MMXV. III. ÉVFOLYAM 2.SZÁM

# NEMZETBIZTONSÁGI SZEMLE

## TARTALOM

*Szijártó Lívia: Az európai szélsőséges szervezeteket érintő hírszerző tevékenység - a radikális csoportok jellemzői térségünkben*

*Bányász Péter: A közösségi média, mint a nyílt forrású információszerzés fontos területe*

*Dely Péter: Afganisztán Nemzeti Rendőrsége I. - Az Afgán Rendőrség fejlesztését célzó nemzetközi törekvések*

*Kovács Róbert: Nemzetbiztonsági célú rövidhullámú stratégiai COMINT rendszerek elektronikai védelmi megfontolásai*

*Balog Károly: A digitális PMR-ek szerepe a szervezett bűnözésben és a kiscsoportos direkt kommunikációban*

*Dr. Dobák Imre: Könyvismertető*

NEMZETI KÖZSZOLGÁLATI EGYETEM
NEMZETBIZTONSÁGI INTÉZET
BUDAPEST

# NEMZETBIZTONSÁGI SZEMLE

A Nemzeti Közszolgálati Egyetem
Nemzetbiztonsági Intézetének
elektronikus (online) megjelenésű tudományos folyóirata

HU ISSN 2064-3756

**III. évfolyam, 2. szám, 2015.**



**Internetes elérhetőség:** http://nbszemle.uni-nke.hu

Szerkesztőség: Nemzeti Közszolgálati Egyetem, Nemzetbiztonsági Intézet
1101 Budapest, Hungária krt. 9-11.

Levelezési cím: Nemzeti Közszolgálati Egyetem, Nemzetbiztonsági Intézet
1581 Budapest, Pf.: 15.

E-mail: nbszemle@uni-nke.hu

**Kiadó:**
Nemzeti Közszolgálati Egyetem
1101 Budapest, Hungária krt. 9-11.

**E számunk szerzői:**


| | |
|---|---|
| Szijártó Lívia | NKE, Hadtudományi Doktori Iskola, PhD hallgató |
| Bányász Péter | NKE, Katonai Műszaki Doktori Iskola, PhD hallgató |
| Dely Péter | Terrorelhárítási Központ munkatársa |
| Kovács Róbert | NKE, Katonai Műszaki Doktori Iskola, PhD hallgató |
| Balog Károly | NKE, Katonai Műszaki Doktori Iskola, PhD hallgató |
| Dr. Dobák Imre | NKE Nemzetbiztonsági Intézet |


**A számban megjelent írásokat lektorálták:**

Dr. habil. Boda József
Prof. Dr. Haig Zsolt
Dr. habil. Kis-Benedek József
Dr. Dobák Imre
Dr. Kenedli Tamás

# Tartalomjegyzék

Szijártó Lívia: Az európai szélsőséges szervezeteket érintő hírszerző tevékenység - a radikális csoportok jellemzői térségünkben .....4

Bányász Péter: A közösségi média, mint a nyílt forrású információszerzés fontos területe .....21

Dely Péter: Afganisztán Nemzeti Rendőrsége I. - Az Afgán Rendőrség fejlesztését célzó nemzetközi törekvések .....37

Kovács Róbert: Nemzetbiztonsági célú rövidhullámú stratégiai COMINT rendszerek elektronikai védelmi megfontolásai .....52

Balog Károly: A digitális PMR-ek szerepe a szervezett bűnözésben és a kiscsoportos direkt kommunikációban .....71

Dr. Dobák Imre: Könyvismertető .....90

# Az európai szélsőséges szervezeteket érintő hírszerző tevékenység - a radikális csoportok jellemzői térségünkben

**Szijártó Lívia**[1]

**Absztrakt:**

A jelen tanulmány a szélsőséges csoportokkal összefüggő hírszerző tevékenységet és ezen szervezetek európai helyzetét mutatja be. Napjainkban kiemelt feladattá vált az információs fölény kivívása, emiatt a korábban használt hírszerzés fogalom helyét átvette a rendszerszemléletű információszerzés és -feldolgozás, mely tevékenység reflektál az új típusú biztonsági kihívásokra is. A nemzetközi terrorizmus és a szélsőséges csoportok működése elleni küzdelemhez szükséges ismerni azokat a gazdasági, politikai és társadalmi körülményeket, melyek segítségével ezek a szervezetek létrejöttek. Az európai trendek azt mutatják, hogy habár hazánkban még nem jelent magas biztonsági kockázatot a radikalizálódás, azonban a jövőben a destruktív folyamatok egyre súlyosabb problémát okozhatnak.

**Abstract:**

The current study describes the intelligence activity related to extremist organizations with a focus on the European situation. Information superiority is a crucial issue; therefore, the previously used intelligence term is replaced by the concept of system approach in information acquisition and processing, which approach is reacting to the new security challenges. Regarding the international terrorist and extremist organizations, it is important to account for the economical, 0political and social circumstances, which resulted in the establishment of these groups. Although the radicalization is not a high security risk in Hungary similarly to other European examples, the extremist groups might cause a serious issue in the future.

[1] *Nemzeti Közszolgálati Egyetem, másodéves doktorandusz, szijartolivia@gmail.com*

## Bevezetés

A bipoláris világrend felbomlása felerősítette az addig csak elszigetelten jelentkező problémákat, mint a regionális konfliktusok, a széteső államok és a különböző vallási, politikai vagy etnikai szélsőséges csoportok, a terrorizmus megjelenése. A radikális szervezetek ma már az egész világon globális fenyegetést jelentenek, mivel eredményesen szólítják meg az elmaradottabb térségből jövő, a társadalom peremterületén élő személyeket. Ezen csoportok veszélyt jelentenek az adott ország társadalmi berendezkedésére, a közbiztonságra és a politikai hatalomra is. A 2008-2009-es gazdasági világválság és az azt követő politikai krízisek elősegítették a szélsőséges irányzatok elterjedését, mivel ezen ideológiák képviselői pozitív jövőképet nyújtanak a kilátástalan helyzetbe került egyének számára. A radikális ideológiát vagy vallást követő csoportok térnyerése gyakran összefüggésbe hozható a terrorista tevékenység megjelenésével, így a 21. században új típusú biztonsági kihívásként jelentkezik az ellenük folyó harc.

A biztonsági környezet megváltozása és a radikális csoportok térnyerése maga után vonta a nemzetbiztonsági, rendvédelmi szervek feladatainak átalakulását is. A társadalomra veszélyes szélsőséges mozgalmak elleni hírszerző tevékenységnek – a probléma komplexitása miatt – reflektálnia kell a politikai, társadalmi és gazdasági összefüggésekre is. Ezen szervek célja, hogy a felderítés során megismerjék az adott extrém csoport működését, felépítését, kapcsolatait, társadalmi hatását és az általa közvetített fenyegetés mértékét. Az alábbiakban elsőként a felderítő munka általános bemutatása, majd a szélsőséges csoportokat érintő feladatok megismerése történik, melyet a fenti mozgalmak tevékenységének felvázolása követ.

### 1.1. A felderítés és a hírszerzés fogalmi meghatározása

A korunkban is zajló információs forradalom miatt olyan tudásalapú társadalmi rendszer alakult ki, melyben a hatalom egyik legfontosabb tényezőjévé az információ megszerzése került. Az információs fölény kivívásának igénye nemcsak a biztonsági szektor működését befolyásolja, hanem a politikai, a pénzügyi, a kulturális szférában is jelentős szerepe van. Az 1990-es évektől a hírszerzés fogalom helyét átvette a rendszerszemléletű információszerzés és -feldolgozás definíciója, mely pontosabban fejezi ki azt a tevékenységet, melyet a felderítő szervek végeznek.[2] Várhalmi szerint, a hírszerzés és a felderítés egymás mellett és helyett is használhatók. A Magyar Hadtudományi Lexikon[3] szerint, a két fogalom

[2] *VÁRHALMI A. M. (2009): A hírszerzés-felderítés szerepe és jelentősége a XXI. századi Európai Unió számára, Hadtudományi Szemle, 2. évf., 1. sz., 2009., 51-59. old.*

[3] *Magyar Hadtudományi Lexikon. Budapest, Magyar Hadtudományi Társaság, 1995.*

"*azon intézkedések, rendszabályok és tevékenységek összessége, melyek az állami apparátus vezetői, szervei és a különböző szintű parancsnokságok alá tartoznak, továbbá amelyek egy ország vagy ország-csoport érdekeiről, célkitűzéseiről, szándékáról, terveiről, tevékenységéről, erőforrásairól, helyzetéről, fegyveres erőinek felépítéséről, csoportosításáról, haditechnikájáról, kiképzettségi színvonaláról, hadrafoghatóságáról, harckészültségi helyzetéről, továbbá a hadszíntérré váló terület előkészítéséről szóló adatok megszerzését, gyűjtését és tanulmányozását célozzák. A felderítés rendeltetését és feladatait tekintve politikai, gazdasági, katonai, tudományos-technikai felderítési ágakra tagozódik*."

A fenti tevékenységforma egyik markáns ága a katonai hírszerzés, mely az ellenséges országok katonai, hadi potenciáljának megismerését szolgálja, a felderítés a katonai feladatok sikeres teljesítésének előfeltétele. Az 1990-es politikai átrendeződés után a konfliktusokat érintő hírszerző tevékenység mértéke lecsökkent, ma már inkább válságkezelő és békefenntartó szerepe van. A felderítés szakaszai között megjelenik az irányítás, az adatgyűjtés, az adatfeldolgozás és a tájékoztató munka is.[4]

Nyeste 2013-as tanulmányában[5] kiemeli, hogy a nemzetbiztonsági szolgálatok tevékenységét szabályozó törvény értelmében a hírszerzés biztosítja a kormányzati döntésekhez szükséges, nemzetbiztonsági szempontból releváns információkat. A stratégiai hírszerző feladatok végrehajtásával megakadályozható a külföldről érkező, Magyarország érdekeit és szuverenitását veszélyeztető törekvések bekövetkezése, továbbá hozzájárul a nemzetbiztonsági stratégia, a helyzetértékelések és a jövőre vonatkozó prognózisok kialakításához. A cikkben foglaltak szerint a nemzetbiztonsági hírszerzés mellett beszélni kell a bűnügyiről is, mely tevékenység az adott nyomozó szerv hatáskörébe tartozó bűncselekmények megelőzését, elhárítását, vagy elkövetés esetén a felelősök felderítését szolgálja. Mind a nemzetbiztonsági, mind a bűnügyi hírszerzésnek fontos feladata, hogy illeszkedjen a döntéshozó információigényéhez.

A stratégiai felderítés lehetséges definíciója szerint "a politikai irányításhoz és a katonai tervezéshez, a nemzeti és nemzetközi szintű kormányzati döntésekhez szükséges információk megszerzése a nyílt és a titkos információgyűjtés módszereivel, valamint azok feldolgozása (elemzése-értékelése) és továbbítása az illetékesekhez."[6] A stratégiai felderítés nem egy adott ügyhöz kötött, hanem arra szolgál, hogy egy közép- és hosszú távú biztonsági stratégiához szükséges információkat biztosítsa, illetve a döntési alternatívák, a cselekvési változatok

[4] *A felderítésről és hírszerzésről ld. még Várhalmi, 2009.*

[5] *NYESTE P. (2013): A nemzetbiztonsági célú stratégiai felderítés/elhárítás és a bűnügyi célú stratégiai hírszerzés összehasonlítása, kiemelten a szervezett bűnözés elleni fellépés területén, Felderítő Szemle, 12. évf., 1. sz., 2013. szeptember-október, 100-120. old.*

[6] *KIS-BENEDEK J. : A stratégiai felderítés összetevői. Előadás a Stratégiai hírszerzés elmélete és gyakorlata c. kurzushoz. 2015. március 3., Nemzeti Közszolgálati Egyetem, Hadtudományi Doktori Iskola, Budapest.*

fejlesztését szolgálja. Kis-Benedek előadásában[7] a nemzetbiztonsági stratégiai hírszerzést az alábbi célterületekre bontja: biográfiai, gazdasági, társadalmi, közlekedési és távközlési, katonaföldrajzi, haderő, politikai és tudományos-technikai. A jelen tanulmány szempontjából a releváns hírszerző tevékenység a gazdasági, a társadalmi és a politikai felderítés: az első a vizsgált térség természetes és emberi erőforrásait, hatékony hasznosítását, a nemzetek gazdasági potenciálját vizsgálja. A hírszerzés kiterjed az adott ország pénzügyi sebezhetőségére, a gazdasági hadviselés lehetőségeire is. A társadalmi/szociológiai felderítés a társadalmi csoportok tanulmányozását foglalja magába, azok tevékenységét, felépítését, a kulturális, vallási sajátosságokat, és a szociális biztonságot, jóllétet érintő fenyegetéseket is. A politikai hírszerzés az idegen hatalmak kül- és belpolitikáját vizsgálja, továbbá a nem kormányzati szervezetek, politikai mozgalmak tevékenységét. Ide tartozik a közbiztonságra, terrorizmusra, hírszerző szolgálatokra vonatkozó információk gyűjtése is.

## 1.2. A hírszerző tevékenység célja és hatásterületei

A fentiekből kiderül, hogy a hírszerzésnek és a felderítésnek nincsen egy elfogadott definíciója, azonban összességében elmondható, hogy a tevékenységek célja, hogy döntési helyzetben olyan jól megalapozott, hiteles információkat szolgáltassanak, melyek hatékony cselekvést tesznek lehetővé az ellenséggel szemben. A hírszerzés célja kettős:[8] egyrészről védelmi, másrészről érdekérvényesítési szerepet tölt be. A biztonsági folyamatok ellenőrzése, a jövőbeni fenyegetések prognosztizálása csak megfelelő prediktív tudással kivitelezhető, melynek a hatékony információszerző tevékenység a szükséges előfeltétele.

Magyarország 2012-ben elfogadott Nemzeti Biztonsági Stratégiájában a harmadik fejezetben tárgyalja azokat a térségünket érintő kihívásokat és fenyegetéseket, melyekkel a nemzetbiztonsági szerveknek foglalkozniuk kell:[9]

- regionális konfliktusok
- tömegpusztító fegyverek proliferációja
- nemzetközi terrorizmus
- kiber-, energia-, pénzügyi biztonság
- globális éghajlat- és környezetváltozás
- természeti és ipari katasztrófák
- szervezett bűnözés

[7] *KIS-BENEDEK, 2015.*

[8] *VÁRHALMI, 2009.*

[9] *A Kormány 1035/2012. (II. 21.) Korm. határozata Magyarország Nemzeti Biztonsági Stratégiájáról, Magyar Közlöny, 2012. évi 19. szám. 1378-1387. old. http://2010-2014.kormany.hu/download/f/49/70000/1035_2012_korm_hatarozat.pdf*

- kábítószer-kereskedelem
- migráció
- radikális szervezetek elterjedése

Az előbbiekben felsorolt veszélyforrásokkal szembeni feladatokat és intézkedéseket a különböző szakterületek által folyamatosan értékelt, elemzett és megosztott információk alapján kell elvégezni. A stratégiai felderítési célok megvalósításához szükséges olyan, a nemzetközi viszonyokra, a külföldön működő magyar szervezetekre, a terrorizmusra, a szervezett bűnözésre és egyéb regionális konfliktusokra vonatkozó információk megszerzése a hírszerző tevékenység által, melyek elengedhetetlenek a megalapozott kormányzati döntésekhez.[10]

A hírszerzés célja összességében a döntéshozók támogatása a megfelelő információkkal. A szükséges, gyakran bizalmas vagy titkos információ megszerzése a titkosszolgálatok, nemzetbiztonsági szervek feladata, melyek a megrendelő - lehet katonai és politikai döntéshozó - igényeitől függnek. A felderítés, hírszerzés jelentősége a speciális adatok megszerzésében mutatkozik meg, és a vezető állami szereplők általában az alábbi területeken használják fel ezeket:

- a közvetlen környezetben felmerülő válság- vagy konfliktus kezelésében
- a létérdekeket, nemzeti érdekeket fenyegető veszélyek esetén
- az általános politikai, katonai stratégiák kialakításában
- a politikai hatalmat fenyegető bármilyen veszély esetén[11]

Egy 2009-es tanulmány[12] szerint a hírszerzés általános céljai közé tartoznak az alábbi tevékenységek:

- információgyűjtés, -elemzés, -értékelés, a megszerzett adatok megosztása, felhasználása más katonai, állami, politikai szereplőkkel
- más országok, politikai hatalmak és mozgalmak információszerző tevékenységnek felderítése, esetleg megakadályozása
- titkos feladatok végrehajtása az ellenséges mozgalmak, országok magatartásának befolyásolása céljából

## 1.3. A hírszerzés és a szélsőséges csoportok kapcsolata

A 2001. szeptember 11-i terrortámadások után megkérdőjeleződött a nemzetbiztonsági szolgálatok hatékonysága. A merénylet utáni kivizsgálások több hiá-

[10] *NYESTE, 2013.*

[11] *IZSÓ J. (2009): A hírszerzés céljáról és rendszeréről, Hadtudomány - Hadügy, 1-2. sz., 2009., 72-84. old.*

[12] *IZSÓ J., 2009.*

nyosságra is rámutattak, többek között arra is, hogy az aszimmetrikus hadviselés elterjedése miatt megváltoztak a hírszerzést meghatározó körülmények. A felderítést napjainkban megnehezíti, hogy az ellenség nem egy adott állam vagy politikai rendszer, hanem a fenyegetést nagyrészt olyan csoportok léte jelenti, melyek szélsőséges tevékenységet folytatnak.[13]

Kis-Benedek[14] szerint ezek a politikailag vagy vallásilag fanatizált szervezetek terrorcselekményeket hajthatnak végre bárhol, illetve sejtszerűen építkeznek, így egyre globálisabbá válnak. A radikális csoportoknak a világ számos pontján vannak szimpatizánsaik, követőik, kialakulásukat több tényező is befolyásolja, melyre a hírszerzésnek reagálnia kell. A radikális mozgalmak megjelenése az elmúlt 20-25 évben markáns biztonsági kockázattá vált, mivel a Szovjetunió felbomlásával, a bipoláris világrend megszűnésével előtérbe kerültek az instabil régiókban - addig marginálisan - megjelenő problémák. Az elmaradottság, a mélyszegénység és a gyenge államapparátus együttesen termékeny táptalajt biztosít a szélsőséges csoportok terjeszkedésének, mely közösségek nagy veszélyt jelentenek a társadalom egészére nézve. Az elmúlt években számos kutatás, konferencia és szakmai fórum foglalkozott a szélsőséges ideológiák, a radikalizálódás kérdéskörével, és összességében elmondható, hogy hatékonyan csak megfelelő háttértudással lehet fellépni a fenti tendencia ellen.

