2018
2.

BELÜGYI SZEMLE

A BELÜGYMINISZTÉRIUM SZAKMAI, TUDOMÁNYOS FOLYÓIRATA

66.
évfolyam

TARTALOM 2018/2.

SZERZŐK 2018/2.

BEZSENYI TAMÁS tanársegéd,
Nemzeti Közszolgálati Egyetem
Rendészettudományi Kar Kriminalisztikai Intézet

DR. HABIL. BODA JÓZSEF dékán,
Nemzeti Közszolgálati Egyetem
Rendészettudományi Kar

DR. CSÁNYI CSABA ügyész, egyetemi adjunktus,
Nemzeti Közszolgálati Egyetem
Nemzetbiztonsági Intézet

DORNFELD LÁSZLÓ doktoranduszhallgató,
Miskolci Egyetem Állam- és Jogtudományi Kar

DRUSZA TAMÁS egyetemi tanársegéd,
Nemzeti Közszolgálati Egyetem
Nemzetbiztonsági Intézet
polgári nemzetbiztonsági tanszék

DR. KASZNÁR ATTILA mb. tanszékvezető, egyetemi adjunktus,
Nemzeti Közszolgálati Egyetem

KOLLÁR CSABA oktató,
Nemzeti Közszolgálati Egyetem
Katonai Műszaki Doktori Iskola

NAGYNÉ DR. TAKÁCS VERONIKA
szabályozási osztályvezető,
NISZ Nemzeti Infokommunikációs Szolgáltató Zrt.

DR. ZALAI-GÖBÖLÖS NOÉMI Terrorelhárítási Központ

SUMMARY

Boda, József
National security education in Hungary [5–21]
The author provides an overview of national security education and curricula form 1990 to 2017 in Hungary.

Kollár, Csaba
The human dimension of information security[22–45]
The author provides an overview of how hacker sub-culture and criminal organizations intertwine, and social engineering in the field of communication.

Zalai-Göbölös, Noémi
The future of Z- and Alfa-generations at national security agencies [46–59]
The author provides an overview of the prospects and challenges of young people in the field of national security.

Drusza, Tamás
Strategic human resources management in the field of national security [60–76]
Reflecting on recent developments, the author provides an overview of recent trends in strategic human resources management in the field of national security.

Csányi, Csaba
Terrorism and organized crime: profit or ideology? [77–85]
Reflecting on recent Eurobarometer findings, the author focuses on the link between terrorism, organized crime and illegal migration.

Nagyné Takács, Veronika
Risk management in information security: a service provider's perspective [86–105]
The author provides an overview of recent trends in risk management.

SUMMARY

Kasznár, Attila
Cybersecurity and anti-terrorist efforts [106–114]
The author provides an overview of the role and development of cyber-security in the field of national security, in particular intelligence, cyber-protection and preventive exploration.

Dornfeld, László
Coercive measures and cyber-crimes [115–135]
The author provides an overview of the constitutional and criminal procedural framework of law enforcement action in the field of cyber-crime.

Bezsenyi, Tamás
The for-hire jobs of the first Hungarian serial killer II. [136–155]
The author provides an overview of the life story of the first Hungarian serial killer: a women taking up male identity, and, hired by their families, hanged men in the early 1920s.

DOI: 10.38146/BSZ.2018.2.1

BODA JÓZSEF

A nemzetbiztonsági képzés helyzete Magyarországon

A nemzetbiztonsági kifejezés igazából csak a rendszerváltással jelenik meg a hazai köztudatban. Az Országgyűlés 1990. január 25-én fogadta el a különleges titkosszolgálati eszközök és módszerek átmeneti szabályozásáról szóló 1990. évi törvényt, és megszületett a 26/1990. (II. 14.) minisztertanácsi (MT) rendelet a *nemzetbiztonsági* feladatok ellátásának átmeneti szabályozásáról.

A különleges titkosszolgálati eszközök és módszerek engedélyezésének átmeneti szabályozásáról szóló 1990. évi X. törvénnyel módosított 1974. évi 17. törvényerejű rendelet 11. §-ának (7) bekezdésében kapott felhatalmazás alapján a Minisztertanács a Magyar Köztársaság nemzetbiztonsági feladatai ellátásáról a következőket rendeli:

1. § (1)

Az 1990. évi X. törvény 2. §-ában és az 1974. évi 17. tvr. 4. §-ában meghatározott feladatokat

a) *a nemzetbiztonsági* szolgálat;
b) az információs szolgálat;
c) a katonai biztonsági szolgálat;
d) a katonai felderítő szolgálat(a továbbiakban együtt: szolgálatok) látja el.[1]

Az MT-rendelet alapján jött tehát létre a Nemzetbiztonsági Hivatal, az Információs Hivatal mint *polgári nemzetbiztonsági szolgálat,* a Katonai Biztonsági Hivatal, és a Katonai Felderítő Hivatal pedig *katonai nemzetbiztonsági szolgálatként.*

A *nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény* megjelenésével kaptunk azután tiszta képet arról, hogy mely szervezeteket sorolt a jogszabályalkotó a nemzetbiztonsági szolgálatok közé.

Az Országgyűlés a Magyar Köztársaság szuverenitásának fenntartása és alkotmányos rendjének védelme érdekében a nemzetbiztonsági szolgálatok alkotmányos működéséről a következő törvényt alkotta:

1 26/1990. (II. 14.) MT rendelet *a nemzetbiztonsági* feladatok ellátásának átmeneti szabályozásáról 1. § (1) bek.

A nemzetbiztonsági szolgálatok szervezete és jogállása

1. § A Magyar Köztársaság *nemzetbiztonsági szolgálatai*
a) az Információs Hivatal,
b) a Nemzetbiztonsági Hivatal,
c) a Katonai Felderítő Hivatal,
d) a Katonai Biztonsági Hivatal,
e) a Nemzetbiztonsági Szakszolgálat
(a továbbiakban együtt: nemzetbiztonsági szolgálatok).

2. § (1) Az Információs Hivatal, a Nemzetbiztonsági Hivatal és a Nemzetbiztonsági Szakszolgálat (a továbbiakban együtt: polgári nemzetbiztonsági szolgálatok), a Katonai Felderítő Hivatal és a Katonai Biztonsági Hivatal (a továbbiakban együtt: katonai nemzetbiztonsági szolgálatok) a Kormány irányítása alatt álló, országos hatáskörű, önálló gazdálkodást folytató költségvetési szervek.[2]

Természetesen a biztonsági, nemzetbiztonsági körülmények változása, és az új külső és belső biztonsági feladatok miatt változott a nemzetbiztonsági szolgálatok alárendeltsége, szervezeti felépítése, sőt egyes esetekben feladatrendszere is, valamint új titkos információ gyűjtésére jogosult rendvédelmi és nemzetbiztonsági szolgálatok alakultak.

Történeti visszatekintés

A második világháború végétől az ötvenes évek elejéig az államvédelmi szolgálatok tagjai számára tanfolyamokat (nyomozói, tájékoztatói) szerveztek. Ebben az időszakban cserélték le az előző rendszer szakértői állományát, egy a szocialista rendszerhez hű, de szakmai ismerettel nem igazán felvértezett garnitúrára. Ezért az Államvédelmi Hatóság (ÁVH) 1948-as megalakulása után az egyik fő feladat az állomány felkészítése volt, amelyet az ÁVH tanulmányi osztálya tervezett, szervezett, és irányított. 1951-től a képzés a Dzerzsinszkij Tiszti Iskolán és a Szovjetunióban folyt. A Belügyminisztérium Idegen nyelvi Főiskola 1958-as megalakításával megkezdődött a külső állambiztonsági vonal szakembereinek hároméves képzése. A Rendőrtiszti Akadémián 1959-ben kétéves képzés vette kezdetét.[3]

2 A nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény 1. és 2. §.

3 Jobst Ágnes: A titkosszolgálatok tudománya az oktatás és a tananyagok tükrében – 1945 után. In: Csóka Ferenc (szerk.): Szakszolgálat Magyarországon, avagy tanulmányok a hírszerzés és titkos adatgyűjtés világából 1785–2011. Nemzetbiztonsági Szakszolgálat, Budapest, 2012, 421. o.

A BM Tartalékos Tisztképző Iskolán a képzés 1967-ben kezdődött (24 hónap), ahol a BM szervek számára képezték a tartalékos tiszti utánpótlást. Az állambiztonsági szolgálatok számára az 1971–1990 között a Rendőrtiszti Főiskola (RTF) állambiztonsági tanszékén oktatták szinte a teljes tiszti állományt, a katonai hírszerzők kivételével. Részükre a Zrínyi Miklós Katonai Akadémián létrehoztak egy speciális, úgynevezett D tagozatot.

1973-tól pedig az RTF szaktanárai és az állambiztonsági hallgatók egy része a Szovjetunióban tanult. Az RTF nappali és levelező tagozatain politikai nyomozó szakra (állambiztonsági) 1990-ig, katonai elhárítónak 1973-ig, idegen nyelvi szakra pedig 1973-ig lehetett jelentkezni.

A BM-hez tartozó állambiztonsági szervek tiszthelyettesi és később a zászlósi állomány képzése belső szaktanfolyamok formájában és a BM Kun Béla Zászlósképző Iskolán zajlott.

A rendszerváltozás következményeként megszűnt az Állambiztonsági Főcsoportfőnökség, és új nemzetbiztonsági szolgálatok létrehozására került sor. Az Állambiztonsági Főcsoportfőnökség megszűnésével szinte egy időben, a kilencvenes évek elején beszüntették az állambiztonsági képzést is a RTF-en.

A nemzetbiztonsági szolgálatok elsősorban toborzás útján az egyetemekről és főiskolákról közvetlenül vették fel munkatársaikat, akik számára belső szakmai tanfolyamokat, továbbképzéseket szerveztek.

Először a Zrínyi Miklós Nemzetvédelmi Egyetem oktatóiban vetődött fel, hogy el kellene indítani a nemzetbiztonsági szolgálatok számára a főiskolai és egyetemi szintű képzést. Első lépésként kidolgozták az akkreditációhoz szükséges okmányokat, és ezek elfogadása után megalakult a Nemzetbiztonsági Szakcsoport (2005–2009), majd a nemzetbiztonsági tanszék, amely 2009 és 2012 között működött. A képzés alap- és mesterszakon, valamint a doktori iskolákon folyt.[4]

Nemzetbiztonsági képzés a Nemzeti Közszolgálati Egyetem Nemzetbiztonsági Intézetében

A Nemzeti Közszolgálati Egyetem megalakulásával szinte egy időben vetődött fel az igény, hogy a katonai és polgári nemzetbiztonsági szolgálatok ál-

4 Héjja István: A „Bolognai folyamat” és a nemzetbiztonsági képzés. Felderítő Szemle, 2009/4.

lománya számára is a speciális igényeknek megfelelő egyetemi szintű képzések induljanak el.

A megalakulástól a polgári nemzetbiztonsági alapképzési szak megindításáig

A nemzetbiztonsági szolgálatok tagjai részére nyújtandó felsőoktatási képzéseket a Nemzeti Közszolgálati Egyetemről, valamint a közigazgatási, rendészeti és katonai felsőoktatásról szóló 2011. évi CXXXII. törvény szabályozza.

Általános rendelkezések

1. § (1) A törvény hatálya kiterjed
   a) a Nemzeti Közszolgálati Egyetemre (a továbbiakban: egyetem),
   b) az általa folytatott államtudományi és közigazgatási, rendészeti, katonai, *nemzetbiztonsági,* valamint nemzetközi és európai közszolgálati felsőoktatási tevékenységre, továbbá az azzal összefüggő szolgáltató és igazgatási tevékenységre, ideértve azon tevékenységet is, amelyet az egyetem Magyarország területén kívül folytat,
3. § 4. nemzetbiztonsági felsőoktatás: a nemzetbiztonsági ágazat szakembereinek felkészítése érdekében indított nemzetbiztonsági alapképzési szak, valamint a hozzá kapcsolódó mesterképzési szak[5];

A nemzetbiztonsági képzés megszervezése, elindítása és végrehajtása céljából az egyetem fenntartói testületének 2011. 08. 19-én elfogadott 3/14/2011. számú határozatával 2012-ben megalakult a *Nemzetbiztonsági Intézet (NBI).* Az egyetemen a tudományos rektorhelyettes alárendeltségében működik az NKE Nemzetbiztonsági Intézet.

A Nemzetbiztonsági Intézet létrehozásával létrejött a titkosszolgálati eszközök alkalmazására felhatalmazott szervezetek szakember-utánpótlásának bázisa. Indulásakor az intézetnek két tanszéke volt, a katonai és a polgári nemzetbiztonsági tanszék.

Az Információs Hivatal, az Alkotmányvédelmi Hivatal, a Nemzetbiztonsági Szakszolgálat vezetői kinyilvánították együttműködési szándékukat abban, hogy a teljes képzési szerkezetben a képzés a következő évben, vagyis 2013-ban kezdődhet. A megrendelő szervezetek szándéka alapján a képzés az

5 A Nemzeti Közszolgálati Egyetemről, valamint a közigazgatási, rendészeti és katonai felsőoktatásról szóló 2011. évi CXXXII. törvény1. § a) és b); 3. § 4. pont.

kezdetekkor elsősorban levelező formában történt, a hallgatók beiskolázása zárt rendszerben zajlott. A tanszékeket a Hungária körúti objektumban helyezték el, az oktatás pedig ott, és más egyéb egyetemi telephelyeken valósult meg. A nemzetbiztonsági képzés jelenléte az egyetemen azt célozta, hogy az ott folyó valamennyi képzésben, és az egyetem minden hallgatójában megerősítse a nemzetbiztonsági tudatosságot.

A Nemzeti Közszolgálati Egyetem ideiglenes szenátusa a 2012. október 3-i ülésén jóváhagyta a *nemzetbiztonsági alap- és mesterképzés* szak tanterveinek módosítását.

A 2012. október 26-án megtartott belügyminiszteri oktatói állománygyűlésen meghatározottak alapján a Nemzetbiztonsági Intézet a fokozatosság elvét betartva elkészítette a nemzetbiztonsági alapszak terrorelhárítási specializációra vonatkozó javaslatot a hadtudományi és honvédtisztképző karon akkreditálva, amelyet a szenátus támogatott a 2015. április 29-i ülésén, a polgári nemzetbiztonsági alapszak tervezetét (rendészettudományi karon akkreditálva), amely 2017. szeptember 1-jén kezdődött, a polgári nemzetbiztonsági mesterszak tervezetét (rendészettudományi karon akkreditálva, amelyet a szenátus támogatott a 2017. szeptember 13-i ülésén).

A belügyminiszter a feladat-meghatározó értekezleten stratégiai célként határozta meg és feladatul szabta a Nemzeti Közszolgálati Egyetem Nemzetbiztonsági Intézet polgári nemzetbiztonsági tanszéke számára az önálló polgári nemzetbiztonsági alap- (2017) és mesterszak (2018) létesítését.

Ennek megfelelően 2013 őszétől mind az alap-, mind a mesterképzésben megkezdődött a képzés a katonai és a polgári nemzetbiztonsági szakirányon.

Az *alapképzés* céljaként határozták meg *nemzetbiztonsági szakértők* képzését a speciális rendeltetésű nemzetbiztonsági szolgálatok, valamint más megrendelők számára. Követelmény a korszerű általános és szaktudományi, elméleti és gyakorlati ismeret, továbbá nemzetbiztonsági szakmai, szaktechnikai, jogi, kriminológiai, kriminalisztikai, pszichológiai, informatikai, biztonságpolitikai és idegen nyelvi szaknyelvi ismeret, továbbá kellő tudás a képzés második ciklusban történő folytatásához.

Külön-külön meghatározták a szakirányok képzési céljait.

A katonai nemzetbiztonsági specializáció céljai a következők:

– a hírszerző szakág cikluson alapuló munkafolyamatának megismerése, és az egyes elemek feladatainak elsajátítása;
– a katonai elhárító szakág által alkalmazott műveleti tevékenység erőinek, eszközeinek és módszereinek megismerése és alkalmazóképes elsajátítása, továbbá a művelettámogató tevékenység keretében alkalmazandó előírá-

soknak, a műveleti tevékenység megfelelő szintű végrehajtását biztosító információs rendszer elemeinek, működésének, az információgyűjtés, -feldolgozás és az információáramlás rendjének elméleti és gyakorlati megismerése;
– a békeműveletek és -missziók hírszerző, elhárító, rádióelektronikai és -felderítő eszközeinek, módszereinek elsajátítása;
– a nyílt forrásokból szerzett információk (OSINT), a rádióelektronikai felderítés (SIGINT), a személyi információszerzés (HUMINT) elméleti és gyakorlati ismeretköreinek szélesítése;
– a Katonai Nemzetbiztonsági Szolgálatnál alkalmazott elemző-értékelő eljárások elméleti és gyakorlati alapjainak megismerése, valamint szakágspecifikus alkalmazásának elsajátítása.

A polgári nemzetbiztonsági specializáció képzésének céljai a következők:
– a polgári nemzetbiztonsági szervezetek feladatrendszere sajátosságainak figyelembevételével az eszközök és módszerek alkalmazásának tervezésére, szervezésére, az egyes szaktevékenységek szakszerű végrehajtására, és döntések előkészítésére alkalmas szakemberek képzése;
– a polgári nemzetbiztonsági tevékenység- és feladatrendszerhez tartozó műveleti és technikai tudásanyag strukturáltabb megismertetése;
– a szakfeladatok végrehajtását elősegítő nemzetbiztonsági, közigazgatási és rendészeti szakismeretek elméleti tudásanyagának elsajátítása mellett a gyakorlati ismeretkörök szélesítése;
– a nemzetbiztonsági feladatok kapcsán a rendszerszintű, komplex gondolkodás elősegítése;
– a műveleti és technikai szakfeladatok ellátása során a váratlan helyzetekben történő szakszerű és hatékony válaszadásra való felkészítés;
– a folyamatosan változó külső, technikai környezetből érkező kockázatokra, veszélyekre és kihívásokra adandó hatékony reagálás érdekében a technikai-szakértői ismeretek és tudásanyag elmélyítése, célorientáltabb megjelenítése.

A képzési időt hat félévben, a szükséges kreditszámot 180-ban, az összes hallgatói tanulmányi munkaidőt 5400 órában állapították meg. Kötelező szakmai gyakorlatként tíz hetet írtak elő.

A polgári nemzetbiztonsági specializáció keretein belül a következő új tantárgyak bevezetésére került sor:
– kriminalisztikai alapismeretek;
– információs rendszerek biztonsága nemzetbiztonsági perspektívából;

– műveleti veszélyhelyzetek megelőzése és kezelése I.;
– nemzetbiztonsági szakismeretek (polgári I);
– nemzetbiztonsági szakismeretek (polgári II);
– nemzetbiztonsági szakismeretek (polgári III);
– szakértői tevékenység I.

A *mesterképzés* céljaként olyan szakemberek oktatását határozták meg, akik a korszerű társadalomtudományi és szakmaspecifikus ismeretek felhasználásával képesek a nemzetbiztonsági szakterület szervezeteiben a munkakörükhöz tartozó követelmények és feladatok eredményes teljesítésére, alkalmasak a szakmai elmélet és módszertan fejlesztésére, a szakmai kultúra és értékrend továbbadására, tanulmányaik PhD-képzés keretében való folytatására.

Mesterszakon a képzési időt négy félévben, a szükséges kreditszámot 120-ban, az összes hallgatói tanulmányi munkaidőt 3600 órában állapították meg. A mesterképzési szakon szerezhető ismeretek a következők:

– nemzetbiztonsági, védelmi, rendvédelmi és társadalomtudományi elméleti és gyakorlati szakismeretek;
– az általános és a nemzetbiztonsági, a védelmi, a rendvédelmi szakterületen alkalmazható vezetéselméleti és alkalmazott pszichológiai ismeretek;
– az államigazgatási, a nemzetközi közjogi és szakmai jogi szabályozás alapvető ismeretei;
– a kutatáshoz vagy tudományos munkához szükséges, széles körben alkalmazható problémamegoldó technikák ismerete;
– a globális társadalmi és gazdasági folyamatok ismerete.

A mesterképzésben is megjelentek új tantárgyak:

– műveleti veszélyhelyzetek megelőzése és kezelése II.;
– a nemzetbiztonsági feladatok technikai-műveleti támogatása;
– a nemzetbiztonság technikai kihívásai a XXI. században;
– a nemzetbiztonság általános elmélete;
– speciális OSINT-ismeretek;
– speciális HUMINT-ismeretek és -gyakorlatok;
– szakértői tevékenység II.

A nemzetbiztonsági szak szakfelelősének az alap- és mesterszak vonatkozásában *Resperger István*t, a katonai nemzetbiztonsági specializáció felelősének *Kobolka István*t, a polgári nemzetbiztonsági specializáció felelősének pedig *Boda József*et hagyta jóvá a szenátus.

Sor került a nemzetbiztonsági képzésbe való felvétel sajátosságainak meghatározására. Mind a nemzetbiztonsági alapképzésre, mind a mesterképzésre a jelentkezők köre korlátozott, csak a polgári nemzetbiztonsági szolgálatok, és a Katonai Nemzetbiztonsági Szolgálat, valamint titkos információgyűjtésre törvényben felhatalmazott szervezetek állományába tartozók jelentkezhettek, akiket a beiskolázási jogkörrel felruházott elöljáró (vezető) az előmeneteli tervek alapján támogatott, és akiknek a C típusú kérdőívhez kötött nemzetbiztonsági ellenőrzése kockázati tényezőt nem tárt fel.[6]

2013-ban sor került a Nemzeti Közszolgálati Egyetem és a nemzetbiztonsági szolgálatok együttműködését szabályozó megállapodások aláírására is.

A Nemzeti Közszolgálati Egyetem Nemzetbiztonsági Intézete 2013-ban mind a nemzetbiztonsági alapképzési, mind a nemzetbiztonsági mesterképzési szakon, katonai és polgári nemzetbiztonsági specializáción, zárt jellegű képzési formában várta először a hallgatók jelentkezését.[7]

2013. szeptember 1-jétől az egyetem intézményfejlesztési tervének megfelelően elindult egy közös képzési modul oktatása az intézmény valamennyi hallgatója részére[8], ennek szerves része egy nemzetbiztonsági tanulmányok című, harmincórás tantárgy oktatása is. A tizenöt tárgyból álló modult[9] szemeszterenként 1500-1700 embernek oktatja a Nemzetbiztonsági Intézet oktatói állománya.

A Nemzetbiztonsági Intézet szervezésében 2015-ben indult a *nemzetbiztonsági felső vezetői tanfolyam,* amelyre a nemzetbiztonsági szolgálatok és a titkos információgyűjtésre feljogosított szervezetek küldhetnek hallgatókat. A tanfolyam levelező rendszerben három féléven keresztül zajlik, havi összevonások teljesítésével, 560 órában. A tanfolyam célja a nemzetbiztonsági felső vezetők speciális felkészítése vezetői feladatkörük ellátására.

A *Nemzeti Közszolgálati Egyetemen* a Nemzetbiztonsági Intézeten belül működik a katonai, a polgári nemzetbiztonsági, valamint a terrorelhárítási tanszék.

---

6 A Nemzeti Közszolgálati Egyetem Ideiglenes Szenátusának 18/2012. (X. 3.) számú határozata.

7 Kovács Gábor: Tájékoztató a Nemzeti Közszolgálati Egyetem megalakulásáról és működéséről. Migráció és társadalom, 2012/1. Online megjelenés.

8 Kovács Gábor: A Nemzeti Közszolgálati Egyetem, mint a közszolgálati képzés bázisa: a jelenlegi helyzetkép, jövőbeni változások, fejlődési tendenciák és kihívások. In: Gaál Gyula – Hautzinger Zoltán (szerk.): Tanulmányok „A biztonság rendészettudományi dimenziói – változások és hatások" című tudományos konferenciáról. Pécs, 2012, 374. o. [Pécsi Határőr Tudományos Közlemények XIII.]

9 Kovács Gábor: Vezetés és szervezéselméleti felkészítés a Nemzeti Közszolgálati Egyetemen. In: Gaál Gyula – Hautzinger Zoltán (szerk.): Tanulmányok a „Biztonsági kockázatok – rendészeti válaszok" című tudományos konferenciáról. Pécs, 2014, 309. o. [Pécsi Határőr Tudományos Közlemények XV.]

Bűnügyi szolgálati ismereteket (bűnügyi hírszerzést és titkos információgyűjtést) oktatnak még az egyetem rendészettudományi karának bűnügyi és gazdaságvédelmi tanszékén.

A Nemzetbiztonsági Intézeten belül a három tanszék gondozásában a katonai, terrorelhárítási és polgári nemzetbiztonsági specializáció keretein belül, alap- és mesterszakokon folyik az oktatás, a szolgálatok tagjai számára, és a tanszékek tagjai egyben az egyetem doktori iskoláinak témahirdetői is.

A *katonai nemzetbiztonsági tanszék* a Katonai Nemzetbiztonsági Szolgálat számára gondoskodik a szakemberek képzéséről, katonai specializáció keretében. Ezek mellett a nemzetbiztonsági felső vezetői tanfolyam vezetését, szervezését végzi, hogy a titkos információgyűjtésre feljogosított szervezetek megkapják a megfelelő felső vezetői utánpótlást. A tanszék vezetője *Kaiser Ferenc* egyetemi docens.

A *polgári nemzetbiztonsági tanszék* a polgári nemzetbiztonsági szolgálatoknak és különleges rendőri szerveknek egyaránt képez szakembereket. Ennek érdekében BSc- és MSc-szintű képzést folytat, polgári specializáció keretében. Vezetője 2017 közepéig Boda József volt, jelenleg pedig *Dobák Imre* egyetemi docens, a Nemzetbiztonsági Szakszolgálattól.

A *terrorelhárítási tanszék* az intézet legfiatalabb tanszékeként Bsc- és MsC-szintű képzést és terrorelhárítási specializációt gondoz. A tanszék feladata, hogy felkészítse azokat a szakembereket, akik hatékony módon és eszközökkel megelőzhetik a terrorista cselekményeket. A tanszék vezetője *Kasznár Attila* egyetemi adjunktus, a Terrorelhárítási Központtól.

A Nemzetbiztonsági Intézet munkatársai, együttműködve a nemzetbiztonsági szolgálatok szakértőivel a megalapítás óta kidolgozták az alap- és mesterszak oktatásához szükséges jegyzeteket, tankönyveket és tanulmányokat[10].

A tudományos munka támogatására, a doktoranduszok és a szakterület kutatói számára az intézet 2013. szeptember 1-jén megalapította a *Nemzetbizton-*

10 Kobolka István (szerk.): Nemzetbiztonsági alapismeretek. Nemzeti Közszolgálati és Tankönyv Kiadó, Budapest, 2013; Dobák Imre (szerk.): A nemzetbiztonság általános elmélete. Nemzeti Közszolgálati Egyetem Nemzetbiztonsági Intézet, Budapest, 2014; Boda József – Parádi József – Regényi Kund Miklós (szerk.): 1872 Felderítő-szolgálati utasítás. Anleitung zum Kundschaftsdienste. Nemzetbiztonsági Szakszolgálat–Szemere Bertalan Magyar Rendvédelem-történeti Tudományos Társaság, Budapest, 2014 [A magyar rendvédelem-történet hagyatéka 1.]; Boda József – Parádi József (szerk.): A XIX-XX. századi magyar állam nemzetbiztonsági szervezetei. Nemzetbiztonsági Szakszolgálat–Szemere Bertalan Magyar Rendvédelem-történeti Tudományos Társaság, Budapest, 2013; Dobák Imre – Regényi Kund Miklós (szerk.): Szakmatörténeti Szemelvények. Nemzetbiztonsági Szakszolgálat, Budapest, 2014; Boda József – Dobák Imre (szerk.): A nemzetbiztonság technikai kihívásai a 21. században. Egyetemi jegyzet. Nemzeti Közszolgálati Egyetem, Budapest, 2015; Boda József: „Szigorúan titkos!?” Nemzetbiztonsági almanach. Zrínyi Kiadó, Budapest, 2016

sági Szemle[11] című folyóiratot, amely évente négy számmal jelenik meg. A folyóirat célja a nemzetbiztonsági szféra tudományos kérdéseinek, szakmaiságának képviselete, és olyan fórum létrehozása, amely az egyetem létrehozásakor megfogalmazott gondolatokkal összhangban teret ad a szakemberek, oktatók, kutatók és hallgatók tudományos értékű eredményei bemutatásának. A szerkesztőbizottság elnöke Boda József, főszerkesztője Dobák Imre.

A folyóiratban megjelenő tudományos közlemények a képzéseket támogatva elősegíthetik, hogy a hallgatók *„bővítsék az egyre inkább komplexebb kérdéseket kutató-vizsgáló nemzetbiztonsági tudományszak eredményeit”*[12].

A Nemzeti Közszolgálati Egyetemen jelenleg négy doktori iskola is működik, a hadtudományi, a katonai műszaki, közigazgatás-tudományi és rendészettudományi, itt lehetőségük van a hallgatóknak nemzetbiztonsági területen is tudományos kutatást folytatni és fokozatot szerezni. Konkrétan a hadtudományi és a rendészettudományi iskolák kutatási területein találhatók meg a nemzetbiztonság kérdéseit tartalmazó témák.

A Nemzetbiztonsági Intézet és azon belül a polgári nemzetbiztonsági tanszék megalakulása óta évente rendez tudományos konferenciákat aktuális nemzetbiztonsági témákban.

Az intézet figyelmet fordít a tehetséggondozásra is, ennek keretében működteti a *Nemzetbiztonsági Szakkollégium*ot. Általában harmincan-harminc-öten vesznek részt az egyetem minden karáról a szakkollégiumi munkában. Folyamatos szakmai előadásokból és tréningekből, szakmai látogatásokból áll a program. A szakkollégium létrehozásában a katonai nemzetbiztonsági tanszéknek vannak elévülhetetlen érdemei. Vezetője jelenleg Dobák Imre.

Az önálló polgári nemzetbiztonsági szakok megalapítása

A korábbi belügyminiszteri ajánlásnak és a rektori utasításnak megfelelően 2017 őszén indult el az rendészettudományi karon akkreditált *önálló polgári nemzetbiztonsági alapszak,* a következő feltételekkel:

1. az alapképzési szak megnevezése: polgári nemzetbiztonsági *(Civilian National Security Studies);*
2. az alapképzési szakon szerezhető végzettségi szint és a szakképzettség oklevélben szereplő megjelölése:

11 http://uni-nke.hu/kutatas/egyetemi-folyoiratok/nemzetbiztonsagi-szemle

12 Dobák Imre: A nemzetbiztonsági képzésről… Nemzetbiztonsági Szemle, 2014/1. Különszám. http://epa.oszk.hu/02500/02538/00004/pdf/EPA02538_nemzetbiztonsagi_szemle_2014_01ksz_068-078.pdf

a) végzettségi szint: alapfokozat (baccalaureus, bachelor; rövidítve: BA),
b) szakképzettség: polgári nemzetbiztonsági szakértő,
c) a szakképzettség angol nyelvű megjelölése: *Civilian National Security Expert,*
d) választható specializációk: humán felderítő, technikai felderítő, terrorelhárítási *(human intelligence, technical intelligence, counter terrorism);*

3. képzési terület: államtudományi;
4. A 2011. évi CXXXII. törvény 3. §-ában meghatározott felsőoktatási terület: nemzetbiztonsági;
5. a képzési idő félévekben: hat félév;
6. az alapfokozat megszerzéséhez összegyűjtendő kreditek száma:180;
7. Az alapképzési szak képzési célja, az elsajátítandó szakmai kompetenciák: a nemzetbiztonsági szolgálatok, valamint más, a titkos információgyűjtésre és titkos adatszerzésre feljogosított szervek – így különösen a Nemzeti Adó- és Vámhivatal, a Nemzeti Védelmi Szolgálat, a rendőrség, a Terrorelhárítási Központ, az ügyészség – számára polgári nemzetbiztonsági szakértők oktatása és nevelése, akik korszerű általános és szaktudományi, elméleti és gyakorlati ismeretekkel, továbbá nemzetbiztonsági szakmai, szaktechnikai, jogi, kriminológiai, kriminalisztikai, pszichológiai, informatikai, biztonságpolitikai és idegen szaknyelvi ismeretekkel bírnak, továbbá kellő ismeretük lesz a képzés mesterszakon történő folytatásához.

A humán felderítő specializáció céljai a következők:

– a polgári nemzetbiztonsági szervezetek feladatrendszerének, valamint a titkos információgyűjtésre és titkos adatszerzésre feljogosított szervezetek sajátosságainak figyelembevételével az eszközök és módszerek alkalmazásának tervezésére, szervezésére, különleges műveleti feladatok szakszerű végrehajtására, és döntések előkészítésére alkalmas szakemberek, leendő beosztott vezetők képzése;
– az emberi forrásból történő információgyűjtés társadalmi és pszichológiai hátterét, pszichológiai alapjait ismerő, az eszközrendszer létrehozását, fenntartását magas szinten végezni tudó szakemberek, leendő beosztott vezetők képzése;
– a nyílt forrásból származó információgyűjtés általános ismereteinek birtokában lévő felderítő szakemberek, leendő beosztott vezetők képzése;
– a polgári nemzetbiztonsági tevékenység- és feladatrendszerhez tartozó műveleti és technikai tudásanyag részletesebb és mélyebb megismertetése;

– a nemzetbiztonsági értékelő, elemző és tájékoztató alrendszer alapelveiben, funkcióiban, technikai hátterében jártas, azt aktuális szinten alkalmazni képes szakemberek, leendő beosztott vezetők képzése;
– a bűnügyi hírszerzés vonatkozó jogszabályainak, alapfogalmainak, alapelveinek elsajátítása, kiemelt szinten történő gyakorlati alkalmazása;
– a szakfeladatok végrehajtását elősegítő nemzetbiztonsági, közigazgatási és rendészeti szakismeretek elméleti tudásanyagának elsajátítása mellett a gyakorlati ismeretkörök szélesítése;
– a nemzetbiztonsági feladatok kapcsán a rendszerszintű, komplex gondolkodás elősegítése;
– a műveleti feladatok ellátása során a váratlan helyzetekben történő szakszerű és hatékony válaszadásra való felkészítése;
– társ- és partnerszolgálatokkal, bűnüldözési szervekkel és szervezetekkel, valamint a hivatásrendek képviselőivel hazai és nemzetközi (Európai Unió, NATO stb.) együttműködésre képes szakemberek, leendő beosztott vezetők képzése;
– a speciális kriminál technikai eszközök alkalmazásának jártasság szinten történő elsajátítása.

A technikai felderítő specializáció céljai a következők:

– a polgári nemzetbiztonsági, valamint a titkos információgyűjtésre és titkos adatszerzésre, feljogosított szervezetek feladatrendszere sajátosságainak figyelembevételével speciális technikai eszközök alkalmazásának tervezésére, szervezésére, egyes szaktevékenységek szakszerű végrehajtására, és döntések előkészítésére alkalmas szakemberek, leendő beosztott vezetők képzése;
– a folyamatosan változó külső, technikai környezetből érkező kockázatokra, veszélyekre és kihívásokra adandó hatékony reagálás érdekében a technikai-szakértői ismeretek elmélyítése, célorientált megjelenítése;
– elektronikus információs rendszerek működésével és használatával kapcsolatos naprakész ismeretekkel felvértezett szakemberek, leendő beosztott vezetők képzése;
– az információs műveletek biztonságos és szakszerű végrehajtásához szükséges ismeretek átadása, az informatikai eszközök használatának szélesítése;
– a kiberbiztonság főbb kihívásaira reagálni képes nemzetbiztonsági szakemberek, leendő beosztott vezetők képzése;
– a nyílt forrásból származó információgyűjtés általános ismereteinek birtokában lévő szakemberek, leendő beosztott vezetők képzése;

– a geoinformációs adatok megszerzésére alkalmas szakemberek képzése;
– társ- és partnerszolgálatokkal, bűnüldözési szervekkel és szervezetekkel, valamint a hivatásrendek képviselőivel hazai és nemzetközi (Európai Unió, NATO stb.) együttműködésre képes szakemberek, leendő beosztott vezetők képzése;
– a technikai szakfeladatok ellátása során a váratlan helyzetekben történő szakszerű és hatékony válaszadásra való felkészítés.

A terrorelhárítási specializáció képzésének céljai:
– a terrorelhárítás elméletének és gyakorlatának ismerete, azok alkalmazása, valamint szervezetek irányítása hazai és nemzetközi együttműködésben;
– a terrorelhárítással kapcsolatos jogszabályok ismerete és azok alkalmazása;
– a terrorfelderítés szervezeti és módszertani feladatainak ellátása, illetve annak irányítása, különös tekintettel a hírszerzés vezette műveletekre, valamint a titkos és nyílt forrásból származó információk alkalmazására;
– a terrorelhárító műveletek tervezése, előkészítése, végrehajtása, erők és eszközök alkalmazása, műveletek irányítása, társszervezetekkel, partnerekkel való együttműködés;
– a pszichológia, a szociológia és a vezetéselmélet korszerű kutatási eredményeinek szakmai alkalmazása a terrorelhárító munkában;
– terrorizmussal kapcsolatos kockázatelemzések elkészítése objektumok, létfontosságú létesítmények és személyek védelme vonatkozásában.

A 2011. évi CXXXII. törvény 3. §-ában meghatározott felsőoktatási területen belüli közös képzési szakasz alapszak szempontjából fontos kompetenciái a következők:
– a polgári nemzetbiztonsági, valamint a titkos információgyűjtésre és titkos adatszerzésre feljogosított szervezetek sajátosságainak megfelelő korszerű, a modern demokráciát és jogállamiságot tükröző társadalom- és természettudományi ismeretek alkalmazásának képessége;
– a vezetés- és szervezéselmélet, az informatikai ismeretek és a menedzsment modern követelményei alkalmazásának képessége;
– a szakmai kompetencia megalapozásához szükséges szaktudományi ismeretek alkalmazásának képessége.

Alapfokozat birtokában a polgári nemzetbiztonsági szakértők – a várható specializációkat is figyelembe véve – képesek

– a biztonsági helyzetet és kihívásokat, a veszélyforrásokat, kockázati tényezőket és fenyegetéseket, a szakmai tevékenység célját, körülményeit a maga konkrétságában, összetettségében, kiemelten Magyarország vonatkozásában értékelni, az eredményes szakmai tevékenységhez a rendelkezésre álló humánforrásokat, titkosszolgálati eszközöket-módszereket, terrorelhárító eljárásokat szakszerűen alkalmazni;
– nemzetbiztonsági és terrorelhárító műveletek végrehajtása során a társ- és partnerszolgálatokkal való hazai és nemzetközi szintű együttműködésre;
– a polgári nemzetbiztonsági feladatok végrehajtása során az előírt algoritmusok szerinti tevékenységre, az előre nem modellezhető helyzetekben a gyors és körültekintő értékelésre, döntések előkészítésére és a döntések meghozatalára;
– a nemzetbiztonsági szolgálatok, egyéb – titkos információgyűjtésre, titkos adatszerzésre, terrorelhárításra kijelölt – szervezetek helyének, szerepének, funkcióinak, valamint a tevékenységekre vonatkozó jogszabályi rendelkezések értelmezésére;
– a polgári nemzetbiztonsági tevékenység tipikus és sajátos eszközei és módszerei alkalmazásának megtervezésére, megszervezésére, a szakmai feladatok végrehajtására és irányítására;
– a szakmai tevékenység végzését szolgáló, segítő külső (nyílt és nem nyílt) információs források, adatbázisok, adattárak, nyilvántartások hozzáférési és adatkérési kezelésére;
– a nyílt és titkos forrásból beszerzett információk elemzésére, értékelésére, feldolgozására, hasznosítására, egyedi és összetett szakmai kérdések komplex értékelésére;
– a személyiség hatékony megismerésére, a bizalmon alapuló együttműködési viszony kialakítására, és a kommunikációs technikák helyzethez igazítására, a szakmai ismeretek átadására, az önművelésre, a szakmai tudás folyamatos fejlesztésére;
– a feladatnak megfelelő magatartás- és viselkedésformák alkalmazására.

Alapfokozat birtokában a polgári nemzetbiztonsági szakértők, leendő beosztott vezetők – a várható specializációkat is figyelembe véve – alkalmasak

– a nemzetbiztonsági, ideértve a felderítési, elhárítási és terrorelhárítási szakmai feladatok végrehajtása során a hazai nemzetbiztonsági szolgálatok, illetve rendvédelmi feladatokat ellátó szervek munkatársaival való hatékony együttműködésre, továbbá nemzetközi kapcsolattartásra és együttműködésre;

– a személy- és iparbiztonsági ellenőrzés gyakorlati feladatainak végrehajtására;
– a hatáskörbe utalt bűncselekmények elkövetési magatartásainak felismerésére, valamint a felderítéssel kapcsolatos gyakorlati tevékenységek végzésére.[13]

A mesterszintű képzésben jelenleg a nemzetbiztonsági szakon, azon belül pedig katonai és polgári nemzetbiztonsági specializáción belül folyik a képzés. 2017 végén megtörtént az alapszakra épülő *polgári nemzetbiztonsági mesterszak* akkreditálása a rendészettudományi karon. Az Oktatási Hivatal FNYF/7-12018. számú határozatával nyilvántartásba vette és engedélyezte a polgári nemzetbiztonsági mesterképzési szakot. A képzés célja olyan nemzetbiztonsági szakemberek oktatása, akik alkalmasak a közigazgatási, a katonai, a rendészeti, tudományos szektorokban vezetői és szakértői feladatok ellátására, szakmai ismereteik és gyakorlati készségeik alapján képesek nemzetbiztonsági problémák értékelésére, elemzésére és megoldására. Felkészültek a politikai intézmények, biztonsági folyamatok, közpolitikák működésének és ezeknek a globális biztonsági-politikai helyzettől függő összefüggésének és egymásra hatásának megértésére, kormányzati válaszok előkészítésének a támogatására. Felkészültségük alapján alkalmasak tanulmányaik doktori képzés keretében történő folytatására is.

A mesterképzésbe való felvétel feltétele, hogy a hallgatónak a kredit megállapítása alapjául szolgáló ismeretek – felsőoktatási törvényben meghatározott – összevetése alapján elismerhető legyen legalább 60 kredit a korábbi tanulmányai szerint a következő ismeretkörökben: társadalomtudományi és természettudományi ismeretek, állam- és jogtudományi ismeretek, rendészettudományi ismeretek, hadtudományi ismeretek, vezetési ismeretek, biztonságpolitikai ismeretek, általános igazgatási ismeretek, szakigazgatási ismeretek, közszolgálati ismeretek, európai uniós ismeretek, műszaki ismeretek, haditechnikai ismeretek, informatikai ismeretek, nemzetbiztonsági ismeretek.

A mesterképzésbe való felvétel feltétele, hogy a felsorolt ismeretkörökben legalább 30 kreditje legyen a hallgatónak. A hiányzó krediteket a mesterfokozat megszerzésére irányuló képzéssel párhuzamosan, a felvételtől számított két féléven belül, a felsőoktatási intézmény tanulmányi és vizsgaszabályzatában meghatározottak szerint kell megszerezni.[14]

---

13 7/2016. (II. 15.) MVM rendelet az államtudományi képzési terület alap- és mesterképzési szakjainak meghatározásáról és azok képzési és kimeneti követelményeiről.
14 Uo.

Nemzetbiztonsági jellegű képzések a hazai felsőoktatásban

A rendszerváltástól a Nemzeti Közszolgálati Egyetem Nemzetbiztonsági Intézetének megalakulása közötti időben megjelentek a nemzetbiztonsági képzések a polgári egyetemeken és főiskolákon is.

2001 őszén indult a *Budapesti Műszaki és Gazdaságtudományi Egyetem*en a Gazdaság- és Társadalomtudományi Kar információ- és tudásmenedzsment tanszék gondozásában a *gazdasági, üzleti, információ- (hír)szerzés oktatása,* először tanfolyami formában, 72 órában. A szervezők célja, hogy olyan módszereket, megoldási javaslatokat adjanak a vállalatvezetőknek, amelyekkel a legálisan megszerezhető hatósági és hivatali információkat minél jobban felhasználhatják és beépíthetik cégük döntéshozatali folyamataiba.[15]

A *Zsigmond Király Főiskolán, ma már egyetem*en nemzetbiztonság és biztonságpolitika szakirányú továbbképzés működik. A képzés először a 2010–2011-es tanévben indult. A képzési idő három félév, és a végén biztonságpolitikai (nemzetbiztonsági) elemző diploma szerezhető.

A szakirányú továbbképzés során érintett főbb témakörök:

– alapvető nemzeti és nemzetközi politikai, gazdasági és jogi ismeretek;
– a nemzetközi biztonságpolitikai helyzet alakulása;
– a nemzetbiztonság, a nemzeti értékek és érdekek megfelelő értelmezése;
– a nemzetbiztonságot érintő stratégiák, koncepciók, elméletek alkalmazási készsége;
– a nemzeti stratégiák, értékek, érdekek és célok;
– a társadalom és az állam döntéshozatali rendszere;
– az információ döntéshozatali rendszerben betöltött jelentősége;
– az információ elemzés-értékelés, tájékoztatás rendszere;
– a nemzetbiztonsági tevékenység specialitásai.[16]

A *Budapesti Corvinus Egyetem*en pedig alapszakon a nemzetközi tanulmányok keretein belül *diplomácia és hírszerzés* témakörében lehet ismereteket szerezni.

A tantárgy szakmai tartalma: a hallgatók kapjanak általános és – a vonatkozó törvények lehetőségein belül – konkrét ismereteket a titkosszolgálatok,

15 Domokos Erika: Megkezdődött az üzleti hírszerzés oktatása a Műszaki Egyetemen. Napi.hu, 2001. november 14. http://www.napi.hu/redirectedbyprint/titleunknown.97332.html

16 http://www.uni-zsigmond.hu/kepzesek/olvas/nemzetbiztonsag-es-biztonsagpolitika-szakiranyu-tovabbkepzes

elsősorban a hírszerzés történetéről, működéséről, a diplomácia és a hírszerzés azonosságairól és különbözőségeiről, helyéről, szerepéről az államigazgatás rendszerében, az államszervezetben betöltött szerepükről, az együttműködés lehetséges területeiről.[17]

Összegzés

A rendszerváltozás után először a katonai szolgálatoknál mutatkozott igény a nemzetbiztonsági felsőoktatás megszervezésére. A Nemzeti Közszolgálati Egyetem megalakulása azután megteremtette a feltételeket ahhoz, hogy a polgári nemzetbiztonsági szolgálatok is aktívan bekapcsolódjanak az egyetemen folyó nemzetbiztonsági képzésbe és az ottani tudományos munkába. A XXI. század biztonsági és nemzetbiztonsági feladatai még inkább szükségessé teszik a kiemelkedően felkészült nemzetbiztonsági szakemberek alkalmazását. A katonai és polgári nemzetbiztonsági mesterszak képzései mindezt lehetővé teszik.

17 http://portal.uni-corvinus.hu/index.php?id=22720&tanKod=7NK40NFV29B

DOI: 10.38146/BSZ.2018.2.2

KOLLÁR CSABA

Az információbiztonság humán aspektusai[1]

A biztonságtudatossági ellenőrzés során alkalmazott social engineering technikák elemzése a SPEAKING modell segítségével

Az információs társadalomban, illetve az e fogalmat fokozatosan leváltó digitális korban, vagy más néven az adatok korában az ezt megelőző korokhoz képest másfajta értékek kerültek a középpontba. A hálózatba kapcsolt vezetékes és vezeték nélküli kommunikációs eszközök (asztali számítógépek, szerverek, okostelefonok, laptopok, tabletek stb.) révén – feltételezve az aktív infokommunikációs kapcsolatot az egyén készüléke és a hálózat között – az emberek aktivitásának egyre nagyobb része valósul meg a digitális világban, a kibertérben. Az olyan tevékenységek mellett, mint a kommunikáció, vagy a munka, a számunkra értékes adatok és információk tárházai is a kibertérbe költöztek, s e folyamat nemcsak az egyénekre, hanem a szervezetekre is jellemző. Az adatok, az információk felértékelődésével párhuzamosan újfajta egyéni és szervezett bűnözési formák jelentek meg. Az elkövetők számára az értéket nem vagy nem elsősorban maga az eltulajdonított tárgy jelenti, hanem az informatikai adathordozón lévő adatok, információk, adatbázisok. A bűnesetek egy részében nem is tárgyakat, hanem csak adatokat és információkat lopnak el az elkövetők. Ez után a megbízóik kívánságainak megfelelően manipulálják, átírják, vagy törlik az adatbázisok, a publikusan, illetve csak a belső hálózatból elérhető weblapok tartalmát stb. Hiba lenne azt állítani, hogy ezek a feladatok kivétel nélkül jelentős informatikai/programozói tudást igényelnek, annál is inkább, mivel a bűnszervezetekben elkövetett tevékenységek jelentős részénél megfigyelhető a munkamegosztás. Az egy területre (például adathalászat, nyomeltakarítás, szerverek feltörése) szakosodott szakemberek között megjelennek azok a bűnelkövetők, akik elsősorban már nem a kódolással, kódfejtéssel foglalkoznak, hanem a kommunikációs, pszichológiai, szociálpszichológiai modellek és általánosságban az emberi visel-

1 A tanulmány az Emberi Erőforrások Minisztériuma ÚNKP-17-3-I-OE-779/45 kódszámú Új Nemzeti Kiválósági Programjának támogatásával készült.

kedés magas fokú ismerői. A feladatuk pedig, hogy a komplex informatikai védelemmel felvértezett szervezetek legsebezhetőbb pontját, rendszerint az azt üzemeltető, fenntartó, fejlesztő, használó (munkavégző) embert vegyék célba, s olyan helyzeteket teremtsenek, ahol a célszemély az általuk elvárt módon viselkedjen. Magyar nyelven is megjelent a *Kevin D. Mitnick* életével foglalkozó két könyv[2], amelyben a főszereplő-szerző külön fejezetben tárgyalja a megtévesztés művészetét, a *social engineering*et. A szerzők megfogalmazása szerint *„a támadó az emberi természet legnemesebb tulajdonságát használja ki: azt a természetes törekvésünket, hogy segítőkészek, udvariasak, pozitívak legyünk, csapatjátékosként viselkedjünk, illetve azt a vágyunkat, hogy elvégezzük a munkánkat”.*

A hackerszubkultúrától a bűnszervezeteken át az információs hadszíntérig

A hackerkultúrával számos könyv foglalkozik[3], gyökerei egészen az 1980-as évekig nyúlnak vissza[4]. Az 1990-es években a jelenséggel már a hatóságok is foglalkoztak[5], az akkor még a nyomaik eltüntetésével nem igazán foglalkozó, a hackelésre inkább csak szubkultúraként tekintő fiatalok számára egy-egy weboldal feltörése, vagy az adatok megszerzése – bár tevékenységükkel törvényt sértettek – egyfajta elismertség kivívásának számított a csoporton belül. A könyv említést tesz a *Fry Guy* nevű hackerről, aki már a humán típusú *social engineering* technikákkal is foglalkozott („kiváló beszélőkészsége volt”), illetve röviden ismerteti a telefonos *social engineering* technikát, hangsúlyozva, hogy az informatikai rendszerekben az azzal kapcsolatban álló ember a leggyengébb láncszem. Ugyancsak a fiatalok történeteit meséli el érdekes és olvasmányos formában *Dreyfus és Assange*[6]. A szerzők megadják a humán típusú *social engineering* ma is elfogadható rövid leírását, miszerint: *„a social engineering a sima/gördülékeny beszédet jelenti azokkal a hatalmi pozícióban lévő emberekkel, akik tesznek valamit a beszélő számára”.*

2 Kevin D. Mitnick – William L. Simon: A legendás hacker. A megtévesztés művészete. Perfact Kiadó, Budapest, 2003; Kevin D. Mitnick – William L. Simon: A legendás hacker. A behatolás művészete. Perfact Kiadó, Budapest, 2006

3 https://percomis.wordpress.com/2013/05/10/hacker-konyvek/

4 Steven Levy: Hackers: Heroes of the Computer Revolution. O’Reilly, New York, 2010

5 Bruce Sterling: The Hacker Crackdown: Law And Disorder On The Electronic Frontier Mass Market. Bantam, New York, 1993

6 Suelette Dreyfus – Julian Assange: Underground. Red Book, Sydney, 1997

Russel[7] egy olyan, számos gyakorló kiberbiztonsági szakember bevonásával megírt művet jegyez, amelyiknél a történet bemutatja, hogy hogyan használta fel a főszereplő (Bob) a hackereket arra, hogy egymástól függetlenül különböző részfeladatokat teljesítsenek (például betörések, adatmanipuláció, adatlopás) annak érdekében, hogy a végén ő meggazdagodhasson. A regény üzenete az, hogy a kiváló szervezőkészséggel, de alapvetően komoly hackertudással nem bíró személyek hogyan tudják befolyásolni a kellően szűk látókörű, s „csak" az informatikához értő hackereket – ez egyfajta példaként szolgált arra is, amit később vállalkozások/kormányok megvalósítottak: megbíztak (igaz, rendszerint fizetésért cserébe) hackereket a (bűn)cselekmények elvégzésével. *Poulsen*[8] *Max Butler* megtörtént eseteken alapuló történetét meséli el, aki a bankkártyaadatok feketepiaca feletti ellenőrzést vette át. A könyv a kibervilágban működő bűnszervezetek tevékenységével is foglalkozik.

