egyáltalán nem volt jelen, sőt az ellenkezője volt az általános. Másként fogalmazva, kapcsolattartó nem

aggódott a kapcsolata miatt, hanem fájó szívvel elfogadta az esetleges veszteséget, hasonlóan például egy harctéri parancsnokhoz.

A HUMINT háttérbe szorulása

A HUMINT-hoz képest az alternatív titkos felderítési módszerek szintén régi múltra tekintenek vissza. Már az antikvitásban is létezett az állami posta, amelynek titkos felderítési célú felhasználása a kortársak számára is magától értetődő volt. Már a reneszánsz idején is voltak rejtjelek és létezett rejtjelfejtés. A 17. században megjelenik az első nyomtatott újság, száz évvel később megjelennek a hírügynökségek, azaz megteremtődnek a nyílt forrású információszerzésnek, az OSINT-nak a feltételei.

A folyamat, azaz a lehetséges alternatívák körének bővülése az ipari forradalom előrehaladtával egyre gyorsul. A 19. században megjelenik a távíró és a telefon, és szinte ezzel egy időben a távíróvonalakat, telefonvonalakat lehallgató harctéri járőrök. A 20. század elején megjelenik a telefonközpont. A kor leleményes detektívjei rábírják a telefonos kisasszonyokat, hogy vagy jegyezék fel egy adott előfizetővel beszélgetést folytató többi előfizetőt, vagy esetleg hallgassanak bele a beszélgetésbe, és gyorsírással rögzítsék azt.

Az I. világháborúban tömegessé válik a légi felderítés, stratégiai jelentőségre tesz szert a katonai vagy diplomáciai rejtjeltáviratok elfogása és megfejtése. (Gondoljunk itt Pokorny Hermannra vagy a Zimmermann-táviratra.) A II. világháborút megelőzően az automata telefonközpontok lehallgatására már Magyarországon is mágnesszalag-alapú hangrögzítést alkalmaztak, a II. világháború alatt a britek pedig a német haditengerészet rejtjeleinek megfejtésére létrehozták az első elektromechanikus számítógépet, az úgynevezett Bombát.

A II. világháború után a fejlődés tovább gyorsul. A leképezés, azaz az IMINT az űrkutatás, vele párhuzamosan pedig a nagy magasságú légi felderítés villámgyors fejlődésével minőségileg magasabb szintre emelkedett. Az „Öt szem", azaz az angolszász titkosszolgálatok együttműködésének köszönhetően létrejön egy globális jelfogó és lehallgató rendszer, amely automatizáltan képes az egyes tartalmakra reagálni, azokat rögzíteni, a kommunikáció résztvevőit pedig azonosítani. A világháló megjelenésével pedig lehetővé vált a nyílt forrású információk lényegében valós időben és elenyésző költségekkel való gyűjtése.

Mindez egy olyan illúziót teremtett, hogy lehetséges, sőt kívánatos egyfajta totális megfigyelése az ellenérdekelt feleknek, amelyek persze akár otthon, hazai

földön is lehetnek. Hallgatjuk telefonjaikat és egyéb elektronikus kommunikációjukat (és más kommunikációjuk gyakorlatilag nincs is), elemezzük a világhálón róluk megjelenő nyílt forrású információkat, legyenek azok szöveg-, hang- vagy képalapúak. És persze valahogyan az is megvalósult, hogy ezeket az információkat az emberek önként és saját költségükön teszik közzé. A műholdak, felderítőgépek és drónok képei pedig, kiegészítve – és ez egy nagyon fontos mozzanat – a biztonsági kamerarendszerek képével, lehetővé teszik akár az egyén teljes, szinte minden földrajzi helyre kiterjedő nyomon követését is.

A technika robbanásszerű, diszruptív jellegű fejlődésén túl melyek az egyéb faktorok, amelyeket itt érdemes megemlíteni? A technikai adatszerzés egy szervezett, gyáriparjellegű tevékenység, amely a rend és az ellenőrzöttség látszatát tudja kelteni a külső szemlélő számára, ellentétben a HUMINT titokzatos, titokzatoskodó és romantikus világával. A technikai adatszerzés hazai földön vagy legalább jórészt hazai földön meg tud valósulni, az emberek tehát nincsenek veszélyben. A megszerzett információk a keletkezéssel szinte vagy teljesen azonos időben, valós időben rendelkezésre állnak, ami túl azon, hogy tényleges előnyökkel jár, látványos is. A megszerzett információk nagyon könnyen feldolgozhatók, kombinálhatók, összesíthetők. Létezik az az illúzió is hogy az, hogy megfigyelnek, önmagában nem fáj, tehát a technikai adatszerzés erkölcsileg is támogatható.

Minden a legnagyobb rendben tehát? A titkosszolgálatok fejlődése arra tanít, hogy nincsen egyedül üdvözítő és minden mást feleslegessé tevő felderítési módszer. A 21. század elejére megmutatkoztak a technikai adatszerzés korlátai is.

A technikai hírszerzés csődje: 9/11

A technikai lehetőségek fejlődésével a technikai eszközökkel folytatott információgyűjtés[6] óriási léptekkel haladt előre.[7] Ennek két fő oka volt. Egyrészt a technikai eszközök olyan új típusú információkat tudtak szolgáltatni, amelyek korábban ismeretlenek voltak. Másrészt a technológiai eszközök alkalmazása jelentősen

[6] A kifejezés jelenti azokat az eszközöket, ahol az információgyűjtés automatizált eszközökkel történik, minimális emberi beavatkozással vagy a nélkül. Elsősorban elektromos jeleket gyűjtő eszközöket kell rajta érteni, de idetartoznak a megfigyelő műholdak, illetve a CCTV-hálózatok is.

[7] Az alfejezethez felhasznált irodalom: A 9/11 Bizottság jelentése: *The 9/11 Comission Report* (é. n.), valamint Erik J. Dahl: *Warning of Terror: Explaning the Failure of Intelligence against Terrorism.* Master of Arts in Law and Diplomacy Thesis, The Fletcher School, 2004.

lecsökkentette az információgyűjtés kockázatait, így a dekonspiráció bekövetkezésének esélyét, valamint az emberi veszteségek mértékét. A gyorsan fejlődő technika egyre inkább átalakította a hírszerzés attitűdjét abba az irányba, hogy a technikai módszereket nem kizárólag az emberi forrásból származó információk kiegészítésére használták, hanem megpróbálták azt helyettesíteni. Az egyensúly így megbillent a technológia javára, amely komoly problémákhoz vezetett, amelyeket az Egyesült Államok példája támaszt alá legjobban.

A Szovjetunió nagyrészt technológiai verseny révén történő legyőzése azt az illúziót alakította ki az USA szolgálataiban, hogy a technológiának kell prioritást adni. A humán forrásokra szánt erőforrásokat csökkenteni kezdték, mondván, hogy már nincs komoly ellenfél, olyan pedig egyáltalán nem létezik, amely képes lenne felvenni a harcot a technikai fölénnyel. A CIA esetében e folyamat megindítását Stansfield Turner személyéhez kötik, aki 1977–1981-ig volt a szervezet igazgatója. Különösen felgyorsult e tendencia az információtechnológia robbanásszerű fejlődésével a 20. század utolsó évtizedeiben.

Ebben a helyzetben érte a titkosszolgálati rendszert egy több szempontból új, szokatlan – ma úgy mondanánk –, aszimmetrikus fenyegetés. Az ideológiailag motivált, mély konspirációra képes, sejtszerűen felépített, jól szervezett iszlám terrorizmus így lépéselőnybe került a hagyományos konspirációs módszerekhez és nagy méretű ellenséges szolgálatokhoz, valamint technológiai fölényhez szokott amerikai szolgálatokkal szemben.

Jól alátámasztják ezt a 2001. szeptember 11-i eseményeket vizsgáló bizottság jelentésében olvasható megállapítások. Ezek elsősorban az értékelés és elemzés, a tájékoztatás és az információmegosztás terén jelentettek döntő fordulatot, de nagy hatású észrevételeket fogalmaztak meg a technikai és az ügynöki adatszerzés helyére, szerepére vonatkozóan is. Miközben az FBI terrorelhárító részlegének költségvetése az 1995–2000 körüli időszakban háromszorosára nőtt, aközben a személyi állományra vonatkozó kiadások stagnáltak, a drogellenes küzdelemben részt vevő hivatásos állomány kétszer nagyobb volt, mint a terrorelhárítással foglalkozók száma.[8] Az FBI emberi erőforrással folytatott információgyűjtési kapacitása emiatt erősen korlátozott volt. Mindezek következménye 1993 és 2001 között számtalan nagy hatásfokú sikeres terroristamerénylet, amelyekben összesen több ezer ember vesztette életét, nem beszélve az óriási anyagi kárról. E merényletek folyományaként a 2000-es évek elejétől, több más jelentős lépés mellett megkezdődött az előző években elhanyagolt HUMINT végzésére alkalmas kapacitások újraépítése.

[8] The 9/11 Comission Report (é. n.): i. m. 77.

A HUMINT napjainkban – a HUMINT reneszánsza

Amikor a HUMINT reneszánszáról beszélünk, magyarázatként nem elégedhetünk meg annyival, hogy a fejlődés ingája egy idő után törvényszerűen elkezd visszafelé lengeni. Ha a 20. század és különösen annak második fele a technikai információszerzés diadala volt, akkor természetes, hogy az ingának a HUMINT felé kell lengeni. Ennél azonban többről van szó.

Kétségtelen, hogy a technikai hírszerzés egyfajta válságba jutott, úgy tűnik, hogy a hagyományos, 20. századi technikai információszerzés elért fejlődésének csúcsára. A hidegháború alatt kifejlesztett, lényegében automatizáltan és igen magas technikai színvonalon működő technikai információszerző rendszerek igen nehezen voltak adaptálhatók egy másfajta, egy aszimmetrikus ellenféllel szemben. Leegyszerűsítve, ha az ellenfél nem használ telefont, e-mailt, távírót, hanem ehelyett lovas futárokon küldi az üzeneteket; ha az ellenfél tudatosan embereket iktat a technikai információtovábbítás láncába (amikor az előbb említett futár például videókazettát vagy pendrive-ot visz magával), nos, ebben az esetben a technikai információszerzés lehetősége csökken, a HUMINT jelentősége – akarva, nem akarva – erősen megnövekszik.

A másik igen nagy kihívás a jogi környezetben található meg. A mindenki számára látható külső ellenség – azaz a nyugati világra vonatkoztatva a Szovjetunió és a Varsói Szerződés – eltűnésével a mindig is jelen lévő jogvédő hangulat, nézetrendszer egyre inkább előtérbe kerül, egyre jelentősebbé, meghatározóbbá válik. Azaz a széles körű technikai adatszerzésre épülő információszerzési rendszer egyre gyakoribb és egyre intenzívebb kritika tárgyát képezi, és ezért alkalmazása belföldön növekvő nehézségekbe ütközik.

Két másodlagos körülményről érdemes itt említést tenni. Az egyik, hogy a posztmodern korban a nemzetbiztonsági szolgálatok fokozódó mértékben a nyilvánosság ellenőrzésének, kritikájának tárgyát képezik, társadalmi megbecsülésükért újra és újra meg kell küzdeniük. A másik, hogy természetesen a technikai hírszerzéssel szemben fellépő nézetek és mozgalmak jelentős lendületet kaptak az utóbbi évek botrányaitól – ehelyütt a Snowden- és WikiLeaks-botrányt említhetjük –, amelyek mögött paradox módon embereket, személyeket találunk, akik irányítottsága mellett komoly érvek hozhatók fel.

A technikai információszerzés paradigmaváltása szintén hozzájárult a HUMINT reneszánszához. Itt a netalapú, felhőalapú kommunikációs csatornák, azaz a VOIP-telefonálás, illetve üzenetküldő és fájlmegosztó alkalmazások

futótűzszerű terjedésére kell gondolunk, amelyek hatékony ellenőrzése új technikai környezetet követel.

A technikai információszerzés kihívásai azonban nem vezettek volna a HUMINT reneszánszához, ha nem került volna előtérbe a HUMINT néhány előnye. Ezek között a HUMINT viszonylagos költséghatékonyságát említjük elsőként. Bármennyire is úgy tűnik, hogy a HUMINT nem olcsó, a valóságban ez téves percepció, hiszen mindez csak viszonyítás kérdése. Például egy globális jelelfogó rendszer költségeihez képest a HUMINT forrásigénye gyakorlatilag kimutathatatlan. Fontos további körülmény, hogy egy ilyen jelfogó rendszer kifejlesztéséhez, továbbfejlesztéséhez szükséges kompetencia sem áll egyenlően rendelkezésre. Arról nem is beszélve, és ez egy nagy jelentőségű tanulság, hogy a HUMINT legfőbb alkotója, az ember nem avul el néhány év, esetleg évtized alatt. Egy emberbe beruházni (időt, pénzt, saját embert) tehát titkos felderítés szempontjából is jó üzlet.

Másik nagyon fontos gondolat, hogy HUMINT legmagasabb szintjének, a titkos kapcsolattartásnak az eszköze – azaz egy kellőképpen felkészített, motivált, bevezetett forrás – rugalmasan alkalmazható. Önmaga képes reagálni a körülmények változására. Egy forrás esetleg más nemzetbiztonsági szempontból releváns területre is átcsoportosítható. Egy ilyen forrás autonóm működésre is képes. Egy ilyen forrás nem igényel bonyolult, részletesen lefektetett és szabályozott eljárási rendet. Kellő motiváció mellett elegendő a feladatot ismertetni számára. Katonai hasonlattal élve egy titkos kapcsolat egyszemélyes harci kötelék.

A gépekhez és a technikai adatszerzéshez fűződő viszonyhoz visszatérve, egy titkos kapcsolat nemcsak hogy nem avul el, hanem képes kitanulni, titkos felderítési szempontokból kiaknázni az újabb és újabb technikai adattároló adattovábbítási rendszereket is – ma is, és holnap is.

Ugyancsak fontos szempont, hogy emberek és emberek közötti viszony jogi szabályozása viszonylag állandó, változása lassú, azaz nem kell attól tartani, hogy embereket feladatra – akár titkosan – alkalmazni, emberekkel beszélni a belátható jövőben tilalom tárgyát képezi majd. Hasonlóképpen, az emberek közötti kapcsolattartás spektrumának vannak olyan elemei, amelyek nem vagy másként hagynak nyomot a kibertérben, azaz a kapcsolattartás egyes elemei a technikai felderítés eszközeivel nem ismerhetők meg.

Szólni kell természetesen azokról a körülményekről is, amelyek a HUMINT reneszánsza ellen hatnak. HUMINT nincs emberek nélkül. Egy titkos kapcsolat kiválasztása, kiképzése, alkalmazása olyan szakértelmet igényel, amely jelentősen eltér a technikai adatszerzés keretén belül szükséges kompetenciáktól. Hasonlóképpen, a kapcsolattartásban részt vevő szakemberek irányítása, vezetése is más,

hagyományosabb eszközöket, módszereket, szervezeti kultúrát igényel. Szerencsére számos esetben ezek a készségek az egyes szervezetekben (még) megvannak, azonban ezeket szinte mindig fejleszteni kell.

Nagyon nagy kihívás a motiváció kérdése. A nemzetállamok lassú eróziójával egyre nehezebb meggyőzni a lehetséges titkos kapcsolatokat arról, hogy érdemes és helyes a nemzetbiztonsági szolgálatot támogatni, azzal együttműködni. A fejlett világban a nyílt vagy burkolt nyomásgyakorlás lehetőségei is behatároltak. (Ez a fejlődő világra nem igaz, gondoljunk a terrorizmusellenes fellépést kísérő kínvallatással kapcsolatos botrányokra.) A rendőrségtől elkülönülten működő nemzetbiztonsági szolgálatok számára is nehézkes a büntetőeljárás adta lehetőségek kihasználása.

Nagy probléma az egyre nagyobb mértékben jelen levő (közterületi, biztonsági) kamerarendszerek, illetve kamerarendszerek által rögzített képeket összekapcsoló és azokat elemezni képes, egyre inkább mesterséges intelligencián alapuló szoftverek rohamos terjedése.[9] A szociális média a már régóta jelen levő precíz és széles körű anyakönyvvezetéssel, továbbá a biometrikus azonosító jelet tartalmazó okmányokkal együtt új kihívás elé állítja a szakembereket a legenda kidolgozása, alkalmazása és alátámasztása terén. E kihívásokra jelenleg nincs általánosan érvényes és mindenki számára használható válaszreakció.

A HUMINT lehetséges jövője

A jelenleg látható trendeket figyelembe véve természetesen nem gondolhatjuk, hogy a technikai adatszerzés eltűnik. Azt azonban látnunk kell, hogy a HUMINT megmarad. Mi lehet a szerepe a HUMINT-nak a közeli jövő titkos felderítésének rendszerében? Egy hasonlattal élve az, mint egy minőségi, esetleg kézzel varrott és méretre készített öltönynek, cipőnek a tömeggyártott fast fashion tengerében; vagy mint egy saját kézzel, természetes alapanyagokból, friss összetevőkből összeállított ételnek a gyorséttermek junk foodjával összehasonlítva. Azaz hosszú távú, minőségi, egyénre szabott és egyéni jellegű eszköz, amelyet egy minőségi cél érdekében szükséges és kell használni, alkalmazni.

Álláspontom szerint egy nemzet titkosszolgálati közössége a jövőben is kell hogy rendelkezzen azzal a képességgel, hogy rövid távon is meg tudjon szólítani embereket, és azokat együttműködésre, titkos együttműködésre tudja bírni.

[9] Lásd Laufer Balázs –Takács Gergely: A HUMINT vége? *Arc és Álarc,* 2. (2018), 1–2. 175–185.

Még inkább szükséges, hogy hosszú távú céljait meghatározva ki tudja választani és kellő titoktartással hosszú távon is tudja alkalmazni az azokat előmozdítani képes személyeket, Ez tehát nagyfokú tudatosságot és a célok viszonylagos állandóságát tételezi fel. Nyilvánvaló, hogy ez csak a legfontosabb célokra lehet igaz. A hosszú távú gondolkodás a legenda kiépítését, a kapcsolat és a kapcsolattartó gondos felkészítését is megköveteli.

Szükségesnek látszik a HUMINT sajátos jellegéhez igazodó szervezeti és irányítási modellek – kulcsszavak: meghatalmazás alapú vezetés, autonómia, bizalom, sikerorientáltság – alkalmazása is. Nyilvánvaló, hogy a leírtakból egy elsősorban a HUMINT-ra specializálódott, kompetitív előnyeit a HUMINT terén megtaláló és növelő, azokat a titkosszolgálati, tágabb értelemben rendészeti közösség, ezen túlmenően az állam és a nemzet biztonsága érdekében hasznosító és megőrző szakosodott szervezet képe rajzolódik ki. Erre nemzetközi példaként a CIA-t említhetjük. Egy ilyen szervezet motivált lesz az előző fejezetben említett kihívásokra adandó adekvát válaszlépések kidolgozásában is.

A humán felderítő szakemberek biztonságuk megőrzése érdekében lemondhatnak a technikai adatrögzítés, adattovábbítás eszközeiről, vagy tudatosan eltekinthetnek azok használatától. Készíthetnek kézzel papírra jegyzeteket, telefon és webchat helyett találkozhatnak, beszélgethetnek személyesen, fizethetnek készpénzzel. Az effajta hagyományőrzés hozzájárulhat egy szolgálat elit jellegéhez, és vonzerőt gyakorolhat a munkatársak és a titkos együttműködők vonatkozásában egyaránt. Ez távolról sem jelenti azt, hogy a jövő titkosszolgálatai nem szükséges módon kell hogy élen járjanak majd a technika alkalmazásában.

Úgy tűnik, hogy a HUMINT és a technikai adatszerzés előnyeit elsősorban a kitermelt információk összesítése, értékelése, elemzése során lehet és kell egyesíteni. Ugyanebben a fázisban lehetséges a hátrányok kiküszöbölése is. Ez azonban már az értékelés–elemzés–tájékoztatás, az esetleges fúziós központok témaköre.

Zárógondolatként érdemes egyértelművé tenni, hogy a HUMINT jövőjének legfőbb záloga az a körülmény, miszerint egy titkosszolgálat, egy rendészeti szerv emberekkel szemben jár el, emberek gondolatait, szándékait, terveit, tetteit igyekszik megismerni és felderíteni. Mivel az ember társas lény, és evolúciójának lassúsága folytán még belátható ideig az is marad, ezért a megismerés komplex rendszerében az embert, azaz a HUMINT eszköztárát meg kell őrizni, attól hiba lenne eltekinteni. Ez a körülmény, ez a megközelítés különösen igaz lehet azokra a szervezetekre, amelyek nem rendelkeznek a technikai adatszerzés kiépítéséhez, fenntartásához és fejlesztéséhez szükséges anyagi és szellemi erőforrásokkal.

Értékelés, elemzés és tájékoztatás a 21. században

Regényi Kund Miklós

Értékelés, elemzés és tájékoztatás a 21. század elején

Nem lehet elégszer hangsúlyozni, hogy a rövid 20. század végének, a hidegháború befejeztének két nagy jóslata közül – tudniillik, hogy a történelem vége vagy a civilizációk összecsapása következik be – az utóbbi látszik valóra válni.[1] Kézenfekvő és igaz a következtetés, hogy világunk, ha emberek milliárdjainak képes is kényelmes és élhető otthont biztosítani, rendkívül összetetté vált. A jólét és szabadság talán csak egy rövid átmenet a mélyben rejlő ellentmondások felszínre kerülése előtt, amelyet Huntington a civilizációk összecsapásaként írt le. Nem kétséges, hogy a rejtett és emberi eredetű kihívások azonosítására hivatott nemzetbiztonsági szolgálatok számára ez folyamatos megmérettetést és alkalmazkodást jelent. Nyilvánvaló az is, hogy a megszerzett ismeretek összegzése, az információszerzés orientálása és mindenekelőtt a döntéshozók adekvát és hiteles, megalapozott tájékoztatása fontosabbak, mint valaha (noha mindig is fontosak voltak).

Ebben a fejezetben azt is be fogjuk mutatni, hogy ez az a terület, ahol a legnagyobb változások következtek be. Hasonlattal élve, egy titkos kapcsolattal lebonyolított találkozó 1917-ben roppant hasonló volt ahhoz, mint ahogy az lezajlott 2017-ben. Ha bárki képes lenne beülni egy időgépbe, és tanúja lehetne egy ilyen beszélgetésnek, a szakember azonnal felismerné, miről van szó. Mindez nem mondható el az értékelés, elemzés és tájékoztatás rendszeréről.

Annak érdekében, hogy a változásokat bemutassuk, érdemes megismerkednünk az alapvető fogalmakkal.[2] Az értékelés, elemzés és tájékoztatás folyamatát gyakran összevontan emlegetjük, ami helyes is, hiszen egymásra épülő folyamatról van szó. A jobb megértés érdekében azonban most szigeteljük el, válaszszuk szét az egyes elemeket. Az értékelés nem más, mint egy olyan gondolati folyamat, amelynek során meghatározzuk, hogy a keletkezett információ mire

[1] Vö. Francis Fukuyama: *A történelem vége és az utolsó ember.* Budapest, Európa, 2014; Samuel P. Huntington: *A civilizációk összecsapása és a világrend átalakulása*. Budapest, Európa, 2019.

[2] Lásd Lowenthal (2017): i. m.; Vida Csaba: A hírszerző elemző-értékelő munka alapjai. *Felderítő Szemle,* 12. (2013), 3. 90–99.

https://doi.org/10.36250/00904_09

jó, azaz a szervezet feladatrendszerének mely elemét mozdítja elő, ha egyáltalán; és mennyire jó, azaz mennyire hiteles és mennyire ellenőrzött.

A gyakorlatban a keletkezett információt négy tengely mentén tudjuk elhelyezni. Az első a hírigény, azaz a keletkezett információ illeszthető-e a hírigény bármelyik eleméhez. A második egy-egy konkrét szakmai munkafolyamat – ez az elhárítás munkájában általában egy-egy ügyfeldolgozás előrevitele – szempontját jelenti, azaz a keletkezett információ mennyire igazolja vagy cáfolja az alapfeltételezést. Két másik tengely is létezik. Az egyik a titkos felderítés feltételrendszerének bővítése. Egy egyszerű példa: amennyiben a szociális médián egy személy kiposztolja, hogy két hétig külföldön lesz szabadságon, az első pillantásra nem segíti szakmai munkánkat, valójában azonban nagyon is, hiszen ezen időszak alatt olyan műveleti intézkedéseket tehetünk, amelyek felderítésünket jobb helyzetbe hozhatják. A negyedik tengely is jelentős, hiszen ide az információknak azt a részét soroljuk, amelyek szervezetünk számára nem relevánsak, azonban együttműködő szervezetek számára jelentősek lehetnek, például egy bűncselekmény vagy bűnszervezet meglétére utalnak, azt bizonyítják. Ebben az esetben az információkat természetesen az együttműködő szervezetek részére át kell adni.