A fentiek alapján kijelenthető, hogy a 2001-es amerikai terrortámadás után megváltoztak a biztonsági körülmények, melyekre mind az EU-nak, mind a NATO-nak új típusú reagálási eljárásokat kellett kidolgozni. A globális terrorizmus megjelenése stratégiai fenyegetést jelent mindkét nemzetközi szervezet számára, melynek egyik legveszélyesebb formája a főként vallási fundamentalizmusra építő csoportok, az etnikai és lokális szervezetek elterjedése.[15] Az euroatlanti térségben megjelenő fenyegetések ellen csak nemzetközi együttműködéssel lehet küzdeni, az esetleges támadások megelőzése, a szélsőséges csoportok tevékenységének nyomon követése, a radikalizálódás lehetőségének megakadályozása a hírszerző szervek kiemelt feladatai közé tartoznak. A fenyegetettség szintje eltérő az egyes országokban, azonban a globalizáció, a telekommunikációs eszközök fejlődése és a migrációs folyamatok miatt egyre magasabb kockázatot jelentenek a radikális mozgalmak az európai és nyugati világ számára.

A napjainkban megjelenő terroristafenyegetés jóval szélesebb körű, mint korábban. A szervezetek kiterjedt hálózatokat működtetnek az egész világon, továbbá az iszlám, közel-keleti gyökerű sejtek mellett továbbra is jelen vannak a szélsőjobb és szélsőbal szervezetek, nacionalista és szeparatista mozgalmak, vagy akár a radikális érzületű magányos elkövetők is. A fenti csoportok tevékeny-

---

*[13] KIS-BENEDEK J. (2004): A terrorizmus ellen folytatott hírszerzés, Nemzetvédelmi Egyetemi Közlemények, 8., 2., 105-110. old.*

*[14] KIS-BENEDEK J. 2004.*

*[15] KIS-BENEDEK J. (2006): Az európai biztonság és stratégia. Az EU és a NATO az új kihívások előtt, közép-európai kitekintéssel. Magyar Minőség, 15. évf., 7. sz., 2006., 2-7. old.*

sége gyakran a terrorizmus és az extrémizmus vékony határvonalán húzódik, az eleinte erőszakmentes magatartás a későbbiekben könnyen vált át agresszív cselekvésbe.[16]

### 2.1.1. A szélsőséges csoportok létrejöttének általános társadalmi, politikai és gazdasági körülményei

Az extrémista csoportok ereje abban rejlik, hogy az adott társadalomban megjelenő valós vagy vélt fenyegetésre adnak megoldási javaslatokat. Ezek a mozgalmak azt állítják, hogy egyes csoportok veszélyben vannak, és ők önként vállalják ennek elhárítását, illetve legitimálják a diszkriminációt bizonyos külső szereplőkkel szemben, akiktől védeni kell a társadalom többi tagját. A radikális ideológiák tehát az erőszakot elfogadhatóvá teszik, hiszen az végső soron a védelmet szolgálja. Ennek megfelelően minél nagyobb a bizonytalanság és a szociális félelem egy adott országban, annál könnyebben tudja megszólítani az embereket egy extrémista szervezet.[17]

Egy nemrég megjelent tanulmány[18] a szélsőséges szervezetek motivációs és viselkedéses hátterét vizsgálja, illetve általános megállapításokat is tesz ezen szervezetek pszichodinamikai jellemzőit illetően. A radikális mozgalmak közös vonása, hogy alapvetően a többségi társadalom tagjait próbálják megszólítani és csatlakozásra bírni. Az ilyen csoportok működését befolyásolják a globális szocioökonómiai, geopolitikai körülmények, a hadi képességek, az ökológiai környezet, az információáramlás lehetőségei az adott térségben. Ezeken felül az állami berendezkedés, a politikai, gazdasági helyzet is meghatározza a radikalizálódási folyamatokat, a széteső, gyenge vezetésű országokban könnyebben terjednek a szélsőséges mozgalmak.

A fenti szervezetek általában eredményesen szólítják meg a társadalmilag, gazdaságilag vagy politikailag kirekesztett egyéneket, a kiábrándult közönséget. A vezetők hamis valahova tartozással és önbecsüléssel ruházzák fel a csalódott embereket, pozitív jövőképet vázolnak fel számukra. Az elesett személyek felkarolása olyan elköteleződést alakít ki bennük, hogy könnyebben vehetők rá jogsértő magatartásra. Általánosságban az ilyen egyházi, vallási szervezetek olyan

---

*[16] DAWSON L., EDWARDS C., JEFFRAY C.: Learning and adapting. The use of monitoring and evaluation in countering violent extremism. A handbook for practitioners. Royal United Services Institute for Defense and Security Studies (RUSI), London, 2014.*

*[17] MIREANU M. (2012): Belföldi extrémizmus - A biztonság és erőszak politikai elemzése. Háttérelemzés Sorozat Tanulmány, Athéna Intézet, Open Society Foundations, 2012. június.*

*[18] BERNARD M. L., BLIER A. B. (2014): Analytical capability to better understand and anticipate extremist shifts within populations in failing states. 5th International Conference on Applied Human Factors and Ergonomics AHFE, Kraków, Poland, 2014.*

térségekben tesznek szert nagy befolyásra, ahol háborúk, fegyveres konfliktusok, éhínség, szegénység és ezekkel párhuzamosan gyenge demokratikus hagyományok tapasztalhatók. A fejlett, nyugati államokban kevesebb hatalommal bírnak, mivel ott az erős politikai vezetés, az egyéni szabadság és az általános jóllét megléte gátolja a személyes befolyásolhatóságot.[19]

A vallási közösségek alapvetően lélektani ráhatással vagy fizikai erőszakkal különítik el a tagokat a többségi társadalomtól, és idővel destruktív cselekedetekre ösztönzik őket. Az Európai Unióban kevésbé markánsan jelennek meg ezek a csoportok, azonban az iszlám indíttatású szélsőséges szervezetek terjeszkedése mindenképpen biztonsági kockázatot jelent. Az EU tagállamai mind a nemzetbiztonsági stratégiájukban, mind a rendvédelmi és felderítő szerveik munkájában reflektálnak erre a kihívásra, a lehetséges fenyegetések elhárításának érdekében két- vagy többoldalú együttműködést valósítanak meg.[20]

### 2.1.2. Az iszlám gyökerű szervezetek működését meghatározó körülmények

Az iszlám terrorizmus sok ideig nem jelentett valós fenyegetést a nyugati országok számára, azonban a 20. század végén megjelentek a térségben is a radikális muszlim mozgalmak. A nemzetközi dzsihád nevében a terroristák igyekeztek minden olyan területen hatalomhoz jutni, ahol kisebb-nagyobb muzulmán közösségek élnek. Európában a 2000-es években jelentek meg az első terrorista sejtek, melyek tagjai már második vagy harmadik generációs iszlám bevándorlók, áttért nyugati emberek. Ezek a csoportok önszerveződéssel jöttek létre, általában nem külföldi támogatással, az angol szakirodalom ezért "homegrown" (bennszülött) szervezeteknek nevezi őket.[21] Az elmúlt években aggasztó tendenciaként jelentkezik, hogy a fenti csoportok egyre gyakrabban keresik a kapcsolatot a közel-keleti terrorista sejtekkel úgy, mint az al-Kaidával és az Iszlám Állammal. A homegrown-tagok kiképzéseken vesznek részt közel-keleti bázisokon, ahonnan visszatérve merényleteket terveznek európai célpontok ellen.

Európában a 60-as évektől jelentek meg az első muszlim vendégmunkások, főként az észak-afrikai országokból, melynek fő oka a nyugat-európai munkaerőhiány volt.[22] Azonban a negatív gazdasági folyamatok[23] miatt megnőtt a mun-

---

*[19] SZABÓ CS.: A szélsőséges vallási csoportok térnyerésének kockázatai. Előadás „A BIZTONSÁG RENDÉSZETTUDOMÁNYI DIMENZIÓI – VÁLTOZÁSOK ÉS HATÁSOK" című nemzetközi tudományos konferencián. Pécs, 2012. június 28.*

*[20] SZABÓ, 2012.*

*[21] RÉPÁSI K. (2013): Európa az iszlamista terrorizmus árnyékában, Hadtudományi Szemle, 6. évf., 1. sz., 2013. 41-56.old.*

*[22] RÉPÁSI, 2013.*

kanélküliség az európai térségben is, mely főként a bevándorlókat sújtotta. Az így kialakult migrációs problémákat tovább mélyítette, hogy a 80-as években megindult a politikai és gazdasági menekülthullám az arab térségből, a muszlimok között sokan szélsőséges mozgalmak tagjai voltak korábban, így nézeteiket tovább terjesztették Európában is.[24] A bevándorlók emellett nehezen tudtak és tudnak a mai napig integrálódni a nyugati társadalomba, ebből fakadóan körükben megjelent a radikalizáció.

A beilleszkedési kísérletek kudarcának egyik fontos aspektusa a befogadás hiánya, a többségi társadalom körében nem ritka a rasszista gondolkodás sem. A migráns családok tagjai így hosszú távon mind az oktatás, mind a munka területén hátrányt szenvednek, mely tovább mélyíti az őslakosok és a bevándorlók közötti szakadékot. Répási cikkében[25] kifejti, hogy a második generációs bevándorlók már nem fogadják el a kirekesztettséget, hanem megkövetelik az őket megillető jogokat. A radikalizálódott fiatalok már nem tudnak azonosulni a szüleik elveivel, kultúrájával, de elutasítást élnek át a nyugati társadalomtól is, ezért az esetükben a szélsőséges mozgalmak elégítik ki a valahova tartozás igényét. Az iszlamista erőszakos politikai követői azonban még így is csak kis részét teszik ki a bevándorlóknak, többségük továbbra is be szeretne illeszkedni. A szélsőjobboldali szervezetek képviselői azonban tevékenységükben nagy hangsúlyt fektetnek arra, hogy felnagyítsák a migrációs problémát, ezzel növelve az előítéleteket a muszlimokkal szemben.

## 2.2. A szélsőséges csoportok működésének lehetséges felvázolása - az FBI hétlépcsős gyűlöletmodellje

Habár napjainkban az iszlámfenyegetés felülreprezentált, nem szabad figyelmen kívül hagyni, hogy más politikai és ideológiai hátterű szélsőséges csoportok is komoly nemzetbiztonsági kockázatot jelentenek. A ma is működő gyűlöletcsoportok tevékenysége irányulhat egy adott népcsoport, továbbá állami vagy kormányzati szervezetek ellen is. Az FBI szakemberei összeállítottak egy hétlépcsős gyűlöletmodellt, mely segítségével analizálni lehet a szélsőséges csoportok potenciális veszélyszintjét.[26] Előzetesen fontos meghatározni, hogy minden gyűlö-

*[23] Az 1973-as arab-izraeli háború során több olajtermelő ország bojkottot hirdetett az Izraelt támogató nyugati országok ellen, így súlyos olajválság alakult ki. Az olaj beszerezhetőségének korlátozása ipari termelési problémákat, gazdasági hanyatlást idézett elő több európai országban és az Egyesült Államokban egyaránt.*

*[24] RÉPÁSI, 2013.*

*[25] RÉPÁSI, 2013.*

*[26] SCHAFER J. R., NAVARRO J. (2003): The Seven-Stage Hate model. FBI Law Bulletin, Vol. 72., No. 3., March 2003., 1-8. old.*

letcsoport alapja egy olyan közös ellenségkép, melyet vallási, ideológiai, nemi, faji vagy egyéb megkülönböztetésre alkalmas alapon a csoport tagjai diszkriminálnak, szélsőséges esetben verbális és fizikai agresszióval élnek a külső egyénnel/csoporttal szemben. Az FBI által végzett vizsgálat szerint azok a fiatal, fehér férfiak hajlamosabbak radikális szervezethez csatlakozni, akik aluliskolázottak és diszfunkcionális családból származnak. A gyűlöletcsoportok kialakulása a kutatások szerint az alábbi hét szakaszban jellemezhető:[27]

1. lépcső: Első lépésként létrejön a csoport, melyet a közös gyűlölet köt össze. Az egyén számára a hozzá hasonlóktól érkező pozitív visszajelzések megerősítőként hatnak, csökkenti a bizonytalanságérzetét a gyűlöletével kapcsolatban.
2. lépcső: A második szakaszban történik a csoport önmegnevezése, ebben a fázisban alakulnak ki a speciális szokások, szimbólumok, melyek megkülönböztetik a tagokat más szerveződésektől. Ezek a jellegzetességek erősítik a csoporthoz tartozás érzését, továbbá lealacsonyítják a külső személyeket, a gyűlölet tárgyát.
3. lépcső: A csoporttagság megszilárdítását, az egyén saját magáról alkotott képének megerősítését szolgálja a gyűlölet tárgyának verbális megalázása. A rasszista szervezetekben a tagok diszkriminatív dalokat, irodalmi műveket terjesztenek, lehetőséget teremtenek a lenézett kisebbség meggyalázására, mely – habár ebben a fázisban még csak szóbeli – az agresszív késztetések miatt általában lassan fizikaivá válik.
4. lépcső: A negyedik lépcső annyiban tér el az előzőtől, hogy ebben a szakaszban a gyűlölködő csoport már nemcsak megalázza, hanem ki is gúnyolja az áldozatait. Ilyen tevékenység lehet az elutasított etnikum lakóterületének rongálása, rasszista graffitik rajzolása, nyílt sértegetés stb.
5. lépcső: A soron következő szakaszba jutott gyűlöletcsoportok már eljutottak arra a szintre, hogy fegyver nélkül támadják a célpontot, itt már az agresszió egyre erősebb, nehezen visszafordítható folyamat. A tagok magányos áldozatokat keresnek, akit csoportosan bántalmaznak. Az adott szervezet általában ilyenkorra a társadalom peremterületére szorul, a többség elutasítja a viselkedésüket.
6. lépcső: A hatodik szakaszban lévő csoportok már fegyveresen (pl. lőfegyver, törött üveg, szúró eszköz stb.) is támadják a gyűlöletük tárgyát, az elkövetők mélységes személyes dühvel jellemezhetők. Itt fellép a tagoknál a dominancia igénye is, mivel a fizikai bántalmazással a másik feletti hatalmukat is kiélhetik.