Ha a hackerek tevékenységét, tudását és értékét az idő folyásában vizsgáljuk, akkor megállapíthatjuk, hogy a korábbi tizenévesek által elkövetett informatikai csínytevések (bár a jelenlegi fiataloknak is kihívást jelent egy-egy weboldal, vagy Facebook-profil feltörése) mellett megjelentek, jelenleg pedig arányait és gazdasági/társadalmi hatását tekintve sokkal gyakrabban találkozhatunk a szervezett bűnözés körébe tartozó hackertámadásokkal. Ezeknél a technikai tudás mellett a szervezőkészség és az álcázás jellemzi a csoportot, amely elsősorban a közvetlen és közvetett anyagi haszonszerzés érdekében végzi tevékenységét, eleget téve a szervezeti, illetve kormányzati megbízásoknak.

Haig és Várhegyi[9] megkülönbözteti az információs hadműveletek között a fizikai, az információs és a tudati dimenziót. Utóbbinál *„közvetlenül az emberi gondolkodást, észlelést, érzékelést, értelmezést, véleményt, vélekedést veszik célba valós, csúsztatott hamis üzenetekkel, amelyeket többek között […] közvetlen beszéd formájában továbbítanak"*. A leírtak és a humán alapú *social engineering* típusú támadások közötti kapcsolat egyértelmű.

7 Ryan Russell: A Háló kalózai. Hogyan lopjunk kontinenst. Kiskapu Kiadó, Budapest, 2005
8 Kevin Poulsen: Kingpin: How One Hacker Took Over the Billion-Dollar Cybercrime Underground. Broadway Paperbacks, New York, 2011
9 Haig Zsolt – Várhegyi István: Hadviselés az információs hadszíntéren. Zrínyi Kiadó, Budapest, 2005

A social engineering értelmezése a személyközi kommunikációs viszonyok között

Ahogy arra már utaltam, a humán alapú *social engineer* támadások alapját elsősorban nem az informatikai, hanem a kommunikációs, pszichológiai, szociálpszichológiai és szociológiai tudás, s e tudás gyakorlati felhasználása és alkalmazása jelenti. Az ember születésétől egészen haláláig szocializációs folyamat(ok)ban vesz részt. Ennek részeként megtanulja az interperszonális kommunikációt fenntartó és mozgató erőket, a különböző társas viszonyokat[10], az első benyomásból megszerezhető információkat, a csoportnormákhoz történő igazodást, a szeretet (szimpátia) és a segítségnyújtás módjait és lehetőségeit, a csoportközi konfliktusok kezelését[11]. Ez a gyakorlati tudás/tapasztalat segíti az egyént abban, hogy a társadalomban, és azon belül a kisebb csoportokban (család, munkahely, iskola, baráti kapcsolatok stb.) otthonosan mozogjon, felismerje a csoporton belüli erőviszonyokat, kialakítsa, meghatározza, megerősítse helyét a csoporton belül, olyan diskurzusokat folytasson, amelyek révén el tudja érni és/vagy céljai érdekében tudja manipulálni beszélgetőpartnerét. Azzal, hogy az ember társas lény[12], késztetést érez arra, hogy egy vagy több csoport tagja legyen, s ha a csoporton belül biztonságban érzi magát, akkor rendszerint megtöri a csendet, és magáról, maga és a csoport viszonyáról közöl információkat, illetve ha a személyes/intim szféráját nem érintő kérdéseket kap, akkor azokra magától értődő módon válaszol is. A közlések és a válaszok többségében megjelennek az érzelmek, illetve az egyén olyan szituációban van/szituációba hozható, amikor megnyilvánulásai mögött érzelmek vannak, mint például harag, félelem, meglepődés, öröm, szomorúság, vidámság, megelégedettség, bűntudat. *Atkinson*[13] nyolc elsődleges érzelmet és a hozzájuk tartozó helyzeteket ismerteti *(táblázat)*.

A *social engineer* már az alapérzelmek és a felismert, beazonosított helyzetek alapján is sikeres támadást tud megvalósítani áldozatával szemben. A személyközi kommunikáció során az Atkinson és társai[14] által bemutatott helyzeti tényezőket is ki tudja használni a támadó azzal, hogy olyan kommunikációs helyzetet épít fel, amelynek az alapját a következő tényezők jelentik:

10 Miles Hewstone – Wolfgang Stroebe – Jean-Paul Codol – Geoffrey M. Stephenson (szerk.): Szociálpszichológia európai szemszögből. KJK, Budapest, 1999

11 Eliot R. Smith – Diane M. Mackie: Szociálpszichológia. Osiris Kiadó, Budapest, 2001

12 Elliot Aronson: The Social Animal. Freeman, San Francisco, 1972

13 Rita L. Atkinson – Richard C. Atkinson – Edward E. Smith – Daryl J. Bem: Pszichológia. Osiris Kiadó, Budapest, 1997

14 Uo.

1. kívánatos és megtörténik: öröm;
2. kívánatos és nem történik meg: bánat;
3. nemkívánatos és megtörténik: aggódás;
4. nemkívánatos és nem történik meg: megkönnyebbülés.

Az eddig felsorolt érzelmek mellett *Oroszi*[15] és a saját véleményem szerint a következő tulajdonságok teszik sebezhetővé, kihasználhatóvá a *social engineer*ek által megtámadott személyt: bosszúállás, befolyásolhatóság, emberi hanyagság és figyelmetlenség, hiszékenység és naivság, kényelmesség, konfliktuskerülés, segítőkészség, tekintélyelvűség, tudatlanság és szakképzetlenség, (szexuális) vonzalom, szimpátia/antipátia.

Érzelem	Helyzet	Munkahelyi példa
1. Szomorúság	Szeretett személy elvesztése	Munkahely elvesztése. Kolléga kilép/kirúgják a munkahelyről.
2. Félelem	Fenyegetettség	Elveszíthetem a munkahelyemet. Nálam jobb, okosabb, csinosabb stb. új kolléga pályázik a helyemre. Nem tudom idejében elvégezni a munkámat. Félek, hogy megint megszid/megszégyenít a főnököm.
3. Harag	Akadály	Utálom a főnökömet, kollégáimat. Nem tudok szakmailag fejlődni. Nem tudom ezt az új rendszert használni.
4. Öröm	Potenciális társ	Kedvelem a kollégáimat. Ő a legjobb munkatársam.
5. Bizalom	Csoporttag	Tudom, hogy a kollégákkal együtt meg tudom csinálni. Jó, hogy van olyan kollégám, akire számíthatok.
6. Undor	Förtelmes tárgy	Utálom a munkámat. Utálom a munkaeszközeimet (például számítógép).
7. Anticipáció	Új territórium	A főnököm magasabb pozíciót ígért nekem, ha megteszem, amit kér. Elhitetik velem, hogy a ranglétrán feljebb léphetek.
8. Meglepődés	Hirtelen új tárgy	Új szoftvert kell alkalmazni holnaptól. Új belépési rend lépett életbe.

15 Oroszi Eszter Diána: Social Engineering: Az emberi erőforrás, mint az információbiztonság kritikus tényezője. Budapesti Corvinus Egyetem, Budapest, 2008. http://krasznay.hu/presentation/diploma_oroszi.pdf

Balázs[16] úgy fogalmaz az érzelmi zavarok kapcsán, hogy *„túlzott emocionális reakcióknál általában a helyzet téves értékelése, az észlelés beszűkülése és torzulása következhet be, valamint a magatartáskészlet kimerülése”. A social engineer* sikerességének tehát az az alapvető mércéje, hogy érzelmi zavarkeltés során képes-e a megtámadottban elérni, hogy a helyzetet a támadó által kívánt módon értékelje, a megtámadott észlelése csak a támadó által szabályozott módon történjen, magatartáskészletében a támadó által elvárt eszközöket használja, illetve szerepet vegye fel.

A gyakoribb szereprelációk (T = támadó, Á = áldozat és/vagy balek) a következők:

– a dohányzó külsős kolléga, beszállító, vásárló (T) – a kijelölt helyen (vagy éppen a tilosban) dohányzók (Á);
– a vállalat székhelyén dolgozó, legfrissebb híreket ismerő kolléga (T) – a telephelyen dolgozó, az információhiány miatt sorsukat bizonytalannak ítélő kollégák (Á);
– az esőben elázott, vékony testalkatú, szemüveges pizzafutár, kerékpáros futár (T) – hasonló életkorú gyermeket nevelő nő (Á);
– az új kolléga, aki segítséget kér a vállalat informatikai rendszereinek a használatához (T) – a kollégák, akik segítenek neki (Á);
– beszállító cég intelligens, sármos középvezetője (T) – a harmincas éveiben járó, a férfiak megbecsülését és igaz szerelmét kereső nő (Á);
– feltűnően csinos és kívánatos nő (T) – saját magát túlértékelő, szexuális vágytól fűtött férfi (Á).

A szakszerűség és megbízhatóság szereprelációi:

– a vállalat tevékenységét ellenőrző külsős személy (T) – a vállalat alkalmazottai (főleg azok, akik tudják, hogy valamilyen munkát nem vagy nem megfelelő minőségben, vagy csak a megadott határidőn túl végeztek el) (Á);
– az informatikus/rendszergazda (T) – a számítógéphez és/vagy az informatikai rendszerhez nem értő kolléga (Á).

Egyéb szereprelációk (általában nem alakul ki szimpátia, de hagyják tevékenykedni az álcázott támadókat):

– karbantartók, javítók (T) – dolgozók (Á);
– kerékpáros futárok, postások, csomagszállítók (T) – dolgozók (Á);
– pénz- és értékszállítók (T) – dolgozók (Á);
– takarítók (T) – dolgozók (Á).

16 Balázs István (szerk.): Pszichológiai lexikon. Magyar Könyvklub, Budapest, 2002

A biztonságtudatossági ellenőrzés kommunikációelméleti megközelítése

A kommunikációs fókuszú biztonságtudatossági ellenőrzés során a szervezet és belső érintettjei, így munkatársai, vezetői, bizonyos esetekben alvállalkozói és beszállítói által közölt információkat, illetve a különböző (személyközi) kommunikációs helyzetekben tanúsított magatartásukat vizsgálják. Tanulmányomban csak a nyílt forrású hírszerzéssel és a *social engineering* típusú módszerekkel foglalkozom, a szabályozásokkal, munkaköri leírásokkal, a fizikai biztonság kialakításának és fejlesztésének módszereivel stb. nem, vagy csak érintőlegesen.

A nyílt forrású hírszerzés *(Open Source Intelligence; OSINT)* során az ellenőrök (illetve, ha nem ellenőrzésről van szó, akkor a támadók) egyebek között a következő forrásokból szereznek szervezeti információkat (NATO, *Lévay*[17]*, Izsa*[18]*,* illetve saját megjegyzések):

– a szervezet munkatársainak digitális lábnyomai;
– a szervezet munkatársaival folytatott beszélgetések;
– a szervezet beszállítóival, vásárlóival, versenytársaival folytatott beszélgetések;
– a szervezet publikus sajtóanyagai (például sajtóközlemények);
– a szervezet weboldalai és egyéb webes platformjai (például LinkedIn, Facebook);
– a szervezetről a nyomtatott és elektronikus médiában megjelenő hírek, információk;
– az internetes keresőkkel megtalálható tartalmak;
– az internet sötét tartalmai *(dark web);*
– kereskedelmi (fizetős) online szolgáltatók tanulmányai, adattárai;
– kereskedelmi műholdak felvételei;
– nem kormányzati szervek (NGO) (például Amnesty International, Nemzetközi Vöröskereszt, Orvosok Határok Nélkül) hivatalos anyagai és az alkalmazottjaival, szakembereivel folytatott beszélgetések;
– szakmai szövetségek, kamarák, érdekképviseleti szervezetek adott szervezetről is szóló beszámolói, elemzései;
– személyes tapasztalatok;

17 Lévay Gábor: OSINT (Open Source Intelligence). Nyílt információs hírszerzés. Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2006
18 Izsa Jenő: Nemzetbiztonsági alapismeretek. Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2009

– szürke irodalom: nem publikált és nem is minősített dokumentumok, tanulmányok, jelentések, amelyek „okos böngészéssel” megtalálhatók;
– tudományos előadások, konferenciák, ahol a szervezetről elhangzanak információk;
– tudományos-kutató szervezetek, egyetemek (például az adott szervezettel közösen végzett kutatások, fejlesztések).

Az adatok és információk feldolgozását segítheti, ha valamelyik kommunikációs modellt használják az elemzők. *Griffin*[19] és *Horányi*[20] számos, a gyakorlatban is alkalmazható kommunikációs modellt mutat be könyveiben, ezek közül az OSINT esetében *Shannon és Weaver*[21] alapmodellje is megfelelő lehet. A küldő meghatározása során ki lehet térni a jogosultságokra (például van-e joga az adott személynek a szervezetről információt megadni), a küldés céljára, a szándékolt, vagy épp ellenkezőleg a felelőtlen közlésre (például egy titkárnő egy Facebook-csoportban kér segítséget azzal a megjegyzéssel, hogy most vezette be az önkormányzat az új szoftvert, de senki nem tudja kezelni). A csatorna elemzésekor részint szabályozni lehet, hogy kinek van joga az adott csatornán a szervezettel kapcsolatos információkat megosztani, de akár az is szabályozható, hogy az adott személy ezt a csatornát nem használhatja. A szervezet azt is megvizsgálhatja, hogy melyek azok a csatornák, amelyeken a szervezetről megjelennek ugyan bizonyos információk, de ezeket a csatornákat nem szeretné a jövőben használni, vagy ellenkezőleg: markánsabban szeretné. A címzett a nyílt forrású információknál mindenki lehet, aki az üzenetet olvassa (még akkor is nyíltnak tekinthető, hogy egy olyan zárt Facebook-csoportban került sor a publikálásra, amihez csatlakozni kell ahhoz, hogy az ott közölt tartalom megtekinthető legyen). Ez lehetővé teszi, hogy a szervezet a konkurencia tudatos félrevezetése céljából hamis információkat adjon meg.

A humán alapú *social engineering* biztonságtudatossági ellenőrzés célja az, hogy modellezett helyzetben/szituációban az ellenőrzés alá vont személyek hogyan viselkednek akkor, amikor a támadó (aki szerepe szerint ügyfél, kolléga stb.) olyan dologra kéri őket, ami a biztonsági szabályzattal ellentétes, vagy olyan kérdésekre válaszolnak, aminek révén ha nem is titkos, de bi-

19 Em Griffin: Bevezetés a kommunikációelméletbe. Harmat Kiadó, Budapest, 2001
20 Horányi Özséb (szerk.): Kommunikáció I–II. General Press, Budapest, 2003
21 Claude E. Shannon: The mathematical theory of communication. In: Claude E. Shannon – Warren Weaver: The mathematical theory of communication. The University of Illinois Press, Urbana, 1964

zalmas információkat mondanak el illetékteleneknek. A *social engineering* (akár támadó, akár ellenőrző céllal történik is) általános lépései a következők:

1. A terv alapozása (találkozás a megbízóval, „szerződés” előkészítése).
2. Felderítés, információszerzés (hírszerzés nyílt forrásokból).
3. Megfelelő célszemély(ek) kiválasztása.
4. A támadás előkészítése (információk kiértékelése, helyszín, módszer, szereplők, történet, időtáv stb. kiválasztása, a megszerzendő adatok és információk meghatározása, „szerződés” elfogadása).
5. Megtévesztés – a bizalom megszerzése (a *social attack* indítása – az első négy másodperc, valamint az első néhány mondat).
6. A megszerzett bizalom kihasználása (például beszélgetés folytatása, bejutás elzárt részekbe).
7. A támadás előkészítése során meghatározott adatok és információk megszerzése.
8. A beszélgetés zárása és/vagy a nyomok eltüntetése.
9. A helyszín elhagyása.
10. A megszerzett adatok és információk feldolgozása és/vagy átadása a megbízónak feldolgozásra.
11. A támadás kiértékelése, tapasztalatok megfogalmazása.

A támadás elemzésére az előbbiekben nevezett forrásokban található modellek közül alapozásként *Philipsen* elméletét, a bemutatott három esettanulmánynál pedig *Hymes* SPEAKING modelljét veszem alapul.

Philipsen beszédkódelmélete

Philipsen beszédkódelmélete[22] öt tételben foglalható össze. Tanulmányomban az öt tétel *social engineering*gel kapcsolatos saját meglátásom szerinti átiratát ismertetem.

1. tétel: egy sajátos kultúrához minden esetben egy sajátos beszédkód társul. Ha a vállalati diskurzusokat leírjuk, akkor felületes szemlélőként közel sem biztos, hogy észrevesszük a sajátos beszédkódokat. A munkatársak egymás közötti beszélgetéseiben, vagy a szervezet hivatalos kommunikációjában (például sajtóközlemények, reklámok, vállalati tájékoztató anyagok) használt szavak és szófordulatok gyakorlatilag mindenki számára megérhetők, akik az

22 Gerry Philipsen: A beszédkódok elmélete. A kommunikáció etnográfiája. In: Em Griffin: i. m. 428–439. o.

adott nyelven beszélnek. Ha azonban a rendelkezésünkre álló szövegkorpuszokat alaposabban elemezzük, legalább két fontos különbségre figyelhetünk fel. 1. Vannak olyan rövidítések, szavak, szókapcsolatok, szófordulatok, amelyeket az adott szervezet kizárólag, vagy legalábbis az átlaghoz képest sokkal gyakrabban használ. Ha ezeken a szövegeken szógyakorisági elemzést végeznénk, s az eredményeket egy szófelhőben ábrázolnánk, egyértelművé és láthatóvá tudnánk tenni, hogy melyek ezek a szavak, szókapcsolatok, szófordulatok. 2. Vannak olyan szavak és szókapcsolatok, amelyek egy adott iparágban/ágazatban dolgozók számára egyfajta összetartozást jelentenek (kulturális/szakmai közösség és hovatartozás), s már néhány mondat után képesek lehetnek észrevenni azt, ha valaki csak felszínesen és hibásan tárja fel ezeket az ismereteit a beszélgetés során. Az összetartozás beszédkódjai egyebek között: a szakmai fogalmak, a szakma alapművei és szerzői, a szakma fontosabb képzőhelyei (közép- és felsőoktatási intézmények), a szakma hazai és nemzetközi rendezvényei, a szakmai tevékenységet folytatók egyesületei/szövetségei, illetve a különböző felügyeleti szervek.

Megjegyzem, hogy léteznek olyan vállalatok, ahol a(z írásbeli) kommunikáció hatékonyságának növelésére kidolgoztak és bevezettek olyan, néhány betűből álló mozaikszavakat, amelyek például az anyacég és a külföldi leányvállalatai közötti kommunikációt azzal teszik időben hatékonyabbá, hogy nem kell a levelezésekben, vagy beszámolókban kiírni a mozaikszavak jelentését, hiszen azok a vállalati beszédkódok mindenki által ismert halmazába tartoznak. Az ilyen mozaikszavak jelentésének ismerete és használata révén a *social engineer*ek sokkal könnyebben képesek a vállalat alkalmazottainak a bizalmába férkőzni.

2. tétel: egy beszédkód magában foglal bizonyos kulturális vonatkozású pszichológiai, társadalmi, retorikai különbségeket. A pszichológiai manipuláció során a megtámadott kommunikációs ágens viselkedésével, mondataival elárulja a szervezetben betöltött szerepét, sőt az esetek jelentős részében azt ki is hangsúlyozza. A manipuláció részeként e szerep megerősítése sikeresebbé teheti a támadást. A szociológiai megközelítésnél az egyén nemcsak magáról, hanem maga és a szervezet többi tagjának kapcsolatáról is ad információt. A *social engineer*ek szerint, ha az egyén tudatosan el akar határolódni a szervezettől, vagy annak bizonyos csoportjaitól (például mérnökök kontra fizikai munkások), akkor ezt a beszédkódokban is kifejezésre juttatja. Ennek felismerése révén a támadó olyan beszédkódokat alkalmazhat, amelyek segítségével könnyebben tud a megtámadott ágens bizalmába férkőzni (például „legalább mi, melósok tartsunk össze”). A retorikai megközelítésnél – igazodva Philip-

sen felvetéséhez – fontos a tekintély vizsgálata és a beszédkódok révén a megfelelő tekintélyviszony kialakítása a támadó és az áldozat között. Amikor a támadás során a támadó az adott szituációt valós időben elemzi, könnyen felméri, hogy inkább az egy csapatba tartozás (szociológia), vagy inkább az alá-fölé rendeltség (tekintély) elve szerint alakítsa-e ki a kommunikációs keretet. Utóbbinál például a segítséget kérő harmincas, dögös támadó nő kihangsúlyozza, hogy mennyire férfiasnak értékeli a manipulálandó biztonsági őrt.

3. tétel: a beszéd jelentősége függ a beszélő és a hallgató által használt beszédkódoktól, amelyeket abból a célból alkalmaznak, hogy segítségükkel létrehozzák és értelmezzék kommunikációjukat. Ezt a tételt némiképp át kell fogalmazni a *social engineering* típusú támadások elemezhetősége érdekében: a manipuláció technikáit jól ismerő támadó olyan keretet ad a beszélgetésnek, ahol akár közvetlen, akár közvetett irányító szerepben határozza meg a beszéd jelentőségét. A *social engineering* típusú támadásoknál a kialakított beszédaktusok bensőségesek, nyíltak, támogató jellegűek lehetnek. A bensőséges viszony rövid időn belüli kialakítása azért is fontos, mert ha a megtámadott ágens mindvégig távolságtartó marad, akkor nem vagy csak részben mondja el a megszerezni kívánt információkat. A nyílt kapcsolat keretében a támadó rugalmas, és úgy alakítja a beszélgetést, hogy ez a rugalmasság megváltoztassa az ágens esetleg merev hozzáállását. A *social engineer* a megtámadott ágens bizalmába tud férkőzni azáltal, hogy támogató jellegű kapcsolatot épít ki és tart fenn a beszédesemény során [például segítséget nyújt neki, vagy bizalmas(nak tűnő) információkat oszt meg vele].

4. tétel: a beszédkódot meghatározó fogalmak, szabályok, premisszák kibogozhatatlanul bele vannak szövődve magába a beszédbe. Az 1. tételnél leírtakat azzal szeretném itt kiegészíteni, hogy a szervezetek jelentős része nem kellő körültekintéssel szabályozza azt, hogy melyek azok az információk, amelyek bárki számára elérhetők a nyilvános platformokon (beleértve a munkatársak/vezetők Facebook-és LinkediIn-oldalait is). A beszédkód fogalmát ennél a tételnél vizsgálódásom fókuszában célszerű kiterjesztett formájában használni. A szervezet és a támadó közötti kommunikáció során elfogadjuk azt, hogy mindkét fél multiplatformos kommunikációt folytathat úgy, hogy a támadási szándék csak a *social engineert* jellemzi, illetve az információ átadásában harmadik, negyedik stb. fél, felek is részt vehetnek.

5. tétel: egy közös beszédkód mesteri alkalmazása elegendő feltétel ahhoz, hogy előre jelezzük, értelmezzük vagy kontrolláljuk a kommunikációs viselkedés érthetőségéről, tisztaságáról és moráljáról folyó diskurzust. Mivel a beszédkódok körébe tartoznak a verbális, nonverbális, illetve metakommu-

nikatív kódok is (a tétel eredeti értelmezésében elsősorban ez utóbbival foglalkozik a szerző), ezek ismerete az adott szituációban segíti a *social engineer*t, hogy megjósolja, illetve kellő szakmai tudás birtokában irányítsa is a beszélgetést úgy, hogy a megtámadott ágens ebből semmit ne vegyen észre.

Az öt tétel összefoglalva:

1. tétel: a szervezeti kultúrához minden esetben sajátos beszédkód társul, aminek megismerése a sikeres *social engineering* akciók egyik alapfeltétele.

2. tétel: a szervezetek munkatársai által használt beszédkód magában foglal bizonyos kulturális vonatkozású pszichológiai, társadalmi, retorikai különbségeket, ezek ismerete és felismerése révén a *social engineer* a megtámadott munkatárs bizalmába tud férkőzni.

3. tétel: a manipuláció technikáit jól ismerő *social engineer* olyan keretet ad a beszélgetésnek, ahol akár közvetlen, akár közvetett irányító szerepben határozza meg a beszéd jelentőségét, tartalmát és folyamát.

4. tétel: a szervezet és a *social engineer* közötti kommunikáció során elfogadjuk, hogy mindkét fél multiplatformos kommunikációt folytat, s a támadó igazi szándéka a beszédből önmagában nem vagy csak nehezen bogozható ki.

5. tétel: a *social engineer* a verbális, nonverbális, illetve metakommunikatív kódok ismeretében úgy képes alakítani a beszélgetést, hogy abból a megtámadott ágens nem vesz észre semmit.

A SPEAKING modell

Hymes a személyközi kommunikáció beszédeseményeinek bemutatására és elemzésére egy olyan modellt dolgozott ki, aminél a beszélő szó angol változatának (SPEAKING) egyes betűiből épül fel a modell a következők szerint:

– *Setting/scene* (beszédhelyzet): a jelenet fizikai körülményeinek (hely, idő) leírására szolgál.
– *Participants* (résztvevők): támadó(k), áldozat(ok), mellékszereplők (például többi kolléga, ügyfél).
– *Ends* (lezárások): melyek azok a célok, amelyeket a támadó el akar érni? Ezek rendszerint a következők: bizalmas/titkos információk megszerzése beszélgetéssel, elérni, hogy beengedjék a nyilvánosságtól elzárt részekre, kapcsolatot kialakítani és fenntartani a további támadások érdekében.
– *Act sequences* (cselekménysorozatok): hogyan épül fel a támadás, milyen kulturális közegbe helyezhető (például köszönés, búcsúzás).

– *Key* (kulcs): milyen verbális, nonverbális, esetleg metakommunikációs elemeket használ a támadó (például a szerepéhez illeszkedő ruházat és kiegészítők, beszédstílus).
– *Instrumentalities* (eszközök): ide soroljuk a kommunikációs csatornákat (szóbeli, írásbeli, telefonos, internetes, közösségi média), a beszéd aktuális formáját (nyelv, szaknyelv, dialektus), valamint a formális nyelvet is (például jogi nyelvezetű üzenet az Országos Rendőr-főkapitányságtól).
– *Norms* (normák): a támadó eldöntheti, hogy a támadást normaszegésre, vagy normakövetésre építi-e fel, illetve meg tudunk különböztetni eltérő érintkezési normákat is (hangos/halk beszéd, kézfogás, távolság, összenézés, megölelés stb.).
– *Genre* (műfaj): fontosabb műfajok lehetnek a tájékoztató, az általános/szakmai beszélgetés, az általános információ kérése/adása, a javaslat, a segítségkérés és -nyújtás, a flörtölés stb.

Tanulmányomban terjedelmi okokból eltekintek a modell részletes bemutatásától, mivel az megtalálható egyebek között Hymes[23], *Ray és Biswas*[24]*, Zand-Vakili és társai*[25]*, Matel*[26]*,* illetve *Kollár*[27] írásaiban, így inkább három esettanulmányt mutatok be a modell gyakorlati felhasználását és hasznosságát szemléltetendő.

Három esettanulmány az elmélet bemutatására

A biztonsági ellenőrzés során a megadott szerepet játszó ellenőr (támadó) és az erről nem tudó munkatárs (áldozat) beszélgetéséről, tehát magáról a humán alapú *social engineering* típusú támadásról hang- és videofelvétel ké-

23 Dell Hymes: Models of the Interaction of Language and Social Life. In: John Gumperz – Dell Hymes (eds.): Directions in Sociolinguistics: The Ethnography of Communication. Holts Rinehart & Winston, New York, 1972, pp. 35–71.; Dell Hymes: Foundations in Sociolinguistics: An Ethnographic Approach. University of Pennsylvania Press, Philadelphia, 1974
24 Manas Ray – Chinmay Biswas: A study on Ethnography of communication: A discourse analysis with Hymes 'speaking model'. Journal of Education and Practice, vol. 2, no. 6, 2011, pp. 33–40.
25 Elham Zand-Vakili – Alireza Fard Kashani – Farhad Tabandeh: The Analysis of Speech Events and Hymes' SPEAKING. Factors in the Comedy Television Series: "FRIENDS". New Media and Mass Communication, 2012
26 Maldona Matel: "The Ethnography of communication". Bulletin of the Transilvania University of Brasov, vol. 2, no. 51, 2009
27 Kollár Csaba: Social engieering a gyakorlatban. Manipulációk értelmezése a SPEAKING modellben. JEL-KÉP, 2017/3.

szül, így rendelkezésre áll egy olyan nyersanyag, ami alkalmas lehet a tudományos igényességű és a gyakorlati életben is alkalmazható elemzésre, majd ennek alapján a biztonságtudatossági programok és tananyagok fejlesztésére. Az esettanulmányok megszervezésénél és elemzésénél *Horváth és Mitev*[28], *Dooley*[29] és *Klenke*[30] munkáira hagyatkozom. Az esettanulmányok elemzésénél két kérdésre keresem a választ: 1. alkalmas-e Hymes SPEAKING modellje a humán típusú *social engineering* támadások elemzésére; illetve ha alkalmas, akkor 2. milyen általánosítható következtetések fogalmazhatók meg az esettanulmányok feldolgozása után. Az adatgyűjtésre 2016 negyedik és 2017 első negyedéve között került sor egy kereskedelmi bank két-két helyszínén (egy budapesti központ, egy regionális/megyei igazgatóság, két kiemelt bankfiók). Mivel a kiválasztott helyszíneken voltak videokamerák (igaz, egy részüket nagyobb felbontásúra kellett cserélni), s előzetesen mikrofonokat is telepítettünk, így a támadás napjára rendelkezésre állt a hang- és videorögzítéshez szükséges technikai háttér. A támadást az ellenőr/auditor a megadott forgatókönyv szerint hajtotta végre, a felvételek elemzése előtt erről tájékoztatták az érintetteket (áldozatok), akik hozzájárultak ahhoz, hogy a felvételeket tudományos céllal elemezzék. Jelen tanulmányban három esetet ismertetek: pizzafutár az ügyfélpultnál, informatikus kolléga a központból, dohányzásra kijelölt hely. Azért esett a választás ezekre az esetekre, mert nagyon világosan és teljeskörűen be lehet mutatni az ellenőrzés során alkalmazott humán típusú *social engineering* támadást a SPEAKING modellben.

Pizzafutár az ügyfélpultnál

Beszédhelyzet

A beszédhelyzet külső időbeli határa, vagyis a támadás teljes időtartama és a térbeli határ is több részre osztható. A teljes időkeret tizenhárom perc volt, ebből a belső időhatár (vagyis, aminek az elemzése az esetleírásnál részletesebben szerepel) négy perc, ezt követte egy másik térben (folyosóról nyíló szoba/szobák) megvalósított adatgyűjtés (ez nem része az elemzésnek), ami hét perc, majd visszatérés az eredeti helyszínre, elköszönés és távozás (két perc). A külső térbeli határ a bankfiók ügyfélpultja és annak környéke. A tá-

28 Horváth Dóra – Mitev Ariel: Alternatív kvalitatív kutatási kézikönyv. Alinea Kiadó, Budapest, 2015

29 Larry M. Dooley: Case Study Research and Theory Building. Advances in Developing Human Resources, iss. 4, 2002, p. 335.

30 Karin Klenke: Qualitative Research in the Study of Leadership. Emerald Group, Bingley, 2008

madás szempontjából a külső térbeli határhoz tartozik az időjárás (borongós, esős idő), a belső térbeli határon a támadó nem változtatott, vagyis a beszélgetést mindvégig úgy irányította, hogy a banki munkatárs a helyén maradjon. A bankban több ügyfélpult volt, a támadó azt választotta ki, amelyiknél a szára optimális banki ügyintéző foglalt helyet (lásd később), s legközelebb volt a biztonsági őr által (elvileg) védett, a lezárt folyosóra nyíló ajtóhoz. A támadás délelőtt történt, a hónap elején (az eső ellenére is többen intézték a banki ügyeiket), az időjárás miatt az emberek hangulata nyomott volt.

Résztvevők

A támadó munkáját megkönnyítette, hogy a biztonsági őr nem volt a helyén. A résztvevőket a támadás szempontjából a következő csoportokba lehet sorolni:

– közvetett résztvevők: ügyfelek, banki alkalmazottak. A banki alkalmazottak kizárása fontos volt a támadás eredményessége szempontjából;
– közvetlen résztvevők: támadó, banki alkalmazott (ügyfélpultos).

A támadó szerepe: kinézetre pizzafutár (céges póló, pizzaszállító táska a kezében), aki elázott, s szeretne elmenni a mosdóba. Húsz év körüli, vékony testalkatú, szimpatikus fiatal.

Az áldozat: negyvenes évei közepén járó nő, akinek a feltételezés szerint hasonló életkorú gyereke/keresztgyereke van/lehet, mint a támadó.

Lezárások

A cél két, egymásra épülő részből tevődik össze. 1. elérni az áldozatnál, hogy engedje be a támadót az ügyfelektől elzárt részbe, ahol a mosdó található; 2. amint a támadó bejutott, szerezzen meg valamelyik munkatárstól bizalmas adatokat, információkat úgy, hogy az irodájából elhoz valamilyen „adathordozót” (például okostelefon, névjegyek, banki szerződések stb.). A támadás mindkét cél tekintetében megvalósult.

Cselekménysorozat

A cselekmény felépítése a következő: 1. az esőben elázott pizzafutár belép a bankfiókba; 2. sorszámot kér az automatából; 3. az automata egy másik ügyintézőhöz irányítja, de ezt nem veszi figyelembe; 4. amikor a kijelzőn a ki-

szemelt ügyintéző pultszáma megjelenik, a kezében hangsúlyosan mutatva a számát tartalmazó lapot, odalép az ügyintézőhöz, a pizzafutáros hordtáskát a széken hagyja. Megjegyzem, hogy itt annyiban szerencséje volt, hogy az az ügyfél, akit az automata a kiszemelt ügyintézőhöz irányított volna, szintén felállt a székről, de a támadó nonverbálisan jelezte, hogy hamar fog végezni, s azt is, hogy siet; 5. a támadó illedelmesen köszön az ügyintézőnek, beszélgetnek néhány mondatban az időjárásról, majd megemlíti, hogy még „pisilni sincs időm, annyi megrendelést kell ma kivinnem", majd szól egy mondatban arról, hogy egyetemista, tandíjra gyűjt, ezért dolgozik; 6. a támadó elmondja a kérését, miszerint szeretne elmenni a mosdóba, illetve megkéri az áldozatot, hogy addig vigyázzon a pizzaszállító táskára; 7. az áldozat először a szabályokra hivatkozik ugyan, de néhány megerősítő mondat után beengedi a támadót azzal a megjegyzéssel, hogy siessen, s addig vigyáz a pizzaszállító táskára. Megjegyzem, hogy a modell szerint idáig tartott a cselekménysorozat, amely után a támadó meg tudta szerezni a szükséges bizalmas/titkos adatokat, s fennakadás nélkül el is hagyta a helyszínt.

Kulcs

A támadó emblémái és kulturális szignáljai (nonverbális kódok) két archetípus köré épültek. A fő archetípus a pizzafutár volt, aki egy létező cég emblémájával ellátott pólóban, farmerban, tornacipőben, kezében pizzaszállító táskával jelenik meg a beszédhelyzetben. Az érzelmileg jobban megérintő (a verbális és nonverbális üzenetek kongruenciájára épülő) archetípus „az én egyetemista gyerekem is lehetne" volt. Itt a támadó – ahogy arra már utaltam – sikeresen alakította az esőben elázó, a tandíjáért dolgozó egyetemistát, aki életkorából adódóan akár az áldozat egyetemista gyereke is lehetne. A szemüveg, a szemüveg megtörlése, a nedves haj és póló tovább erősítette ezt a szerepet. A támadó kedves, illemtudó, hangszíne barátságos. A társadalmi közhelyek szintjén bebizonyítja (elsősorban az áldozatnak), hogy vannak még rendes, dolgos fiatalok. A banki ügyintéző archetípusa a távolságtartó, az ügyre fókuszáló dolgozó, akiben a támadó kulcsainak segítségével ezt az archetípust át tudja írni anyára, keresztanyára.

Eszközök

A kommunikációs csatorna a személyközi kommunikáció során verbális és nonverbális. A jelentéstartalmak tekintetében épít a metakommunikatív jegyekre is.

Normák

A támadó ráveszi áldozatát, hogy normaszegést kövessen el, vagyis hogy beengedje az ügyfelektől elzárt területre.

Műfaj

Segítségkérés/-nyújtás, rövid beszélgetés.

Az informatikus kolléga a központból

Beszédhelyzet

A támadás három beszédhelyzetből tevődik össze: 1. a személyes látogatást megelőzően, ebédidőben a támadó felhívja a vidéki központ/igazgatóság egyik osztályát azzal az ürüggyel, hogy a budapesti központ informatikai igazgatóságáról jön, mindjárt odaér, és mivel nincs helyismerete, ezért megkéri az áldozatot, hogy várja a bejáratnál. 2. A támadó megérkezik a vidéki központba, ahol a kollégák szeretettel fogadják. A támadás időkerete nem lényeges, mivel az információkat valamennyi – számára fontos – gépről meg tudta szerezni, illetve az áldozatok hozzáférésein keresztül el tudja érni a vállalati adatbázisokat is. Megjegyzem, hogy ha nem audit, hanem éles támadás lett volna, akkor a támadó kártékony kódokat is tudott volna telepíteni a gépekre (kihasználva az informatikai biztonsági réseket), az audit során azonban csak azt vizsgálták, hogy a *social engineering* támadás elérte-e a célját, vagyis hogy elhitték-e a kollégák, hogy a támadó a bank központjában dolgozó informatikus. Külső térbeli határnak jelen esetben a regionális központ/igazgatóság irodáit, belsőnek pedig az egyes áldozatok mikrokörnyezetét, vagyis az íróasztaluk és a számítógépük környezetét értem. 3. A támadó beszédhelyzetei az egyes áldozatokkal. Ezt az elemzésem szempontjából nem tekintem jelentősnek, mivel a dialógusok néhány egyszerű mondatra korlátozódnak, s ezekről nem is készült külön felvétel.

Résztvevők

Az első esettel ellentétben a résztvevőket másfajta szempontok szerint osztályoztam ennél a leírásnál:

– Az a kolléga, aki felvette a telefont (első beszédhelyzet). Az ő feladata az volt a támadásban, hogy még a támadó megérkezése előtt megerősítse a helyi kollégákat abban, hogy a pesti informatikus kolléga mindjárt itt lesz. Ezzel akaratán kívül eloszlatott minden esetlegesen meglévő fenntartást az idegen, soha nem látott támadó kapcsán.
– Helyi kollégák: áldozatok, akik természetes módon engedték a számítógépükhöz a támadót.
– Támadó. A támadónak az első két esethez képest nem csak humán alapú *social engineering* ismeretei vannak. Az archetípusa rendszergazda/informatikus, aki szemüveges, farmernadrágban, kissé gyűrött ingben, a nyakában a vállalat hamisított (színesben kinyomtatott) belépőkártyájával jelent meg. Előzetesen felkészült a vállalatból a vállalatról szóló nyilvánosan elérhető információk alapján (OSINT).

Megjegyzem, hogy a támadás sikeressége nagymértékben azon múlt, hogy a támadás napján a vidéki központ valamennyi informatikai munkatársa a budapesti központban egy konferencián vett részt. Mivel a bank támogatta ezt a konferenciát, így tudni lehetett, hogy a kollégák részt is vesznek rajta. A támadó felhívta előzetesen a szervezőket, akik elkotyogták, hogy a vidéki igazgatóság teljes létszámmal képviselteti magát.

Lezárások

A három beszédhelyzet célja rendre a következő: 1. telefonon bizalmat ébreszteni a kollégákban, hogy jön egy informatikus a központból, aki megszereli a gépeket; 2. megerősíteni a vidéki kollégákat abban, hogy a budapesti informatikus kolléga néhány beállítást hajt végre a gépeken, aminek következtében a gépek gyorsabbak lesznek; 3. az áldozatok számítógépéről és annak környezetéből megszerezni a szükséges belépési neveket/jelszavakat, illetve hozzáférni a banki adatbázisokhoz.

Cselekménysorozat

1. telefonos beszélgetés a vidéki igazgatóság egyik munkatársával. a) A támadó ebédidőben felhívja a bank vidéki igazgatóságának egyik osztályát, hogy rövidesen érkezik, de eltévedt. Mivel a nyilvános forrásokból megismerhető vállalati kultúra része, hogy a kollégák egymást tegezik, ezért a támadó is tegezi a kollégát. b) Elmondja, hogy a budapesti központból jön, mert a szá-

mítógépeken el kell végeznie néhány nagyon fontos beállítást, mindjárt odaér, s megkéri a kollégát, hogy mivel nem ismeri a helyszínt, várja a bejáratnál. 2. c) a támadó megérkezéséig a kolléga elmondja az osztály többi dolgozójának, hogy mindjárt megérkezik a budapesti informatikus kolléga (gyakorlatilag megismétli azt, amit a támadó neki mondott); d) a telefonos áldozat várja a bejáratnál; e) a recepciós kolléga a hamis belépő alapján feljegyzi a támadó adatait, s beengedi őt; f) a telefonos áldozat bemutatja a támadót az osztály többi munkatársának; g) a támadó még egyszer elismétli a látogatása célját (egy fontos beállítást kell elvégeznie az osztály valamenynyi számítógépén az új biztonsági protokollok életbelépése miatt). 3. h) a támadó leül az áldozatok számítógépéhez; i) megkéri őket, hogy lépjenek be az általuk használt adatbázisokba, illetve ellenőrizzék, hogy a támadónál lévő név/jelszó páros egyezik-e (természetesen nem egyezik, merthogy a támadó „véletlenül” egy másik listát hozott magával); j) mivel nem egyezik, ezért új nyilvántartó lapot készítenek, ahol megadják a szükséges adatokat; k) a támadó kihasználva a rendszer biztonsági réseit, az adatbázisok számára releváns tartalmát egy másik tárhelyre másolja.

Kulcs

A támadás során az alapvető kulcs a támadó rendszergazda/informatikus szerepének az eljátszása. A korábban leírt formai jegyek mellett fontos, hogy a támadónak legyen valódi informatikai tudása, illetve legalább alapszinten ismerje a bank működését és szervezeti kultúráját/stílusát. A támadó stílusa precíz és szakmaiságot tükröző („végre egy rendes rendszergazda”), aki készségesen válaszol a feltett kérdésekre (a kérdések kivétel nélkül a szövegszerkesztő és táblázatkezelő szoftverekkel, a levelezőrendszerrel, illetve a nyomtatással voltak kapcsolatosak. Ezek a kérdések szinte valamennyi cégnél előfordulhatnak, tehát nem tekinthetők iparág-, illetve ágazatspecifikusnak).

Eszközök

A kommunikációs csatorna a személyközi és a csoportkommunikáció során verbális és nonverbális. A támadás csatornái között megjelenik a telefonos is.

Normák

A támadó elsősorban a normakövetésre épít, kihangsúlyozva, hogy a beállítások utáni nap – amikor az új rendszer elindul – a gépek sokkal gyorsabbak lesznek, így a munka is hatékonyabbá és kényelmesebbé válik.

Műfaj

A támadás során több műfajjal lehet találkozni: telefonon általános információ adása, szakmai beszélgetés, segítségnyújtás.

Dohányzásra kijelölt hely

Beszédhelyzet

A dohányzásra kijelölt hely – a helyi adottságok figyelembevételével – olyan, rendszerint a szabadban található hely lehet, amit mindenféle engedély nélkül meg lehet közelíteni, illetve ott lehet tartózkodni. A bank székhelye ilyen volt. Az időbeli keretnél a támadás két részre bontható (az elemzésben részletesen csak az első rész szerepel): a dohányzás közbeni rész és a nyilvánosságtól elzárt részekbe (folyosó, irodák) történő bejutás jelenti a keret első, míg a bejutás után a kémkedés a második részt. Az időbeli külső határ tizenkét perc volt, mialatt részint a cigarettázás, részint az elzárt részekbe történő bejutás megtörtént. A külső térbeli határ a dohányzásra kijelölt helyet, a recepciós pultot, valamint a csak belépőkártyával megközelíthető területeket jelenti. A belső térbeli határnál a dohányzás helyszínén a „megszokott” körbeállás, a recepciós pult környékén a csoportos vonulás, az elzárt részekbe történt bejutás után pedig a szétválás, illetve közös liftezés volt a jellemző. Az eset tehát két beszédhelyzetet azonosít: 1. dohányzás közbeni eszmecserére; 2. proxemika segítségével történő bejutás.

Résztvevők

A támadásban a következő résztvevők/szerepek azonosíthatók:

– Aktív áldozatok, akik a dohányzásra kijelölt helyen cigarettáznak, s érdeklődve hallgatják a támadó rövid beszámolóját arról, hogy milyen új törvényi változások várhatók a bankszabályozás területén.

– Recepciós (passzív áldozat), aki nem figyel arra, hogy a banki belépőkártyával bíró kollégák közé keveredett a támadó, akit így tudtán kívül átenged a lezárt részekbe.
– Biztonsági őrök (passzív áldozat), akik nem figyeltek arra, hogy a csoporthoz egy idegen is csatlakozott.
– Támadó, aki a pénzügyi szervezetek felügyeletéért felelős hatóság munkatársának adta ki magát. Megjelenése: határozottságot és magabiztosságot, egyszersmind egyfajta barátságot is sugall. A dohányzásra kijelölt helyen lévő áldozatokkal (közel) azonos konzervatív, sötét színű öltönyt, fehér inget, nyakkendőt, bőrcipőt visel, kezében kisebb, bőr aktatáska. Nyakában a hatóság hamisított belépőkártyája, illetve van hamis névjegykártyája arra az esetre, ha az áldozatok közül valaki kérne tőle. Életkorát tekintve a harmincas évei elején jár.

Lezárások

A támadás célja a cigarettázás befejezése után a dohányosokhoz csapódva bejutni a csak a bank érvényes belépőkártyájának felmutatása után megközelíthető elzárt irodarészekbe.

Cselekménysorozat

A támadást megelőzően a támadó elkészíti a szükséges hamisított belépő-, illetve névjegykártyát. Előzetes megbeszélés szerint a támadó mindvégig tegezi az aktív áldozatokat. A cselekménysorozat fontosabb elemei a következők: 1. támadó megkérdezi, hogy a csoport ismeri-e azt a vezetőt, akinek a hivataltól egy nagyon fontos borítékot hozott (ehhez előzetesen olyan személyt választ ki, akit arcról felismer, s nem dohányzik legalább a támadás idején); 2. tüzet kér a dohányzásra kijelölt helyen cigarettázó banki alkalmazottaktól; 3. a támadó belefolyik a csoportos beszélgetésbe; és 4. felméri, hogy az aktuális csoportban ki a hangadó, illetve azt is, hogy miként tudja néhány perc alatt felhívni magára a figyelmet. Esetünkben ez az új banki szabályozásról szóló bizalmas információk megosztása volt, ami valóban felkeltette a csoporttagok érdeklődését. A dohányzás befejezése után 5. a beszélgetést folytatták; miközben 6. beértek a bank székhelyének az előcsarnokába. Az előcsarnokban a biztonsági őrök egymással beszélgettek, így 7. nem vették észre, hogy a csoporthoz egy idegen is csatlakozott. A recepciós nő – mert így szokás – 8. a pultból vezérelte azt a kaput, amelynél a kollégák ellenőrzés

nélkül át tudtak menni csoportosan. A támadó 9. bejutott a védett részekbe. Az audit során csak eddig vizsgáltuk a támadást, ha azonban éles támadás lett volna, akkor a támadó a bejutás után olyan irodákba megy be, ahonnan értékes/titkos információkat, vagy „csak” céges mobiltelefonokat lop el.

Kulcs

Ennél a támadásnál az adott szerep eljátszása mellett fontos tényező a proxemika. A csoporttal történő rövid (kb. tízperces) interakció során, a magasabb, így a támadót bejutáskor takaró áldozat, illetve a csoporton belüli tagok és a támadó közötti távolság helyes megválasztása révén valósítható meg a sikeres *social engineering* akció.