A következő munkafolyamat, az elemzés részletesebb taglalást kap majd a fejezet következő részében. Itt azt jegyezzük meg, hogy az elemzés a rejtett összefüggések feltárásának, a párhuzamosságok azonosításának és kiküszöbölésének, az információs összkép megalkotásának folyamata. Ez az a szint, amely orientálja a titkos felderítést; továbbá ez az a szint, ahol megvalósul a titkos felderítés új ismereteinek figyelembevételével a műveleti helyzetkép módosítása, adaptálása a valósághoz.

A tájékoztatás pedig, mint neve is jól mutatja, azt a munkafolyamatot jelenti, amikor a döntéshozók releváns, hiteles és naprakész ismereteket kapnak, amelyek alapján meghozhatják azokat a stratégiai döntéseket, amelyek az ország, de legalábbis a nemzetbiztonsági szféra szempontjából kiemelkedő jelentőségűek. A tájékoztatás történhet megrendelésre, ez a hírszerző cikluskénti elhíresült szakmai modellnek felelne meg, de természetesen elvárás, hogy egy szervezet felhívja a döntéshozók figyelmét azokra folyamatokra, jelenségekre, amelyek rejtve maradhattak, a felszínen nem jelentek meg. Nyilvánvaló, hogy a tájékoztatásnak a javasolt intézkedésekre, azok előnyös és hátrányos hatásaira is ki kell terjednie.

Az elemzés új arca

Mint már utaltunk rá, az elemzés az adatfeldolgozási folyamat legizgalmasabb része. Itt képződik a nemzetbiztonsági szervezetrendszer által az információkhoz hozzáadott értékek jó része. Ez az a munkafázis, amely a 21. század elején a legtöbb változást mutatja a korábbi évekhez képest. Egy mozzanatként meg kell említeni, hogy az információkat azonosítható, rendezhető és újrarendezhető módon kell tárolni. Ehhez az adatokra vonatkozó adatok, azaz metaadatok szükségesek. Metaadatokat mi magunk is képezhetünk, de értelemszerűen ilyenek az információ helyére, forrására, a benne szereplő személyekre, eszközökre, gépjárművekre stb. való utalások is. Az adatok tárolása már régebb óta elektronikus formában történik, ez természetesen felveti az adatok hitelességének kérdését. Az alapadatoknak nem módosítható formában kell az elemzők rendelkezésére állnia.

Ennél is izgalmasabb kérdés, hogy a korábbi évtizedekre jellemző strukturált adattáraknak – amelyek előre meghatározott (és folyamatosan bővített) szempontrendszer alapján valósították meg az adatok elhelyezését és aztán a tárolt adatok lekérdezését –, úgy tűnik, bealkonyul, hiszen a mesterségesintelligencia-alapú[3] keresőmotorok az előzetes szempontok meghatározását talán feleslegessé teszik. Erre majd a későbbiekben visszatérünk. Ugyancsak kihívás, hogy eddig az információk döntően szövegalapon álltak az elemzők rendelkezésére. Teljesen nyilvánvaló, hogy ez a helyzet gyorsan változik. Az információk túlnyomó többsége ma már kép- és hangalapon jelenik meg. Ezek gyors tárolása, visszakeresése különösen fontossá válik, figyelembe véve az elemzők új, digitális bennszülöttek közé sorolható generációjának mind nagyobb ütemű térnyerését is.

Újabb gyakorlati szempontú dilemma a belső információáramlás kérdése. Jelenleg zajlik az a folyamat, amikor is a jelentésből kivonat, a kivonatból újabb kivonat készítésének, azaz az alapinformációk kézi munkával történő fáradságos, időrabló és nem utolsósorban lélekölő folyamatát egyre inkább felváltja a rögzített információhoz való különböző mértékű és szintű hozzárendelések automatikus biztosítása, nyilván előre meghatározott szempontrendszerek és keresőszavak alapján. Amennyiben erre az adatbiztonság szempontjából szükség van, a hozzárendelés helyett küldés, azaz fizikailag más tárhelyen való elhelyezés, áthelyezés is elképzelhető.

[3] A fogalomról jogi megközelítésű, jó leírást ad Eszteri Dániel: A mesterséges intelligencia fejlesztésének és üzemeltetésének egyes felelősségi kérdései. *Infokommunikáció és Jog,* 12. (2015), 62–63. 45–57.

Az elemző munka talán legfontosabb dilemmája az információbiztonság és az információmegosztás dilemmája. Az információbiztonság alapvetően az információszerzés klasszikus gyakorlatának felel meg, eszerint az információkból mindenki csak annyit ismerhet meg – de annyit mindenképpen meg kell ismernie –, ami munkájának elvégzéséhez szükséges. Ez az alapelv jó szolgálatot tett a titkosszolgálatok fejlődésének elmúlt évszázadaiban, és ma is jó szolgálatot tesz a titkos felderítés, a szorosabban vett információszerzés fázisaiban. Ezzel szemben áll az információ megosztásának a szempontja, amely arra utal, hogy a rejtett összefüggések feltárása és a műveleti helyzetkép részleteinek megalkotása érdekében az egyes elemzőnek vagy az elemző csoportnak az információk minél szélesebb, lehetőleg teljes körét célszerű megismerni, hiszen összetett világunkban gyors és hatékony helyzetfelismerés csak így lehetséges. Jól látható, hogy a két szempont meglehetősen ellentétes.

Egy nemzetbiztonsági szolgálat munkájában a biztonság, az információbiztonság szempontjait sohasem hanyagolhatjuk el. Hogyan lehet feloldani az ellentmondást? Nyilván kiemelkedő fontosságú, hogy kimutatható legyen, miszerint egy-egy adathoz ki, mikor és miért fért hozzá. Természetes, hogy azt is ki kell tudni mutatni, hogy egy összesítés, egy összefoglaló elkészítéséhez milyen alapinformációkat használtak fel, hasonlóan egy tudományos munka lábjegyzeteihez, még hogyha ezeket a lábjegyzeteket nem is jelenítjük meg feltétlenül. Nyilvánvaló az is, hogy műveleti erők és eszközök komplex alkalmazásával egyfajta védelmet kell megvalósítani az elemző munkaterülete, elektronikus eszközei és személye körül, amely az egyszerű rezsimszabályoktól a számítógépes biztonság elemein keresztül a humán biztonságra is kiterjed. Mindezen szabályok csak akkor tölthetik be céljukat, ha azokra az állományt felkészítik, azok rendezőelveit bemutatják, és ezáltal egyfajta belső azonosulást teremtenek az elemzők és a munkájukat felszínen bonyolultabbá tevő – valójában azonban egyáltalán lehetségessé tevő – rezsimszabályok között.

Minőségi változást eredményezett az elemző folyamatokban a rendelkezésre álló adatok mennyiségének robbanásszerű növekedése. Ma már az elemi adatok számát nem százezrekben, hanem milliókban mérik. Ez a változás további nagyon fontos változásokat indukál, ami egyszerre jelent esélyt és kihívást a nemzetbiztonsági elemző munka számára. Esélyként kell megjeleníteni a platformfúziót. Itt ez alatt azt értjük, hogy különböző rendszerekből származó adatok egyszerre, azonos platformon állnak az elemző vagy egyszerűbb adatok esetében az információszerzésben részt vevő szakember rendelkezésére. Egyszerű példa: ha az igazoltatás során az intézkedés alá vont személyről a szociális médiában

meglévő ismeretek is megjelenítődnek, akkor az orientálhatja az intézkedést, és jelentősen előremozdítja az adekvát válaszlépések megtételét.

Következő nagy probléma és kihívás, hogy nagy mennyiségű adatokat hogyan lehet megtalálni, visszakeresni és a közöttük levő kapcsolatokat azonosítani, ábrázolni, esetleg értelmezni. Nyilvánvaló, hogy ehhez számítógépek kellenek, nyilvánvaló, hogy ehhez olyan öntanuló, azaz magukat továbbfejleszteni képes számítógépes programok kellenek, amelyeket elterjedt kifejezéssel mesterséges intelligenciának nevezünk. Ez jelentős mértékben átformálja az értékelő-elemző munkát, hiszen sok esetben, sőt a leggyakrabban nem az információval magával kell dolgozni, hanem a számítógépet kell irányítani. A megérzés, az intuíció, a feladattal való személyes azonosulás e körülmények között is, úgy vélem, megőrzendő érték.

A számítógépek, számítógépes programok térhódítása az elemzőtől új képességeket követel meg. Már nemcsak egy adott témakörrel, sőt nemcsak a titkos felderítés, illetve a szervezet munkafolyamataival és feladatrendszerével kell tisztában lennie, hanem a számítógépes adatfeldolgozáshoz is értenie kell. Óriási kihívás ilyen széles körben képzett embereket megtalálni, vagy kinevelni, kiképezni. Nyilvánvaló, hogy mind a két utat járni kell, azaz megfelelő alapképzettségek birtokában levő szakembereket be kell vonzani a szolgálatokhoz, és ezzel párhuzamosan a meglevő állományt képezni kell a technikai rendszerek minél magasabb szinten való alkalmazása érdekében.

Érdekes jelenség, hogy a számítástechnika folyamatosan terjedő saját belső világa egyre inkább olyan embereket teremt, akik annyira specializálódtak, hogy a számítástechnika világában szinte mindent képesek megoldani, azonban a számítástechnika világán kívül nem mozognak annyira magabiztosan. Várható, hogy egy új szakembertípus fog megjelenni: egy olyan szakember, aki egyfajta kapcsolódási pontként viselkedik a számítástechnika világa és a nemzetbiztonsági kihívások világa között; képes a problémákat úgy megérteni és megfogalmazni, hogy az a másik oldal számára is érthető és kezelhető legyen.

A következő jelenség, hogy nagy mennyiségű adat elemzésével újfajta minőség jön létre, amely nem feltétlenül a klasszikus értelemben vett értékelő-elemző munka jellemzőit hordozza, sokkal inkább egyfajta információszerzésként – azaz későbbi elemzési folyamatok tárgyává váló alapinformációk keletkezéseként – írható le.[4] Ez a szervezet nézőpontjából azt jelenti, hogy

[4] Stratégiai megközelítések alapjává, rendezőelvévé teszi a jelenséget Alfred Rolington: *A hírszerzés a 21. században – a mozaikmódszer*. Budapest, Antall József Tudásközpont, 2015.

az elemzés és a titkos felderítés, műveleti adatszerzés fázisai összemosódnak. Egy példa: közterületi képrögzítő kamerák adatainak elemzésével egy célszemély mozgásmintája és kapcsolatrendszere megalkotható, azaz adatelemzéssel olyan típusú ismeret birtokába juthatunk, amely klasszikus munkamódszer szerint műveleti adatszerzést folytató szerv, jelesül a figyelés munkájának eredményeképpen jön létre. (Másik ilyen terület a nyílt forrású információk elemzése lehet.)

A gépi tanulás (*„machine learning”,* ML) működésének sajátossága, hogy öntanuló képességét csak minél szélesebb körű használattal, illetve a próba és bukás *(„trial and error”)* elvének minél szélesebb körű alkalmazásával tudja kamatoztatni, hasonlóképpen, mint ahogy megalkotója, az ember is tanul. Ebből az a kézenfekvő következtetés adódik, hogy mesterségesintelligencia-alapú programokat nemcsak minél szélesebb körben kell használni, hanem úgynevezett tanuló adatokat, azaz konkrét feladathoz nem köthető, de szakmailag releváns adatokat is alá kell vetni a rendszer által történő feldolgozásnak a majdani minél hatékonyabb használat érdekében. Ennek nemcsak a technikai feltételeit kell megteremteni, hanem a jogi feltételeit is, hiszen a készletező típusú adatgyűjtés, illetve az adatok hosszabb időn keresztül való tárolása sok esetben jogszabályi korlátokba ütközik.

Már utaltunk rá, hogy a mesterséges intelligencia fejlődése adott esetben feleslegessé teheti a strukturált adattárak fenntartását és továbbfejlesztését. Másképp fogalmazva, az adatok rendszerezése, adattárba rögzítése – történjen ez akár kézi, akár gépi munkával – feleslegessé válhat, az erre fordított munkaerő, munkaidő és anyagi források másutt jobban hasznosulhatnak. Ez a lehetőség kétségtelenül roppant csábító. Az előnyök mellett azonban a strukturált adattárak megszüntetésének hátrányai is vannak. Egy rendezetlen adathalmazból mesterséges intelligenciával történt adatkinyerés eredménye mindig nagyobb találati mezőt eredményez, gondoljunk egyszerűen csak egy Google keresőmotor által végzett lekérdezés értékelésének, felhasználásának dilemmájára. Ez a munkaszervezésre vonatkoztatva azt jelenti, hogy az a munka, amelyet látszólag megtakarítottunk az adatok rendszerezésének során, az nem tűnik el, csak átalakul; azt az adatok kinyerése, a kinyert információhalmaz értelmezése során kell elvégeznünk. Azaz a megtakarítás rendszerszinten nem, csak egyes alrendszerek vonatkozásában jelentkezik.

A tájékoztatás új arca

Miután az elemzés problémáit áttekintettük, érdemes pár gondolatot szánni a tájékoztatás esetleges dilemmáira is. A 2001-es terrortámadások nagyon kiterjedt rendszerszintű vizsgálatokhoz vezettek az amerikai nemzetbiztonsági közösségen belül. Az egyik nagy tanulság az volt, hogy a rendszerben egymástól elkülönülten sok olyan információ megvolt, amelyek összegezve elvezethettek volna a terrortámadások meghiúsítására is alkalmas nyílt intézkedések meghozatalához. Ezek az információk azonban nem találkoztak, ez pedig egyebek között arra a tényre vezethető vissza, hogy a rendvédelmi és nemzetbiztonsági szolgálatok hierarchikus működésű, erősen strukturált rendszerek, ahol a tájékoztatás bejáratott úton, az illetékesség és hatáskör szabályainak betartásával zajlik. Ez önmagában is egyfajta gátlást jelent az adatszerzők és elemzők számára, olyan értelemben, hogy késlelteti az elsődleges következtetések megfogalmazását és szolgálati úton való felterjesztését. Ez emberileg érthető, hiszen ki akarná elsőre bolondosnak tűnő meglátásaival, sejtéseivel, az addigi gondolkodásmódba nem vagy alig illeszthető eszmefuttatásaival felhívni magára a vezetés figyelmét. Ennek eredményeképpen azonban az információk nem jutottak el a döntéshozókhoz, és nem találkozhattak, hogy alapos elemzés tárgyát képezhették volna. Meg kell teremteni tehát annak feltételeit, hogy a tájékoztatás egyfajta „információs felhőben" (azaz kevéssé hierarchizáltan, szélesebb, előre esetleg nem is teljesen meghatározható személyi kör számára) történjen.

Logikailag hasonló, de szervezetileg nagyon különbözik az információs fúziós központok fogalma. Ez olyan szervezetekre utal, amelyek nem egy, hanem sok, lehetőleg az összes rendvédelmi és nemzetbiztonsági szerv információinak a birtokában vannak, és így valamennyi információ követésével, az esetleges ellentmondások kiszűrésével képesek a döntéshozók hatékony, időt és energiát egyaránt kímélő, úgynevezett egycsatornás tájékoztatására. Nyilván egy ilyen szervezetnek meg kell találnia helyét, szerepét a nemzetbiztonsági közösség régebb óta létező tagjaival, tagjai között. Hogy ez mennyire nem egyszerű folyamat, azt jól mutatja az amerikai OSS és a CIA fejlődéstörténete.[5]

Átalakulóban van a tájékoztatást hordozó médium is. Napjainkban a tájékoztató munka túlnyomórészt papíralapú, szöveges, képekkel és térképekkel kiegészített jelentések, tájékoztatók formájában valósul meg. Emellett felértékelődik a közvetlen szóbeli tájékoztatás, idegen szóval a *briefing* műfaja,

[5] Elődszervezete az Office of Strategic Services – Stratégiai Szolgálatok Hivatala.

amelynek során a vezető vagy a szakértő szóban tájékoztatja a megrendelőt a rendelkezésre álló ismeretekről, természetesen általában vetített képes ábrákkal kiegészítve. Ez a műfaj megerősíti, elmélyíti az információt megrendelők, azaz a döntéshozók, és az információt kitermelő nemzetbiztonsági szervezetek közötti kölcsönös bizalmat. A felek kölcsönösen megismerik egymás gondolkodásmódját, világképét. Ugyancsak nagy előny, hogy az esetleges ellentmondások, homályos részletek tisztázására azonnal mód van. Ugyancsak azonnal mód van a tájékoztatóhoz kapcsolódóan feladatok, intézkedések megfogalmazására, kiadására is. Nyilvánvaló, hogy ezeket írásban kell rögzíteni.

A spektrum másik végén is változások készülődnek. Figyelembe kell venni, hogy már döntéshozó pozícióban van az a generáció, amely ismereteit alapvetően szociális médiából, internetes csatornákon keresztül, mobil eszközök révén szerzi be, és kézenfekvő, hogy ehhez a médiumhoz döntéshozóként is ragaszkodik. A probléma technikai és biztonsági vonatkozásaira most nem térünk ki, hiszen ezek önálló tanulmányt is megtöltenének. A tájékoztatómunka szempontjából ez azt jelenti, hogy az információt nem szöveg, hanem kép és/vagy infografika formájában kell rögzíteni. Ez ismét olyan kérdéseket vet fel, mint amelyeket a számítástechnika általános térnyerése kapcsán már említettünk. Egyértelmű, hogy új képességekkel kell gazdagodni az értékelő-elemző szakma gyakorlóinak.

Természetesen a szociális médiumokon nevelkedett megrendelők az információmegosztás dilemmájához is másként viszonyulnak, hiszen a megosztás a Facebook és klónjai világában egy érték. Úgy vélem, ehelyütt komoly edukációs folyamatra van szükség, amelynek középpontjában a felhasználó felelőssége kell hogy álljon, azaz annak tudatos vállalása, hogy a részére juttatott – és egyébként rendkívül izgalmas, tehát a megosztást szinte kiprovokáló – információ birtoklása őt arra kötelezi, hogy ettől a megosztástól tekintsen el a nagyobb jó, az ország, a haza, esetleg a szövetségi rendszer biztonsága, versenyelőnyének megőrzése érdekében. Hogy ez a probléma valós, arra a közelmúlt botrányai (például hivatali levelezés magánpostafiókból való folytatása) rávilágítottak.[6]

Zárógondolatként egy kérdést kell megfogalmazni: ha megjelennek és elterjednek a széles körű – igényszinten teljes körű – ismereteket összpontosítottan hordozó, az ismereteket egymással szabadon összekapcsoló és ezáltal új értéket

[6] A jelenség súlyára rámutat, hogy az Amerikai Egyesült Államok elnöke – a kézirat írásakor Donald Trump – aki előszeretettel használja érdemi tájékoztatásra Twitter-fiókját, 77,7 millió követővel rendelkezik, és a fogalomra a Google keresőmotor több mint 1 millió találatot adott 2020. április 20-án.

teremtő központok, úgy ez a jelenség vajon milyen hatást gyakorol majd az úgynevezett ügygazdák szerepére? Azaz hol lesz a helyük azoknak a szakembereknek, akik egy-egy ügy feldolgozásában valamennyi részismeret birtokában tervezik-szervezik és hajtják végre a műveleti felderítés soron következő lépéseit? Vajon nem áll fenn annak veszélye, hogy az adatszerzésben közvetlenül részt vevők egyre kisebb mértékben fogják megismerni az adatszerzés tulajdonképpeni valós célját, és egyre inkább a végrehajtás tágabb értelemben vett technikai megvalósítására törekszenek majd? Egyáltalán, kell-e ettől félnünk, vagy inkább üdvözölnünk és gyorsítanunk kell a folyamatot?

A kérdésekre a választ jelenleg még nem tudjuk megadni. A HUMINT-ról írt fejezetben azonban megfogalmaztunk egy olyan hipotézist, hogy az autonóm módon cselekedni képes és kész személyeknek helye van a jelen és a jövő titkos felderítésének rendszerében. Úgy vélem, ha másutt nem is, az emberi erőforrásokból végzett információszerzés során a mai értelemben vett ügygazdák szerepe megmarad. Nyilván az ő elemző támogatásuk újabb előrelépést jelenthet a mind bonyolultabb világban történő, mind hatékonyabb munkavégzés szempontjából, és erre az előrelépésre szükség is van.

A KIHÍVÁSOKRA ADOTT VÁLASZOK SAJÁTOS TERÜLETEI

Vákát

A nemzetbiztonság fejlődő egyetemi kapcsolatai

Dobák Imre

A nemzetbiztonsági szolgálatok esetében különösen igaznak tekinthető, hogy új, naprakész ismeretek szükségesek feladataik ellátásához, az információk pontos értelmezéséhez, eszközeik, módszereik fejlesztéséhez. A szükséges ismeretek többek között a természettudományok, a társadalomtudományok, a műszaki tudományok vagy akár a bölcsészettudományok tudományterületein jelennek meg. Gondoljunk a már ismertetett, nemzetközi színtereken zajló biztonságpolitikai folyamatok vagy akár az infokommunikáció világában zajló rendkívül gyors fejlődés „megértésének" és „követésének" szükségességére, és az ezek mentén megjelenő tudományok sokoldalúságára.

Központi együttműködési szerep hárul így az egyetemi és tudományos környezetre, amellyel a „titkosszolgálatok" a történelemben visszatekintve is hagyományosan sokrétű kapcsolatokat folytattak. Ezek előzményei a hidegháború időszakáig visszatekintve mind a nyugati, mind a keleti blokk országaiban megtalálhatók, de napjainkban is személyi utánpótlásuk biztosítása, képzése, vagy akár az új ismeretek megszerzése érdekében általánosan fordulnak a civil egyetemi és kutatói közeg felé. Az alábbiakban a nemzetközi színtérre kitekintve – túlnyomórészt az amerikai példát ismertetve – ennek a kapcsolatrendszernek a sajátosságait és jellemzőit mutatjuk be.

Az egyetemi együttműködési felületek

Az egyetemek és nemzetbiztonsági szolgálatok közötti viszonyt tekintve a nemzetközi szakirodalmak alapján az alábbi fő együttműködési irányok, felületek láthatók:

– *képzési együttműködések:* Az egyetemek irányába hagyományos területként jelenik meg a nemzetbiztonsági ágazat munkaerő-utánpótlása biztosításának és az állomány képzésének igénye. Idesorolhatjuk a szolgálatok számára is nélkülözhetetlen civil (például jogi, műszaki, informatikai), valamint az egyre szélesebb körben értelmezhető (nemzet)biztonságot szolgáló képzéseket (például önálló nemzetbiztonsági) szakokat, akár szakosított intézményi formákat;

https://doi.org/10.36250/00904_10

- *kutatási együttműködések:* Ilyenek a kölcsönös előnyöket biztosító tudományos kutatások és fejlesztési együttműködések, amelyek egy része egyéb állami, illetve gazdasági szereplőkével azonos formában valósul meg, más részüknél azonban már szerepet kapnak a tudományos kutatások nemzetbiztonsági szempontjai (például nemzetbiztonsági védelem) is;
- *biztonságtudatosítás területe:* Egyre szélesebb körben látható a fiatal generációkat is veszélyeztető terrorizmus elleni küzdelem feladata, a radikalizáció megakadályozása, de idesorolhatók a kiberbiztonság biztonságtudatosító irányai is. A nemzetközi színtérre kitekintve az elmúlt években számos felsőoktatási program, gyakorlati képzési elem, kutatás jött létre a témakörökben;
- *külföldi hallgatók jelenlétéhez kapcsolódó együttműködés:* Sajátos területként értelmezhetők az egyetemeken tanuló nagyszámú külföldi hallgató jelenlétéhez kapcsolódó (nemzet)biztonsági szempontok. Amíg ezek alapját gyakran diplomáciai, illetve gazdasági jellegű együttműködések és partnerségi lehetőségek teremtik meg, addig egyfajta melléktermékként jelen lehetnek a tudományos eredmények kiáramlásától való félelmek (ipari kémkedés veszélye), vagy akár a nemzetközi hallgatói migráció összetett folyamatai.

A fentiek az egyik oldalról (egyetem) a nyílt tudományos rendszerek és gondolkodás, a másik oldalról (nemzetbiztonság) a szinte minden országban védett működést szükségessé tevő zártabb, biztonsági gondolkodás találkozását mutatják. A témakör áttekintését nehezíti, hogy a nemzetbiztonsági szféra érthető módon kevés információt oszt meg az állományát, képességét, vagy akár a fejlesztési irányait érintő kérdésekben. Igaz, az elmúlt években ezen a téren is változásokat láthattunk, amelyek mögött vagy egyes biztonsági szempontok felerősödése (például terrorizmus jelensége), vagy éppen a nyilvánosságot kapott titkosszolgálati botrányok hatásai álltak.