*A tanulmány elérhető magyarul is az Athéna Intézet Honlapján: http://www.athenaintezet.eu/hatter/olvas/7*

[27] *SCHAFER, NAVARRO, 2003.*

7. lépcső: A gyűlöletcsoportok esetében a végső fázis a célpont elpusztítása. Ebben az esetben a kegyetlenkedések már afféle isteni hatalom érzésével is párosulnak, ahol a rasszista szervezet élet és halál urává válik.

A fenti módszer hatékonysága abban rejlik, hogy egy adott szélsőséges csoport besorolása a rá jellemző szakaszba elősegíti mind a szervezet identitásának megértését, mind a lehetséges preventív eljárás alkalmazását. A rendvédelmi szervek a modell segítségével fel tudják mérni, hogy történt-e bűncselekmény, továbbá, hogy mikor várható, hogy a tagok tényleges bűnelkövetővé válnak. Érdemes kiemelni, hogy a szélsőséges eszmék terjesztése nem feltétlenül függ össze terrorista merényletek elkövetésével, tehát a radikalizálódási folyamat nem okoz egyértelműen agresszív végeredményt. A társadalomra veszélyes vallási mozgalmakkal itthon az Alkotmányvédelmi Hivatal foglalkozik, és ezen csoportok célja, hogy növeljék a befolyásukat mind az állami döntéshozatalban, mind a szociális életben.[28]

## 2.3. Az Európában működő szélsőséges csoportok jellemzői

Az Európában megjelenő mozgalmak eltérő ideológiát, vallást és politikai gondolkodást követnek. A csoportok működésének jobb megértéséhez tisztázni kell a különböző indíttatású szélsőséges viselkedést.

Az Európai Unió éves szinten jelentést készít a térséget érintő terrortevékenységekről. A TE-SAT (Terrorism Situation and Trend Report) iratok[29] nyilvánosan elérhetők az interneten, és általuk teljes képet kaphatunk az elmúlt évek európai terrorfenyegetettségéről. A jelentésekben szereplő statisztikák szerint térségünkben az alábbi ideológiájú extrém csoportok és terrorista szervezetek működnek:[30]

Az iszlám terrorizmus kapcsán már kiderült, hogy főleg a 21. században jelent meg Európában, azóta a hatóságok számos terrorcselekményt hiúsítottak meg a megfelelő preventív munkával, főleg Franciaországban, Olaszországban, Spanyolországban és Hollandiában. A radikális iszlamisták többsége észak-afrikai származású volt 2006-ban és többségük már második vagy harmadik generációs bevándorló.[31]

Az etnonacionalista és szeparatista terrorizmus jellemzője, hogy egy adott etnikai kisebbség képviselői követnek el merényleteket, hogy autonómiát szerezzenek egy történelmileg jelentősséggel bíró területen. Az elmúlt években a

---

[28] *SZABÓ, 2012.*

[29] *TE-SAT, Terrorism Situation and Trend Report, European Police Office, 2007-2014. A jelentések letölthetők innen: https://www.europol.europa.eu/latest_publications/37*

[30] *TE-SAT, 2008.*

[31] *TE-SAT, 2007.*

trendek szerint nagyrészt a baszk régióban és Korzikán történtek szeparatista terrorcselekmények, illetve a kurdok tevékenysége jelentős még Törökország területén. Ezek a szervezetek nem feltétlenül kormányzati célpontokat támadnak, továbbá céljuk nem a halálos áldozatok magas száma, hanem pusztán nyomásgyakorlás, mely természetesen többször jár együtt emberélet kioltásával.

A baloldali és anarchista terroristák főként Görögországban, Olaszországban, Spanyolországban és Németországban rendelkeznek bázissal, a tagok kis intenzitású támadásokat követnek el üzleti és kormányzati célpontok ellen.

Európában a szélsőjobboldali terrorizmus kevésbé van jelen, inkább a nacionalista mozgalmak váltak meghatározóvá a térségben. Az európai szélsőjobboldali szervezetek nagy része az 1970-80-as években alakult, mely csoportok újfasiszta vagy neonáci ideológiát követve hajtottak végre terrortámadásokat. Ezek a szervezetek a kezdeti időkben rendszeresen követtek el civil áldozatokkal járó merényleteket, azonban az utóbbi években – ahogy majd a későbbiekben szereplő statisztikák is mutatják – tevékenységük korlátozottá vált. Az ideológiai hátteret megnézve megállapítható, hogy Európában nemcsak a hagyományos, faji alapú – főként antiszemita – gondolkodásmód terjedt el, hanem megjelentek a muszlim bevándorlókat, az iszlámot, a multikulturalizmust elutasító szélsőjobboldali csoportok is. A tagok szemében a muzulmánok fenyegetést jelentenek az európai eszmékre, a nemzeti szokásokra, értékekre; ezen szervezetek főként azokban a nyugati országokban ütötték fel a fejüket, ahol komoly belpolitikai problémát jelent a bevándorlók jelenléte. A kelet-európai államokban továbbá is a zsidó- és romaellenesség a markáns ideológia a radikális csoportokban.[32] Anders Breivik 2011-es terrortámadása és a Németországban leleplezett neonáci halálbrigád által elkövetett gyilkosságok rávilágítanak arra, hogy a szélsőjobboldali terrorizmus nem szűnt meg Európában, csak marginalizált formában jelentkezik.[33]

Európában számos olyan gyűlöletcsoport működik, mely valamilyen kapcsolatban áll a terrorizmussal, esetleg olyan extrémista cselekedeteket hajt végre, melyek veszélyeztetik az adott ország társadalmi berendezkedését. A TE-SAT jelentésekben[34] található statisztikák szerint nagyrészt a nyugat-európai országok érintettek a terrorizmusban, kisebb-nagyobb támadások és terrorizmussal összefüggő hatósági intézkedések többségében Franciaországban, Spanyolországban, Olaszországban, Belgiumban, Nagy-Britanniában, esetleg Németországban fordultak elő.

Az európai hatóságok a konkrét támadásokon túl vizsgálják a terrorszervezetek pénzügyi hátterét, az internethasználatot és egyéb működési mechanizmu-

---

*[32] A szélsőjobboldali csoportokról ld. részletesen: RÉPÁSI K. (2012): Újjáéled-e az európai szélsőjobboldali terrorizmus? Biztonságpolitikai Szakkollégium Egyesülete, 2012. Megjelent 2012. december 18-án a biztonsagpolitika.hu-n.*

*[33] RÉPÁSI, 2012.*

*[34] TE-SAT, 2007-2014.*

sokat is. Az eddigi statisztikák szerint a terrorista csoportok finanszírozása többségében csalásból, rablásokból, emberrablásokból és zsarolásból történik, illetve kimutathatóan jobb pénzügyi lehetőségei vannak az iszlám mozgalmaknak, mint a nem-iszlám szervezeteknek.[35] Nem ritka, hogy alapítványok, vallási központok biztosítják a szélsőséges csoportok pénzügyi hátterét. A 2014-es TE-SAT kiadvány szerint komoly problémát jelent a terrorista csoportok és a szervezett bűnözés összefonódása: a fegyver- és emberkereskedelem, a személyazonossággal összefüggő lopások, az illegális bevándorlás, a menekültek szállítása mind szervezett bűnözői csoportokon keresztül valósul meg az európai országokban.[36]

A szélsőséges csoportok számára elengedhetetlen a nyilvánosság mind a merényletekkel elért hatás kivívásához, mind a további tagok toborzásához. Az elmúlt években főként fiatalsági szervezeteken, internetes oldalakon keresztül propagálták tevékenységüket, mivel a statisztikák szerint a szociális közösségi oldalakon eredményesen lehet befolyásolni az arra hajlamos fiatalokat. A radikalizálódás összességében egyre nagyobb problémát jelent Európában, a webes kommunikáció miatt már nagy földrajzi távolságok mellett is lehetőség van arra, hogy a szélsőséges gondolkodású személyek csatlakozzanak egyes terrorszervezethez, továbbá, e csoportok üzenetei, utasításai is hatékonyan eljuttathatók a célközönséghez.[37]

A TE-SAT 2012-es kiadványában[38] jelenik meg először különálló pontban a kiberterrorizmus kérdésköre. A szélsőséges mozgalmak egyre nagyobb számban követnek el hackercselekményeket, mely egyrészről ideológiai célokat szolgál – nézetek terjesztése megtámadott honlapokon, másrészről anyagi jellegű – pénzszerzési lehetőségek kiaknázása a webes hálózatokon.

A fentiek mellett a TE-SAT jelentésekből az is kiolvasható, hogy mind a tervezett és elkövetett merényletek, mind a terrorizmushoz köthető letartóztatások száma csökkenő tendenciát mutat. 2006-ban nagyjából 600 terrorizmushoz köthető bűncselekményt regisztráltak, nagyjából 1000 letartóztatással, míg 2013-ban 153 támadás történt és az elfogások száma 535 volt.

Az Athena Intézet[39] 2013-ban kiadott egy jelentést,[40] melyben a magyarországi radikális szervezetek nyilvános tevékenységeiről osztott meg információkat. Az intézet munkatársai folyamatosan nyomon követték a Magyarországon jelen-

[35] *TE-SAT, 2009.*

[36] *TE-SAT, 2014.*

[37] *TE-SAT, 2010.*

[38] *TE-SAT, 2012.*

[39] *Az Athéna Intézet célja a radikális szervezetek és ideológiák visszaszorítása Európában. Ennek érdekében független és objektív vizsgálatokat folytat az extrém csoportok működését illetően, az elemzések, kutatások nyilvánosan elérhetők a szervezet honlapján: http://www.athenaintezet.eu/index/*

[40] *FOMINA V. (2012): Mapping the network of Hungarian extremist groups. An in-depth analysis sequence paper. Athena Institute, Open Society Foundations, December 2013.*

lévő szélsőséges mozgalmakat, a hozzájuk köthető nyílt adatokat, a közöttük lévő esetleges kapcsolatokat, és megállapították, hogy többször tartanak közös rendezvényeket a hasonló gondolkodású csoportok. Hazánkban főként a szélsőjobboldali ideológia terjedt el, a legtöbb mozgalom ehhez kötődik, és a kuruc.info nevű weboldal jelenik meg fő összekötő kapocsként és propagandafelületként. A tagok gyakran hangoztatnak antiszemita, rasszista kijelentéseket, nemzeti érzelmű rendezvényeket szerveznek és nacionalista hagyományok szerint élnek, öltözködnek. A kisebbségek iránt érzett gyűlöletük verbális szinten korlátozódik, esetleg tüntetésekkel, tiltakozó akciókkal hívják fel magukra a figyelmet. Magyarországon általánosságban elmondható, hogy a szélsőséges elemek egyelőre nem jelentenek valós veszélyt a társadalomra nézve.

## 3. Összegzett következtetések

A fentiekből kiderült, hogy számos radikális csoport jött létre Európában az elmúlt évtizedekben, emiatt a rendvédelmi és nemzetbiztonsági szervek munkájában kiemelt figyelmet kapott a velük kapcsolatos információszerzés. A szélsőséges és terrorista szervezetek létrejötte, motivációs és ideológiai háttere, működésmódja nem érthető meg az adott térség társadalmi, politikai és gazdasági viszonyainak ismerete nélkül. A közel-keleti térséget sújtó belpolitikai válságok, a széteső államok és gazdasági nehézségek miatt az ott élő személyek súlyos szegénységben, kirekesztettségben élnek, emiatt fogékonyak a radikális, pozitív alternatívát nyújtó eszmék iránt.

Az európai és nyugati térségben, napjainkban a fő problémát a 2008-2009-es gazdasági világválság és a fejlődő országokból érkező bevándorlók jelentik. Ezekben az országokban kialakult egy főleg migránsokból álló réteg, akik a társadalom peremterületére szorultak, az integrációs törekvéseik akadályozottak, továbbá mind az oktatás, mind a munkalehetőségek terén hátrányban vannak. A beilleszkedési problémák miatt két negatív folyamat is megindult: a – főként muszlim származású – bevándorlók közül számos fiatal csatlakozik radikális ideológiát valló, vallási fundamentalista csoportokhoz, míg a többségi társadalomból többen szimpatizálnak olyan szélsőjobboldali mozgalmakkal, melyek elutasítják az iszlám migrációt és a multikulturalizmust. Vélhetően a jövőben mind a közel-keleti térségből kiinduló, vallási terrorizmus, mind a rasszista, nacionalista szervezetek jelentette veszély növekedni fog a nyugati országokban. Habár az utóbbi csoportok egyelőre inkább politikai és ideológiai színtéren jelentenek biztonsági kockázatot, nem szabad kizárni annak a lehetőségét, hogy a későbbiekben megnő a szélsőjobboldali fizikai támadások száma a muszlim bevándorlókkal szemben.

Az európai trendek egyelőre azt mutatják, hogy a térség alacsony kockázatú (pl. 2012-ben 17-en veszítették életüket terrortámadás következtében) a terrorizmus szempontjából, azonban az elmúlt időszak történései óvatosságra adnak

okot. A 2015 telén történt párizsi és koppenhágai merényletek[41] is azt mutatják, hogy kisebb terrorista csoportok hatékonyan tudnak támadásokat végrehajtani európai civil célpontok ellen.

A fenti példák azért is kiemelkedőek, mert azt mutatják, hogy a jövőben számolni kell a magányos merénylőkkel is. Ezek a fiatalok csak lazán vagy egyáltalán nem kapcsolódnak szélsőséges szervezetekhez, de az ideológiájukat magukénak vallják, és a nevükben követhetnek el terrortámadásokat. Az ún., „magányos farkasok" felderítése és nyomon követése még nehezebb, mint a radikális mozgalmak vizsgálata, mivel amennyiben nem adnak ki maguktól információt, nehéz azonosítani őket. A jövőben a szélsőséges szervezetek mellett nagyobb hangsúlyt kell fektetni a hírszerző tevékenység során az ilyen típusú elkövetőkre és a kisebb, elszigetelt csoportokra is.

[41] *2015. január 7-én két álarcos behatolt a Charlie Hebdo nevű szatirikus lap szerkesztőségébe, és megöltek 12 újságírót. Egy nappal később Amédy Coulibaly megölt egy rendőrnőt Montrouge-ban, majd a következő napon túszokat ejtett egy párizsi kóserboltban, és ott négy embert agyonlőtt. A merényleteket iszlám gyökerű bevándorlócsaládból származó fiatalok követték el, a támadások megszervezését a jemeni al-Kaida vállalta magára, és az Iszlám Állam is üdvözölte a történéseket. Egy hónappal később Koppenhágában egy arab kinézetű férfi több lövést adott le a "Művészet, blaszfémia vagy véleményszabadság" című rendezvény résztvevőire, majd egy zsinagóga előtt lövöldözött. Omar Abdel Hamid el-Hussein a támadás során két személyt halálosan megsebesített.*

**Felhasznált szakirodalom**


- A Kormány 1035/2012. (II. 21.) Korm. határozata Magyarország Nemzeti Biztonsági Stratégiájáról, Magyar Közlöny, 2012. évi 19. szám. 1378-1387. old.
- BERNARD M. L., BIER A. B. (2014): Analytical capability to better understand and anticipate extremist shifts within populations in failing states. 5th International Conference on Applied Human Factors and Ergonomics AHFE, Kraków, Poland, 2014.
- DAWSON L., EDWARDS C., JEFFRAY C.: Learning and adapting. The use of monitoring and evaluation in countering violent extremism. A handbook for practitioners. Royal United Services Institute for Defense and Security Studies (RUSI), London, 2014.
- FOMINA V. (2012): Mapping the network of Hungarian extremist groups. An in-depth analysis sequence paper. Athena Institute, Open Society Foundations, December 2013.
- IZSÓ J. (2009): A hírszerzés céljáról és rendszeréről, Hadtudomány - Hadügy, 1-2. sz., 2009., 72-84. old.
- KIS-BENEDEK J. (2004): A terrorizmus ellen folytatott hírszerzés, Nemzetvédelmi Egyetemi Közlemények, 8., 2., 105-110. old.
- KIS-BENEDEK J. (2006): Az európai biztonság és stratégia. Az EU és a NATO az új kihívások előtt, közép-európai kitekintéssel. Magyar Minőség, 15. évf., 7. sz., 2006., 2-7. old.
- KIS-BENEDEK J.: A stratégiai felderítés összetevői. Előadás a Stratégiai hírszerzés elmélete és gyakorlata c. kurzushoz. 2015. március 3., Nemzeti Közszolgálati Egyetem, Hadtudományi Doktori Iskola, Budapest.
- Magyar Hadtudományi Lexikon. Budapest, Magyar Hadtudományi Társaság, 1995.
- MIREANU M. (2012): Belföldi extrémizmus - A biztonság és erőszak politikai elemzése. Háttérelemzés Sorozat Tanulmány, Athéna Intézet, Open Society Foundations, 2012. június.
- NYESTE P. (2013): A nemzetbiztonsági célú stratégiai felderítés/elhárítás és a bűnügyi célú stratégiai hírszerzés összehasonlítása, kiemelten a szervezett bűnözés elleni fellépés területén, Felderítő Szemle, 12. évf., 1. sz., 2013. szeptember-október, 100-120. old.
- RÉPÁSI K. (2012): Újjáéled-e az európai szélsőjobboldali terrorizmus? Biztonságpolitikai Szakkollégium Egyesülete, 2012. Megjelent 2012. december 18-án a biztonsagpolitika.hu-n. Letöltve innen (2015. 03. 30.): http://old.biztonsagpolitika.hu/documents/1367862597_REPASI_Krisztian_Europai_szelsojobboldali_terrorizmus_-_biztonsagpolitika.hu.pdf
- RÉPÁSI K. (2013): Európa az iszlamista terrorizmus árnyékában, Hadtudományi Szemle, 6. évf., 1. sz., 2013. 41-56.old.