Eszközök

A kommunikációs csatorna a személyközi és a csoportkommunikáció során verbális és nonverbális.

Normák

A támadás alapvetően a normakövetésre épít. A banki alkalmazottak örömmel hallgatják a munkájukat segítő bizalmas információkat.

Műfaj

A támadás során több műfaj is megjelenik: az elején segítségkérés, majd felvilágosítás, illetve tanácsadás.

Összegzés

Az esettanulmányok feldolgozása után a következő konzekvenciák fogalmazhatók meg (második hipotézis). Az esettanulmányok rámutattak azokra a pszichológiai és kommunikációs csapdákra, amelyekbe mindannyian beleeshetünk. Ezek a csapdák nemcsak a vizsgált üzleti, hanem a magánéletben is megtalálhatók. Vannak olyan emberek, akik különösebb előképzettség nélkül is eredményesen képesek manipulálni a környezetükben élőket. A *social engineerek* erre a „szakmára” rendszerint tudatosan készülnek, s ha birtoká-

ban vannak is egy bizonyos manipulatív eszközkészletnek, szakmai ismereteiket folyamatosan fejlesztik. Jelen korunk programozói és hálózati ismeretekkel felvértezett hackereihez hasonlóan a humán alapú támadásokkal (vagy azzal is) foglalkozó *social engineerek* is egyre ritkábban dolgoznak szórakozásból, a háttérben szervezeti és kormányzati megrendelők állnak. A szervezetek informatikai sebezhetősége egyre nehezebb feladatot ad valamennyi szervezet számára. Ennek része, hogy a *social engineer* tudással felvértezett ellenőrök/auditorok a szervezetnél ad hoc jelleggel különböző teszttámadásokat hajtanak végre, és a tapasztalatok alapján a biztonsági előírásokra, képzésre, a tudatosság fejlesztésére vonatkozó ajánlásokat fogalmaznak meg, illetve programokat indítanak el. Meggyőződésem, hogy ebben a folyamatban Hymes SPEAKING modelljének használata többletinformációval gazdagítja az információbiztonsági eseteket/incidenseket elemző szakembereket. A tanulmányomban bemutatott, illetve további esettanulmányok elemzése után az első hipotézist, miszerint Hymes SPEAKING modellje alkalmas a humán típusú *social engineering* támadások elemzésére, szintén elfogadottnak tekintem.

IRODALOM

Aronson, Elliot: The Social Animal. Freeman, San Francisco, 1972

Atkinson, Rita L. – Atkinson, Richard C. – Smith, Edward E. – Bem, Daryl J.: Pszichológia. Osiris Kiadó, Budapest, 1997

Balázs István (szerk.): Pszichológiai lexikon. Magyar Könyvklub, Budapest, 2002

Dooley, Larry M.: Case Study Research and Theory Building. *Advances in Developing Human Resources,* iss. 4, 2002

Dreyfus, Suelette – Assange, Julian: Underground. Red Book, Sydney, 1997

Griffin, Em: Bevezetés a kommunikációelméletbe. Harmat Kiadó, Budapest, 2001

Haig Zsolt – Várhegyi István: Hadviselés az információs hadszíntéren. Zrínyi Kiadó, Budapest, 2005

Hewstone, Miles – Stroebe, Wolfgang – Codol, Jean-Paul – Stephenson, Geoffrey M. (szerk.): Szociálpszichológia európai szemszögből. KJK, Budapest, 1999

Horányi Özséb (szerk.): Kommunikáció I–II. General Press, Budapest, 2003

Horváth Dóra – Mitev Ariel: Alternatív kvalitatív kutatási kézikönyv. Alinea Kiadó, Budapest, 2015

Hymes, Dell: Models of the Interaction of Language and Social Life. In: **Gumperz, John – Hymes, Dell (eds.):** Directions in Sociolinguistics: The Ethnography of Communication. Holts Rinehart & Winston, New York, 1972, pp. 35–71.

Hymes, Dell: Foundations in Sociolinguistics: An Ethnographic Approach. University of Pennsylvania Press, Philadelphia, 1974

Izsa Jenő: Nemzetbiztonsági alapismeretek. Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2009

Klenke, Karin: Qualitative Research in the Study of Leadership. Emerald Group, Bingley, 2008

Kollár Csaba: Social engieering a gyakorlatban. Manipulációk értelmezése a SPEAKING modellben. *JEL-KÉP,* 2017/3.

Lévay Gábor: OSINT (Open Source Intelligence). Nyílt információs hírszerzés. Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2006

Levy, Steven: Hackers: Heroes of the Computer Revolution. O'Reilly, New York, 2010

Matel, Maldona: "The Ethnography of communication". *Bulletin of the Transilvania University of Brasov,* vol. 2, no. 51, 2009

Mitnick, Kevin D. – Simon, William L.: A legendás hacker. A behatolás művészete. Perfact Kiadó, Budapest, 2006

Mitnick, Kevin D. – Simon, William L.: A legendás hacker. A megtévesztés művészete. Perfact Kiadó, Budapest, 2003

Oroszi Eszter Diána: Social Engineering: Az emberi erőforrás, mint az információbiztonság kritikus tényezője. Budapesti Corvinus Egyetem, Budapest, 2008. http://krasznay.hu/presentation/diploma_oroszi.pdf

Philipsen, Gerry: A beszédkódok elmélete. A kommunikáció etnográfiája. In: **Em Griffin:** Bevezetés a kommunikációelméletbe. Harmat Kiadó, Budapest, 2001, 428–439. o.

Poulsen, Kevin: Kingpin: How One Hacker Took Over the Billion-Dollar Cybercrime Underground. Broadway Paperbacks, New York, 2011

Ray, Manas – Biswas, Chinmay: A study on Ethnography of communication: A discourse analysis with Hymes 'speaking model'. *Journal of Education and Practice,* vol. 2, no. 6, 2011

Russell, Ryan: A Háló kalózai. Hogyan lopjunk kontinenst. Kiskapu Kiadó, Budapest, 2005

Shannon, Claude E.: The mathematical theory of communication. In: **Shannon, Claude E. – Weaver, Warren:** The Mathematical Theory of Communication. The University of Illinois Press, Urbana, 1964

Smith, Eliot R. – Mackie, Diane M.: Szociálpszichológia. Osiris Kiadó, Budapest, 2001

Sterling, Bruce: The Hacker Crackdown: Law And Disorder On The Electronic Frontier Mass Market. Bantam, New York, 1993

Zand-Vakili, Elham – Kashani, Alireza Fard – Tabandeh, Farhad: The Analysis of Speech Events and Hymes' SPEAKING. Factors in the Comedy Television Series: "FRIENDS". New Media and Mass Communication, no. 2, 2012

DOI: 10.38146/BSZ.2018.2.3

ZALAI-GÖBÖLÖS NOÉMI

A Z és az alfa generációk jövője a nemzetbiztonsági szolgálatoknál

Korábban egy cikkben már foglalkoztam a nemzetbiztonsági szolgálatokat érintő generációváltás általános kérdéseivel és kihívásaival[1], mivel azonban a következő években ezek egyre erőteljesebben jelentkeznek majd, ezért szükségszerű a változásokra történő megfelelő felkészülés. A nemzetbiztonsági szolgálatok hagyományosan konzervatív szemléletű szervezetek, évtizedek óta kialakult és alkalmazott standardokkal, miközben a globálisan változó biztonságpolitikai környezet és a robbanásszerűen fejlődő technológiák arra kényszerítik őket, hogy folyamatosan fejlesszék képességeiket. A fejlődés azonban nem korlátozódhat csupán az eszközök és módszerek felülvizsgálatára, hiszen végső soron a feladatok végrehajtásának sikeressége nem pusztán a technikai fejlettségen és a korszerű módszereken, hanem az azokat működtető és a speciális feladatokat végrehajtó személyzeten múlnak. Jelen tanulmányban elsősorban a Z és az alfa generáció sajátosságaira helyezem a hangsúlyt, mert ők lesznek a jövő alkalmazottai, és a nemzetbiztonsági szolgálatoknak az ő sajátosságaikat figyelembe véve kell majd megújulniuk, ha fenn kívánják tartani a hatékony és sikeres feladat-végrehajtás eddigi gyakorlatát.

A Z generáció (1995–2009) sajátosságai és elvárásai[2]

A digitális bennszülöttek generációja, képviselői belenőttek a virtuális világ adta lehetőségekbe, és szinte minden fontos kérdésre elsősorban a világhálón keresik a válaszokat. Újfajta kommunikációs felületeken élik a szociális életük nagy részét, és hozzászoktak ahhoz, hogy az információk mindig és min-

1 Zalai Noémi: Új típusú kihívások: generációváltás a nemzetbiztonsági szolgálatoknál. Nemzetbiztonsági Szemle, 2016/1., 34–44. o.

2 Kissné András Klára: Generációk, munkaerőpiac és a motiváció kérdései a 21. században. http://www.ohe.hu/hrmagazin/cikkek/generaciok-munkaeropiac-es-a-motivacio-kerdesei-a-21-szazadban;
Pais Ella Regina: Y és Z generáció mint a jövő munkavállalói. http://www.kormanyhivatal.hu/download/2/18/60000/Y%20%C3%A9s%20Z%20gener%C3%A1ci%C3%B3%20mint%20a%20j%C3%B6v%C5%91%20munkav%C3%A1llal%C3%B3i.pdf

denkor, szinte azonnal rendelkezésre állnak. Éppen ezért mind az oktatás, mind a tanulás terén más metodikát részesítenek előnyben, nehezen fókuszálnak kizárólag egy feladatra, legfőbb sajátosságuk az úgynevezett *multi-tasking,* vagyis több feladat egyidejű végrehajtásának igénye és képessége.

Arról, hogy miként alkalmazkodnak egy munkahelyi környezethez, még korlátozott információk állnak rendelkezésre, hiszen nagy részük csak most lép be a munkaerőpiacra. Ettől függetlenül a generációs sajátosságaik alapján bizonyos munkavállalói viselkedésjegyeik és elvárásaik megjósolhatók. Gyorsabban képesek alkalmazkodni a változásokhoz, nem ijednek meg az új technológiáktól, kifejezetten érdeklődők és kíváncsiak, azonban a figyelmüket jóval nehezebb hosszú távon lekötni. Egyes kutatások szerint egy dologra legfeljebb nyolc–húsz másodpercre koncentrálnak, utána átváltanak egy másikra. Hozzászoktak a folyamatos és állandó kapcsolattartáshoz, amely nagy részben a virtuális térhez kapcsolódik, általánosságban a szocializálódásuk is ebben a közegben történik. Ugyanakkor a magabiztosságuk is elsősorban ebben a környezetben érvényesül a legjobban, hiszen többet kommunikálnak ebben a formában, mint ténylegesen. Ez nem jelenti azt, hogy teljes mértékben elszigetelődnek a hagyományos emberi kapcsolatoktól, de adott esetben nehezebben mehet a szemtől szembe kommunikáció, mint a chatelés. Ennek ellenére a Z generáció tagjai a kutatások szerint igénylik a munkahelyi szociális környezet meglétét, a közvetlen kommunikáció lehetőségét, de ezt elsősorban kis csoportban és rövidebb ideig érzik komfortosnak. A generáció tagjai egyre kevesebb időt töltenek olvasással, viszont egyre többet játszanak például számítógépes vagy logikai játékokkal.

A kommunikációs eszközök fejlődésével egyre több információhoz jutnak, amelyeket azonban máshogy dolgoznak fel, és részben emiatt másképp is gondolkodnak. Nehezen viselik, ha kizárólag egy dologra kell figyelniük, és azt is, ha megfosztják őket a lételemüknek számító kommunikációs eszközeiktől, lehetőségeiktől. Egy olyan munkahely, amely nem támogatja az okostelefonok, iPadek és egyéb eszközök napi és rendszeres használatát, hosszú távon valószínűleg nem számíthat a Z generáció elkötelezettségére.

Az alfa generáció (2010–) karakterisztikája

Az alfa generációról még viszonylag kevés információnk van, hiszen a legidősebb tagjai is csak kisiskolások, de a jövőkutatók már aktívan foglalkoz-

nak a jellemzőikkel, hiszen tizenegy-tizenöt éven belül ők is belépnek a munka világába.

Ez a generáció már egyáltalán nem ismeri azt a világot, amikor még nem volt internet. A leginkább virtuálisan függők, és ezért talán az eddigi legmagányosabb generáció lesznek. Olyan nehézségekkel kell szembenézniük, mint például a globális éghajlatváltozás és ennek következményei, vagy a társadalmi elöregedés, amelynek megoldásait tőlük várják majd.

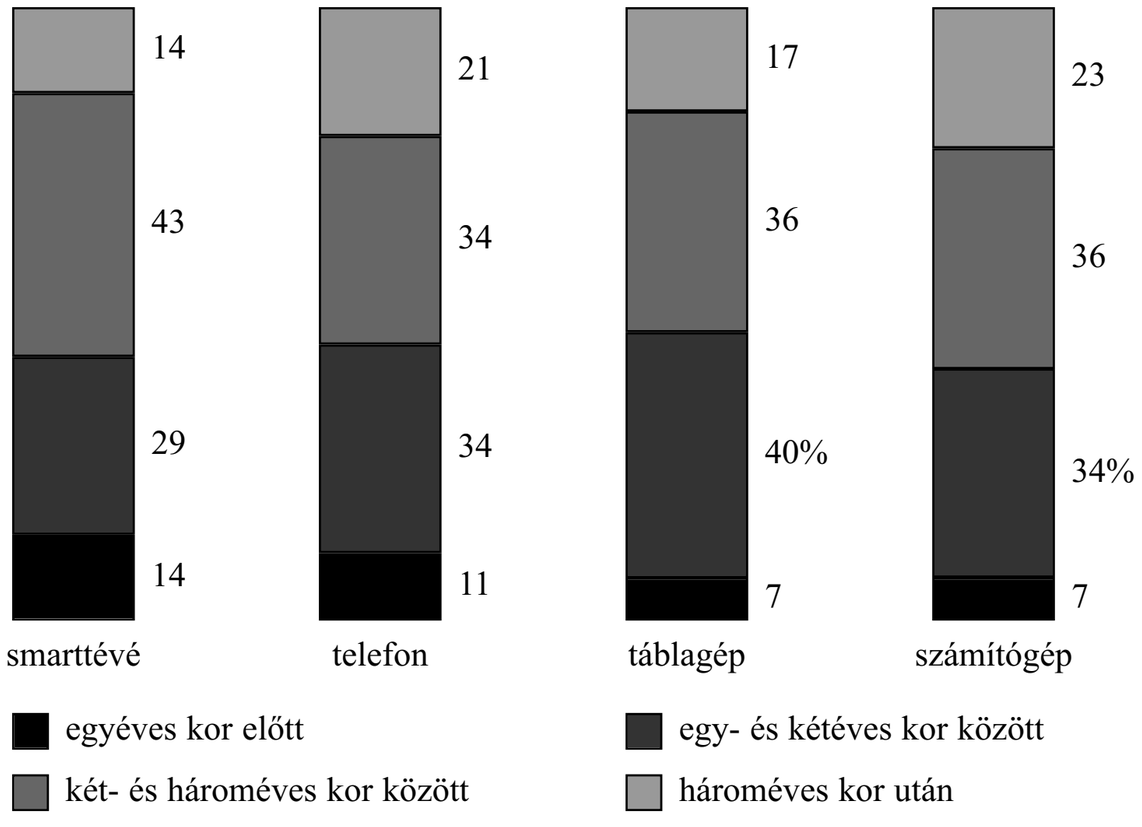
Az állandó virtuális jelenlét miatt tanulási és információfeldolgozási szokásaik az előző generációkhoz képest is jelentősen megváltoznak éppúgy, ahogy a fogyasztási és munkavállalói preferenciáik is.

Jól példázza a generáció sajátosságait annak a kérdőíves kutatásnak az eredményeit bemutató ábra, amely az alfa generációval kapcsolatos tapasztalatokat mérte fel, és amelyet 2015 őszén önként töltött ki 95 óvodáskorú gyermek valamelyik felnőtt hozzátartozója.

Azt, hogy pontosan milyen lesz az alfa generáció, még korai lenne meghatározni, de a következő szempontok hasznos támpontot adhatnak a jövőbeni kutatásokhoz:

– Az alfa generáció fejlett és dinamikusan fejlődő technológiai környezetben nő fel, elsődleges kommunikációs forrásként pedig a mobiltelefonokat, és

Eszközhasználat kezdete (%)[3]



3 Forrás: Pintér Marianna: Milyen tapasztalatokkal kerül az alfa-generáció az iskolába? http://folyoiratok.ofi.hu/uj-kozneveles/milyen-tapasztalatokkal-kerul-az-alfa-generacio-az-iskolaba

az ahhoz fejlesztett applikációkat fogják használni, háttérbe szorítva a laptopokat és egyéb technológiai eszközöket. Ha fel akarjuk kelteni majd ennek a generációnak a figyelmét, akkor azt könnyen használható, vizuálisan megnyerő, és az igényeikhez igazított applikációkon keresztül tehetjük meg.

– Sokkal jobban képzettek és hatékonyabbak lesznek az előző generációkhoz képest. Mivel várhatóan a változó globális környezet meghatározó lesz az életükre, és a rájuk vonatkozó követelmények is sokkal magasabbak lesznek, ezért ehhez úgy fognak alkalmazkodni, hogy a kezükbe veszik a saját életük, képzésük, felkészülésük irányítását. Vélhetően előnyben fogják részesíteni az online képzési formákat a hagyományos és költséges oktatási rendszerekkel szemben, és jóval hamarabb megkezdődik a tanulási ciklusuk, amely ténylegesen élethosszig tart majd.
– Az életük nagy részét az interneten keresztül menedzselik majd, a vásárlástól a hivatalos ügyintézésig, ezért paradox módon sokkal elszigeteltebbek lesznek, annak ellenére, hogy online mindent és mindenkit elérnek.
– Vállalkozóbbak és bátrabbak lesznek, mint elődeik, sokuk már egész kiskorában ismertségre tehet szert, hála az internet adta lehetőségeknek. Hamarabb megismerkednek a „self-made man” filozófiával, és mivel előbb tesznek szert tapasztalatokra, ezért gyorsabban is fejlődnek majd, különösen a munka világában.

Az, hogy mennyire igazolódnak be ezek a feltételezések, még a jövő kérdése, de az biztos, hogy mindenképpen nagy próbatételt fognak jelenteni a munkáltatók szempontjából, és alapjaiban változtathatják meg a munkaerőpiaci tendenciákat.

A hazai nemzetbiztonsági szolgálatok jellemzői és elvárásai

A nemzetbiztonsági szolgálatok feladatköre, végrehajtásuk és alkalmazásaik lehetősége törvényben szabályozott, különböző szintű engedélyekhez kötött, és szigorú ellenőrzési mechanizmusok garantálják a törvényi feltételek teljesülését. Mindez a speciális működési sajátosságokból adódik, és mindenképpen szükségszerű. Ennek meglétén nem lehet és nem is szabad változtatni, hiszen a nemzetbiztonsági tevékenység során alkalmazott titkos információgyűjtő eszközök és módszerek csak megfelelő jogi szabályozottság mellett tölthetik be alapvető rendeltetésüket. Ugyanakkor a szabályozottság nemcsak

a feladatok végrehajtásának körülményeire, hanem a szolgálatok állományában lévő személyekre is vonatkozik. Ennek elsődleges oka az alkalmazott módszerek, és egyben a végrehajtó állomány védelme, valamint a titkosság alapelvének, mint meghatározó működési sajátosságnak a fenntartása. Ez szintén elengedhetetlen és szükségszerű, amikor a konkrét feladat-végrehajtásról beszélünk. A szabályozottság, a fegyelem, az erősen hierarchikus szervezeti felépítés, és a konzervatív szemlélet alapvetően évtizedek óta előkelő helyen szerepel a nemzetbiztonsági szolgálatok jellemzői között, és ennek megfelelően az állománnyal szemben támasztott elvárások nagy része is ezekre épül. A terhelhetőség, a stressztűrés, a szabálykövetés, a felelősségtudat, az elhivatottság, a lojalitás, az együttműködési készség, a stabil értékrend, az erkölcsi szilárdság, a megbízhatóság, a koncentrációkészség, a pontos, precíz munkavégzés, mind-mind olyan elvárások, amelyek a mai napig megtalálhatók a nemzetbiztonsági szolgálatok általános követelményei között. Természetesen ezen felül az egyes munkakörök betöltőinek számos egyéb kompetenciára van szükségük, de az alapvetően elvárt értékek központi elemét az előbbi jellemzők adják.

Új generációs paradoxonok

A szigorú szabályozottság szükségszerűsége mellett a nemzetbiztonsági szolgálatoknak, mint szervezetnek, és mint munkáltatónak elengedhetetlenül változtatniuk kell, ha a jövőben is garantálni szeretnék a kiemelkedő színvonalú munkavégzést. Ha a szervezeti értékek és a munkahelyi szemlélet nem képes alkalmazkodni a munkaerőpiaci tendenciák változásaihoz, akkor törvényszerű lesz a munkáltatói és munkavállalói követelmények közti különbség exponenciális növekedése. Természetesen sokszor találkozni azzal a véleménnyel, hogy a nemzetbiztonsági szolgálatok nem piaci szereplők vagy multinacionális vállalatok, és egészen más szabályok, illetve munkaerőpiaci sajátosságok szerint működnek. Ezzel részben egyet is értek, azonban ez nem jelenti azt, hogy a szervezeti kultúra és munkahelyi környezet terén ne lenne szükség, és legfőképpen lehetőség a fejlődésre és változásra. Ez a paradoxon már régóta jelen van szakmai körökben, de véleményem szerint a kettő korántsem zárja ki egymást, ahogy erre számtalan nemzetközi példát is láthatunk.[4]

4 Gondolok itt elsősorban a brit és amerikai szolgálatok gyakorlatára, amely a szervezeti kultúra és a társadalmi megjelenés tekintetében messzemenően haladó szemléletű.

Mindamellett azt is tudomásul kell venni, hogy csak egy munkaerőpiac létezik Magyarországon, és ugyanabból a bázisból meríthetnek a multinacionális vállalatok és az egyéb piaci szereplők, mint a nemzetbiztonsági szolgálatok. Az új generációk pedig hamarosan meghatározó szereplői lesznek ennek a piacnak, és azok a vállalatok, szervezetek lesznek eredményesek hosszú távon, amelyek képesek alkalmazkodni és megújulni, ezáltal a legjobb képességű munkavállalókat magukhoz vonzani.

Ha az elvárások oldaláról vizsgáljuk meg a kérdést, jól látható, hogy mely területeken mutatkozhat majd jelentősebb eltérés munkavállalói és munkáltatói szempontból. Az utóbbi években a munkáltatókat, a humánerőforrás-gazdálkodással foglalkozó szakembereket és a szociálpszichológusokat egyre inkább foglalkoztatja az a kérdés, hogy milyen munkavállalók lesznek a következő generációk, ezért több ilyen jellegű felmérés születik a mostani tizen- és huszonéves fiatalok körében.

Magyarországon 2017 februárjában készítettek egy közös gyorsfelmérést a Monster.hu állásportál és a Future Work Festival munkatársai az 1996 után születettek körében. Ez azt hivatott vizsgálni, hogy mit várnak el ennek a generációnak a tagjai a jövőbeni munkahelyüktől, munkáltatóiktól.[5] A felmérésből egyebek között kiderül, hogy a Z generáció tagjai nagyra értékelik a visszajelzést, és többségük a leendő vezetőitől elsősorban a törődést, az odafigyelést, az emberséget, a segítőkészséget, és a munkatársakkal való megfelelő bánásmódot várja el. Alapvetően elutasítják a tekintélyelvű vezetést, sokkal többre értékelik, ha partnerként kezelik őket. A klasszikus vezetői kompetenciák, mint a határozottság, magabiztosság és szakmai hozzáértés csak ezek után szerepelnek az igények között. A szakemberek a válaszokból azt a következtetést is leszűrték, hogy a Z generáció tagjai elsősorban akkor tudnak kibontakozni egy munkahelyen, ha ott biztonságban érzik magukat, és bátorítást kapnak a kreativitásra, önmegvalósításra. Az általuk nyújtott kompetenciák között elsősorban a lendület, tanulékonyság, pontosság és fejlődés szerepel. A kommunikációs képességet kevésbé érzik fontosnak, ennél előrébb valónak tartják az egyéni képességet. Kiemelt szerepet kapott még a kreativitás, a pozitivitás és a vidámság, miközben az önállóság, a segítőkészség, a csapatmunka és a lojalitás csak a lista végén kapott helyet. Az ideális munkakörülményekre vonatkozó kívánalmak között a rugalmas munkaidő végzett az élen, de emellett fontosnak tartják a barátságos környezetet, a nyi-

5 Pálfi Károly: Emberséget vár főnökeitől a Z generáció. Origo.hu, 2017. február 23. http://www.origo.hu/gazdasag/20170223-baratkozos-fonokot-szeretnenek.html

tott gondolkodású, őszinte kollégákat, a világos, tiszta irodákat is. Az is kiderül a felmérésből, hogy ez a generáció szeret társaságban, csoportban, közösségi irodában dolgozni, és nem riad vissza a nem hagyományos munkarendtől, ha az nem feltétlenül helyhez kötött. A vizsgálat kitért a fiatalok kommunikációs szokásaira is, ebből egyértelmű, hogy az e-mail már jelentősen háttérbe szorult, elsődlegesen a Facebook, a Snapchat és az Instagram a kapcsolattartás alapvető fóruma. A felmérés kiemeli, hogy ez a generáció már szimbiózisban él a technikával, ezért a munkaadóknak a munkahelyi környezetben sem érdemes megfosztaniuk őket a közösségi média használatától.

Ha a munkáltatói oldalról vizsgáljuk a kérdést, elsősorban a nemzetbiztonsági szolgálatok oldaláról, akkor észlelhető, hogy vannak markánsan eltérő különbségek a követelmények tekintetében, miközben bizonyos szempontokból közelíthetnek egymáshoz a kritériumok. A tekintélyelvűség elutasítása és a lojalitás háttérbe szorítása nyilvánvalóan nem kedvez a szolgálatoknak, mint ahogy a közösségi média munkahelyen történő folyamatos használata sem. Mindazonáltal a kreativitás, lendület, tanulékonyság mind olyan készségek, amelyeket a szolgálatok is szívesen vesznek. A rugalmas munkaidő érdekes kérdés, hiszen bizonyos speciális munkakörök eleve nem működhetnek más formában, azonban a klasszikus rugalmasság terén még lehet, és kell is fejleszteni a jövőben. A munkahelyi közösségekre és a vezetői kvalitásokra vonatkozó elvárások támpontot adhatnak a szervezeti egységek kialakítása és a vezetők felkészítése terén. Természetesen nem az a cél és nem is megvalósítható, hogy a munkáltatók és a munkavállalók minden szempontból egységes elvárások alapján válasszanak vagy változzanak, ezek a vizsgálatok azonban mindenképpen hasznosak, ha teljesebb képet szeretnénk kapni a szükséges jövőbeni fejlesztési, fejlődési irányokról.

A szükségszerű változás területei

Az előbbiekből egyértelműen látszik, hogy a változtatás szükségszerűsége nagyon sok területet érinthet, beleértve a külső és belső tényezőket egyaránt. A következőkben azokra a szegmensekre, és az ezekhez kapcsolódó lehetőségekre szeretném felhívni a figyelmet, amely minden szolgálat számára saját hatáskörben elérhető, megvalósítható.

Branding és társadalmi kommunikáció

Az új generációk számára kiemelt fontosságú lesz, hogy a jövőbeni munkahelyük milyen szerepet tölt be a társadalmi hierarchiában és milyen küldetése van. Előbbi azért lényeges, mert a Z és az alfa generáció tagjainak meghatározó lesz a munkahely ismertsége és főleg elismertsége, utóbbi pedig azért, mert e generáció tagjainak jó néhány globális nehézséggel kell szembenéznie, amelyek megoldását tőlük várják majd, ezért nem mindegy, hogy milyen ügy mellé állnak.

A hazai nemzetbiztonsági szolgálatok a társadalmi kommunikáció terén meglehetősen visszafogottak, szervezetükről, feladatköreikről, sikereikről, eredményeikről vajmi keveset tudhat meg az átlagos érdeklődő. Ha egy reprezentatív felmérés készülne a magyar lakosság körében, ami arra irányul, hogy mennyire ismerik a nemzetbiztonsági szolgálatokat, feltehetően az átlag populáció legfeljebb a létezésük tényével lenne tisztában. Ez egyrészt kedvez a titkosságnak, mindamellett jól példázza az úgynevezett *branding,* vagyis a márkaépítés hiányát. Felvetődhet a kérdés, hogy egyáltalán miért van szüksége egy nemzetbiztonsági szolgálatnak arra, hogy brand legyen. Jelen esetben ez inkább meghatározó arculatot jelent, mintsem konkrét márkát, de a kialakításának folyamata nagyon is hasonló. Az arculatra azért van szükség, mert a munkaerőpiac jövőbeni szereplői számára fontos lesz, hogy büszkék lehessenek arra az intézményre, ahol dolgoznak, legyen az egy vállalat vagy egy kormányzati szerv. A társadalmi ismertség és az egyedi jellemzők együtt adják egy szervezet brandjét, amelynek – bármennyire elrugaszkodottnak tűnhet is egy nemzetbiztonsági szolgálat esetében – a jövőben az eddiginél is nagyobb jelentősége lesz. Gondoljunk csak arra, hogy mi jut eszünkbe, ha az Amerikai Egyesült Államok rendvédelmi szerveiről kérdeznek. Minden bizonnyal az FBI és a CIA, de ugyanez a helyzet Nagy-Britanniával is, ahol az MI5, az MI6 vagy a Scotland Yard azok a szervek, amelyekről a világon mindenki hallott. Ebben az esetben elmondhatjuk, hogy ezek a szervezetek önálló brandek, társadalmi ismertségük és elismertségük pedig egyértelmű. Emellett ugyanúgy végzik a feladataikat, anélkül hogy ez a fajta ismertség a munka hatékonyságának a rovására menne. Ha egy új generációs munkavállaló az adott országokban ilyen jellegű hivatást/munkát keres, pontosan tudni fogja, hol és hogyan jelentkezhet, és mit várhat az adott szervezettől. Ehhez képest a hazai nemzetbiztonsági szolgálatok esetében sokszor még az is gondot okozhat a potenciális érdeklődőnek, hogy egyáltalán tisztába kerüljön azzal, hogy melyik szervezetre kell rákeresnie az interneten. Mert abban szin-

te biztosak lehetünk, hogy a jövő generációinak ez lesz az elsődleges forrásuk, ahonnan tájékozódni fognak.

Egy kutatás eredményei szerint a Z generációt sikeresen célzó márkáknak a következő tulajdonságaik kell hogy legyenek[6]:

1. Digitalizált – a Z generáció tagjai iPodokon, sms-en, a Facebookon, okostelefonokon és a YouTube-on nőttek fel. Az internet az életük mindennapi része, ezért fontos, hogy az adott márka, szervezet is jelen legyen a digitális világban, különben elkerüli a fiatalok figyelmét.
2. Mobil – fontos, hogy a márka elérhető legyen az okostelefonjaikon is, bárhol vannak, hiszen e generáció tagjai előszeretettel használják telefonjukat is információkeresésre, időtöltésre.
3. Interaktív – a fiatalok számára fontos a szórakoztatás, ezért a marketingeseknek minél interaktívabb eszközöket kell beépíteniük a kampányaikba.
4. Azonnali – folyamatos és azonnali kommunikációra vágynak.
5. Közösségi – a Z generáció a közösségi oldalakon tartja a kapcsolatot barátaival, és naponta többször is fellép, hogy megnézze, van-e valami fontos esemény, új történés. Ennek megfelelően a márkák szempontjából is fontos, hogy elérhetők legyenek a különböző közösségi oldalakon.
6. Komplex – mivel a fiatalokat rendkívül sok információ éri, így nagyon sokat is tudnak. Persze kifejezetten csak az őket érdeklő területekről van mélyebb tudásuk, ennek ellenére komplex, jól megalapozott és hiteles kommunikációval lehet őket elérni.

Az előbbi kutatási eredmények elsősorban a fogyasztói szokások szempontjából vizsgálták ugyan a Z generáció tagjait, de a megállapítások összességében kiindulópontot adhatnak akár a jövőbeni munkáltatóknak is, hogy mivel és hogyan lehet felkelteni ennek a generációnak az érdeklődését.

Toborzás

Az iménti jellemzők alapján természetesen a toborzás folyamata és legfőképpen a felülete is változtatást igényel. A nemzetbiztonsági szolgálatok speciális szerepet töltenek be a munkaerőpiacon, tekintettel a sajátos feladat- és munkaköreikre. Az utóbbi években a szolgálatok sokkal nyitottabban jelen-

6 Pais Ella Regina: Alapvetések a Z generáció tudománykommunikációjához. Pécsi Tudományegyetem Pollack Mihály Műszaki Kar, Pécs, 2013. www.zgeneracio.hu/getDocument/1391

tek meg az olyan hagyományos rendezvényeken, mint a különböző állásbörzék és egyéb, erre a célra szervezett események. Mindamellett kevés előrelépés történt az interneten keresztül elérhető, jelentkezésre alkalmas felületek megújítása terén.

Ha megvizsgáljuk a hazai nemzetbiztonsági szolgálatok honlapjait, láthatjuk, hogy alapvetően a kötelező tájékoztatás és a kifejezetten konzervatív megjelenés dominál. Összességében minden szolgálat webes felületén megtalálhatók ugyan a jelentkezéshez szükséges tudnivalók, a felvételi követelmények, az önéletrajz beküldésére szolgáló elérhetőségek, ezek megjelenési formája azonban egyáltalán nem kelti fel a következő generációk figyelmét. Ezek a honlapok ugyanis legkevésbé sem tükrözik azt a modernitást, kreativitást és fejlettséget, amelyet a huszonegyedik században egy ilyen típusú szervezetnek tulajdonítanak a potenciális jelentkezők, és amely sok tekintetben a szolgálatokat feltehetően jellemzi is. Ezenfelül a már korábban említett branding szemlélettel is teljes mértékben ellentétesek, hiszen a száraz tények mellett nem szerepelnek olyan információk, amelyek a társadalmi ismertség és elismertség megszerzését céloznák. Korábban már említettem, hogy nemzetközi téren számtalan példát láthatunk ennek az ellenkezőjére, és ebből kettőt ki is emelnék.

Az angol Secret Intelligence Service (SIS), közismertebb nevén az MI6 honlapja[7] vagy a Security Service, más néven az MI5 honlapja[8] sok tekintetben jó kiindulási alap lehet egy jövőbeni korszerűsítéshez. Az általános és kötelező információk mellett számos olyan érdekes és figyelemfelkeltő elem található a felületeken, amely hosszabb időre lekötheti az érdeklődők figyelmét. Egyebek között részletes leírások szemléltetik az aktuális trendeket, feladatokat, próbatételeket, valamint bepillantást kapunk a különböző munkakörök sajátosságaiba, és az alkalmassági követelményekbe. Az MI5 honlapján érdekes, munkakör-specifikus feladatokat is találunk, amelyek elvégzése támpontot adhat a jelentkezőknek a saját képességeikről az adott munkakör követelményeivel kapcsolatban[9]. Természetesen ezek a játékos feladványok nem helyettesítik a valós felvételi feladatokat, de arra mindenképpen alkalmasak, hogy a potenciális jelentkezők teljesebb képet kaphassanak a munkakör sajátosságairól és önmagukról. Az ilyen típusú feladatok megfelelő informatikai háttérrel megtámogatva akár egyfajta előszűrőként is szol-

7 https://www.sis.gov.uk/index.html
8 https://www.mi5.gov.uk/
9 https://www.mi5.gov.uk/careers/opportunities/intelligence-collection

gálhatnak az adott szervezet számára, amennyiben kitöltésüket például regisztrációhoz kötik.

A hazai nemzetbiztonsági szolgálatok felvételi rendszere összetett, többlépcsős és hosszadalmas folyamat, amelynek bármely pontján kieshet a jelentkező, ha nem felel meg a követelményeknek. Bizonyos munkakörök esetében az előszűrési folyamatot egyszerűsíteni és rövidíteni lehetne azáltal, ha a szolgálatok a saját igényeiknek megfelelő, munkakör-specifikus, mérhető és ellenőrizhető online feladatokat, kérdőíveket, teszteket stb. fejlesztenének és helyeznének el a honlapjukon.

Kiválasztás

A nemzetbiztonsági szolgálatok kiválasztási rendszere, ahogy azt már említettem, többlépcsős, összetett folyamat. A honlapokon szereplő felvételi követelmények alapján egyebek között vizsgálják a jelöltek pszichikai, fizikai alkalmasságát, a munkakörrel összefüggő kompetenciáikat, valamint meg kell felelniük a nemzetbiztonsági ellenőrzés kritériumainak is. Az utóbbi években a kiválasztással foglalkozó szakemberek minden bizonnyal tapasztalták, hogy a fiatalabb generációhoz tartozó jelentkezők sok tekintetben különböznek a korábbiaktól. Gondolok itt például arra, hogy az életkori és a generációs sajátosságokból adódóan akár eltérő fizikai vagy pszichés kondíciók mutatkozhatnak a kiválasztási folyamat során. Ezért a felvételi rendszert időről időre célszerű felülvizsgálni és szükség esetén módosítani. Ha egy adott vizsgálati kritérium esetében tendenciaként jelentkezik eltérés a korábban tapasztaltakhoz képest, például tízből nyolc jelentkezőnek rosszabb a látása, akkor érdemes megvizsgálni a változtatás lehetőségét, természetesen figyelembe véve azt is, hogy a munkaköri érdek ne sérüljön aránytalanul.

Felkészítés, továbbképzés

A nemzetbiztonsági szolgálatok az állományuk felkészítését alapvetően belső képzések, tanfolyamok keretében hajtják végre, tekintettel arra, hogy az egyes munkakörökhöz szükséges speciális ismeretek, kompetenciák megszerzésére más formában nincs lehetőség. Mindamellett nagyon fontos szempont lesz a későbbiekben a képzési rendszer reformja, hiszen a jövőbeni munkatársak, a Z és az alfa generáció tagjai már merőben más oktatási for-

mákra lesznek fogékonyak. A hagyományos iskolarendszerű felkészítés egyre kevésbé alkalmas e korosztályok képzésére, tekintettel a megváltozott információfeldolgozási sajátosságaikra és igényeikre.

Ahogy arra már korábban utaltam, az új generációk tagjai sokkal hatékonyabban teljesítenek a nem hagyományos képzési környezetben, hiszen az ő figyelmüket már nem lehet lekötni hosszabb, elméleti jellegű oktatással, és tradicionális képzési formákkal. Az előadások, a poroszos oktatási módszerek egyre kevésbé érik el a céljukat, ezért ezen a téren is a modernebb, gyakorlatiasabb és kompaktabb képzési fórumok lehetnek sikeresek a jövőben. Előtérbe kell helyezni az online kurzusokat, az önálló gondolkodásra, feladatmegoldásra lehetőséget adó feladványokat, a kiscsoportos, tréning jellegű oktatási formákat, és a különböző szituációs gyakorlatokat, játékokat. Ezek beiktatása rövidítheti, hatékonyabbá és munkakör-specifikusabbá teheti a felkészítést, amely végső soron mind a szolgálatoknak, mind az állománynak közös érdeke.

Munkahely és/vagy küldetés

A generációs sajátosságokból kiderül, hogy a munka világába hamarosan tömegesen belépő Z generáció már nem feltétlenül csak munkahelyet keres, hanem küldetést, célt, amelyben kiteljesedhet, és amelyben megvalósíthatja önmagát. Ennek megfelelően azok a munkáltatók élveznek majd előnyt, amelyeknek határozott víziójuk van, és azt a lehető legvonzóbb formában tudatják a világgal. Nem véletlen, hogy szinte valamennyi nagyobb vállalatnak, szervezetnek van egy olyan dokumentuma, amely tartalmazza a legfőbb célokat, és az azok eléréséhez szükséges eszközök és módszerek kínálatát. Az úgynevezett küldetés és jövőkép (Mission & Vision) dekrétum nem véletlenül szerepel kiemelt helyen e szervezetek honlapjain.

A hazai nemzetbiztonsági szolgálatoknak is van markánsan elkülöníthető és meghatározható küldetésük, feladatrendszerük, de nem tulajdonítanak olyan nagy jelentőséget ezek kinyilvánításának, mint például a nemzetközi partnerszolgálatok. A jövő generációi azonban igénylik és elvárják majd, hogy annak a szervezetnek, cégnek, amelynél dolgoznak, egyértelműen deklarált és társadalmilag elismert céljai legyenek.

A másik lényeges és az iméntinek ellentmondó szempont, hogy az új generációk egyre kevésbé kötelezik el magukat egy-egy szervezet iránt. Ahogy azt a korábban bemutatott egyik kutatás is megállapította, a lojalitás már ke-

vésbé preferált jellemző. Éppen ezért arra is fel kell készülniük a jövőbeni munkáltatóknak, hogy az új generációs munkavállalók jóval rövidebb időt töltenek majd el egy-egy munkahelyen, sokkal hamarabb váltanak, főként ha a személyes érvényesülésük a tét. Ez a nemzetbiztonsági szolgálatok esetében talán az egyik legnagyobb próbatételt jelentő szempont, hiszen a munka és a szervezet jellege – különös tekintettel a minősített információkra és a titkos információgyűjtő eszközökre és módszerekre – megkövetelné a hosszabb távú elköteleződést. Mindamellett e tendenciának nem lehet gátat szabni, legfeljebb azon lehet dolgozni, hogy az egy munkahelyen töltött idő minél hosszabbra nyúljon. Ez azonban csak akkor lehetséges, ha az új generációs munkavállalók elvárásainak részben vagy egészben meg tudnak felelni. Éppen ezért a humánerőforrás-menedzsmentnek az eddigieknél is nagyobb szerepe lesz az igények és követelmények mindkét fél számára megfelelő szempontú összehangolásában. Míg a küldetés és jövőkép a figyelemfelkeltéshez, a brandépítéshez és a minőségi munkaerő bevonzásához járul hozzá, addig a szervezetfejlesztés és a tudatos humánerőforrás-gazdálkodás az új munkaerő minél hosszabb távon történő megtartását segíti elő.

Összességében megállapítható, hogy nincsenek könnyű helyzetben a munkáltatók a jövő generációinak ismeretében, de számtalan lehetőség és mód adódik a fejlesztésre és fejlődésre. A jelenlegi globális biztonságpolitikai környezetben az eddiginél is nagyobb szerepük és jelentőségük van és lesz a rendvédelmi szerveknek és a nemzetbiztonsági szolgálatoknak, azonban a hatékony működésüket csak akkor tudják fenntartani, ha a jövőben is minőségi állományuk van. Ezért minél többet tudunk az előttünk álló tendenciákról, annál jobban és sikeresebben tudunk alkalmazkodni, felkészülni, és ez nemcsak a biztonságpolitikát veszélyeztető külső faktorokra, hanem a szervezeti fejlődést szolgáló belső tényezőkre is igaz.

IRODALOM

Kissné András Klára: Generációk, munkaerőpiac és a motiváció kérdései a 21. században. http://www.ohe.hu/hrmagazin/cikkek/generaciok-munkaeropiac-es-a-motivacio-kerdesei-a-21-szazadban

Pais Ella Regina: Alapvetések a Z generáció tudománykommunikációjához. Pécsi Tudományegyetem Pollack Mihály Műszaki Kar, Pécs, 2013. www.zgeneracio.hu/getDocument/1391

Pais Ella Regina: Y és Z generáció, mint a jövő munkavállalói. http://www.kormanyhivatal.hu/download/2/18/60000/Y%20%C3%A9s%20Z%20gener%C3%A1ci%C3%B3%20mint%20a%20j%C3%B6v%C5%91%20munkav%C3%A1llal%C3%B3i.pdf

Pálfi Károly: Emberséget vár főnökeitől a Z generáció. *Origo.hu,* 2017. február 23. http://www.origo.hu/gazdasag/20170223-baratkozos-fonokot-szeretnenek.html

Pintér Marianna: Milyen tapasztalatokkal kerül az alfa-generáció az iskolába? http://foly-oiratok.ofi.hu/uj-kozneveles/milyen-tapasztalatokkal-kerul-az-alfa-generacio-az-iskolaba

Tari Annamária: Z generáció. Tericum Kiadó, Budapest, 2011

Zalai Noémi: A humánerőforrás-gazdálkodás kérdéseinek vizsgálata a nemzetbiztonsági szolgálatoknál. Doktori (PhD-) értekezés. Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Hadtudományi Doktori Iskola, Budapest, 2012

Zalai Noémi: Új típusú kihívások: generációváltás a nemzetbiztonsági szolgálatoknál. Nemzetbiztonsági Szemle, 2016/1., 34–44. o.

DOI: 10.38146/BSZ.2018.2.4

DRUSZA TAMÁS

Stratégiai emberierőforrás-menedzsment nemzetbiztonsági területen

Magyarországon két dolog van, amihez mindenki ért: a foci és az emberierőforrás-menedzsment. Félretéve a viccet, biztosan mindenki ismeri azt a helyzetet, amikor egy szervezet humánpolitikai kérdéseit illetően minden munkatársnak határozott véleménye van. A humánpolitikai kérdések azonban gyakran leszűkülnek annak megítélésére, hogy egy személy adott pozícióra alkalmas-e, vagy sem. Utóbbi megítélésében azonban az emberek többsége hajlamos a szubjektív tényezőket az objektív tényezők elé helyezni. Ennek feltehetően az az oka, hogy a személyekhez kapcsolódó döntések könnyen váltanak ki belőlünk érzelmeket, pozitív és negatív töltetűeket egyaránt, ami viszont ritkán segíti elő a higgadt, megalapozott véleményalkotást.

Persze e jelenség önmagában nem probléma, véleménye mindenkinek lehet, ez az emberi természet része. Felelős döntéseket hozni azonban más tészta. Fontos, hogy akik a valódi döntéseket hozzák, e folyamat során képesek legyenek a tudatosság sokkal magasabb szintjét képviselni. *„Az emberek hatékony vezetésére vonatkozó tudás lefordítása vezetési elvekre és működési gyakorlatra”* – tartja az emberierőforrás-menedzsment egyik legáltalánosabb meghatározása[1]. E definícióból az is következik, hogy minél különlegesebb egy szervezet, minél egyedibb a működési gyakorlata, annál inkább érdemes „személyre szabott” figyelmet szentelni az emberierőforrásmenedzsment-rendszer kialakításának.

A nemzetbiztonsági terület esetében azonban e figyelmet nem csak a tevékenység különlegessége indokolja. Fontosabb, hogy a társadalmi változások olyan hulláma (Z generáció munkaerőpiacra lépése, ipari forradalom 4.0 stb.) előtt állunk, amelyek feladataik ellátása és humán erőforrásuk szempontjából is az eddigiekhez képest radikális mértékben újszerű helyzet elé fogják állítani és ezen keresztül növekvő nyomás alá fogják helyezni a szolgálatokat. A terület e próbatételeknek csak akkor fog tudni megfelelni, ha

1 Bokor Attila – Szőts-Kováts Klaudia – Csillag Sára – Bácsi Katalin – Szilas Roland: Emberi erőforrás menedzsment. Aula Kiadó, Budapest, 2009, 46. o.

emberierőforrásmenedzsment-rendszerét a modern elveknek megfelelően alakítja ki és működteti.

A nemzetbiztonsági szervezetek egyedi vizsgálata a terület érthető érzékenysége miatt nehézkes, azonban az ágazat együttes vizsgálatának nincs akadálya[2]. Meg tudjuk vizsgálni a társadalmi, jogszabályi, strukturális kérdéseket, a tevékenység sajátos jellemzőit. Mindezekből pedig következtetéseket tudunk levonni arra vonatkozóan, hogyan célszerű felépíteni és működtetni azt a rendszert, amely gondoskodik a nemzetbiztonsági ágazat megfelelő minőségű és mennyiségű emberi erőforrással történő ellátásáról.

Stratégiai emberierőforrás-menedzsment

A stratégiai emberierőforrás-menedzsment alapgondolata az, hogy az emberierőforrásmenedzsment-rendszerek működésének célja és mércéje a szervezeti eredményesség és hatékonyság, így az emberierőforrásmenedzsment-rendszernek és folyamatoknak a felső vezetői tevékenység integráns részévé kell válniuk, attól nem különülhetnek el.

A stratégiai emberierőforrás-menedzsment kialakulását olyan társadalmi változások indukálták, amelyek jelentősen megváltoztatták a szervezetek működési környezetét, a munkavállalók gondolkodását. Mint minden menedzsmentrendszer – azaz valamilyen tevékenységet vezető, tervező, szervező, irányító (ellenőrző)[3] –, ez is szerves fejlődés eredménye. Az emberi erőforrással kapcsolatos szervezőmunka fejlődésének következő lépcsőfokait lehet egymástól megkülönböztetni.[4]

1. *Személyügyi adminisztráció:* E korai – manapság munkaügynek nevezett – tevékenységi forma egyetlen feladata a munkaviszonyhoz kapcsolódó dokumentumok elkészítése, kezelése volt. E fejlődési szinten a humán terület általában valamely más szervezeti egység alárendeltségébe tartozott.
2. *Személyügyi menedzsment:* A fejlődésnek ezen a fokán már önálló szervezeti egységként működik a humán terület, belső tagozódásában korlátozott számban megjelennek az önálló szakértői ismereteket igénylő elkülönült funkciók, úgymint például oktatás-képzés, kiválasztás.

---

2 Természetesen az egyes szervezetek között lehet és van is különbség. Véleményem szerint azonban ez a különbség nem jelentős, illetve elsősorban nem tartalmi, hanem formai értelemben mutatkozik meg.