Képzési kapcsolatok

A nemzetbiztonsági szolgálatok és az egyetemek közötti kapcsolati-intézményi modell fő kereteit keresve Liam Gearon tanulmányában olvasható az a hármas modell[1] *(covert, overt, covert-overt),* amely segíthet a nemzetbiztonsági

[1] Liam Gearon: The counter-terrorist campus: Securitisation theory and university securitisation – Three Models. *Transformation in Higher Education,* 2. (2017), a13. 2519–5638.

szolgálatok egyetemekkel való (esetünkben főként képzési kérdésekre irányuló) kapcsolatát vizsgálni.

- A *fedett (covert)* modell a szerző megfogalmazását értelmezve a II. világháború és a hidegháború időszakának terméke, amely a hírszerzés professzionalizálásának időszaka. Idesorolhatók a hírszerzők felkészítésére szakosodott egyetemi szintű oktatási és képzési központok, felölelve a biztonság területeivel és az információgyűjtéssel kapcsolatos elemeket.
- A *nyílt (overt)* modell a felsőoktatási képzés vagy akár a kutatás nagyobb elszámoltathatóságot biztosító nyitott formája, amely rendkívül széles körű együttműködési lehetőségeket jelenthet.
- A *fedett-nyílt (covert-overt)* modellhez sorolja a szerző például a „titokban kémkedéssel foglalkozó egyetemi akadémikusokat, miközben azok teljes mértékben nyitott tudományos feladatokat látnak el".[2]

Leginkább a nyílt modellhez tartozó elemek vizsgálhatók, ahol az egyetemekkel megvalósuló tudományos és képzési kapcsolatokat számos projekt, nyíltan közzétett partnerségi megállapodás, egyetemeken kiírt ösztöndíjak és egyéb pályázati formák is jeleznek. Itt említhetők meg a humán erőforrás biztosítására irányuló képzési célú, akkreditált nyílt felsőoktatási programok, gyakorlati-gyakornoki képzési együttműködések és egyéb közös pályázati formák.

Az egyetemi szféra és a védelmi/nemzetbiztonsági szféra átfogó kapcsolatrendszere vizsgálatának nehézségét jelzi, hogy teljességgel nem nyilvános annak száma és pontos szerkezete. Példaként az Egyesült Államok említhető, ahol az amerikai hírszerzés (CIA) már a 20. század közepén titkos formában jelen volt az egyetemeken, majd az 1960-as évek végén beszivárgott az amerikai Nemzeti Diákszövetségbe is, elősegítve ezzel toborzási tevékenységét és hidegháborús ideológiájának támogatását az egyetemi campusokon. Igaz, válaszként Lyndon Johnson elnök megtiltotta a CIA tevékenységét a felsőoktatásban,[3] de az 1980-as évektől a szervezet visszatért az egyetemek campusaira.

Napjaink viszonyait tekintve nehéz megbecsülni, hogy pontosan hány együttműködés, program létezik,[4] azonban ezek látható módon kiterjednek többek

[2] Gearon (2017): i. m.

[3] Tony Vellela: *New Voices. Student Political Activism in the '80s and '90s.* Boston, South End Press, 1988. 60.

[4] Scott Firsing: The Growing Link between Intelligence Communities and Academia. *The Conversation,* 2015. szeptember 30.

között a nemzetbiztonsági és hírszerzési jellegű új egyetemi képzésekre. Egy 2015-ben megjelent amerikai tanulmány szerint az Egyesült Államokban több mint 250 intézmény kínált diplomákat, tanúsítványokat a tágan értelmezett belbiztonság területén, ahol a képzések több területet is felöleltek (például kiberbiztonság, katonai hírszerzés, rendvédelem). Az állami finanszírozás mellett jelen voltak a magánfinanszírozási elemek, valamint a 2001 utáni megváltozott környezethez és kihívásokhoz igazodva bizonyos területek képzését a biztonsági szféra ki is szervezte, illetve teret nyertek az online programok.[5] A tanulmány „90 ezer személy hírszerző közösséghez (IC) való kapcsolata" alapján állított fel rangsort[6] az Egyesült Államok 100, a védelmi-nemzetbiztonsági szférához leginkább közel álló felsőoktatási intézményéről. Mint megfogalmazzák, a

> „VICE News listáján a felsőoktatási intézmények 4 kategóriája dominál, így azok az iskolák, ahol a hallgatók alapvetően online diplomákat kapnak, amelyek érintettek a védelmi, hírszerzési és biztonsági kutatás-fejlesztésekben, amelyek Washington, D. C.-ben vannak; valamint azok, amelyek a belbiztonságra újonnan helyezik a hangsúlyt".[7]

Érdekesség, hogy „az adathalmazt jelentő 90 000 személy közül kevesebb mint 400 rendelkezett diplomával a nemzetbiztonsági tanulmányokban, kevesebb mint 5%-ának van közép- vagy felsőfokú végzettsége politikai tudományi területen, és még alacsonyabb volt a nemzetközi kapcsolatok aránya".[8]

Egyetemi kutatási kapcsolatok

Már a hidegháború szemben álló feleire jellemző volt az egyetemi tudományos kapcsolatok felhasználása, a biztonság területeihez kapcsolódó kutatóintézeti környezet kialakítása. A különböző fejlesztéseknél azonban törekedtek a nemzeti, illetve szövetségi szinten elért eredmények, megoldások

[5] Firsing (2015): i. m.

[6] A rangsorolás kialakításánál figyelembe vették, hogy a hírszerző közösségben (IC) hány embernek volt diplomája, igazolása az egyes iskolákból, majd 51 további tényező alkalmazásával kiigazították. William M. Arkin – Alexa O'Brien: The Most Militarized Universities in America: *A VICE News,* 2015. november 6.

[7] Arkin–O'Brien (2015): i. m.

[8] Arkin–O'Brien (2015): i. m.

alkalmazására (és megtartására). Általánosságban mind a nyugati, mind a keleti blokk titkosszolgálatainak feladatrendszerében megtalálhatjuk a tudományos és technológiai hírszerzési feladatokat, szervezeti elemeket,[9] továbbá kiemelt szerepet kapott a katonai jellegű kutatás-fejlesztés, amelynek jelentősége a hidegháború végével azonban globálisan csökkent.[10] Ennek az időszaknak a fejlesztési sajátosságaira többek között az alábbiak voltak jellemzők:

- a hidegháborús szembenálláshoz igazodó rendkívüli technológiai verseny;
- a fejlesztések során az állami/védelmi/katonai szempontok meghatározó szerepe;
- az ipari, technológiai, gazdasági jellegű hírszerzés kiemelt jelentősége;
- a nemzeti szinteken rendelkezésre álló K+F képességek és kapacitások felhasználása,
- a nemzeti szintű (állami) „külső" kutatóintézetek, egyetemek nem nyilvános módon történő bevonása;
- a szövetségesi rendszerben partnerként megjelenő országokkal való technikai, technológiai és tudományos együttműködések, tapasztalatcserék.

Az új technológiák, innovatív megoldások kutatása, rendszerbe állítása napjaink nemzetbiztonsági szolgálatainál is jelen van, aminek során a technológiai környezet nyomon követése egyre fontosabbá válik. Ezek sajátos jellemzői között láthatók:

- a zártság, amely a nemzetbiztonsági K+F tevékenységek egész folyamatára kiterjedhet;
- a kutatási tevékenység nemzetbiztonsági jellegű védelme;
- a kutatásokba bekapcsolódó személyek körének korlátozottsága;

[9] A korábbi Szovjetunió szolgálatai esetében bővebben lásd Fredrik Westerlund: *Russian Intelligence Gathering for Domestic R&D – Short Cut or Dead End for Modernisation?* Stockholm, Defence Analysis FOI Memo 3126, 2010. A tudományos és technológiai hírszerzési tevékenységek jelentősége napjainkban sem csökkent. Nemzetközi példák alapján jól látható, hogy számos titkosszolgálat jelenleg is erőfeszítéseket tesz a technológiai és tudományos hírszerzés érdekében. Ezek közé sorolható, amikor egyes országok ipari szegmensük fejlesztése, a hazai K+F elősegítése és gazdasági versenyképességük növelése érdekében alkalmazzák a hírszerzésnek ezt az irányát.

[10] Csiki Tamás – Tálas Péter: A védelmi beszerzés és kutatás-fejlesztés kapcsolata a védelmi tervezés rendszerében – nemzetközi tapasztalatok. *Nemzet és Biztonság,* (2013), 3–4. 107–142.

- a titoktartás és a tudományos nyitottság gyakran egymásnak ellentmondó szempontjai;
- a kutatásokba bekapcsolódni tudó állomány elvándorlása;
- valamint az egyedi finanszírozási formák, illetve a nyílt és zárt rendszerek (projektek) hatékony együttműködését biztosító működtetési modellek kialakítása.

Az európai védelmi kutatás-szervezés kereteinek védelmi szektorban történő vizsgálatát a Csiki–Tálas szerzőpáros végezte el tanulmányában, ahol több modellt is ismertetnek. Egyrészről a szervezetek minisztériumokhoz való közelsége szerint egy „angolszász" és egy „kontinentális" modellt kategorizáltak.[11] A tanulmányukban hivatkozott[12] védelmi kutatás-fejlesztés súlypontja alapján felállított másik felosztásban a katonai modell és az ügynökség-modell mellett megjelenik az állami vállalati/állami egyetemi kutatási modell, valamint az egyetemi modell. Utóbbi két, egyetemekhez kapcsolódó forma esetében a felsőoktatásban egy-egy témakörben rendelkezésre álló kiemelt kutatási képességre építenek.

A kérdést feltéve, hogy a nemzetbiztonsági szféra számára kutatási kérdésekben miért válik egyre fontosabbá az egyetemek szerepe, a válasz több részből tevődhet össze. Egyrészről, az egyetemek a tudományos és technológiai ismeretek legjelentősebb központjai, azok a helyszínek, ahol multidiszciplináris megoldásokat lehet keresni új problémákra.[13] A különböző tudományterületek képviselői koncentráltan vannak jelen, ami a nemzetbiztonság egyre szélesebb értelmezését tekintve hatékonyan biztosíthatja adott témakörökben új eredmények létrehozását, közvetve a szolgálatok munkájának hatékonyságát. Másrészről, az egyetemek lényegében teret adnak a gazdasági-üzleti élet vagy akár az állam (idesorolva a nemzetbiztonsági szféra) működését elősegítő új

[11] A Csiki–Tálas (2013) szerzőpáros írásukban megállapítják, hogy az angolszász modellt a „kutatás-fejlesztés növekvő mértékű kiszervezése jellemzi a civil fejlesztési források bevonásával", míg a kontinentális modell esetében „a védelmi kutatás-szervezés erősen kötődik a védelmi minisztériumokhoz".

[12] Rudolf Urban –Martin Macko: *Place and Role of the Defense Science in the Czech Research and Development System.* Brno, University of Defence, 2011. idézi Csiki–Tálas (2013): i. m.

[13] Gearon (2017): i. m. 192.

tudományos eredmények létrehozásának,[14] innovatív megoldások kidolgozásának. A közegben adottak a nemzetközi szintű, rendkívül gyors, tudományos információcserét biztosító kapcsolatok, valamint jól működnek a hagyományos szervezeti formákon kívüli virtuálisnak tekinthető nemzetközi tudományos közösségek, kutatócsoporti keretek.[15]

A látható kutatási irányokat tekintve napjaink egyik legmeghatározóbb együttműködési iránya a kiberbiztonság témaköre, amelyben az egyén, a gazdasági élet szereplői és az állami szféra érdeke kölcsönösen találkozik, elősegítve ezzel a közös innovatív gondolkodást. Az egyetemi együttműködések számos formája jött létre (kiválósági központok, oktatási kiválósági központok, felsőoktatási képzések és akkreditált képzési helyek vagy akár a vállalati szféra bevonásával járó közös projektek, programok), ahol a partnerek közös céljai a kiberbiztonsági kutatás, innováció vagy akár új „kiberbiztonsági termékek és szolgáltatások" fejlesztése.

Az egyetemek irányába is megmutatkozó (nemzet)biztonsági célzatú K+F együttműködésre széles körben ismert példaként a globális nagyhatalom Amerikai Egyesült Államok 1958-ban létrehozott DARPA szervezete említhető, amely a mindennapi életünket meghatározó új technológiák létrejöttében vált közismertté. A kutatókat, egyetemeket, kutatóközpontokat, PhD-kutatásokat szponzoráló, projekteket indító szervezet története[16] és az élet számos területén napjainkban már nélkülözhetetlen alkalmazásai jól példázzák a védelmi/nemzetbiztonsági struktúrákon belüli innovatív gondolkodás szükségességét. A szervezet jelentősége a fejlett technológiákhoz kapcsolódó új tudományos eredmények létrehozásában, a kutatásokba bevonásra kerülő civil szereplők, intézetek, egyetemek kutatási, innovációs munkáján keresztül meghatározó.[17]

[14] A világ egyetemeinek rangsora alapján (QS rangsor) 2019-ben 19 egyesült államokbeli és nyolc nagy-britanniai egyetem szerepel a legjobb 50 egyetem között. A külön mért kutatási intenzitást tekintve ezek mindegyike nagyon magas értékkel jelölt intézmény. A magán finanszírozású, illetve széles körben nyitva álló állami kategóriákat tekintve közel megegyezik a megoszlásuk. A világ legjobb 50 egyeteme között megjelenő amerikai és brit egyetemek hivatalos weboldalait áttekintve is jól látható, hogy jelen vannak a (nemzet)biztonsági kérdéskörök, képzési felületek, vagy akár a (nemzet)biztonsági célú kutatási kapcsolatok. Lásd Top Universities: www.topuniversities.com/university-rankings/world-university-rankings/2019

[15] Lásd például: www.researchgate.net/, www.academia.edu/

[16] William Regli: Universities in Service to National Security, DARPA's Call to Academia. In *DARPA Defense Advanced Research Projects Agency 1958–2018 (60 years).* Faircount Media Group, 2018. 134–136.

[17] Kadtke–Wharton (2018): i. m.

A megoldás nem egyedülálló, és mint Major Milán kutatásában részletesen ismerteti, 2012-ben Oroszország is létrehozta az amerikai DARPA-hoz hasonló „Perspektivikus Kutatások Alapját", elősegítve ezzel új technológiák fejlesztését (kiemelten a robotika, a pilóta nélküli repülőeszközök [UAV-k], valamint a nanotechnológia területén).[18]

A nemzetbiztonsági szolgálatok K+F együttműködéseit tekintve, visszatérve az amerikai példához, a Nemzetbiztonsági Ügynökség (NSA) emelhető ki, ahol hagyományosan jelentős szerepet játszik a partnerségi forma. A szervezet 2012-ben közzétett, *Access to innovation: NSA's Technology Transfer Program*[19] című tanulmánya alapján az NSA már 1990-ben létrehozta TTP-programját „az NSA feltalálóinak a szövetségileg finanszírozott szellemi tulajdon megosztására és együttműködő kutatások végzésére a magánvállalatokkal, tudományos helyekkel, nonprofit szervezetekkel, más szövetségi ügynökségekkel, valamint állami és helyi önkormányzatokkal".[20] Az NSA programja esetében olyan megoldásokat láthatunk, mint a szabadalmi licencmegállapodások,[21] amelyek lehetővé tehetik a partnerekkel való közös kutatási és fejlesztési tevékenységet,[22] biztosíthatják a tapasztalatok megosztását, képzések nyújtását,[23] valamint technológiatranszfert nyújthatnak[24] más kormányzati ügynökségek számára.[25]

Az Egyesült Államokban a 2000-es évek közepe óta erősödött fel annak a kormányzati igénye, hogy a nemzetbiztonsági szervezetek fokozottabban működjenek együtt külső, tudományos felekkel az innováció és képességeik továbbfejlesztése érdekében. A szervezet az elmúlt időszakban is folyamatosan bővítette a nemzetbiztonsággal, kriptográfiával, kiberbiztonsággal kapcsolatos egyetemi együttműködéseit. 2013-ban például ötéves partnerséget alakítottak ki a North Carolina State Universityvel az analitikai tudományok laboratóriumának

[18] Mint Major Milán kutatásában részletesen ismerteti, Oroszország esetében a rendkívül összetett portfólióval rendelkező védelmi ipar elmúlt évtizedekben történt átszervezéseit követően jelenleg is több millió alkalmazottat foglalkoztat. Az idesorolható cégek és szereplők esetében is fontos szempont a kutatás-fejlesztés, és ezen keresztül az Oroszországi Föderáció innovációs előrehaladásához való hozzájárulás. Lásd Major Milán: Az orosz védelmi ipari komplexum a Szovjetunió szétesésétől napjainkig. *NKE Stratégiai Védelmi Kutatóintézet Nézőpontok,* (2020), 2. 1–10.

[19] Access to innovation: NSA's Technology Transfer Program. *The Next Wave,* 19. (2012), 3.

[20] Access to innovation (2012): i. m.

[21] *Patent License Agreements* (PLAs).

[22] *Cooperative Research and Development Agreements* (CRADAs).

[23] *Educational Partnership Agreements* (EPAs).

[24] *Technology Transfer Sharing Agreements* (TTSAs).

[25] Access to innovation (2012): i. m.

(LAS) létrehozására, amely küldetése a szolgálat, a tudományos szféra és az ipar közötti együttműködés a big data kérdéskörrel kapcsolatos kihívások megoldására.[26]

A nyíltnak tekinthető együttműködési formákhoz sorolva, az amerikai mellett a brit GCHQ[27] mint technikai feladatkörrel rendelkező nemzetbiztonsági szolgálat esetében is kiemelt hangsúlyt fordítanak a fiatal generációkat megcélzó utánpótlásra, a kapcsolódó képzésekre, kapcsolatrendszerekre. Egyetemi partnerségi programokkal rendelkeznek a kiberbiztonság területein, elősegítve a témakör külső felekkel történő közös kutatását.[28] Példaként említhető, hogy a GCHQ már évekkel ezelőtt „nyolc egyetemet választott partnerévé a kiberbiztonsági tevékenységben",[29] de itt emelhető ki az Alan Turing Intézettel fennálló együttműködés is, amely a GCHQ-val közösen indította el az egyetemi tudományos vagy akár a vállalati szféra felé is kapcsolatot biztosító működését az adattudományok terén.[30]

Az együttműködések védelmének szükségessége

A (nemzet)biztonsági ágazat jellegéből adódóan a szféra érdeklődési körébe tartozó kutatások és infrastruktúra sajátos védelmet igényel.[31] Ez a védelem

[26] Christopher Kampe et al.: Bringing the National Security Agency into the Classroom: Ethical Reflections on Academia-Intelligence Agency Partnerships. *Science and Engineering Ethics,* (2019), 25. 869–898.

[27] GCHQ *(Government Communications Headquarters)* Nagy-Britannia technikai feladatrendszerű nemzetbiztonsági szolgálata. Széles körben ismertek a brit titkosszolgálatok keretei között fejlődő SIGINT-képességek történeti előzményei, így például a híres Bletchley Parkban a II. világháború idején folytatott kódfejtési tevékenység. Összetett feladatrendszere mentén, a GCHQ feladataival már 1946 óta segíti a brit kormány és szövetségesei katonai, diplomáciai és bűnüldöző szerveinek tevékenységét. Lásd GCHQ: *Bletchley Park & WWII* (é. n.).

[28] GCHQ: *Education & Outreach* (é. n.).

[29] Richard Tyler: GCHQ Recruits Eight Universities to Counter Cyber Attacks*. The Telegraph,* 2012. április 1.

[30] Secure Trend 2015, valamint The Alan Turing Institute: *Current Partnerships and Collaborations* (é. n.).

[31] David Dwaine Cornely: *Leadership and Security: Factors that Support or Prevent Successful Integration into Research and Development Organizations.* Dissertation Presented in Partial Fulfillment of the Requirements for the Degree Doctor of Management in Organizational Leadership. University of Phoenix, 2003.

azonban nem pusztán ágazati sajátosság, hiszen a profitorientált gazdasági környezetben zajló, üzleti titkokat, új innovációkat érintő kutatások terén hasonló kritériumokkal találkozhatunk. Mivel az új technológiák, megoldások mindig is a másik fél hírszerző szervezetének érdeklődési körét képezték, nem lehet kétségünk afelől, hogy a tudományos és technológiai hozzáértés megszerzésének célja napjainkban is jelen van[32] (akár az idegen államok érintett szervei, akár a vállalatok oldaláról jelentkező ipari kémkedés előtt). Megjelenésük az új tudományos eredmények, innovációk létrehozásával párhuzamosan erősödhet fel, akár a humán információgyűjtés, akár a kibertérben végzett információgyűjtési megoldásokon keresztül.

A védett tudományos információk megszerzésére irányuló törekvések azonban hosszú távon negatív hatással lehetnek annak elkövetőjére, hiszen tudományos partnerei részéről bizalomvesztést eredményezhetnek. Ennek következményeként – akár jelentős gazdasági hátrányokat okozva – elzárulhatnak az új tudományos eredményekhez való hozzáférés forrásai. Az ipari kémkedés lehetőségének ellensúlyozására, a zárt tudományos kutatási területeknél érthető módon így jelen kell lennie a biztonságtudatos szemléletnek, valamint hatékony biztonsági programokat kell beágyazni a K+F szervezetekbe.[33] Az új eredmények, innovációk nemzetbiztonság célú felhasználása mellett fontossá válik az ott keletkező információk védelmének kialakítása,[34] a szükséges információvédelmi protokollok kidolgozása, a minősített információk megfelelő kezelése.

A nemzetbiztonsággal való egyetemi együttműködések során felmerülhetnek egyéb bizalmatlansági kérdések is. Idesorolhatók akár egyes tudósok, kutatók azon félelmei, hogy a nemzetbiztonsági szférával való együttműködés rányomhatja a bélyegét (például ipari kémkedés gyanúja) megjelenésükre a nemzetközi környezetben és tudományos kapcsolataikra is, így kevesebb eséllyel válhatnak részeseivé az új tudományos eredményeket létrehozó nemzetközi projekteknek. Mint Fredrik Westerlund felveti tanulmányában: „A hírszerző szolgálatokkal való kapcsolattartás valószínűleg nem csak tönkreteheti az egyes tudósok, vagy vállalkozók nemzetközi helyzetét, hanem megzavarhatja a kutató szervezetet és korlátozza a külföldi szereplőkkel folytatott szoros együttműködés lehetőségeit."[35] A legrosszabb esetben aláássa a bizalmat az adott intézmény irányába.

[32] Westerlund (2010): i. m.
[33] Cornely (2003): i. m. 4.
[34] Peter McPherson – Mary Sue Coleman: We Must Have Both. *Inside Higher Ed,* 2019. augusztus. 5.
[35] Westerlund (2010): i. m.

A nemzetbiztonsági területen nem ismeretlen annak gyakorlata sem, hogy a szférába kerülő, korábban nyílt tudományos életet és kapcsolatrendszert folytató kutató számára a védett kutatásokon alapuló tudományos eredményeinek nyílt publikálása érthető módon elmarad.

Az új tudományos eredmények kiáramlásához kapcsolódó félelmek

Az új tudományos eredmények kiáramlásához kapcsolódó félelmek, az egyetemeken folyó kutatások irányába megjelenő „indokolatlan érdeklődés" (így például egy másik ország által motivált információszerzés) témaköre az elmúlt években egyre nagyobb visszhangot kapott a nemzetközi politikai színtéren. Az Egyesült Államok esetében a „félelmek" közvetlenül érintették az egyetemi és tudományos szférát is, egyrészről a „veszélyesnek" ítélt országok (például Kína, Irán, Oroszország, Észak-Korea) diákjainak és kutatóinak jelenléte, másrészről az ezen országokhoz köthető „tehetséggondozási" programokban való részvételek miatt. Ezek közül a legjelentősebb veszélynek az országban tudományos kutatásokban részt vevő nagyszámú kínai hallgatói és kutatói közösséget tekintik. John Negroponte[36] szerint Kínából „évente 250 000 hallgatót küldenek az Egyesült Államokba", akik egy részéről feltételezhető, hogy a világ legjelentősebb gazdasági hatalmává válni akaró Kína nyomást gyakorol rájuk, hogy hazatérésükkor jelentsenek a kínai kormánynak.[37] Kína egyébként is egyre emelkedő létszámú hallgatót küld a világ különböző országainak oktatási intézményeibe, így amíg 2008-ban közel 180 ezer, addig 2018-ban már 662 ezer hallgató tanult külföldön.[38] Ebből az Egyesült Államokban a 2009/2010-es tanévben több mint 127 ezer, de a 2018/2019-es tanévben már több mint 369 ezer hallgató tanult, amivel Kína a nemzetközi hallgatók elsődleges forrása.[39]

Általánosan elmondható, hogy a mérnöki, a matematikai és a számítástechnikai tudományok területén a nemzetközi hallgatók teszik ki az amerikai egyetemeken a doktori fokozatot szerző hallgatók többségét. 2017-ben például

[36] Az USA első Nemzeti Hírszerzési Igazgatója (DNI) 2005–2007 között.