- SCHAFER J. R., NAVARRO J. (2003): The Seven-Stage Hate model. FBI Law Bulletin, Vol. 72., No. 3., March 2003., 1-8. old.
- SZABÓ CS.: A szélsőséges vallási csoportok térnyerésének kockázatai. Előadás „A BIZTONSÁG RENDÉSZETTUDOMÁNYI DIMENZIÓI – VÁLTOZÁSOK ÉS HATÁSOK" című nemzetközi tudományos konferencián. Pécs, 2012. június 28.
- TE-SAT, Terrorism Situation and Trend Report, European Police Office, 2007-2014. https://www.europol.europa.eu/latest_publications/37
- VÁRHALMI A. M. (2009): A hírszerzés-felderítés szerepe és jelentősége a XXI. századi Európai Unió számára, Hadtudományi Szemle, 2. évf., 1. sz., 2009.,51-59. old.

# A közösségi média, mint a nyílt forrású információszerzés fontos területe

**Bányász Péter**

**Absztrakt:**

A közösségi média napjaikban az otthonok, munkahelyek elválaszthatatlan részévé vált, beszivárogva szinte az összes társadalmi alrendszerbe, mindezt alig egy évtized lefolyása alatt. Nem véletlen tehát, hogy a különböző nemzetbiztonsági szolgálatok korán felismerték az új technológiában rejlő lehetőségeket. Jelen tanulmány a nyílt forrású információszerzés közösségi médiában történő alkalmazásának lehetőségeit vizsgálja meg, ismertetve a közösségi média trendjeit.

**Kulcsszavak:** közösségi média, nyílt forrású információgyűjtés, OSINT

**Abstract:**

Barely within one decade the social media became the part of our home, workplace and filter into almost each social subsystem. Consequently the national security early realised the opportunities of this new technology. This document research the possibilities of OSINT in the social media, beside set forth the trend of the social media.

**Keywords:** social media, open source intelligence, OSINT

## Bevezetés

A közösségi média hírszerzésben betöltött szerepe 2013 óta, az Edward Snowden nevével fémjelzett kiszivárogtatás következtében kiemelt érdeklődésre tart számot a sajtóban. Mint a nyilvánosságra került iratokból ismerté vált, az amerikai Nemzetbiztonsági Ügynökség (továbbiakban NSA) és társszervei 2007-től a PRISM[1] rendszeren keresztül folyamatosan hozzáfértek a nagy tech cégek (Apple, Microsoft, Facebook stb.) által tárolt adatokhoz. Különbséget kell tenni azonban az ilyen irányú adatgyűjtő eljárás és a nyílt forrásból történő információszerzés között (ami jelen dolgozat tárgyát képezi).

A közösségi média alig egy évtizedes múltja átformálta a társadalmakat. A közösségi média Andreas Kaplan - Michael Haenlein definíciója alapján „*internetes alkalmazások olyan csoportja, amely a web 2.0 ideológiai és technológiai alapjaira épül, ami elősegíti, hogy kialakuljon és átalakuljon a felhasználó által létrehozott tartalom.*"[2] A kezdetekben szórakoztatatásra létrehozott oldalak hamar túlléptek alapfunkciójukon, és – többek között – a politikai döntéshozatal befolyásolás, a hírszerzés fontos elemeivé váltak. De mit is értünk a közösségi média alatt? Ha a legegyszerűbb megközelítést választjuk, olyan oldalak és alkalmazások összessége, amelyben a tartalmat a felhasználók állítják elő (legyen szó videóról, bejegyzésről stb.), a szolgáltató csupán a keretet biztosítja.

Az első közösségi oldalak a 2000-es évek elején jelentek meg, majd életünk mindennapos részévé váltak. A fejlődésük töretlennek tűnik, ami elsősorban nem egy adott közösségi oldal használatában értelmezendő, gondoljunk csak a magyar fejlesztésű IWIW-re, amely 2014. június 30-án megszűnni kényszerül.[3] A magyarázatot az átalakuló felhasználói preferenciákban kell keresnünk, amelyek

---

*[1] A PRISM a SIGAD (SIGINT Activity Designator, vagyis rádióelektronikai felderítő tevékenységet meghatározó alfanumerikus azonosító) US-984XN kódnevű titkos tömeges megfigyelésre képes elektronikus adatbányász rendszer, ami az 1978-as Foreign Intelligence Surveillance Act (továbbiakban FISA) 2008-as módosítása, és a 2001-es, de 2007-ben módosított Patriot Act rendelkezésein alapul. A megfigyelések jogszerűségének ellenőrzését, illetve a titkos adatgyűjtésre az engedélyt a FISC biztosítja. A PRISM nem egyenlő a kormányzati megfigyelő programmal, csupán a közel két tucat megfigyelő rendszer egyike.*

*[2] KAPLAN, Andreas- HAENLEIN, Michael: Users of the world, unite! The challenges and opportunities of Social Media, Business Horizons, 2010.*

*[3] STRAUB Ádám: Tizenkét év után bezár az iWiW, In. [origo], 2014. május 15. http://www.origo.hu/techbazis/20140514-tizenket-ev-utan-bezar-az-iwiw.html (2014. május 26.).*

megítélésem szerint alapvetően az digitális bennszülöttekre,[4] illetve az ún. C-generációra[5] vezethető vissza. A C-generáció (szemben az "X" vagy "Y" vagy „Z"[6] generációkkal) nem szigorúan demográfiai, születési évek alapján képzett csoport, hanem életmód csoport. Számukra a közösségi média, az okostelefonok használata már-már a Maslow-féle szükséglet hierarchia legalsó szintjén, a fiziológiai szükségletek szintén jelentkezik. Jellemző rájuk továbbá, hogy napjaik nagy részét online töltik, a tartalomfogyasztást, a kapcsolattartást elsődlegesen ezeken az eszközökön végzik, illetve elvárják, hogy az élet minden területén érvényesüljenek a közösségi alapelvek, mint a transzparencia, hozzáférés, megoszthatóság, bevonás, kommentelhetőség.

A tanulmány a célja a közösségi média nyílt forrású hírszerzésben betöltött szerepének vizsgálata. Ennek érdekében a tanulmányban foglalkozom a nyílt forrású információszerzés trendjeivel, a közösségi média ismertetésével.

## A nyílt forrású információszerzés[7]

A nyílt forrású információszerzés (Open Source Intelligence, továbbiakban OSINT) olyan információgyűjtő eljárás, amelynek során a nyilvánosan elérhető forrásokból az információkat felkutatják, elemzik, értékelik és felhasználják egy adott cél érdekében. Az OSINT nem egyenlő az Internetről, a közösségi média eszközeiből szerzett információgyűjtéssel, mint ahogy ebből következően nem az elmúlt évtizedek új eljárása. A hagyományos (nyomtatott és elektronikus) média, szürke irodalom, szakértők és megfigyelők tapasztalatai, kereskedelmi műholdas felvételek, könyvtárak anyagai, tanulmányok, nyilvános konferenciák előadásai, de prospektusok, reklámanyagok mind-mind részét képezhették a nyílt forrású információgyűjtésnek. Ez egyben azt is jelenti, hogy ezt a hírszerző eljárást nem csak a nemzetbiztonsági szolgálatok végzik, hanem a politikai, üzleti, civil szférában egyaránt alkalmazzák.

A nyílt forrású hírszerzést Lévay Gábor fogalmi meghatározását kölcsönözve az alábbiak alapján határozhatjuk meg: *„Az OSINT a katonai felderítés és a hírszerzés rendszerén kívül létező, a publikum (tehát minden egyén) számára nyilvánosan, legális eszközökkel megszerezhető, vagy korlátozott körben terjesztett, de*

---

*[4] PRENSKY, Marc: Digital Natives, Digital Immigrants, On the Horizon. MCB University Press, Vol. 9 Iss: 5, No. 5,2001. október, p. 1-6.*

*[5] Connect, create, contribute, communicate, content creating generation*

*[6] Az „X" generáció alatt 1965 és 1980 között születetteket, „Y" generáció alatt 1980 és 1995 között születetteket, „Z" generáció alatt pedig az 1996-tól születetteket értjük.*

*[7] KENEDLI Tamás: A nyílt információszerzés, In.: Dobák I. (szerk.):A nemzetbiztonság általános elmélete, NKE Nemzetbiztonsági Intézet, Egyetemi jegyzet, Budapest, 2014. pp 183-193.*

*nem minősített adatok szakmai szempontok alapján történő felkutatását, gyűjtését, szelektálását, elemzését-értékelését és felhasználását jelenti*."[8]

Napjainkra a nyílt forrásból megszerezhető adatok száma rendkívüli mértékben megnőtt. Az OSINT jelentőségét erősíti, hogy kis költséggel nyerhető ki nagy mennyiségű információ. Természetesen az OSINT nem képes helyettesíteni a minősített információkat, de ahogy Ferenczy Gábor fogalmazta meg „*a nyílt információforrások a 70-90%-át elégítik ki a teljes felderítő igényeknek. Olyan összefüggéseket tárhat fel, amelyek rámutathatnak egy adott téma lényegére, illetve segíthetik azt, hogy a minősített anyagokban milyen irányban kell összpontosítani a keresést*".[9]

Az OSINT további előnyeként nevesíthető a költséghatékonyság mellett, hogy kockázatmentesen végezhető a kutatás; „up to date", azaz akár valós időben követhetjük az események alakulását; minden területre kiterjed; a szabadon hozzáférhető adatok miatt együttműködés lehetőségét biztosítja külső szakértőkkel, illetve a hírszerző szervekkel. Természetesen az OSINT-nak is megvan a maga árnyoldala, ami elsősorban a hozzáférhető adatok nagy számából, valamint sokféleségéből, eltérő interpretációk gyűjtéséből ered, illetve abból a tényből, hogy a megszerzett adatok akár pontatlanok lehetnek, vagy azokat dezinformációs szándékkal állították elő. A nyílt forrásból hozzáférhető információk dezinformációs céllal történő előállítását hadtörténelmi példák sora igazolja, elég, ha csak Napóleon és Nelson admirális párharcára gondolunk, amikor a francia kormány a Le Moniteurban folyamatosan félrevezető információkat közölt a touloni armada létszámáról, felszereltségéről, rendeltetési helyéről.[10] [11]

Napjainkban már a nyílt forrásból szerzett információk jelentős része származik internetes forrásokból, amelyeknek egy részét a közösségi média szolgáltatja.

## A közösségi média trendjei

A közösségi média az állandó változás terepe. Az egyes oldalak a növekvő reklámbevételekért folytatott harcban folyamatos innovációra kényszerülnek, ami

---

*[8] LÉVAY Gábor: OSINT (Open Source Intelligence) – Nyílt információs hírszerzés. ZMNE, Egyetemi jegyzet, Budapest, 2006. p. 6.*

*[9] FERENCZY Gábor: Internet alapú nyílt információszerzés elvi rendszertechnikai megvalósítása, PhD értekezés, 2007., ZMNE HDI, p. 17.*

*[10] KEEGAN, John: A háborús felderítés, Európa Könyvkiadó, Budapest, 2005.*

*[11] Az már egy másik kérdés, hogy a nem kormányzati ellenőrzés alatt álló újságok indiszkrét szerkesztési elvei, illetve a Napóleon által bevont tudósok pletykái ennek ellenére az Admiralitás, Külügyminisztérium és Hadügyminisztérium más forrásból megszerzett információit erősítették meg.*

rendre új lehetőséget biztosít a nyílt forrású hírszerzésben.[12] De nem csak az eszközök, a felhasználói igények is folyamatosan változnak. A gazdaság, a technikai fejlődés, a felhasználói attitűdök hármasa alapjaiban alakítja át nem csak a társadalom működését, de azokat az eszközöket is, amelyeket nap, mint nap használunk.

2013 áprilisában egy elgondolkodtató írás látott napvilágot a Forbes magazin online felületén.[13] A szerző azzal a felvetéssel játszik el, miszerint a közösségi média eredete Isaac Newtonig vezethető vissza. A tudományos folyóiratok megjelenése, írja a szerző, a 18. századra datálható. Ekkor publikálta a Philosophical Transactions-ben Newton a gravitációs elméletét, aminek hatására tudósok akár hónapokat is hajlandóak voltak utazni Londonba, hogy bekapcsolódjanak a tudományos diskurzusba. Természetesen az analógia csalóka, hiszen a társadalmakban mindig jelen volt az erős közösségi igény, ez csupán átalakult, az internet elterjedésével, leküzdve a legnagyobb idő- és térbeli távolságokat, kiszélesedett a kapcsolattartás lehetősége. A 18. század óta végbement változás folyamatát érzékeljük fejlődésnek.[14]

A közösségi média az én értelmezésemben olyan internetes oldalak és alkalmazások összessége,[15] amelyeknél a tartalmat nem a szolgáltató állítja elő, hanem a felhasználók, a szolgáltató csupán a keretet biztosítja. Az előállított tartalmat aztán a többi felhasználó kiegészítheti, megoszthatja, kommentelheti,[16] ez által új/részben új tartalmat létrehozva (lásd az előbbi ana-

*[12] Nem csupán a különböző adatvédelmi beállítások folyamatos változtatására kell gondolnunk itt, mint pl. a Facebook által bevezetett Graph Search kereső, amelynek hatására a korábban letiltott adatok is nyilvánosságra kerülhettek, míg újból le nem tiltottuk a hozzáférést, hanem a különböző felvásárolt szolgáltatások, start up-ok integrálására is, amelyek adott esetben újabb felületet biztosítanak a felhasználók aktivitásának, preferenciáinak elemzésére.*

*[13] LOELL, Keith: Did Sir Isaac Newton Invent Social Media? In. Forbes, 2013. április 18., http://www.forbes.com/sites/gyro/2013/04/18/did-sir-isaac-newton-invent-social-media/ (letöltve: 2014. május 29.).*

*[14] Bővebben lásd Thomas Kuhn, A tudományos forradalmak szerkezete című művét, melyben ezt a folyamatot „whig" történetírásnak nevezi. KUHN, Thomas S.: A tudományos forradalmak szerkezete, Osiris Kiadó, Budapest, 2002.*

*[15] Pl. közösségi oldalak (Facebook, LinkedIn), a különböző makro- és mikroblogok (Twitter, Blog.hu), kép- és videómegosztó oldalak (Picasa, YouTube) stb.*

*[16] Rendkívül izgalmas kérdés a kommentelésnél az Alkotmánybíróság 2014 májusában meghozott határozata, amely szerint az Internetes tartalomszolgáltató felelős az oldalán megjelenő, nem moderált kommentek tartalmáért. Több jogvédő szervezet, de maga az EBESZ is a véleménynyilvánítás szabadságának sérüléseként értelmezte a határozatot (Bővebben lásd: Tofalvyt: Az Ab komment-döntése veszélyezteti a véleménynyilvánítás szabadságát). Az AB döntése várhatóan átrendezi a felhasználók és a tartalomszolgálta-*

lógia esetében a tudományos diskurzus hatására az elméletek alakulását, formálódását). Elméletileg ez a tartalom folyamatosan változhat. A közösségi médiához sorolom a különböző okostelefonokra írt alkalmazásokat is, hiszen az alkalmazások többsége a felhasználói interakción alapul, illetve integratív szerepet tölt be az egyes közösségi oldalak között. *A tanulmánynak nem célja az egyes közösségi oldalak ismertetése, ezt több cikkemben elvégeztem korábban (pl. „A közösségi média szerepe a katasztrófaelhárításban a Sandy - hurrikán példáján keresztül",[17] illetve „A közösségi média szerepe a 21. század hadseregeiben"[18]).*

Az integráció legjobb példáját a Google szolgáltatja, amely eredetileg egy keresőszolgáltatásként indult, mára azonban az internet megkerülhetetlen részévé vált, egy személyben egyesítve a különböző közösségi eszközöket. A cég szolgáltatásait több tucatban mérhetjük, a felhasználók többsége naponta használja. Nem csupán blogszolgáltató, fénykép- és videómegosztó, közösségi hálózat, de okostelefon platform, műhold- és térképszolgáltatás stb.