3 Fejes Miklós: Menedzsment alapok. Tansegédlet. Kézirat. Budapest, 2010, 4. o. http://www.ata-narur.hu/wp-content/uploads/2013/10/menedzsment-alapok.pdf

4 Bakacsi Gyula – Bokor Attila – Császár Csaba – Gelei András – Kováts Klaudia – Takács Sándor: Stratégiai emberi erőforrás menedzsment. Akadémiai Kiadó, Budapest, 2006, 44–46. o

3. *Emberierőforrás-menedzsment:* Ez a lépcsőfok az előzőkhöz képest egyrészt a funkciók bővülését jelentette, másrészt azonban új megközelítést és szemléletet is takar. Ezen a szinten az emberi erőforrás már nem pusztán számokkal leírható mennyiségeket jelent, hanem a szervezet fontos erőforrásainak egyikévé vált. Ez pedig abba az irányba hatott, hogy az emberierőforrás-menedzsmenttől már hatékony és érdemi hozzájárulást, hozzáadott értéket, a szervezeti folyamatokba történő közreműködést vártak a szervezet vezetői.
4. *Stratégiai emberierőforrás-menedzsment:* A stratégiai menedzsment elterjedésével, alakult ki a stratégiai emberierőforrás-menedzsment szemléletmód. A fő különbség a 3. pontban vázolt „sima" emberierőforrás-menedzsment szemlélethez képest a következőkben ragadható meg:
   – a humán funkció fontosból kritikussá válik a szervezet működése tekintetében, így a humán terület szervezeti fontossága is felértékelődik;
   – a felső vezetői nézőpont megjelenése, azaz a stratégiai vezetési szint aktív résztvevőjévé válik a humánmenedzsment-rendszer működésének;
   – az emberierőforrás-menedzsment funkció integráló szereppel bír a szervezet egészét érintően, azaz a szervezeti döntések jelentős részében megjelennek és koordináló szerepet töltenek be az emberierőforrás-menedzsment szempontjai, eszközei, módszerei.

Az előbbiekből látható, hogy a stratégiai emberierőforrás-menedzsment az embert helyezi a szervezeti működés középpontjába, első számú feladatának azt tekinti, hogy a szervezeti folyamatok összehangolása révén a szervezeti működés minden pontján kellő időben a lehető legjobb minőségben álljon rendelkezésre a szükséges humán kapacitás.

A nemzetbiztonsági terület sajátosságai

A nemzetbiztonsági terület az államigazgatás speciális területe. Fő feladata az ország nemzetbiztonsági érdekeinek védelme, fenntartása, az ezekhez szükséges információk megszerzése, illetve az ezeket fenyegető emberi tevékenységek – az úgynevezett nemzetbiztonsági kockázatok – felderítése és elhárítása. Másképp megfogalmazva: a nemzetbiztonsági terület az ország érdekeinek érvényesítéséért, biztonságáért felelős.[5]

5 Vida Csaba: A nemzetbiztonsági tevékenység szerepe a társadalomban. Hadtudomány (online) 2015/25., 224. o. http://real.mtak.hu/29936/1/19_VIDA_CSABA.pdf

A vonatkozó jogszabály a nemzetbiztonsági érdekek körébe Magyarország függetlenségét, alkotmányos rendjét, fontos politikai és gazdasági érdekeit sorolja.[6] Az ezeket fenyegető tényezők között az ellenérdekelt országok (titkosszolgálati) törekvéseit, a terrorizmust, szélsőséges és erőszakos eszmék követését, az ipari kémkedést, valamint a szervezett bűnözést szokták említeni. A felderítendő ismereteket védő rendszerek, illetve a nemzetbiztonsági kockázati tényezők az esetek többségében olyan különleges jellegzetességekkel bírnak, amelyek kezelése speciális feladat, mivel ezek[7]

– jól szervezettek;
– mélyen konspiráltak, jól leplezettek és védettek;
– sokszor teljesen kiszámíthatatlanok, újszerűek, egyediek;
– hétköznapi érdekviszonyok és tevékenységek mögé rejtettek;
– a társadalom minden szeletét érinthetik;
– legtöbbször nemzetközi vonatkozással bírnak;
– alapvető negatív társadalmi hatásuk lehet.

E tulajdonságokból fakadóan, a nemzetbiztonsági tevékenységhez kapcsolódó munkafeladatoknak is egyedi jellegzetességeik vannak:

– rendkívül komplexek;
– konspirációt igényelnek;
– speciális ismereteket, eszközöket és módszereket igényelnek;
– erős pszichés megterhelést jelentenek;
– költségesek;
– jövőorientáltak (előrejelző, megelőző jelleg);
– érzékenyek.

Általánosságban véve a nemzetbiztonsági tevékenység megfelel a speciális szakértelmiségi tevékenység kritériumainak.[8] Az iménti jellemzőkből olyan alapvetések származnak a nemzetbiztonsági szervezetek munkavégzési rendszerei tekintetében, amelyek determinálják az emberi erőforrás fontosságát a rendszer egészét illetően. A nemzetbiztonsági tevékenység ennek alapján:

1. *Humánerőforrás-intenzív:* Ez azt jelenti, hogy minden alapvető munkafolyamat igényli az ember érdemi közreműködését, szinte semmit nem lehet

6 A nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény.

7 Zalai Noémi: A humánerőforrás-gazdálkodás kérdéseinek vizsgálata a nemzetbiztonsági szolgálatoknál. PhD-értekezés. Budapest, 2012, 5–6. o.

8 Izsa Jenő: A titkosszolgálatok tevékenységének általános jellemzői, ellenőrzésük és irányításuk kérdései. Szakmai Szemle, 2009/2., 10. o.

teljesen automatizálni, hosszú távon sem. A hírszerzési ciklus alapján a nemzetbiztonsági tevékenység központi elemei: az információigény értelmezése, az adatszerzés, az adatfeldolgozás, az elemzés-értékelés és a tájékoztatás[9].

– A tevékenység kiindulópontja az információigények, illetve a feladatrendszer alapján a tevékenység megtervezése és megszervezése.[10] Ezek klasszikus vezetői feladatok, figyelembe véve, hogy az átlagnál nagyobb felelősséggel járnak.
– Az elektronikus hírszerzési módszerek (például Signals intelligence [SIGINT], Imagery intelligence [IMINT]) adatszerzés mellett az információszerző rendszer egyik fő eleme a human intelligence (HUMINT), azaz az emberi erőforrás közreműködésével gyűjtött információ. A források kialakítása és irányítása az egyik legösszetettebb és legnagyobb kihívást jelentő titkosszolgálati szakfeladat.
– Az adatfeldolgozás részben automatizálható tevékenység, a jövőben ezen a területen nagy fejlődés várható. Ugyanakkor a releváns feldolgozási szempontok összeállításában, meghatározásában az emberi tényező kiváltására teljes mértékben nincs lehetőség.
– Az elemzés-értékelés során a feldolgozott adatokból tudományos és szakmai ismereteken alapuló eljárások segítségével következtetéseket, értékeléseket és előrejelzéseket állítanak elő.[11] E következtetések színvonala jelentős részben a mögötte álló szakmai tudás, tapasztalat, illetve összetett elemzőkészségek és -képességek, azaz az emberi tényező kompetenciájának szintjétől függ.
– A tájékoztatás szintén alapvetően emberi közreműködést igénylő tevékenység, ugyanis a tájékoztató tartalmi összeállítása nem automatizálható. Ráadásul, mivel a nemzetbiztonsági szervezetek tájékoztatójában foglalt ismeretek kormányzati vagy egyéb intézkedések alapjául szolgálhatnak, ennek pontos és szakszerű összeállítása kiemelt fontosságú, egyben nagyon összetett feladat.

2. *Magas emberi hozzáadott értékű:* A nemzetbiztonsági tevékenység során a keletkező ismeretek számos folyamaton, többszintű értékelésen mennek keresztül. Ennek során a beszerzett, önmagukban keveset jelentő adatokból feldolgozott ismeretek keletkeznek. Mivel az adatok sosem állnak teljeskö-

9 Vida Csaba: Létezik-e még a hírszerzési ciklus. Felderítő Szemle, 2013/1., 43. o.
10 Uo.
11 Vida Csaba: A hírszerző elemző értékelő munka alapjai. Felderítő Szemle, 2014/3., 1. o. http://real.mtak.hu/14875/13/jav_real__2013-3.pdf

rűen rendelkezésre, a hiányosságokat a szaktudás és az elemző-értékelő módszerek használata révén létrehozott ismeretek pótolják. E gondolati tevékenység során a kezdeti egyedi adatok feldolgozottsági foka, összetettsége lényegesen megnő, azaz jelentős hozzáadott érték keletkezik.

3. *Speciális személyiséget és szaktudást igényel:* A nemzetbiztonsági tevékenység a speciális munkafolyamatok okán olyan személyiségjegyeket, készségek, képességek egyidejű kimagasló szintjét, valamint speciális szaktudás (gazdasági, informatikai stb.) meglétét feltételezi, amelyek így együttesen jellemzően a munkaerőpiacon megjelenők kis hányadát jellemzik. E személyek kiválasztása érdekében az ágazat szervezetei különböző szűrési eljárásokat rendszeresítettek, mindazonáltal éppen az értékük miatt a munkaerőpiacon más szervezetekkel kell versenyezni értük[12].
4. *Hosszú és költséges felkészülési időt igényel:* A munkatevékenység speciális jellegét, egyedi munkafolyamatait figyelembe véve még a kiemelkedő képességű személyek felkészítése is rendkívül összetett, erőforrás-igényes feladat. Intenzív felkészülés mellett is hat–tizenkét hónap, mire az új munkatárs kiképezhető a feladatra, és három–öt év, mire teljes értékű műveleti szakemberré válik, aki önállóan képes a rá bízott feladat minden munkafolyamatát átlátni és önállóan kivitelezni. Bizonyos speciális munkafolyamatok (például HUMINT) ehhez képest is hosszabb felkészülési időt igényelnek. Általánosságban elmondható, hogy egy teljes értékű műveleti tiszt kiképzése körülbelül húszmillió forintba kerül.[13]
5. *Széles körű kooperációt igényel:* A nemzetbiztonsági munka folyamán a munkatársak a társadalom minden területével és szegmensével kapcsolatba kerülhetnek, és képeseknek kell lenniük együttműködni bárkivel. Ennek nehézségét fokozza a konspiráció szükséglete, a terület érzékenysége, illetve az, hogy érdemi segítséget a másik fél az esetek jelentős részében csak önkéntes elhatározásból ad, erre kényszeríteni nem lehet.

Az előbbiek alapján *a humán erőforrás a nemzetbiztonsági szervezetrendszer stratégiai fontosságú erőforrása,* mivel tevékenysége, illetve annak minősége alapvetően és hosszú távra meghatározza a terület működését, annak ered-

12 Zalai Noémi: Új típusú kihívások a nemzetbiztonsági szolgálatoknál. Nemzetbiztonsági Szemle, 2016/1., 38. o.

13 Ez a számítás tartalmazza a kiválasztás, az oktatás, illetve a mentorálás személyi és tárgyi költségeit (kb. fejenként kétmillió forint), illetve az első három év illetményének költségét (kb. tizennyolcmillió forint), amíg az adott személy általában nem tud teljes értékű munkát végezni. Ha csak az első év költségét számítjuk, amikor az illető még a szervezet működéséhez nem tesz hozzá, akkor is körülbelül nyolcmillió forintba kerül egy tiszt kiképzése.

ményességét és hatékonyságát. A kimagasló szintű emberi tényező részt vesz minden alapfolyamatban, rendelkezésre állása kiemelt fontosságú, mindamellett nem magától értődő, specializált szervezési folyamatot igényel.

Múlt és jelen

A nemzetbiztonsági terület humán erőforráshoz való viszonyát, kezelésének módját manapság két tényező határozza meg döntő mértékben. Egyrészt az a tény, hogy a terület az államigazgatás része, másrészt az a történelmi örökség, amely a nemzetbiztonsági szervezeteket alapvetően a rendvédelmi terület részének tekintette, ehhez igazítva e szervezetek emberképét és az emberek kezelésére hivatott rendszereiket. A szakirodalomban élénk vita folyt és folyik, hogy a nemzetbiztonsági szervezetrendszer a rendvédelem része-e. E tanulmánynak nem célja, hogy ebben a vitában állást foglaljon, azt gondolom, hogy a szervezetrendszer humán rendszerét elsősorban a terület funkciója és a munkavégzési rendszerének jellege kell hogy meghatározza.

A rendszerváltás előtti úgynevezett személyzeti tevékenységet általánosságban igen pejoratív kontextusban említik, feltehetően amiatt, hogy az akkori döntések a szervezet minden szintjén jelentős politikai motivációt hordoztak. E politikailag motivált kádermunka fontosságát mutatja a BM III/6. Osztály ügyrendje, amely szerint az osztály fő feladataként végzi *„a III. Főcsoportfőnökség központi állománya káder- és személyzeti munkáját”*[14]. Az előbbi kategorizálást tekintve ez a tevékenység a személyügyi menedzsment egyszerűsített formája volt. Az önálló szervezeti egységben a tevékenység célja egyértelműen az adminisztráció volt, mindamellett megjelent a kiválasztási funkció.[15] Az oktatás ekkor elsődlegesen egy külső szervezet, a Rendőrtiszti Főiskola feladata volt.[16]

A rendszerváltás után a nemzetbiztonsági szervezetrendszer önálló szolgálatok formájában alakult újjá[17], és a humán szervező funkció az egyes szervezetek hatáskörébe került. Ezzel együtt a tevékenysége a humánpolitika irá-

14 A Belügyminisztérium III/6. Osztály Ügyrendje. 1972 https://www.abtl.hu/sites/default/files/forrasok/ugyrend_11.pdf

15 Uo.

16 Boda József: A tudomány az állambiztonság és a nemzetbiztonság szolgálatában. Nemzetbiztonsági Szemle Különszám, 2014, 85–86. o.

17 Kovács Zoltán András – Dobák Imre: Korszakváltások a magyar nemzetbiztonsági intézményrendszerben. In: Sabjanics István – Finszter Géza (szerk.): Biztonsági kihívások a 21. században. Dialóg Campus, Budapest, 2017, 178. o.

nyába tolódott el. Az elnevezés utal ugyan valamiféle – az emberek szerepét felértékelő – minőségi változásra, ez a tevékenység azonban továbbra is elsősorban adminisztratív jellegű volt[18]. Továbbra is az igazgatási (dokumentálás, nyilvántartás) funkció dominált, e mellett működött még az utánpótlási és a képzési funkció, de összességében továbbra sem haladta meg a személyügyi menedzsment kereteit. Szervezeti szempontból bizonyos értelemben még visszalépés is volt a rendszerváltás előtti időkhöz képest, hogy számos esetben más funkciók (például gazdasági, jogi) alárendeltségébe kerültek a humán tényezőért felelős szervezeti egységek.

A 2000-es évek közepére a társadalmi változások egyre nagyobb kényszerítő erőt jelentettek a biztonsági és ezen belül a nemzetbiztonsági szolgálatok számára. A technikai fejlődés és az újszerű társadalmi jelenségek adta feladatok elengedhetetlenné tették a képzettebb fiatal generációk szervezetbe történő gyors ütemű integrálását. Ez a szükség elindította azt a folyamatot, amelynek során a nemzetbiztonsági szervezetek humán egységei is elmozdultak a modernebb eszközök és módszerek (például informatikai rendszerek, összetett kiválasztási folyamatok) használatának az irányába, miközben összességében a személyügyi menedzsment kereteit továbbra sem sikerült érdemben meghaladni. Ezt mutatja számos máig hiányzó funkció (stratégiai tervezés, munkakör-, karrier- és teljesítménymenedzsment, HR-kontrolling, outplacement stb.), továbbá az a tény, hogy a humán szakterület továbbra is „csak” egy a többi funkcionális terület mellett. Utóbbit támasztja alá, hogy az utóbbi időszakban a humán szakterületek elhelyezésére a szervezetek többségében több hierarchiai szint távolságban, más területekkel együtt került sor.

Az előbbiekből levonható a következtetés, hogy a humán szervező rendszerek tekintetében a nemzetbiztonsági területen nem történt modellváltás, továbbra is a hetvenes évektől megszokott személyzeti gondolkodásmód a jellemző. Bár az alkalmazott módszerek és eszközök tekintetében kétségtelen a fejlődés[19], a rendszerváltás előtti időszak – személyügyi menedzsment szintjét képviselő – elvi keretei és szemléletmódja továbbra is megmaradt, nem érte el a humánerőforrás-menedzsment szintjét. Ez a helyzet már a jelenben is problémákat okoz[20], azonban a jövőre nézve válik igazán kockázatossá, mert a humán erőforrás felértékelődése már a modern menedzsmenttechnikák szükségességének irányába mutat. Ennek kialakítása azonban nemcsak tech-

18 Balajti László – Bathelt Sándor: A humánpolitikától a humánerőforrás menedzsmentig. Szakmai Szemle, 2009/2., 157. o.
19 Uo. 157. o.
20 Zalai Noémi (2016): i. m. 35. o.

nikai jellegű változásokat, hanem szemléletbeli változást, a humán tényezőhöz való viszony radikális újragondolását igényli. Ez történhet például új értékek (kreativitás, önállóság) meghonosításával[21], eszköze lehet a stratégiai menedzsment révén végrehajtott szervezetikultúra-váltás, illetve -fejlesztés.

Ha pedig nem történik meg a humán terület megújítása, akkor a nemzetbiztonsági ágazatnak már rövid távon súlyos munkaerőhiánnyal, erős fluktuációval és kontraszelekcióval, valamint az állomány motivációjának tartósan alacsony szintjével kell szembenéznie.

Mit lehet tenni?

Mielőtt a konkrét megoldáson gondolkodnánk, szükséges egy alapvetés lefektetése: a nemzetbiztonsági szervezetrendszerben a jövő legfontosabb erőforrása az ember lesz.

E gondolat eredője kettős: Egyrészt a modern emberierőforrás-menedzsment egyik fő gondolata az, hogy *„az emberi erőforrás önmagában azért is meghatározó szerepet játszik, mert a többi erőforrás hatékony felhasználása, működtetése emberi tényező nélkül lehetetlen”*[22]. Nagyobb jelentőségű azonban az a tény, hogy a társadalmi folyamatok jelentősen megváltoztatják az emberek viselkedését, munkához való viszonyát, valamint felértékelik a humán erőforrás szerepét. Utóbbit jól példázza, hogy miközben például titkosszolgálati szervezetek és ellenfeleik között intenzív kreativitási verseny zajlik, az ötletek „előállítására” képes – erősen korlátos számú – humán erőforrásért öldöklő verseny indult a munkaerőpiacon[23]. A minőségi munkaerő iránti kereslet ekként átalakítja a munkaerőpiaci viszonyokat és jelentősen javítja a munkavállalók alkupozícióját a munkáltatókkal, nagymértékben nehezítve utóbbiak helyzetét.

A munkavállalói viselkedés változásának fő forrása a társadalmi fejlődés, az általa generált és már évtizedek óta zajló attitűdváltozás, illetve az új generációk felnőtté – és egyben társadalomformáló erővé – válása, valamint munkaerőpiacra történő belépése. Az attitűdváltás oka, hogy az emberek motivá-

21 Uo. 40. o.

22 Hajós László – Berde Csaba (szerk.): Emberi erőforrás gazdálkodás. Egyetemi tankönyv. Debreceni Egyetem, Debrecen, 2007, 7. o. http://miau.gau.hu/avir/intranet/debrecen_hallgatoi/tananyagok/jegyzet/06-Emberi_eroforras_gazdalkodas.pdf

23 https://szazadveg.hu/hu/kutatasok/az-alapitvany-kutatasai/otletmuhely/az-otletek-az-uj-szukos-eroforras

ciói is változnak. A munkavállalói döntések során az anyagi megbecsülés mellett egyre inkább megjelenik az önállóság, az önmegvalósítás igénye. Széles körben elfogadott, hogy e folyamat a maslow-i szükséglethierarchiával mutatható be a legegyszerűbben. E szerint a szükségletek egymásra épülnek és az emberek a szükségleteiket alapvetően alulról felfelé haladva elégítik ki.[24]

Az attitűdváltás fő mozgatórugója, hogy a munkavállalók alacsonyabb rendű szükségletei a társadalmi fejlődés következtében kielégítődnek, így egyre inkább a piramis csúcsán található belső motivátorok adják a valódi motiváló erőt. A magasabb rendű motivációk kielégítése pedig elsősorban a munkahelyen, munkatevékenység által lehetséges.[25] Végső soron *„a munkavállaló személyes stratégiáját olyan kihívó, fejlődést jelentő problémák felvállalása és megoldása jelenti, amelyek a szervezet és az egyén számára is sikerre vezetnek”*[26].

Az új generációk megjelenése által okozott problémákat vizsgálva fontos megjegyezni, hogy itt már nem pusztán a generációk különbözőségéről van szó, hanem ennél sokkal többről, a társadalmi generációváltás folyamata változott meg. *„Napjainkban ez az átmenet minőségileg különbözik az eddigiektől, az értékrendek módosulnak, az informatikai forradalom hatására ma már nem egyértelmű, hogy ki tanul kitől, a tanulás, a munka értelmezése és módszertana teljesen új dimenzióban jelenik meg.”*[27] A szervezetekhez újonnan belépők ma főként az Y generációhoz tartoznak, amely az első digitális nemzedék. E korosztály jelentőségét mégis inkább az adja, hogy ez az első fordított szocializációs generáció[28], azaz tudásuk jelentős részét nem a korábbi generációtól kapják, hanem a saját korcsoportjukba tartozóktól.[29] Ez jelentős hatást gyakorol az értékrendjükre, a magatartásukra, arra, hogy különösen az idősebb generáció tagjaival nem az elvárt és megszokott módon viselkednek. A 2020-as évektől a munkaerőpiacra belépő Z generáció ugyanezt az utat járja be, csak robbanásszerűen növekvő sebességgel, így a korábbi generációkkal *„a békés elsimítás, összeolvasztás lehetetlen”*[30]. Mindez társadalmi szinten általánosságban növekvő konfliktuspotenciált jelent, de különösen olyan

24 Dobák Miklós: Szervezeti formák és vezetés. KJK-Kerszöv, Budapest, 2002, 145. o.
25 Bakacsi Gyula – Bokor Attila – Császár Csaba – Gelei András – Kováts Klaudia – Takács Sándor: i. m. 23. o.
26 Uo. 24. o.
27 Besenyei Lajos: A generációváltás forradalma. Opus et Educatio, 2016/4., 372. o. http://epa.oszk.hu/02700/02724/00009/pdf/EPA02724_opus_et_educatio_2016_04_366-367.pdf
28 Uo. 374. o.
29 Uo.
30 Uo. 375. o.

erős, tekintélyelvű szervezetekben vezethet súlyos belső konfliktusokhoz, amilyenek a nemzetbiztonsági szervezetek is.

A múlt és jövő e konfliktusának a legjobb összefoglalást *McGregor* – szintén a maslow-i elméletre épülő – X és Y emberképpel kapcsolatos, elmélete[31] adja. Az X emberkép szerint a munkavállalók

– általánosságban lehetőség szerint kerülik a munkát, a vezető fő feladata, hogy ezt ellensúlyozza különböző eszközökkel;
– külső kényszerítő erejű ráhatásokkal irányítani, illetve ellenőrizni kell a munkavállalókat azért, hogy rábírhassuk őket a szervezet céljai érdekében történő erőfeszítésre;
– a felelősséget igyekeznek elhárítani maguktól, igénylik az irányítást.

Ez a felfogás a vezetés domináns szerepeit emeli ki, míg a beosztottakat kezdeményezés nélküli, passzív szerepbe kényszeríti. Ennek általában egyenes következménye a kölcsönös bizalomhiány és az ebből fakadó folyamatos ellenőrzés, ami végső soron feszültségnövelő és nagy eséllyel teljesítménycsökkentő hatású.

Ezzel szemben a másik véglet az Y emberkép, amely szerint a munkavállalók egyebek között

– nem idegenkednek a munkától, az természetes és kívánatos számukra;
– képesek elkötelezni magukat szervezeti célok érdekében, és így nem csak a külső kényszer motiválja őket;
– elkötelezettségüket javíthatja a jutalmazás;
– megfelelő feltételek fennállása esetén vállalják a felelősséget a munkájukért.

Míg a katonai hierarchiára és a parancsuralmi rendszerre épülő, masszív szervezeti kultúrájú nemzetbiztonsági szervezetrendszer emberképe, vezetői attitűdje inkább az X emberképhez áll közel, addig az újabb generációk az Y emberképhez, sőt bizonyos értelemben már meg is haladták.

Az előbbiek alapján a stratégiai emberierőforrás-menedzsment hasznossága elsősorban ott nyilvánulhat meg, hogy alkalmazásával a nemzetbiztonsági szervezetrendszer képessé válhat a társadalmi változásokhoz való alkalmazkodásra, és feladatellátása folyamán nem elszenvedője, hanem hasznosítója lehet e változásoknak.

Ahhoz, hogy javaslatokat tehessünk a stratégiai emberierőforrás-menedzsment alkalmazására, első lépésként célszerű megvizsgálni, mi lehet an-

31 Dobák Miklós – Antal Zsuzsanna: Vezetés és szervezés. Aula Kiadó, Budapest, 2010, 351. o.

nak az oka, hogy az elmúlt évtizedekben erre nem került sor. Véleményem szerint ennek alapvetően három oka van:

– a nemzetbiztonsági szervezetrendszer az államigazgatás része;
– a nemzetbiztonsági szervezetrendszer erős és zárt szervezeti kultúrája;
– a magyar stratégiai kultúra alacsony színvonala.

Azzal, hogy a nemzetbiztonsági szervezetrendszer az államigazgatás része, törvényszerűen átveszi azt a gondolkodásmódot, azokat a szervezési és működési elveket, amelyek e szervezeteket jellemzik. Általánosságban ezek a lineáris és hierarchikus szervezés, a bürokratikus kontroll dominanciája, illetve a lassú reakció a környezeti változásokra, az alacsony szintű megújulási képesség.

A nemzetbiztonsági szervezetrendszer a jellegéből adódóan zárt, működése, belső viszonyai kevesek számára megismerhetők. Szervezeti kultúrájának elemei a több ezer éves katonai múltban gyökeredznek, ezen kívül a szovjet típusú állambiztonsági modell negyven éve gyakorolt rá meghatározó hatást. A rendszerváltást követő időszakban, a szervezetrendszeri jogutódlás és a személyi állomány átvétele továbbra is életben tartotta ezt a fajta szemléletmódot, amely a 2000-es években, külső események hatására kezdett csak lassan átalakulni. A megújulás megkezdését, annak sebességét és minőségét feltehetően érdemben ronthatta az a körülmény, hogy a nemzetbiztonsági terület társadalmi kontrollja elég gyenge. Az ágazat problémáiról, jövőjéről – mint ahogy a biztonságpolitikai kérdésekről általánosságban – széles körű, nyilvános társadalmi diskurzus egészen a közelmúltig valójában nem kezdődött. Jó hír azonban, hogy elsősorban a Nemzeti Közszolgálati Egyetem Nemzetbiztonsági Intézetének tevékenysége révén a szakmai diskurzus élénkülése tapasztalható, mert ez mindenképp feltétele a társadalmi vitának, végső soron pedig hajtóereje lehet a szakmai megújulásnak[32].

A stratégiai kultúra vizsgálata viszonylag új kutatási terület, amely eddig elsősorban a védelem- és biztonságpolitikai témakörben vizsgálta a magyar stratégiai kultúrát, egészen pontosan annak hiányát[33]. Ezt a hiányt mutatja a nemzeti biztonsági stratégia és az abból származó ágazati stratégiák helyzete. Az első nemzeti biztonsági stratégia már 2004-ben elkészült, és már akkor rögzítette egyebek között a nemzetbiztonsági ágazati stratégia szükségességét, ennek kidolgozására azonban azóta sem került sor, és a közeljövőben er-

32 Regényi Kund: Tudományosság, mint új kihívás az Alkotmányvédelmi Hivatal számára. Hadtudomány, 2013/1–2., 92. o.
33 Tálas Péter: A nemzeti katonai stratégia és a magyar stratégiai kultúra. Hadtudomány, 2013/3–4., 15. o.

re kevés esély is mutatkozik[34]. Témánk szempontjából a kérdés relevanciáját inkább az adja, hogy mi okozza a stratégiai kultúra hiányát, és ez miben nyilvánul meg. A legfőbb ok valószínűleg a stratégiával kapcsolatos ismeretek hiánya, másrészt ettől nem függetlenül egy olyan gondolkodásmód, amely akadályozza a stratégiai szemlélet gyakorlatban történő kipróbálását. A stratégiára még a mai napig is legtöbben úgy gondolnak, mint valamilyen elvont, túlságosan elméleti, a napi gyakorlattól távol eső dologra. Jóllehet a stratégiai menedzsment módszertanát, gyakorlati lépéseit pont azért fejlesztették ki, hogy a turbulens környezeti viszonyok között is fenn lehessen tartani az egyes szervezeti funkciók folyamatos összhangját.[35]

A stratégiai háttértudás hiánya arra vezethető vissza, hogy a közép- és felsőfokú oktatásban a stratégiai alapismeretek és szemléletmód átadása, illetve a stratégiai menedzsment gyakorlati oktatása, leszámítva bizonyos gazdasági képzéseket, általánosságban nem része a tananyagnak. Továbbképzés, például a rendészeti vezetővé, illetve mestervezetővé képző tanfolyam keretében megtörténik ilyen jellegű ismeretek átadása, mindamellett ezek hatékonysága nem vetekedhet a közép- és felsőfokú oktatás időkeretével, nem beszélve a fiatalabb korból adódó könnyebb adaptáció előnyéről.

A szemléletbeli akadályozó tényezőket – a szervezeti kultúra analógiáját segítségül híva – olyan *téves hiedelmek és hibás előfeltevések* jelentik, amelyek megakadályozzák a stratégiai gondolkodás beindulását. Ezek közül a fontosabbak a következők:

A stratégia kizárólag gazdasági szervezetek számára hasznos és indokolt – gyakori vélemény, hogy a stratégia, a stratégiai menedzsment csak a profitorientált vállalkozások eszköze lehet. Valójában a stratégia mint eszköz állami „termék”, amikor is az országok létükben való fenyegetettségükre a hadi célokra alkalmazható erőforrások optimális felhasználását elősegítő hosszú távú (katonai) terveket dolgoztak ki. Ezeket a módszereket vette át és fejlesztette tovább a civil szféra a szervezeti hatékonyság fokozása érdekében. Ennek alapján a stratégiaalkotás minden szervezet számára hasznos lehet, amely meghatározott céljait az optimális erőforrás-felhasználás mellett szeretné elérni. Ilyen cél nemcsak a profit lehet, hanem bármely olyan eredmény, amely egy közösség, ország számára hasznos.

34 Drusza Tamás: A nemzetbiztonsági stratégiáról a Nemzeti Katonai Stratégia tükrében. Nemzetbiztonsági Szemle, 2017/3., 87. o.

35 Barakonyi Károly: Stratégiai menedzsment. Nemzeti Tankönyvkiadó Digitális Tankönyvtár, 2011. http://www.tankonyvtar.hu/hu/tartalom/tamop425/2011_0001_519_42551/ch01s02.html

Az állami szervezeteknek nincs szükségük stratégiára, mert a jogszabály határozza meg a céljukat – valójában a jogszabályok sosem a szervezetek céljait határozzák meg, sokkal inkább a funkciójukat, létezésük okát, stratégiai nyelven szólva a küldetésüket. A küldetés pedig megjelenik a stratégiai tervezésben, ennek folyamatában fontos szerepet kap. Ez azonban nem keverendő össze az adott szervezet konkrét időtávra meghatározott stratégiai céljaival. A katonai területet példaként hozva: a hadsereg küldetése az ország védelme a külső katonai fenyegetéssel szemben, de egy adott időszakban a felkészülés a legvalószínűbb konkrét ellenséges fenyegetés ellen zajlik. E külső fenyegetés forrása és jellege idővel akár változhat is, ezáltal kényszerítve az adott ország hadseregét új stratégiai tervek készítésére és végrehajtására.

A hosszú távú stratégia gátolja a rugalmas reagálást és a döntéshozatalt – a stratégiaalkotás, a stratégiai menedzsment célja nem az, hogy évekre előre eldöntsön mindent, hanem hogy garantálja a kitűzött célok egymással való összhangját, illetve azt, hogy az ezek elérése érdekében tett napi intézkedések ne egymás ellen hassanak, hanem egymást támogassák. Ha egy szervezet cél- és erőforrásrendszere letisztult, akkor a stratégiai menedzsment sokat segíthet ezek összehangolásában. Amennyiben ezek közül valamelyik hiányzik, vagy a szervezetben egymásnak ellentmondó célok vannak jelen egyidejűleg, akkor a stratégia támogató szerepe ott mutatkozik meg, hogy segít feltárni és kiküszöbölni ezeket az ellentmondásokat. Mindezek mellett a stratégia hosszú távú (koncepcionális) és rövid távú (operatív) része is tetszés szerint módosítható, alakítható, hogyha valami – legtöbbször a környezet változása – ezt indokolja. Az egyetlen kritérium, hogy e két előbbi rész, illetve a célok és intézkedések összhangja továbbra is meg kell hogy maradjon.

Adódik a kézenfekvő következtetés: az államigazgatásban meg kellene honosítani a stratégiai szemléletmódot és eszközrendszert. Ennek megvalósítása azonban csak hosszú távú programként lehetséges, optimista becsléssel is minimum évtizedes időigénnyel. Véleményem szerint a nemzetbiztonsági ágazat ideális „kísérleti” terep lenne a stratégiai humanerőforrás-menedzsment államigazgatáson belül történő alkalmazására, mivel olyan egyedi terület, ahol egyszerre vannak jelen a szigorú jogszabályi keretek, valamint a proaktivitás, illetve a nagyfokú kreativitás igénye.

Ennek megvalósulása két lépésben történhet. A következőkben vázolt két lépés nem feltételezi egymást, de a második megvalósulása jelentősen javítaná az első pontban felrajzoltak esélyét, és csökkentené a megvalósításhoz szükséges időt.

Szervezeti szintű stratégiai humánerőforrás menedzsment rendszerek kialakítása és működtetése – a stratégiai emberierőforrás-menedzsment funkció a nemzetbiztonsági szervezetrendszer jelenlegi szervezeti és működési kereteibe minden további nélkül beilleszthető, természetesen a titkosszolgálati szakmai szabályok teljes figyelembevétele mellett. Alkalmazása igényel ugyan egy újszerű szemléletmódot, de véleményem szerint ez a rendszer kiépítésének folyamata révén nagyrészt megszerezhető, másrészt az előnyök rövid távú megmutatkozásával a szervezet gyorsan magáévá tudja majd tenni. A nemzetbiztonsági szervezeteknek, illetve vezetőiknek megvan az a felhatalmazásuk, hogy szolgálataik humánerőforrás-rendszerét új szemlélettel szervezzék meg és működtessék. Ennek lépései például a következők lehetnek:

a) Megfelelő emberi erőforrás biztosítása: egy ezerfős szervezetben a meglévő erőforrások optimalizálása mellett két-három, egyetemi szintű végzettségű, naprakész humánerőforrásmenedzsment-ismerettel felvértezett szakértő alkalmazása elégséges stratégiai emberierőforrás-menedzsment funkciók megvalósításához.
b) HR-stratégia elkészítése, stratégiai tervező funkció kialakítása.
c) Az első számú vezető közvetlen alárendeltségébe telepített, önálló (azaz más funkcionális szervezeti egységektől teljesen független) szervezeti egységben kell elhelyezni ezt a funkciót, mivel ez biztosítja a szervezeten belüli integrációs szerep betöltését és a hatásos felső vezetői részvételt és kontrollt. A humán szervezeti egységen belül az igazgatási és a menedzsment (a megfelelő munkaerő rendelkezésre állását elősegítő) munkafeladatokat szükséges szétválasztani, hogy mindkét terület működése optimalizálható lehessen.
d) A „megfelelő embert a megfelelő helyre” elv érvényesítése érdekében a következő fontos és szükséges, de még hiányzó emberierőforrásmenedzsment-funkciók kialakítása:
   – teljesítménymenedzsment, amelynek célja nem pusztán a teljesítmény objektív mérése, hanem a teljesítmény növelési lehetőségeinek feltárása;
   – karriermenedzsment (tehetségmenedzsment, karrierívtervezés, utánpótlás-menedzsment);
   – munkakörökre épülő munkavégzési rendszer alkalmazása. A 2015-ben hatályba lépett új Hszt. alapelvei között szerepel a munkakörökre történő átállás támogatása;
   – HR kontrolling-rendszer kialakítása annak érdekében, hogy a vezetésnek objektív, naprakész és folyamatszemléletű helyzetképe legyen a humán erőforrásról;

– outplacement rendszer kialakítása annak érdekében, hogy a szervezetbe nem illeszkedő munkavállalók ne ragadjanak benne a rendszerben.

Politikai szándék kinyilvánítása, jogszabályi alátámasztása – az első pontban meghatározottak támogatására célszerű lenne a következők megvalósítása, az ehhez szükséges alacsonyabb szintű jogszabályok megalkotása:

a) ágazati szintű (humán) stratégiai alapelvek kialakítása és rögzítése;
b) humánerőforráskoncepció- (stratégia) kialakítási és -alkalmazási kötelezettség – legalább utalás szintjén történő – rögzítése a szervezetek számára. Utóbbi a magyar jogszabályi kultúrában kétségtelenül újszerű kezdeményezés lenne. Mindamellett például az Egyesült Államok jogszabályalkotásában, éppen a hírszerző közösség vonatkozásában is található erre példa[36];
c) a szükséges – egyébként nem túl jelentős – plusz erőforrások rendelkezésre bocsátása támogathatja a humán szervező tevékenység kiegészítését, megújítását.

Végezetül, az előbbi két pont támogatása érdekében érdemes röviden megvizsgálnunk, hogy a nemzetbiztonsági rendszer küldetését, jelenlegi helyzetét, működési környezetét figyelembe véve a szolgálatoknak milyen jellegű humánerőforrás-stratégiát célszerű készíteniük és alkalmazniuk. Ehhez a tevékenységhez szükséges munkaerő két jellemzőjét, az egyediséget és az értékességet szokták vizsgálni, a *táblázat* szerint.[37]

	Inkább értékes	Kevésbé értékes
Inkább egyedi	Belső fejlesztés	Szövetség
Kevésbé egyedi	Felvásárlás	Szerződés

Tekintettel arra, hogy a korábban leírtak alapján a nemzetbiztonsági területen tevékenykedők értékes és teljesen egyedi tevékenységet végeznek, ezért a *nemzetbiztonsági szervezetek esetében egy belső fejlesztő jellegű emberierőforrás-stratégia indokolt.* A vázolt feltételeknek megfelelő munkatársak *„tekinthetőek alapvető szervezeti képességet hordozó (»core«) munkaerőnek, megtartásuk és fejlesztésük kulcsfontosságú. Kiválasztásuk és megtartásuk során nem első sorban azonnali teljesítményük, hanem a bennük rejlő potenciál és a szervezethez való illeszkedésük a legfontosabb. Cél a hosszú távú*

36 Intelligence Reform and Terrorism Prevention Act of 2004
37 Bakacsi Gyula – Bokor Attila – Császár Csaba – Gelei András – Kováts Klaudia – Takács Sándor: i. m. 76. o.

elkötelezettség megteremtése hosszú távú karrierterveken és ösztönzési csomagokon keresztül."[38] Meggyőződésem szerint e cél a jövőben eredményesen a stratégiai emberierőforrás-menedzsment alkalmazásával valósítható meg.

Összegzés

Már a közeljövő társadalma, és így a nemzetbiztonsági szervezetek is, olyan új jelenségekkel néznek majd szembe, amelyek kezelése új szemléletet igényel. *„A problémák elvi okai az exponenciálisan felgyorsult időben keresendők, konkrétan abban, hogy az egyre gyakoribbá váló minőségi ugrások, forradalmi változások olyan új helyzetet eredményeznek, amelyek megértése és kezelése a hagyományos, régi szemléletmódban lehetetlen."*[39] Szerencsére léteznek eszközök arra, hogy a jövő problémáit megvizsgáljuk, és azokra megoldásokat találjunk, ehhez azonban fel kell ismerni a cselekvés szükségességét, ki kell alakítani a tettvágyat, ami minden újító cselekvés alapja.[40] Az előzőekben áttekintettük, vázoltuk a nemzetbiztonsági ágazat mibenlétét, a humán kihívások jelentős elmeit, illetve egy lehetséges megoldási javaslatot. Szokták mondani, hogy az állami szervezetekben sokszor csak külső körülmények okozta válsághelyzetek kényszerítő ereje képes érdemi változást elindítani és véghezvinni. Ez a tanulmány azonban abból a meggyőződésből született, hogy a jelen és a jövő körülményeinek alapos és következetes elemzése és a gondolatok közrebocsátása, ha kicsit lassabban és nehézkesebben is, de képes beindítani a szükséges változásokat. A változás szelei már erősen fújnak, a vitorlák kifeszítése pedig csak – stratégiai – döntés kérdése.

38 Uo.
39 Besenyei Lajos: i. m. 375. o.
40 John P. Kotter: Tettvágy – változásmenedzsment stratégiai vezetőknek. HVG Kiadó Zrt., Budapest, 2009, 11–12. o.

DOI: 10.38146/BSZ.2018.2.5

CSÁNYI CSABA

Terrorizmus és szervezett bűnözés, avagy profit vs. ideológia?

Az Európai Parlament rendszeresen rendel közvélemény-kutatásokat a huszonnyolc tagállamban. Az Eurobarometer közelmúltban készített felmérése alapján az európai polgárokat leginkább a terrorizmus, a szervezett bűnözés, valamint az illegális migráció témaköre érdekli.[1]

Joggal vetődik fel az a kérdés mindenkiben, hogy mi lehet az a közös pont, ami összekapcsolja ezt a három témakört. Erre próbálom megadni az esetleges választ.

Szervezett bűnözés

A szervezett bűnözés fogalmát nehéz tökéletesen definiálni, ezért inkább néhány jellemző ismérvén keresztül próbálják meg értelmezni, amelyek e bűncselekmények elkövetési forma bármely fajtájánál jelentkeznek.[2] Az uniós értelmezés szerint a négy kötelező kritérium mellett további két esetleges ismérv megléte szükséges az adott szervezett bűnözői csoport bűnszervezetként történő meghatározásához. Figyelembe véve az előbbieket, a hagyományos értelemben vett „szervezett bűnöző csoport” kifejezés egyre problémásabb lehet. Az Eu-

1 Az Európai Parlament speciális Eurobarometer-felmérését a TNS Opinion végezte el 2016. április 9. és 18. között az unió huszonnyolc tagállamában. http://www.europarl.europa.eu/atyourservice/hu/20160623PVL00111/Európai-polgárok-2016-ban-vélemények-és-elvárások-a-terrorizmus-és-a-radikalizálódás-elleni-küzdelem

2 Az Európai Tanács szervezett bűnözés büntetőjogi és kriminológiai kérdéseivel foglalkozó szakértői csoportja által meghatározott kriminológiai ismérvek. Ezek két fő csoportra bonthatók, egyik csoport a kötelező kritériumok csoportja, a másik pedig az esetleges kritériumoké. A kötelező kritériumok ezek szerint: három, vagy több személy együttműködése; hosszú távú, vagy meghatározatlan időre szóló együttműködés; súlyos bűncselekmények gyanúja, vagy azok elkövetése; anyagi haszonszerzési, és/vagy hatalmi pozícióba kerülési cél. Az előbbiekkel szemben az esetleges kritériumok közé pedig a következők tartoznak: minden egyes résztvevőnek meghatározott feladata, vagy szerepe van; valamely belső fegyelmi vagy ellenőrzési forma használata; megfélemlítés céljából erőszak, vagy egyéb eszközök alkalmazása; befolyás kiterjesztése a politikusokra, a médiára, közigazgatásra, a rendészeti szervekre, az igazságszolgáltatásra, illetve a gazdasági élet szereplőire korrupció vagy bármely más módszer alkalmazásával; kereskedelmi, vagy üzleti jellegű struktúrák felhasználása; részvétel a pénzmosásban; nemzetközi szinten történő működés.

rópai Tanács definíciója[3] egyebek közt tartalmazza a stabilitásra és potenciális tartósságra vonatkozó kritériumot. Ez a definiálási mód, bár szükséges, kizárhatja a bűnözői együttműködés több formáját is, amelyek egyébként megfelelnének a hagyományos szervezett bűnözői kritériumoknak.

A szervezett bűnözés megjelenése, elterjedtsége, nemzetközivé válása napjaink szinte magától értődő jelensége, amely az Európai Unió tagállamait is érinti. A technológiai fejlődés, valamint a növekvő globalizáció új lehetőségeket kínál a szervezett bűnözésben részt vevő csoportoknak. A Közös Piac egyik alapelve a munkaerő szabad áramlása a tagállamok közt[4], ezzel összefüggésben a tagállamok a belső határok fizikai és technikai felszámolására törekedtek. De a határok korlátlan átjárhatósága a tagállamok között maga után vonta az illegális migráció és a szervezett bűnözés elterjedését, illetve elterjedésének veszélyét.[5]

A szervezett bűnözés jellemzője, hogy aláaknázza a jogszerű gazdaságokat, és destabilizáló tényező a társadalom szociális és demokratikus felépítésében is, valamint a profit maximalizálása mellett/maximalizálásáért kapcsolatot próbál kialakítani a politikával.

Az új közlekedési, kereskedelmi és kommunikációs eszközöket magabiztosan használó szervezett bűnözés földrajzi terjeszkedésének egyértelműen kedvez az új, nyitott Európa, miközben a bűnüldöző szolgálatokat még mindig sok esetben terhelik a mindennapi tevékenységüket akadályozó jogi és adminisztratív kötelezettségek.

A szervezett bűnözői csoportok egyre összetettebb és strukturáltabb üzleti szervezetekké válnak, amelyek képesek behatolni a gazdasági és pénzügyi piacokra, illetve eltorzítani azokat olyan legális gazdasági közegeket keresve, amelyekbe illegálisan szerzett jövedelmeiket – gyakran kifinomult pénzmosási műveletek révén – beáramoltathatják.

A szervezett bűnözők dolgát könnyíti a passzív és alulinformált közvélemény, a gyakran a közigazgatásba is beszivárgó korrupció, valamint azok a bürokratikus nehézségek, amelyek gátolják a közösségi szinten működő bűnüldöző szervek működését.

---

3 6204/2/97. számú dokumentum. Enfopol 35 rev2. http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&type_doc=COMfinal&an_doc=2005&nu_doc=232&lg=en

4 A személyek szabad mozgása az Európai Unió egyik tartópillére, az Európai Gazdasági Közösségek alapításáról szóló 1957. március 25-i római szerződés 3. cikk c. pontja és az 1986-os egységes európai okmány óta szerves része az integrációs folyamatnak.

5 John Lambert: EU single market success leads to some problems. European Dialogue, no. 3, 1998, p. 2.

Az egyre professzionálisabb bűnözők a jogi, gazdasági és technológiai keretfeltételek változásaihoz való rugalmas alkalmazkodással bűncselekményeket követnek el a kábítószerek tiltott kereskedelme terén, üzleti, társasági formák felhasználásával illegális ügyleteket legális gazdasági tevékenységekkel kapcsolnak össze, és készek arra, hogy céljaikat, nevezetesen nyereségük maximalizálását és hatalmi törekvéseik kielégítését könyörtelenül, a személyek és vagyontárgyak ellen irányuló erőszakkal vagy az azzal való fenyegetéssel, valamint a politikára, a gazdaságra és a közigazgatásra gyakorolt befolyásuk felhasználásával érjék el.

Az Europol szerint az unióban tevékenykedő bűnszervezetek körülbelül fele uniós tagállamok polgáraiból áll, és jelentős részüknek különféle bűncselekményekkel összefüggésben az unión kívüli országokban más kapcsolataik is vannak.[6]

Az Europol szerint jelenleg körülbelül háromezer-hatszáz szervezett bűnözéssel foglalkozó csoport tevékenykedik az unió területén, ezekben pedig mintegy negyvenötezer személy részvétele ismeretes. Ezek a tagállamok által rendelkezésre bocsátott adatokon alapuló számok azonban pusztán szemléltető jellegűek, a valóságban bizonyára sokkal magasabbak. A csoportok mérete, szerkezete, szervezettsége és egyéb jellemzői mind tagállamokon belül, mind azok között eltérő.

Az európai szervezett bűnözői csoportok mindenféle bűnözői tevékenységben részt vesznek, közülük ki kell emelni a fegyver- és kábítószer-kereskedelmet, az illegális bevándorlást, az emberkereskedelmet, a prostitúciót, valamint az ezekhez kapcsolódó szervkereskedelmet, hagyományos bűncselekménynek mondható csempészetet, a műkincsrablást, bérgyilkosságot, zsarolást, a csalást és a pénzügyi visszaéléseket.

Terrorizmus

A terrorizmus nem új keletű probléma, és abban sincs újdonság, hogy a terrorfenyegetettség és a terrorcselekmények szinte mindig jelen voltak a különböző történelmi korokban. Mindezek ellenére mégis csak az utóbbi évtizedben jelent meg világszinten a biztonságra való fókuszálás, ami a jelenkori, modern terrorizmus mindent behálózásával és növekvő mértékével magyarázható.

6 http://www.europol.eu.int/index.asp?page=publar2004#INTRODUCTION

A terrorizmus kapcsán is elmondható: sokan, sokféleképp próbálták már definiálni, de absztrakt, mindenki által elfogadott definíció még nem született.

A terror (latinul *formidilosus, terror* = ijedtség, rettegés, rémület) a nyílt erőszak alkalmazása rémület, rettegés kiváltása céljából, a terrorizmus kifejezés pedig erre épülve (a legáltalánosabban elfogadott megfogalmazás szerint) valamely szervezet által politikai okokból végrehajtott erőszakos, félelemkeltő akciók sorozata.[7]

A *Harmat–Bukva* szerzőpáros szerint a terrorizmus az erőszak alkalmazásának, vagy az azzal való fenyegetésnek olyan stratégiája, amelynek elsődleges célja félelem, zavar keltése és ennek révén meghatározott politikai eredmények elérése, vagy a hatalom megtartása. A félelemkeltés az erőszak minden formájának velejárója (a kocsmai verekedéstől a hagyományos hadviselésig), segítője lehet, de a terrorizmus esetében ez a viszony fordított, az erőszak közvetlen áldozatai, kárvallottai legfeljebb csak szimbolikus kapcsolatban állnak az akció valódi céljával, kiválasztásuk másodlagos jelentőségű, legtöbbször véletlenszerű.[8]

Fletcher szerint lehetetlen a terrorizmus egzakt definícióját meghatározni, álláspontja szerint meghatározott feltételek, ismérvek megléte esetén beszélhetünk terrorizmusról.[9]

Ezt az álláspontot osztja *Ben Saul* is, de véleménye szerint nincs különbség a belső politikai erőszak és a terrorizmus között.[10]

Korinek László is egyetért azzal, hogy bizonyos, előre meghatározott ismérvek vizsgálata szükséges a terrorizmus meghatározásakor. Álláspontja szerint a terrorizmus általános ismérve a jogellenes erőszak, a politikai (vallási, ideológiai) célok követése, a nyilvánosság keresése, a propaganda. Véleménye szerint fontos szempont a meghatározáshoz az, hogy a terroristák nem tekintik magukat bűnözőnek.[11]

Az előbbiek mellett számos külföldi és hazai kutató megpróbált rendet teremteni a terrorizmus definíciója kérdésében – kevés sikerrel.