[37] Green (2019): i. m.

[38] Adatok forrása: Number of Students from China Going Abroad for Study from 2008 to 2018. *Statista,* (2020).

[39] Adatok forrása: Number of College and University Students from China in the United States from Academic Year 2009/10 to 2019/20, *Statista*.

a Kínából érkező hallgatók 5157 tudományos és mérnöki doktori fokozatot szereztek, ami abban az évben az USA-ban szerzett 41 438 doktori fokozat több mint 12%-a volt.[40]

Idesorolhatók az USA és Kína 2018–2020 közötti gazdasági háborújának légkörében felszínre került egyéb sérelmek,[41] illetve a kínai technológiai nagyvállalatok térnyerése[42] elleni szankciók is, amelyek hátterében az Egyesült Államok attól való félelmei állnak, hogy kínai távközlési gyártók eszközein keresztül a kínai kormány számára lehetővé válik az USA elleni kémkedés. A válaszként 2018-ban aláírt amerikai jogszabály (*National Defense Authorization Act,* NDAA) létrehozása azonban jelentős hátrányt okozhat az egyetemi-tudományos szférának, hiszen az amerikai egyetemeken évek óta meghatározók a kínai támogatások, a kínai hallgatói és kutatói állomány létszáma, valamint számos területen közös érdek az új kutatási eredmények létrehozása. Az egyetemek számára így a kínai féltől való eltávolodás egyik oldalról akár adott kutatási projektek visszaesését, másik oldalról a jogszabály 2020 augusztusáig történő nem teljesítése esetén az állami kutatási támogatások elvesztését jelentheti.[43] Mindez jól jelzi a gazdasági és nemzetbiztonsági érdekek, valamint az egyetemi kutatások „nemzetközi" határokon átnyúló jellegét, összetett megjelenését.

Az áttekintett forrás alapján 2019-ben az FBI, a kínai diákok és kutatók részvételével zajló, védelmi iparban felhasználható kutatások felülvizsgálatát kérte több egyetemtől, és tájékoztattak több vállalatot, kutatóintézetet a kínai hírszerzési és kiberbiztonsági fenyegetésekről.[44] Egyes egyetemek megszakították

[40] A tudomány és biztonság kapcsolatát vizsgáló tanulmány megfogalmazza, „ha az akadémikusok és a csúcstechnológia más őrzői nem lesznek óvatosabbak, az USA azt kockáztatja, hogy más országoknak – nevezetesen Kínának – lehetővé teszi, hogy ellopják az amerikai adófizetők által finanszírozott kutatás gyümölcseit, és megalapozzák, hogy technikai előnyt szerezzenek bizonyos kritikus tudományos és technológiai területeken". Elizabeth Redden: Science vs. Security. *Inside Higher Ed,* 2019. április 16.

[41] Deák András György: Kevés egyezmény, kívánt eredmény? – Trump kínai „vámháborújának" mérlege. *NKE Stratégiai Védelmi Kutatóintézet Elemzések,* (2020), 8. 1–12.

[42] „Peking hivatalos célja Kínát egy innováció-alapú országgá tenni 2020-ig, illetve a világ vezető innovációs központjainak egyikévé válni 2030-ig." Forrás: Külgazdasági és Külügyminisztérium Magyarország Nagykövetsége, Peking, Vezetői összefoglaló, 2017–18 TET éves beszámoló.

[43] Heather Somerville – Jane Lanhee Lee: U.S. Universities Unplug from China's Huawei under Pressure from Trump. *Reuters,* 2019. január 24.

[44] Diákmunka: Az FBI diákokkal figyelteti a kínaiakat. (MTI) *Librarius,* 2019. június 30.

a Kínával folytatott közös kutatásaikat, együttműködéseiket,[45] mások azonban ellenérzéseket fogalmaztak meg a nemzetbiztonsági szervek kéréseivel kapcsolatosan. Jelen pillanatban még nem látható, hogy a 2020 elején kirobbant világjárvány elleni küzdelem közös, országokon túlmutató érdeke hogyan fogja formálni ezeket a nemzetközi kutatási együttműködéseket.

Összességében a nemzetbiztonság részeként jól láthatók a K+F+I területek védelmének indokai és ellentmondásai, az egyetemi „tudományos nyitottság" és a „nemzetbiztonsági érdekek" találkozásának komplex kérdései. A biztonságpolitikai színtéren zajló folyamatok pedig napjainkra tovább erősítették a tudomány és kutatás szabadságához, valamint a nemzetbiztonsági-gazdasági érdekek biztosításához kapcsolódó teoretikus vitákat.

Egyetemek vs. nemzetközi hallgatói migráció

Szinte minden jelentősebb egyetem képzési-kutatási területein és hallgatói létszámában meghatározó a külföldi hallgatók jelenléte. Egy-egy nagyobb egyetem akár többezres külföldi hallgatói létszám fogadására és folyamatos képzésére is vállalkozik, amely sajátos, egyes elemeiben a nemzetbiztonsági szféra feladatrendszeréhez sorolható kérdésköröket is eredményezhet. Mint M. Császár Zsuzsa és szerzőtársai tanulmányukban megfogalmazzák, „a nemzetközi hallgatói migráció napjaink felsőoktatásának egyik leginkább kutatott jelensége".[46] Az előző kínai hallgatói példán is látva tényként kezelhető, hogy a külföldi hallgatók jelenléte a képzést kínáló országoknak és maguknak az egyetemeknek is rendkívül fontos, nemcsak az államok nemzetközi kapcsolatainak erősítése, hanem az intézmény tudományos hírnevének erősítése terén is. Vitathatatlanul fontos, hogy a külföldi hallgatók által „befizetett tandíjak közvetlen gazdasági hasznot jelentenek".[47] Érthető tehát az egyetemek nyitottsága, fogadókészsége a külföldi diákok iránt, amely folyamat azonban biztonsági szempontból is

[45] Itt említhetők meg a Konfuciusz Intézetek bezárásához kapcsolódó viták, amelyek a hasonló nemzetközi intézményekhez képest nem önállóan, hanem együttműködések révén adott egyetemeken belül jöttek létre.

[46] A nemzetközi hallgatói migráció biztonságpolitikai kockázatait részletesen vizsgálja tanulmányában M. Császár Zsuzsa et al.: A nemzetközi hallgatói migráció biztonságpolitikai kockázatainak egyes aspektusai. *Nemzetbiztonsági Szemle,* 6. (2018), 3. 49–64.

[47] M. Császár et al. (2018): i. m.

megközelíthető. A kapcsolatok pozitívumainak részletes bemutatásától eltekintve, a biztonsági szervek munkáját igénylő feladatként azonosíthatók:

- egyes tudományos kutatási területeken a gazdasági hátrányokat és nemzetbiztonsági érdekeket sértő, versenyhátrányt okozó lehetséges információszerzési tevékenységek (tudományos-gazdasági hírszerzés, ipari kémkedés) felderítése, megakadályozása;
- a távoli, akár terrorizmussal sújtott térségekből (például tanulói vízummal) érkező, biztonsági kockázatot jelentő személyek kiszűrése,[48] vagy akár az egyetemeken esetlegesen felbukkanó radikalizáció nyomon követése.

Befejező gondolatok

A nemzetbiztonsági struktúrák számára egyre fontosabbá válnak az egyetemi, tudományos környezet nyújtotta lehetőségek. A kialakuló együttműködési felületek a hagyományos képzési területeken túl katalizátorszerepet tölthetnek be a tudományos kutatások és új innovatív technológiák mentén. A közös érdekeken alapuló együttműködések lehetőségeket teremthetnek az alapvetően zártan működő nemzetbiztonsági szolgálatok számára a társadalom felé történő nyitására, a bizalmatlanság csökkentésére, valamint a gazdasági szereplők szükséges mértékű bevonására a K+F tevékenységek, az új technológiák és műszaki megoldások fejlesztése terén.

A hidegháború időszakának „nemzetbiztonsági célzatú" fejlesztési modelljeinek felhasználása a 21. század technológiai versenyben számos elemében már idejétmúltnak tekinthető, és a nyílt, globális tudományos környezetben rendkívül gyorsan formálódó innovációk megjelenését a zárt struktúrák nem tudják kellően lekövetni. Mint O'Connell megfogalmazza, egyetlen „titkosítási/minősítési" rendszer „sem akadályozhatja meg a tudomány fejlődését",[49] hiszen a fejlődés lehetősége a hírszerzési/információgyűjtési, valamint az elhárítási/védelmi technológiák innovációjának lehetőségét is magában hordozza.

[48] Példaként említhető, hogy a 2001. szeptember 11-i Egyesült Államokbeli terrortámadás előkészítői között külföldről, diákvízummal érkező személy is megtalálható volt.

[49] Kevin M. O'Connell: The Role of Science and Technology in Transforming American Intelligence. In Peter Berkowitz (szerk.): *The Future of American Intelligence.* Hoover Press, 2005. 153.

Napjainkra a nemzetközi szintű kutatási kapcsolatok, a különböző projektek mentén alakuló új együttműködési formák jelentős része már a virtuális térbe tolódott át. Megszűntek a fizikai értelemben vett zárt határok a tudományos eredmények megosztásában és

> „a különböző tudományágak technológiai közösségei egymást elősegítve, eredményeit felhasználva új tudományterületeket hozhatnak létre, a hatékonyság maximalizálása érdekében a multinacionális kutatóintézetek ötleteket, embereket és erőforrásokat mozgathatnak könnyedén nemzeti határokon át".[50]

Az együttműködések jelentőségére és a változásokra felhívva a figyelmet, William Regli 2018-ban a DARPA-ról szóló kiadványban fogalmazza meg, hogy az új technológiák egyidejűleg furcsának, csodálatosnak és zavarónak bizonyulnak, sőt a változások gyorsasága kapcsán felveti, hogy a technológiai fejlődéshez és az új eredmények megjelenéséhez kapcsolódó kihívások közül „sok meghaladja a kormányzati válaszidőket, az egyetemek ciklusait"[51] is. Mindez új megközelítéseket kíván, és mindkét oldalról megköveteli, hogy új mechanizmusokat találjanak a nem nyilvános kutatások és ösztöndíjak támogatására, amelyek érzékeny kérdéseket érinthetnek – biztosítva mind az akadémiai és kutatói szabadságot, mind a nemzeti érdekeket.[52]

Ezek jelentősége a nemzetbiztonsági szervezetek számára is kiemelten fontos, hiszen lehetővé válhat, hogy a technológiailag hagyományosan meghatározó nagy nemzetek mellett a korábban fejletlenebb képességekkel rendelkező országok is egy-egy kutatási területen jelentős eredményeket érjenek el. A partnerségek révén új, a nemzetbiztonsági szolgálatok feladatait támogató kutatási források jelenhetnek (például pályázati konzorciumok) meg, amelyek közvetve hozzájárulhatnak a szervezeteknél az állomány megtartásához, a tudományos munkatapasztalatok beépüléséhez és a szakértelem növekedéséhez.

A változások a nemzetbiztonságért felelős szervezetektől is innovatív gondolkodást, a változó környezet nyomon követését igénylik, utat nyitva a nemzetbiztonsági szempontokat szem előtt tartó jövőbeli együttműködések létrehozásának.

[50] Kadtke–Wharton (2018): i. m.
[51] Regli (2018): i. m. 134–136.
[52] Regli (2018): i. m. 134–136.

A biztonságtudatosítás felértékelődő szerepe

Mezei József

A megelőzés, a prevenció célja valamely nemkívánatos állapot bekövetkezésének elkerülése. A megelőző tevékenység jelen van minden olyan ágazatban, az élet minden olyan területén, ahol az egyes embert, a társadalom valamely csoportját, rendszereket, folyamatokat olyan veszélyek fenyegetnek, amelyek bekövetkezése esetén jelentős kár keletkezik, és a veszély realizálódása bizonyos intézkedésekkel megelőzhető, vagy mértéke, következményeinek káros hatásai csökkenthetők, minimalizálhatók. A megelőzés érdekében folytatott tevékenységeknek számtalan formája lehet, kezdve a különböző szintű szabályozásoktól az egyén számára biztosított védőeszközökön keresztül a veszélyes környezet biztonságossá tételéig, vagy a személy biztonságtudatosságának fokozásával.

A különböző veszélyek kapcsán a biztonságos állapot megtartását szolgáló vagy a veszély hatásait csökkentő emberi viselkedés sok esetben megtanulható, a szükséges képességek, készségek elsajátíthatók, kialakíthatók. A legtöbb emberben az ehhez szükséges ismeret nagyon sok területen idővel tapasztalatszerzés által, önképzés eredményeként fel is halmozódik. Napjainkban azonban a korábbi évtizedekhez viszonyítva egyre gyorsuló ütemben újabb és újabb biztonsági kihívások jelennek meg környezetünkben, amelyek gyakran jelentős veszélyt is hordoznak. Ezek a veszélyek sokrétűek, az élet számos területén előfordulhatnak, megjelenési formáikat tekintve változatosak, sok esetben összetettek, így az ellenük való védekezés is bonyolult, nehéz feladat. Az emberek biztonságtudatosságának célzott, külső szervezet általi fejlesztése egy prevenciós eszköz, amely jelentős segítséget tud nyújtani e helyzetek kezelésében azáltal, hogy lerövidíti egy adott kockázat felismeréséhez, megelőzéséhez szükséges ismeretek megszerzésének időtartamát. A 2019 végén megjelenő és nagyon rövid idő alatt világjárvánnyá váló SARS-CoV-2 új típusú koronavírus-fertőzést kísérő sajnálatos eseményeknél, illetve az egyes nemzetállamok által meghozott védelmi intézkedéseknél talán semmi nem szemlélteti aktuálisan jobban, érthetőbben a megelőzés és ennek részeként az emberek biztonságtudatossága fokozásának szükségességét, célját, módszereit és hatékonyságát.

A prevenciós tevékenység nem a 21. század terméke. A megelőzés a rendészet területén is régóta jelen van. Az angol Henry Fielding a 18. század második

https://doi.org/10.36250/00904_11

felében már a bűnmegelőzés fontosságáról beszélt, gondolkodott és írt.[1] Ez irányú munkásságának elismerése jeléül a bűnmegelőzés atyjaként is emlegetik. Az ő munkásságát folytatta e téren Sir Robert Peel belügyminiszter, későbbi miniszterelnök, aki 1829-ben létrehozta a londoni rendőrséget, emellett pedig megalkotta a közösségi rendőrség kilenc alapelvét is, amely több ponton érinti a rendőrség és a közösség együttműködésének fontosságát.[2] Peel többek között azt vallotta, hogy a bűncselekményekkel kapcsolatos információkat meg kell osztani a társadalommal. Az Amerikai Egyesült Államokban az első bűnmegelőzési osztályt 1925-ben, Kaliforniában hozták létre,[3] amely az első ilyen feladatkörrel rendelkező szervezet volt a rendőrség történetében. A nemzetbiztonság területén a társadalom széles körű tájékoztatásának mint a megelőzés egyik módszerének történetét kutatva példaként hozhatjuk Pilch Jenő ezredest,[4] magyar katonatisztet, akinek szerkesztésében 1936-ban jelent meg magyar nyelven a *Hírszerzés és kémkedés története* című összefoglaló mű. A kiadvány előszavában a szerzőktől a könyv megszületésének indokai között az alábbiakat olvashatjuk:

> „[…] elrettentsük honfitársainkat olyan cselekményektől, amelyek miatt, akárcsak a bélpoklosokat, kitaszítják őket a nemzet és a becsületes társadalmi osztályok kebeléből. […] De azt is akarjuk, hogy ennek az agyonsanyargatott magyar hazának minden becsületes polgára felfigyeljen és az ádáz ellenségeink által ellenünk irányított kémkedés elhárításában és kiirtásában segítőkezet nyujtson (sic!) azoknak, akik erre intézményesen hivatottak."[5]

Ezek a sorok jól szemléltetik, hogy már közel száz évvel ezelőtt is megfogalmazódott az a gondolat, hogy a nemzetbiztonság veszélyeiről tájékoztatni kell a társadalmat, mert azzal egyrészt eltántoríthatók az állampolgárok az ilyen

[1] Francis Dodsworth: Police and the Prevention of Crime: Commerce, Temptation and the Corruption of the Body Politic, from Fielding to Colquhoun. *British Journal of Criminology,* 47. (2007), 3. 439–454.

[2] Anna Ramsay – Augusta Whittall: *Sir Robert Peel.* New York, Books for Library Press, 1969.

[3] www.cityofberkeley.info/police/history/history.html

[4] Pilch Jenő (Pécs, 1872. május 28. – Budapest, 1937. szeptember 12.): hadtörténész író, a Magyar Tudományos Akadémia tagja (levelező tag: 1918, rendes tag: 1935). A Ludovika Akadémia elvégzése után a pécsi hadapródiskolában, majd a budapesti Ludovika Akadémián tanított katonai földrajzot. 1920-tól a Hadtörténeti levéltár és múzeum igazgatója. 1914-től a *Hadtörténeti Közlemények,* 1919–1920-ban a *MOVE* című hetilap, a *Magyar Mars* és a *Magyar Katonai Közlöny* szerkesztője. Kenyeres Ágnes (szerk.): *Magyar Életrajzi Lexikon.* Budapest, Akadémiai Kiadó, 1994.

[5] Pilch (1936): i. m. 177.

típusú tevékenységektől, másrészt a szolgálatok megnyerhetik őket feladataik támogatásához. Az is fontos körülmény, hogy e gondolatok akkor merültek fel, amikor „egymást érték a kémek elítélésére vonatkozó igen szigorú bírósági ítéletek […] a hazaárulásban, szinte vészes fokozatosságot állapíthatunk meg”,[6] vagyis amikor a szolgálatra hirtelen nagy mennyiségű feladat hárult.

A nemzetbiztonsági tevékenység kapcsán az azokkal foglalkozó szervezeteket, a működésükre vonatkozó szabályzókat, az alkalmazott eszközöket és módszereket, sőt az ezen a területeken elért eredményeket is a kezdetektől a titkosság, a társadalom irányába az ezzel összefüggő tájékoztatás szinte teljes hiánya jellemezte. Ez számos okra vezethető vissza, azonban ezek közül az egyik legalapvetőbb az, hogy maguk a titkosszolgálatok nem törekedtek, illetve a szabályzók alapján nem is törekedhettek egy széles körű tájékoztatásra, illetve nyilvános együttműködési felületek kialakítására a társadalommal.

A 20. században a kockázatok elhárítása során a titkosszolgálatok szinte kizárólag az adott üggyel közvetlenül összefüggésbe hozható személlyel/személyekkel léptek kapcsolatba, működtek együtt, illetve osztottak meg információkat. Előfordult néha, főleg a hidegháború időszakában, hogy a szolgálatok tevékenységébe a társadalom bepillantást nyerhetett, de ez a legtöbb ilyen esetben nem szakmai, hanem politikai érdekeket szolgált. A társadalommal való kapcsolat tekintetében nem az együttműködés hatékonyabbá tétele volt a cél, és ezek az esetek nem is a társadalom preventív célú tájékoztatását jelentették, sokkal inkább az ellenség rossz színben történő feltüntetése és a saját állampolgárok elrettentése volt az indok.[7]

A 20. század végén, a 21. század elején azonban több olyan változás is történt, amelyek ösztönzőleg hatottak a társadalom és a titkosszolgálatok közötti együttműködés kiszélesítésére, bizonyos szintű elmélyítésére. Ezek közül az egyik a terrorizmus erőteljes megjelenése volt. A 21. század első két évtizedében

[6] Pilch (1936): i. m. 177.

[7] 1966-ban három magyar állampolgárt is elítéltek hazánkban a CIA részére folytatott kémkedés miatt. Az esetekről széles körben tájékoztatták a nyilvánosságot. Elkészült egy dokumentumfilm, amelyben megszólaltatták az érintetteket. A filmet a Magyar Televízió 1967. március 22-én be is mutatta. A bírósági tárgyalásokról cikkek jelentek meg az újságokban (lásd *Békés Megyei Újság,* 1966. május 27.). Kiadtak egy füzetet, amely fényképekkel illusztrálva, az ügy feldolgozása során megállapított szakmai ismeretek széles körű és mélységi bemutatásával foglalta össze az eseteket. (Bán Ernő: *Kémek – hazaárulók.* Budapest, Zrínyi, 1966.)

számos, jelentős emberáldozattal járó terrortámadás történt[8] az USA-ban és Európában, amelyek következtében a társadalom részéről határozott elvárásként fogalmazódott meg a biztonság iránti igény a kormányok, illetve közvetetten a titkosszolgálatok, rendvédelmi szervek irányába, másrészt az, hogy többet tudjanak a terrorizmusról.

Egy másik fontos változás, amely ösztönző tényezőként jelentkezett a biztonságtudatossági módszerek széles körű bevezetése kapcsán, az a technológia, azon belül is az informatikai eszközök, rendszerek és az ezekkel összefüggő egyéb technológiák robbanásszerű fejlődése és rendkívül széles körű elterjedése. Az informatikai eszközök, rendszerek használata nagyon rövid idő alatt a mindennapi élet nélkülözhetetlen részévé vált. Magánemberek, állami és civil szervezetek, gazdasági szereplők mind-mind egyre szélesebb körben aknázzák ki az informatikai eszközök, rendszerek és a rajtuk futtatható programok által kínált lehetőségeket. Már most is jelentős és folyamatosan növekvő adatmennyiséget tárolnak ezekben az eszközökben, rendszerekben, amelyek sok esetben érzékenyek, üzleti titkok, vagy minősített adatok. Az állam, illetve a gazdasági szereplők informatikai rendszerek segítségével működtetnek folyamatokat, amelyek kritikusak is lehetnek az állam rendeltetésszerű működése, vagy akár biztonsága szempontjából is. Ennek következtében a 21. század elejére az információtechnológiához köthetően olyan új típusú, bekövetkezésük esetén súlyos következményekkel járó kockázatok jelentek meg, amelyek elhárítása a titkosszolgálatok számára jelentős többletfeladatokat eredményezett. Példaként említhető, hogy az ellenérdekelt hírszerző szervek tevékenysége a valós térből nagyon rövid idő alatt széles körben áthelyeződött a virtuális térbe[9] úgy, hogy

[8] Az al-Káida 2001. szeptember 11-én az USA-ban hajtott végre utasszállítók eltérítésével öngyilkos támadásokat, amelynek következtében 2996 ember vesztette életét. 2004. március 11-én tíz robbantásos merénylet történt Madridban, aminek következtében 191 ember halt meg. 2005. július 7-én Londonban, a tömegközlekedési rendszereket érintően hajtottak végre robbantásos merényleteket. A támadásnak 56 halálos áldozata volt.

[9] A „Snowden-ügyként" elhíresült eseménysor kapcsán napvilágot látott információk többek között nyilvánvalóvá tették, hogy az informatikai eszközök és rendszerek adatbiztonsági szempontból mennyire sok irányból támadhatók, illetve azt, hogy egyes titkosszolgálatok nagyon komoly képességekkel rendelkeznek e téren. Greenwald (2014): i. m.

mellette a korábbi kihívások sem tűntek el, de a terroristaszervezetek is nagyon hamar felfedezték az új felület kínálta lehetőségeket is.[10]

Emellett nyilvánvalóvá vált, hogy ezek a rendszerek, a bennük tárolt adatok, valamint az általuk irányított folyamatok biztonsága szempontjából kulcsfontosságú az azokat kezelő ember, valamit e személyeknek az információbiztonsággal kapcsolatosan meglévő ismeretei. Ezzel összefüggésben fontos, a biztonság szempontjából pedig már kritikus körülmény, hogy a technológia fejlődésének dinamikája olyan mértékű volt az elmúlt néhány évtizedben, hogy a felhasználók jelentős hányada csak egyes elemeiben tudta az azok biztonságos használatához szükséges ismereteket elsajátítani.