Nem célom jelen tanulmányban a közösségi média fejlődéstörténetét vizsgálni, annyiban mégis szükségesnek ítélem, hogy világosság váljék, a közel két évtizedes léte egy intenzív evolúciós folyamat, melynek az egyes szolgáltatók között erős innovációs kényszert eredményez a minél magasabb profit maximalizálás érdekében.[19] Ennek igazolására elég, ha összehasonlítjuk a nagyobb oldalak felhasználókra vetített átlagbevételét, Kleiner Perkins Caufield & Byers 2014-

*tók gyakorlatát, akár teljes egészében tiltva a kommentelés lehetőségét. Ez egyben az új tartalmak előállításának csökkenését is magában foglalhatja, hiszen a felhasználó vagy a tartalomszolgáltató úgy ítélheti meg, hogy a birtokában levő információ megosztása kárt okozhat számára. Másrészt nem szabad figyelmen kívül hagyni, ha egy adott személy preferenciáiról gyűjtünk nyílt forrásból információkat, az internetes aktivitása, ezen belül az általa megosztott kommentek rendkívül hasznos lehet. Tofalvyt: Az Ab kommentdöntése veszélyezteti a véleménynyilvánítás szabadságát, In. Magyarországi Tartalomszolgáltatók Egyesülete, 2014. május 29., http://mte.blog.hu/2014/05/29/ab_kommentdontes_velemenynyilvanitas (letöltve: 2014. június 12.).*

*[17] BÁNYÁSZ Péter: A közösségi média szerepe a katasztrófaelhárításban a Sandy - hurrikán példáján keresztül, In. Fejezetek a kritikus infrastruktúra védelemből, Magyar Hadtudományi Társaság, Budapest, 2013., pp. 281-292.*

*[18] BÁNYÁSZ Péter: A közösségi média szerepe a 21. század hadseregeiben, In. Hadtudomány, 2012/1-2, pp. 152-161.*

*[19] Mi sem mutatja jobban ezt a kényszert, mint a bevezetőben említett, egykoron népszerű magyar közösségi hálózat, az IWIW. Az oldal olyan népszerűségnek örvendett, hogy a magyar lakosság egy részének az internetet jelentette. Azonban a globális versenyben egyre több kihívó lépett színpadra, amelyekre nem volt képes választ adni és megújulni, így a felhasználók átköltöztek másik közösségi oldalakra, elsősorban az állandóan változó, a szolgáltatásokkal kísérletező Facebookra, így az IWIW marganizálódott, a tulajdonos Magyar Telekom pedig 2014 júniusával pedig végleg megszünteti az oldalt.*

es internetes trendjeit elemző jelentéséből kiderül, idén a Google hatszor nagyobb összeget tudhat a magáénak a reklámbevételekből, mint a Facebook, és tizenkétszer, mint a Twitter, igaz, a Facebook és Twitter közel tízszeres ütemben növeli reklámbevételeit.[20]

Annak érdekében, hogy minél többen használják az oldalakat és ezáltal, növeljék reklámbevételeiket, a cégek több ezer szempont alapján értékelik a felhasználókat, hogy minél pontosabban, személyre szabottan célozhassák a reklámokat. Ilyen értékelés alá vetik többek közt, hogy kikkel tartjuk rendszeresen a kapcsolatot, milyen tartalmakra kattintunk, milyen rendszerességgel stb. Ez az eljárás a pontosabb célzás mellett azonban nagyon pontos trend előrejelzést is lehetővé tesz. Nem nehéz ennek a mértékű adatgyűjtésnek a jelentőségét látnunk, ha belegondolunk, egy nap hány esetben használjuk csak a Google valamelyik szolgáltatását szöveg, kép, videó vagy térkép alapú kereséshez, e-mailek kezeléséhez, naptárat, felhő alapú szolgáltatást, Androidos okostelefont, közösségi hálózatot. Online aktivitásunk minden pillanata naplózásra kerül, így az adatbázisokhoz való hozzáférés nem csupán e cégeknek, de a hírszerző szolgálatoknak is rendkívül értékes.[21]

Az elmúlt egy évben nem végeztek részletes szociológiai tényezők alapján elkészített felmérést a hazai közösségi média használatról, de a magyarországi és nemzetközi internethasználat összehasonlításából viszonylag pontos képet nyerhetünk. A Világbank adatai alapján megállapíthatjuk, hogy a magyarországi internethasználat 100 főre vetítve 72 fő.[22] Egy 2013. novemberi nemzetközi kutatás[23] szerint az internetezők alapvetően három oldaltípust böngésznek rendszeresen (1. számú táblázat), amely a hazai látogatottság tekintetében a közösségi oldalak használatában, illetve az e-mailek kezelésében több mint 10%-os többletet jelez, mint globális átlagban véve (míg itthon ez 75 és 68%, nemzetközi viszonylatban 64 és 55%).

---

*[20] MEEKER, Mary: Internet Trends 2014, Kleiner Perkins Caufield & Byers, 2014. május 28., http://s3.amazonaws.com/kpcbweb/files/85/Internet_Trends_2014_vFINAL_-_05_28_14-_PDF.pdf?1401286773 (letöltve: 2014. június 10.).*

*[21] BÁNYÁSZ Péter: A közösségi média használat biztonsági kérdései a védelmi iparban, In. Hadtudomány (Online), 24:1, pp.49-67., 2014.*

*[22] WORLD BANK DATABASE: Internet users (per 100 people), 2013., http://data.worldbank.org/indicator/IT.NET.USER.P2/countries/1W?display=default (letöltve: 2014. június 10.).*

*[23] IPSOS: A különböző internetes oldalak három típusát látogatja heti rendszerességgel a netezők többsége, In. Ipsos, 2013. november 5., http://www.ipsos.hu/site/a-k-l-nb-z-internetes-oldalak-h-rom-t-pus-t-l-togatja-heti-rendszeress-ggel-a-netez-k-t-bbs-ge/ (letöltve: 2014. június 10.).*

| Oldal típus látogatottsága legalább heti rendszerességgel | Nemzetközi viszonylatban (%) | Magyarországi viszonylatban (%) |
|---|---|---|
| Google szolgáltatás | 74 | 67 |
| Közösségi oldalak | 64 | 75 |
| Levelek kezelése | 55 | 68 |

***1. táblázat: Internetes oldalak látogatottsága 2013-ban (saját szerkesztés, forrás: Ipsos)[24]***

A GfK piackutató cég naponta 207 percben mérte 2012-ben az átlag magyar felhasználó napi internethasználatát.[25] Tovább árnyalja a képet egy 2013 januárjában publikált felmérés, amely a közösségi média használat nemzetközi és hazai trendjeit vizsgálta (2. számú táblázat).[26] Ez a hazai közösségi média használatot a globális napi 3,6 órás használattal szemben 2,8 órában mérte, ami korcsoport szerinti bontásban megegyezett az 50 éven felüliek nemzetközi átlagával. A 35 év alattiak, illetve a 36 és 49 év közötti csoportok esetében azonban a nemzetközi használattal megegyező adatokat mértek a kutatók.

| Korcsoport | Nemzetközi viszonylat (óra) | Magyarországi viszonylat (óra) |
|---|---|---|
| Átlag | 3,6 | 2,8 |
| 35 év alatt | 4,2 | 4,2 |
| 35-49 év | 3,1 | 3,1 |
| 50 év fölött | 2,8 | 2,3 |

***2. táblázat: Közösségi média használattal töltött idő (saját szerkesztés, forrás: Ipsos)[27]***

A Digital Insight 2013-as mérése alapján a Facebook még mindig toronymagasan vezet a többi közösségi oldallal szemben (3. számú táblázat),[28] azonban a növe-

[24] *Ipsos, 2013. november 5., http://www.ipsos.hu/site/a-k-l-nb-z-internetes-oldalak-h-rom-t-pus-t-l-togatja-heti-rendszeress-ggel-a-netez-k-t-bbs-ge/ (letöltve: 2014. június 10.).*

[25] *GFK: Egyre nő az internethasználat Magyarországon, In. GfK, 2012. június 10., http://www.gfk.hu/pressreleases/press_releases/articles/010194/index.hu.html (2014. június 10.).*

[26] *Ipsos: A közösségi média úgy vonzza az embereket, mint fény a pillangókat, In. Ipsos, 2013. január 10., http://www.ipsos.hu/site/a-k-z-ss-gi-m-dia-gy-vonzza-az-embereket-mint-f-ny-a-pillang-kat/ (letöltve: 2013. december 8.).*

[27] *Ipsos i.m. 2013. január*

kedési üteme lassulni bizonyul, így a konkurens szolgáltatások csillagászati áron történő felvásárlására kényszerül, hogy az elszivárgó felhasználókat megtartsa. Természetesen a táblázatban szereplő oldalak kultúrafüggőek, a nyugaton kevésbé elterjedt oldalak (pl. a kínai Sina Weibo, a Qzone és a Tencent) a globális versenyben többüket megelőzik.[29]

| Közösségi oldal | Felhasználók száma |
|---|---|
| Facebook | 1,15 milliárd fölött |
| Twitter | 500 millió fölött |
| Google + | 500 millió fölött |
| LinkedIn | 238 millió fölött |
| Instagram | 130 millió fölött |
| Pinterest | 70 millió fölött |

***3. táblázat: Közösségi oldalak a felhasználók száma alapján 2013-ban (saját szerkesztés, forrás: Digital Insights)[30]***

Napjaink tendenciája, hogy a közösségi eszközök a mobil platform irányába mozdulnak el. A 2007-ben piacra dobott iPhone-al számítjuk az okostelefonok megjelenését, ekkor három év alatt 100 millió okostelefont értékesítettek, ami egy év alatt háromszorosára emelkedett, 2013-ra pedig elérte az 1,2 milliárdot. Az előrejelzések 2017-re 4,5 milliárd eladott okostelefonnal/tablettel számolnak.[31]

## A közösségi média OSINT-ban betöltött szerepe

A 2013 nyarától tudjuk, az amerikai Nemzetbiztonsági Ügynökség és partnerszervezetei rendkívül korán felismerték, a közösségi oldalak rengeteg releváns információval szolgálnak. 2007 óta, csupán pár évvel a közösségi média megjelenése után, a PRISM globális megfigyelő és adatbányász rendszer segítségével

*[28] AJMERA, Harsh: Social Media facts, figures and statistics 2013, In. Digital Insights, 2013. szeptember 4., http://blog.digitalinsights.in/social-media-facts-and-statistics-2013/0560387.html (letöltve: 2014. június 10.).*

*[29] BULLAS, Jeff: 5 Insights into the Latest Social Media Facts, Figures and Statistics, In. Jeffbullas.com, 2013. június 4., http://www.jeffbullas.com/2013/07/04/5-insights-into-the-latest-social-media-facts-figures-and-statistic/ (letöltve: 2013. december 8.).*

*[30] AJMERA i.m.*

*[31] BÁNYÁSZ Péter: A közlekedést támogató alkalmazások biztonsági aspektusai, In. Fejezetek a létfontosságú közlekedési rendszerelemek védelmének aktuális kérdéseiről, Nemzeti Közszolgálati Egyetem, Budapest, 2014. pp. 47-60.*

folyamatosan monitorozzák a felhasználói szokásokat, személyes kommunikációt.

Ha figyelembe vesszük, hogy a nagy közösségi oldalak 2007-ben csupán pár éve léteztek, akkor mindez az amerikai szolgálatok gyors helyzetértékeséről tanúskodik. A felhasználók többsége kevésbé érzékeny az adat- és információbiztonságára, így a növekvő internethasználat következtében rengeteg információt gyűjthetünk össze a személyekről, legyen szó preferenciáiról, kapcsolati hálójáról, aktuális tartózkodásáról. Minél többet használ egy személy egy adott eszközt, annál pontosabban következtethetünk egy jövőbeli viselkedésmintára.

Fontos azonban hangsúlyozni a tanulmány elején említett kitételt: ez az eljárás nem képezi részét a nyílt forrású hírszerzésnek, hiszen a nyilvánosság elől védett információkhoz is hozzáfér.

A különbségtétel azért is indokolt a közösségi médiából történő nyílt vagy nem nyílt információszerzés kapcsán, mivel bár mindkettő a közösségi oldalak elemzését végzi, utóbbi olyan információkhoz fér hozzá, amelyet a felhasználók nem osztanak meg nyilvánosan. Ez utóbbit biztosította például az XKeyscore nevet viselő program,[32] amely lehetővé tette, hogy bármilyen bírósági felhatalmazás nélkül, gyakorlatilag egy személyes adat felhasználásával (legyen szó telefonszámról, IP-címről) bármelyik állampolgárt alapos megfigyelés alá vonják. Az ügynökök a program segítségével hozzáférhettek a megfigyelt személy összes e-mailhez, chatbeszélgetéshez, keresési előzményhez.

Az OSINT esetében különbséget kell tennünk a nyílt forrású információgyűjtés céljaiban is, ugyanis teljesen más eljárásokat fogunk követni, amennyiben egyénre bontva vagy tömeges mértékben végzünk információgyűjtést. Egyének esetében elsősorban a célszemély preferenciáit, kapcsolati hálóját térképezhetjük fel, amely a későbbiekben akár irányt adhat egy esetleges titkos információgyűjtésnek vagy ún. social engineeringnek.[33] Az ez irányú információgyűjtés a felhasználók alacsony szintű adat- és információérzékenységén alapul, amit nem szabad alulbecsülni. 2009-ben nagy port kavart a brit sajtóban egy eset, amikor az MI-6 frissen kinevezett igazgatójának felesége Facebookon megosztotta lakcímüket.[34]

---

*[32] GREENWALD, Glenn: XKeyscore: NSA tool collects 'nearly everything a user does on the internet', In. The Guardian, 2013. július 31., http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data (letöltve: 2014. június 12.).*

*[33] A social engineering a pszichológiai manipuláció azon fajtája, amelynek során egy jogosultsággal rendelkező személy bizalmába férkőzünk, hogy az általa birtokolt információkhoz hozzájussunk, vagy egy védett rendszerhez ily módon hozzáférést biztosítson.*

*[34] WALKER, Kirsty: Farce of the Facebook spy: MI6 chief faces probe after wife exposes their life on Net, Daily Mail, 2009. július 6., http://www.dailymail.co.uk/news/article-1197757/New-MI6-chief-faces-probe-wife-exposes-life-Facebook.html (letöltve: 2014. június 12.).*

Azt gondolhatnánk, hogy az eltelt 5 évben, ahogy ezek az eszközök életünk mindennapos részévé váltak, erősödött a felhasználók ez irányú érzékenysége, azonban erre Aamir Lakhani és Joseph Muniz kutatásában rácáfolt.[35] Kísérletükben egy fiatal, csinos hölgyismerősük engedélyével, annak fényképeit felhasználva létrehozták a kitalált Emily Williams hamis Facebook és LinkedIn profilját, majd kapcsolatépítésbe kezdtek egy meg nem nevezett, a kiberbiztonság területén érdekelt amerikai kormányügynökség dolgozóival. Az ismertségek előrehaladtával vacsorameghívásokat, ajánlatokat, de még laptopot is kapott Emily. A következő lépésben egy elektronikus képeslapot küldött Emily a partnereinek, amelynek megnyitása egy fertőző honlapra irányult. Az így feltelepült malware[36] ezt követően különféle jogosultságokhoz, jelszavakhoz jutatta hozzá a támadókat, alkalmazásokat telepítettek a rendszerbe, bizalmas információkat tartalmazó dokumentumokat loptak el. Az áldozatok egyike a hivatal informatikai biztonságáért felelős vezető személy volt. Láthatjuk, könnyűszerrel lehet megtéveszteni azokat a személyeket is, akik elméletileg hivatalból érzékenyebbek az adat- és információbiztonságra, mi több, ők felelősek ennek megvalósításáért.