Az egyértelműen megállapítható, hogy nagyon nehéz, bonyolult a terrorizmus komplex meghatározása. Ha elfogadjuk, hogy a terrorizmus definiá-

---

7 https://hu.wikipedia.org/wiki/Terror

8 Harmat Árpád Péter – Bukva Kármen: A terrorizmus története. Történelemcikkek.hu, 2015. február 7. http://tortenelemcikkek.hu/node/185

9 George P. Fletcher: The Indefinable Concept of Terrorism. Abstract. Journal of International Criminal Justice, vol. 4, iss. 5, 2006. http://jicj.oxfordjournals.org/content/4/5/894.abstract

10 Ben Saul: Defining 'Terrorism' to Protect Human Rights. FRIDE, February 2006. [Working Paper 20] http://fride.org/download/WP20_DefinTerro_ENG_feb06.pdf

11 Korinek László: A terrorizmus. Belügyi Szemle, 2015/7–8.

lásához különböző feltételek, jellemzők meglétét kell vizsgálni, akkor azt is el kell fogadnunk, hogy nem mindig kell az összes tényezőnek feltétlenül teljesülnie.

Ha egyetértés nem alakult is ki a meghatározás kapcsán, az kijelenthető, hogy a nemzetközi közösség tagjai között egyetértés mutatkozott a megítélésben.[12]

Migráció

A menekült (migráns) olyan személy, aki származási vagy szokásos lakhelyének országán kívül van, mert faji, vabűncselekményeket is elkövetnekllási, nemzetiségi vagy politikai üldözés éri, vagy mert egy üldözött társadalmi csoport tagja.[13] A bevándorlás emberek életvitelszerű áttelepülése születési országukból vagy korábbi lakóhelyükről egy másik országba. 2013-ban a világ népességének mintegy 3,25 százaléka volt bevándorló.

Az áttelepülők általában igyekeznek az új hazájukban legalizálni helyzetüket, ezért tartózkodási és munkavállalási engedélyt, majd állampolgárságot kívánnak szerezni. A népvándorlást nyomó és húzó erők teszik indokolttá. A nyomó erők közt lehetnek politikai okok (például kirekesztés, üldöztetés), gazdasági okok (szegénység, munkanélküliség, egészségtelen környezet), háborús vagy egyéb okok; a húzóerők közt szerepelhet a befogadó ország megnövekedett munkaerőigénye, szervezett betelepítés, a magasabb minimálbér, a gazdag országok esetében a képzettebb tömegek „elszívása” a szegényebb országokból.[14]

Diszkusszió

Terrorizmus – migráció

A terrorszervezetek számára egy felkészített, megfelelő ideológiával bíró embert – egy terroristát – sokkal egyszerűbb és biztosabb kerülő úton, repülővel, vonattal bejuttatni Európába, mint a migránsok között. Egy kiképzett, a

12 Tálas Péter – Póti László – Takács Judit: A terrorizmus elleni küzdelem fogalmi és tartalmi keretei, különös tekintettel annak katonai dimenziójára. ZMNE Stratégiai Védelmi Kutató Központ Elemzések, 2004/3.

13 https://hu.wikipedia.org/wiki/Menekült

14 https://hu.wikipedia.org/wiki/Bevándorlás

feladatokat híven végrehajtó terrorista a szervezet számára jelentős értéket képvisel, nem veszélyeztetnék azzal, hogy a migránsok között rejtik el, kockáztatva akár a célországtól történő visszafordítását, akár azt, hogy már az út során valamilyen baj éri, például belefullad a Földközi-tengerbe az átkelés közben. Ezt az álláspontot képviseli *Alain Rodier* terrorizmus- és szervezett-bűnözés-szakértő is, aki korábban a francia titkosszolgálat egyik vezető tisztségviselője volt.[15] Álláspontját a tekintetben én is osztom, miszerint elképzelhető, hogy a már a célországban tartózkodó migránsok közül az aktivisták újabb híveket toboroznak. Ez azért is lehetséges forgatókönyv, mert sok migráns csalódott az európai fogadtatásban/elutasításban. Másrészt ezek az emberek nem egyszer háborús övezetből érkeznek, így ismerik a különböző fegyverek kezelését, valamint harci tapasztalatuk is lehet. E tényezők megkönnyítik a helyszínen az aktivisták/beszervezők munkáját, akik így könnyen kialakíthatnak új sejteket.

Terrorizmus – szervezett bűnözés

Míg a szervezett bűnözés jelenléte állandósult Európában, addig a terrorizmus – bár terroristák egyre többször csapnak le Európa különböző országaiban – szerencsére nem mindennapos a kontinensen.

Az viszont kijelenthető, hogy a drogterjesztéssel, fegyverkereskedelemmel, prostitúcióval foglalkozó bűnbandák kapcsolatba kerülnek/kerülhetnek terrorista csoportokkal/sejtekkel. A szervezett bűnözés és a terrorista csoportok egymással párhuzamosan működnek, de ideológiájuk, céljuk eltér egymástól. Az együttműködés során csak és kizárólag a nyereségvágy, a profit a cél. A szervezett bűnözés arra specializálódott, hogy illegális úton minél nagyobb nyereségre tegyen szert, legyen szó akár fegyver-, drog-, ember-, szervkereskedelemről, -csempészetről. A céljaik elérése érdekében a terrorcsoportok a bűnözői csoportok döntéshozókkal kialakított kapcsolatait veszik igénybe.

A terrorszervezetek beszerzőként és disztribútorként is támaszkodnak a maffiaszervezetekre. A bűnözői körök értékesítik a terrorszervezetektől származó kábítószert, fosszilis energiahordozót (olaj), lopott műkincseket. A terrorszervezetek számára a maffiacsoportok gondoskodnak a napi javakról, műszaki cikkekről, amikor számukra nem megoldható a kereskedelem. A maffiacsoportok a terroristák rendelkezésére bocsátják – busás haszon fejé-

15 Dezső András: A csalódott migránsokból szervezhetnek terrorista sejteket. Index.hu, 2016. március 9. http://index.hu/kulfold/2016/03/09/francia_exhirszerzo_az_indexnek_a_csalodott_migransokbol_szervezhetnek_terrorista_sejteket/

ben – a már általuk kialakított és bejáratott csatornákat a terroristákhoz kerülő piszkos pénz tisztára mosására is.

A fegyverkereskedő szervezett bűnözői köröknek teljesen mindegy, hogy kinek értékesítik a fegyvert, csak az illető fizesse ki a kialkudott összeget. Itt kell megemlítenem az egyes államoktól esetleg bűnözői körökhöz került vegyi fegyvereket, amelyek lehetséges vásárlói terrorista csoportok.

A szervezett bűnözői körökhöz hasonlóan a terrorista csoportok sem ismernek határokat, sőt az is hasonlóság, hogy sokszor az anyagi bázisuk fenntartása érdekében köztörvényes bűncselekményeket is elkövetnek (emberrablás, -kereskedelem, pénzintézetek ellen intézett támadás, kábítószer-termesztés, -kereskedelem stb.).

Az említettek ellenére – az együttműködésen túl – markáns különbségek is megfigyelhetők a két típusú szervezet között. Más a csoportok motivációja, érdekeltsége. Míg a terrorista csoport még a köztörvényes bűncselekményeket is politikai és/vagy ideológiai célból hajtja végre, addig a szervezett bűnözői csoport pusztán csak gazdaságossági számítást végez, és az alapján hoz döntést, hogy milyen típusú (bűn)cselekmény hozza a legnagyobb profitot a legkisebb befektetés és kockázat mellett.

Konklúzió

Álláspontom szerint egyértelműen megállapítható a kapcsolódás a szervezett bűnözés–terrorizmus–illegális migráció hármasában. Az ellenük való fellépés azért nehéz, mert tevékenységüket konspiratív módon végzik, valamint nem tartják őket vissza határok, nemzeti/nemzetközi szabályok.

A sikeres fellépés kulcsa a titkosszolgálatok, bűnüldöző szervek számára az együttműködés, az információmegosztás.

Az Európai Unió a szervezett bűnözést és a terrorizmust – főként 2001 szeptembere után – mindig is olyan jelenségként értékelte és kezelte, amely súlyosan veszélyezteti a demokratikus rendszereket. A terrorizmus és a bűncselekmények egyéb formái az unió minden egyes polgárát fenyegetik. A terrorcselekmények nemcsak az adott országot érintik, amelyben elkövetik őket, hanem az Európai Unió egészét, hiszen azok az unió alapjául szolgáló értékeket támadják. Bár a szervezett bűnözést és a terrorizmust már régóta az európai biztonságot fenyegető legfontosabb veszélynek tekintik[16], az unió fe-

16 Például a 2003. december 12-i európai biztonsági stratégiában.

lelőssége kiterjed az általában vett bűnözés megakadályozására, illetve az ellene való küzdelem fejlesztésére is. Az Európai Uniót létrehozó szerződés 29. cikke egyértelmű küldetésként határozza meg az unió számára, hogy a tagállamok rendőri szerveinek, vámhatóságainak és egyéb, hatáskörrel felruházott hatóságainak szorosabb együttműködése által, a szervezett vagy egyéb bűnözés, így különösen a terrorizmus, az emberkereskedelem és a gyermekek sérelmére elkövetett bűncselekmények, a tiltott kábítószer-kereskedelem és a tiltott fegyverkereskedelem, a korrupció és a csalás megelőzésével és az ezek elleni küzdelemmel gondoskodjon a polgárok magas szintű biztonságáról.

E feladat elvégzésére született az Európai Unió 2005-ben elfogadott terrorizmusellenes stratégiája.[17] 2015 májusában a tanács és az Európai Parlament új szabályokat fogadott el a pénzmosás és a terrorizmus finanszírozásának megakadályozása érdekében. Az Európai Bizottság 2016 júliusában a hatályos szabályok módosítására vonatkozó javaslatot tett közzé a terrorizmus finanszírozása elleni küzdelem további erősítése érdekében. A tanács 2016. április 21-én irányelvet fogadott el az utasnyilvántartási adatállományban (PNR) lévő adatok felhasználásának uniós szintű harmonizálása céljából. Az irányelv értelmében az utasnyilvántartási adatok kizárólag a terrorista és a súlyos bűncselekmények megelőzése, felderítése, nyomozása és a vádeljárás lefolytatása érdekében használhatók fel.

Az Európai Unió stratégiai kötelezettségvállalása, hogy a terrorizmus elleni globális küzdelem az emberi jogok egyidejű tiszteletben tartásával valósuljon meg, Európa biztonságosabbá tételével lehetővé váljon, hogy polgárai a szabadságon, a biztonságon és a jog érvényesülésén alapuló térségben éljenek. A program célja a határokon átnyúló bűncselekmények hatékonyabb felderítése, a biztonsági követelmények és az alapvető jogok védelmének összehangolása, valamint a migráció kezelése.

A programnak megfelelőbb egyensúlyt kell teremtenie a polgárok biztonsága (például a külső határok védelme, a határokon átnyúló bűnüldözés) és az egyéni jogaik védelme között.

A biztonságos Európa legitim célkitűzés, és a bizottság egyetért azzal, hogy fontos folyamatosan fejleszteni és erősíteni az EU közös politikáit a terrorizmus elleni harc, a szervezett bűnözés, az illegális bevándorlás, az emberkereskedelem és a szexuális kizsákmányolás területén is.

Az előbbiekből megállapítható, hogy az Európai Unió a terrorizmussal és a szervezett bűnözéssel kapcsolatos problémakört mindig kiemelt kérdésként

17 http://register.consilium.europa.eu/doc/srv?f=ST+14469+2005+REV+4&l=hu

kezelte és kezeli jelenleg is, ennek bizonyítékai a korábban említett programok célkitűzései is.

Reményem szerint ennek meglesz a megfelelő hatása, és az biztonságosabbá teszi az Európai Unió állampolgárainak mindennapjait.

DOI: 10.38146/BSZ.2018.2.6

NAGYNÉ DR. TAKÁCS VERONIKA

Információbiztonsági kockázatmenedzsment a Nemzeti Infokommunikációs Szolgáltató Zrt. szemszögéből

A közigazgatás fejlesztésének évszázados története során a témával foglalkozók számos alkalommal fordultak az üzleti világban bevált megközelítésmódhoz, módszerekhez, technikákhoz. A közigazgatási munkaszervezés és a teljesítményértékelés során – megfelelő transzformációval – sor került a mennyiségi (ügyintézési határidőre, meghatározott idő alatt elintézett/elintézendő ügyek számára stb. vonatkozó), majd a minőségi (az ügyfél elégedettségét célként megfogalmazó) elvárások átvételére, érvényesítésére.

A technikai, majd az informatikai, infokommunikációs eszközök[1] alkalmazása a közigazgatási tevékenység tervezése, szervezése, irányítása során újabb szempont – az adatok, információk, valamint az azt kezelő eszközök védelmének – egyre hangsúlyosabb figyelembevételét tette szükségessé. Az információvédelem követelménye nemcsak belső (szervezeten belüli), hanem a jogalkotó által megfogalmazott külső követelményként is megjelent.

A jogalkotói elvárás természetesen nem öncélú, hanem a nemzetközi tendenciákra adott válasz. Ismét egy, az üzleti világból vett példa: az Allianz Global Corporate & Specialty a vállalati kockázatokat évente kiadott felmérésében elemzi. A negyven ország több mint nyolcszáz kockázatkezelőjének és biztosítási szakértőjének bevonásával a 2016-os évről összeállított dokumentum szerint *„a kiberbiztonsági események […] bekerültek a három vezető kockázatnem közé”*[2]. Az elemzés a kiberbiztonsági események körébe sorolja a kiberbűncselekményeket, az adatokat érintő támadásokat és a számítástechnikai meghibásodásokat.[3]

Az, hogy a közigazgatási szervezetrendszer által kezelt és feldolgozott adatok – az állampolgárok, a közigazgatási szervek és a gazdasági szereplők számára is – értéket képviselnek, szakmai és jogi szempontból is elismert és

1 Jelen tanulmány a témában tapasztalható fogalmi következetlenségek tisztázására nem vállalkozik, a továbbiakban az infokommunikációs eszközök kifejezést használja.
2 Allianz Kockázati Barométer 2016. Allianz.hu, 2016. január 28., 3. o. https://www.allianz.hu/hu/sajtoszoba/kockazati-barometer-2016.html/
3 Uo. 4. o.

sokszor hivatkozott tény. Elegendő utalni a nemzeti adatvagyon körébe tartozó állami nyilvántartások fokozottabb védelméről szóló 2010. évi CLVII. törvény adatvagyon-fogalmára, vagy a későbbiekben hivatkozott szabványok vagyontárgyfogalmára. A jogszabály szerint *„nemzeti adatvagyon: a közfeladatot ellátó szervek által kezelt közérdekű adatok, személyes adatok és közérdekből nyilvános adatok összessége”*[4]. A szabványok alapján *„vagyontárgy […] bármi, ami a szervezet számára érték”*[5]*;* elsődleges vagyontárgy a működési folyamatok és tevékenységek, valamint az információ (a kezelt adatok és dokumentumok, továbbá a működéshez szükséges adatok és dokumentumok), másodlagos vagyontárgy a hardver, szoftver, hálózat, személyzet, elhelyezkedés, szervezeti struktúra.[6]

Ha valamilyen értéktárgyat, vagyonelemet – jelen tanulmány tárgya tekintetében az adatokat és az infokommunikációs rendszereket – védeni szükséges, a védelmet, nem utolsósorban az eredményesség és a költséghatékonyság érdekében, meg kell tervezni. Ebben nyújthat segítséget – figyelemmel az infokommunikációs rendszerek sérülékenységére és az esetükben azonosítható fenyegetésekre – a kockázatfelmérés. A védelem megvalósítása során pedig a már azonosított kockázatok kezelése (is) történik.

Jelen tanulmány először a témával kapcsolatos alapvetéseket tekinti át, ez után az ISO/IEC 27005:2011 (E) szabvány[7] kockázatmenedzselésre vonatkozó ajánlásait ismerteti[8], kitérve a magyar információbiztonsági jogszabályokkal – az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvénnyel (Ibtv.) és az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelettel (technológiai rendelet) – közös pontokra, majd néhány konkrét észrevé-

---

4 A nemzeti adatvagyon körébe tartozó állami nyilvántartások fokozottabb védelméről szóló 2010. évi CLVII. törvény 1. § 1. pont, http://www.njt.hu/cgi_bin/njt_doc.cgi?docid=133022.228523

5 MSZ ISO/IEC 27001:2006, 21. o.

6 ISO/IEC 27005:2011 (E) B függeléke, 33. o.

7 ISO/IEC 27005:2011 (E) Information technology – Security techniques – Information security risk management.

8 Jelen tanulmány szabványismertetéssel foglalkozó fejezetei felhasználják a szerzőnek a 2015 decemberében, a Nemzeti Közszolgálati Egyetem *Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára* című minősített képzése keretein belül készített dolgozatának *(Egy, az Ibtv. hatálya alá tartozó szervezetnél alkalmazásra kerülő [közelebbről meg nem határozott] levelező rendszer kockázatfelmérésének végrehajtása az ISO/IEC 27000-es szabványcsoportban foglaltak alapján, figyelemmel az Ibtv. és technológiai rendelete elvárásaira)* a megállapításait.

telt, javaslatot fogalmaz meg (a hivatkozott jogszabályokra is tekintettel) a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. mint a magyar közigazgatás meghatározó infokommunikációs szolgáltatója szemszögéből.

A tanulmány hangsúlyosan a kockázatfelmérés végrehajtásának előkérdéseivel foglalkozik, a kockázatkezelés tekintetében az elméleti háttér bemutatására szorítkozik, és nem tér ki a gyakorlati megvalósítás kérdéseire. Egyrészt azért, mert amíg a kockázatfelméréssel kapcsolatos szakmai konszenzus nem alakul ki, a nem egységesen felmért és értékelt kockázatok kezeléséről több szervezetet érintő javaslatok megfogalmazása idő előttinek tűnik. Másrészt pedig azért, mert az Ibtv. a védelmi intézkedések vonatkozásában kötelezően végrehajtandó előírásokat rögzít, ami meglehetősen szűkíti a kockázatkezelés „játékterét”; szélsőséges esetben annak eldöntésére, hogy a szervezet az erőforrások hiányában még meg nem valósított védelmi intézkedéseket – a kétévenkénti biztonságiosztály-emelési kötelezettségre is tekintettel – milyen sorrendben tervezi és valósítja meg. A tanulmány szándékosan nem tér ki a technológiai rendeletben foglalt védelmi intézkedések tartalmával, teljesítésével összefüggő kérdésekre sem.[9]

A kockázatról és menedzseléséről általában

„Minden szervezet szembesül olyan külső és belső tényezőkkel, hatásokkal, amelyek bizonytalanná teszik céljai elérését, illetve a célok elérésének időpontját. Ennek a bizonytalanságnak a hatását nevezzük kockázatnak.”[10] A szervezetek menedzselik (felmérik és kezelik) a kockázatokat. A kockázatmenedzsment alkalmazható az egész szervezetre, egyes területeire, különböző szintjeire, speciális funkcióira, projektjeire, tevékenységeire.

Az előbbi mondatok az MSZ ISO 31000:2015 szabvány bevezetőjéből származnak és kellően általánosak ahhoz, hogy segítsék a téma gyors áttekintését és a tanulmány szempontjából legfontosabb gondolatok felidézését.[11]

A kockázatok tehát magukban hordozzák a bizonytalanságot, amit az egyes szervezeteknek a saját jellemzőik (céljaik és körülményeik) alapján va-

9 Utóbbi kérdéskörrel kapcsolatban lásd például Nagyné dr. Takács Veronika: Az Ibtv. és végrehajtási rendeletei alkalmazásával és alkalmazhatóságával összefüggő kérdések. Bolyai Szemle, 2014/4., 76–88. o.

10 MSZ ISO 31000:2015 Kockázatfelmérés és -kezelés. Alap- és irányelvek. 5. o.

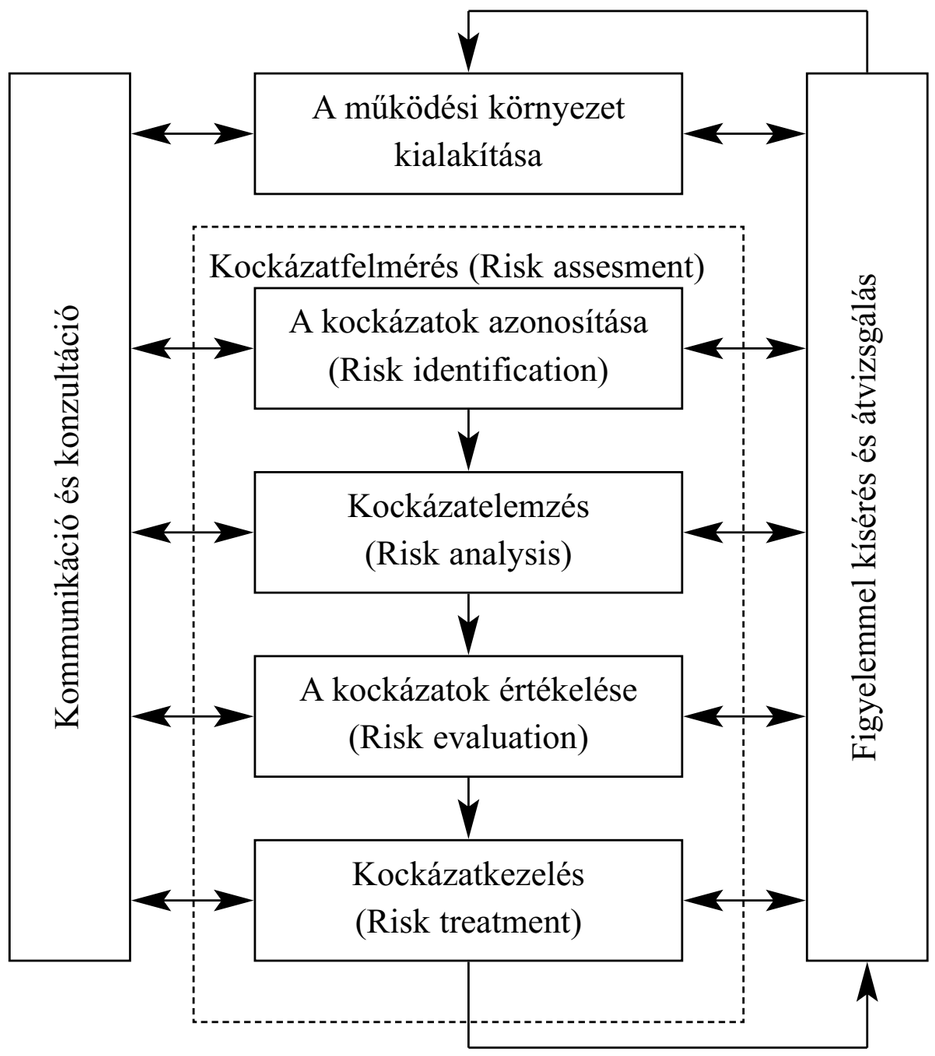
11 A kockázat számos definíciójának értékelésével, a kockázatkutatás elméletével és történetével a tanulmány nem foglalkozik. A tárgyban lásd például Vasvári Tamás: Kockázat, kockázatészlelés, kockázatkezelés – szakirodalmi áttekintés. Pénzügyi Szemle, 2015/1., 29–48. o.

lamiképpen mégis meg kell mérniük, ki kell számítaniuk és ez után kezdeniük kell velük valamit. A kockázatfelmérés az élet számos területén jelentős hagyományokat felmutató tevékenység, olykor külön szakma, kialakult módszertanokkal. Ugyanez igaz a kockázatkezelés elméletére és gyakorlatára is.

A kockázatmenedzsment folyamata – az MSZ ISO 31000:2015 szabvány alapján – az *1. számú ábrá*n látható.

1. számú ábra

A kockázatmenedzsment folyamata az MSZ ISO 31000:2015 szabvány alapján[12]



Az információbiztonsági kockázatmenedzsment a közigazgatásban

Az információbiztonsági kockázatmenedzsment célja – az előbbi definíció értelemszerű szűkítésével – az adott szervezet vagy szervezetek infokommunikációs rendszereinek tervezésével, fejlesztésével, üzemeltetésével és használatával, valamint kivezetésével összefüggő kockázatok felmérése és kezelése.

12 A szerző szerkesztése.

Az információbiztonsági kockázatmenedzsment-rendszer kialakítása, működtetése és folyamatos korrekciója az információbiztonsági irányítási rendszer kiépítésének egyik első lépése; utóbbi elméletével és gyakorlatával a tanulmány (terjedelmi okok miatt) nem foglalkozik.

Az információbiztonsági kockázatmenedzsment-rendszer kiépítése lehet egy szervezet saját döntése alapján megvalósuló tevékenysége; a magyar közigazgatási szervek és a közigazgatás működését támogató egyes nem közigazgatási szervezetek esetében – az Ibtv. óta – ez jogszabályban előírt kötelezettség.

Az Ibtv. a kockázatmenedzsment-folyamat elemeit, tartalmát nem részletezi; a technológiai rendelet a kockázatelemzési módszertan alkalmazását általában írja elő a következők szerint: *„Az elektronikus információs rendszerek biztonsági osztályba sorolását az elektronikus információs rendszerben kezelt adatok és az adott elektronikus információs rendszer funkciói határozzák meg. A besorolást, amelyet az érintett szervezet vezetője hagy jóvá, kockázatelemzés alapján kell elvégezni. A Nemzeti Elektronikus Információbiztonsági Hatóság ajánlásként kockázatelemzési módszertanokat adhat ki. Ha a szervezet saját kockázatelemzési módszertannal nem rendelkezik, az így kiadott ajánlást köteles használni.”*[13]

Jelenleg még nem áll rendelkezésre egységes, központilag kidolgozott kockázatelemzési módszertan, így minden szervezet szembesül a módszertan kiválasztásának, kidolgozásának (testre szabásának) nem könnyű feladatával.

A tanulmány a továbbiakban az ISO/IEC 27000-es szabványcsoport kockázatelemzést tárgyaló elemeit[14] ismerteti. A 27000-es szabványcsoport kiválasztása mellett szóló érv, hogy egyes tagjai magyar szabványokká váltak, így magyar nyelven is hozzáférhetők, következetes alkalmazásuk hozzájárulhat a jelenleg tapasztalható értelmezésbeli különbségek, terminológiai pontatlanságok felszámolásához, továbbá az Ibtv. indokolása is tartalmaz a szabványcsoport alkalmazhatóságára vonatkozó utalást.[15]

A szabvány rövid tartalmi ismertetésének célja nem utolsósorban az, hogy segítséget nyújtson a közös megközelítéshez, kiindulási alapot teremtsen egy

13 1. melléklet a 41/2015. (VII. 15.) BM rendelethez, 1.2. bekezdés. http://njt.hu/cgi_bin/njt_doc.cgi?docid=176725.332228

14 MSZ ISO/IEC 27001:2006 Informatika. Biztonságtechnika. Az információbiztonság irányítási rendszerei. Követelmények, MSZ ISO/IEC 27002:2011 Informatika. Biztonságtechnika. Az információbiztonság irányítási gyakorlatának kézikönyve, ISO/IEC 27005:2011 (E) Information technology – Security techniques – Information security risk management.

15 Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény indokolása. Részletes indokolás a 24. §-hoz.

kockázatfelmérést célzó együttműködés, tárgyalás vagy egy szakértő bevonására irányuló beszerzés előkészítéséhez. Fontos hangsúlyozni, hogy a fejezetben foglaltak nem tekinthetők kockázatelemzési módszertannak – ez a szabványnak sem célja, hiszen mindössze „keretrendszert" kíván nyújtani –, csak segítséget adnak ahhoz, hogy egy módszertan elkészíthető, vagy egy elkészített módszertan „megítélhető" legyen.

A tanulmány az Ibtv. és a technológiai rendelet előírásain túl a következő szabványokban foglaltakat alkalmazza:

– MSZ ISO/IEC 27001:2006 Informatika. Biztonságtechnika. Az információbiztonság irányítási rendszerei. Követelmények.
– MSZ ISO/IEC 27002:2011 Informatika. Biztonságtechnika. Az információbiztonság irányítási gyakorlatának kézikönyve.
– ISO/IEC 27005:2011 (E) Information technology – Security techniques – Information security risk management.

A kockázatmenedzsment lépései az ISO/IEC 27005:2011 (E) szabvány szerint

Az *1. számú ábrá*n bemutatott kockázatmenedzsment-folyamatot részletezi és értelmezi a címben szereplő szabvány. A folyamat lépéseit és az egyes lépésekkel kapcsolatban megfontolandó legfontosabb kérdéseket a fejezet vázlatosan ismerteti a következők szerint.

1. A működési környezet kialakítása

Meg kell határozni a kockázatmenedzsment-folyamat

– külső/belső összefüggéseit és célját; ezekből következően
– hatókörét és határait;
– alapvető értékelési kritériumait és alkalmazott módszereit/megközelítést (kockázatértékelési, hatásértékelési, kockázatelfogadási kritériumok);
– felelősét és folyamatát.

A kockázatértékelési kritériumok meghatározásánál figyelembe veendő:

– a szakmai folyamatok stratégiai értéke;
– az érintett információ-vagyontárgyak kritikussága;
– a jogi, szabályozási és szerződéses kötelezettségek;

– a bizalmasság, sértetlenség, rendelkezésre állás működési és szakmai jelentősége;
– az érintettek elvárásai, véleménye;
– a szervezet presztízse, jó hírnév elvesztésének következményei.

2. A kockázatfelmérés

Választani kell a kétféle megközelítés közül:

– a magas szintű kockázatfelmérés a tevékenységek fontosságát és időrendjét veszi alapul, és mivel különböző (például pénzügyi) okokból nem lehet minden intézkedést (kontrollt) egyszerre megvalósítani, csak a legkritikusabb fenyegetésekre koncentrál;
– a részletes kockázatfelmérés mélységi értékelés, ami jelentős idő- és erőforrás-ráfordítást, szakértői tudást igényel, és amelynek során minőségi és mennyiségi jellemzők is használhatók (az előbbire példa a mérsékelt, jelentős kifejezések használata, az utóbbira például a pénzügyi mutatók).

A szabvány fontos megjegyzése, hogy idő előtti a kockázatfelmérés, ha az intézkedések bevezetését csak egy-két éven belül tervezik.

3. A kockázatazonosítás (öt azonosítási folyamatot tartalmaz)

a) Vagyontárgyak azonosítása

A szabvány – ajánlásként, azaz nem kötelező jelleggel – a következő vagyontárgyak azonosítását javasolja (vagyontárgy minden, ami a szervezet számára értéket képvisel):

– elsődleges: működési folyamatok és tevékenységek; információk (kezelt, illetve a működéshez szükséges adatok és dokumentumok);
– másodlagos: hardver; szoftver; hálózat; személyzet; elhelyezkedés; szervezeti struktúra.

b) Fenyegetések és forrásaik azonosítása

A fenyegetésekkel kapcsolatos információk beszerezhetők a vagyontárgyak tulajdonosaitól, a felhasználóktól, biztonsági, információvédelmi szakemberektől, bármilyen más forrásból (például különböző módszertanokból). A korábbi biztonsági incidensek tapasztalatai az egyes fenyegetések relevanciájának megítéléséhez nyújthatnak segítséget. Mindazonáltal ügyelni kell arra, hogy a fenyegetések folyamatosan módosulnak, különösen, ha a külső környezet vagy maga az infokommunikációs eszköz, rendszer változik.

A fenyegetések (a szabvány példálózó jelleggel több mint negyvenet nevesít)[16] eredetük szerint lehetnek az emberi tevékenységtől függetlenek (környezetiek, K) vagy az emberi tevékenységgel összefüggők, ezen belül véletlenek (V) vagy szándékosak (Sz). Az *1. számú táblázat* a szabvány által felsoroltakból néhány jellemzőbbet idéz.

1. számú táblázat

Példák a fenyegetésekre az ISO/IEC 27005:2011 (E) szabvány szerint

Típus	Fenyegetés	Eredet
Fizikai kár	Tűz	K, V, Sz
Fizikai kár	Berendezés megsemmisülése	K, V, Sz
Természeti jelenség	Földrengés	K
Információ kompromittálódása	Lehallgatás	Sz
Műszaki hiba	Berendezés rosszul működése	V
Nem engedélyezett tevékenység	Jogosulatlan adatfeldolgozás	Sz
Működés veszélyeztetése	Jogosultság nem engedélyezett átengedése	Sz

c) A létező és tervezett védelmi intézkedések (kontrollok) azonosítása

A létező vagy a tervezett kontrollok figyelembevétele munka- és költségmegtakarítást eredményezhet (például a nem indokolt intézkedések bevezetésének elkerülésével). A már létező kontrollok azonosításakor meg kell győződni arról, hogy azok valóban jól működnek, ellenkező esetben újabb sérülékenységet okozhatnak.

A szabvány által elvárt tevékenység végrehajtásához az MSZ ISO/IEC 27002:2011 szabványban felsoroltak adhatnának támpontot. Az információbiztonsági kockázatmenedzsment-rendszer kiépítéséhez a 27002:2011 szabvány 11 fejezetben 39 fő biztonsági kategóriában 132 kötelezően teljesítendő intézkedést sorol fel, az egyes intézkedésekhez bevezetési útmutatót és egyéb információt fűz. Megjegyzendő, hogy a technológiai rendelet 4. mellékletében szereplő Védelmi intézkedés katalógusban három fő csoportban (adminisztratív, fizikai és logikai védelmi intézkedések), 21 témakörben, 186 intézkedés szerepel (egyes intézkedések további alábontásokat tartalmaznak). A két kontrolljegyzék csak részben feleltethető meg egymásnak. Figyelemmel arra, hogy a jogszabály az Ibtv. hatálya alá tartozó szervek esetében kötelező, egyértelmű, hogy a technológiai rendelet katalógusában foglaltakat teljesíteni szükséges.

16 ISO/IEC 27005:2011 (E) C függeléke, 42. o.

d) A sérülékenységek azonosítása

A sérülékenység önmagában nem okoz kárt, utóbbinak feltétele, hogy a fenyegetés a sérülékenységet kihasználja. Az a sérülékenység, amelyhez nem azonosítható fenyegetés, nem igényel kontrollt (védelmi intézkedést), azonban folyamatosan figyelemmel kell kísérni, mivel e tekintetben bármikor bekövetkezhet változás. Figyelemmel kell lenni arra is, hogy egy nem megfelelően megvalósított kontroll (védelmi intézkedés) maga is sérülékenységet okozhat.

Az előzőkből következik, hogy amennyiben egy fenyegetéssel összefüggésben nem azonosítható sérülékenység, a fenyegetés nem jelenthet kockázatot. A szabvány a különböző vagyontárgyakhoz – példálózó jelleggel – több mint nyolcvan fenyegetést, illetve sérülékenységet sorol fel. A *2. számú táblázat* vagyontárgyanként egyet-egyet idéz.[17]

2. számú táblázat

Példák sérülékenységre és fenyegetésre az ISO/IEC 27005:2011 (E) szabvány szerint

Vagyontárgy típusa	Példa sérülékenységre	Példa fenyegetésre
hardver	nem védett tároló	berendezés ellopása
szoftver	tesztelés elmaradása	jogosultsággal visszaélés
hálózat	nem védett kommunikációs csatorna	lehallgatás
személyzet	biztonságtudatosság hiánya	felhasználói hiba/hibás működés
elhelyezkedés	árvízveszélyes területen elhelyezés	árvíz
szervezet	nincs vagy nem megfelelő az SLA[18]	szolgáltatáskiesés

e) A következmények azonosítása

A vagyontárgyak bizalmassága, sértetlensége és rendelkezésre állása elvesztésének következményeit kell meghatározni. Ezek lehetnek

– eredményesség csökkenése;
– kedvezőtlen működési feltételek;
– szakmai tevékenységgel összefüggő negatív hatás;
– jó hírnév elvesztése;
– kár.

A következményeket a technológiai rendelet is részletezi (ez a második, a jogalkotó által részletesebben kifejtett terület; lásd később).

17 ISO/IEC 27005:2011 (E) D függeléke, 45–48. o.

18 SLA: Service Level Agreement (szolgáltatásiszint-megállapodás; az ügyfél és a szolgáltató megállapodása a nyújtandó szolgáltatás lényeges minőségi elemeiről).

4. A kockázatelemzés (két felmérési és egy definíciós folyamatot tartalmaz)

A kockázatelemzés – a vagyontárgyak jelentőségétől, az ismert sérülékenységek és a szervezetnél korábban bekövetkezett biztonsági incidensek menynyiségétől, terjedelmétől függően – különböző részletezettséggel, mélységben valósulhat meg. A kockázatelemzés lehet minőségi vagy mennyiségi vagy a kettő kombinációja. A minőségi elemzés a lehetséges következmények nagyságának és bekövetkezési valószínűségüknek a meghatározásához skálát használ (javasolt a háromfokozatú: alacsony–közepes–magas). Előnye a könnyen érthetőség, hátránya a szubjektív skálázás.

A mennyiségi elemzés számszerűsített értékeket tartalmazó skálát alkalmaz a következmények és a bekövetkezési valószínűségek vonatkozásában, az elemzés minősége a rendelkezésre álló adatok pontosságától és teljességétől függ; előnyei és hátrányai ebből a tényből fakadnak.

a) A következmények felmérése

Az előző lépésekben végrehajtott azonosítások után a szakmai, szervezeti tevékenységet érintő következmények (hatások) meghatározására kerül sor, figyelemmel a vagyontárgyak bizalmassága, sértetlensége és rendelkezésre állása elvesztésének következményeire.

A vagyontárgyak és a bekövetkezhető hatások értékelése a folyamat legérzékenyebb szakasza, mivel különböző jellegű vagyontárgyak és különböző jellegű következmények összevetésén alapuló, egyedi értékelést tartalmaz. Az értékelés lehet minőségi vagy mennyiségi (ha az érték pénzben kifejezhető).

Az érték meghatározásának alapja lehet

– a vagyontárgy beszerzésének/előállításának költsége, helyettesítésének vagy újbóli beszerzésének/előállításának költsége vagy nem materiális érték (például szervezet elismertsége);
– a bizalmasság, sértetlenség, rendelkezésre állás biztonsági esemény miatti sérüléséből, elveszéséből eredő költségek (helyreállítási költségek, működésre, működési környezetre ható következmények).

Az azonosított vagyontárgyak értékét és a bekövetkezhető hatást a következő értékelési kritériumok szerint célszerű meghatározni:

– belső működés megszakadása;
– a szervezet által nyújtott szolgáltatás megszakadása;
– külső fél működésének megszakadása;
– társadalmi, kormányzati válság;
– jogszabályok megsértése;

– belső rendelkezések megsértése;
– szerződésszegés;
– jogi (büntető-) eljárások a szervezettel szemben;
– ügyfelek, partnerek, társadalom bizalomvesztése;
– ügyfelek, partnerek személyes adataival, személyiségi jogaival összefüggő sérelem;
– alkalmazottak vagy ügyfelek, partnerek személyi sérülésének lehetősége;
– pénzügyi, anyagi veszteségek;
– ügyfelek, partnerek veszteségei.

Az értékelési kritériumok rögzítése mellett fokozatokat is meg kell határozni (jellemzően három–tíz fokozatú skálát célszerű használni, ügyelve arra, hogy a túlzott differenciálás nehézségeket okozhat). A szabvány ötfokozatú (0–4) skálát ajánl.
Ugyancsak figyelemmel kell lenni a vagyontárgyak közötti függőségekre (például az adatok sértetlenségére vonatkozó kritérium vonatkozik az azokat kezelő rendszerelemekre is az adatok teljes életciklusa alatt, a rendszerelemek [hardver, szoftver] sértetlensége függ a környezeti biztonsági feltételek – áramellátás, légkondicionálás – teljesülésétől). Az egymástól függő vagyontárgyak esetében a magasabb értéket kell figyelembe venni.
Egyes vagyontárgyakból a szervezet több példányt (másolatot, tartalékot) is őrizhet, az értékelésnél figyelembe kell venni, hogy ezek a vagyontárgyak könnyen helyettesíthetők.
A vagyontárgyakat érhető hatások felmérése során figyelemmel kell lenni arra, hogy egy biztonsági esemény hatásának mértéke nem minden esetben azonos az érintett vagyontárgy értékével, emiatt a két fogalmat meg kell különböztetni.
A hatás lehet azonnali (működési) és jövőbeli (stratégiai). Az azonnali hatás lehet közvetlen (például helyreállítási költségek) vagy közvetett (például jogszabályok, egyéb szabályozó eszközök előírásainak megsértése).
A hatások felmérésének eredménye ugyanazon vagyontárgy esetében a későbbiekben változhat a beépített kontrollok következtében. A szabvány a hatások értékelésére ötfokozatú (0–4: nagyon alacsony–alacsony–közepes–magas–nagyon magas) skálát ajánl.
A technológiai rendelet 1. melléklete – iránymutatásként – az érték és a hatás kategóriáját összevonva a rendszer biztonsági osztályba sorolásához ad szempontokat. A szabvány nemcsak a bekövetkezhető hatások kiválasztását (azonosítását), hanem azok „skálázását” is a szervezetre bízza, így a

szabvány javaslatai alapján a technológiai rendeletből megismert „fokozatok” előzetesen nem azonosíthatók. A *3. számú táblázat* a két „segédlet” felfogásbeli különbségét is mutatja (kiemelve a mindkettőben egyértelműen azonosítható, javasolt szempontokat).

b) A bekövetkezési valószínűség felmérése

A szabvány szerint meg kell határozni a biztonsági esemény (incidens-szcenárió) bekövetkezésének valószínűségét. A felmérés történhet minősé-

3. számú táblázat

Lehetséges következmények a technológiai rendelet és az ISO/IEC 27005:2011 (E) szabvány szerint

Biztonsági osztály	Bekövetkezhető káresemény nagysága	Technológiai rendelet 1. melléklet	ISO/IEC 27005:2011 szabvány B függeléke
1.	jelentéktelen	– rendszer nem kezel jogszabály által védett adatot; – nincs bizalomvesztés, a probléma szervezeten belül marad és megoldható; – közvetlen és közvetett kár a szervezet költségvetéséhez képest kicsi.	– ügyfelek, partnerek személyes adataival, személyiségi jogaival összefüggő sérelem; – belső működés megszakadása; – ügyfelek, partnerek, társadalom bizalomvesztése; – pénzügyi, anyagi veszteségek.
2.	csekély	– személyes adat sérülhet; – működési szempontból csekély értékű adat vagy rendszer sérülhet; – társadalmi-politikai hatás a szervezeten belül kezelhető; – közvetlen és közvetett kár eléri a szervezet költségvetésének egy százalékát.	lásd 1. biztonsági osztálynál
3.	közepes	– különleges személyes adat sérülhet, személyes adatok nagy mennyiségben sérülhetnek; – működési szempontból érzékeny adat vagy rendszer sérülhet; – egyéb, jogszabállyal védett adat sérülhet; – bizalomvesztés a szervezeten belül vagy szervezeti szabályokban foglalt kötelezettségek sérülhetnek; – közvetlen és közvetett kár eléri a szervezet költségvetésének öt százalékát.	lásd 1. biztonsági osztálynál, valamint: – belső rendelkezések megsértése.

Biztonsági osztály	Bekövetkezhető káresemény nagysága	Technológiai rendelet 1. melléklet	ISO/IEC 27005:2011 szabvány B függeléke
4.	nagy	– különleges személyes adat nagy mennyiségben sérülhet; – személyi sérülések esélye megnőhet; – működési szempontból nagy értékű adat(tömeg), üzleti titok vagy rendszer (jelentősen) sérülhet; – jogszabályok betartása elmaradhat; – bizalomvesztés a szervezeten belül, a vezetésben felelősségre vonást kell alkalmazni; – közvetlen és közvetett kár eléri a szervezet költségvetésének tíz százalékát.	lásd 1. biztonsági osztálynál, valamint: – jogszabályok megsértése.
5.	kiemelkedően nagy	– különleges személyes adat kiemelten nagy mennyiségben sérülhet; – emberi életek kerülnek közvetlen veszélybe, személyi sérülések nagy számban következhetnek be; – a nemzeti adatvagyon helyreállíthatatlanul megsérülhet; – az ország, a társadalom működőképességének fenntartását biztosító létfontosságú rendszer rendelkezésre állása nem biztosított; – súlyos bizalomvesztés a szervezettel szemben, alapvető emberi vagy a társadalom működése szempontjából kiemelt jogok sérülhetnek; – működési szempontból nagy értékű üzleti titok, kiemelten érzékeny adat(tömeg) vagy rendszer (jelentősen) sérülhet; – közvetlen és közvetett kár eléri a szervezet költségvetésének tizenöt százalékát.	lásd 1. biztonsági osztálynál, valamint: – társadalmi, kormányzati válság.

gi vagy mennyiségi elemzéssel. A cél annak megállapítása, hogy egy biztonsági esemény (egy sérülékenység fenyegetés általi kihasználása) milyen gyakran, illetve milyen könnyen következhet be (lásd *4. számú táblázat*).

4. számú táblázat

Lehetséges bekövetkezési valószínűségek az ISO/IEC 27005:2011 (E) szabvány szerint

Fenyegetés bekövetkezési valószínűsége	Alacsony (A)			Közepes (K)			Magas (M)		
Sérülékenység szintje	A	K	M	A	K	M	A	K	M
Incidens bekövetkezési valószínűsége	0	1	2	1	2	3	2	3	4

A felmérés során figyelemmel kell lenni a következőkre:

– a különböző fenyegetések bekövetkezési gyakoriságára vonatkozó statisztikák;
– az egyes fenyegetések forrásainak – folyamatosan változó – jellemzői (képességek, egyes sérülékenységek kihasználását érintő tapasztalatok, trendek);
– a sérülékenységek jellemzői egyenként és összegezve;
– a létező kontrollok hatékonysága.

c) A kockázati szint meghatározása

A kockázatelemzés – minőségi vagy mennyiségi – értéket rendel a kockázat bekövetkezési valószínűségéhez és következményéhez. A becsült kockázat egy biztonsági esemény (incidensszcenárió) bekövetkezési valószínűségének és következményeinek kombinációja *(5. számú táblázat)*.

5. számú táblázat

Lehetséges kockázati szintek az ISO/IEC 27005:2011 (E) szabvány szerint

		Incidens bekövetkezési valószínűsége				
		0	1	2	3	4
Vagyon-	0	0	1	2	3	4
tárgy	1	1	2	3	4	5
vagy	2	2	3	4	5	6
hatás	3	3	4	5	6	7
értéke	4	4	5	6	7	8

Alacsony kockázat: 0–2 Közepes kockázat: 3–5
Magas kockázat: 6–8.

5. A kockázatértékelés

A becsült kockázatokat a kockázatértékelési (kockázatelfogadási) kritériumok alapján rangsorolni kell, ez szolgál majd a kockázatkezelési intézkedésekre vonatkozó döntések alapjául.

A kockázatértékelés során azon fenyegetések rangsorolása történik meg, amelyek esetében

– a sérülékenység és fenyegetés együtt azonosítható; és
– nincs még intézkedés.

A kockázatértékelés során a döntések sok esetben az elfogadható kockázati szintre alapoznak, de az alacsony vagy közepes kockázatok felhalmozódása jelentősebb, beavatkozást igénylő helyzetet is kialakíthat.

6. A kockázatkezelés

Idetartoznak mindazon tevékenységek, amelyek a kockázatok csökkentését célozzák, a következők szerint:

– a megfelelő kontrollok alkalmazása (kockázat forrásának megszüntetése, a bekövetkezési valószínűség vagy a hatás csökkentése stb.);
– a kockázatok tudatos és tárgyilagos elfogadása, vállalása;
– a kockázatok elkerülése (nem kezdik el vagy nem folytatják a kockázathoz vezető tevékenységet);
– a kockázatok áthárítása, megosztása további partnerrel, partnerekkel (beleértve a szerződéskötést és a kockázatfinanszírozást).

A kockázatkezelés következtében új kockázatok keletkezhetnek vagy a korábbi kockázatértékelés eredménye változhat.

A kockázatkelés során a különböző kockázatkezelési formák nem zárják ki egymást, kombinálhatók, egy kockázatkezelési forma több kockázatra is vissza tud hatni.

A szervezet vezetői általi döntés elősegítése érdekében

– össze kell állítani a kockázatkezelési tervet, amely tartalmazza, hogyan mérték fel a kockázatokat és hogyan vetették azokat össze a kockázatelfogadási kritériumokkal;
– rögzíteni kell a maradványkockázatokat.

A szervezet vezetői általi döntés eredménye az elfogadott kockázatok listája, erre (is) tekintettel a döntést dokumentálni kell.

7. Kommunikáció és konzultáció

A kommunikáció során a kockázatfelmérés és -kezelés eredményeit meg kell osztani a döntéshozókkal és az egyéb érintettekkel, a további teendők hatékony és eredményes végrehajtása és a teendők megindokolása, elfogadtatása érdekében. Ügyelni kell arra, hogy a kommunikáció kétirányú legyen, formájában igazodjon a szervezeti kultúrához és vegye figyelembe az intézkedések sürgősségét.

8. Figyelemmel kísérés és átvizsgálás

A kockázatok nem statikusak, emiatt folyamatosan figyelemmel kell kísérni

– a kockázatokat és tényezőiket (vagyontárgyak értéke, hatások, fenyegetések, sérülékenységek, bekövetkezési valószínűségek) a változások felfedése érdekében;
– a kockázatmenedzsment folyamatát a szükséges módosítások meghatározása érdekében.

A NISZ Zrt. szolgáltatói szerepe és információbiztonsági feladatai

A NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. – jogszabályi kijelölés alapján – a magyar közigazgatás meghatározó szolgáltatója[19], jogelődeivel együtt fél évszázados múltra tekint vissza.