A technika ez irányú fejlődése azonban – ahogy feljebb már utaltunk rá – nem csak kihívásokat jelentett a titkosszolgálatok számára. Számos területen megkönnyítette a feladatok végrehajtását, például kibővítette a társadalommal való kapcsolattartás, a kommunikáció lehetőségeit. Ezek felhasználásával szélesebb körben, időtől és távolságtól függetlenül, olcsóbban és többféle módon tudnak ismereteket átadni. Természetesen egyéb tényezők is hatottak arra, hogy a titkosszolgálatok szélesebb körben nyissanak a társadalom felé, de az előzőkben leírtakból egyértelműen kirajzolódik, hogy a 21. század elejére olyan irányú változások történtek, amelyek alapján – némi túlzással – a társadalom bármely tagja nemzetbiztonsági kockázatok célpontjává vagy akár áldozatává válhatott. Tekintettel arra, hogy a kockázattal érintett személyi kör ennyire kiszélesedett, valamint figyelembe véve azt, hogy a nemzetbiztonsági kockázatok esetében alapvető elvárás a megelőzés, a szolgálatoknak szakítaniuk kellett a korábbi megközelítéssel. Az egyes ügyekben érintett személlyel való együttműködés helyett át kellett térni a kockázat szempontjából releváns személyi kör előzetes, biztonsági szempontú tájékoztatására, felkészítésére. Ez a módszer kapta a biztonságtudatosítás[11] elnevezést, amely összefoglalva nem más, mint a nemzetbiztonsági kockázatok szempontjából érintett személyi kör adott területen meglévő biztonsági ismereteinek, képességeinek célirányos fejlesztése.

[10] „Az internet a terroristák stratégiai eszközévé vált, használják új tagok azonosítására, toborzására és kiképzésére; pénzeszközök gyűjtésére és továbbítására; terrorcselekmények megszervezésére; az erőszak ösztönzésére; és egyre inkább a számítógépes támadások elkövetésére." OSCE: *Countering the Use of the Internet for Terrorist Purposes* (é. n.).

[11] A nemzetközi gyakorlatban az *awareness* kifejezéssel találkozhatunk, tekintettel arra, hogy ezt a fajta tevékenységet nyugati tapasztalatok alapján vezették be a szolgálatok.

A nemzetbiztonság területén a biztonságtudatosító tevékenység elsődlegesen az elhárító tevékenységek részeként van jelen, azon belül is leginkább a terrorelhárítás, a kémelhárítás, az adatvédelem, valamint az infokommunikációs rendszerek biztonsága részterületeken. Az átadandó ismeretek, információk nyíltak, minősített adatokat nem tartalmaznak. Sok esetben a szolgálatok az egyszerű információközléseken túl esettanulmányokon, elképzelt helyzetek bemutatásán keresztül segítik az ismeretek megértését. A biztonságtudatosítással a nemzetbiztonsági szervezetek célja sokrétű, amelybe beletartozik:

- az állampolgárok tájékoztatása a biztonsági kockázatokról;
- nem kötelező érvényű javaslatok megfogalmazása a veszélyhelyzetek megelőzése érdekében és a veszélyhelyzet bekövetkezése során követendő magatartásra vonatkozóan;
- a kölcsönös információcserét lehetővé tevő csatornák kialakítása;
- az esetleges későbbi együttműködés kereteinek megteremtése;
- a szolgálatok iránti bizalom kialakítása;
- a szolgálatok társadalmi elfogadottságának növelése;
- a társadalommal való kapcsolat erősítése.

A célok megfogalmazása kapcsán fontos szempont, hogy a biztonságtudatosítás során nem az az eredmény, ha az állampolgárok hozzászoknak a félelemérzethez.[12] A cél az, hogy a felkészített személyek el tudják kerülni a kockázatokat, illetve a kockázatok esetleges észlelésekor megfelelő időben helyes válaszokat tudjanak adni. A nemzetbiztonságot érintő kockázatok kapcsán a biztonságtudatosság növelése során általánosságban az alábbi területek érintettek:

- a nemzetbiztonsági kockázatok (motivációk, szereplők, célok, eszközök, módszerek, megnyilvánulási formák);
- az összefüggések megértését segítő esettanulmányok;
- a problémakörrel foglalkozó szervezetek;
- a megelőzést segítő javaslatok;
- a kockázat realizálódásakor a negatív hatások csökkentése érdekében követendő magatartásformák.

[12] Kasznár Attila: A terrorelhárítás feladatrendszere a turizmusban. In Kiglics Norbert szerk.: *II. Turizmus és Biztonság Nemzetközi Tudományos Konferencia Konferenciakötet.* Nagykanizsa, Pannon Egyetem, 2017. 48–55.

A biztonságtudatosság növelését célzó ismeretek átadásának jelenleg több módját is alkalmazzák a szolgálatok, próbálják a technika nyújtotta lehetőségeket maximálisan kihasználni. Napjainkban előfordulnak előadások,[13] oktatóvideók,[14] mobiltelefonos applikációk,[15] elektronikus kiadványok,[16] komplex e-learning-tananyagok.[17]

A biztonságtudatossági tevékenységeket gyakran egy program keretében valósítják meg az egyes országok, amelyeknek egyes esetekben rövid, figyelemfelkeltő neveket is adnak. Az Amerikai Egyesült Államokban a terrorprevenció részeként folytatott egyik biztonságtudatossági program neve a „Ha látsz valamit, mondd el!”,[18] egy másiké a „Fuss! Rejtőzz! Harcolj!”. A terrorprevenció népszerűsítése céljából az ez irányú feladatok egyik fő felelőse, a Belbiztonsági Minisztérium szeptember 25-ét kinevezte a nemzeti, „Ha látsz valamit, mondd el!”-tudatosság napjának. A programokat néhol a titkosszolgálatok saját állományukkal hajtják végre,[19] de előfordul, hogy az több szolgálat, illetve civil vagy

[13] Szalai Flóra: *A terrorizmus és a terrorelhárítás törzsfejlődése.* A TEK előadása az ÁJK-n. 2017. március 13.

[14] Egy, a brit rendőrség által a terrorizmus elleni fellépés keretében elkészített videót egy év alatt 7 millió ember nézett meg. A videó létrehozását a 2015-ben, Sousse-ban elkövetett terrortámadás motiválta, amelynek következtében 30 brit állampolgár vesztette életét. Lásd NPCC: *More than Seven Million People Watch Counter Terrorism Safety Video as UK Policing Increases Its Global CT Presence* (2018.július 6.).

[15] Ilyen például a brit Nemzeti Terrorizmus Elleni Biztonsági Hivatal (*National Counter Terrorism Security Office,* NaCTSO) gazdasági társaságok számára elérhető applikációja, amely gyakorlati tanácsokkal és útmutatásokkal segíti a vállalkozásokat, valamint információkat szolgáltat arról, hogyan kell reagálni terrortámadás esetén. Lásd Government of the United Kingdom: *New ACT App Launched* (2020. március 5.).

[16] A TEK által 2019-ben kiadott *Mindennapi biztonság* című kiadvány összegzi a terrorelhárítással kapcsolatos aktuális ismereteket, továbbá javaslatokat és ajánlásokat fogalmaz meg a terrorcselekmények megelőzésével, egy ilyen jellegű cselekmény kezelésével összefüggésben. Jasenszky Nándor (szerk.): *Mindennapi biztonság.* Budapest, Terrorelhárítási Központ, 2019. 7–8.

[17] A NaCTSO egy bárki számra ingyenesen elérhető, komplett, jól átgondolt és felépített, könnyen érthető, megfelelő alapot biztosító interaktív e-learning-képzést állított össze magánszemélyek és gazdasági társaságok részére a terrorelhárítás témakörében, amely videókat, leírásokat, magyarázó szövegeket, valamit a megértést mérő teszteket is tartalmaz. A képzés elvégzéséről igazolást is kiállít a szervezet. Lásd: https://ct.highfieldelearning.com/

[18] U.S. Department of Homeland Security: *If You See Something, Say Something.* (é. n.).

[19] Ebbe a körbe tartoznak például a magyarországi szolgálatok.

rendvédelmi szakmai partner bevonásával, együttműködésben valósul meg.[20] Néhol a terrorelhárítással összefüggő biztonságtudatosítást rendvédelmi szerv koordinálja,[21] de van, hogy ilyen tevékenységet egy civil kezdeményezés eredményeként létrejött szervezet önállóan végez.[22] Általában a programok nemzeti szinten, az országhatárokon belül valósulnak meg, de találhatunk olyan kezdeményezést is, ahol civil szervezet országhatárokon átnyúló programokat folytat.[23] Van példa arra, hogy a program sikeressége érdekében szakértői, tanácsadói hálózatokat is kialakítanak.

A biztonságtudatossági programok megvalósításának nincs egységes modellje. A célok azonosak, a megvalósítás módszerei bárki számára elérhetők, azonban a kivitelezésben eltérések tapasztalhatók. A mintát a nagyobb nemzetbiztonsági kockázatnak kitett, megfelelő kormányzati támogatással, anyagi, humán és technikai háttérrel rendelkező országok adják. (Magyarországon a rendészeti jellegű, a biztonságtudatosság fokozását célzó tevékenység nincs központosítva, azt a biztonsági szervek önállóan oldják meg. Az Alkotmányvédelmi Hivatal,[24] a Nemzetbiztonsági Szakszolgálat[25] és a Terrorelhárítási Központ[26] is aktív, kezdeményező ezen a területen, és számos formában él ezzel a módszerrel.)

[20] A német Szövetségi Alkotmányvédelmi Hivatal a Szövetségi Hírszerző Szolgálattal, a Szövetségi Bűnügyi Rendőrséggel és a Szövetségi Információbiztonsági Hivatallal közösen hoztak létre egy biztonságtudatossági programot, a Gazdaságvédelmi Kezdeményezést, amelybe jelentős számban be tudták vonni a német gazdasági társaságokat különböző ernyőszervezeteken keresztül. A program célja, hogy segítséget adjon a vállalatoknak a számítógépes bűnözés, az ipari kémkedés és az informatikai biztonság témaköreiben.

[21] Az Egyesült Királyságban a terrorelhárítási feladatokért elsődlegesen a Biztonsági Szolgálat (Security Service, korábban MI5) felel, azonban a terrorelhárítás területéhez köthető biztonságtudatosításban meghatározó szerepe van a rendőrségen belül működő Nemzeti Terrorizmus Elleni Biztonsági Hivatalnak, amely több formában, rendkívül széles körben folytatja, koordinálja ezt a tevékenységet.

[22] Sandy Hook Promise: Gun violence warning signs. *Youtube,* (2016. december 6.).

[23] Lásd: https://sacc-ejc.org/security-awareness/

[24] Az Alkotmányvédelmi Hivatal 2011. január 1-jén kezdte el Awareness tevékenységét, amelynek fő iránya a feladatkörében is markánsan megjelenő információvédelem. Lásd Alkotmányvédelmi Hivatal: *Awareness Program* (é. n.).

[25] A Nemzetbiztonsági Szakszolgálat a kiberbiztonság területén folytat, a magyar viszonyokat tekintve rendkívül innovatív módon tudatosító tevékenységet. Lásd: https://nki.gov.hu/it-biztonsag/kiadvanyok/szorolapok/

[26] A TEK többféle megoldással, előadásokon, kiadványokon keresztül segíti az állampolgárokat a terrorcselekmények megelőzéséhez szükséges ismeretek elsajátításában. Lásd Jasenszky (szerk.) (2019): i. m.

A 21. század elején kialakult, titkosszolgálati jellegű biztonságtudatossági projektek több szinten valósulnak meg. A projektekkel, attól függően, hogy milyen jellegű nemzetbiztonsági kockázatról van szó, megszólítják a rendvédelmi, kormányzati szerveket, a gazdasági szereplőket, a társadalom egyes csoportjait és az egyes állampolgárokat is. A biztonságtudatosítás elsődlegesen a felnőtteket célozza, hiszen ők azok, akik leginkább célpontjai lehetnek nemzetbiztonsági kockázatoknak, illetve egy ilyen esemény kapcsán részükről várható el olyan magatartás, amely segíthet a kialakult helyzet megelőzésében, megszüntetésében vagy a károk minimalizálásában.

Az elmúlt időszak megváltozott körülményei nemcsak a biztonságtudatosságot hívták életre, ezen felül is egyre több helyen találkozhatnak az állampolgárok a nemzetbiztonsággal összefüggő, aktuális, releváns információkkal. A mindennapok részévé vált például, hogy politikusok nyíltan beszélnek jelenlegi titkosszolgálati problémákról, és a médián keresztül juttatnak el üzenetet ellenfeleiknek, de akár szövetségeseiknek is.[27] Megfigyelhető továbbá, hogy egyes hírszerző szervezetek a weboldalaikat felhasználva adnak – akár részletekbe menő – tájékoztatást feladataikról, elért eredményeikről, aktuális biztonsági kockázatokról.[28] Egyes médiumokban[29] vagy akár a nemzetbiztonság tárgykörével foglalkozó szakmai folyóiratokban ismét csak részletes és időszerű beszámolókkal találkozhatnak az arra nyitott, fogékony emberek a nemzetbiztonsági kockázatokról. A globalizálódott kommunikáció eredményeként ezek az ismeretek a világ bármely pontján élő emberhez eljuthatnak. Mindazonáltal e felületek elsődleges célja nem az állampolgárok biztonságtudatosítása, habár kétségkívül ilyen eredménye is lehet.

[27] Az USA kormányzata, illetve Donald Trump elnök az elmúlt időszakban élesen bírálja Kínát, illetve a Huaweit az 5G hálózat kiépítésével összefüggésben. Azzal vádolja őket, hogy a kiépített rendszert felhasználva hírszerző tevékenységet fognak folytatni. Szövetségeseinek is burkoltan üzent a Trump-adminisztráció, miszerint aki a rendszereibe beengedi a kínai szállítót, azzal érdemi hírszerzési információt nem fognak megosztani. Lásd U.S. Embassy in Luxembourg: *Secretary Pompeo and Secretary Esper Speak at Munich Security Conference 2020* (2020. február 19.).

[28] Az USA Szövetségi Nyomozó Irodája (Federal Bureau of Investigation – FBI) évek óta folytatott titkos nyomozást orosz, illegális hírszerzőket érintően. A személyek 2010 nyarán történt letartóztatását követően egy évvel, szokatlan módon részletes – képeket, videófelvételeket, eredeti dokumentumokat tartalmazó – beszámolót tettek közzé a nyomozásról a weboldalukon. FBI: *Operation Ghost Stories* (2011. október 31).

[29] A *The Diplomat* című újság részletes elemzést közölt 2018. november 28-án a kínai hírszerzőknek az USA-t érintő tevékenységéről. Lásd Nicolas Eftimiades: Uncovering Chinese Espionage in the US. *The Diplomat,* 2018. november 28.

A biztonságtudatosítás során – az egyes nemzetbiztonsági kockázatok összetettsége, az általuk érintett szervezeteknek, személyeknek az elhárítás szempontjából eltérő jelentősége okán – szükségszerűen megtörténik az egyes területeken az átadott ismeretanyagok specializálódása. Már most megfigyelhető az átadandó ismereteknek az egyes élethelyzetekre, illetve azon belül az egyes érintettekre történő testreszabása úgy horizontálisan, mint vertikálisan. Gondoljunk csak bele, hogy egy zárt térben megszervezett, nagy létszámú, nyilvános esemény kapcsán más dolgokra kell felhívnia a látogatók figyelmét a titkosszolgálatoknak, más tartalmú tájékoztatást kell tartania a szervezőknek, és megint mást a rendezvény biztosításában részt vevő biztonsági szolgálat munkatársainak a terrorcselekmények megelőzése érdekében. Ugyanez megfigyelhető az információbiztonság területén is, hiszen más javalatokat kell megfogalmazni egy külföldi kiutazás előtt, mint mondjuk a közösségimédia-felületek használatát érintően, de mondjuk egy védett intézmény informatikai rendszereinek biztonsága kapcsán is más tanácsokat kell adni a felhasználóknak, illetve a rendszergazdáknak.

A biztonságtudatosítás nem az egyetlen válasz a 21. század elején hirtelen jelentkező széles körű nemzetbiztonsági kihívások kezelésére. Az információtechnológia exponenciális fejlődése valós lehetőségként villantotta fel a tömeges adatgyűjtést is mint megoldást. Egyes országok ezt az utat (is) választották, amely azonban a személyiségi jogok kapcsán erős ellenérzéseket váltott/vált ki a társadalomból.

Összefoglalva a fentieket, a 21. század elején több olyan, az egyes államok biztonságát érintő változás következett be a világban, amelyek hatására a demokratikus országokban jelentősen átalakult a titkosszolgálatok és a társadalom kapcsolata. A szolgálatokat addig markánsan jellemző bezárkózást felváltotta egy tudatos nyitás a társadalom felé, és a jövőben ezt tovább kell mélyíteni.[30] A biztonságtudatosság fejlesztése, amelynek keretében a titkosszolgálatok szükséges mértékben tájékoztatják a társadalom tagjait a nemzetbiztonsági kockázatokról, mint új módszer jelentősen növelte a nemzetbiztonsági szolgálatok elhárító tevékenységének hatékonyságát. Ennek alapja, hogy minden nemzetbiztonsági kockázat – amely nem közvetlenül a titkosszolgálatokat érinti, az – a társadalom valamely szereplőjéhez kapcsolódik, a veszélyt ő érzékeli, az őt célozza. A biztonságtudatossági program eredményeként viszont nagyobb a valószínűsége annak, hogy a jelentkező kockázatokat az állampolgárok érzékelik, helyesen

[30] Drusza Tamás: Jövőbeni kihívások a (polgári) nemzetbiztonsági elhárítás területén. In Drusza Tamás (szerk.): *A magyar elhárítás fejlődése.* Budapest, Dialóg Campus, 2019. 211–238.

értelmezik, így az nem következik be, arról a nemzetbiztonság időben értesül, illetve amennyiben mégis realizálódik, úgy az esetleges károk csökkenthetők. Figyelembe véve azt, hogy a biztonságtudatossági programok életre hívása mögött lévő okok a közeljövőben nem szűnnek meg, vélelmezhető, hogy a titkosszolgálatok ez irányú tevékenysége a 21. század további részében is megmarad, a kihívások változása és a technológia fejlődésének függvényében a szervezeti kerete, módszerei, tartalma tovább fejlődhet, módosulhat.

Válaszok az aktuális kihívások tükrében

Csányi Csaba

Magyarország számára biztonsági kockázatot jelentő kihívások más országok számára is kockázati elemként jelentek meg, így a világ más államai által ezekre adott – jogi vagy nem jogi – válaszok iránymutatásul szolgálhatnak hazánk számára is. A fenti biztonsági kockázatot vagy fenyegetést jelentő elemek közül néhányat önkényesen kiemelve, mint például a kiberbiztonság, valamint hozzá kapcsolódóan a mesterséges intelligencia, a migrációs fenyegetettség, valamint az általam biztonsági kockázatként értékelt elemeket mint hiátust – úgymint adatkezelés versus adatvédelem, innováció, K+F kérdéskör mint nemzetbiztonsági kérdés – beemelve és megvizsgálva kívánom bemutatni az azokra adott lehetséges válaszokat.

Kiberbiztonság

A kiberbiztonság a nemzetbiztonsági stratégia egyre központibb elemévé válik. Az Európai Unió szigorította a kiberbiztonsági szabályait, hogy kezelni tudja a kibertámadások jelentette egyre nagyobb fenyegetést, valamint hogy kihasználja az új digitális kor által kínált lehetőségeket. A Tanács 2019. április 9-én rendeletként elfogadta az úgynevezett kiberbiztonsági jogszabályt, amely bevezeti az egész EU-ra kiterjedő tanúsítási rendszerek keretét, valamint létrehozta az Európai Uniós Kiberbiztonsági Ügynökséget, amely bővített hatáskörrel átveszi a jelenlegi Európai Hálózat- és Információbiztonsági Ügynökség (ENISA) szerepét.

E kiberbiztonsági reform részeként az uniós intézmények olyan jogszabályon is dolgoznak, amely létrehozza majd a Kiberbiztonsági Ipari, Technológiai és Kutatási Központot, amelynek tevékenységét a nemzeti koordinációs központok hálózata fogja támogatni. A Kiberbiztonsági Ipari, Technológiai és Kutatási Központ révén javulni fog a kiberbiztonsági kutatás és innováció koordinálása. Ez a központ emellett az EU fő eszköze lesz ahhoz, hogy összevonja a kiberbiztonsági kutatás, technológia és ipari fejlesztés területére irányuló beruházásokat.

A Kiberbiztonsági Kompetenciahálózatot a tagállamok által kijelölt nemzeti koordinációs központok alkotják majd. A nemzeti központok rendelkeznek majd kiberbiztonság-technológiai szakértelemmel, illetve ehhez hozzáférésük lesz,

https://doi.org/10.36250/00904_12

például az olyan területeken, mint a kriptográfia, az IKT hálózatvédelem vagy a biztonság emberi tényezői.

A Kiberbiztonsági Ipari, Technológiai és Kutatási Központ a kompetenciahálózattal együttműködve végrehajtási mechanizmusként szolgál majd az Európai horizont és a Digitális Európa program keretében megvalósuló, kiberbiztonsági célú pénzügyi támogatáshoz. Együttesen hozzájárulnak majd az uniós kiberbiztonsági ipar versenyképességének növeléséhez, és a kiberbiztonságot versenyelőnnyé teszik a többi uniós iparág számára. E központok finanszírozását elsősorban a Digitális Európa és az Európai horizont program fogja biztosítani, de egyúttal lehetőség lesz önkéntes tagállami hozzájárulások biztosítására is.

A javaslat harmadik struktúraként létrehoz egy kiberbiztonsági kompetenciaközösséget is, amely összefogja a fő érdekelt feleket azért, hogy az EU egészében javuljon, és elérhetővé váljon a kiberbiztonsági szakértelem. A közösség tagjai közé fognak tartozni többek között az ágazati és a felsőoktatási szervezetek, a nonprofit kutatóhelyek, a működési és technikai kérdésekkel foglalkozó állami szervezetek, valamint – adott esetben – kiberbiztonsági kihívásokkal szembesülő egyéb ágazatok szereplői. A központ a 2021. január 1. és 2029. december 31. közötti időszakra jön létre. Ezt követően felszámolják, kivéve, ha a vonatkozó rendelet felülvizsgálata során más döntés születik.

Ezzel párhuzamosan az EU olyan horizontális intézkedéseket dolgoz ki, amelyek egyszerre több területen veszik fel a küzdelmet a kiberfenyegetésekkel. Idetartozik például a szervezett bűnözés elleni küzdelem, ahol a kiberbűnözés a 2018–2021-es időszak tíz legfontosabb prioritásai között szerepel a közös kül- és biztonságpolitika, ahol a kibertámadásoktól való elrettentés alapvetően fontos az Európai Unió közös kül- és biztonságpolitikája (KKBP) céljainak elérése szempontjából, vagy a kibervédelem, amelynek kereteit az EU a változó biztonsági kihívásokra figyelemmel aktualizálta.

Az egyre növekvő kiberbiztonsági kihívások fényében az EU-nak jobban fel kell hívnia a figyelmet a tagállamokkal vagy uniós intézményekkel szembeni kibertámadásokra, és javítania kell az azokra adandó válaszlépéseket. Ezek a nemzeti és uniós határokon átnyúló kihívások nemcsak a biztonságot és a stabilitást, hanem a jólétünket és a demokratikus rendet is veszélyeztetik. Mára valósággá vált a „dolgok internete", és az EU-ban 2020-ra várhatóan több tízmilliárd összekapcsolt digitális eszköz lesz.

Az uniós polgároknak támogatásra van szükségük, hogy bizalom alakuljon ki bennük e technológiák iránt, kezdve a testen hordható eszközöktől a hálózatba kapcsolt autókig. Lehetővé kell tenni egyúttal, hogy az uniós vállalkozások

igénybe vehessék e technológiákat a határokon átnyúló üzleti tevékenységükhöz, legyen szó akár ipari automatizálásról, akár intelligens energiahálózatokról. A mai IKT-rendszerek ugyanakkor komoly károkat szenvedhetnek biztonsági események, például üzemzavarok vagy vírusok miatt. Ezek az események, amelyeket gyakran hálózat- és információbiztonsági (NIS) eseményeknek neveznek, egyre sűrűbben fordulnak elő, és egyre nehezebb őket kezelni, továbbá a vállalkozásokat és a közszolgáltatásokat egyaránt érinthetik, ami pedig aláásható a fogyasztók bizalmát.

Kiberbiztonsági tanúsítási rendszerek

Az Európai Bizottság a 2017 szeptemberében elindított reformcsomagban javaslatot tett az IKT-termékekre, -szolgáltatásokra és -folyamatokra vonatkozó uniós tanúsítási rendszerek bevezetésére. A kezdeményezés célja az uniós kiberbiztonsági piac növekedésének elősegítése.