A támadók rendkívül gyors helyzetfelismerésről, adaptív tulajdonságról tesznek tanúbizonyságot. A tanulmányban már említett IWIW 2014. június 30-ai megszüntetése kapcsán nagyon hamar létrehoztak egy adathalász oldalt, amely a nosztalgiára és tudatlanságra alapozva próbált meg hozzáférni a gyanútlan felhasználók adataihoz, azt ígérve, hogy az oldal nem szűnik meg, csupán máshol folytatja szolgáltatását.[37]

Mivel a nyílt forrású hírszerzést gyakorlatilag bárki végezheti, így nem szabad e kérdéskör tárgyalásakor figyelmen kívül hagynunk a védekezés kérdéseit, hiszen ugyanúgy célpont lehet mindenki. Megítélésem szerint a legfontosabb a megfelelő adat- és információérzékenység kialakítása. Ahogy a közösségi média trendjeinél igazoltam, a gazdasági verseny hatására a nagy oldalak állandó innovációs kényszerben vannak, így az adatvédelmi beállításaink is folyamatos változtatáson esnek át.[38] A kockázatok széleskörűek. Amennyiben elfogadjuk az általam javasolt közösségi média meghatározást, ami a közösségi média körét kiter-

---

*[35] LAKHANI, Aamir- MUNIZ, Joseph: Social Media Deception, In. RSA Konferencia Európa 2013, 2013. október 29-31, http://itcafe.hu/dl/cnt/2013-11/102992/hum-w01-social-media-deception.pdf (letöltve: 2014. június 14.).*

*[36] Az angol malicious software (rosszindulatú szoftver) összevonásából kialakított mozaikszó, a rosszindulatú számítógépes programok összefoglaló neve. Ezek közé soroljuk többek között a vírusokat, férgeket (worm), kémprogramokat (spyware), agresszív reklámprogramokat (adware), a rendszerben láthatatlanul megbúvó, egy támadónak emelt jogokat biztosító eszközöket (rootkit).*

*[37] DAJKÓ, Pál: Átverés az IWIW2, In. SG.HU, 2014. június 18., http://itcafe.hu/hir/iwiw2_adahalasz.html (letöltve: 2014. június 18.).*

*[38] Elég, ha pl. a Facebookra gondolunk, ahol korábban le lehetett tiltani, hogy a nevünkre bárki rákeressen, nemrégiben ezt az opciót megszüntették.*

jeszti az okos eszközökre is, úgy a kockázatok száma is növekszik. Nem csak az esetleges, akár már a gyártósoron feltelepített kémprogramok jelentenek veszélyeket, hanem az egyes feltelepített alkalmazások is, hiszen használatuk érdekében különböző hozzáféréseket biztosítunk személyes adatainkhoz. A Facebook például az alábbi adatokhoz kér hozzáférést: személyes adatok (névjegyadatok), tartózkodási hely (hálózatalapú és GPS alapú helymeghatározás), hálózati kommunikáció (teljes internet hozzáférés), fiókok adatai (üzenetek olvasása), tárhely (lehetőség az USB-tároló tartalmának módosítására vagy törlésére), telefonhívások, hardvervezérlők (fénykép és videókészítés, hangrögzítés), rendszereszközök (szinkronizálás). Természetesen eldönthetjük, hogy feltelepítjük-e az alkalmazást a telefonunkra, de hasonló engedélyeket kér a Google is a szolgáltatásai használataiért cserébe, már pedig egy Androidos telefon esetében nincs döntési lehetőségünk, nem távolíthatjuk el a telefonról a Google alkalmazásait.[39]

A nyílt forrású információgyűjtés esetében megítélésem szerint ez egy szürke zónaként értelmezhető, hiszen bár mi magunk biztosítunk hozzáférést adatainkhoz, ezt csupán az adott alkalmazás készítőjének tesszük. 2013 második negyedévében a Google Playben 1.000.000, az Apple Storeban 900.000 letölthető alkalmazást találhattunk.[40] Nem csak az elérhető alkalmazások száma növekszik rohamosan, hanem a mobileszközökre írt kártékony kódoké is. Míg 2012-ben egészében 35 000 rosszindulatú kódmintát azonosítottak, addig 2013 első felében ez a szám már meghaladta a 47 000-et. Egy kártékony kóddal fertőzött alkalmazás a személyes adatokhoz való hozzáférés mellett a felhasználók pénzét is ellophatja. Nem szükséges azonban fertőzött alkalmazást telepítenünk a telefonunkra, hogy visszaéljenek az adatainkkal, azokat bármikor eladhatják harmadik fél részére, ahogy ez egy zseblámpa alkalmazást használó 100 millió felhasználó esetében is megtörtént.[41]

A nyílt forrású információgyűjtés egy másik iránya a trendelemzés. Az előző fejezetben ismertetett statisztikai adatokból kitűnik, hogy óriási mennyiségű információt birtokolnak az adatbázisok internetes aktivitásunkról. E tanulmány keretei között azonban csupán az elméleti keretek rövid felvázolására nyílik lehetőség. Az NSA vagy a brit Government Communications Headquarters nem csupán titkos információgyűjtést alkalmaz, hanem a különböző közösségi oldalak (blogok, közösségi hálózatok stb.) szisztematikus elemzésével igyekszik prognózisokat, trendelemzéseket végezni belföldön és külföldön egyaránt. Ezen a téren való lemaradását ismerte fel a német Szövetségi Hírszerző Szolgálat

*[39] Van mód természetesen az eltávolításra, de az „rootolás”-nak nevezett eljárás komolyabb informatikai tudást igényel, amellyel az átlag felhasználó ritkán rendelkezik.*

*[40] CZIPPERER Dia: Duplázott a Google Play – 1 millió alkalmazás, In. Prím, 2013. július 25., http://hirek.prim.hu/cikk/2013/07/25/duplazott_a_google_play_1_millio_alkalmazas (2014. június 14.).*

*[41] INDEX: Lebukott a kémkedő zseblámpa, In. Index, 2013. december 6., http://index.hu/tech/2013/12/06/lebukott_a_kemkedo_zseblampa/ (2014. június 14.).*

(Bundesnachrichtendienst), és megbízta a müncheni Bundeswehr Egyetemet, vizsgálja meg annak lehetőségét, hogyan lehetséges a közösségi oldalakon folytatott kommunikáció, tartalommegosztás valós időben történő, automatizált elemzésére.[42]

Az amerikai Titkos Szolgálat (Secret Service) túllépve a közösségi média felületeken keletkező nagy mennyiségű tartalom szintetizálására és vizuális ábrázolására képes analitikus programon, egy olyan alkalmazás kifejlesztését tűzte ki céljául, amely többek között automatizálja a közösségi médiát monitorozó műveleteket, valamint felismeri a szarkazmust a megosztott tartalmakban.[43] Figyelembe véve, hogy egy átlag felhasználó mennyire képes értelmezni a szarkazmust az internetes tartalmakban, amennyiben egy szoftver képessé válik rá, az igen komoly lépésként értelmezhető a mesterséges intelligencia irányába.

## Összefoglaló gondolatok

Tanulmányomban kísérletet tettem a közösségi médiának, mint a nyílt forrású információgyűjtés fontos területének bemutatására. Meglátásom szerint a társadalmi, illetve a technológiai evolúció speciális összefonódása szolgál magyarázatul a közösségi oldalak elterjedésének. Ez a népszerűség a modern gazdaság releváns részét is jelenti egyben, ami kiélezett versenyre kényszeríti a szolgáltatókat a minél nagyobb bevételek megszerzése érdekében. Mindez állandó innovációs folyamatban jelentkezik a különböző oldalak esetében, amely a számos pozitív lehetőség mellett rengeteg kockázatot és kihívást is generál. A nemzetbiztonsági szolgálatok korán felismerték az új technológiában rejlő lehetőségeket, amelyekre szinte azonnal válaszokat adtak a kor és a technológiai lehetőségeknek megfelelően. Ahogy az eszközök, felhasználói preferenciák változnak, úgy a szolgálatoknak is alkalmazkodni kell.

A változás egyben azt is jelenti, hogy e tanulmányban példaként említett kutatások (pl. a Bundesnachrichtendienst vagy a Secret Service esetében) a cikk megírása és annak publikálása között feltehetően jelentkező időbeli eltérés okán már olyan eredményeket adhatnak, amelyek további kutatások témájaként szolgálnak. A folyamatos revízió egyben a kutatók felelősségét is felveti, hiszen ebben a

[42] *Valós időben ellenőrizné a közösségi oldalakat a német titkosszolgálat, In. SG.HU, 2014. június 4., http://sg.hu/cikkek/105721/valos-idoben-ellenorizne-a-kozossegi-oldalakat-a-nemet-titkosszolgalat (letöltve: 2014. június 14.).*

[43] *Zezima, Katie: The Secret Service wants software that detects social media sarcasm. Yeah, sure it will work., In. Washington Post, 2014. június 3., http://www.washingtonpost.com/blogs/the-fix/wp/2014/06/03/the-secret-service-wants-software-that-detects-social-media-sarcasm-yeah-sure-it-will-work/ (letöltve: 2014. június 14.).*

speciális szférában a tudományos eredmények gyakorlati hasznosíthatósága elengedhetetlen.

**Felhasznált irodalom**


- AJMERA, Harsh: Social Media facts, figures and statistics 2013, In. Digital Insights, 2013. szeptember 4., http://blog.digitalinsights.in/social-media-facts-and-statistics-2013/0560387.html (letöltve: 2014. június 10.).
- BÁNYÁSZ Péter: A közösségi média használat biztonsági kérdései a védelmi iparban, In. Hadtudomány (Online), 24:1, pp. 49-67., 2014.
- BÁNYÁSZ Péter: A közösségi média szerepe a 21. század hadseregeiben, In. Hadtudomány, 2012/1-2, pp. 152-161.
- BÁNYÁSZ Péter: A közösségi média szerepe a katasztrófaelhárításban a Sandy - hurrikán példáján keresztül, In. Fejezetek a kritikus infrastruktúra védelemből, Magyar Hadtudományi Társaság, Budapest, 2013., pp. 281-292.
- BÁNYÁSZ Péter: A közlekedést támogató alkalmazások biztonsági aspektusai, In. Fejezetek a létfontosságú közlekedési rendszerelemek védelmének aktuális kérdéseiről, Nemzeti Közszolgálati Egyetem, Budapest, 2014. pp. 47-60.
- CZIPPERER Dia: Duplázott a Google Play – 1 millió alkalmazás, In. Prím, 2013. július 25., http://hirek.prim.hu/cikk/2013/07/25/duplazott_a_google_play_1_millio_alkalmazas (letöltve: 2014. június 14.).
- DAJKÓ Pál: Átverés az IWIW2, In. SG.HU, 2014. június 18., http://itcafe.hu/hir/iwiw2_adahalasz.html (letöltve: 2014. június 18.).
- GFK: Egyre nő az internethasználat Magyarországon, In. GfK, 2012. június 10., http://www.gfk.hu/pressreleases/press_releases/articles/010194/index.hu.html (letöltve: 2014. június 10.).
- GREENWALD, Glenn: XKeyscore: NSA tool collects 'nearly everything a user does on the internet', In. The Guardian, 2013. július 31., http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data (letöltve: 2014. június 12.).
- FERENCZY Gábor: Internet alapú nyílt információszerzés elvi rendszertechnikai megvalósítása, PhD értekezés, 2007., ZMNE HDI
- INDEX: Lebukott a kémkedő zseblámpa, In. Index, 2013. december 6., http://index.hu/tech/2013/12/06/lebukott_a_kemkedo_zseblampa/ (letöltve: 2014. június 14.).
- IPSOS: A közösségi média úgy vonzza az embereket, mint fény a pillangókat, In. Ipsos, 2013. január 10., http://www.ipsos.hu/site/a-k-z-ss-gi-m-

dia-gy-vonzza-az-embereket-mint-f-ny-a-pillang-kat/ (letöltve: 2013. december 8.).
- IPSOS: A különböző internetes oldalak három típusát látogatja heti rendszerességgel a netezők többsége, In. Ipsos.hu, 2013. november 5., http://www.ipsos.hu/site/a-k-l-nb-z-internetes-oldalak-h-rom-t-pus-t-l-togatja-heti-rendszeress-ggel-a-netez-k-t-bbs-ge/ (letöltve: 2014. június 10.).
- LAKHANI, Aamir- MUNIZ, Joseph: Social Media Deception, In. RSA Konferencia Európa 2013, 2013. október 29-31, http://itcafe.hu/dl/cnt/2013-11/102992/hum-w01-social-media-deception.pdf (letöltve: 2014. június 14.).
- LÉVAY Gábor: OSINT (Open Source Intelligence) – Nyílt információs hírszerzés. ZMNE, Egyetemi jegyzet, Budapest, 2006.
- LOELL, Keith: Did Sir Isaac Newton Invent Social Media? In. Forbes, 2013. április 18., http://www.forbes.com/sites/gyro/2013/04/18/did-sir-isaac-newton-invent-social-media/ (letöltve: 2014. május 29.).
- KAPLAN, Andreas- HAENLEIN, Michael: Users of the world, unite! The challenges and opportunities of Social Media, Business Horizons, 2010.
- KEEGAN, John: A háborús felderítés, Európa Kiadó, Budapest, 2005.
- KENEDLI Tamás: A nyílt információszerzés, In.: Dobák I. (szerk.):A nemzetbiztonság általános elmélete, NKE Nemzetbiztonsági Intézet, Egyetemi jegyzet, Budapest, 2014. pp 183-193.
- KUHN, Thomas S.: A tudományos forradalmak szerkezete, Osiris Kiadó, Budapest, 2002.
- MEEKER, Mary: Internet Trends 2014, Kleiner Perkins Caufield & Byers, 2014. május 28., http://s3.amazonaws.com/kpcbweb/files/85/Internet_Trends_2014_vFINAL_-_05_28_14-_PDF.pdf?1401286773 (letöltve: 2014. június 10.).
- PRENSKY, Marc: Digital Natives, Digital Immigrants, On the Horizon. MCB University Press, Vol. 9 Iss: 5, No. 5,2001. október, p. 1-6.
- STRAUB Ádám: Tizenkét év után bezár az iWiW, In. [origo], 2014. május 15. http://www.origo.hu/techbazis/20140514-tizenket-ev-utan-bezar-az-iwiw.html (letöltve: 2014. május 26.).
- SZILÁGYI Szabolcs: A közösségi média története, In. WikiTech, 2011. január 25., http://www.wikitech.hu/mobil/2011/01/25/a-kozossegi-media-tortenete/ (letöltve: 2014. május 29.).
- TOFALVYT: Az Ab komment-döntése veszélyezteti a véleménynyilvánítás szabadságát, In. Magyarországi Tartalomszolgáltatók Egyesülete, 2014. május 29., http://mte.blog.hu/2014/05/29/ab_komment-dontes_velemenynyilvanitas (letöltve: 2014. június 12.).
- Valós időben ellenőrizné a közösségi oldalakat a német titkosszolgálat, In. SG.HU, 2014. június 4., http://sg.hu/cikkek/105721/valos-idoben-

ellenorizne-a-kozossegi-oldalakat-a-nemet-titkosszolgalat (letöltve: 2014. június 14.).