Elődei az 1964-ben alapított Konjunktúra- és Piackutató Intézet (Kopint) és az 1968-ban létrehozott Datorg Külkereskedelmi Adatfeldolgozó és Szervező Rt., amelyek összevonásával 1987-ben jött létre a Kopint-Datorg Konjunktúra-, Piackutató és Informatikai Intézet. 2005 júliusától a vállalat egyedüli tulajdonosa a magyar állam lett, azóta zártkörű részvénytársaságként működik. 2007 óta fő tevékenysége teljes körű infokommunikációs szolgáltatások nyújtása az állami és a közigazgatási szervek számára. 2008-ban a tu-

19 A kormányzati célú hálózatokról szóló 346/2010. (XII. 28.) kormányrendelet; a központosított informatikai és elektronikus hírközlési szolgáltatásokról szóló 309/2011. (XII. 23.) kormányrendelet; egyes, az elektronikus ügyintézéshez kapcsolódó szervezetek kijelöléséről szóló 84/2012. (IV. 21.) kormányrendelet; a központosított informatikai és elektronikus hírközlési szolgáltatásokat egyedi szolgáltatási megállapodás útján igénybe vevő szervezetekről, az elektronikus ügyintézés részletszabályairól szóló 451/2016. (XII. 19.) kormányrendelet, valamint a központi szolgáltató által üzemeltetett vagy fejlesztett informatikai rendszerekről szóló 7/2013. (II. 26.) NFM rendelet.

lajdonosi jogokat a Magyar Nemzeti Vagyonkezelő Zrt. vette át, a társaság neve 2011-től NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. Legnagyobb megrendelői a közigazgatási szervek, de gazdálkodó szervezetek, vállalkozások és magánszemélyek is igénybe veszik egyes szolgáltatásait.[20]

A NISZ Zrt., mint központosított informatikai és elektronikus hírközlési szolgáltató, az Ibtv. és végrehajtási rendeletei hatálya alá tartozó szervezet, ezen túlmenően – jelentőségére tekintettel – a jogalkotó önálló jogszabályban[21] további információbiztonsági feladatokat határozott meg számára. A külön jogszabályban meghatározott feladatok között szerepel az információbiztonsági irányítási rendszer kialakítása, az infokommunikációs tevékenységgel kapcsolatos nyilvántartások vezetése (szolgáltatások, azok végfelhasználói, üzemeltetői, fejlesztői, hozzáférési jogosultságaik, a szolgáltatások biztosításához szükséges vagyonelemek, igénybe vett külső szolgáltatások stb.), külön hangsúlyt kap az azonosítási és hozzáférés-kezelési tevékenység, a szolgáltatások biztonsági állapotának folyamatos ellenőrzése és a biztonsági események kezelése, valamint a folyamatos kockázatkezelés.

Észrevételek és javaslatok

Az előzőekben felsorolt feladatokat a NISZ Zrt. értelemszerűen csak a szolgáltatásait igénybe vevő szervekkel (ellátotti kör) együttműködve tudja végrehajtani, és ugyanez a helyzet az ellátotti kör szemszögéből is. A feladat- és felelősségmegosztás szükségességét az Ibtv. rögzíti[22], ugyanakkor a feladatelhatárolásra, illetve a közösen végrehajtandó feladatok, tevékenységek azonosítására nem született iránymutatás, a kérdést az érintett feleknek kell rendezniük.

A feladatok közös ellátásának igénye (és célszerűsége) mellett a – fogalmi, tartalmi – egységesség követelményének érvényesítéséről is szükséges lenne dönteni.

Jelenleg sem a jogszabályi környezet, sem a szakirodalom, sem az ezzel foglalkozó szakértői kör nem tud teljes körű és könnyen adaptálható kockázatfelmérési módszertant ajánlani a közigazgatás számára. A megfelelő módszertan kiválasztása és alkalmazása tehát nem könnyű feladat, különösen

20 http://www.nisz.hu/hu/rolunk

21 A központosított informatikai és elektronikus hírközlési szolgáltató információbiztonsággal kapcsolatos feladatköréről szóló 186/2015. (VII. 13.) kormányrendelet.

22 Ibtv.11. § (1)–(3) bekezdés. http://njt.hu/cgi_bin/njt_doc.cgi?docid=160206.339954

azon kisebb – jellemzően önkormányzati – szervek esetében, ahol az informatikai tudással, képesítéssel felvértezett munkatársak létszáma nagyon alacsony; olykor mindössze egy munkatárs lát el ilyen jellegű feladatokat.

A megfelelő létszám hiánya mellett nehézséget jelenthet a feladat az egyes szervezetek ezzel a kérdéssel korábban nem foglalkozó, munkaidejükben jellemzően másfajta tevékenységet végző alkalmazottai számára is, hiszen a főleg külföldi szakirodalom feldolgozása után, példálózó segédletek áttekintését követően a saját szervezetükre vonatkozó, egyediesített és szakmailag korrekt, ráadásul hatóság által számon kérhető kockázatfelmérést kell végrehajtani.

Felvetődhet a feladat végrehajtásának kiszervezése külső vállalkozó számára. Ha egy szervezet így dönt, nem eshet a feladatkipipálás csapdájába; nem szerencsés a feladatot egy külső cég összeollózott sablonok alkalmazásával készített „eredménytermékével" letudni. A kiszervezés hasznos lehet, ha a szervezet „megveszi" a kockázatelemzési tudást, amit a továbbiakban használni is akar és megteremti a saját – szervezetismerettel bíró és így az egyediesítést és az alkalmazható eredményt garantáló – belső erőforrásokat a kockázatfelmérés végrehajtásához.

Mindezzel természetesen – bár egyedi jó megoldások születhetnek – a kockázatfelmérési megközelítés és gyakorlat még nem lesz egységes a közigazgatásban. A különböző módszertanok, ajánlások egyedi kombinációinak létrehozása nem feltétlenül célravezető, ráadásul – a szervezetrendszer egészét tekintve – erőforrás-igényes. Makroszinten – például a közigazgatás vagy csak a központi államigazgatás vagy csak az önkormányzatok szintjén – célszerű lenne egységes (részben testre szabható) módszertant kialakítani és alkalmazni és ehhez megfelelő segédleteket biztosítani.

A megfelelő módszertan kiválasztása mellett a módszertan alkalmazásának megfelelőségére is figyelemmel kell lenni. A kockázatazonosítási folyamatban, a vagyontárgyak azonosításakor, a szervezet által a feladatellátáshoz használt (a NISZ Zrt. esetében: üzemeltetett) elektronikus információs rendszerekről az értékeléshez szükséges minden (leíró) adatnak – naprakészen – rendelkezésre kell állnia, beleértve az adatgazdára vonatkozó konkrét adatokat, hiszen ő tud (köteles) nyilatkozni a kezelt, feldolgozott adatok értékéről, az elektronikus információs rendszer szervezetben betöltött szerepéről, jelentőségéről. Ráadásul ezek az adatok ebben a kontextusban még csak egy szervezetről szólnak; az infokommunikációs szolgáltató szemszögéből az említett adatoknak „szervezet közötti" szinten is következeteseknek, összemérhetőknek kellene lenniük. A NISZ Zrt. által ellátott intézmények száma meghalad-

ja a kétszázötvenet; a társaság nyilvántartásai alapján mintegy ezerötszáz alkalmazásról van szó, amelyek adatgazdai értékelése szervezetenként történt (vagy nem történt) meg; ehhez kell a szolgáltatások tartalmát és a jogszabályok által előírt információvédelmi intézkedéseket meghatározni úgy, hogy például csak a levelezőrendszerre vonatkozó értékelések a 3. és az 5. biztonsági osztály kategóriái között szóródnak.

A kockázatfelméréshez is szükséges kötelező vagy ajánlott leltárak és nyilvántartások összeállításának, tartalommal feltöltésének eltérő módszertana mellett a szervezeti kultúrák sokféleségéből adódó további különbözőségeket is figyelembe kell venni, gondoljunk például a szabályozási vagy szerződés-előkészítési hagyományok, szokások, eljárásrendek eltéréseire. Ha már a szervezeten belüli – belső – szabályozási rendszerek eltérő felfogásban kezelik a feladatok és a felelősségek meghatározásának, megfogalmazásának kérdéseit, hogyan lehet ezt az ellátotti kör tekintetében a szolgáltató részéről egységessé tenni úgy, hogy az mindkét oldal (és az egyik oldal sok szereplőjének) megelégedésére szolgáljon? Megoldásként felvetődhet a 309/2011. kormányrendelet alapján a 1469/2011. (XII. 23.) kormányhatározattal létrehozott Informatikai Felhasználói Munkacsoport[23] keretein belüli egyeztetések lehetősége is.

A szervezetek közötti egyeztetéseknek természetesen akkor lehet eredményük, ha a kockázatfelméréssel megbízott vagy megbízandó munkatársak a szervezeteken belül megfelelő képzést, felkészítést kapnak a feladatok elvégzéséhez. E feltétel teljesíthetőségének vizsgálatakor ismét felvetődik a szervezetenkénti önálló végrehajtás és azt követő konszolidáció vagy az előre, „központilag” elkészített módszertan és ütemterv szerinti haladás lehetőségei közötti választás. A NISZ Zrt. jelenleg a saját és az ellátotti körbe tartozó, együttműködő intézmények adatszolgáltatásaiból származó információk feldolgozása, konszolidálása alapján végzi a jogszabályok által előírt információbiztonsági feladatokat, a már említett feladat- és felelősségmegosztás megvalósításához még sok a tennivaló.

JOGSZABÁLYOK

A nemzeti adatvagyon körébe tartozó állami nyilvántartások fokozottabb védelméről szóló 2010. évi CLVII. törvény.

23 A 309/2011. (XII. 23.) kormányrendelet 5. § (1) bekezdése szerint a munkacsoport *„a központi szolgáltatási megállapodásban foglalt követelmények meghatározását és ellenőrzését”* végzi, koordinációs és konzultációs fórumként is működik, működhet.
http://njt.hu/cgi_bin/njt_doc.cgi?docid=140272.342120

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény.

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről szóló 41/2015. (VII. 15.) BM rendelet.

A központosított informatikai és elektronikus hírközlési szolgáltató információbiztonsággal kapcsolatos feladatköréről szóló 186/2015. (VII. 13.) kormányrendelet.

A kormányzati célú hálózatokról szóló 346/2010. (XII. 28.) kormányrendelet.

A központosított informatikai és elektronikus hírközlési szolgáltatásokról szóló 309/2011. (XII. 23.) kormányrendelet.

Egyes, az elektronikus ügyintézéshez kapcsolódó szervezetek kijelöléséről szóló 84/2012. (IV. 21.) kormányrendelet.

A központosított informatikai és elektronikus hírközlési szolgáltatásokat egyedi szolgáltatási megállapodás útján igénybe vevő szervezetekről, az elektronikus ügyintézés részletszabályairól szóló 451/2016. (XII. 19.) kormányrendelet.

A központi szolgáltató által üzemeltetett vagy fejlesztett informatikai rendszerekről szóló 7/2013. (II. 26.) NFM rendelet.

1469/2011. (XII. 23.) kormányhatározat az Informatikai Felhasználói Munkacsoport létrehozásáról.

DOI: 10.38146/BSZ.2018.2.7

KASZNÁR ATTILA

A kibervédelem fontossága a terrorelhárítás jelenlegi és jövőbeni rendszerében

A kiberfenyegetettség mind nagyobb próbatétel a nemzetbiztonsági és a terrorelhárítási szolgálatok számára, mivel az információs technológia fejlődése által kínált lehetőségeket a terrorszervezetek egyre gyakrabban használják fel képességeik bővítésére és javítására.[1] Mindamellett, bár mind több és több a jele az újfajta veszélynek, látni kell, hogy a védekezés terén – sem a társadalmi, az egyéni és a vállalati szegmensben, sem a rendvédelmi és nemzetbiztonsági szektorban – még mindig nincs meg az a fajta elvárható tudatosság, amely szükségesnek mutatkozhat. *„Mindenekelőtt két olyan állítás fogalmazható meg, amelyben mindenki egyetért, aki így vagy úgy kiberbiztonsággal foglalkozik. Az egyik, hogy a kiberbiztonság, illetve a kiberfenyegetettség a következő évtizedek egyik legfőbb biztonsági kihívását jelenti. A másik, hogy a kiberbiztonság megvalósítására irányuló erőfeszítések jelenleg elég fragmentáltak, azaz a különböző szereplők hatékony együttműködése még hagy maga után kívánnivalót.”*[2]

Biztató pontként említhető, hogy a hazánkban jelenleg is érvényben lévő Nemzeti biztonsági stratégia külön is kiemeli a kiberbiztonság szerepét: *„Az állam és a társadalom működése – a gazdaság, a közigazgatás, vagy a védelmi szféra mellett számos más területen is – mind meghatározóbb módon a számítástechnikára épül. Egyre sürgetőbb és összetettebb kihívásokkal kell számolnunk az informatikai- és telekommunikációs hálózatok, valamint a kapcsolódó kritikus infrastruktúra fizikai és virtuális terében. Fokozott veszélyt jelent, hogy a tudományos és technológiai fejlődés szinte mindenki számára elérhetővé vált eredményeit egyes államok, vagy nem-állami – akár terrorista – csoportok arra használhatják, hogy megzavarják az információs és kommunikációs rendszerek, kormányzati gerinchálózatok rendeltetésszerű működését.”*[3] A jogszabályban foglaltak bizakodásra adnak okot, amikor jel-

1 Gianluca Riglietti: Defining the threat: what cyber terrorism means today and what it could mean tomorrow. The Business and Management Review, vol. 8, no. 3, 2016, p. 12.

2 Hankiss Ágnes: Kiberbiztonság: az Európai Parlament feladatai. Magyar Rendészet, különszám, 2013, 27. o.

3 Magyarország Nemzeti Biztonság Stratégiája, 31. bek. http://2010-2014.kormany.hu/download/f/49/70000/1035_2012_korm_hatarozat.pdf

zik, hogy a legfelsőbb politikai döntéshozó szinten felismerték a problémát, a mindennapok tapasztalatai azonban azt mutatják, hogy a társadalom kiterjedt felületén mutatkoznak veszélyhelyzetet előidéző hiányosságok.

Az a speciális – a hagyományos társadalmi közegnél jóval nehezebben feltárható, illetve ellenőrizhető – fenyegetettségi környezet, amelyet a kibertér bővülése és használatának mindennapossá válása hozott, korábban sosem látott nehézségeket idézett elő a terrorelhárítás feladatrendszerében. A kiberterrorizmus ugyanis szerves része az aszimmetrikus hadviselésnek, amely *„a hibrid hadszínterek hibrid fenyegetései által a hibrid műveletek és az ellenük való védekezés lehetősége (kontrahibrid műveletek), a jelenlegi kor egyik fő kihívása”*[4]. E kihívások pedig új válaszmechanizmusok kidolgozását teszik szükségessé, mivel a korábbi biztonsági környezetre tervezett reakciók az új dimenziókban nem vagy nem elég hatékonyan alkalmazhatók, márpedig olyan *„időkben, mint amilyen a miénk, mikor nemcsak vízszintesen, hanem függőlegesen is történik minden, az ember helyesen cselekszik, ha megtanul a frontkatona óvatosságával élni”*[5], és minden figyelmét az új veszélyek leküzdésére fordítja.

Jelen tanulmány nem kíván komplex válaszokat adni a kiberterror elleni védekezés kérdéseiben, hanem elsősorban felderítési szempontból kívánja felhívni a figyelmet arra, milyen összetett strukturális nehézségekkel kell szembenézni a kibertérből érkező terrorfenyegetettségek elhárításakor, amelyek tulajdonképpen a terrorizmus és a kibertér konvergenciájának tekinthetők[6], e meghatározást több szakértő is elfogadottnak tartja.[7]

Az elsődleges feladatot a preventív fellépésben, vagyis a felderítőmunkában szükségszerűen bekövetkezett változások adják. A terrorelhárításhoz kötődő – de ugyanígy igaz a megállapítás minden nemzetbiztonsági felderítőmunkára is – felderítés lehetőségei számos aspektust alapul véve rendkívül kiterjedtek a kibertér adta lehetőségek hatására, mindamellett talán ennél hangsúlyosabban jelentkeznek az új típusú közeg jelentette nehézségek, mivel *„a hagyományos tevékenységeket megkönnyítő szerepén túl, az internet komoly biztonsági kockázatokat is magában rejt”*[8].

---

4 Resperger István: Az aszimmetrikus hadviselésre adható válaszok. Honvédségi Szemle, 2017/1., 24. o.

5 Márai Sándor: Füves könyv. Helikon Kiadó, Budapest, 2005, 99. o.

6 Gabriel Weimann: Cyberterrorism – How Real Is the Threat? Special Report, no. 119, United States Institute of Peace, 2004. https://www.usip.org/sites/default/files/sr119.pdf

7 Dorothy E. Denning: Cyberterrorism. 24 August, 2000, p. 1. http://palmer.wellesley.edu/~ivolic/pdf/Classes/Handouts/NumberTheoryHandouts/Cyberterror-Denning.pdf

8 Szijártó Lívia: Az internethasználat biztonságetikai kérdései. A virtuális lét rejtett veszélyforrásai. Nemzetbiztonsági Szemle, 2016/1., 46. o.

A felderítés újonnan jelentkező nehézségeit azok a kiterjedt lehetőségek (anonimitás, közösségi, illetve kapcsolattartó szolgáltatások, sötét web stb.) okozzák, amelyek nyomán a szolgálatok információszerző lehetőségei eddig nem tapasztalt nehézségekbe ütközhetnek.

A terrorizmus ugyanis nem statikus jelenség, hanem komplex rendszer, amelynek egyes momentumai a fejlődés irányába mutató evolúciós folyamatok összetevőinek tekinthetők, a *„fejlődése során végig követhető a módszerek, eszközök és elkövetők változása”*[9]. A kijelentés úgy is értelmezhető, hogy *„a terrorizmus nem ér véget az erőszakos tettel, ez csak a kezdete”*[10], a folyamat ugyanis folytatódik, mint azt a társadalmi funkcionális folyamatmodellek híven leírják, interakciók következtében megtörténik visszajelzés, és az inputok hatására újabb folyamatok generálódnak. Ezek természetesen mindig változó tényezőkből állnak össze, és a környezetük, valamint az az által gyakorolt hatás is minden esetben más, azonban közös bennük, hogy mindegyik a rendszer – a terrorizmus – része. Egy ilyen fejlődési lépcsőnek, a rendszer egy folyamatának tekinthető maga a kiberterrorizmus is.

Az előbbiek tekintetében elmondható, hogy a sikeres elhárítómunka is minden esetben dinamikus tevékenység kell hogy legyen, amely ennek jellegzetességei okán egyértelmű, hogy számos ponton, jelen esetben a kiberterrorizmus jelentette új, szokatlan feladatok miatt nehézségekbe ütközik. A nehézségek jellegzetessége azonban, hogy azok minden esetben ideiglenesek, mivel az új típusú feladat (input) generálta válaszok, azaz megoldások (output) részben vagy egészben feloldják a problémát; természetesen nem hagyható figyelmen kívül, hogy az output a visszajelzés folytán inputként fog jelentkezni, vagyis ismételt elhárítási nehézséget okoz, ez azonban maga a már leírt jellegzetesség.

A kiberterrorizmust minden esetben a terrorizmus rendszerének egyik folyamataként kell értelmeznünk, ezáltal pedig figyelembe kell vennünk, hogy az általa támasztott kérdésekre adott válaszok milyen új inputokat generálhatnak, és ezek maximális optimalizálására, illetve kezelhetőségére kell törekedni.

Milyen új feladatot teremt a kibertér? A felsorolás számos elemet tartalmazhat, és valószínűsíthető, hogy egyiket sem lehetne teljesnek tekinteni, mert – pontosan annak dinamikus voltánál fogva – újabb és újabb tagokkal

9 Bács Zoltán György: A radikalizáció és a terrorizmus kapcsolata, egyes formái, gondolatok a megelőzés lehetséges perspektíváiról. Nemzetbiztonsági Szemle, 2017/1., 5. o.

10 Marie-Helen Maras: A terrorizmus elmélete és gyakorlata. Antall József Tudásközpont, Budapest, 2016, 240. o.

lenne kiegészíthető, ezért e tanulmány szubjektíven emel ki néhányat a legfontosabbnak ítélt tényezők közül.

Globális lehetőségek

A terrorizmusra általános értelemben is igaz, hogy *„minden más bűncselekménytől különbözik abban, hogy egyfelől ideológiai-politikai motivációt követ, másfelől globális, azaz természeténél fogva átnyúlik földrészeken és országhatárokon”*[11]. A kibertér már a létezésével megteremti annak a lehetőségét, hogy a terrorizmus említett sajátosságait érvényesíteni tudja. Mára bátran kijelenthető, hogy az internet alapjaiban változtatta meg a terrorizmus lehetőségeit, a módszerek széles kínálatát nyújtva, miközben új nehézségek elé állította az terrorelhárításban részt vevő szolgálatokat. Ennek egyik legjellemzőbb példája a radikalizáció terén lelhető fel. *„Az internet átvitt értelemben úgy tekinthető, mint az elektronikus világ fő út- és vasúthálózata, amely rendkívül hatékony »szállítást« tesz lehetővé, és nagyon messzire és szétszórtan élő személyeket is elér, valamint befolyásolni képes azok közösségi és egyéni világnézetét.”*[12] A világháló globális elterjedésével párhuzamosan vált igazzá, hogy *„a radikalizációs folyamat fontos elemévé lépett elő az internet”*[13], amely meggyorsította és határok nélkülivé tette a szélsőséges eszmék terjesztését.

A radikalizálni kívánók szempontjából

A radikális tanoknak az azokra esetlegesen fogékony személyekhez történő eljuttatásának az internet korszakában gyakorlatilag csak nyelvi akadálya lehet, egyébként könnyebben, gyorsabban, konspiráltabban, és a szolgálatok hagyományos felderítő tevékenysége elől jóval védettebben van rá lehetőség. A különböző, gyakran védett internetes felületek a kapcsolattartás (sok terrorista használ a kommunikációja során titkosítást, amely megnehezíti az ellenük való fellépést[14]), a tiltott kereskedelem és más illegális tevékenységek so-

11 Hankiss Ágnes: Vékony jégen. Arc és Álarc, 2017/1., 85. o.
12 Alfred Rolington: Hírszerzés a 21. században. A mozaikmódszer. Antall József Tudásközpont, Budapest, 2015, 100. o.
13 Zalai Noémi: A XX. század háborúi és a terrorizmus elleni harc jellemzőinek összehasonlítása katonai, politikai és társadalmi kontextusok alapján. Szakmai Szemle, 2008/2., 49. o.
14 Dorothy E. Denning: i. m. 3. o.

rát teszik lehetővé úgy, hogy jellegzetességeik, valamint nagy mennyiségük következtében is számos problémát okozhat a szűrésük.[15]

A radikalizálódásra alkalmas személyek szempontjából

A szélsőséges nézetekre és cselekményekre fogékonyságot mutató, legtöbbször valamilyen társadalmi vagy szociális zsákutcából kiutat kereső személyek lehetősége a téves, később végzetesnek bizonyuló „válaszok" elérésére nemcsak nagyobb, mint a világhálón kívüli életben, de mivel legtöbbször rendkívüli frusztráltság jeleit mutatják, ezért a vélt vagy valós anonimitás miatt, biztosabbnak is tűnhet számukra ez a megoldás. Vagyis aktívabban kereshetik az internetes felületeken a segítséget, emiatt tulajdonképpen tálcán kínálják önmagukat a szélsőséges ideológusoknak, vagy a már radikalizálódott személyeknek. Az elmúlt időszak európai terrorcselekményeit végrehajtó személyek pszichológiai hátterének elemzése is megerősíteni látszik az iménti feltevést, mivel az elkövetőkre igaznak bizonyult, hogy azok *„számos esetben megpróbálnak kapcsolatot teremteni terrorszervezetekkel, de ami még jellemzőbb, hogy az interneten keresztül radikalizálódott személyekkel vesznek fel kapcsolatot"*[16]. Ezek a személyek, annak ellenére, hogy jogilag elkövetővé válnak, gyakorlatilag maguk is áldozatok, akik sebezhetőségükből kifolyólag *„legfeljebb csak szimbolikus kapcsolatban állnak az akció valódi céljával"*[17].

Információbőség

A kibertér világa bebizonyította, hogy terrorelhárítási szempontból is igaz, hogy *„van annál nagyobb probléma is, mint kevés információval rendelkezni – mégpedig az, ha túlságosan sok információ vesz körül bennünket"*[18]. Az információs társadalomban generálisan jelentkező probléma az információ-

15 Az említett probléma a jelzettnél is súlyosabb gondokat okozhat a web sötét oldala esetében. Az általa okozott nehézségekre jelen tanulmány külön nem tér ki.

16 Farkas Johanna: A magányos merénylők radikalizálódása. Acta Humana, 2016/5., 23. o.

17 Boda József: Biztonsági kihívások – nemzetbiztonsági válaszok. In: Gaál Gyula – Hautzinger Zoltán (szerk.): Tanulmányok a „Biztonsági kockázatok – rendészeti válaszok" című tudományos konferenciáról. Pécs, 2014, 42. o. [Pécsi Határőr Tudományos Közlemények XV.]

18 Jasenszky Nándor: Adatszerzés – Információhasznosulás – Biztonságtudatos vállalati kultúra. In: Szamos Tamás (szerk.): A nyílt információgyűjtés fejlődő területei. Belügyi Tudományos Tanács, Budapest, 2015, 58. o.

többlet, ebből adódóan mára mindinkább háttérbe szorul a humán erőforrás információhordozó képességének fontossága a munkaerő információszintetizáló képességéhez képest. Az előző gondolatból adódóan, ma már a szolgálatok számára sem elsődleges cél a mind több adat és információ felhalmozása, mivel annak korlátlansága gátolhatja az eredményes munkát. Inkább *„az információk szelektálása, szűkítése, gyors értékelése, megfontolt elemzése, mindez pedig szoros határidővel, hiszen a legfőbb szempont a politikai vezetés döntéseinek információs támogatása, alternatívák felállítása”*[19]. Különös fontosságú az információtöbblet kezelése, mivel az

1. lassíthatja a feldolgozás sebességét, ami jelentékeny – akár emberéletekben is mérhető – időveszteséget okozhat;
2. lehetőséget adhat a terroristáknak a zavaró információhalmazban való elrejtőzésre;
3. megfelelő, manipulált kontextusok felállítása mellett, a szolgálatok félrevezetését, megzavarását is lehetővé teheti.

Térinformatika

„A térinformatikai adatok/információk és eszközök alkalmazása igen nagy előnyökkel jár a terrorelhárító tevékenységben, ugyanakkor a terroristákat is hasznos információkhoz segítheti a támadások szervezésében. Mind a terroristák, mind a terrorelhárítók számára ugyanazok az általános pozitívumok: a megnövekedett információmennyiség[20] *és a jó minőségű térinformatikai részletek.”*[21] Az általános vélekedés szerint a térinformatika a modern társadalom egyik kiemelkedő hatású technikai vívmányának tekinthető, azonban, mint az a jelenlegi biztonságpolitika egyik legnagyobb tekintélyű nemzetközi szakértőjének soraiból is levezethető, a kép ennél jóval árnyaltabb, és a pozitív hozadékok mellett az alkalmazása során megjelennek a társadalom egészének rendszerét (gazdaság, politika, kultúra stb.), valamint az egyén személyét is érintő fenyegetések.

19 Laufer Balázs: Az új kihívások hatása a nemzetbiztonságra – a nemzetbiztonsági szolgálatok megváltozott szerepe napjainkban. Felderítő Szemle, 2010/3–4., 56. o.

20 Ebben az esetben azonban szükséges visszautalni a túlzott mennyiségű információval összefüggésben kifejtett gondolatokra, ami természetesen a terroristák számára is jelentkezhet negatívumként.

21 Marie-Helen Maras: i. m. 498. o.

Internetes média

Külön problémakörbe tartoznak az internetes médiában terjedő, az általános megítélésben propagandaanyagokként értelmezett terroristavideók, amelyek tartalma azonban ennél sokkal bonyolultabb. Az utóbbi időben elsősorban az Iszlám Állam által, profin készített és terjesztett, brutális kivégzéseket, valamint kínzásokat bemutató videók ugyanis túlmutatnak a propagandán, és hatásmechanizmusuk – sokkoló, félelmet keltő tartalmuk – alapján a terrortevékenység egy új fajtájának tekinthetők. Az új típusú támadások megfelelnek azon kitételnek, *hogy „a globalizált és interdependenssé váló mediatizált külpolitikai közegben a terrorista akciók szimbolikus értékű agresszióként aposztrofálhatók, a támadások egész társadalmak, kultúrák és politikai berendezkedések számára hordoznak üzenetet, az erőszakos cselekmények félelemkeltésre irányuló hatásfoka a korábbi trendekhez képest sokszorosára nőtt”*[22]. Az említett digitális tartalmak elleni fellépés elsődleges fontosságú lehet a jövő terrorelhárító tevékenységében.

Az internet mint a terrortámadás eszköze és helyszíne

Mind több jele mutatkozik annak, hogy a világháló maga is egyben terroristaeszközzé, illetve terroristacélponttá válik. Indokolt a jelen idő használata, mivel a kibertámadások mára a mindennapok részévé váltak, de valószínűsíthető az is, hogy a jelenlegi tudásszint mellett a szakértők számára sem felfogható az a méretű állam, társadalom, továbbá egyén elleni támadási potenciál és felület, amelyet a jövő információs társadalma hordoz majd magában. Az informatikai fejlődésben a következő áttörést a mesterséges intelligencia felhasználása jelentheti, ez várhatóan alapjaiban alakítja át az emberiség életét, és félő, hogy sosem látott lehetőségeket kínál majd a terroristáknak is, miközben minden korábbinál nehezebb feladat elé állítja a felderítő és elhárító szolgálatokat.

Összegzés

A kibertérrel kapcsolatos, illetve *„az információs technológia terrorista csoportok, vagy egyének általi saját célok elősegítése érdekében való felhaszná-*

22 Király Zoé Adrienn: A terrorizmus médiainterpretációja és a terrorista szervezetek médiahasználatának változása a digitális korban. Politikatudományi Tanulmányok, 2016/1., 12. o.

lása”[23] témájában végzett kutatások alapján mind fontosabbnak tekinthető a strukturális és technológiai újítások alkalmazása annak érdekében, hogy sikerrel lehessen felvenni a küzdelmet a terrorizmus újszerű biztonsági kockázataival. Fontos annak a kérdésnek a megválaszolása, hogy a *„jelenlegi kibervédelmi szervezetek alkalmasak-e a kiberhadviselés kezelésére, ha nem, akkor pedig milyen szervezetfejlesztés szükséges e feladatok ellátásához?”*[24]

Talán az egyik legmeghatározóbb feladatként jelentkezhet a kiberalapú felderítési potenciál további növelése, amelynek során *„alapvetően azon kommunikációs csatornák és formák ellenőrzése lehet meghatározó, amelyet a társadalom békés tagjai között meghúzódó terroristák is használhatnak (így pl. a mobiltelefonok, valamint az internet-alapú szolgáltatások)”*[25]. Az információszerző mechanizmusok megfelelő irányú fejlesztése azonban csak abban az esetben lehet eredményes, ha ezzel párhuzamosan megtörténik a hozzá tartozó értékelőkapacitás fejlesztése is.

Mind több jele mutatkozik, hogy a kibertér védelme az egyik leglényegesebb momentum. Az információtechnológia fejlődése és terjedése merően újszerű eszközöket teremtett a szélsőséges ideológiákat megjelenítő személyek és csoportok – különösen a terrorista csoportok – számára, és ezek alapjaiban változtatják meg a globális biztonsági környezetet. Az internet, valamint annak speciális alkalmazásai (különösen a közösségi felületek) révén a radikalizációs folyamatok a korábbiaknál gyorsabban, szélesebb körben és jóval kevésbé ellenőrizhetőn mehetnek végbe. A közösségi oldalak és egyéb kapcsolattartó alkalmazások elterjedésével a szélsőséges eszmék közvetítésében gyakorlatilag mindössze a nyelvi különbségek jelentkezhetnek nehézségként. Elsősorban az Iszlám Állam utóbbi időben kifejtett tevékenysége bizonyosságát adta, hogy az internet egyben kiemelkedő propagandafelületet is teremt a különböző terrorista csoportoknak, ezek professzionális kihasználására pedig egyre nagyobb erőfeszítéseket tesznek. Kiemelt probléma lehet az egyes terrorszervezetek kibertámadásokra irányuló törekvése is, ezekkel olyan anyagi és eszmei károkat okozhatnak, amelyek korábban nem vagy csak kevéssé ismert hatású demoralizáló és sokkoló hatást válthatnak ki a közvéleményben.

---

23 Mitko Bogdanoski – Drage Petreski: Cyber terrorism – global security threat. International Scientific Defence, Security And Peace Journal, July 2013, p. 59.

24 Boda József – Boldizsár Gábor – Kovács László – Orosz Zoltán – Padányi József – Resperger István – Szenes Zoltán: A hadtudományi kutatási irányok, prioritások és témakörök. Állománytudományi Műhelytanulmányok, 2016/16., 18. o.

25 Dobák Imre: Technikai típusú információgyűjtés a változó biztonsági kihívások tükrében. Hadmérnök, 2017/2., 243. o.

„Nem különösebben homályos, se nem igazán új az a gondolat hogy mind a technikai fejlődés, mind a társadalmi változás megváltoztatja a stratégiai környezetet is – és így az eszközöket is, amelyekkel a háborúkat vívják.”[26] A globális terrorban bekövetkezett alapvető, stratégiai változások megkövetelik a gyökeres szemléletváltoztatást a terrorelhárítás területén is, hiszen a rendvédelmi szerveknek *„évtizedes hagyományok alakították ki a szervezeti kultúra- és értékrendszerüket”*[27]. Az új típusú fenyegetést jelentő terrorszervezetek nemcsak jól finanszírozottak, hanem a modern technikai megoldások implementálására is fogékonyak.[28] A modern, kibereszközöket is felhasználó terrorizmus, és annak mélyre nyúló társadalmi beágyazottsága, olyan flexibilis szociológiai állapotot teremtett, illetve a mesterséges intelligencia a jövőben olyan változásokat idéz elő, amelynek következtében elengedhetetlen, hogy a nemzetbiztonsági és terrorelhárító szolgálatok a korábbi, statikus alapokon építkező tevékenységüket a korábbiaknál eredményesebb, a napi változásokat aktívabban követő metódusok alapján végezzék. Sosem szabad figyelmen kívül hagyni, hogy a terroristák is tisztában vannak az alapszabállyal, az ellenséget *„Ott támadd meg, ahol készületlen! Ott ronts rá, ahol nem is számít rá.”*[29]

26 Roland Dannreuther: Nemzetközi biztonság. Antall József Tudásközpont, Budapest, 2016, 297. o.
27 Zalai Noémi: Új típusú kihívások: generációváltás a nemzetbiztonsági szolgálatoknál. Nemzetbiztonsági Szemle, 2016/1., 35. o.
28 Sarah Gordon – Richard Ford: Cyberterrorism? Symantec.com, 2003, p. 9. https://www.symantec.com/avcenter/reference/cyberterrorism.pdf
29 Szun-Ce: A háború művészete. Cartaphilus Kiadó, Budapest, 2006, 12. o.

DOI: 10.38146/BSZ.2018.2.8

DORNFELD LÁSZLÓ

A kibertérben elkövetett bűncselekményekkel összefüggésben alkalmazható kényszerintézkedések*

A büntetőeljárás során, annak sikere érdekében az eljáró hatóság egyik kiemelkedően fontos eszköze a kényszerintézkedések alkalmazása. Ezek céljuk szerint többféleképpen csoportosíthatók, azonban témánk szempontjából a releváns szempont, hogy míg bizonyos kényszerintézkedések a terhelt, illetve más személy jelenlétét, addig mások a bizonyítékok beszerzését, illetve megőrzését, valamint a büntetőjogi szankció végrehajtását hivatottak szolgálni.[1] Elektronikus környezetben, kiberbűncselekményekkel összefüggésben elsősorban utóbbi két kategóriának van speciális jelentősége, hiszen az idetartozó kényszerintézkedések végrehajtása speciális szaktudást igényel.

A kényszerintézkedések minden esetben valamilyen alapjogot korlátoznak, ezért meg kell felelniük a szükségesség–arányosság Alkotmánybíróság által kidolgozott kritériumainak. Ez különösen fontos kérdés az informatikai bűncselekményeknél folytatott nyomozás esetén, hiszen a modern infokommunikációs eszközökön számos személyes adat található, amelyek alapján a felhasználó élete teljes egészében feltárható.[2]

Tanulmányom megírásának egyik apropóját az új büntetőeljárási törvény elfogadása adta[3], amely számos változást hozott a kényszerintézkedések rendszerében is, nem csak a digitális világ kihívásainak való megfelelés terén.[4] Elsősorban a magyar szabályozást kívánom vizsgálni, összehasonlítva a hatályos és az új törvény különbségeit az elektronikus tér szemszögéből, valamint e különbségek lehetséges hatásaival is foglalkozom. Emellett a hazai és külföldi szakirodalom által felvetett kérdéseket, javaslatokat is áttekintem.

* Köszönettel tartozom témavezetőmnek, prof. dr. Róth Erikának.

1 Király Tibor: Büntetőeljárási jog. Osiris Kiadó, Budapest, 2003, 401. o.

2 Berecz Péter: A Német Szövetségi Alkotmánybíróság „számítógép-határozata”. Studia Juvenum, 2009/1., 71–72. o.

3 2017. évi XC. törvény

4 Ezekkel kapcsolatban bővebben lásd Róth Erika: A kényszerintézkedések változó rendszere és részletszabályai. Ügyészek Lapja, 2016/3–4., 39–50. o.

Az elektronikus bizonyítékgyűjtés

Az elektronikus bizonyíték fogalma

A kiberbűncselekményekkel kapcsolatban alkalmazható kényszerintézkedések jobb megértéséhez fontos megvizsgálni azt, hogy milyen specifikus problémák vetődnek fel az elektronikus bizonyítékok beszerzése során. E körülmények ismerete ugyanis elengedhetetlen a téma megfelelő áttekintéséhez.

Elsőként magának az elektronikus bizonyítéknak a fogalmát szükséges megmagyarázni. Az egyik leggyakoribb meghatározás szerint ideértendő minden olyan bizonyító erővel bíró adat, amelyet digitális formában tárolnak, feldolgoznak vagy továbbítanak.[5] *Casey* egy sokkal általánosabb megfogalmazással él, szerinte az elektronikus bizonyíték minden olyan bizonyító erővel bíró adat vagy információ, amelyet számítógép segítségével tárolnak vagy továbbítanak.[6] A fogalom meghatározása azonban – a kiberbűnözéshez köthető legtöbb fogalomhoz hasonlóan – igen bizonytalan, és a lehetőségek gyors fejlődése miatt nem is alkotható olyan definíció, amely minden aspektust magában foglal.[7]

Bizonytalanság mutatkozik például annak kérdésében, hogy a digitális- és elektronikusbizonyíték-fogalmak azonos értelműek-e.[8] Napjainkban ez egyértelműen megvalósul, hiszen a felhasználók kivétel nélkül digitális számítógépeket és egyéb infokommunikációs eszközöket (például okostelefon, tablet) használnak. Azonban korántsem biztos, hogy ez a tendencia a jövőben is folytatódik, és ez a fajta szűkítés a technológiasemlegesség kritériumának sem felel meg. Így véleményem szerint helyesebb az elektronikus bizonyíték kifejezést használni. Fontos szempont még az is, hogy az adathordozók körét nem lehet kizárólag a számítógépre redukálni, hiszen ma már számos egyéb eszköz is tartalmazhat releváns információkat.

A jogi szabályozásra áttérve, az elektronikus bizonyíték fogalmát használja több cikkében is az Európa Tanács számítástechnikai bűnözésről szóló egyezménye[9], azonban a fogalom meghatározásával adós marad. Hasonlóan a

5 Antonela Gropeneanu – Adrian Iacob: Investigative issues regarding cybercrime. European Journal of Public Order and National Security, no. 2, 2016, p. 10.

6 Eoghan Casey: Foundations of Digital Forensics. In: Eoghan Casey (ed.): Digital Evidence and Computer Crime. Academic Press, 2011, p. 7.

7 Ez magára a szabályozásra is igaz, amely így hamar anakronisztikussá válhat, ha túlságosan is technikai részletekbe bocsátkozik. Lásd Szádeczky Tamás: Az IT biztonság szabályozásának konfliktusa. Infokommunikáció és Jog, 2013/3., 149. o.

8 Sorbán Kinga: A digitális bizonyíték a büntetőeljárásban. Belügyi Szemle, 2016/11., 81. o.

9 Az Európa Tanács 2001. november 23-án, Budapesten kelt számítástechnikai bűnözésről szóló egyezménye (ETS No. 185). Kihirdette a 2004. évi LXXIX. törvény.

hatályos büntetőeljárásról szóló 1998. évi XIX. törvény (a továbbiakban: Be.) rendelkezései között is hiába keresnénk az erre vonatkozó szabályozást, és a bizonyítási eszközök között sem kerül sor a feltüntetésére. Kétféle elmélet alakult ki azt illetően, hogy mi tekinthető az elektronikus bizonyíték forrásának. Az egyik szerint azok a tárgyi bizonyítási eszközök, amelyek az adatokat hordozzák, képesek megjeleníteni, tárolni, továbbítani azt (például CD, DVD, számítógép stb.).[10] A másik, elsősorban angolszász területen elterjedt elmélet az elektronikus adatot tekinti a forrásnak.[11] Ez jelenti egyrészt a hardverelemeket irányító adatokat (például operációs rendszer, programok stb.), illetve a felhasználói adatokat (például képek, szöveges dokumentumok stb.), amelyek a felhasználó tevékenysége nyomán jönnek létre. *Peszleg Tibor* megközelítésében az adathordozó valóban szükséges az adatok rögzítéséhez, de ahogy egy nyomtatásban elkövetett bűncselekménynél, akként a digitális térben sem a rögzítő közeg, hanem a rögzített adat a lényeges a bizonyítás szempontjából.[12]

Jelentős változást hozott a büntetőeljárásról szóló 2017. évi XC. törvény (a továbbiakban: új Be.), amelynek 165. §-a már egyértelműen a bizonyítási eszközök közé sorolja az elektronikus adatot, és a 205. §-ban meg is határozza azt. Az új Be. szerint ideértendő *„a tények, információk vagy fogalmak minden olyan formában való megjelenése, amely információs rendszer általi feldolgozásra alkalmas, ideértve azon programot is, amely valamely funkciónak az információs rendszer által való végrehajtását biztosítja”*. Ez a megfogalmazás lényegét tekintve azonos a büntető törvénykönyvről szóló 2012. évi C. törvény (a továbbiakban: Btk.) 423. § (5) bekezdésében megtalálható meghatározással. Az információs rendszer fogalmát a Btk. 459. § (1) 15. pontja úgy határozza meg, hogy *„az adatok automatikus feldolgozását, kezelését, tárolását, továbbítását biztosító berendezés, vagy az egymással kapcsolatban lévő ilyen berendezések összessége”*.

A paragrafus (2) bekezdése arról rendelkezik, hogy az elektronikus adatot a tárgyi bizonyítási eszközzel azonosan kell kezelni, hacsak a törvény külön nem rendelkezik ettől eltérően. Az előbbiekben taglalt dogmatika szempontjából elmondható, hogy a jogalkotó az angolszász megoldást fogadta el, és a tárgyi bizonyítási eszközzel azonos szabályok alkalmazását mindössze praktikus szempontok vezérelték, mint az a szakaszhoz fűzött indokolásból is kitűnik.

10 Laczi Beáta: A számítógépes környezetben elkövetett bűncselekmények nyomozásának és a nyomozás felügyeletének speciális kérdései. Magyar Jog, 2001/12., 728–729. o.
11 Sorbán Kinga: i. m. 84. o.
12 Peszleg Tibor: A digitális bizonyítási eszközök megszerzésének elvei és gyakorlati érvényesítésük. Ügyészek Lapja, 2010/2., 25–26. o.

Az elektronikus bizonyítékgyűjtés nehézségei

Az elektronikus környezetben elkövetett bűncselekményekre vonatkozó egyedi jellemzők közül a legfontosabb az, hogy a felhasználókat olyan veszélyek fenyegetik a kibertérben, amelyek újak, nehezen megelőzhetők és üldözhetők.[13] Az elkövetőknek sokszor jóval elmélyültebb az informatikai tudásuk, mint a nyomozó hatóság tagjainak, de az ügyészeknek és a bíróknak is, így a gyanúsított félrevezető védekezése sokszor nehezítheti az eljárást.[14] Napjainkban azonban már egyre több az olyan elkövető, akinek nincsenek különleges ismeretei, hanem mások által illegális célokra készített programokat használnak. Az ilyen igények kielégítésére elterjedőben vannak a bűnözést mint szolgáltatást *(Crime-as-a-Service)* kínáló csoportok, amelyek például rosszindulatú programokat készítenek, botneteket hoznak létre és használnak fel szolgáltatásmegtagadással járó támadásokra *(Distributed Denial of Service; DDos)* stb. A kis kockázat mellett magas profitszerzés lehetősége a hagyományos szervezett bűnözés érdeklődését is felkeltette.[15]

A kibertérben elkövetett bűncselekmények ügyében folyó nyomozás elején gyakran semmilyen más bizonyíték nem áll rendelkezésre, csakis az elektronikus adatok, így a kriminalisztika olyan hagyományos eszközei, mint a daktiloszkópia, itt még nem kapnak szerepet.[16] Az elektronikus adatok nagyon könnyen manipulálhatók, elrejthetők vagy megsemmisíthetők, így elengedhetetlen a megfelelő technikák ismerete a bizonyításhoz való biztosításuk érdekében.[17] Peszleg Tibor kiemeli, hogy akárcsak más bizonyítási eszközök beszerzésénél, a digitális térben is fontos a törvényesség és szakszerűség, és a zárt bizonyítási lánc megléte.[18] *Wang* szerint három alapvető kritériumot kell az ilyen nyomozások során betartani: a bizonyíték beszerzésénél ne sérüljön vagy módosuljon az eredeti adat, bizonyítható legyen az egyezés az eredetivel, és a bizonyíték elemzése ne változtassa meg azt.[19] Az adatok bizonyí-

13 Vertes-Oltenau Andreea: Evolution of the Criminal Legal Frameworks for Preventing and Combating Cybercrime. Journal of Eastern-European Criminal Law, no. 1, 2014, p. 85.
14 Parti Katalin: Tiltott pornográf felvétellel visszaélés az interneten – az empirikus kutatás adatai. In: Virág György (szerk.): Kriminológiai Tanulmányok, 44. OKRI, Budapest, 2007, 98. o.
15 Nagy Zoltán, András – Mezei, Kitti: The organised criminal phenomenon on the Internet. Journal of Eastern-European Criminal Law, no. 2, 2016, pp. 137–140.
16 Laczi Beáta: i. m. 726. o.
17 Shiuh-Jeng Wang: Measures of retaining digital evidence to prosecute computer-based cyber-crimes. Computer Standards & Interfaces, no. 2, 2007, p. 216.
18 Peszleg Tibor: i. m. 26. o.
19 Shiuh-Jeng Wang: i. m. 218. o.

tó erejüket csak akkor tartják meg, ha megőrzik a beszerzésüket közvetlenül megelőző állapotukat, és így a vizsgálati eredmény reprodukálható marad.[20]

Házkutatás

A Be. 149. §-a ekként határozza meg a házkutatást: a ház, lakás, egyéb helyiség, az azokhoz tartozó bekerített hely vagy a jármű átkutatása, továbbá az ott elhelyezett információs rendszer vagy ilyen rendszerben tárolt adatokat tartalmazó adathordozó átvizsgálása az eljárás eredményessége érdekében. Az 1998-as Be. hatálybalépése előtt a felsorolás nem tartalmazott elektronikus adatokra vonatkozó kitételt, így vita folyt azzal kapcsolatban, hogy egy rendszer vagy adathordozó átvizsgálása házkutatásnak vagy pedig szemlének tekintendő-e.[21] Már az Európa Tanács R(95) 13. miniszteri bizottsági ajánlásának 6. pontja megfogalmazza azt az igényt, hogy a számítógépek átvizsgálására a házkutatás általános szabályai legyenek alkalmazhatók.

A Be. 152. § (1) bekezdés alapján a lefoglalás érdekében a házkutatás során – más keresett dolgokhoz hasonlóan – az információs rendszer vagy az ilyen rendszerben tárolt adatokat tartalmazó adathordozó birtokosát vagy az adat kezelőjét fel kell szólítani, hogy a tárolt adatot tegye hozzáférhetővé. A kért adatok átadása önmagában nem akadálya annak, hogy a házkutatás folytatódjon. A Be. 149. § (4) bekezdés szintén hasonló rendelkezést tartalmaz, itt azonban már szerepel az a kitétel, hogy a házkutatást be kell fejezni abban az esetben, ha a kért adatot a felszólítás után átadják. Ha más bizonyítási eszköz fellelése is valószínűsíthető, akkor azonban a kényszerintézkedés tovább folytatható.

A házkutatás fontos mozzanat a későbbi nyomozási cselekmények szempontjából, hiszen számos kérdés már ekkor eldönthető. Például vizsgálni kell azt, hogy ha található a házban wifi, akkor megfelelően védett-e jelszóval, ennek hiánya esetén ugyanis fennáll az a lehetőség, hogy valaki más kapcsolódott rá a vezeték nélküli hálózatra, és követte el az adott bűncselekményt.[22] A Nemzeti Nyomozó Irodánál töltött tudományos gyakornoki időm alatt elmondták, hogy ilyenkor gyakorlat az is, hogy az információs rendszerben olyan vizsgálatokat végeznek, amelyekre később már nem biztos, hogy lehetőség adódik. Például ha egy adatot felhőszolgáltatásban tárolnak, és a ház-

20 Tóth Fanni: Az informatikai bűnözéshez kapcsolódó kényszerintézkedések. Büntetőjogi Szemle, 2017/1., 79. o.
21 Laczi Beáta: i. m. 730. o.
22 Vadász Viktor: A számítógép demisztifikálása. Ügyészek Lapja, 2010/2., 30. o.

kutatás során a rendszerből elérhető, érdemes még akkor elvégezni a vizsgálatát, mivel később az internetre csatlakozás már veszélyeztetheti az adathordozón található adatok integritását.

A kiberbűncselekmények szakképzett elkövetői számos módon igyekeznek kijátszani a nyomozó hatóságot. Ezek közül az egyik, ha az illegális adatokat (például gyermekpornográfiát) elkülönített adathordozón vagy rendszerben tárolják, amit gondosan elrejtenek. Napjainkban például a pendrive-ok gyakran egyszerű hétköznapi tárgyaknak látszanak, így problémás lehet ezek mindegyikét felkutatni. További nehézséget okozhat az is, ha az eljárást megelőzően az elkövető a rendszerét vagy annak egy részét titkosítással látja el. A titkosított adatok nem megismerhetők a nyomozó hatóság számára, így a bizonyításban sem használhatók fel. Némelyik titkosítás könnyedén feltörhető a nyomozó hatóság által, míg például a VeraCrypt 256 bites titkosítása a gyakorlatban nem fejthető meg belátható időn belül. Kérdésként vetődik fel tehát, hogy a titkosítást feloldó kulcs átadására kötelezhető-e a terhelt. Bizonyos államokban, így például Franciaországban a btk. 434-15-2. szakasza szerint bűncselekményként értékelendő a jelszó hatóság részére történő átadásának megtagadása, míg például Németországban különleges rendőri egységek bevetésével, rajtaütésszerű házkutatással kívánják ennek elejét venni. Az Egyesült Államokban ezzel szemben az önvádra kötelezés tilalmába ütközőnek tartják az ilyen kötelezést, hiszen ezzel a terhelt tulajdonképpen elismeri, hogy rendelkezik a rendszerben található jogsértő adatok felett.[23] Úgy gondolom, mindkét megoldás mögött fontos érvek állnak: míg az egyik álláspont az állam büntetőigényét, addig a másik a polgárok jogait tartja fontosabbnak. A különbség elsősorban értékrendbeli, így a kérdésben nehéz objektív módon állást foglalni.