E tanúsítási rendszerek szabályok, műszaki követelmények és eljárások formájában valósulnának meg. Csökkentenék a piac széttagoltságát, és felszámolnák a szabályozási akadályokat, továbbá segítenék a bizalomépítést is. Emellett valamennyi tagállamban alkalmaznák őket, ami megkönnyítené a vállalkozások számára a határokon átnyúló kereskedelmet.

Európai Uniós Kiberbiztonsági Ügynökség

A Bizottság javasolta továbbá azt is, hogy a meglévő Európai Uniós Hálózat- és Információbiztonsági Ügynökség (ENISA) struktúráját felhasználva jöjjön létre egy uniós kiberbiztonsági ügynökség. Az új ügynökség állandó jogállással rendelkezne, és nagyobb szerepet töltene be az európai kiberbiztonság területén. E továbbfejlesztésnek köszönhetően az Európai Uniós Kiberbiztonsági Ügynökség támogatná a tagállamokat, az uniós intézményeket és a többi érdekelt felet a kibertámadások kezelésében.

Az Egyesült Államok is hasonló úton jár. 2018. november 16-án az Egyesült Államokban Trump elnök aláírta a Kiberbiztonsági és Infrastruktúra-biztonsági Ügynökség törvényt. Ez az irányadó jogszabály a DHS-en[1] belüli korábbi

[1] *Department of Homeland Security.*

Nemzeti Védelmi és Program Igazgatóság (NPPD) küldetését emelte ki, és létrehozta a Kiberbiztonsági és Infrastruktúra-biztonsági Ügynökséget (CISA). A CISA összehangolja a biztonsággal és az ellenálló képességgel kapcsolatos erőfeszítéseket megbízható partnerségek felhasználásával a magán- és az állami szektorban, valamint technikai segítséget és értékeléseket nyújt a szövetségi érdekelt felek, valamint az infrastruktúra tulajdonosai és üzemeltetői számára országszerte. Magyarországon a Nemzetbiztonsági Szakszolgálat (NBSZ) szervezetén belül 2015. október 1-jén szintén létrehozták a Nemzeti Kibervédelmi Intézetet.

Innováció és nemzetbiztonság a 21. században

Azok az országok, amelyek képesek kihasználni a jelenlegi innovációs hullámot, kihasználni annak átalakító erejét, azok enyhíteni tudják a jövőbeni lehetséges problémákat, ebből kifolyólag gazdasági és katonai előnyben lesznek a potenciális riválisokkal szemben. Álláspontom szerint a nemzetbiztonság szempontjából eddig egy nagyon fontos fel nem használt terület a K+F+I.

Az amerikai Külkapcsolatok Tanácsa[2] az amerikai technológiai innováció jelenlegi helyzetének felmérésére egy munkacsoportot hozott létre. A munkacsoport megjegyezte, hogy az innováció, a kutatás és a technológia megfelelő módon – egységesen – történő kezelése és finanszírozása a II. világháború után az Egyesült Államokat a világ legbiztonságosabb és gazdaságilag legfejlettebb országává tette. „Ma ez a vezetői pozíció veszélyben van" – figyelmeztetett a munkacsoport. A K+F szövetségi támogatása és finanszírozása az elmúlt két évtizedben stagnált. „Washington nem tudta fenntartani az alapvető tudományok megfelelő szintű állami támogatását és finanszírozását. A K+F-be fektetett szövetségi beruházások GDP-hez viszonyított aránya 1964-ben 1,86%-ot ért el, de az 1990-es kicsit több mint 1%-ról 2016-ban 0,66%-ra csökkent."[3]

Az innovációt három tényező: a sebesség, a szétszakadás és a méretarány jellemzi manapság. Érdemes megfigyelnünk ezt az alábbi példákon keresztül: 50 év telt el a telefon feltalálásától addig, amíg az összes amerikai ház felébe

[2] A Council on Foreign Relations, CFR 1921-ben alapított magánintézet azzal a céllal, hogy külpolitikai problémák kutatásával foglalkozzon. Hivatalosan független, pártatlan szervezet.

[3] Irving Wladawsky-Berger: Innovation and National Security in the 21st Century. *The Wall Street Journal,* 2020. január 17.

eljutott egy, de az amerikaiak felének a mobil feltalálása után már öt évvel volt okostelefonja. Az emberi genomot először 2003-ban szekvenálták, a költségei hihetetlenül sokba kerültek. Ma 50 órára vállalnak genomszekvenálást, és a kezdeti százmillió dollárról már 1000 dollár alá csökkentek a költségek. A gazdasági teljesítmények egyre inkább távolodnak egymástól, a szétszakadás üteme és mértéke mindinkább növekszik. Az átlagos idő, amelyet a vállalatok a Standard & Poor's 500-on[4] töltöttek, az 1958-as 61 évről 2011-re 17 évre csökkent. Szakemberek az elkövetkező tíz év alatt azt várják, hogy a jelenleg az S & P-on működő vállalatoknak csak 25%-a marad benne.

Három fő tényező veszélyezteti a gazdasági fejlődést és a nemzetbiztonságot világszinten. Az első, hogy a globális innováció felgyorsult, ezáltal zavart okozva a különböző iparágaknak, a gazdaságoknak és a társadalmaknak. A második veszély, hogy a magánszektor globális ellátási láncai és piacai most fejlesztenek több nemzetbiztonsági technológiát és forgalmaznak is, amelyek a különböző államok mindegyike számára elérhető, és a harmadik, hogy Kína – amely mind az USA gazdasági partnere, mind pedig stratégiai versenytársa lett – jelentősen növeli a kormány által irányított kutatás-fejlesztési beruházásokat, így kíván versenyelőnyt teremteni a maga számára mind az Egyesült Államok, mind az EU ellenében.

Az új technológiák és eljárások, mint például a Mesterséges Intelligencia (MI) és az automatizálás jelentős változásokhoz vezet a munkaerőpiacon. A McKinsey Global Institute 2017. évben egy publikációt jelentetett meg ezzel kapcsolatban. A McKinsey-tanulmány arra a következtetésre jutott, hogy míg 2030-ig a foglalkozások kevesebb mint 10%-a lesz teljesen automatizált, addig a munkahelyek 60%-a átalakul az alkotóelemeik jelentős részének automatizálása révén. A tanulmány megjegyezte, hogy „bár a legtöbb forgatókönyv szerint elegendő munka áll fenn a teljes foglalkoztatás 2030-ig tartásáig, az átmenetek nagy kihívást jelentenek".[5]

A CFR-tanulmány megállapításai szerint az évtizedes amerikai vezetés az innováció és a K+F területén most veszélyben van. Ennek okai a K+F szövetségi finanszírozásának csökkentése; az otthoni oktatási kezdeményezések hiánya; bevándorlási akadályok, amelyek megnehezítik a tehetséges külföldi

[4] A Standard & Poor's 500 index rövidített elnevezése, amely a NYSE és a NASDAQ által jegyzett, érték alapján legnagyobb amerikai vállalatok indexe.

[5] James Manyika et al.: *Jobs Lost, Jobs Gained: What the Future of Work Will Mean for Jobs, Skills, and Wages.* McKinsey Global Institute, 2017. november 28.

hallgatók és munkavállalók vonzását és megtartását; és olyan kereskedelempolitika, amely elidegeníti a korábbi gazdasági partnereket, szövetségeseket és együttműködőket. Kína gyorsan behozza technológiai hátrányát az Amerikai Egyesült Államokkal szemben. Kína jelentős forrásokat fektet be új technológiák fejlesztésébe, és 2030 után valószínűleg a világ legnagyobb kutatási és fejlesztési büdzséje lesz. Noha valószínűleg nem fogja teljes egészében utolérni az Egyesült Államok képességeit, várhatóan vezető szerepet fog játszani a kulcsfontosságú technológiákban, beleértve az MI-t, a robotikát, az energiatárolást és az 5G-s mobilhálózatokat. Tehát Kína más típusú kihívást jelent az USA számára, mint a régi Szovjetunió. Kína gazdasági partner és stratégiai versenytárs is jelenleg a világpiacon. Az Egyesült Államok és Kína egyaránt részesültek a kétoldalú beruházásokból és a kétoldalú kereskedelemből származó előnyökből. Ugyanakkor Kína arra irányuló erőfeszítései, hogy tudományos és technológiai hatalommá váljanak, hozzájárulhat a globális jólét előmozdításához, de a szellemi tulajdon másolása/lopása és annak piaccal manipuláló iparpolitikája veszélyezteti az Egyesült Államok gazdasági versenyképességét és a nemzetbiztonságot.[6]

A CFR-munkacsoport szerint az Egyesült Államoknak – ha továbbra is sikeres akar lenni a világban, valamint nemzetbiztonsági érdekeit is megfelelően kívánja védeni és érvényesíteni – új innovációs stratégiát kell kidolgoznia, amely négy kulcsfontosságú pillérre kell hogy épüljön:

A K+F szövetségi támogatását vissza kell állítani a múltbeli átlagra, a GDP jelenlegi 0,7%-át kitevő összegről (146 milliárd dollár) minimum a GDP 1,1%-ára (230 milliárd dollár) növelve. A kormányzatnak támogatnia kell a *moonshot* kezdeményezéseket[7] olyan kulcsfontosságú területeken, mint az MI, 5G, a genomika és a szintetikus biológia. Ugyanakkor a szövetségi és az állami kormányoknak évente dollármilliárdokkal kell növelniük az egyetemekbe történő beruházásokat, hogy támogassák a gazdasági és nemzetbiztonsági területeken folytatott kutatásokat.

Tudományos és technológiai munkaerő vonzása és oktatása. A kormányzatnak és az egyetemeknek ki kell dolgoznia egy kutatási, kutatói, hallgatói programot azzal a céllal, hogy versenyképes egyetemi ösztöndíjat és diplomás ösztöndíjjal támogatva kibővítse a tehetségek körét, különös figyelmet fordítva a kisebbségek és a nők alulreprezentáltságának kezelésére a területen. Hasonló kezdeményezés kezdetei, alapjai vannak lefektetve Magyarországon

[6] Manyika et al. (2017): i. m. 9.

[7] Értsd: első pillanatban hihetetlen, őrült ötletek.

az Innovációs és Technológiai Minisztérium, a Nemzeti Kutatási, Innovációs és Fejlesztési Hivatal, valamint a felsőoktatási intézmények által a különböző tudományterületeken az úgynevezett „Nemzeti Laboratórium" projekt által, amelynek a nemzetbiztonsági kutatások témakörében a Nemzeti Közszolgálati Egyetem lenne a felelőse.

Támogatni kell a kormányzatnak a K+F eredmények, technológiák bevezetését, alkalmazását a védelmi ágazatban. „A szövetségi ügynökségeknek és a katonai szolgálatoknak költségvetésük 0,5–1%-át kell a technológia gyors integrálására fordítaniuk."[8]

Technológiai szövetségek és ökoszisztémák létrehozása. Ez magában foglalja a technológiai szövetségek létrehozását a kritikus feltörekvő technológiák felhasználására és irányítására, együttműködés a kereskedelmi partnerekkel a biztonságos és szabad adatáramlás kapcsán, valamint a közös technológiai szabványok kidolgozásának előmozdítása érdekében. Ösztönözni kell az amerikai vállalatokat, hogy fektessenek be, exportáljanak és hozzanak létre kutatási és fejlesztési partnerségeket a cégekkel szerte a világon. Nemzetközi együttműködésre kell törekedni, tudományos és technológiai partnerségek hálózatát fejleszteni az élvonalbeli technológiák alkalmazására olyan globális kihívásokra, mint például az éghajlatváltozás.

Magyarországon a már korábban említett „Nemzeti Laboratórium" projekt keretében az egyetemeken a nemzetközi tudományos láthatóság megerősítése érdekében nemzetbiztonsági témakörben kutatócsoportok bekapcsolásával interdiszciplináris tudományos és technológiai kihívásokat célzó kutatási tevékenységek támogatására nyílna lehetőség a kormány által, továbbá nemzetközi szinten is elismert kutatóközpontot alakíthatnak ki.

Adatkezelés vs. adatvédelem

Az adatkezelés globális architektúrájának értékelése

A digitális gazdaság fellendülése példátlan növekedést és innovációt hajtott végre az elmúlt évtizedekben, de új politikai kihívásokat is támaszt a globális vezetők számára. A következőkben a Digital Rights Ireland-ítélet és a Schrems-ítélet kapcsán vázolom az adatvédelem és a biztonság, a digitális kereskedelem

[8] Manyika et al. (2017): i. m. 12.

és a technológia kapcsolatát az adat-ökoszisztéma megértése érdekében, valamint azt, hogy ezen ítéletek kapcsán milyen jogszabályi módosítások képzelhetők el. A cél az adatvédelmi törvények legfontosabb kihívásainak feltárása mind a nemzetek, mind az EU szintjén, amelyeket a tömeges megfigyelés során le kell küzdeni, hogy az állampolgárok/magánélet és az államok/nemzetbiztonság között megfelelő egyensúlyt lehessen fenntartani.

Snowden[9] 2013-ban hozott nyilvánosságra olyan szigorúan titkos NSA-dokumentumokat, amelyekből kiderült, hogy az amerikai titkosszolgálatok széles körben megfigyelik az emberek mobiltelefon-hívásait és internetes tevékenységét, ezzel a magánélet és a biztonság kérdését a nyilvános reflektorfénybe állítva. Ezek kihangsúlyozták az erős adatvédelmi keret szükségességét. Ugyanakkor a biztonsági aggályok és a terrortámadások elleni küzdelemre való hivatkozás gyengítheti a magánélet és az adatvédelem szigorát.

Az Európai Unió Bírósága (EUB) két kiemelkedő ítélete, nevezetesen a Digital Rights Ireland-ítélet, amely hatálytalanítja az adatvédelmi irányelvet, és a Schrems-ítélet, amely érvényteleníti a Safe Harbour-határozatot,[10] amely a transzatlanti adattovábbítás jogalapját képezi, lettek azok a döntések, amelyeknek messzemenő hatása volt az EU és a nemzeti adatvédelmi mechanizmusokra, valamint a határokon átnyúló adattovábbítási keretre is. A határozatok jelentősége abban állt, hogy meghatározták a magánélethez és az adatvédelemhez való jogot a digitális tömegmegfigyelés keretében, az USA részére átadott személyes adatok kapcsán az európai állampolgárok esetében.

Az EUB számos mérföldkőnek számító ítéletet fogadott el annak értékelésére, hogy az adatkezelés és a személyes adatok összegyűjtése összhangban álljon a 2004-ben meghatározott magánélethez való joggal és az adatvédelemmel. Az EUB 2014 áprilisában a Digital Rights Ireland-ítéletben[11] megsemmisítette az adatmegőrzési irányelvet.

A Digital Rights Ireland-ügyben 2014. április 8-án az EUB megvizsgálta a 2006/24/EK irányelv (adatmegőrzési irányelv) összeegyeztethetőségét a Charta 7. és 8. cikkével. Az irányelv kötelezte az elektronikus hírközlési szolgáltatókat,

[9] Edward Joseph Snowden (Elizabeth City, Észak-Karolina, USA, 1983. június 21.) amerikai számítógépes szakember, volt CIA-alkalmazott.

[10] Az Egyesült Államokba menő adatforgalom biztonságáról szóló Safe Harbour- (biztonságos kikötő) megállapodás.

[11] Európai Unió Bírósága, C-293/12. és C-594/12. sz. Digital Rights Ireland és Seitlinger és társai egyesített ügyek.

hogy a forgalommal és a helymeghatározással kapcsolatos adatokat legalább hat és legfeljebb 24 hónapig megőrizzék, és hogy az illetékes nemzeti hatóságok számára hozzáférést biztosítsanak ezen adatokhoz súlyos bűncselekmények megelőzése, felderítése, kivizsgálása és büntetőeljárás alá vonása érdekében. Az irányelv nem engedélyezte az elektronikus kommunikáció tartalmának megőrzését. Az EUB megjegyezte, hogy az irányelv alapján a szolgáltatók által megőrzendő adatok tartalmazzák a közlés forrásának és címzettjének megtalálásához és azonosításához, továbbá valamely közlés napjának, időpontjának, időtartamának meghatározásához szükséges adatokat, a hívó telefonszámát és a hívott számot, valamint az IP-címet. Ezek az adatok

> „együttesen véve, igen pontos következtetések levonását tehetik lehetővé azon személyek magánélete vonatkozásában, akiknek az adatait megőrizték, így például a napi szokások, az állandó vagy ideiglenes tartózkodási helyek, a napi vagy egyéb helyváltoztatások, a gyakorolt tevékenységek, az e személyek társadalmi kapcsolatai és az általuk látogatott társadalmi közegek tekintetében”.[12]

Ezért a személyes adatok irányelv szerinti megőrzése a magánélet és a személyes adatok védelméhez való jogba történő különösen súlyos beavatkozásnak minősült. Az EUB azonban úgy vélte, hogy a beavatkozás nem befolyásolta hátrányosan e jogok lényegét. A magánélethez való jogot illetően nem sérült a jog lényeges tartalma, mivel az irányelv nem tette lehetővé magának az elektronikus közlések tartalmának a megismerését. Hasonlóképpen, a személyes adatok védelméhez való jog lényege sem sérült, mivel az irányelv előírta az elektronikus hírközlési szolgáltatók számára bizonyos adatvédelmi és adatbiztonsági elvek betartását, illetve e célból megfelelő technikai és szervezési intézkedések megvalósítását. A Bíróság döntött a nyilvánosan elérhető elektronikus hírközlési szolgáltatások nyújtása, illetve a nyilvános hírközlő hálózatok szolgáltatása keretében előállított vagy feldolgozott adatok megőrzéséről szóló 2006/24/EK európai parlamenti és tanácsi irányelv érvénytelenségéről. Az EU Bírósága ebben az ítéletben utalt arra, hogy az arányosság elve megköveteli, hogy az uniós intézmények aktusai alkalmasak legyenek a szóban forgó szabályozás által kitűzött jogszerű célok elérésére, és ne haladják meg az e célok eléréséhez szükséges mértéket. E feltételek tiszteletben tartásának bírósági felülvizsgálatát tekintve elmondható, hogy ha alapvető jogokba való beavatkozásról van szó, az uniós jogalkotó mérlegelési jogkörének terjedelme korlátozott lehet bizonyos körülményektől

[12] C-293/12. és C-594/12. sz. Digital Rights Ireland és Seitlinger és társai egyesített ügyek, 21.

függően, amelyek között szerepel többek között az érintett terület, a szóban forgó, Charta által biztosított jog jellege, a beavatkozás jellege és súlyossága, valamint annak célja. A szóban forgó Digital Rights Ireland-ügyben a Bíróság kimondta, hogy – figyelembe véve egyrészről azt a fontos szerepet, amelyet a személyes adatok védelme tölt be a magánélet tiszteletben tartásához való alapvető jog tekintetében, másrészről pedig az e jogot érintő, a 2006/24/EK irányelv által megvalósított beavatkozás mértékét és súlyosságát – az uniós jogalkotó mérlegelési jogköre korlátozott, és ezért azt szigorú felülvizsgálatnak kell alávetni.[13]

A Bíróság 2015. október 6-án hozott ítéletet a Schrems-ügyben.[14] Az ítélet az egyének védelmével foglalkozott személyes adataik harmadik országba – az adott esetben az Egyesült Államokba – továbbítását illetően. Schrems, egy osztrák állampolgár, aki éveken keresztül Facebook-felhasználó volt, panaszt nyújtott be az ír adatvédelmi felügyeleti hatóságnál, amelyben kifogásolta személyes adatainak továbbítását a Facebook ír leányvállalatától a Facebook Inc. vállalat részére, és az USA-ban lévő szerverekre, ahol azokat kezelték. Azzal érvelt, hogy figyelemmel Edward Snowdenre, a megfigyelési visszaélést bejelentő amerikai személy által 2013-ban az Egyesült Államok hírszerző szolgálatainak a tevékenységeire vonatkozóan kiszivárogtatott információkra, az Egyesült Államok joga és gyakorlata nem biztosít elégséges védelmet az amerikai területre továbbított személyes adatok tekintetében. Snowden feltárta, hogy a National Security Agency (Nemzetbiztonsági Ügynökség) közvetlenül rákapcsolódik cégek, például a Facebook szervereire, és elolvashatja a csevegések és privát üzenetek tartalmát.

Az adatok USA-ba történő továbbítása egy 2000-ben elfogadott bizottsági megfelelőségi határozaton alapult, amely lehetővé teszi az adattovábbítást azon amerikai vállalatok számára, amelyek nyilatkoztak arról, hogy az EU-ból továbbított személyes adatokat védik, és megfelelnek az úgynevezett „biztonságos kikötő" adatvédelmi elveknek. Amikor az ügyet az EUB elé vitték, a Bíróság a Charta alapján vizsgálta meg a bizottsági határozatot. Emlékeztetett arra, hogy az EU-ban az alapjogok védelmével szemben támasztott követelmény, hogy az érintett jogokra vonatkozó eltérések és korlátozások a feltétlen szükségesre korlátozódjanak. Az EUB az olyan szabályozást, amely lehetővé teszi a közjogi hatóságok számára, hogy általános jelleggel hozzáférjenek az elektronikus kommunikációk tartalmához, úgy tekintette, hogy az „a magánélet tiszteletben

[13] C-293/12. és C-594/12. sz. Digital Rights Ireland és Seitlinger és társai egyesített ügyek, 17.
[14] EUB, Maximillian Schrems kontra Data Protection Commissioner, C-362/14. sz. ügy.

tartásához való, a Charta 7. cikkében biztosított alapvető jog lényegét sérti". A jogot a lényegétől fosztaná meg, ha az amerikai hatóságok válogatás nélkül hozzáférhetnének az elektronikus kommunikációhoz anélkül, hogy szükség lenne az érintett egyénekkel konkrét kapcsolatban nemzetbiztonsági vagy bűnmegelőzési megfontolásokra alapított objektív igazolásra, és anélkül hogy e megfigyelési gyakorlatokhoz megfelelő visszaélésekkel szembeni garanciák társulnának.

Ráadásul az EUB megállapította, hogy „az olyan szabályozás, amely nem biztosítja a jogalany számára a jogorvoslat lehetőségét abból a célból, hogy a rá vonatkozó személyes adatokhoz hozzáférést kapjon, vagy azokat helyesbíttesse, illetve töröltesse",[15] összeegyeztethetetlen a hatékony bírói jogvédelemhez való alapjoggal (Charta 47. cikk). Ezért a biztonságos kikötőről szóló határozat lényegét tekintve nem biztosította az alapjogoknak a Charta fényében értelmezett irányelv alapján az EU-ban garantált védelmi szinttel egyenértékű védelmét. Az EUB következésképp érvénytelenítette a határozatot.

Az EUB-ítéletek kapcsán néhány kérdéskört kívánok vizsgálni a magánélettel és a nemzetbiztonsággal kapcsolatos alapvető kérdések és kihívások témakörében. A terrorizmus elleni küzdelem szükségessége, különösen a szeptember 11-i támadások után, vezetett a tömeges megfigyelési gyakorlatok bevezetéséhez mind az EU-ban, mind az Egyesült Államokban. Fontos megjegyezni, hogy az EU adatvédelmi szabályai nemcsak a gazdasági fejlődés fontos eszközévé váltak, hanem a nemzetbiztonsági célok megvalósítójává is, ily módon befolyásolva a magánélethez való jogot. Ennek kapcsán szükséges feltárni az adatvédelmi törvény és a nemzeti, valamint az uniós szintű politikai kihívásokat, amelyeket a tömeges digitális megfigyelésre adott válaszként le kell küzdeni annak érdekében, hogy fenntartható legyen a megfelelő egyensúly a magánélet és a nemzetbiztonság között.

A biztonság mint az EU adatvédelmi szabályainak célja

Az információs és kommunikációs technológiák ágazatának gyors fejlődése új lehetőségeket, de új kihívásokat is felszínre hozott. A határok nélküli információkhoz való hozzáférés képessége döntő jelentőségű a társadalmi és gazdasági kölcsönhatások és a technológiai fejlődés szempontjából. Az adatfeldolgozás

[15] C-362/14. sz. ügy 24.

növekvő gazdasági jelentősége azonban aggodalmakat vet fel az alapvető jogok hatékony védelme miatt az információs társadalomban.

Az új uniós adatvédelmi szabályok végleges elfogadása jelentős lépést tett az uniós polgárok alapvető jogainak a digitális korban történő megerősítése érdekében. Az adatvédelmi csomag magában foglalja az általános adatvédelmi rendeletet,[16] amely 2016. május 24-én lépett hatályba, és 2018. május 25-től alkalmazandó. Ez magában foglalja a rendőrség és a büntető igazságügyi hatóságok adatvédelmi irányelvét,[17] amely 2016. május 5-én lépett hatályba és amelyeket az EU-tagállamoknak 2018. május 6-ig kellett átültetniük a nemzeti jogukba. Ezeknek a célja az adatvédelem megfelelően magas szintjének biztosítása volt.