- WALKER, Kirsty: Farce of the Facebook spy: MI6 chief faces probe after wife exposes their life on Net, Daily Mail, 2009. július 6., http://www.dailymail.co.uk/news/article-1197757/New-MI6-chief-faces-probe-wife-exposes-life-Facebook.html (letöltve: 2014. június 12.).
- WORLD BANK DATABASE: Internet users (per 100 people), 2013., http://data.worldbank.org/indicator/IT.NET.USER.P2/countries/1W?display=default (letöltve: 2014. június 10.).
- ZEZIMA, Katie: The Secret Service wants software that detects social media sarcasm. Yeah, sure it will work., In. Washington Post, 2014. június 3., http://www.washingtonpost.com/blogs/the-fix/wp/2014/06/03/the-secret-service-wants-software-that-detects-social-media-sarcasm-yeah-sure-it-will-work/ (letöltve: 2014. június 14.).

# Afganisztán Nemzeti Rendőrsége I. - Az Afgán Rendőrség fejlesztését célzó nemzetközi törekvések

**Dely Péter**

**Absztrakt:**

A cikk az Afganisztáni polgári válságkezeléssel foglalkozik. Bemutatja a Rendőrség képesség- növelésére irányuló nemzetközi projekteket 2001-től napjainkig. Egyrészről az Európai Unió civil kezdeményezéseit, a bilaterális programoktól az Eupolig, másrészt a NATO és az Amerikai Haderő által vezetett rendőrségi fejlesztésekig. Kiemelten foglalkozik a magyar szerepvállalással. Leírja annak történetét, a magyar kiképzők által tartott képzéseket, és a misszió körülményeit.

**Kulcsszavak:** Afganisztán, polgári válságkezelés, képesség fejlesztő programok, Eupol, ISAF

**Abstract:**

The contribution deals with the civilian crisis management of Afghanistan. Introduces the international policeo the capacity building programs since 2001 till lately. On the one hand the EU civilian initiatives, from the bilateral programs to the Eupol, on the other hand the police development of the NATO and the OEP. The hungarian role is accentuated described. Shows its history, the trainings led by hungarian instructors, and the mission conditions.

**Keyworlds:** Afghanistan, civilian crisis management, capacity-building programs, Eupol, ISAF

## Bevezetés

Jelen írásomban az afgán rendvédelem fejlesztésével, annak buktatóival, és azok nemzetbiztonsági hatásaival kívánok foglalkozni. Teszem mindezt két okból. Az első ok, hogy megítélésem szerint a téma aktuális, mert a nemzetközi békefenntartásban Magyarország szerepvállalása az utóbbi pár évben, Afganisztánban csúcsosodik ki, mind katonai, mind rendőri területen. Az Afganisztánban 2004 óta szolgálatot teljesítő rendőrök szinte kizárólagosan, a katonai alakulatok pedig egyéb feladataik mellett végzik a helyi rendőri egységek képzését. A nemzetközi szinten dollár milliárdokra rúgó befektetés felveti a hatékonyság kérdésének vizsgálatát. Ugyancsak nem elhanyagolható kérdés a gyenge rendőrségnek felróható problémák kérdése, melyek hatással vannak hazánk nemzetbiztonságára is, elég csak megemlíteni az Afganisztánban szolgáló magyarok biztonsági helyzetét, a nemzetközi kábítószer kereskedelem hatását, vagy a növekvő számú afgán menekülteket Magyarországon.

A másik ok személyes: 2004-2010 között személyes tapasztalatokat gyűjtöttem az országban. 2004-2005 években a Kabuli Rendőr Akadémia oktatója voltam, bilaterális egyezmény alapján, majd a 2008-as évben az Európai Unió Rendőri Missziójának[1] (EUPOL-Afg) kábítószer ellenes főtanácsadója voltam. 2009-et követően még három alkalommal volt lehetőségem Pol-e Khumriban a magyar Tartományi Újjáépítési Csoport[2] bázisán tevékenykedő magyar rendőri egységnél oktatóként közreműködni kábítószer ellenes tanfolyamok megtartásával.

Ebben az időszakban közvetlen tapasztalatokat, és élményeket szereztem mind a polgári békefenntartás szépségeivel- buktatóival, mind az Afganisztánból induló, vagy onnan eredeztethető nemzetbiztonsági kockázatokkal kapcsolatban.

Terjedelmi korlátok miatt írásomat két részletben közlöm. Az első rész a különböző nemzetközi fejlesztési projektekkel, és kiemelten a magyar szerepvállalással foglalkozik.

A második részben a modern afgán rendőrség felépítését, és a szervezetépítés során tapasztalható problémákat, nehézségeket kívánom taglalni.

## 1. Nemzetközi rendőri projektek, a bilaterális egyezményektől az EUPOL-ig

Mivel Afganisztán újjáépítése nem volt lehetséges a biztonság feltételeinek megteremtése nélkül, ezért a nemzetközi közösség a biztonsági szektor reformját tartotta a legsürgetőbb feladatnak, valamint kiemelt jelentőségűként kezelte és kezeli a mai napig. Az ENSZ felkérése alapján Németország 2002-ben elindította

[1] *EUPOL-Afghanistan (European Union Police Mission in Afghanistan) EUPOL-Afg*

[2] *Provincional Reconstruction Team- PRT*

az afgán rendőrség és határőrség újjáalakítását ezzel is támogatva az Afgán Átmeneti Adminisztrációt. A Németország által elindított fejlesztési program a Német Rendőri Programiroda volt.[3] A németek természetesen látták, hogy egyedül nem képesek a tervezett feladatokat végrehajtani, ezért segítséget kértek az Európai Unió országaitól.

A felhívásra Norvégia és Magyarország válaszolt. Norvégia létrehozta a Norvég Rendőri Programirodát,[4] amely az EUPOL megalakulása után is önálló maradt, megközelítőleg 15 fővel tevékenykednek Kabulban. Fő tevékenységi körük a tanácsadás és mentorállás emberjogi, bűnügyi és kábítószer ellenes területeken. Magyarország egymillió dollár értékű felajánlást tett 2002 januárjában a Tokiói konferencián, a terrorizmus elleni harc elősegítése érdekében. A Magyar Kormány létrehozta a külügyminiszter elnökletével működő Nemzetközi Fejlesztési és Együttműködési Tárcaközi Bizottságot (NEFE), és a 2323/2003 Kormányhatározattal döntött az afganisztáni rendőrség kiképzésében való magyar részvételről.

2004-ben került az első hat fő magyar rendőri szakértő Afganisztánba, a Kabuli Rendőr Akadémiára. A misszió első része 2005-ben véget ért. 2007-ben a magyar Tartományi Újjáépítési Csoport létrehozását követően a magyar rendőrök Baghlan tartományban, Pol-e Khumri városban tevékenykedtek, majd 2010. március 01-jén teljesen beleolvadtak az EUPOL misszióba. A magyar rendőrök tevékenységét a későbbiekben külön kívánom tárgyalni. Németország közben belátta, hogy forrásai még így sem elegendőek az Afgán Nemzeti Rendőrség teljes reformjához, így soros uniós elnöksége alatt kezdeményezte az EUPOL-Afganisztán rendőri válságkezelő erő felállítását, amely 2007. június 15-én megkezdte működését.

A békeműveletek szempontjából tekintve az Afganisztánban működő valamennyi rendőri misszió tevékenysége a békeépítő aktivitási körhöz tartozik. A missziók nem vesznek részt fegyveres műveletekben — fegyvert kizárólag önvédelmi célokra vehetnek igénybe — és nincsenek felhatalmazva rendőri intézkedések foganatosítására a fogadó országban. Nem adhatnak szakmai utasításokat az afgán rendőrök részére, kizárólag ajánlásokat fogalmazhatnak meg, oktatói, kiképzői tevékenységen keresztül tapasztalatokat és szakmai ismeretanyagot adhatnak át.

## 1.1. EUPOL-Afganisztán

Az EUPOL misszió 2007. június 15-én kezdte meg a működését Kabul székhellyel. Mandátuma 2014. december 31-én járt volna le, de az Európai Unió tanácsának 2014. június 23-i döntése meghosszabbította 2016 végéig. A misszió éves költ-

[3] *German Police Project -GPP*

[4] *Norvegian Police Project Office- NPPO*

ségvetése 108 millió euró. Létszáma 281 fő nemzetközi rendőr és 197 fő helyi alkalmazott. Az EUPOL jelenlegi vezetője Karl Aghe Rokhe főfelügyelő (Svédország)[5]

Az EUPOL missziójának három alapvető pillérje van. Ezek:

- A belügyminisztérium szervezeti reformja
- Az Afgán Nemzeti Rendőrség fejlesztése
- A rendőrség csatlakoztatása az igazságügyi reformhoz.

Ezen három pillér megvalósítása céljából hat fő feladatkört határoztak meg:

- A rendőrségi parancsnoklási, ellenőrzési és kommunikációs rendszer reformját
- A hírszerzés alapú rendőri munkát
- A nyomozati részleg képességfejlesztését
- Korrupció-ellenes stratégia bevezetését
- A rendőrségi- igazságszolgáltatási együttműködést
- Az emberjogi és nőjogi aspektusok megerősítését az Afgán Nemzeti Rendőrségen belül[6]

Az EUPOL szervezeti felépítését tekintve egy Kabul székhellyel működő főparancsnokságra, és négy tartományi parancsnokságra oszlik. Ezek: Északi Regionális Parancsnokság- Mazar-e Sharif,[7] Nyugati Regionális Parancsnokság- Herát[8], Déli Regionális Parancsnokság- Kandahár[9], és Központi Regionális Parancsnokság- Kabul[10] (Érdekességként megemlítendő, hogy a központi régió parancsnoka 2008. február és december között egy magyar rendőrtiszt, Kotricz János r. alezredes volt.). Működése során az EUPOL többször átszervezte saját struktúráját. A jelenlegi szervezete négykomponensű, mindegyik komponenst egy helyettes misszióvezető képviseli.[11]

A négy komponens a következő:

- Jogrendi Részleg[12] Feladata: a törvényi szabályozás elősegítése, erős kapcsolat kialakítása a rendőrség és a bűnügyi igazságügyi szektor más szereplőivel,

[5] *www.eupol-afg.eu Letöltve: 2014.11.17.*

[6] *www.eupol-afg.eu/ factsheet 2014 october Letöltve: 2014.11.17.*

[7] *Regional Comman Nort- RCN*

[8] *Regional Command West- RCW*

[9] *Regional Command South-RCS*

[10] *Regional Command Central- RCC*

[11] *A valóságban három helyettes van, ugyanis Thomas Stabler úr képviseli a képzési és a régiós komponenst is.*

[12] *Rule of Law Component*

és a hat fő feladatkörből hármat (korrupció ellenes stratégia, emberjogi, nőjogi aspektusok, rendőrség-igazságszolgáltatási együttműködés) felügyel.

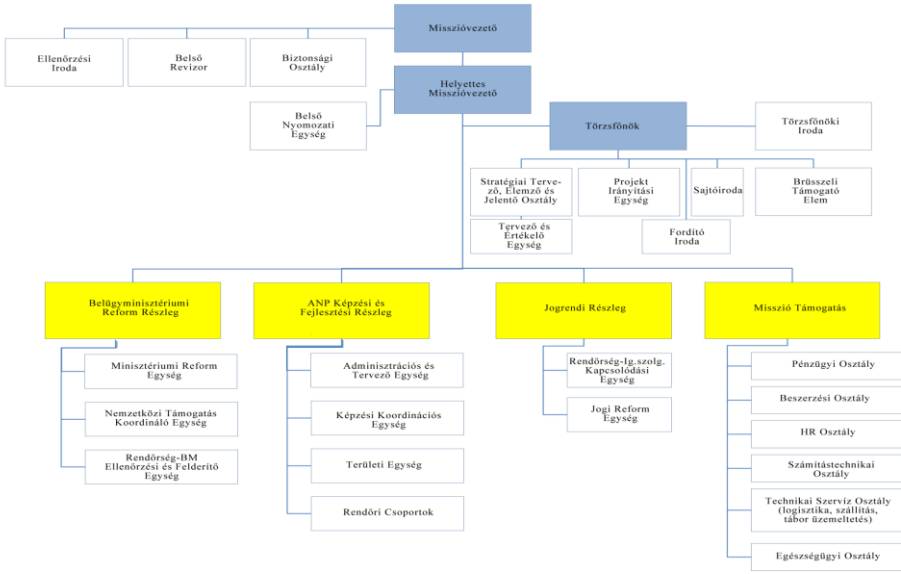
- Képzési Részleg[13] Fő feladata a felsővezető képzés, a bűnügyi nyomozói képzés, és a kiképzők kiképzője[14] képzés. Ezen kívül irányítják az EU két – zászlóshajónak számító – projektjét, az új Rendőrtiszti Főiskolát, és a szintén új Bűnügyi Kollégiumot.
- Rendőrségi Részleg[15] Irányítja a misszió másik három fő feladatkörének megvalósulást, jelesül a rendőrségi parancsnoklási, ellenőrzési és kommunikációs rendszer reformját, a hírszerzés alapú rendőri munkát, és a nyomozati részleg képességfejlesztését
- Területi Részleg[16] A rendőrség, és az ügyészségek munkáját segíti, támogatja a régiós területeken.

2015 januárjától az EUPOL új mandátum alapján tevékenykedik 2016. december 16-ig. Az új mandátum új szervezeti struktúrával jár együtt. Az új struktúra szerint három szakmai és egy támogató részleget állítanak fel. A három szakmai rész a Belügyminisztérium reformjáért felelős részleg[17], az Afgán Nemzeti Rendőrség fejlesztési és képzési részleg[18], és a Jogrendi részleg[19]. A negyedik a Missziótámogató részleg[20]. A misszióban jelenleg szolgálatot teljesítő magyar rendőrök tájékoztatása szerint jelenleg a működési rend kialakítása zajlik. Ami már látható, hogy a rendőri egységekkel szinte minden kapcsolat megszűnik, a mentorállás, fejlesztés csak a minisztériumi és a rendőrség legfelső vezetési szintjén valósul meg. A legújabb szervezeti felépítést az 1. számú függelék tartalmazza.

Kabulban az EUPOL saját központot tart fenn, azonban a régiókban, és a tartományokban kizárólag az ott lévő Tartományi Újjáépítési Csoportok (PRT-k) katonai bázisain tudott működni. Ez biztonsági és logisztikai okokból nem is működhetett másként. A misszió költségvetése saját fenntartását fedezi, így fejlesztési, képzési projektekre külön költségvetést kell találni. Ennek két fő forrása lehet: egyrészről a résztvevő államok a saját, fejlesztésre szánt pénzüket az EUPOL misszión keresztül invesztálják az országba (amint azt a magyar misszió esetében leírtam), másrészt sok esetben amerikai fejlesztési tervekhez biztosít-

[13] *Training Component*
[14] *Train the trainer.*
[15] *Police Component*
[16] *Field Component*
[17] *MOI Reform Component*
[18] *ANP Professionalization and Training Component*
[19] *Rule of Law Component*
[20] *Mission Support*

ják a szakemberállományt. Erre jó példa az amerikai katonai művelet (OEF[21]) által életre hívott vidékfejlesztési program, az FDD[22].




**1.sz. ábra: az EUPOL-Afg felépítése[23]**

Az EUPOL azt is nagyon hamar felismerte, hogy nem az egyetlen szervezet, amelyik rendőrképzéssel, rendőrök mentorállásával foglalkozik. A korábban már említett német és norvég rendőri programirodákon túl a legtöbb PRT folytatott rendőrképzést (például a német Katonai Rendőrség, az olasz Carabinierik). Maga az ISAF is feladatának tekintette a rendőrképzést. Az OEF létrehozott egy saját, rendőrképzést is koordináló szervezetet a CSTC-A-t,[24] valamint alkalmazott két magáncéget, az alap rendőrképzést irányító DynCorpot, és a CNPA-t mentorálló és képző Blackwater céget (megszűnése után SOS International néven jelent meg újra), illetőleg a déli területeken az amerikai tengerészgyalogság[25] is elindított

[21] *Tartós Szabadság Hadművelet – Operation Enduring Freedom- OEF, 2015.01.01. óta Tartós Béke Hadművelet – Operation Enduring Peace-OEP*

[22] *Focus District Development Programe – FDD*

[23] *forrás: EUPOL Stratégiai Tervezési Osztály (fordította: szerző)*

[24] *Combined Security Transition Command- Afghanistan - Összefegyvernemi Biztonsági Átalakítási Parancsnokság*

[25] *US Marine Corps*

egy saját programot. Ezen kívül említést érdemel az UNAMA, az ENSZ afganisztáni missziója, ahol az UNODC[26] képviselői is jelen voltak, illetve számos civil szervezet, NGO[27] is.