Az új Be. 302. §-a immár kutatásként hivatkozik a kényszerintézkedésre, amely az indokolás szerint jobban illeszkedik annak tartalmához, hiszen nemcsak ház, de jármű és információs rendszer is lehet tárgya. A kutatás elrendelésének köre kibővül a hatályos törvényhez képest, így az eddigi esetek mellett akkor is alkalmazható, ha elkobozható, illetve vagyonelkobzás alá eső dolog megtalálására vagy információs rendszer, illetve adathordozó átvizsgálására vezet. Utóbbi abban különbözik a „bizonyítási eszköz megtalálása” esetétől, hogy itt az ezeken az eszközökön tárolt elektronikus adat tekinthető bizonyítási eszköznek, így a kitétel külön történő szerepeltetése indokolt.

23 Susan W. Brenner: Budapesti Law – A United States Perspective. In: Eoghan Casey (ed.): Digital Evidence and Computer Crime. Academic Press, 2011, pp. 115–118.

Lefoglalás

A Be. 151. § (1) alapján a lefoglalás célja a bizonyítási eszköz biztonságba helyezése a bizonyítás érdekében, illetve az elkobzás, vagyonelkobzás alá eső dolgok biztosítása, és ennek érdekében vonja el a rendelkezési jogot a birtokostól. A jogintézménynek nagyon fontos szerepe van a kibertérben elkövetett bűncselekmények üldözésében az elektronikus bizonyítékok megszerzésének és megőrzésének egyik eszközeként.

Kemény viták folynak azzal kapcsolatban, hogy pontosan mit is kell az eljárás során lefoglalni: a teljes információs rendszert, az adathordozót vagy pedig csak magát az adatot. A hatályos Be. 151. § (2) bekezdése mindháromra lehetőséget teremt, ezzel széles mozgásteret kínálva a nyomozó hatóságnak. Az adat lefoglalását a 2013. évi CLXXXVI. törvény 21. §-a illesztette be a törvény szövegébe, 2014. január 1-jei hatállyal. Ezt megelőzően bevett gyakorlat volt a számítógép egészét lefoglalni (sokszor a büntetőeljárás szempontjából lényegtelen hardvereszközökkel, például a monitorral, billentyűzettel együtt), később azonban sokszor már csak a merevlemezt, majd a Be. módosítása után csak magát az adatot foglalták le. *Vadász Viktor* ugyanakkor nem ért egyet ezzel a tendenciával, mivel egyrészt az elkövetés eszköze elkobzás alá esik, másrészt magából a merevlemezből nem nyerhető ki minden információ, amely fontos lehet az eljárás és a bizonyítás folyamán.[24] Ezekkel a megállapításokkal egyetértve elengedhetetlen megjegyezni, hogy az adat lefoglalásának akkor lehet igazán jelentősége, ha azt olyan rendszerre alkalmazzák, amely nem az elkövetés eszköze volt, de valamilyen nyomozási szempontból fontos adatot tartalmazhat (például a bűncselekmény által érintett rendszer), hiszen ebben az esetben túlzott sérelmet okozhatna a használónak a rendszer hosszabb időre történő teljes lefoglalása. A törvény ugyanakkor nem él ezzel a distinkcióval, így ennek kidolgozása a gyakorlatra váró feladat.

Ennek gyakorlati végrehajtására kétféle megoldás létezik: a rendszer helyszíni átvizsgálása után meghatározzák az átmásolandó adatok körét vagy pedig az egész rendszerről készítenek hash kulccsal ellátott másolatot, így garantálva az adatok hitelességét.[25] Előbbi módszer kisebb mennyiségű információ esetén jól alkalmazható, ugyanakkor a bizonyításnál problémát okozhat, mivel az eredmény már nem reprodukálható az eredeti rendszerből.

24 Vadász Viktor: i. m. 20. o.
25 Sorbán Kinga: i. m. 88–89. o.

Adathordozók önmagában történő lefoglalása is problémás lehet, hiszen ha a merevlemezt eltávolítják az egyedi környezetéből, a programok nagy része már nem lesz elindítható, valamint a verziószám, és számos releváns tényező se lesz már megállapítható.[26] Az is elképzelhető, hogy a lefoglalt adathordozó inkompatibilis a vizsgáló rendszerével, és bizonyos eszközöknél (például RAID tömbök) az egység megbontása lehetetlenné teszi az adattartalom visszaállítását.[27] Előfordult, hogy bizonyos adatokat nem közvetlenül az adathordozón, hanem például egy felhőszolgáltatást igénybe véve tárolnak, és ezeket az adott rendszer segítségével lehet a legkönnyebben elérni.

Ez alapján egyértelműen kijelenthető, hogy a nyomozás érdekeit az szolgálja leginkább, ha az egész rendszert foglalja le a nyomozó hatóság, ez ráadásul különösebb informatikai szakértelmet sem igényel. Figyelembe kell azonban venni, hogy egy teljes rendszer lefoglalása súlyos jogsértésekkel, és akár károkkal is járhat. Egyrészt a technológia folyamatos avulása miatti jelentős értékvesztésként valósulhat meg egy elhúzódó eljárás, de akár egy vállalkozás működését is ellehetetlenítheti.[28] Másrészt, adatvédelmi szempontból is aggályos lehet a lefoglalás, főként ha az több személy adatait is tartalmazza. A rendőrségről szóló 1994. évi XXXIV. törvény 90. szakasza előírja, hogy bűnüldözési célra azok a személyes adatok kezelhetők, amelyek tényleges veszély elhárításához, illetve meghatározott bűncselekmény megelőzéséhez, felderítéséhez, bizonyításához szükségesek. Az adatvédelmi biztos 2009-es állásfoglalásában úgy találta, hogy az eljáráshoz nem szükséges adatokhoz való hozzáférés csak észszerű időtartamra korlátozható, és az ügyben felvetődő féléves lefoglalás már túlmutat ezen.[29]

A fő problémát véleményem szerint az jelenti ezzel összefüggésben, hogy az adatokat mindenképp át kell vizsgálni a büntetőjogi szempontból releváns információk (például gyermekpornográfiát ábrázoló felvételek) megtalálása és lefoglalása érdekében. Különösen igaz ez, ha feltehető, hogy az elkövetők valamilyen módszerrel, például szteganográfiával igyekeztek leplezni magukat.[30] Így az eljáró hatóság mindenképp megismeri az információs rendszerben található adatokat, legyenek azok bármennyire érzékenyek. Mint ko-

26 Vadász Viktor: i. m. 30. o.
27 Sorbán Kinga: i. m. 88. o.
28 Uo. 87. o.
29 Trócsányi Sára: Első oldal. Infokommunikáció és Jog, 2009/6., 1. o.
30 A szteganográfia a rejtett üzenetek létrehozásának egy formája, informatikai környezetben úgy valósítható meg, hogy a tiltott tartalmat (például gyermekpornográfia) egy másik, legális tartalom mögé rejtik el. Mohamed Chawki: Online Child Sexual Abuse: The French Response. Journal of Digital Forensics, Security and Law, no. 4, 2009, pp. 11–12.

rábban utaltam már rá, ezek a rendszerek, adathordozók olyan adatokat tartalmazhatnak, amelyek alapján a birtokos teljes élete feltérképezhető. Személyes felvételek, elektronikus számlák és banki kivonatok, orvosi leletek, vallási, politikai meggyőződésre utaló információk, számos egyéb magánjellegű adat található a rendszerekben, és általában a használó kapcsolati köre is feltérképezhető ezek alapján.[31] A németországi szövetségi alkotmánybíróság az információs technika személyiség kibontakoztatására gyakorolt nagy hatása miatt döntött úgy 2008-ban, hogy új alapjogként az információs önrendelkezési jogból levezeti az információs rendszer bizalmasságához és integritásához való jogot.[32] A döntés külön tényezőként emelte ki azt a tényt is, hogy itt akár harmadik, a büntetőeljárásban nem érintett személyek adatai is megismerhetővé válnak.

Jelenleg nincs a világon sehol olyan megoldás, amely ezt a súlyos ellentétet feloldaná, és a tendenciák a lehetséges kár mérséklése irányába mutatnak. Az adatvédelmi biztos 2009-es jelentése kapcsán ismertté vált a kapitánysági rendőrségi gyakorlat is, amely szerint a személyes adatokhoz csak az igazságügyi informatikai szakértő, az ügy előadója és elöljárói férhetnek hozzá, és olyan vizsgálati környezetben dolgoznak, ahonnan kizárják az illetékteleneket.[33] A Nemzeti Nyomozó Iroda gyakorlata alapján a lefoglalt rendszerről teljes másolatot készítenek, és ennek átvizsgálására kerül sor az eljárásban, ami szintén korlátozza az érzékeny adatokhoz hozzáférő személyek körét. Jelenleg úgy tűnik, hogy nem zárható ki teljesen ezen adatok megismerése a büntetőeljárás során, így a legjobb megoldás valóban az azokhoz hozzáférők körének minél erőteljesebb szűkítése.

Az új Be. által hozott változások

Az új Be. számos változást hoz a lefoglalás kapcsán, elsősorban az elektronikus bizonyítékgyűjtéssel összefüggésben. A törvény először az általános szabályokat tartalmazza, majd külön foglalkozik az okirat, illetve az elektronikus adat lefoglalásáról. A 308. § (3) bekezdéséből kikerült a korábbi hármas felsorolás, a törvény már nem nevesíti külön a rendszert és az adathordozót, csak az elektronikus adatot mint a lefoglalás tárgyát.

31 Az emberi méltóság, a személyiségi és kegyeleti jogok tiszteletben tartásának fontosságát hangsúlyozza Peszleg Tibor is. Lásd Peszleg Tibor: i. m. 23. o.
32 Mohácsi Barbara: Bűnüldözési érdek contra emberi jogok – az online házkutatás alkotmányossági megítélése Németországban, néhány tanulsággal. Magyar Jog, 2008/12., 829. o.
33 Trócsányi Sára: i. m.

Új szabályként került a 309. § (3) bekezdésébe a vádemelés előtt kizárólag ügyész, azt követően bíró által elrendelhető lefoglalás körébe a címzettnek még nem továbbított, elektronikus hírközlési szolgáltatás során továbbítandó közlés vagy küldemény, amelyet a jogalkotó a postai küldeményektől külön kezel. A gyakorlatban nem világos, mi tekinthető még el nem küldött elektronikus közlésnek, ahogy a továbbítottnak tekintendőség időpontját se határozzák meg, és e kérdésekre vonatkozóan az indokolás sem tartalmaz iránymutatást.

A lefoglalást fő szabályként birtokba vétellel kell végrehajtani, ez alól az új Be. 311. § (2) bek. három kivételt ismer. A lefoglalást az érintett őrizetében hagyással vagy a megőrzés más módon történő biztosításával lehet végrehajtani, ha

– a dolog birtokba vételre nem alkalmas;
– a dolog vagy elektronikus adat birtokosának, kezelőjének azok használatához fűződő érdeke ezt indokolja; vagy
– más fontos ok ezt szükségessé teszi.

Ez az információs rendszerben tárolt adat megőrzésére kötelezés kényszerintézkedéshez hasonló megoldás, ahol szintén a birtokos vagy kezelő őrizetében hagyják az adatokat. A hasonlóságot tovább erősíti, hogy a törvény 316. §-a immár nem önálló kényszerintézkedésként, hanem a lefoglalás részeként szabályozza a megőrzésre kötelezést. Az indokolás szerint ennek alapja az, hogy ez a lefoglalással analóg kényszerintézkedés. A kettő között a fő különbség azonban az, hogy míg a megőrzésre kötelezés a hatályos szabályozáshoz hasonlóan legfeljebb három hónapig, illetve az átvizsgálásig tarthat, addig itt nem szerepel ilyen kitétel.

A törvény 315. §-a a hatályos Be.-nél jóval részletesebben tartalmazza az elektronikus adat lefoglalásával kapcsolatos szabályokat. A szakasz (1) bekezdése alapján elektronikus adat lefoglalásának módja lehet

– elektronikus adatról másolat készítése;
– elektronikus adat áthelyezése;
– információs rendszer vagy adathordozó teljes tartalmáról történő másolat készítése;
– információs rendszer vagy adathordozó lefoglalása;
– egyéb, jogszabályban meghatározott mód.

A törvény indokolásából kitűnik, hogy a különböző módszerek között fokozatosság áll fenn, és ezt a szakasz további rendelkezései is megerősítik. A paragrafus (4) bekezdése szerint a lefoglalást úgy kell végrehajtani, hogy a bün-

tetőeljárás céljából szükségtelen elektronikus adatra lehetőleg ne terjedjen ki, illetve az ilyen elektronikus adatot a legrövidebb ideig érintse. Az (5) bekezdés határozza meg, mely esetekben lehetséges az egész rendszert vagy adathordozót lefoglalni: ha elkobozható, illetve vagyonelkobzás alá esik; ha tárgyi bizonyítási eszközként bír jelentőséggel; vagy ha a bizonyítás érdekében előre nem meghatározható vagy jelentős mennyiségű elektronikus adat átvizsgálására van szükség. Az érdeksérelem további mérséklését célozza a (6) bekezdés, amely szerint ilyen esetekben az elektronikus adattal rendelkezni jogosult kérésére másolatot kell készíteni az általa megjelölt elektronikus adatról, amennyiben ez a büntetőeljárás érdekét nem veszélyezteti. Utóbbi, mivel nem a lefoglalt rendszer birtokosát, hanem az adattal rendelkezni jogosultat nevezi meg kérelmezőként, lehetővé teszi, hogy mindazok a nyomozó hatósághoz forduljanak, akiknek adatát az adott rendszerben vagy adathordozón tárolták.

Bizonyos kérdésekben azonban az új Be. sem ad iránymutatást, így például arra vonatkozóan, hogy ha az információs rendszer vagy adathordozó és az adat más tulajdona, illetve ha egy rendszer több személy adatait is tartalmazza (például egy szervergép), akkor melyikre kell elrendelni a lefoglalást. Probléma lehet ilyen esetben annak eldöntése is, hogy kinek ad a törvény jogorvoslati lehetőséget. Ugyanis, ha a rendszerre nézve rendelik el a lefoglalást, akkor a nyomozó hatóság határozata csak annak tulajdonosára vonatkozóan tartalmaz közvetlen rendelkezést, de az adat tulajdonosára nem, így a hatályos Be. 195. §-a alapján csak ő jogosult panaszt tenni.

Bitcoin lefoglalása

Fontos új változtatást jelent még az új Be. 315. szakasz (2) bekezdése, amelyben a fizetésre használt elektronikus adat lefoglalásáról található rendelkezés. Ennek megértéséhez fontos megvizsgálni, pontosan mit is értünk az elektronikus pénz fogalmán. Többféle definíció létezik erre mind a szakirodalomban, mind jogszabályokban[34], én ezek közül az elektronikuspénz-kibocsátó intézmények tevékenységének megkezdéséről, folytatásáról és prudenciális felügyeletéről szóló 2009/110/EK irányelvet emelném ki, amely szerint az elektronikus pénz a kibocsátóval szembeni követelés által megtestesített, elektronikusan tárolt – ideértve a mágneses tárolást is – monetáris érték, ame-

34 Bővebben lásd Szathmáry Zoltán: Az elektronikus pénz és a bitcoin biztosítása a büntetőeljárásban. Magyar Jog, 2015/11., 639–641. o.

lyet pénzeszköz átvételével bocsátanak ki. Az egyik legismertebb a bitcoin, amely peer-to-peer hálózati működési elvű nyílt forráskódú úgynevezett kriptovaluta, amelynek alapja számítástechnikai rendszerek erőforrása. Maga a bitcoin egy generált adat, amely matematikai algoritmussal keletkezik a tranzakciók feldolgozása és jóváhagyása révén (ezt nevezik bányászásnak).[35] A bitcoin azonban nem tekinthető általános értelemben elektronikus pénznek, hiszen nincs kibocsátója, semmilyen szervezet nem gyakorol felügyeletet felette, és nem áll mögötte semmilyen vagyoni fedezet.[36] A bitcoin teljes anonimitást ad a használóknak, így sok esetben különböző bűncselekmények során használják fel azt, ami értelemszerűen a hatóságok figyelmét is ráirányítja a jelenségre.

A fő problémát a bitcoinnal – és minden más, hasonló technológián alapuló virtuális pénzzel – kapcsolatosan a hiányzó jogi dogmatika jelenti, hiszen mint Szathmáry is rámutat, vagyonelkobzás vagy polgári jogi igény biztosítása érdekében történő biztosítása tulajdonképpen legitimálja azt.[37] Az új Be. 315. § (2) bekezdése úgy szabályozza a kérdést, hogy a fizetésre használt elektronikus adat lefoglalását lehetővé teszi, végrehajtásáról pedig úgy rendelkezik, hogy annak során az elektronikus adattal olyan műveletet végeznek, amely megakadályozza az érintettnek az elektronikus adat által kifejezett vagyoni érték feletti rendelkezési lehetőségét. A törvény nem nevesíti kifejezetten a bitcoint, és az indokolás is csak példálózó jelleggel említi, de elterjedtsége miatt kijelenthető, hogy a rendelkezés apropóját a kriptovaluta egyre inkább elterjedt használata adta.

Elektronikus adat megőrzésére kötelezés

Eredete, fogalma

A jogintézmény alapja az Európa Tanács 2001-es, Budapesten aláírt, a számítástechnikai bűnözésről szóló egyezmény 16. cikke, amely a tárolt számítástechnikai adat gyors megőrzése elnevezést kapta. Ez előírja a tagállamoknak, hogy tegyék lehetővé az illetékes hatóságok számára számítástechnikai adatok megőrzésének elrendelését. A személy, akinek ellenőrzése alatt vagy birtokában az adatok vannak, legfeljebb kilencven napig kötelezhető megőrzésre. A

35 Lakatos Alexandra Anna: Az informatikai bűncselekmények és a bitcoin. Belügyi Szemle, 2017/1., 29. o.; Szathmáry Zoltán: i. m. 642– 643. o.
36 Lakatos Alexandra Anna: i. m. 30. o.
37 Szathmáry Zoltán: i. m. 645. o.

jogintézmény a lefoglalással ellentétben nem vonja el az adat birtoklásának jogát a kötelezettől. Fontos sajátossága még az is, hogy nemcsak bizonyítási eszközökre, de az azok begyűjtése érdekében a bűncselekménnyel összefüggésbe hozható bármilyen más adatra is kiterjed.[38]

A magyar Be.-be a 2002. évi I. törvény vezette be a jogintézményt számítástechnikai rendszer útján rögzített adatok megőrzésére kötelezés cím alatt, amely 2003. január 1-jén lépett hatályba, a törvény egészével együtt. A Be. 158/A §-ban szabályozott kényszerintézkedés elnevezése a bevezetése után tíz évvel megváltozott, és a *„számítástechnikai rendszer útján rögzített”* helyére *az „információs rendszerben tárolt”* kifejezés került (2013. évi CLXXXVI. törvény 72. §), mivel ez utóbbi jóval tágabb megfogalmazás, és a jogalkotó így igazodott a technika fejlődése által támasztott kihívásokhoz.[39] Hiszen napjainkban már nemcsak számítógépek, de más eszközök is érintettek lehetnek a kiberbűnözésben, például az okostelefonok. Az új Be. 316. §-a ismét változtat a megnevezésen, és az elektronikus adat megőrzésére kötelezést használja, amely összhangban áll a törvény többi változtatásával, vagyis az elektronikus adat mint bizonyítási eszköz megjelenésével.

A jogintézménnyel kapcsolatos fogalmi problémák korábban is jelen voltak, így például a nyomozás részletes szabályait tartalmazó 23/2003. (VI. 24.) BM–IM rendelet (a továbbiakban: Nyor.) 84. §-a még mindig a kényszerintézkedés 2013 előtti elnevezését használja. Hasonló módon felveti a módosítás igényét az új Be. megváltozott elnevezése is. A 2013. évi CLXXXVI. törvény a Btk. módosításával a 287. §-ban szabályozott zártörés tényállását módosítva kriminalizálta az információs rendszerben tárolt adatok megőrzésére kötelezéssel érintett adat jogosulatlan személy számára történő megismerhetővé tételét, eljárás alóli elvonását, illetve módosítását.

Szabályai

Az információs rendszerben tárolt adat megőrzését a nyomozó hatóság, az ügyész és a bíróság rendelheti el, ezzel ideiglenesen korlátozva az adat birtokosának, feldolgozójának, valamint kezelőjének az adat feletti rendelkezését. A Nyor. 84. §-a alapján az elrendelő határozatnak tartalmaznia kell a megőrzendő adatok körét, a Be. 158/A § meghatározott bekezdéseiben foglalt köte-

38 Villányi József: Az Európa Tanács Informatikai bűnözéssel kapcsolatos egyezményéről. Magyar Jog, 2001/8., 470. o.

39 Czine Ágnes: VIII. fejezet. In: Belegi József (szerk.): Büntetőeljárás I–III. Kommentár a gyakorlat számára. HVG-ORAC Kiadó, Budapest, 2014, 88. o.

lezettségeket, valamint fokozott biztonságú elektronikus aláírás vagy időbélyegző használata esetén az erre történő utalást. Ez utóbbira nem található utalás a Be. szövegében, gyakorlatilag annak igazolására szolgál, hogy az elhelyezése idején az adatok változatlan formában léteztek. A fokozott biztonságú elektronikus aláírást az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény 1. § 22. pontja a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról 910/2014/EU rendeletre utalással határozza meg. Ennek 26. cikke szerint a fokozott biztonságú elektronikus aláírás

– kizárólag az aláíróhoz köthető;
– alkalmas az aláíró azonosítására;
– olyan, elektronikus aláírás létrehozásához használt adatok felhasználásával alkotják meg, amelyeket az aláíró nagy megbízhatósággal kizárólag saját maga használhat;
– olyan módon kapcsolódik azokhoz az adatokhoz, amelyeket aláírtak vele, hogy az adatok minden későbbi változása nyomon követhető.

Ha az adatok kizárólag egy belső hálózaton (intranet) elérhetők, akkor a rendszergazdát kell kötelezni a megőrzésükre.[40]

A kényszerintézkedés célja nagyobb mennyiségű adat biztosítása a nyomozó hatóság számára átvizsgálás céljából. Ennek oka, hogy jelentősebb adathalmazra nem rendelhető el lefoglalás, hiszen meghatározhatatlan, mely adatok szükségesek[41], és ennek technikai végrehajtása is jelentős problémákba ütközne. A Be. 158/A § (7) bekezdésből kitűnik, hogy az elrendelés után az elrendelőnek haladéktalanul meg kell kezdenie az adatok átvizsgálását, és ennek nyomán az adatot információs rendszerbe vagy más adathordozóra történő átmásolással lefoglalni.

Ez előnyös lehet a nyomozó hatóság számára, hiszen nem kell nagyobb mennyiségű adat lefoglalásáról gondoskodniuk, és a kötelezett számára is, mivel a lefoglalással ellentétben itt hozzáférhet a kényszerintézkedés által érintett adatokhoz. A (3) bekezdés alapján azonban köteles az adatot változatlanul megőrizni, és – szükség esetén más adatállománytól elkülönítve – gondoskodni annak biztonságos tárolásáról. Ezen kívül meg kell akadályoznia az adat megváltoztatását, törlését, megsemmisülését, továbbítását, másolat jo-

40 Uo. 806. o.
41 Tóth Fanni: 77. o.

gosulatlan készítését, illetve az adathoz való jogosulatlan hozzáférést. A Nyor. 85. §-a arról rendelkezik, hogy a végrehajtásról jegyzőkönyvet kell felvenni. A Be. 158/A § (4) bekezdése további kötelezettségként állapítja meg a megőrzésre kötelezett részére, hogy tájékoztassa az elrendelőt arról, ha az érintett adatot jogosulatlanul megváltoztatták, törölték, átmásolták, továbbították, megismerték, vagy ha ezek megkísérlésére utaló jelet észlelt.

Mindezekből következik, hogy elrendelésre csak az elkövetésben nem érintett személyek esetén kerül sor, hiszen egyébként az eljárás sikerét veszélyeztetné az adatok birtokos rendelkezési körében történő hagyása. Erre utal a Kúria vonatkozó ítélete is[42], amely kimondja, hogy valaki *„a számára egyébként terhelő adatok megőrzésére nem kötelezhető”*. A gyakorlat is abba az irányba mutat, hogy csak a bűncselekményben nem érintett számítógépek esetén írják elő az adatok megőrzésére kötelezést, míg egyéb esetekben lefoglalásra kerül sor.[43]

Mivel a kötelezett általában nem kapcsolódik a büntetőeljáráshoz, így a méltányosság különösen fontos szerepet kap. Akárcsak más, bizonyítékok beszerzésére és biztosítására vonatkozó kényszerintézkedések esetén, itt is hangsúlyosan megjelenik a kötelezett kíméletének szándéka. Egyrészt a Be. 158/A § (8) bekezdése kilencven napban maximálja a megőrzési kötelezettség időtartamát, másrészt a (4) bekezdés lehetőséget teremt arra, hogy ha az adat eredeti helyen történő megőrzése a fő tevékenységet jelentősen zavarná, akkor az elrendelő engedélyével az adatokat másik adathordozón vagy rendszerben is tárolhatja.

Elektronikus adat ideiglenes hozzáférhetetlenné tétele

A tartalombűncselekmények elleni fellépés szükséges lehet, különösen az olyan súlyosan sértő tartalmak esetén, mint a gyermekpornográfia. Ennek napjainkban preferált eszköze a tartalomszűrés, vagyis a jogsértő tartalmak kiszűrése, majd eltávolítása vagy más módon történő elérhetetlenné tétele. A gyermekek szexuális bántalmazása, szexuális kizsákmányolása és a gyermekpornográfia elleni küzdelemről szóló 2011/93/EU irányelve a gyermekpornográfiát tartalmazó vagy azt terjesztő weboldalak elleni intézkedések címet viselő 25. cikke teremt lehetőséget az állami tartalomszűrés bevezetésére. A

42 Kúria Pfv.IV.21.941/2012/5.
43 Tóth Fanni: i. m. 79. o.

cikk (2) bekezdése ugyanis kimondja, hogy a tagállamok – átlátható eljárás keretében, a megfelelő garanciák mellett, arányos és szükséges módon – intézkedéseket tehetnek a gyermekpornográfiát tartalmazó vagy azt terjesztő weboldalakhoz való hozzáférés meggátlására.

Az e rendelkezésnek való megfelelés érdekében került be a Btk. hatálybalépésével egy időben, 2013. július 1-jei hatállyal a Btk. 77. §-ba intézkedésként az adat végleges hozzáférhetetlenné tétele, valamint ennek eljárásjogi párjaként a Be. 158/B–D §-ba kényszerintézkedésként az elektronikus adat ideiglenes hozzáférhetetlenné tétele.[44] Utóbbival a jogalkotói cél az volt, hogy még a büntetőeljárás ideje alatt megszüntethető legyen a jogsértő állapot. A 158. § (1) bekezdése úgy határozza meg a kényszerintézkedést, mint az elektronikus hírközlő hálózat útján közzétett adat feletti rendelkezési jog ideiglenes korlátozását, és az adathoz való hozzáférés ideiglenes megakadályozását. A kényszerintézkedés kapcsán fogalmi pontatlanság érhető tetten: míg a kényszerintézkedés elnevezése *„elektronikus adat ideiglenes hozzáférhetetlenné tétele”,* addig a cím, amely alá tartozik, az *„elektronikus hírközlő hálózat útján közzétett adat”* fogalmát használja. Mint a bekezdésből is kitűnik, a kettő a törvény szerint felcserélhető, mindazonáltal az eltérő elnevezés használata indokolatlan, és valószínűleg jogalkotói figyelmetlenség következménye.

A kényszerintézkedés elrendelésének feltételeit a paragrafus (2) bekezdése tartalmazza. E szerint az adat ideiglenes hozzáférhetetlenné tétele alkalmazásának akkor van helye, ha az eljárás olyan közvádra üldözendő bűncselekmény miatt folyik, amellyel kapcsolatban elektronikus adat végleges hozzáférhetetlenné tételének van helye, és az a bűncselekmény folytatásának megakadályozásához szükséges. A Btk. 77. § (1) bekezdése alapján véglegesen hozzáférhetetlenné kell tenni az olyan elektronikus adatokat,

– amelynek hozzáférhetővé tétele vagy közzététele bűncselekményt valósít meg;
– amelyet a bűncselekmény elkövetéséhez eszközül használtak; vagy
– amely bűncselekmény elkövetése útján jött létre.

A Be. 159/C § (1) bekezdése alapján a kényszerintézkedés kötelezettje nem az adat birtokosa, hanem a tárhelyszolgáltató, az ő együttműködése híján pedig az elektronikus hírközlési szolgáltató. A közvetítő szolgáltató fogalmát az elektronikus kereskedelmi szolgáltatások, valamint az információs társada-

44 Uo. 81. o.

lommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény 2. § l) pontja határozza meg, ennek a körnek a része az igénybe vevő által biztosított információt tároló tárhelyszolgáltató is. Mivel mind a Be., mind az e törvény 12/A §-a is csak ezt a szűkebb kört jelöli ki a kényszerintézkedés kötelezettjeként, arra más közvetítő szolgáltatók (például gyorsítótárat kínáló) nem kötelezhetők.[45]

A Be. 158/B § (4) bekezdése alapján a kényszerintézkedés elrendelhető elektronikus adat ideiglenes eltávolításával (158/C §), illetve elektronikus adathoz való hozzáférés ideiglenes megakadályozásával (158/D §), és a rendelkezést a magyar jogrendbe beiktató 2013. évi LXXVIII. törvény indokolása egyértelművé teszi a kettő közötti fokozatosság meglétét.[46] A törvény az eltávolítást preferálja, és a bíróság először a tárhelyszolgáltatót kötelezi a tartalom eltávolítására, aminek egy munkanapon belül eleget kell tennie. A határozat tartalmát az 11/2014. (XII. 13.) IM rendelet 142. §-a tartalmazza, e szerint az elektronikus adat forrását a következők megadásával kell azonosítani:

– IP-cím ipv4 vagy ipv6 szabvány szerint és alhálózati maszk;
– doménnév;
– URL-cím;
– portszám.

A szolgáltató kötelezettsége nemcsak az adat eltávolítására, de a Be. 158/C § (4) bekezdése alapján az adat visszaállítására is kiterjed, a határozat közlésétől számított egy munkanapon belül. A bíróság a (2) bekezdés alapján elrendeli az adat visszaállítását, amennyiben megszűnt az elrendelés oka, vagy ha megszüntetik a nyomozást, és nem rendelik el a Btk. 77. § szerinti végleges hozzáférhetetlenné tételt. Hasonlóan megszűnik az ideiglenes eltávolítás, hogyha befejeződik a büntetőeljárás. Amennyiben a szolgáltató valamely kötelezettségét elmulasztja teljesíteni, rendbírsággal sújtható, amelynek összege eltér a rendbírság általános szabályainál meghatározottól.

Ha a tárhelyszolgáltató eltávolítási kötelezettségét nem teljesítette vagy az eltávolításra vonatkozóan külföldi jogsegély iránti megkeresés harminc napon belül nem vezetett eredményre, akkor a Be. 158/D § (1) bek. b) pontjában taxatíve felsorolt kilenc bűncselekményi kör esetén helye van a hozzáférés ideiglenes megakadályozása elrendelésének. Ennek kötelezettje már nem a tárhelyszolgáltató, hanem az elektronikus hírközlési szolgáltatók, a végre-

---

45 Gaiderné Hartmann Tímea: Elektronikus adatok ideiglenes és végleges hozzáférhetetlenné tétele – egy új intézmény első évei. Magyar Jog, 2015/2.,109. o.

46 http://www.parlament.hu/irom39/09246/09246.pdf

hajtást pedig a Nemzeti Média- és Hírközlési Hatóság felügyeli, a határozat és az elektronikus adat elérésének a központi elektronikus hozzáférhetetlenné tételi határozatok adatbázisában történő rögzítéssel.[47]

Az új Be. 335–338. §-a tartalmazza a kényszerintézkedésre vonatkozó szabályokat. Az észrevehető legnagyobb különbség, hogy már élesen elkülönül egymástól az adat ideiglenes eltávolítása és a hozzáférés ideiglenes megakadályozása. A fejezet első része a két elrendelési mód közös szabályait tartalmazza, majd ezt követően külön-külön foglalkozik a specifikus szabályokkal. A hozzáférés ideiglenes megakadályozásának szövegezése módosult, és véleményem szerint a zárt bűncselekményi lista előrébb helyezése, és az eddig nehezen érthetően megfogalmazott két konjunktív feltétel egyben történő megfogalmazása mind dogmatikailag, mind közérthetőség szempontjából is jóval előnyösebb szerkesztési megoldás.[48] A lényegi változások körében kiemelendő, hogy a hozzáférés megakadályozását megelőző eltávolítás sikertelenségével kapcsolatos listát két új tétellel is kiegészíti a törvény. Így megalapozhatja az alkalmazását az is, ha az eltávolításra kötelezett azonosítása lehetetlen vagy aránytalan nehézséggel járna, illetve ha az elektronikus adat ideiglenes eltávolítására vonatkozóan a külföldi hatóság jogsegély iránti megkeresésétől eredmény nem várható vagy a megkeresés aránytalan nehézséggel járna.

A jogintézményt már javaslatként való felvetésének pillanatától kezdve kemény viták övezték. Egyebek között a Társaság a Szabadságjogokért (TASZ) részéről, amely túlságosan tágnak gondolta az eltávolítható tartalmak meghatározását, és zárt felsorolást javasolt alkalmazni, amely végső soron meg is jelent a fokozatosság formájában.[49] Azonban míg a tételes felsorolás kezdetben a gyermekpornográfiát, az állam elleni bűncselekményt és a terrorcselekményt foglalta magában, később a 2015. évi LXXVI. törvény tágította ennek körét, így napjainkban már kilenc bűncselekmény esetén rendelhető el az ideiglenes hozzáférhetetlenné tétel. A legnagyobb vitát az internetes tartalomszűrés szólásszabadságot befolyásoló lehetséges következményei szülték, hiszen a jogintézményt a világ számos országában – mint például Oroszország, Kína és Törökország – használják különböző mértékű politikai cenzúrára. Hazánkban – mivel a határozatokat tároló központi elektronikus hozzáférhetetlenné tételi határozatok adatbázisa csak a Nemzeti Mé-

47 Az eljárás pontos részleteiről bővebben lásd Gaiderné Hartmann Tímea: i. m. 113. o.

48 Így például elkerülhetők az olyan félreértések is, miszerint a két feltételt külön-külön esetkörnek, és nem összetartozónak vélik. Például lásd Gaiderné Hartmann Tímea: i. m. 112.

49 A Társaság a Szabadságjogokért véleménye. https://tasz.hu/files/tasz/imce/2011/tasz_velemeny_20121026.pdf

dia- és Hírközlési Hatóság és az elektronikus hírközlési szolgáltatók számára hozzáférhető – hiányzik a jogintézmény feletti társadalmi kontroll, ami aggályokat vet fel. További probléma a rendszer technikai kiforratlansága, és a jogintézmény kiforratlanságát mutatja az is, hogy 2016-ban a központi elektronikus hozzáférhetetlenné tételi határozatok adatbázisának rendszerében nulla bejegyzés szerepelt.[50]

Mindamellett technikai nehézségek is bőségesen felvetődnek, így például, hogy a szűrés technikájától függően nagy az esélye annak, hogy túlszűrés (vagyis nem jogsértő tartalmak korlátozása), illetve alulszűrés (jogsértő tartalmak továbbra is elérhetők) valósuljon meg. A szűrés bevezetése pontosan ezen bukott meg Németországban.[51] Ez a fajta hibalehetőség kikerülhető, ha – mint azt például véleményében a TASZ is megfogalmazza – a hozzáférhetetlenné tétel csak az URL-címre terjed ki. Ugyanakkor ez a megoldás a legkönnyebben kijátszható, hiszen elegendő a tartalmat egyszerűen más URL-címre mozgatni, hogy újra mindenhol, bárki számára elérhetővé váljon. *Gaiderné Hartmann Tímea* és *Ficsór Gabriella* véleménye szerint azonban ez kiküszöbölhető lenne azzal, ha a bírósági határozat nem a hozzáférhetetlenné tenni rendelt adatelérés útját, hanem az adattartalmat jelölné meg.[52]

A legsúlyosabb gond azonban, hogy a tartalomszűrés napjainkra egyre kevésbé alkalmas az eredetileg kijelölt céljára, az online gyermekpornográfia elleni fellépésre, hiszen annak fő területe már nem a tartalomszűrés által érintett nyílt web. A jogintézmény által érintett területek folyamatos kiterjesztése (például a tiltott szerencsejáték-szervezést megvalósító és a hamis vagy nem engedélyezett gyógyszert forgalmazó oldalakra) is egyre inkább eltolódást mutat az eredeti alkalmazási körtől, és ennek kapcsán sokan kifejezték az aggályaikat.[53]

Összegzés

Tanulmányomban igyekeztem átfogó képet nyújtani a kibertérben elkövetett bűncselekményekkel kapcsolatban alkalmazható kényszerintézkedések sza-

50 Gyömbér Béla: Így működik az állami internetcenzúra Magyarországon. 2017 https://jogalappal.hu/igy_mukodik_az_internetcenzura_magyarorszagon/

51 Parti Katalin: „10 dolog, amit utálok benned”, avagy a kormányzati szintű internet-blokkolás kritikája a német törvény kapcsán. Infokommunikáció és Jog, 2010/38., 97–98. o.

52 Gaiderné Hartmann Tímea: i. m. 115. o.

53 Detrekői Zsuzsa: Blokkolás Magyarországon – hogyan jutottunk el a gyermekpornográfia elleni küzdelemtől a szerencsejáték-oldalak blokkolásáig. Infokommunikáció és Jog, 2014/60., 185–187. o.; Tóth Fanni: i. m. 85. o.

bályairól, kihívásairól, esetleges hibáiról. Mint a büntetőeljárás-jog sok más, a digitális forradalom által érintett területén, itt is elengedhetetlen a technika fejlődésével egyszerre történő haladás, méghozzá úgy, hogy ne szülessen belőle túlzottan nagy terjedelmű és követhetetlen, és így alkalmazhatatlan jog-anyag.

Véleményem szerint az új Be. szabályozása szinte minden kapcsolódó jogintézménynél a megfelelő irányba tett lépéseket, régóta fennálló dogmatikai vitákat és nehezen megítélhető helyzeteket szüntetve meg. Példaként említeném az elektronikus adat önálló bizonyítási eszközként való megjelenését, illetve az adatok lefoglalásával kapcsolatos szabályok sokkal részletesebb kidolgozását.

Bizonyos kérdésekben azonban nem tartalmaz új rendelkezéseket a törvény, így például arra, a mindennapi életben gyakran előforduló esetre, amikor más az információs rendszer és az adat tulajdonosa, illetve több személy adatai is ugyanabban a rendszerben találhatók. Ez különösen a lefoglalásnál idézhet elő jogilag nehezen feloldható helyzeteket. Mindamellett, ahogy az új Be. is bizonyítja, ezek a problémák nem megoldhatatlanok, és reményeim szerint a mostani tendencia a jövőben is folytatódik, tovább javítva a kapcsolódó kényszerintézkedések szabályrendszerén, illetve ezek gyakorlatán.

IRODALOM

Andreea, Vertes-Oltenau: Evolution of the Criminal Legal Frameworks for Preventing and Combating Cybercrime. *Journal of Eastern-European Criminal Law,* no. 1, 2014

Berecz Péter: A Német Szövetségi Alkotmánybíróság „számítógép-határozata". *Studia Juvenum,* 2009/1.

Brenner, Susan W.: Budapesti Law – A United States Perspective. In: **Casey, Eoghan (ed.):** Digital Evidence and Computer Crime. Academic Press, 2011, pp. 115–118.

Casey, Eoghan: Foundations of Digital Forensics. In: **Casey, Eoghan (ed.):** Digital Evidence and Computer Crime. Academic Press, 2011

Chawki, Mohamed: Online Child Sexual Abuse: The French Response. *Journal of Digital Forensics, Security and Law,* no. 4, 2009

Czine Ágnes: VIII. fejezet. In: **Belegi József (szerk.):** Büntetőeljárás I–III. Kommentár a gyakorlat számára. HVG-ORAC Kiadó, Budapest, 2014

Detrekői Zsuzsa: Blokkolás Magyarországon – hogyan jutottunk el a gyermekpornográfia elleni küzdelemtől a szerencsejáték-oldalak blokkolásáig. *Infokommunikáció és Jog,* 2014/60.

Gaiderné Hartmann Tímea: Elektronikus adatok ideiglenes és végleges hozzáférhetetlenné tétele – egy új intézmény első évei. *Magyar Jog,* 2015/2.

Gropeneanu, Antonela – Iacob, Adrian: Investigative issues regarding cybercrime. *European Journal of Public Order and National Security,* no. 2, 2016

Gyömbér Béla: Így működik az állami internetcenzúra Magyarországon. 2017. https://jogalappal.hu/igy_mukodik_az_internetcenzura_magyarorszagon/

Király Tibor: Büntetőeljárási jog. Osiris Kiadó, Budapest, 2003

Laczi Beáta: A számítógépes környezetben elkövetett bűncselekmények nyomozásának és a nyomozás felügyeletének speciális kérdései. *Magyar Jog,* 2001/12.

Lakatos Alexandra Anna: Az informatikai bűncselekmények és a bitcoin. *Belügyi Szemle,* 2017/1.

Mohácsi Barbara: Bűnüldözési érdek contra emberi jogok – az online házkutatás alkotmányossági megítélése Németországban, néhány tanulsággal. *Magyar Jog,* 2008/12.

Nagy Zoltán, András – Mezei, Kitti: The organised criminal phenomenon on the Internet. *Journal of Eastern-European Criminal Law,* no. 2, 2016

Parti Katalin: Tiltott pornográf felvétellel visszaélés az interneten – az empirikus kutatás adatai. In: **Virág György (szerk.):** Kriminológiai Tanulmányok, 44. OKRI, Budapest, 2007, 98. o.

Parti Katalin: „10 dolog, amit utálok benned", avagy a kormányzati szintű internet-blokkolás kritikája a német törvény kapcsán. *Infokommunikáció és Jog,* 2010/38.

Peszleg Tibor: A digitális bizonyítási eszközök megszerzésének elvei és gyakorlati érvényesítésük. *Ügyészek Lapja,* 2010/2.

Róth Erika: A kényszerintézkedések változó rendszere és részletszabályai. *Ügyészek Lapja,* 2016/3–4.

Sorbán Kinga: A digitális bizonyíték a büntetőeljárásban. *Belügyi Szemle,* 2016/11.

Szádeczky Tamás: Az IT biztonság szabályozásának konfliktusa. *Infokommunikáció és Jog,* 2013/3.

Szathmáry Zoltán: Az elektronikus pénz és a bitcoin biztosítása a büntetőeljárásban. *Magyar Jog,* 2015/11.

Tóth Fanni: Az informatikai bűnözéshez kapcsolódó kényszerintézkedések. *Büntetőjogi Szemle,* 2017/1.

Trócsányi Sára: Első oldal. *Infokommunikáció és Jog,* 2009/6.

Vadász Viktor: A számítógép demisztifikálása. *Ügyészek Lapja,* 2010/2.

Villányi József: Az Európa Tanács Informatikai bűnözéssel kapcsolatos egyezményéről. *Magyar Jog,* 2001/8.

Wang, Shiuh-Jeng: Measures of retaining digital evidence to prosecute computer-based cyber-crimes. *Computer Standards & Interfaces,* no. 2, 2007

DOI: 10.38146/BSZ.2018.2.9

BEZSENYI TAMÁS

Az első magyar sorozatgyilkos bérgyilkosságai II.[1]

A Szeged környéki tanyavilágban a XX. század első felében egy *Pipás Pista* nevű napszámos több alkalommal is emberölést követett el. A később ellene indult per és a róla szőtt legendák szerint csak házas férfiakat ölt meg, akik a felbujtó feleségek elmondása alapján iszákosak, erőszakosak és erkölcstelenek voltak.

Az eset főszereplőjének, Pipás Pistának a tanúvallomása két részre osztható: *Börcsök István* halála kapcsán először tagadott, majd nagyrészt beismerte, *Dobák Antal* ügyében azonban jelentéktelennek tüntette fel a szerepét.

Jelen tanulmányban is a kriminológiai, illetve a kriminalisztikai szempontokat összekapcsolva vizsgálom, hogy Pipás Pista gyilkosságainak történeti tényállását minél aprólékosabban feldolgozva milyen mintákat lehet felfedezni Pipás öléseiben. Az első gyilkosság jelentőségét az adja, hogy Pipás az eljárás kezdetén tagadta az ebben való részvételét, míg Dobákéban nem tagadta, pusztán gyengíteni próbálta. A két eltérő módozat mögött szemléletesen felsejlik, hogy eltérő emocionális háttérrel közelített a két asszonyhoz, valamint családjukhoz.

*Börcsökné*nek, valamint *Dobákné*nak a tanulmány első részében bemutatott vallomásai alapján látható, hogy az első, rábizonyított emberölés után vissza kívánt illeszkedni abba a rurális társadalmi közegbe, amelyben szocializálódott, míg a második ölése már ennek teljes kudarcát, valamint az egyértelműen kívülálló *(outlaw)* szerep elfogadását feltételezi.

Kovács Lajos az emberölések utólagos felderítésének kriminalisztikájával kapcsolatosan kiemeli, hogy az érintettek, az elkövetésben érdekelt személyek között az idő múlásával megváltozó kapcsolatrendszer, későbbiekben kialakuló haragos viszonya elősegítheti egy emberölési ügy sikeres felderíthetőségét.[2]

Pipás Pista ügyében különleges jelentőséget kap ez az érdekelti körben bekövetkező változás, az emberi kapcsolatok felbomlása, mert így vált lehe-

1 A tanulmány első része a 2018/1. számban jelent meg.

2 Kovács Lajos: Az emberölés utólagos felderítésének helyzete és tapasztalatai Magyarországon. Belügyi Szemle, 2005/1., 3–13., különösen 7–9. o.

tővé, hogy a sorozatgyilkos-jegyek egyre inkább átforduljanak bérgyilkosi magatartássá.

A nemzetközi kriminalisztikai szakirodalom igen elvétve tárgyalja a bérgyilkosságokat, mivel a felderítési dilemmákon túl rendkívül nehéz több cselekményt is kötni ugyanahhoz a személyhez, hiszen tapasztalt bérgyilkosok előszeretettel változtatnak a modus operandin, az elkövetési módon. Kriminológiai szempontból pedig probléma, hogy az áldozat és az elkövető dichotóm, de szociálpszichológiai szempontból értelmezhető kapcsolatrendszerét újraszabja egy harmadik fél megjelenése, hiszen ekkor az elkövető mint felbujtó már jóval nehezebben azonosítható be egyértelműen, így a hipotézisek, a gyanúk és a pletykák szegmentálják az adott ügy vagy ügyek elemzésének érvényességét. *Schlesinger* egészen odáig megy, hogy *„alig megérthető típusú emberölésnek”* tekinti a bérgyilkosságokat.[3] *Calhoun* pedig egyenesen egy titkos világ beszüremkedésével magyarázza a hatékony ügyfeldolgozás hiányát.[4]

Pipás ügyében természetesen a *Donal MacIntyre, David Wilson* és társaik által kialakított tipológiát nem lehet használni[5], ahogy a korábbiakat sem[6], hiszen a fizikai jelenlétnek, az erőszak jelentősebb szerepének az adott korszakban nem volt olyan bizonyító ereje, mint a ma, a DNS-, illetve a mikroanyagmaradványok világában.[7] Pipás kezdetlegesnek tűnő módszere ellenére is rendkívül alaposan felkészült, továbbá beállította a helyszínt öngyilkosságnak álcázva. A kor öngyilkosságokra vonatkozó szociológiai diskurzusát nem ismerve, mégis az akasztás módszerével fedte el emberölési szándékát. A módszer hatékonyságát emeli ki *Konek Sándor* 1867-es megállapítása[8], illetve a XX. század végén *Zonda Tamás* és kollégáinak kutatása: meghúzták Nyíregyháza és Pécs között azt a tengelyt, amely alatt, vagyis az ország délkeleti részén az öngyilkosságok száma magasabb, mint északnyugaton, valamint az önakasztás módszerével elkövetett cselekmények is számottevőbbek.[9]

3 Louis B. Schlesinger: The Contract Murderer: patterns, characteristics and dynamics. Journal of Forensic Science, no. 5, 2001, pp. 1119–1123.

4 Laurie Calhoun: The phenomenology of paid killing. International Journal of Human Rights, no. 6, 2002, pp. 1–18.

5 Donal MacIntyre – David Wilson – Elisabeth Yardley – Liam Brolan: The British Hitman: 1974-2013. Howard Journal of Criminal Justice, no. 4, 2014, pp. 325–340.

6 Louis B. Schlesinger: i. m. 1119–1123. o.

7 Jegesy Andrea – Harsányi László – Angyal Miklós: Az öngyilkosság következtében meghaltak megelőző egészségi állapota. Népegészségügy, 1995/3., 111–115. o.

8 Konek Sándor: Magyarország öngyilkossági statisztikájához. Statisztikai és Népgazdasági Közlemények és Nemzetgazdasági Szemle, 1867/4., 97–104. o.

9 Zonda Tamás – Paksi Borbála – Veres Előd: Az öngyilkosságok alakulása Magyarországon (1970-2010). KSH, Budapest, 2013, 29–32. o. [KSH Műhelytanulmányok 2.]

Az utólagos felderítés problematikája

Az 1932. július 22-én felvett tanúvallomásában Pipás[10] annyit ismer el, hogy a haláleset után az áldozat fia, *Börcsök Ferenc* szólt neki az apja haláláról, és arra kérte, menjen el a rendőrségre jelenteni a halálesetet. Ezután Börcsökékhez ment, ahol egy szekér elé lovat fogatott be, és elment értesíteni a hatóságokat. Más semmit nem tud mondani az esetről. Továbbá azt is tagadja, hogy Dobáknénak említette volna a Börcsök halálában való bűnrészességét.