Hasonlóképpen, a terrorizmus elleni küzdelem szükségessége korábban olyan adatmegőrzési rendszerek bevezetéséhez vezetett, amelyek lehetővé tették a kommunikáció állami megfigyelését biztonsági célokból. Az adatmegőrzési irányelvet a madridi (2004) és a londoni (2005) terroristatámadásokra adott válaszként hozott sürgős terrorizmusellenes intézkedésként vezették be. Az alapvető jogok tiszteletben tartásával kapcsolatos aggodalmak ellenére hatalmas politikai nyomás alatt gyorsan elfogadták, és 2006-ban lépett hatályba. Az adatmegőrzési irányelv a tagállamokat arra kötelezte, hogy a távközlési és internetszolgáltatókat kötelezzék a forgalmi és helymeghatározási adatok tárolására a vezetékes és a mobiltelefon, valamint az internetes e-mail-kommunikáció vonatkozásában legalább hat hónapig, de legfeljebb két évig, és ezekhez biztosítsanak hozzáférést kérésre a bűnüldöző hatóságok számára a súlyos bűncselekmények és a terrorizmus kivizsgálása, felderítése és üldözése céljából. A Digital Rights Ireland-ügyben az EUB azonban érvénytelennek nyilvánította az adatmegőrzési irányelvet azon az alapon, hogy az indokolatlanul sérti az alapvető jogokat.

[16] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyek védelméről a személyes adatok feldolgozása során és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről. EK (általános adatvédelmi rendelet) [2016]. HL L 119.

[17] Az Európai Parlament és a Tanács (EU) 2016/680 irányelve (2016. április 27.) a természetes személyek védelméről a személyes adatoknak az illetékes hatóságok általi feldolgozása során az ilyen személyek megelőzése, kivizsgálása, felderítése vagy üldözése céljából, bűncselekmények vagy büntetőjogi szankciók végrehajtása, valamint az ilyen adatok szabad mozgásáról, valamint a 2008/977/IB tanácsi kerethatározat hatályon kívül helyezéséről miközben javítja az egész Európában a terrorizmus és más súlyos bűncselekmények elleni küzdelem terén folytatott együttműködést. A személyes adatok védelmére vonatkozó új uniós szabályok tehát a digitális egységes piaci stratégia, valamint az EU biztonsági menetrendje alapvető elősegítői.

A kommunikációs adatok megőrzését a terrorizmus elleni küzdelem eszközeként széles körben alkalmazták az Atlanti-óceánon túl is. A szeptember 11-i terrorista támadások után az Egyesült Államok egyoldalúan elkezdte kiaknázni a digitális kommunikációs technológiák sebezhetőségét az elektronikus megfigyelés és a kommunikáció lehallgatása érdekében mind az Egyesült Államokban, mind a világ más országaiban. Az USA Nemzeti Biztonsági Ügynöksége (NSA) volt alkalmazottjának, Edward Snowdennek a 2013. évi leleplezése során felfedték a korábban elképzelhetetlen léptékű globális megfigyelését az Egyesült Államok állampolgárainak és más, külföldi személyek telekommunikációjának és adatáramlásának, az úgynevezett „Öt Szem"[18] hírszerzési információhálózat segítségével. Az „Öt Szem" magában foglalja az Egyesült Királyságot, az Egyesült Államokat, Ausztráliát, Kanadát és Új-Zélandot, az NSA irányításával, valamint kiterjedt együttműködés jött létre az EU különböző tagállamainak hírszerző hatóságai között, különösen az Egyesült Királyságban, Németországban és az Egyesült Államokban.

Ezek a felfedések globális aggodalomra adtak okot az emberi jogokra gyakorolt negatív hatásaik miatt. A nemzetközi közösség, különösen az Egyesült Nemzetek Szervezete (ENSZ) szervei komoly aggodalommal figyelték a kommunikáció megfigyelésének és lehallgatásának, valamint a személyes adatok gyűjtésének kialakult gyakorlatát. A digitális kommunikációs technológiák jogellenes vagy önkényes megfigyelésének és elfogásának kockázata visszatarthatja az innovációt és alááshatja a digitális gazdaság nyújtotta lehetőségeket, mivel a magánélet védelmét kritikusnak tekintik a bizalom szempontjából, amely különösen fontos eszköz a globális online környezetben.

Az extraterritoriális digitális tömegmegfigyelés feltárása szintén befolyásolta a transzatlanti kapcsolatokat, és kérdéseket vetett fel az Egyesült Államok és az EU közötti hosszú távú adattovábbítási megállapodások jogszerűségéről. A személyes adatok harmadik országokba történő továbbításának fő szabályait az EU adatvédelmi irányelvének 25. és 26. cikke tartalmazza, amely meghatározza azt az alapelvet, miszerint a személyes adatok átadására csak akkor kerülhet sor, ha a harmadik ország megfelelő szintű védelmet biztosít (Schrems-ügy). Nevezetesen ebben az esetben az alapvető kérdés az volt, hogy az Egyesült Államok biztosítja-e az adatvédelem megfelelő szintjét az uniós polgárok személyes adataival való visszaélésének megakadályozása érdekében, mivel a „biztonságos kikötő" szabályait a nemzetbiztonsági követelmények felülbírálhatják.

[18] UKUSA-egyezmény, Five Eyes, FVEY.

A magánélet védelméhez és az adatvédelemhez fűződő beavatkozások indokolása a nemzetbiztonság érdekében

Az EUB mindkét ítéletében elismerte, hogy a magánélethez és az adatvédelemhez való jog beavatkozása a Charta 52. cikkének (1) bekezdése alapján szigorú szükségesség és arányosság vizsgálatát követeli meg. E cikk értelmében korlátozásokat lehet előírni az alapvető jogok és szabadságok gyakorlására, mindaddig, amíg ezeket a korlátozásokat törvény írja elő, vizsgálva azt, hogy tiszteletben tartják e jogok és szabadságok lényegét, és az arányosság elvére figyelemmel szükségesek-e, és valóban megfelelnek az EU által elismert általános érdekű céloknak, vagy mások jogai és szabadságai védelmének szükségességéhez. A Schrems-ügyben kijelentette, hogy az Egyesült Államok jogszabályai, a hatóságok általános hozzáférési lehetősége a kommunikációs adatok tartalmához veszélyeztetik a magánélethez való jog lényegét.

Az EUB felhívta a figyelmet a magánélet és az adatvédelem fogalmai közötti különbségekre annak az elméletnek megfelelően, hogy a magánélethez való jog „optikai eszköz", amely tiltja a behatolást a magánszférába, míg az adatvédelemhez való jog „átláthatósági eszköz", amely a személyes adatok kezelésére vonatkozik, és felhatalmazza az egyént az adatok és a felhasználásuk bizonyos szintű ellenőrzésére.

Az ítéletek következményei

Az adatvédelem következményei a tagállamokban

Az EUB ítéletei jelentősen befolyásolják a tagállami adatvédelmi törvényeket, valamint a tagállamok adattovábbítási gyakorlatait is. A Digital Rights Ireland-ítélet eltérő igazságügyi és jogalkotási reakciókat váltott ki a tagállamok között a nemzeti adatvédelmi törvények tekintetében. A Schrems-ítélet emellett felhívta a figyelmet arra, hogy politikai megállapodásra kell jutni a tagállamok között az állami felügyeleti kérdésekben. Az EUB jelentősen megerősítette az adatvédelmi hatóságok szerepét azáltal, hogy felhatalmazta őket arra, hogy megvizsgálják a harmadik országok adatvédelmének szintjét az alapvető jogok megsértésére alapított egyedi igények kezelése érdekében. A hatóságok korlátozhatják az adattovábbítást, amennyiben az alapvető jogok megsértését találják.

Az adatvédelem következményei az EU-ban

Az EUB ítéleteiben körvonalazott alapelveket figyelembe kellett venni az adatkezelő rendszerek vonatkozásában. A személyes adatok továbbítását lehetővé tevő, harmadik országokkal kötött megállapodásokat szintén felül kellett vizsgálni a Schrems- és a Digital Rights Ireland-ítéletek fényében, például az Egyesült Államokkal, Kanadával és Ausztráliával kötött PNR-megállapodásokkal és az EU–USA TFTP[19] megállapodással kapcsolatban. A Schrems-ítélet jelentősen felgyorsította a személyes adatok transzatlanti cseréjére vonatkozó új adatvédelmi rendszerről folytatott tárgyalásokat. Az Európai Bizottság 2016. július 12-én elfogadta az EU – Egyesült Államok adatvédelmi pajzsot, amely felváltotta a korábbi, az EUB által érvénytelenített Safe Harbour-határozatot.

A fent említett kihívásokat, amelyekkel az EU szembesül, a jelenlegi nemzetközi kontextusban kell vizsgálni, ahol az adatok tömeges megjelenése és a növekvő biztonsági igények új megoldásokat igényelnek. A megfigyelésre és a nemzetközi adatvédelmi normákra vonatkozó új nemzetközi normák kidolgozására irányuló globális kezdeményezések lehetnek a nemzetbiztonság és a magánélet közötti közösen elfogadott egyensúly megteremtésének új eszközei.

Következtetések

Az EU adatvédelmi szabályai nemcsak fontos gazdasági fejlesztési eszközökké váltak, hanem a nemzetbiztonság elősegítőjévé is. A növekvő biztonsági fenyegetések az EU-polgárok személyes adatainak belföldi és extraterritoriális digitális megfigyelését eredményezte, amely komoly aggodalmakat vet fel az alapvető jogok hatékony védelme miatt. Ezek az aggodalmak az EUB-nál jelentkeztek elsőnek, amely két mérföldkőnek mondott – korábban is említett – ítéletet fogadott el, nevezetesen a Digital Rights Ireland-ítéletet és a Schrems-ítéletet, amelyeknek nagy jelentősége van a Charta 7. és 8. cikkében rögzített, magánélethez és az adatvédelemhez való jog megerősítése szempontjából.

Az EUB mindkét esetben szigorú szükségesség és arányosság követelménye vizsgálatát követeli meg az alapvető jogokba való beavatkozás értékelésekor

[19] A terrorizmus finanszírozásának felderítését célzó program (*Terrorist Finance Tracking Programme,* TFTP) keretében pénzügyi adatok átadása ellenőrzött keretek között.

a nemzetbiztonság érdekében, és ösztönzi az erős eljárási biztosítékok, például a független felügyeleti mechanizmusok és a hatékony jogorvoslatok alkalmazását tömeges adatgyűjtés és a személyes adatok cseréje során. E garanciák ellenére azonban az egyének nemzetbiztonsági célú nagyszámú és válogatás nélküli felügyelete nem tekinthető indokoltnak. Az EUB szerint további tisztázást igényel annak kérdése, hogy a tömegmegfigyelési intézkedések milyen mértékben tartják tiszteletben a magánélethez és az adatvédelemhez való jog lényegét, és összhangban állnak-e ezekkel a jogokkal.[20]

Az EUB ítéletei politikai megállapodásra szólítanak fel az EU tagállamai között a tömeges megfigyelés kérdésében. A Digital Rights Ireland-ítélet eltérő igazságügyi és jogalkotási reakciókat váltott ki az EU-tagállamokban; ugyanakkor lassan felülvizsgálják a tagállamok a nemzeti adatmegőrzési törvényeket a meghatározott alapjogi normák fényében. Hasonlóképpen, a Schrems-ítélet, amely felhatalmazza a nemzeti adatvédelmi hatóságokat arra, hogy adatküldés esetén megvizsgálják a harmadik országok adatvédelmének szintjét, eltérő személyes adatvédelmi előírások alkalmazását eredményezheti. Az EUB ítéleteit figyelembe kell venni minden olyan létező vagy tervezett uniós jogszabály vonatkozásában, amely a személyes adatok nagyszabású gyűjtését és feldolgozását vonja maga után. Látni kell, hogy az EU-n belüli adatmegőrzési mechanizmusok, különösen az EU PNR-irányelv, valamint a harmadik országokkal kötött PNR-megállapodások[21] megfelelnek-e a Digital Rights Ireland-ítéletben megállapított követelményeknek. Figyelembe véve a Schrems-ítéletnek a transzatlanti adattovábbítási keretre gyakorolt hatását, az EU–USA adatvédelmi pajzs,[22] bár új eljárási biztosítékokat vezet be, nem lesz képes hatékony védelmet nyújtani a nemzetbiztonsági célokból történő megfigyelés ellen. Ezek a kihívások új megközelítéseket igényelnek mind az EU-n belül, mind azon kívül, hogy meghatározzák a megfelelő korlátokat a tömeges digitális megfigyelés számára, és megtalálják a nemzetbiztonság és a magánélet közötti közösen elfogadott egyensúlyt.

[20] Irena Nesterova: *Crisis of Privacy and Sacrifice of Personal Data in the Name of National Security: The CJEU Rulings Strengthening EU Data Protection Standards.* European Society of International Law, (ESIL) 2016 Annual Conference (Riga). 2017.

[21] Utasnyilvántartási adatállomány.

[22] Az adatvédelmi pajzs akkor engedi meg a személyes adatok továbbítását az EU-ból egy amerikai vállalathoz, ha az amerikai vállalat a személyes adatok kezelése (például felhasználása, tárolása és továbbadása) során szigorú adatvédelmi szabályok és biztosítékok szerint jár el.

Felhasznált irodalom

Arkin, William M. – Alexa O'Brien: *The Most Militarized Universities in America: A VICE News,* 2015. november 6. Online: www.vice.com/en_us/article/j59g5b/the-most-militarized-universities-in-america-a-vice-news-investigation

Balogh László Levente: Állam és erőszak. *Politikatudományi Szemle,* 20. (2011), 1. 119–132. Online: www.poltudszemle.hu/szamok/2011_1szam/balogh.pdf

Bailey, Ronald: Is Russia's Surveillance State Being Modelled on the West? New Russian Anti-encryption and Data Retention Laws Look Sadly Familiar. *Reason,* 2016. július 22. Online: https://reason.com/archives/2016/07/22/is-russias-surveillance-state-being-mode/print

Bán Ernő: *Kémek – hazaárulók.* Budapest, Zrínyi, 1966.

Barker, Anne: Captagon: Evidence Paris Attackers Used 'Jihadist's Drug' Favoured by Islamic State Fighters. *ABC News,* 2015. november 25. Online: www.abc.net.au/news/2015-11-24/captagon-the-drug-that-kept-the-paris-attackers-calm/6970464?nw=0&r=Gallery

Besenyei Lajos: A generációváltás forradalma. *Opus et Educatio,* 3. (2016), 4. 371–378. Online: https://doi.org/10.3311/ope.19

Beke József: Az Európai Unió hírszerző képességének technikai támogatása. *Nemzetbiztonsági Szemle,* 6. (2018), 2. 56–68. Online: https://epa.oszk.hu/02500/02538/00023/pdf/EPA02538_nemzetbiztonsagi_szemle_2018_02_056-068.pdf

Béres János: A hírszerzés feladatrendszere. In Dobák Imre (szerk.): *A nemzetbiztonság általános elmélete.* Budapest, Nemzeti Közszolgálati Egyetem, 2014. 117–128. Online: http://m.ludita.uni-nke.hu/repozitorium/bitstream/handle/11410/8567/Teljes%20sz%C3%B6veg%21?sequence=1&isAllowed=y

Béres János (szerk.): *Külföldi nemzetbiztonsági szolgálatok.* Budapest, Zrínyi, 2018.

Bischoff, Paul: The word's most-surveilled cities. *Comparitech,* 2019. Online: www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/

Boda József – Regényi Kund (szerk.): *A hírszerzés története az ókortól napjainkig.* Budapest, Dialóg Campus, 2019. Online: https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/12692/web_PDF_Hirszerzes_tortenete_okortol_napjainkig.pdf;jsessionid=0572E51ED460A99D94B07ADDAE7657EA?sequence=1

Bond, David: Britain Preparing to Launch New Cyber Warfare Unit. *Financial Times,* 2018. szeptember 21. Online: www.ft.com/content/eef717f2-bb6e-11e8-8274-55b72926558f

Börcsök András – Vida Csaba: A nemzetbiztonsági szolgálatok rendszere (Nemzetközi gyakorlat a nemzetbiztonsági rendszer kialakítására). *Nemzetbiztonsági Szemle,* 2. (2014), 1. 63–100. Online: https://folyoirat.ludovika.hu/index.php/nbsz/article/view/2066

Buda András: Generációk, társadalmi csoportok a 21. században. *Magyar Tudomány,* 180. (2019), 1. 120–129. Online: https://doi.org/10.1556/2065.180.2019.1.12

Bulgakov, Mihail A.: *A Mester és Margarita.* (ford. Szőllősy Klára) Budapest, Európa, 2019.

Burds, Jeffrey: *The Second Oldest Profession. A World History of Espionage.* Boston, Recorded Books, 2011.

Bures, Oldrich – Helena Carrapico: Private Security beyond Private Military and Security Companies: Exploring Diversity within Private-Public Collaborations and its Consequences for Security Governance. *Crime, Law and Social Change,* 67, (2017), 3. 229–243. Online: https://doi.org/10.1007/s10611-016-9651-5

Brown, Dalvin: The U.S. Navy banned TikTok from Government-issued Smartphones over Cybersecurity Concerns. *USA Today,* 2019. december 23. Online: https://eu.usatoday.com/story/tech/2019/12/23/us-navy-bans-personnel-using-tiktok-government-issued-phones/2732203001/

Chikán Attila: *Vállalatgazdaságtan.* Budapest, Aula, 2008.

Cornely, David Dwaine: *Leadership and Security: Factors that Support or Prevent Successful Integration into Research and Development Organizations.* Dissertation Presented in Partial Fulfillment of the Requirements for the Degree Doctor of Management in Organizational Leadership. University of Phoenix, 2003.

Contentgroup: Social Media on the Campaign Trail: Barack Obama and Donald Trump. (2017). Online: https://contentgroup.com.au/2017/09/social-media-campaign-trail-obama-trump/

Csepeli György: *Szociálpszichológia.* Budapest, Osiris, 2001.

Csiki Tamás – Tálas Péter: A védelmi beszerzés és kutatás-fejlesztés kapcsolata a védelmi tervezés rendszerében – nemzetközi tapasztalatok. *Nemzet és Biztonság,* (2013), 3–4. 107–142. Online: www.nemzetesbiztonsag.hu/cikkek/nb_2013_3-4_09_csiki_tamas-talas_peter_-_a_vedelmi_beszerzes_es_kutatas-fejlesztes_kapcsolata_a_vedelmi_tervezes_rendszereben_-_nemzetkozi_tapasztalatok.pdf

Dahl, Erik J.: *Warning of Terror: Explaning the Failure of Intelligence against Terrorism.* Master of Arts in Law and Diplomacy Thesis, The Fletcher School, 2004. Online: https://dl.tufts.edu/pdfviewer/nc580z70h/ks65hq04h

Dalha, Tenzin: Beijing's Export of Surveillance Technology. *Modern Diplomacy,* 2020. január 7. Online: https://moderndiplomacy.eu/2020/01/07/beijings-export-of-surveillance-technology/

Dhami, Mandeep K.: Behavioural Science Support for JTRIG'S (Joint Threat Research and Intelligence Groups) Effects and Online HUMINT Operations. 2011. *The Intercept,* 2015. június 22. Online: https://theintercept.com/document/2015/06/22/behavioural-science-support-jtrig/

Deák András György: Kevés egyezmény, kívánt eredmény? – Trump kínai „vámháborújának" mérlege. *NKE Stratégiai Védelmi Kutatóintézet Elemzések,* (2020), 8. 1–12. Online: https://tinyurl.com/3w5c9je7

Deák Veronika: Social engineering alapú információszerzés a kibertérben megvalósuló lélektani műveletek során. *Hadtudományi Szemle,* 12. (2019), 3. 95–111. Online: https://doi.org/10.32563/hsz.2019.3.6

Dobák Imre: Technológiai fejlődés – titkosszolgálatok. In Fekete Károly (szerk.): *Kommunikáció.* Budapest, Nemzeti Közszolgálati Egyetem, 2013. 61–71.

Dobák Imre (szerk.): *A nemzetbiztonság általános elmélete.* Budapest, Nemzeti Közszolgálati Egyetem, 2014. Online: http://m.ludita.uni-nke.hu/repozitorium/bitstream/handle/11410/8567/Teljes%20sz%C3%B6veg%21?sequence=1&isAllowed=y

Dobák Imre: Technikai típusú információgyűjtés a változó biztonsági kihívások tükrében. *Hadmérnök,* 12. (2017), 2. 235–249. Online: http://hadmernok.hu/172_19_dobak.pdf

Dobák Imre: OSINT – Gondolatok a kérdéskörhöz. *Nemzetbiztonsági szemle,* 7. (2019), 2. 83–93. Online: https://doi.org/10.32561/nsz.2019.2.7

Dobák Imre – Regényi Kund (szerk.): *Szakmatörténeti szemelvények.* Budapest, Nemzetbiztonsági Szakszolgálat, 2014.

Dodsworth, Francis: Police and the Prevention of Crime: Commerce, Temptation and the Corruption of the Body Politic, from Fielding to Colquhoun. *British Journal of Criminology,* 47. (2007), 3. 439–454. Online: https://doi.org/10.1093/bjc/azl054

Domokos Erika: Oroszország letilt egy üzenetküldő szolgáltatást. *Napi.hu,* 2018. április 13. Online: www.napi.hu/tech/oroszorszag_letilt_egy_uzenetkuldo_szolgaltatast.660552.html

Drobinina, Ekaterina: Russian Search-Engine Yandex Passed Information to FSB. *BBC News,* 2011. május 3. Online: www.bbc.com/news/business-13274443

Drusza Tamás: A szervezeti kultúra jelentősége a generációs kihívás és a nemzetbiztonsági szolgálatok fejlesztése szempontjából. *Nemzetbiztonsági Szemle,* 6. (2018), 2. 69–89. Online: https://folyoirat.ludovika.hu/index.php/nbsz/article/view/1591

Drusza Tamás: Jövőbeni kihívások a (polgári) nemzetbiztonsági elhárítás területén. In Drusza Tamás (szerk.): *A magyar elhárítás fejlődése.* Budapest, Dialóg Campus, 2019. 211–238.

Eftimiades, Nicolas: Uncovering Chinese Espionage in the US. *The Diplomat,* 2018. november 28. Online: https://thediplomat.com/2018/11/uncovering-chinese-espionage-in-the-us/

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

Európai Unió Alapjogi Ügynöksége – Európa Tanács: *Európai adatvédelmi jogi kézikönyv* 2018. évi kiadás, Luxembourg, Az Európai Unió Kiadóhivatala, 2019. Online: www.echr.coe.int/Documents/Handbook_data_protection_HUN.pdf

Eszteri Dániel: A mesterséges intelligencia fejlesztésének és üzemeltetésének egyes felelősségi kérdései. *Infokommunikáció és Jog,* 12. (2015), 62–63. 45–57.

Finszter Géza: Állambiztonság – nemzetbiztonság. *Nemzetbiztonsági Szemle,* 7. (2019), 3. 98–117. Online: https://doi.org/10.32561/nsz.2019.3.8

Firsing, Scott: The Growing Link between Intelligence Communities and Academia. *The Conversation,* 2015. szeptember 30. Online: http://theconversation.com/the-growing-link-between-intelligence-communities-and-academia-47184

Foulkes, Imogen: Swiss Crypto AG Spying Scandal Shakes Reputation for Neutrality. *BBC News,* 2020. február 16. Online: www.bbc.com/news/world-europe-51487856

Fukuyama, Francis: *A történelem vége és az utolsó ember.* Budapest, Európa, 2014.

Galántai Zoltán: Big data, tudomány, kauzalitás. *Információs Társadalom,* 16. (2016), 2. 32–43. Online: https://doi.org/10.22503/inftars.XVI.2016.2.2

Gearon, Liam: The Counter-Terrorist Campus: Securitisation Theory and University Securitisation – Three Models. *Transformation in Higher Education,* 2. (2017), a13. 2519–5638. Online: https://doi.org/10.4102/the.v2i0.13

Green, J. J.: The Fog of Espionage. Part 3: 'A Bewildering Variety of Poisonous Snakes'. *Wtop News,* 2019. szeptember 27. Online: https://wtop.com/j-j-green-national/2019/09/the-fog-of-espionage-part-3-a-bewildering-variety-of-poisonous-snakes/

Greenwald, Glenn: *A Snowden-ügy: korunk legnagyobb nemzetbiztonsági botránya*. Budapest, HVG, 2014.