Habár az eset után tizenhárom évvel nyilatkozik, Pipás mégis emlékszik, ki szólt neki Börcsök haláláról, de Börcsökné a vallomásában nem nevezi meg egyértelműen az illetőt. Továbbá arra sincs magyarázat, mi szükség volt Pipást a Börcsök-tanyára (vissza)hívni, ha már ott volt *Török János,* Börcsökné bátyja és *Ótott Kálmán* szomszéd is.

1932. július 30-i második vallomásában már[11] elismeri bűnösségét, és részletesebb vallomással szolgál. A Börcsök Istvánnéval való megismerkedését 1916-ra teszi, amikor a közelükben lakott és többször vetőmagot is cserélt Börcsök Istvánnal. 1919 elején egyezett meg Börcsöknével, hogy odamegy a tanyájukra lakni, amiért ötvenezer koronát fizetett. Saját elmondása szerint három héttel korábban költözött oda, de már hónapokkal korábban panaszkodott az ura iszákosságára és elviselhetetlen magatartására. Pipás elmondása szerint Börcsökné ajánlgatta a gyilkosságot mondván, a férje az ital miatt úgyse élne sokáig, ő pedig adna érte búzát, kukoricát és egyéb dolgokat. Sőt megígérte Pipás lányának a kiházasítását is. Az asszony többször zaklatta az akasztás gondolatával, Pipás szerint maga Börcsökné ajánlotta, hogy egy társat is fizet, és a kötél is az ő ötlete volt, mivel ezzel a legkönnyebb az öngyilkosság látszatát kelteni.

Vecsernyés János felbérlését úgy meséli el, ahogy maga Vecsernyés, de arra már nem emlékszik pontosan, vajon *Börcsök Imre* együtt ment-e velük a Börcsök tanyára, vagy csak ketten mentek. Arra sem emlékszik, ő vagy Börcsök Imre zaklatta-e fel a lovakat. A hangra azonban kijött egy lámpával Börcsök István, ekkor Vecsernyés Jánossal egészen az udvarig dulakodtak, ahol ő a kötelet az áldozat nyakára tette. Vecsernyéssel együtt bevonszolták és felakasztották. Börcsökné kérésére átvitték a kamrába a testet, ott akasztották fel újra. Sem Vecsernyés, sem Pipás vallomásban nem szerepel az a Börcsökné által említett körülmény, hogy már majdnem hajnal van, vagyis

10 CSML VII. 2. b. B5336/1932. Pipás Pista vallomási jegyzőkönyve Börcsök István haláláról.
11 CSML VII. 2. b. B5336/1932. Pipás Pista folytatólagos vallomási jegyzőkönyve.

mindez elég kockázatos. Pipás szerint Börcsök Imre is segített a holttest cipelésében, majd a munka végeztével először Vecsernyés, majd ő is távozott a tanyáról. De hajnali öt-hat óra felé Börcsök Ferenc felkeltette, és kérte, menjen el a rendőrökért, mert az apja felakasztotta magát.

Börcsökné még aznap azt mondta *Rieger Pálné*nak, költözzön át a kistanyáról a nagytanyára hozzá. Elmondása szerint egy évig itt élt, és segített a gazdaságban.

Pipás szerint még a háznál volt a halott, mikor Vecsernyés eljött a pénzért, a Börcsökné által adott pénzt Pipás csak továbbadta társának, de annak pontos összegéről nem tudott semmit.

Pipás saját elmondása szerint semmit sem kapott Börcsöknétől, mert haragban váltak el, ezért ott maradt az ő rőzséje, illetve az az öt métermázsa és ötven kilogramm búza, amit megkapott, azt az özvegy nem a sajátjából adta ki, hanem *Szűcs Viktor*nak a búzáját Pipás vágta, és onnan járt neki ez a mennyiség.

Három nappal korábban, július 19-én tanúvallomást tesz *Dobák Antal* halála ügyében, amelyben csak részben ismeri el a bűnösségét.[12]

A családdal való megismerkedését az első világháború utáni évekre teszi, de pontosan nem jelöli meg. Egy környéken laktak, és később, 1921-ben két-három hónapig náluk élt, amíg a szomszédságban lévő tanyát kitatarozta. Ez a tanya is Dobákék tulajdonában állt, *Tombácz Piros* vallomásából tudjuk, hogy Pipás Pista többszöri engedélyével itt találkozhatott a szerelmével.

Pipás azzal folytatja, hogy ismerős viszonyba került a családdal, így lehetősége volt megtapasztalni a rossz viszonyt a házastársak között. Dobákot ideges, indulatos természetű embernek írja le, aki a családját napi rendszerességgel az őrületbe kergette vagy elzavarta otthonról. Tombácz Pirost viselte a legnehezebben, aki akkor eladósorban volt, és emiatt főként a háztól távol vállalt cselédmunkát. Ekkoriban udvarolt a lánynak *Császár József,* aki sógoránál, *Bende István*nál lakott egy környékbeli férfi, *Kispéter András* tanyáján.

Dobákné 1922 elején többször panaszkodott az urára, és elviselhetetlennek tartott élete miatt állt elő azzal az ötlettel, hogy meg kellene ölni a férjét. Ezeket a kijelentéseit Pipáson kívül Bende István és Császár József előtt is megtette. Pipás szerint e két személy egyébként is mindennapos vendég volt a Dobák-tanyán, főként, ha Dobák nem volt otthon, ugyanis az áldozat nem szívelte túlzottan őket.

12 CSML VII. 2. b. B5336/1932. Pipás Pista vallomási jegyzőkönyve Dobák Antal haláláról.

1922 márciusában, egy vasárnap Dobákné Bende Istvánnal meglátogatta Pipást, hogy áthívják a tanyájukra, ahol már Császár József is várta őket. Itt Dobákné előadta, hogy elhatározta a férje megölését, ehhez keresett segítséget: *„nézzed komám, ha úgy lesz, és segítesz a férjem elföldelésében, akkor 1 mm búzát, 1 sonkát és 28 liter bort fogok neked adni”*. Ugyanilyen paraméterekben ajánlott fel díjazást Császárnak és Bendének is. Pipás szerint ők hárman kérdeztek rá, miként képzeli a gyilkosságot Dobákné: *„az anyja ide-oda Istenit, kössétek fel, akkor nem veszik úgy észre, mintha úgy vernétek agyon”*. Pipás tanúvallomása szerint akkoriban nagyon szegény volt, a betevője is alig volt meg, emiatt úgy válaszolt, hogy hajlandó ott lenni, de nem vesz részt a cselekményben, mert mint Dobákné tudja, ő a halott embert nem fogja meg. Ennél a mondatnál egy valamilyen közös tapasztalatra vagy beszélgetésre hivatkozhatott, ahol előkerült kettőjük között a halál és a halottak kérdése. Ám a Pipás-legendának része a hatóságok előtt is vállalt tulajdonsága, hogy akasztás után a halotthoz csak a segédek nyúlhatnak.

Ezen a megbeszélésen történt a gyilkosság dátumának kijelölése, de vallomása szerint ezután távozott, míg Bende és Császár ott maradt, és valószínűleg az emberölés további részleteit beszélték meg.

A kijelölt időpontban, ami a megbeszélés utáni második vagy harmadik nap volt, az esti órákban, körülbelül hét-nyolc óra körül megjelent, amikor még csak a három gyermek volt otthon. Bende és Császár kevéssel utána érkezett, majd negyedórával később Dobák maga lépett be elsőként a konyhába, ahol az elrejtőzött Bende és Császár közösen elkapta, és nyakán a kötéllel vonszolták be a szobába. Ott égő lámpa mellett Pipás várt a három gyerekkel együtt, akik azonnal kiszaladtak, mihelyt az apjukat így látták. Dobákné a konyhaajtóban állt, így akadályozva meg, hogy a gyerekein kívül bárki elhagyja a szobát. Pipás nem látta, ki tette a kötelet még a konyhában Dobák nyakára, de Bende István hozta magával. A szobában az áldozatot Császár fogta meg, míg a kötelet Bende átvetve a mestergerendán öt-hat percig húzta. Pipás nem látta, hogy Dobák rúgkapált volna a kötélen lógva, ezért úgy gondolta, már a konyhában elvesztette az eszméletét, attól hogy kötelet tettek a nyaka köré.

Vallomása szerint nem vett részt a gyilkosságban, csak a halál beállta után Dobákné kérésére vette ki Dobák zsebéből a bugyellárisát és adta oda az asszonynak. Ez olyan momentum, amely megdönti Pipás vallomásának, és legendájának azt a darabját, miszerint sohasem nyúl halotthoz.

Bende leengedte a kötélről a testet, és Császárral együtt kivitték a kamrába. Dobáknéval együtt Pipás is követte őket, a gyermekek is látták, sőt a kamrába

be is mentek, amikor a testet újra felakasztották. Bende egy szakajtót tett a hulla alá, és többször elmozdította, mintha Dobák rúgta volna ki, illetve a szakajtó körül toporgott, mivel Bende megállapította, hogy ugyanolyan csizmát visel, mint amilyen Dobák lábán van. A test elrendezése után egy hordóból bort szívott ki egy pohárba, és megitta, mintha csak az áldozat tette volna az öngyilkossága előtt. Ezek után mindannyian visszamentek a házba, ahol Dobákné borral kínálta őket, de Pipás szerint ő elsőként távozott a lakásába. Pipás nem említi a halott melletti italozást, amit másik két bűntársa egyaránt bevall.

Az eset után két héttel, jóval Dobák temetését követően megkapta Dobáknétól az egy métermázsa búzát, az egy sonkát, valamint huszonnyolc liter bor harmad részét. Ráadásként Dobák tajtékpipája is az övé lett. A másik két bűntárs javadalmazásáról közelebbit nem tud, de biztosra veszi, hogy nem hagyták Dobáknénál, hiszen szegény emberek.

Külön kérdésre előadta, hogy a gerenda, amelyre Dobákot felkötötték, bizonyosan festett volt, de a pontos színről nem tud határozott választ adni; vagy zöld, vagy kék volt. Szintén kérdésre válaszolva közölte, hogy a kapott élelmet felélte, a tajtékpipát viszont egy évvel később eladta egy majsai lakosnak egy kilogramm faggyúért és egy törött pipáért.

Vallomását azzal zárja, hogy a gyilkosságot illetően mindig nyugtalan volt: *„Szinte vártam, mikor fog a rendőrség hozzám egyszer ezért betoppanni.”* Nem tudható biztosan, ez vajon a megfontolt bűnöző félelme a falusi pletykáktól, vagy a bűntudatos elkövető képének megerősítése.

Az ügyben szereplő vádlottak és tanúk között ő az egyetlen, aki nem tud írni-olvasni, ezért az aláírása helyett az ujjlenyomatával, és egy kereszttel jelezte elismerő szándékát. Abban is egyedülálló, hogy nem tudja pontosan a születési dátumát, így az életkora a hivatalos papírokon folyton változott, végül 1886-ot jelölik ki mint legvalószínűbb évet.

Bűntársak a Dobák-gyilkosságban

A Dobák-gyilkosságban Pipás két bűntársa nagyrészt egybehangzó tanúvallomást tett. Bende Istvánnak az eljárás alatt több nevére is fény derült (Horváth János, Bende István, Bönde István, Katona István), ám okát tekintve semmilyen információ sincsen. Az 1932. július 23-i vallomásában az ellene felhozott bűncselekmények miatti gyanúsítást megértette, magát bűnösnek vallotta.[13]

13 CSML VII. 2. b. B5336/1932. Bende István vallomási jegyzőkönyve.

Vallomása szerint a Dobák-gyilkosság előtt két hónappal ismerte meg Pipás Pistát, kíváncsiságból meglátogatta. Nem fejti ki bővebben, de könnyen elképzelhető, hogy Pipás egyfajta látványosság lehetett a szűkebb-szélesebb környezet számára. Később maga Pipás is többször meglátogatta Bendét Kispéter András általa bérelt tanyáján, ahol Császár Józseffel és annak testvérével, Katalinnal élt együtt. Néhány heti ismeretség után felkereste őt Rieger Pálné. A vallomásban a férjezett neve mellett a születési neve *Földi Viktor*ként szerepel, mintha maga a vallomást felvevő rendőr se tudná, hogy nő valójában. A találkozáskor Pipás felveti *„a jó bolt lehetőségét”,* a könnyű pénzszerzés módjaként Dobák Antal megölését tünteti fel. A munka nélküli Bende hajlandó volt rá, ha jól megfizetik. A vallomásából nem derül ki egyértelműen, vajon ki, Pipás vagy a feleség az értelmi szerzője a gyilkosságnak. Később szólt Császár Józsefnek az ügyről, aki szintén hajlandó volt részt venni benne. Nem derül ki biztosan, hogy Pipás kért egy másik bűntársat, vagy Bende saját ötletéről van szó, esetleg önmagát így akarta biztosítani (tudniillik ha a sógora is benne van egy ilyen veszélyes vállalkozásban, akkor számíthat rá veszély esetén). Pipás legközelebb már úgy jön megbeszélni a tennivalókat, hogy előtte egyeztetett Császárral. Ez azt implikálja, hogy akár Bende, akár Pipás vagy Dobákné ötlete volt a további bűnsegéd, a tett végrehajtásának koordinálása Pipás kezében összpontosult. Vallomásában leszögezte, hárman fogják akasztással elkövetni a gyilkosságot, ám magának az ölési módnak az ötletadójára már nem emlékezett egyértelműen, de úgy vélte, Dobákné lehetett, aki egyszer jelen volt egy megbeszélésükön. Éppen ezen az alkalmon ígért a feleség egy bárányt, százezer koronát fejenként, ötven liter bort és egy sonkát.

Többször beszéltek az elkövetés mikéntjéről Pipással és Császárral is, utóbbi testvére, Bende akkori vadházastársa is hallott sok mindent, de a cselekményben tevőlegesen nem vett részt. A Dobák-tanyánál is jártak, magával Dobák Antallal is találkoztak, de Bende elmondása szerint egyáltalán nem voltak odajáró vendégek, mint ahogy azt Pipás állította. A Dobákkal való első találkozás után a feleséggel és Pipással megbeszélték, hogy Dobákné jelez aznap, amikor a férjével későn jön haza, hogy ők már nyugodtan várhassák a házban.

1922. március 22-én értesítette Dobákné Pipást, aki Bendéhez ment a hírrel: ma este lesz a gyilkosság. Ez az információ is arra világít rá, hogy az ügy valós középpontja és kapcsolattartója Pipás volt. Császár Józsefet is értesítve hárman érkeztek meg a tanyára, a három kisgyerek volt csak otthon. A Bende által beszerzett istrángot Pipás fogta a konyhaajtó mögött, míg Bende és Csá-

szár úgy helyezkedett el, hogy az előbbi az áldozat testét, illetve a torkát tudja elkapni, mialatt Pipás a nyakára teszi a hurkolt kötelet. Ennek megfelelően cselekedtek, a szobába becipelve a zöld mestergerendára húzta fel Pipás és Császár, Bende pedig továbbra is Dobák kezét fogta le. Itt Bende megemlíti, hogy zöld volt a gerenda, amit a rendőrök már kérdeztek Pipástól.

Amikor először lefogták, Bende szerint csak annyit mondott, hogy *„Vigyázzatok, a pipám eltörik”*. Majd így kiáltott: *„Ne bántsatok.”* A gyerekek az akasztást nem is látva kirohantak, az anyjuk viszont a konyhaajtóban állva figyelt. Miután kiszenvedett, leemelték a testet, az egyik kezét Császár, a másikat Bende vitte, miközben Pipás a lábait fogta; így vitték át a kamrába. A két társ fogta a testet, és legjobb emlékezete szerint ő maga akasztotta fel másodszorra. Kért egy szakajtót, amit többször elmozdítva öngyilkosság hatását akarta kelteni. A vádlottak kivétel nélkül egyetértettek a szakajtó létében és szerepében, de nem tudjuk, ki találta ki az ötletet, egyáltalán előkészített ötlet-e, vagy a helyszínen találták ki.

Utána lopótökkel hordóból szívott bort töltöttek, Pipás az öngyújtójával világított. Bende szerint csak a három tettes ivott, vagyis Dobákné nem. Hiába volt már teljes jogúan az ő háza, hiába nézte végig a férje halálát, nem ivott; adódik a kérdés vajon neki nőként nem volt szabad a férje teteme mellett férfiakkal poharaznia, vagy nem volt gyomra ehhez. Minthogy a házba visszatérve már együtt iszik az elkövetőkkel, valószínűbb az utóbbi. Az öngyújtó kérdése pedig megkérdőjelezi Pipás vallomását az ő szegénységéről, illetve pénztelenségéről. A Szeged környéki tanyavilágban folytatott kutatómunkánk[14] részeként helybeli idős emberekkel készítettem interjút, akik vagy látták gyerekként Pipás Pistát, vagy hallottak róla. *Rozsnyói Mária* említette, hogy az első világháború után többen készítettek töltényekből és egyéb tűzkőféle eszközökből öngyújtókat. Ám ezek az emberek vagy birtokos gazdák vagy állami alkalmazásban lévő emberek voltak.[15] Nem jelent feltétlenül jómódúságot az öngyújtó birtoklása, lehetséges, hogy amint Dobák tajtékpipája, úgy az öngyújtó is egy felakasztott embertől *„megszerzett ajándék”*.

Miután egy fél pohár bort otthagytak a hordó tetején Dobák utolsó italozását megkreálva, bementek a házba, ahol már Dobákné is csatlakozott hozzájuk, ott javasolta, hogy le kellene venni a birkaól ajtaját, így az állatok majd összetapossák a helyszínen a lábnyomokat. Ráadásul a rendőröknek állíthatja, ő erre a hangra ment ki és vette észre férje öngyilkosságát. Dobákné csak

14 Pipás Pista történetéből dokumentum-, illetve játékfilm készül a szerző közreműködésével.
15 Rozsnyói Mária-interjú. Öreg-Átokháza, 2010. június 30.

az utóbbi szempontot említette saját vallomásában, és azt is Bendének tulajdonította. Bende szerint Rieger Pálné ment ki elintézni, elrendezni az egészet. Addig ő megkérte Dobáknét, hogy miután a rendőrök elmennek, és a holttestet leszedik, a kötelet szerezze meg valahogy tőlük, és égesse el, amilyen gyorsan csak tudja. Felvetődhet a kérdés, miért volt ez ilyen fontos. Egyfelől akkor, ha éppen ilyen kötélből nem volt a Dobák-tanyán, másfelől a kötélre kötött csomó miatt. Ha az akasztókötélen talált csomót a rendőrök összevetik a házban egyéb helyen található, bizonyosan az áldozattól származó csomóval, és az nem egyezik, az megdöntheti az öngyilkosság teóriáját. Dobák temetése után Rieger Pálné szólt Bendének arról, hogy Dobákné a kemencébe dobta a kötelet. Vagyis a kapcsolattartás a gyilkosság után is Pipás Pistán keresztül történt.

Bende szerint hárman közösen távoztak éjjel három körül, amikor is megkapták hordóban az ötven liter bort, ebből már Bendééknél két cserépköcsögben megkapta a részét Pipás is. Távozása után *Császár Katalin* kérdésére közölték, hogy minden rendben van, majd a nő ivott még velük a borból.

Öt-hat nappal a történtek után Rieger Pálnéval közösen Dobáknéhoz mentek a fizetségért, mindketten kaptak egy-egy darabot egy disznólábból, és valamennyi pénzt. Két hét múlva Pipással megint megjelentek, amikor is Bendééknél elosztották a húsz kilogramm rozslisztet.

Császár fizetségéért is Bende ment mindkét alkalommal, vagyis a két férfi kapott annyit, mint Pipás egyedül. Ez azt feltételezi, hogy Pipásnak többet kellett tennie a gyilkosságban, mint egy háromfős elkövetői csoport egyik tagjának. Főként, hogy a gyilkosság után két hónappal Bende már csak egyedül kért Dobáknétól pénzt vagy kenyeret. Az özvegy adott neki ötvenezer koronát és négy-öt kilónyi rozskenyeret. Vagyis habár Pipás a jövedelmi helyzetét tekintve egy szintre sorolta magát Bendével, ő az adatok szerint mégsem szorult rá ilyen adományokra.

Bende azt vallja, semmit sem tud Börcsök István haláláról, csak az önakasztást hallotta. Elképzelhető, hogy nem akart magának vagy Pipásnak ártani azzal, hogy mégis elmond valamit erről, de tegyük fel, hogy igazat mond; ebben az esetben ő nem is hallhatta Pipás szájából a történetet, vagyis azt Riegerné megnyugtatásképpen egyedül Dobáknénak mondta el. Ha ez igaz, akkor nehezen hihető, hogy az akasztás Dobákné ötlete lett volna. Az egyik bűntárs mégis úgy emlékszik, Dobákné javasolta ezt az ötletet, tehát egy merész feltételezéssel élve Rieger Pálné személyében egy igen csavaros eszű bűnözőt ismerhetünk meg, aki felajánlja szolgálatait a *„kiszolgáltatottnak tűnő”* feleségeknek, korábbi akasztásaiból egy esetet (bizalmat akar éb-

reszteni, de önvédelmi okokból nem mond többet) megoszt a kvázi felbujtóval, akit aztán a bűntársak előtt már valódi felbujtóként tud felmutatni. Bende a vallomásában szinte kivétel nélkül a férjezett nevén említi Pipást, a gyilkosság tervezésénél egy alkalommal viszont ál- és valódi nevével együtt. De ennek hivatalos megfogalmazása miatt nem tudható, hogy ez nem a hivatalos szervek munkája-e.

Császár József 1932. július 25-i vallomásában a terhére rótt cselekményeket megértette, magát bűnösnek érzi.[16] 1920 óta Kiskunhalason és környékén élt, amikor 1922 tavaszán elment *Horváth János*hoz (Császár a vallomásában következetesen így hívja Bende Istvánt), aki az ő testvérével élt vadházasságban. Császártól megtudjuk, hogy Császár Katalin férjezett asszony volt *Vecsernyés Ferencné* néven. Tehát egy-két hónappal az akasztás előtt érkezett, és a haláleset után még három-négy hétig maradt, de eredetileg nem az ügy miatt jött. Érkezésekor Pipás többször járt át Bendéékhez, de ő nem hallotta a gyilkosságról beszélni. Viszont a testvére élettársával több alkalommal vonultak el kettesben sugdolózni.

A gyilkosság előtt négy-öt nappal Bende kétszer is szólt neki arról, hogy Pipás Pista szerint Dobákné *„el akarja tétetni láb alól a férjét”*[17]. Adna ezért ötven liter bort, egy birkát, gabonát, sonkát és pénzt, de az összegre már a vallomásában nem emlékezett.

Először nem kívánt benne részt vállalni, de a tél miatt régóta nem volt munkája, és így éppen Bende tartotta el. Ez egyszerre magyarázhatja, miért ment a testvére szeretője mellé élni, és miért vállalta a részvételt a gyilkosságban. Császár szerint Pipás a Dobák felakasztása előtti nap is elment hozzájuk a gyilkosság kivitelezéséről beszélni. Vagyis nem csak a tett elkövetése napján ment át Pipás hozzájuk, ahogy azt Bende állította. De Császár és Bende vallomása megegyezik abban, hogy Pipás a gyilkosság estéjén eljött, kettesben beszélgetett Bendével, majd mindketten Császár elé állva kérték a segítségét. Pipás ekkor is megnyugtatta Császárt, hogy Dobákné elrendezett mindent, nekik csak át kell menniük aznap este. Császár vallomásában nem emlékezett rá, ki hozta magával a kötelet, ő már csak Dobák nyakán látta meg. Bende hangsúlyozhatta ugyan a saját fontosságát azzal, hogy ő szerezte be a kötelet, de ha tekintetbe vesszük Pipás feltételezhető óvatosságát, akkor Pipás nem akart hozzá köthető nyomokat hagyni, ha Dobákné esetleg mégsem tudja a kötelet elégetni.

16 CSML VII. 2. b. B5336/1932. Császár József vallomási jegyzőkönyve.
17 Uo.

A Dobák-tanyára érve csak a három gyereket találták otthon, Császár szerint Pipás megkérdezte tőlük, hol az apjuk, ők pedig azt mondták, hogy a szomszédban. Egy ilyen helyzetben érdemes feltenni a kérdést, ki szólítja meg a gyerekeket; minden valószínűség szerint az, aki a legtöbbet találkozik velük, és nem érzik idegennek. Ez megkérdőjelezi Pipás azon állítását, hogy Bende és Császár gyakorta járt a házhoz. Császár szerint a gyerekeknek nem mondtak semmit, a szobában beszélgettek, amíg ők játszottak. Este kilenc óra felé az egyik kisgyerek a kutyaugatás miatt kiszaladt az udvarra, és visszatérve szólt a három férfinak, hogy közelednek a szülei.

Lépéseket hallva Pipás Császárt és Bendét kiküldte a konyhába, ahol az előbbi a szabadkémény alá, a másik az ajtó mögé rejtőzött. Pipás a szobában maradt, Bende a bejövő Dobáknak a kezét kapta el, Császár pedig a torkát, hogy könnyebben tudják a szoba felé tuszkolni. Onnan lépett elő Pipás, Császár szerint a kabátja alól elővette az instrángot, amit meghurkolva Dobák nyakára tett, és meghúzta. Pipás a mestergerendán átdobva a kötelet Császárral együtt felhúzta a testet. Bende lefogta a testet, mert Dobák le akarta szedni a nyakáról a kötelet. A három gyerek kiszaladt az udvarra, Császár emlékezete szerint tízpercnyi küzdelem után vették észre az áldozat halálát. Dobákné Pipásnak szólt, vegye ki a férje zsebéből a pénzt. Ki is vette, odaadta a nőnek, majd leeresztették a testet, és kint a kamrában Bende kötötte fel. Arra nem emlékezett, ki hol fogta, de mindannyian vitték. Ez némiképp megkérdőjelezi Pipás állítását, miszerint nem nyúl halotthoz. Illetve Dobákné kérése Császár vallomásában is egyértelműen Pipásnak szólt *(„Pipás, vedd ki a zsebéből a pénzt”*[18]*)*.

A szakajtó használatát ő is megemlíti, és az utána következő poharazgatást úgyszintén. Dobákné kérésére Pipás és Bende vitt be bort a házba, ahol tovább folytatták az iszogatást, de Császár, a saját elmondása szerint, annyira izgatott volt, már pár pohár bortól berúgott és elaludt. Nem emlékszik, ki keltette fel, de emlékezete szerint hárman mentek hazafelé. A haza vitt bort, az ebből Pipásnak kiadott részt szinte ugyanúgy beszéli el, mint Bende, de sokkal kevesebbre emlékszik, és a Katalin nevű testvére kérdéseit meg sem említi.

Harmadnapra Pipás megjelent náluk, és beszámolt a fejleményekről, hogy a rendőrök megállapították az öngyilkosságot. Itt szintén a kapcsolattartó pozíciója mutatkozhatott meg, hiszen egyfelől az általa hozott információkkal meg tudta nyugtatni a bűntársait, másfelől fel tudta mérni, kiknek beszélhet-

18 CSML VII. 2. b. B5336/1932. Császár József vallomási jegyzőkönyve.

tek az esetről, mennyire viselte meg őket, bármilyen formában gyanúba hozták-e magukat.

Császár szerint Bende és Pipás társaságában ő is elment Dobáknéhoz elkérni a javadalmazásukat. A Bende által említett két találkozóból ő csak az elsőn volt ott, ahol emlékei szerint egy darab sonkát kaptak kétfelé vágva. Itt ő is megerősíti, Bendével közösen kapott annyit, mint Pipás. Pár héttel később már távozott Bendééktől, akit egyébként 1927-ben látott utoljára. Ám távozása előtt Bende és Pipás egyaránt megfenyegette, ha bárkinek beszél az esetről, akkor megölik.

Külön kérdésre előadta, ott-tartózkodása alatt Bende elmondta neki, hogy a Tanácsköztársaság idején Kiskunfélegyházán hóhérként működött. Ezt valószínűleg Pipás is tudta, ezért kérhette fel bűntársnak.

Bűntárs a Börcsök-gyilkosságban

1932. július 30-i vallomásában a vádat megértette, a bűnösségét elismerte. Saját elmondása szerint tizenegy-tizenkét éves kora óta ismeri Pipást, mert ekkor kezdett dolgozni nála. Ottlétéről annyit jegyez meg: Pipás *„mindig úgy szerepelt, mint férfi és férfiruhában is járt, de sokan beszélték, hogy tulajdonképpen nő”*[19]. Vecsernyés 1900-ban született tehát az 1910-es évek elejéről beszélt így, vagyis Pipás már a férjével való együttélése idején is férfiként viselkedett.

1919 májusában Pipás felkereste Vecsernyést a lakhelyén, és közölte vele, nagy összeget kereshet, ha segít Börcsök István felakasztásában. Vecsernyés konkrét összeg megbeszélése nélkül egyezett bele munkanélkülisége miatt (is). 1922. május 22-én este jött el újra Pipás, közölte Vecsernyéssel, hogy most fogják megölni Börcsök Istvánt. A tanyára 23 óra tájban értek, de ott emlékezete szerint nem találkoztak Börcsök Imrével. Éjjel háromig vártak, mikor Pipás ütögetni kezdte a lovak fenekét, ennek a hangjára jött ki Börcsök István. Vecsernyés megpróbálta lefogni ugyan, de verekedéssé fajult a helyzet már az udvaron, ahol Pipás fogta le a férjet, majd Vecsernyéssel visszacipelték az istállóba. Pipás az alacsony gerenda ellenére felakasztotta Börcsököt. Vecsernyés nem emlékszik, mikor került elő a kötél, arra se, hogy Pipás magával hozta-e egyáltalán, vagy ott szedte össze. Az akasztás idején látta meg először Börcsök Imrét is.

19 CSML VII. 2. b. B5336/1932. Vecsernyés János vallomási jegyzőkönyve.

Vecsernyés vallomása alapján a gyilkosságot nemcsak hogy Pipás maga készítette elő és koordinálta, hanem a verekedésnél is az ő segítségével lehetett a gyilkosságot befejezni. Körülbelül negyedóra múlva vették le, és vitték át a kamrába, ahol megint Pipás húzta fel, amíg Vecsernyés a testet emelte. Ezután Vecsernyés állítólag azonnal hazament, tehát nem maradtak tovább a házban, ahogy azt Börcsök Istvánné vallotta.

Egy héttel később jött el újra érdeklődni, Pipás ekkor adott neki ezer koronát, amit Vecsernyés elmondása szerint addig tartogatott, míg teljesen értéktelen lett. Pipásról mást nem tudott meg, azt sem, vajon Pipás biztatta-e fel Börcsöknét a gyilkosságra, vagy fordítva. Mindkét esetben a bűntársak egyetértettek abban, hogy Pipás tette fel az áldozatokra a kötelet.

Az áldozatok családjában lévő gyerekek tanú-, illetve Börcsök Imre esetében vádlotti vallomásai nem tartalmaznak további releváns információkat. Egyetlenegy szempontból fontos Börcsök Imre és Dobák Mária vallomása, mindketten az egész esetből leginkább Pipás Pistára emlékeznek, és bűntársainak időnkénti megemlítésétől eltekintve emlékeikben az esemény egészére ráülepedett a férfias Pipás Pista személye.[20] Ennyiben teljesen illik rá a John Money-féle transzszexuális-definíció, ugyanis *„az egyik nem morfológiai és szaporodási sajátosságaival rendelkezik, miközben kitartóan a másik nem szerepeire és kiváltságaira tart igényt”*[21].

A sorozatgyilkos mint bérgyilkosságokat elkövető értelmezése

Milyen feltételek okozhatták és ezzel párhuzamosan segíthették elő Rieger Pálné Fődi Viktória átváltozását Pipás Pistává? *René Grémaux* a férfivá vált nőket elemezte a Balkánon történt esetek[22] segítségével, ő a Pipáshoz hasonló nőket *„átlépetteknek”* nevezte. Ezzel a konkrét ruhaváltás mellett a szellemi metamorfózisra utalva, ám a szó ilyetén használata mégis valamiféle befejezettséget sugall, ami ezekben az esetekben inkább kérdéses, mintsem magától értődő. Emiatt is érdemesebbnek látom magyarul átlépőkként hivat-

20 CSML VII. 2. b. B5336/1932. Börcsök Imre vallomási jegyzőkönyve, Dobák Mária tanúkihallgatási jegyzőkönyve.

21 John Money: A transzszexualizmus és a feminológia elvei. In: Evelyne Sullerot (szerk.): A női nem – tények és kérdőjelek. Gondolat Kiadó, Budapest, 1983, 249–257., különösen 249. o.

22 René Grémaux: Woman becomes man in the Balkans. In: Gilbert Herdt (ed.): Third Sex Third Gender – Beyond Sexual Dimorphism in Culture and History. Zone Books, New York, 1994, pp. 241–284.

kozni rá. Ám az igazi probléma, hogy nem tudja megindokolni, miért fordulnak elő ilyen nagyszámban Kelet-Európában ezek a típusú nők. Egyáltalán valóban csak kelet-európai sajátosságról van-e szó?

Átmeneti rítusok[23] című könyvének *A materiális átmenet* című fejezetében *Arnold von Gennep* használja a hasonlatot az országok határaival kapcsolatban, amely szerint a modern kori országhatárok alapján a különböző államok *„összeérnek”,* de ezeket a királyságokat a korai feudalizmus évszázadaiban egy széles, semleges sáv vette körül. Ezek a földsávok egyes kultúrák számára szentnek számítottak, de minden esetben különösnek minősültek az ott-tartózkodók, hiszen két ország (világ) határán voltak. Ennek a konkrét helyzetnek a megfelelőjét megtalálta olyan vallási, mágikus és profán helyzetekben, amelyeket összefoglalóan határhelyzeti rítusoknak nevezett, ennek részei az elválasztó, határhelyzet alatti és a befogadó rítusok. Diszkurzív szómágiával úgy fogalmazhatunk Pipás Pista *„többszörös határsértő”,* aki a szerb–magyar határon élt[24], és biológiailag nőként társadalmi nemét férfira kívánta változtatni. Többszörösségének utolsó *„szorzója”* a bűnözői karrierje mint a társadalmi szabályok megsértője.

Grémaux értelmezésében az úgynevezett átlépők megteremtődésének strukturális előfeltétele a férfi szerepének és a maszkulinitásnak az óriási tisztelete a kultúrában. Egy háztartás – ha társadalmi, gazdasági, morális és kulturális tényezők összességének fogadjuk el – halálra van ítélve, ha eltűnik belőle a férfi örökös. Grémaux-nak az e gondolatot kifejtő értelmezésével *(„Egy-egy ilyen család státusvesztést szenved el a közösségén belül…”)* nem teljesen értek egyet, hiszen a jól kiházasítható lány is jelenthet értéket, ahogy a Nagy-Alföldet néprajzi szempontból „megfogalmazni” kívánó *Kiss Lajos* is állítja.[25]

Grémaux további vitatható megállapításai remek értelmezési lehetőséget adnak Pipás magánéletének megértéséhez. A tradicionális kontextusban a *„maszkulinizált nők”* összekapcsolódnak az örökké tartó szüzességgel, mivel a maszkulinitás és a szüzesség is ugyanazt jelképezi, a tisztaságot és az erőt. A szüzesség praktikus hozadékának tekinti, hogy megóvja a nőket a törvénytelen gyerekek lehetőségétől, míg a férfierőhöz kapcsolja, hogy a gyerekek

23 Arnold van Gennep: Átmeneti rítusok. L’Harmattan–MTA Néprajzi Kutatóintézete–PTE Néprajz Kulturális Antropológia Tanszék, Budapest, 2007, 54–55. o.

24 Kutatómunkánk során Tompa egykori cigánysorán ráakadtunk id. Fliber Antalra, aki Fliber Józsefnek, a szóbeszéd szerint Pipás Pista kocsistársának a fia. A beszélgetéskor elmondta, hogy az apjával rengeteg árut cseréltek át Szeged és Szabadka között. Ez az eufemisztikus megfogalmazás nagyrészt csempészetet takart. Fliber Antal-interjú. Tompa, 2010. július 4.

25 Kiss Lajos: A szegény emberek élete, 2. kötet. Gondolat Kiadó, Budapest, 1981, 343–384. o.

első számú kreátora a férfi. Noha Grémaux-val ellentétben úgy gondolom, a tradicionális kultúra inkább köti a szüzességet a bűn előtti állapothoz, mint a férfierőhöz (jó példája ennek a hajadon fogalma és képe), maga Grémaux is a bizonytalanság és az egyenetlenség figyelembevételével kapcsolja össze a maszkulin nőket a szüzességgel, hogy feltehesse a kérdést: vajon ezek a *„szüzek”* mindig tartózkodni kívántak a férfiakkal folytatott szexuális élményektől, vagy inkább jobban élvezték a szexualitás szabadságát?

A heteroszexualitás hiányának ennyire plasztikus megjelenése inkább kérdéses Pipás esetében, az elmeorvosi vizsgálatának első részében Pipás közlései jelzik ezeket a problémákat.[26] Valószínűleg 1886-ban született Szeged-Átokházán, de sem a hónapot, sem a napot nem tudja. Apja és anyja az eljárás idején már elhalálozott, az előbbi gutaütésben, a másik száraz hektikában, az öt testvéréből pedig csak ketten nőttek fel. András testvére azonban *Ember Judit* kutatásai szerint felakasztotta magát, de ezzel nem Pipást gyanúsították, mivel a fiú többször emlegette öngyilkos gondolatait. Állítólag testi és szellemi fogyatékos és süket volt, és haláláig Pipás gondozta.[27]

Tizenöt-tizenhat éves koráig pásztorként dolgozott, mígnem tizenhét évesen feleségül vette *Rieger Pál,* akit az elmondása szerint sohasem szeretett, a szülei erőltették a házasságot. A férjével való szexuális együttlétet egyáltalán nem élvezte; hat gyermeket szült, közülük egy maradt életben. Az együtt töltött hét évben nagyon rosszul éltek, nagy valószínűséggel a férj agresszív viselkedése miatt. A hét év alatt született hat gyerek még egy kora újkori társadalomban is súlyos megterhelés lett volna egy nőnek, az pedig, hogy ebből csupán egy maradt életben, más kérdéseket is felvet, például, hogy történt-e csecsemőgyilkosság, vagy bármilyen más erőszak. E tekintetben semmilyen adatunk nincs.

„A szegény asszony élete a libapásztorkodással kezdődik”[28] – ezzel a mondattal indítja Kiss Lajos kötetének a nehezen élő alföldi nőkről szóló részét. Nem tudjuk, milyen állatok legeltetését bízták Pipás Pistára (akkor még Fődi Viktóriára), de a Kiss Lajos-i struktúrát követve tizenkét-tizennégy évesen a pásztorkodásból kinőve egy szegény lány cseléd vagy pesztonka feladatokat kap. Pipás viszont még tizenöt évesen is állatok terelésével foglalkozott, elképzelhető, hogy nagyobb testű jószágokat (marha, disznó, birka) is rábíztak. Ember Judit kutatásai között egy interjúban Rieger Pál egyik, még

26 CSML VII. 2. b. B5336/1932. Pipás Pista/Rieger Pálné elmeorvosi jelentése.
27 Ember Judit: Pipás Pista. In: Zalán Vince (szerk.): Az Ember-lépték. Osiris Kiadó, Budapest, 2006, 187. o.
28 Kiss Lajos: i. m. 5. o.

a Pipással kötött házassága előtt született lánya úgy tudta, *Fődi Lukács,* Pipás apja juhászember volt.[29] A falusi, tanyasi társadalomban a pásztorkodó emberek kötetlenebb, szabadabb életvitele közismert toposza a népdaloknak, de jelen esetben nem tudjuk, vajon saját állatai voltak, vagy csupán javadalom fejében vállalt pásztormunkát. Ám ha hihetünk Pipásnak, úgy került feleségként egy férj hatalma alá, hogy előtte még soha nem végzett szolgálói munkát, hanem a vele egyidős fiúk feladatát végezte mint állatterelő. Ennek a viszonylagos szabadságnak a vágya elkísérhette házasként.

A Rieger Pállal kötött frigy Kiss Lajos szerint nem nevezhető késői házasságnak Pipás szempontjából, mivel *„a szegény ember lánya”* közelébe, ha *„otthon tartották”,* tizenhat-tizenhét évesen *„beeresztették a kérőt”*[30]. Rieger viszont ötven körüli ember volt, több gyerekkel, talán öreg korára egy megbízható ápolót kívánt maga mellé, ezért elnézte jövendőbelije rossz szokásait. Pipás saját elmondása szerint tizenhárom éves kora óta pipázott, a kórházban szokott rá, ahol kezelték. A tárgyalásán a bíró kérdésére ismerte el, az orvosok ajánlották neki a betegségére, de később már nem tudta elhagyni.[31] Tizenöt-tizenhat évesen úgy bedagadt a lába, hogy járni is alig bírt. Utóbbi magyarázat lehet arra, miért éppen ennyi idős koráig foglalkozott pásztorkodással. Saját bevallása[32] szerint fiatalon többször ivott, részeg is gyakran volt, de soha nem keveredett kocsmai verekedésbe. Ezeknek akár egyike is elég alapot nyújthatott olyan pletykákhoz, szóbeszédekhez, amelyek megnehezítették a házasodását.

Rieger Pál egyik veje úgy nyilatkozott Pipás férjéről, mint nagydarab emberről, aki igen erős volt, az italt és a kártyát is nagyon szerette, de soha nem bántott senkit.

Összességében a házasság rossz tapasztalatai származhattak konkrét erőszakból, vagy csupán az uralkodni vágyó férfi magatartásából, aki a feleségétől egyfajta *„szolgai”* magatartást követelt, ez pedig idegenül hatott az évekig szabadon élő pásztorlánynak.

Pipás hét év után megelégelte a helyzetét, saját szavai szerint férfiruhába öltözött, mert úgy gondolta, többet kereshet így. Dolgozott kocsisként, cselédként és napszámos munkában. A büntetőügy miatt kezdeményezett elmevizsgálaton azt vallotta, csak a munka és a jobb fizetség reményében öltözött férfinak.

29 Ember Judit: i. m. 151. o.
30 Kiss Lajos: i. m. 148. o.
31 Délmagyarország, 1933. január 11.
32 CSML VII. 2. b. B5336/1932. Pipás Pista/Rieger Pálné elmeorvosi jelentése.

A Pipás-ügy narratíváinak átalakulása vagy további szálakkal való bővülése a korszak sajtójának is tulajdonítható. *Az Est* 1932. július 24-i számában[33] a következő címmel jelent meg cikk: *Felakasztotta férjét egy pusztamérgesi asszony. – Tíz év múlva derült ki a bűne.* Július 29-re[34] már pontosabb információkat szerzett az országos napilap: *Miért lett férfi Pipás Pista és hogyan követett el két gyilkosságot?* Itt a gyilkosságok helyett már inkább a transzvesztitizmus egyéni indítóokait boncolgatta a cikkíró, főként a férfiak brutális viselkedésével magyarázva a kérdést. A *Délmagyarország* ugyanezen a napon[35] inkább az ügyészség dilemmájával foglalkozott: a férfiak vagy a nők közé zárják-e Pipás Pistát? Hiszen nő lévén a férfiakhoz mégsem tehették, de egy nadrágos ember az asszonyok közé se kerülhet, ezért úgy döntöttek, szoknyát adnak rá. A cikk szerint a gyanúsított feszengett az új ruhájában, még fél óra múlva is az övet kereste a szoknyán. A társadalmi nemi hovatartozás szenzációvá emelésén túl plauzibilis magyarázatkeresés helyett az újságírók a brutális gyilkos fogalma alá söpörték az ügyet. A téma 1933 elején került ismét napirendre: január 11-én az ítélethirdetés közeledtével[36] már *Az Est* címlapjára kerülő ügyben elsőként a brutális gyilkosok várható súlyos büntetése volt a téma, de ez a következő szövegközi kiemeléssel: *„Pipás Pista babos kékszoknyában”* bonyolódott. *Az Est* tudósítója a kegyetlen gyilkos és bűnbánó anya fogalmainak antagonizmusát a *„nőiség, mint álca”* segítségével oldotta fel.

A január 14-i ítélethirdetést *Az Est* már csupán a harmadik oldalon hozta, hiába szabtak ki halálos ítéletet Pipásra. A tárgyaláson hallható védő- és vádbeszédek nagyon kevéssé reflektáltak egymásra. Pipás Pista védője, *dr. Fekete László* megállapította: *„Semmi oka nem volt arra, hogy elhagyja a házát […] társtalanul bolyongjon az országban, férfiruhában.”* Az egész védőbeszédét úgy építette fel, hogy Pipás nem más, mint egy szexuális aberráció áldozata, amit gonosz asszonyok kihasználtak.[37] Az ügyész a vádlott nemiségével nem is törődve egy kalap alá vette az összes elkövetőt, és beszéde az előre megfontoltságuk hangsúlyozásában merült ki.[38]

1933 végén *Horthy Miklós*nak írt kegyelmi kérvényt[39], ebben nem is mentegette testi és szellemi elváltozását, de az előre megfontoltságot tagadta. Bör-

33 Az Est, 1932. július 24., 6. o.
34 Uo.
35 Délmagyarország, július 29., 1. o.
36 Az Est, 1933. január 11., 1. o.
37 CSML VII. 2. b. B5336/1932. Dr. Fekete László védőbeszéde.
38 CSML VII. 2. b. B5336/1932. Ügyészi vádbeszéd.
39 CSML VII. 2. b. B5336/1932. Pipás Pista/Rieger Pálné kegyelmi kérvénye.

csökné szembesítéskori beismerésére hivatkozott, miszerint a gyilkosságot nem ő találta ki, hanem a feleség. Elképzelhető, hogy a lánya kiházasítása, a tartós megtelepedés reménye miatt döntött a gyilkosság mellett. Ember Judit kutatásában is található egy nő, *Kiss Antalné Császár Marcsa,* akit Pipás menyasszonyként kívánt magának. A nő elbeszélése szerint meg akarta ölni az urát, hogy együtt élhessen vele, de Kiss Antalné megleste pisilés közben, és így szólt: *„Meglestem én magát, de magának is csak olyan tepsije van, mint nekem, Pista bácsi. Az uramnak pikulája is van hozzá. Az ember rossz, az igaz, de a pikulája, az jó. Hű de mérges lett! Nem szólt többé énhozzám egész úton.”*[40] Minden önállóságra törekvő, vándorló életmódja ellenére lehetett letelepedési szándéka, hogy férfiként egy tanyai háztartás családfője legyen. Börcsökné ennek meghiúsulását Pipás munkakerülésében jelölte meg, maga Pipás csak az összekülönbözést jegyzi meg. Összességében a családi élet kudarcát fordított helyzetben már megélte, most mintha a másik oldalát is megtapasztalta volna.

A Dobák-gyilkosságnál már jelentősebb tervezést igénylő ügyről lehetett szó. A Börcsök esetében még a későbbi együttélés miatt egy az érintettségét igazoló valóságos helyzetet használhatott fel, azonban a Dobák-gyilkosságnál már minden személyes befolyásolásra vonatkozó részlet konfabuláltnak tűnt, mivel a családtól eltávolodott az ölés után. Noha minden vallomás megegyezik abban, hogy Pipás járt a legtöbbet mindenkihez információkat hozni, a gyilkosságot megbeszélni. Sőt vele mentek a gyilkosság fizetségéért is. Vagyis az elkövetés legfontosabb organizátoraként teljesíti a bérgyilkosság legfontosabb, főként önvédelmi szempontjait.[41] Elsőként önkezűségnek állítja be az eseteket, az elkövetéshez használt gyilkos eszköz alkalmi, közvetlenül nem köthető az elkövetőhöz. Általában a bérgyilkos nem ismerkedik meg az áldozattal személyesen, kivéve, ha így tud kapcsolatot teremteni azzal, akinek érdekében áll a kijelölt személy halála.

A statisztikai szempontból a női bűnözés magyar aranykorában élő Pipás a gyilkosságokban részt vevőket mind megfenyegette a tettek elkövetése után, így biztosítva a hallgatásukat. Ezzel akár akaratlanul, de akár tudatosan is gerjesztve a tőle való félelmet, ami erősíthette sorozatgyilkosi minőségét mint a paraszti társadalom hierarchiájának felborítóját. Mint már esett róla szó, a XIX. század végén *Kraft-Ebing* a homoszexualitáshoz sorolta a transzvesztitizmust, mondván a társadalmi konvenciók ellen fellépő magatartásnak minősül.

---

40 Ember Judit: i. m. 164. o.

41 A magyarországi bérgyilkossággal kapcsolatos hiányos információk miatt nagyon hasznosnak bizonyult Kovács Lajos tipológiája és szempontjai.

Elkövetési helyszínek mint a bérgyilkosság felderítését elősegítő információk

Liam Brolan és kutatótársai egy nagymintás kutatás alapján azt vizsgálták, hogy milyen következtetéseket lehet levonni az elkövetés helyszíne alapján. A legjellemzőbbnek az áldozat otthona (26 százalék) számított, majd az elkerített, nyilvános tér (22), ez után a nyitott tér (19) bizonyult a harmadik legjellemzőbbnek. A kutatásuk alapján látható, hogy a helyszín Pipás Pista ügyét alapul véve nem változott meg jelentősen, inkább a felkészülés módja alakult át, amennyiben a fizikai anyagmaradványok elkerülése érdekében a kontaktust kerülő magatartás gyakori, amelyet az emel ki, hogy előre megtervezett helyről főként lőfegyverrel történik az emberölés. A különbségeket elsősorban az jelenti, hogy nincs szándék az emberölés tényének elfedésére, vagyis a beállított helyszín megalkotására. Ugyanakkor *Budvári Róbert* egykori, kiváló igazságügyi orvos szakértő tapasztalataira hivatkozva fontos megállapítani, hogy a leplezett emberölések a legritkább esetben adnak arra lehetőséget, hogy felderítsék őket, továbbá listázzák és adatbázist készítsenek abból[42], ami az igazszolgáltatás inkompetenciájából, intézményesített közönyéből fakadóan csak egy-egy elhivatott kutató számára válik láthatóvá időről időre.[43]

Éppen az igazságszolgáltatási szervek kompetenciahiányának, illetve szervezeti hiátusainak volt a következménye, hogy Pipás Pista úgy vált egyszerre sorozat- és bérgyilkossá, hogy anyagilag volt érdekelt a bosszúálló legendáját felépítő történetekké torzuló, brutális gyilkosságokban.

42 Budvári Róbert: A titkolt emberölés leleplezése. Belügyi Szemle, 1966/6., 52–57. o.

43 Megfontolandó példa Angyal Miklós: Ismeretlen személyazonosságú holttestek kriminalisztikai és szakértői azonosítása. Doktori értekezés. Pécsi Tudományegyetem Állam- és Jogtudományi Kar, Pécs, 2014.