Gutheil, Mirja – Quentin Liger – Aurélie Heetman – James Eager – Max Crawford: *Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices*. Study for the LIBE Committee, European Union, 2017. Online: www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf

Haig Zsolt – Kovács László – Ványa László – Vass Sándor: *Elektronikai hadviselés.* Budapest, Nemzeti Közszolgálati Egyetem, 2014. Online: http://m.ludita.uni-nke.hu/repozitorium/bitstream/handle/11410/10964/webview.pdf?sequence=1&isAllowed=y

Harris, Matthew: The Limit of Intelligence Gathering: Gianni Vattimo and the Need to Monitor 'Violent' Thinkers. In Jai Galliott – Warren Reed (szerk.): *Ethics and the future of spying, Technology, National Security and Intelligence Collection*. Routledge, 2016. 27–38.

Héjja István: Nemzetbiztonsági szervezeti modellek. In Dobák Imre: *A nemzetbiztonság általános elmélete.* Budapest, Nemzeti Közszolgálati Egyetem, 2014. 57–72.

Huntington, Samuel P.: *A civilizációk összecsapása és a világrend átalakulása.* Budapest, Európa, 2019.

Jávor Endre: A hír, az adat, az információ és a dokumentáció fogalma, helye, szerepe a döntéshozatalban. *Nemzetbiztonsági Szemle,* 5. (2017), 3. 36–60. Online: https://folyoirat.ludovika.hu/index.php/nbsz/article/view/1679

Jasenszky Nándor (szerk.): *Mindennapi biztonság.* Budapest, Terrorelhárítási Központ, 2019.

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

Joint Economic Committee: *Soviet Economy in the 1980's: Problems and Prospects Part 1.* Washington, Joint Committee Print, 1983. Online: www.jec.senate.gov/reports/97th%20Congress/Soviet%20Economy%20in%20the%201980s%20-%20Problems%20and%20Prospects%20Part%20I%20%281185%29.pdf

Kadomtsev, Andrej: 5G: A New Stage in Civilization Development amid Global Competition. *Modern Diplomacy,* 2019. december 26. Online: https://moderndiplomacy.eu/2019/12/26/5g-a-new-stage-in-civilization-development-amid-global-competition/

Kadtke, James – John Wharton: Technology and National Security: The United States at a Critical Crossroads. *Defense Horizons,* 2018. március 1. Online: https://inss.ndu.edu/Portals/68/Documents/defensehorizon/DH-84.pdf

Kampe, Christopher – Gwendolynne Reid – Paul Jones – S. Colleen – S. Sean – Kathleen M. Vogel: Bringing the National Security Agency into the Classroom: Ethical Reflections on Academia-Intelligence Agency Partnerships. *Science and Engineering Ethics,* (2019), 25. 869–898. Online: https://doi.org/10.1007/s11948-017-9938-7

Kasznár Attila: A terrorelhárítás feladatrendszere a turizmusban. In Kiglics Norbert (szerk.): *II. Turizmus és Biztonság Nemzetközi Tudományos Konferencia Konferenciakötet.* Nagykanizsa, Pannon Egyetem, 2017. 48–55. Online: https://uni-pen.hu/files/konferencia/2017/Teljes_konf_tanulmanykotet.pdf

Kenedli Tamás: A nyílt forrású információszerzés (OSINT). In Dobák Imre (szerk.): *A nemzetbiztonság általános elmélete.* Budapest, Nemzeti Közszolgálati Egyetem, 2014.

Kenyeres Ágnes (szerk.): *Magyar Életrajzi Lexikon.* Budapest, Akadémiai Kiadó, 1994.

Kis-Benedek József: A nemzetbiztonsági szolgálatok nemzetközi együttműködése *Hadtudomány,* 23. (2013), 1–2. 100–114. Online: www.mhtt.eu/hadtudomany/2013/1_2/HT_2013_1-2_mhtt.pdf

Kovács Zoltán: Az alkalmazásszolgáltatók törvényes ellenőrzésének jövője – a technológiák konvergenciájának tükrében. *Nemzetbiztonsági Szemle,* 4. (2016), 1. 79–99. Online: https://folyoirat.ludovika.hu/index.php/nbsz/article/view/1815/1105

Külgazdasági és Külügyminisztérium Magyarország Nagykövetsége, Peking, Vezetői összefoglaló, 2017–18 TET éves beszámoló.

Kris, Davis S.: Trends and Predictions in Foreign Intelligence Surveillance: The FAA and Beyond. *Hoover Institution Essay, Aegis Paper Series,* (2016), 1601. Online: www.hoover.org/sites/default/files/research/docs/kris_trendspredictions_final_v4_digital.pdf

Laufer Balázs – Takács Gergely: A HUMINT vége? *Arc és Álarc,* 2. (2018), 1–2. 175–185. Online: www.hamvasintezet.hu/wp-content/uploads/2018/10/HAMVAS_2018_TAVASZ_NYAR_net.pdf

Lenyűgöző közösségi média statisztikák I. rész. *Szubjektív,* (2018. szeptember 12.). Online: https://szubjektiv.com/lenyugozo-kozossegi-media-statisztikak-1/

Loringhoven, Arndt Freytag von: Adapting NATO intelligence in support of "One NATO". *NATO Review,* 2017. szeptember 8. Online: www.nato.int/docu/review/articles/2017/09/08/adapting-nato-intelligence-in-support-of-one-nato/index.html

Loringhoven, Arndt Freytag von: A New Era for NATO Intelligence. *NATO Review,* 2019. október 29. Online: www.nato.int/docu/review/articles/2019/10/29/a-new-era-for-nato-intelligence/index.html

Lowenthal, Mark M.: *A titkoktól a politikai döntésig.* Budapest, Antall József Tudásközpont, 2017.

Mackinnon, Amy: How Russia is Strong-Arming Apple. *Foreign Policy,* 2019. január 31. Online: https://foreignpolicy.com/2019/01/31/how-russia-is-strong-arming-apple-data-security-icloud/

Major Milán: Az orosz védelmi ipari komplexum a Szovjetunió szétesésétől napjainkig. *NKE Stratégiai Védelmi Kutatóintézet Nézőpontok,* (2020), 2. 1–10. Online: https://svkk.uni-nke.hu/document/svkk-uni-nke-hu-1506332684763/SVKK_N%C3%A9z%C5%91pontok_2020_2_Az%20orosz%20vedelmi%20ipari%20komplexum%20a%20Szovjetunio%20szetesesetol%20napja%20inkig_(Major%20M.).pdf

Manyika, James – Susan Lund – Michael Chui – Jacques Bughin – Jonathan Woetzel – Parul Batra – Ryan Ko – Saurabh Sanghvi*: Jobs Lost, Jobs Gained: What the Future of Work Will Mean for Jobs, Skills, and Wages.* McKinsey Global Institute, 2017. november 28. Online: www.mckinsey.com/featured-insights/future-of-work/jobs-lost-jobs-gained-what-the-future-of-work-will-mean-for-jobs-skills-and-wages

McPherson, Peter – Mary Sue Coleman: We Must Have Both. *Inside Higher Ed,* 2019. augusztus 5. Online: www.insidehighered.com/views/2019/08/05/research-universities-must-bolster-both-security-and-openness-opinion

M. Császár Zsuzsa – Bányai Bence – Gyura Gábor – Farkas Marcell: A nemzetközi hallgatói migráció biztonságpolitikai kockázatainak egyes aspektusai. *Nemzetbiztonsági Szemle,* 6. (2018), 3. 49–64. Online: https://folyoirat.ludovika.hu/index.php/nbsz/article/view/1498/820

Meretei Barbara: Generációs különbségek a munkahelyeken. *Vezetéstudomány,* 48. (2017), 10. 10–18. Online: https://doi.org/10.14267/VEZTUD.2017.10.02

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

Moody, Glyn: Revised Snooper's Charter Ignores Key Criticisms, Widens Police Powers Further. *Ars Technica,* 2016. március 2. Online: http://arstechnica.co.uk/tech-policy/2016/03/revised-snoopers-charter-ignores-key-criticisms-widens-police-powers-further/

Moraes, Claude*: Working Document 1 on the US and EU Surveillance Programmes and their Impact on EU Citizens Fundamental Rights.* Committee on Civil Liberties, Justice and Home Affairs, 2013. Online: www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/wd_moraes_1012434/wd_moraes_1012434en.pdf

M. Tóth Balázs – Pap András László: *A hatékonyság mítosza. Az etnikai profilalkotás alkotmányos és rendészeti kérdőjelei.* Budapest, L'Harmattan, 2012.

Nesterova, Irena: *Crisis of Privacy and Sacrifice of Personal Data in the Name of National Security: The CJEU Rulings Strengthening EU Data Protection Standards.* European Society of International Law, (ESIL) 2016 Annual Conference (Riga), 2017. Online: https://doi.org/10.2139/ssrn.2911999

Nishimura, Hiroshi – Kanoshima, Emiko – Kono, Kazuhiro: 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. 15–26. Online: https://doi.org/10.1007/978-981-13-2775-9_2

O'Connell, Kevin M.: The Role of Science and Technology in Transforming American Intelligence. In Peter Berkowitz (szerk.): *The Future of American Intelligence.* Hoover Press, 2005.

Pap András László: *A megfigyelés társadalmának proliferációjától az etnikai profilalkotáson át az állami felelősség kiszervezéséig.* Budapest, L'Harmattan, 2012.

Pál Eszter – Törőcsik Mária: *Irodalmi áttekintés a Z generációról.* Pécs, Pécsi Tudományegyetem, 2013. Online: https://ktk.pte.hu/sites/ktk.pte.hu/files/images/szervezet/intezetek/mti/pal_torocsik_irodalmi_attekintes_a_z_generaciorol_2013.pdf

Perry, Tom: Factbox: Hezbollah and Allies Gain Sway in Lebanon Parliament. *Reuters,* 2018. május 22. Online: www.reuters.com/article/lebanon-election-parliament-factbox-idINKCN1IN1OB

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

Pilch Jenő: *A hírszerzés és kémkedés története* I–III. Budapest, Franklin Társulat, 1936.

Privacy and Civil Liberties Oversight Board: *Report on the Surveillance Program Operated Pursuant to Section 702 of the FISA* (2014. július 2.). Online: https://documents.pclob.gov/prod/Documents/OversightReport/823399ae-92ea-447a-ab60-0da28b555437/702-Report-2.pdf

Pink, Daniel H.: *Motiváció 3.0.* Budapest, HVG Könyvek, 2016.

Ladetto, Quentin: *Defence Future Technologies, Emerging Technology Trends 2015.* (DEFTECH) Federal Department of Defence, Civil Protection and Sport DDPS armasuisse Science and Technology, 2016. Online: https://deftech.ch/wp-content/uploads/2018/07/DefenceFutureTechnologies_EmergingTechnologyTrends2015.compressed.pdf

Ramsay, Anna – Augusta Whittall: *Sir Robert Peel.* New York, Books for Library Press, 1969.

Regényi Kund Miklós: OSINT a második generációs internetet megelőző korokban. *Nemzetbiztonsági Szemle,* 7. (2019), 2. 32–37. Online: https://doi.org/10.32561/nsz.2019.2.3

Regényi Kund (szerk.): *Információszerzés kapcsolati forrásai.* Budapest, Nemzeti Közszolgálati Egyetem, 2019. Online: https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/14284/Informacioszerzes_kapcsolati_forrasai_2019.pdf?sequence=1

Redden, Elizabeth: Science vs. Security. *Inside Higher Ed,* 2019. április 16. Online: www.insidehighered.com/news/2019/04/16/federal-granting-agencies-and-lawmakers-step-scrutiny-foreign-research

Regli, William: Universities in service to National Security, DARPA's call to academia. In *DARPA Defense Advanced Research Projects Agency 1958–2018 (60 years).* Faircount Media Group, 2018. 134–136. Online: www.darpa.mil/attachments/DARAPA60_publication-no-ads.pdf

Report of the U.S. Senate Select Committee on Intelligence and U.S. House Permanent Select Comittee on Intelligence (2002). Online: www.intelligence.senate.gov/sites/default/files/documents/CRPT-107srpt351-5.pdf

Révész Béla: Állambiztonság és pszichológia. Beszélő, 10. (2005), 5. 48–62. Online: http://beszelo.c3.hu/cikkek/allambiztonsag-es-pszichologia

Rolington, Alfred: *A hírszerzés a 21. században – a mozaikmódszer.* Budapest, Antall József Tudásközpont, 2015.

Somerville, Heather – Jane Lanhee Lee: U.S. Universities Unplug from China's Huawei under Pressure From Trump. *Reuters,* 2019. január 24. Online: www.reuters.com/article/us-usa-china-security-universities-insig/u-s-universities-unplug-from-chinas-huawei-under-pressure-from-trump-idUSKCN1PI0GV

Spracher, William C.: *National Security Intelligence Professional Education: A Map of U.S. Civilian University Programs and Competencies*. The Faculty of The Graduate School of Education and Human Development of The George Washington University in partial fulfillment of the requirements for the degree of Doctor of Education, Dissertation, 2009. Online: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.604.7161&rep=rep1&type=pdf

Steinhart, Amit: *The Future is Behind us? The Human Factor in Cyber Intelligence: Correlations between Cyber-HUMINT and Hackers' Social Engineering* (é. n.). Online: www.academia.edu/8457596/The_future_is_behind_us_The_human_factor_in_cyber_intelligence_Correlations_between_Cyber-HUMINT_and_Hackers_Social_Engineering

Stout, Mark: The Pond: Running Agents for State, War, and the CIA. The Hazards of Private Spy Operations. *Studies in Intelligence,* 48. (2004), 3. 69–82. Online: https://ia903106.us.archive.org/16/items/DTIC_ADA523244/DTIC_ADA523244.pdf

Swire, Peter – Kenesa Ahmad: Encryption and Globalization. *The Columbia Science & Technology Law Review,* 13. (2012), Spring. Online: https://doi.org/10.2139/ssrn.1960602

Szabó Károly: Az OSINT – Gondolatok a tevékenységről és az alkalmazás közegéről. *Nemzetbiztonsági Szemle,* 7. (2019), 2. 68–82. Online: https://doi.org/10.32561/nsz.2019.2.6

Szalai Flóra: *A terrorizmus és a terrorelhárítás törzsfejlődése.* A TEK előadása az ÁJK-n. 2017. március 13. Online: https://juratus.elte.hu/a-terrorizmus-es-a-terrorelharitas-torzsfejlodese-a-tek-eloadasa-az-ajk-n/

Tóth Balázs: Hatszorosára gyorsult a jégtakarók olvadása. *Index,* 2020. március 12. Online: https://index.hu/techtud/2020/03/12/hatszorosara_gyorsult_a_jegtakarok_olvadasa/

Tóth Tamás: Egyes Social Engineering módszerek elhatárolása és rendszerezése. *Szakmai Szemle,* 18. (2020), 1. Online: www.knbsz.gov.hu/hu/letoltes/szsz/2020_1_szam.pdf

Tyler, Richard: GCHQ Recruits Eight Universities to Counter Cyber Attacks. *The Telegraph,* 2012. április 1. Online: www.telegraph.co.uk/finance/newsbysector/industry/defence/9179442/GCHQ-recruits-eight-universities-to-counter-cyber-attacks.html

Törőcsik Mária – Szűcs Krisztián – Kehl Dániel: Generációs gondolkodás – A Z és az Y generáció életstílus csoportjai. *Marketing & Management,* (2014), 2. ksz. 3–15. Online: https://journals.lib.pte.hu/index.php/mm/article/view/861/732

Urbán Attila: A koordinációs folyamatok intézményi hátterének evolúciója a magyar nemzetbiztonsági igazgatásban. *Nemzetbiztonsági Szemle,* 8. (2020), 1. 5–32. Online: https://doi.org/10.32561/nsz.2020.1.1

Urban, Rudolf – Martin Macko: *Place and Role of the Defense Science in the Czech Research and Development System.* Brno, University of Defence, 2011.

Varga Krisztián: Katonai biztonsági magánvállalatok amerikai alkalmazása Irakban. *Nemzet és Biztonság,* 2. (2009), 3. 57–69. Online: www.nemzetesbiztonsag.hu/cikkek/varga_krisztian-katonai_biztonsagi_maganvallalatok_amerikai_alkalmazasa_irakban.pdf

Vellela, Tony: *New Voices: Student Political Activism in the '80s and '90s.* Boston, South End Press, 1988.

Vida Csaba: A hírszerző elemző-értékelő munka alapjai. *Felderítő Szemle,* 12. (2013), 3. 90–99.

Wagner, Kurt: Facebook Says Cambridge Analytica may have had Data from as Many as 87 Million People. *Vox,* 2018. április 4. Online: www.vox.com/2018/4/4/17199272/facebook-cambridge-analytica-87-million-users-data-collection

Weir, Fred: Russian Internet Giant Yandex Takes Rare Stand Against State Snooping. *The Christian Science Monitor,* 2019. június 14. Online: www.csmonitor.com/World/Europe/2019/0614/Russian-internet-giant-Yandex-takes-rare-stand-against-state-snooping

Weinbaum, Cortney – Richard Girven – Jenny Oberholtzer: *The Millenial Generation – Implications for the Intelligence and Policy Communities.* Santa Monica, Rand Corporation, 2016. Online: www.rand.org/content/dam/rand/pubs/research_reports/RR1300/RR1306/RAND_RR1306.pdf

Westerlund, Fredrik: *Russian Intelligence Gathering for Domestic R&D – Short Cut or Dead End for Modernisation?* Stockholm, Defence Analysis FOI Memo 3126, 2010.

Wladawsky-Berger, Irving: Innovation and National Security in the 21st Century. *The Wall Street Journal,* 2020. január 17. Online: https://blogs.wsj.com/cio/2020/01/17/innovation-and-national-security-in-the-21st-century/

Zalai-Göbölös Noémi*:* A Z és az alfa generációk jövője a nemzetbiztonsági szolgálatoknál. *Belügyi Szemle,* 66. (2018), 2. 46–59. Online: https://doi.org/10.38146/BSZ.2018.2.3

Jogi források

1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról

Európai Unió Bírósága, C-293/12. és C-594/12. sz. Digital Rights Ireland és Seitlinger és társai egyesített ügyek. Online: http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=hu&mode=lst&dir=&occ=first&part=1&cid=3050767

Európai Unió Bírósága, Maximillian Schrems kontra Data Protection Commissioner [nagytanács], C-362/14. sz. ügy

Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyek védelméről a személyes adatok feldolgozása során és az ilyen adatok szabad áramlásáról, valamint a 95/46 / irányelv hatályon kívül helyezéséről

Az Európai Parlament és a Tanács (EU) 2016/680 irányelve (2016. április 27.) a természetes személyek védelméről a személyes adatoknak az illetékes hatóságok általi feldolgozása során az ilyen személyek megelőzése, kivizsgálása, felderítése vagy üldözése céljából, bűncselekmények vagy büntetőjogi szankciók végrehajtása, valamint az ilyen adatok szabad mozgásáról, valamint a 2008/977 / IB tanácsi kerethatározat hatályon kívül helyezéséről

Internetes források

2015 Charlie Hebdo Attacks Fast Facts. *CNN,* (2020. december 18.). Online: www.cnn.com/2015/01/21/europe/2015-paris-terror-attacks-fast-facts/index.html

A 9/11 Bizottság jelentése (The 9/11 comission report) (é. n.). Online: https://govinfo.library.unt.edu/911/report/911Report.pdf

Access to innovation: NSA's Technology Transfer Program. *The Next Wave,* 19. (2012), 3. Online: www.nsa.gov/Portals/70/documents/resources/everyone/digital-media-center/publications/the-next-wave/TNW-19-3.pdf

Alkotmányvédelmi Hivatal: *Awareness Program* (é. n.). Online: https://ah.gov.hu/awareness-program/

The Alan Turing Institute: *Current Partnerships and Collaborations* (é. n.). Online: www.turing.ac.uk/collaborate-turing/current-partnerships-and-collaborations

The Apple-F.B.I. Case. *The New York Times,* (2016). Online: www.nytimes.com/news-event/apple-fbi-case

The Art of Deception. *Edwardsnowden.com,* (é. n.) Online: https://edwardsnowden.com/docs/doc/the-art-of-deception-training-for-a-new.pdf

Diákmunka: Az FBI diákokkal figyelteti a kínaiakat. *Librarius,* (2019. június 30.). Online: https://librarius.hu/2019/06/30/diakmunka-az-fbi-diakokkal-figyelteti-a-kinaiakat

Establishment of the DNI Open Source Center. *ODNI News Release,* (2005. november 8.). Online: www.dni.gov/files/documents/Newsroom/Press%20Releases/2005%20Press%20Releases/20051108_release_content.htm

FBI: *9/11 Investigation* (é. n.). Online: www.fbi.gov/history/famous-cases/911-investigation

FBI: *East African Embassy Bombings* (é. n.). Online: www.fbi.gov/history/famous-cases/east-african-embassy-bombings

FBI: *Operation Ghost Stories* (2011. október 31.). Online: www.fbi.gov/news/stories/operation-ghost-stories-inside-the-russian-spy-case

FBI: *USS Cole Bombing* (é. n.). Online: www.fbi.gov/history/famous-cases/uss-cole-bombing.GCHQ: *Bletchley Park & WWII.* (é. n.). Online: www.gchq.gov.uk/section/history/bletchley-park-and-wwii

GCHQ: *Education & Outreach* (é. n.). Online: www.gchq.gov.uk/section/culture/education-and-outreach

Gemeinsames Terrorismusabwehrzentrum: Verfassungsschutz.de. Online: www.verfassungsschutz.de/EN/protection-of-the-constitution/mission-and-working-methods/national-and-international-co-operation/national-and-international-co-operation_node.html

Government of the United Kingdom: *New ACT app launched* (2020. március 5.). Online: www.gov.uk/government/news/new-act-app-launched

Institute for Human Rights and Business: *Lawful Interception and Government Access to User Data: Designing a Rights-Respecting Model* (2016. január 15.). Online: www.ihrb.org/focus-areas/information-communication-technology/report-lawful-interception-and-government-access-to-user-data

The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA): *Justice Information Sharing* (2004). Online: https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1282

MTI: Hadat üzent a Gmail-nek a francia kormány. *Napi.hu,* (2013. szeptember 13.). Online: www.napi.hu/nemzetkozi_gazdasag/hadat_uzent_a_gmail-nek_a_francia_kormany.564438.html?p=2

National Commission on Terrorist Attacks Upon the United States (2004). Online: www.9-11commission.gov/

NATO: *Civilian Intelligence Committee (CIC)* (2011. november 16.). Online: www.nato.int/cps/en/natohq/topics_69278.htm

Number of College and University Students from China in the United States from Academic Year 2009/10 to 2019/20. *Statista*. Online: www.statista.com/statistics/372900/number-of-chinese-students-that-study-in-the-us/

Number of Monthly Active Facebook Users Worldwide as of 1st quarter 2020. *Statista,* (2021). Online: www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/

Number of Students from China Going Abroad for Study from 2008 to 2018. *Statista,* (2020). Online: www.statista.com/statistics/227240/number-of-chinese-students-that-study-abroad/#statisticContainer

Secure Trend 2015. Online: www.secure-trend.hu/2015/blog/posts/207

Security Service MI5: *Joint Terrorism Analysis Centre* (é. n.). Online: www.mi5.gov.uk/joint-terrorism-analysis-centre

Sandy Hook Promise: Gun Violence Warning Signs. *Youtube,* (2016.december 6.). Online: www.youtube.com/watch?v=9qyD7vjVfLI

NPCC: *More Than Seven Million People Watch Counter Terrorism Safety Video as UK Policing Increases its Global CT Presence* (2018. július 6.). Online: https://news.npcc.police.uk/releases/more-than-seven-million-people-watch-counter-terrorism-safety-video-as-uk-policing-increases-its-global-ct-presence

Office of the Director of National Intelligence: *About the ISE* (é. n.). Online: www.dni.gov/index.php/who-we-are/organizations/national-security-partnerships/ise/about-the-ise

OSCE: *Countering the use of the Internet for Terrorist Purposes* (é. n.). Online: www.osce.org/secretariat/107810

Terrorist drives truck through a Bastille Day celebration. *History,* (2016. július 14.). Online: www.history.com/this-day-in-history/2016-nice-terrorist-attacks

U.S. Embassy in Luxembourg: *Secretary Pompeo and Secretary Esper Speak at Munich Security Conference 2020* (2020. február 19.). Online: https://lu.usembassy.gov/secretary-pompeo-and-secretary-esper-speak-at-munich-security-conference-2020/

U.S. Department of Homeland Security: If You See Something, Say Something. (é. n.). Online: www.dhs.gov/see-something-say-something/about-campaign/seesay-day

Vault 7: CIA Hacking Tools Revealed. *WikiLeaks,* (é. n.). Online: https://wikileaks.org/ciav7p1/

Vákát

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.

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 rendelkezésükre a megfelelő kezelési technikák.

9 789635 316373