A rengeteg szervezet tevékenysége átláthatatlan volt, ezért az EUPOL – megalakulásával egy időben – létrehozta saját alszervezetét, a Nemzetközi Rendőri Koordinációs Testületet,[28] az IPCB-t. Ez a szervezet később a legnagyobb ellenlábasa lett a rendőri fejlesztések irányításában. Példaként elég megemlíteni, hogy 2008-ban a CSTC-A delegáltja, Many-Bear Grindel amerikai ezredes volt az IPCB vezetője. Az általános vélemény az volt a fenti szervezetekről, hogy a legtöbben koordinálni szerettek volna, de senki sem tartott igényt arra, hogy koordinálják.

Az EUPOL fennállása óta számos alapvető problémával kénytelen megküzdeni. Ezek közül is a legnagyobb és legjelentősebb a biztonsági helyzet, és az általa generált nehézségek. 2007 óta gyakorlatilag háborús helyzet van az országban, az afgán biztonsági erők csak Kabulban, és a nagyvárosok belső területein tartják fent az ellenőrzést, de a saját biztonságukat sem képesek teljes mértékben garantálni. Ebben a helyzetben kell/kellene polgári missziót üzemeltetni, polgári rendőrségi szakértőkkel. A legtöbb ország rendőrsége nincs felkészülve az ilyen körülmények közötti munkavégzésre.

Az EUPOL polgárbarát rendőrség létrehozására törekszik,[29] míg az ISAF és főként az OEF félkatonai szervezetet akart, amely átvette volna az ellenőrzést az általuk „megtisztított" területeken.

Ugyancsak probléma a finanszírozás is. Mint említettem, az EUPOL rendelkezik költségvetéssel saját fenntartásához, de nincs pénze a projektek finanszírozásához. Az egyes államok a fejlesztésre szánt pénzükhöz programokat is találnak ki, és nem veszik jó néven, ha az EUPOL bele kíván avatkozni az anyagi források felhasználásába. Más szavakkal ez azt is jelenti, hogy az EUPOL csak az „arcát" adja a nemzeti fejlesztési projektekhez, azokba érdemi beleszólása nincs. A Brüsszel által elvárt, és gyakran hangoztatott „átfogó megközelítést"[30] nem sikerült megvalósítani.

Az utolsó általam megemlíteni kívánt probléma a belső szabályozás. Az EUPOL Szervezeti és Működési Szabályzatát[31] civil szakemberek írták, akik csak Kabulban jártak. Ez alapján kötöttek együttműködési megállapodást a Nemzetközi Biztonsági Együttműködő Erőkkel. Sem a megállapodás, sem a Működési Szabályzat nem volt alkalmazható a Tartományi Újjáépítési Csoportok bázisain, vagy más katonai táborokban. Az ott szolgálatot teljesítő rendőröknek azzal kel-

[26] *UN Office on Drugs and Crime – ENSZ Kábítószer és Bűnüldözési Iroda*

[27] *Non-Govermental Organisation*

[28] *International Police Coordination Board- IPCB*

[29] *community-policing*

[30] *comprehensive approach*

[31] *Standard Operational Procedures -SOP*

lett szembesülniük, hogy vagy irodáikban ülnek érdemi munka nélkül, vagy folyamatosan megsértik saját belső szabályzóikat. (Ezen megállapításom igazolására a következő példát hozom: az ISAF saját fényképes azonosító kártyát adott ki, amely nélkül nem lehet katonai táborban mozogni. Ebből természetesen több féle volt jogosultság/lehetőség szerint, ezek egymástól színükben – jól látható módon –eltértek. Az EUPOL tagjai a rózsaszín „Civil" jelzésű kártyára voltak jogosultak. Ezzel szabadon mozoghattak a katonai táborokban, de nem léphettek kíséret nélkül a hadműveleti területre, az étkezdébe, a sportkomplexumokba, és nem voltak jogosultak az egészségügyi segélyhelyek szolgáltatásainak igénybe vételére sem. Ez Kabulban, a saját EUPOL tábor esetében nem okozott gondot, ám aki életvitelszerűen ISAF táborban tartózkodott, az hivatalosan működésképtelen volt a rózsaszín kártyával. Természetesen minden nemzet katonai egysége kiadta saját országa rendőrei számára a szürke „Military" jelzésű kártyát, amelylyel ezek a problémák megszűntek. A kártya használatával viszont az EUPOL alkalmazásában álló rendőr folyamatosan megsértette a Működési Szabályzatot. A probléma 2008-ban mindenki számára ismert volt, és hallgatólagosan mindenki szürke kártyát használt, de megoldás nem született.)

## 1.2. A magyar szerepvállalás története

### 1.2.1. Kabuli Rendőr Akadémia 2004-2005

Mint korábban említettem, az első magyar rendvédelmi szakemberek 2004 májusában kerültek a Kabul Rendőr Akadémiára. A hat fő először két hónapot töltött ott. A következő hat fős kontingens 2004 augusztusában érkezett és decemberig maradt. 2005 februárjában ismét érkezett egy négyfős csoport, amely augusztusig maradt. Ezt követően 2007-ig nem volt magyar rendvédelmi szakember Afganisztánban.

Ebben az időszakban a Német Rendőri Programiroda (GPP) irányítása alatt rendvédelmi szakembereink az akadémián oktattak, főként felsővezetői kurzusokon. Tevékenységük ideje alatt 1100 fő tábornok és ezredes végezte el a tanfolyamot, gyakorlatilag az akkori afgán rendőri felső vezetés egésze. Eredetileg rendőri alapképzésre érkeztek, de azt idő közben az amerikai DynCorp nevű magáncég átvette Afganisztán teljes területén, és végzi a mai napig is, több millió dolláros költségvetéssel, saját alapfokú rendőriskola rendszer kiépítésével.

A magyar szakemberek által oktatott témakörök a rendőri „túlélési technikák", tömegdemonstrációk kezelése, a katasztrófa helyzetekre történő rendőri reagálás, személyvédelem, közlekedés-szervezés baleseti helyszínelés, és a terrorizmussal kapcsolatos rendőri feladatok voltak, mivel ezekben a témakörökben sem a német, sem a norvég fél nem rendelkezett oktatókkal.

Az akkoriban Kabulban állomásozó magyar Könnyű Vegyes Gyalogszázad felkérésére járőr és forgalomirányítási ismereteket is oktattak a magyar ISAF alegység felelősségi körzetében lévő rendőrállomás állományának.[32]

## 1.2.2.Magyar Rendőri Kontingens Pol-e Khumriban 2007-2009

Tekintettel a kabuli kiképző csoport eredményeinek pozitív nemzetközi megítélésére, az Igazságügyi és Rendészeti Minisztérium a 2115/2006. (VI. 29.) számú kormányhatározat megjelenését követően megkezdte a Tartományi Újjáépítési Csoportban való rendvédelmi szerepvállalás előkészítését. 2007. február 26. és március 3. között rendőri előkészítő csoport utazott a magyar PRT-ba. Feladatuk a tájékozódás, oktatási programok egyeztetése a nemzetközi és helyi rendőrséggel, állapotfelmérés, és az oktatási helyszín kiválasztása volt. A tényleges misszió 2007 augusztusában kezdődött.

A körülmények és a biztonsági helyzet leírására abból a jelentésből idézek, melyet kollégáimmal a Külügyminisztérium számára készítettünk:

*„Az Afgán Nemzeti Rendőrség működési körülményeiről megállapítható, hogy a bizonytalan stabilitású ázsiai országban jelentős kockázatnak teszi ki magát az, aki a rendőri hivatást vállalja. A lázadó szélsőséges csoportok a rendőrségben ellenséget látnak és támadásaik célpontjai gyakran a járőröző, vagy ellenőrzőáteresztő pontot működtető rendőri egységek.*

*Hiányos felszerelés, jelentős kiképzésbeli hiányosságok és erősen amortizálódott technikai eszközpark, valamint leromlott állapotú rendőrségi épületek jellemzik meg a tartományi rendőrséget.*

*Nemegyszer előfordul, hogy tálib, vagy szervezett bűnözői csoportok aknát telepítenek a járőrözési útvonalaikra, rakétavetővel támadják a rendőrőrsöket, vagy öngyilkos merénylő robbantja fel magát a közelükben. Minden veszély ellenére van jelentkező a rendőri pályára. Az újonnan felszerelők közül egyre többen látják úgy, hogy az afgán rendőrség kulcsfontosságú szereplője az ország belbiztonsági környezetének és csak alapos felkészültséget követően lehet hatékonyan fellépni az őket érő támadásokkal szemben. Az is világossá vált számukra, hogy a nemzetközi erők nem fognak örökre Afganisztánban maradni és ebből adódóan az afgán rendőrségnek – valamint a hadseregnek is – olyan felkészültségi szintet kell elérnie, ahol már önállóan is képesek hazájuk biztonságát szavatolni. Komoly problémát jelenít meg, hogy a rendőri állományba kerülésnek nem feltétele az írni és olvasni tudás.*

*Az alacsony fizetések miatt a rendőri testület korrupcióval erősen áthatott, és jelentős a fluktuáció. Az afgán rendőrségről alkotott lakossági kép erősen változó képet mutat. Vannak olyan területei az országnak, különösen a központi irányí-*

[32] *Afgán Misszió 2007 PPT előadás (Magyar Rendőri Kiképző Kontingens)*

*tástól távoli tartományokban, ahol a rendőrség tagjai jövedelmüket kábítószer-csempészetből és bűncselekmények elkövetéséből egészítik ki. Az ilyen helyeken a lakosság nem a biztonság felelőseit és védelmezőiket látja a rendőrökben, hanem „kirablóiknak" tartja őket.*

*A tartomány közlekedési rendőrsége ellenőrzi Afganisztán egyik legfontosabb útszakaszát, amely a fővárost, Kabult köti össze az északi tartományokkal és az északról szomszédos országokkal – Tádzsikisztánnal, Üzbegisztánnal és Türkmenisztánnal. Ezen az úton van továbbá az ország kereskedelmének és közlekedésének stratégiai fontosságú átjárója, a Salang-hágó – a Hindukus-hegység 3450 méter magasságban levő egyetlen észak-déli átjárója – amelynek alagútjait folyamatos őrizettel szintén a közlekedési rendőrség biztosítja. A közlekedési szabályok betartatására a rendőrség egyre nagyobb hangsúlyt fektet, és erőteljes törekvések vannak a közlekedési balesetek visszaszorítására.*

*A tartományi büntetés-végrehajtási intézet személyzete szintén a rendőrség állományából kerül ki. A börtönben – európai szemmel nézve – szinte elképzelhetetlen állapotok uralkodnak. Itt a börtön valóban súlyos büntetést és bűnhődést jelent annak, akit szabadságvesztésre ítélnek és idekerül. Az intézményben nincs vezetékes víz, a szennyvíz nagyrészt a földfelszínen folyik el, a zárkákban legtöbb helyen csak földre vetett szőnyegen alszanak az elítéltek és nincs fűtés sem. Ellenben van: sorban állás a napi betevő falatért és az alig iható vízért, valamint nyáron rekkentő hőség és télen dermesztő hideg a cellákban."*

A rendőri kontingens kettős tevékenységet végzett az afgán rendőrség fejlesztése érdekében. Egyrészt szervezett körülmények között oktatásokat, vezetői felkészítéseket és gyakorlati kiképzést nyújtottak a képzésre rendelt állománynak, másrészt a rendőrség technikai és infrastrukturális környezetében hajtottak végre fejlesztéseket.

Az oktatás és képzés a Pol-e Khumri rendőrkapitányságon kialakított oktatóépületben valósult meg. Az épület megfelelővé tétele a kontingens munkájának volt köszönhető, ami alkalmassá vált arra, hogy egyidejűleg 28-30 fő tanuló oktatása valósuljon meg oktatás-technikai eszközök — laptop, projektor, tábla — alkalmazása mellett. A képzési munka alapvetően a Magyarországról érkező oktatók, valamint a kontingens által közösen kéthetes ciklusokban megtartott tanfolyamaira épült, ami kiegészült olyan tanfolyam megtartásával is, ahol az előadó – speciális tárgy miatt – a helyi szakemberek közül került kiválasztásra. Ebből következik, hogy a három fő állandó jelleggel Afganisztánban tartózkodó rendőrtiszt nemcsak oktatásokat tartott, de megszervezte azokat a képzési ciklusokat is, amelyekre Magyarországról érkeztek szakemberek.

A teljesség igénye nélkül felsorolva az alábbi képzéseket vezették le a magyar oktatók 2007. júliustól 2010. januárig:

- Közlekedési baleseti helyszínelői tanfolyam
- Intézkedéstaktikai képzés

- Kiképzők kiképzése tanfolyam
- Középvezetők részére szervezett tanfolyam
- Afgán rendőrnők részére szervezett tanfolyam I.
- Afgán rendőrnők részére szervezett tanfolyam II.
- Bűnügyi nyomozói tanfolyam
- Bűnügyi helyszínelői tanfolyam I.
- Bűnügyi helyszínelői tanfolyam II.
- Közlekedésrendészeti tanfolyam
- Taktikai és lőkiképzési tanfolyam
- Műszaki mentő és tűzoltási szaktanfolyam
- Tűzszerész ismeretek képzés, kiegészítve elsősegély nyújtási oktatással
- Alkotmányjogi és választásjogi képzés
- Számítástechnikai képzés
- Írás-olvasás, oktatás
- Angol nyelvoktatás

A vezényelt hallgatók napidíjat és étkezési költségtérítést kaptak a tanfolyamokon való részvételükért. Azoknak az afgán rendőröknek, akik korábban nem tanultak meg írni és olvasni, a kontingens helyi tanító alkalmazásával írás-olvasás tanfolyamot szervezett. A tanfolyamok minden alkalommal gyakorlati vizsgával, vagy felméréssel zárultak. Baghlan tartomány 2008 – 2009 években mintegy 1.100 fős rendőri állománnyal rendelkezett, amiből 2009. február végéig 321 fő vett részt olyan oktatáson, amit a magyar rendőri kontingens szervezett.

Mindezen tanfolyamokhoz és fejlesztésekhez a Külügyminisztérium biztosított évi 92 millió forintos költségvetési keretet.

A magyar részvétellel párhuzamosan 2007-ben elindult az EUPOL misszió is, és küldött rendőröket a magyar PRT-ba. Magyar szempontból a lényegi különbség a Pol-e Khumriban tevékenykedő magyar missziós és EUPOL állományú rendőr között az volt, hogy az utóbbi logisztikai támogatását és napidíját az EUPOL finanszírozta. Ezen tényre való tekintettel a magyar missziót felügyelő rendőri és politikai vezetés a magyar kontingens „átsapkázása", az EUPOL missziója történő beléptetése mellett döntött, így a KüM által biztosított költségvetés teljes egészét a fejlesztési projektekre lehetett fordítani. 2010 óta a magyar rendőrök kizárólag EUPOL alárendeltségben tevékenykednek.

## 2. Az ISAF/RSM rendőrséget érintő programjai, stratégiája, és az FDD

Mint azt már korábban leírtam, a 2001 decemberében Afganisztánban megjelenő nemzetközi és amerikai haderő elsődleges feladatának tartotta a biztonsági erők reformját. A tálib rezsim megszűnését követően sem jó, sem rossz biztonsági rendszer nem maradt hátra. Az országban uralkodó polgárháborús viszonyok miatt ésszerű választásnak tűnt a katonai jellegű szervezetek kiépítése. Megjele-

nésük elején az újjászervezett Rendőrség (és természetesen a Haderő is) az OEF/ISAF által megtisztított területek felügyeletét kapta meg elsődleges feladatának. A klasszikus rendőri munka a tálib rendszer előtti időből megmaradt szakemberek, és az ellenállásban érdemeket szerzett – főként mudzsahed – harcosok által alkotott új szervezet felügyelete alá került. Az OEF létrehozta saját szervezetét, a CSTC-A-t, mely a biztonsági erők reformjáért volt felelős. Azt már a legelején felmérték, hogy a katonai erők nem képesek a rendőri oktatás/képzés megszervezésére, így azt magáncégekre bízták. A DynCorp nevű magán biztonsági cég kapta meg a munkát. Az országban nyolc helyen alapított rendőri alapképző intézményt.[33] Az oktatás nyolc hétig tartott, a tananyagot az akkori igényekhez alakították. A gyakorlatban ez azt jelenti, hogy az első hét hétben főleg katonai, harcászati anyagokat oktattak, csak az utolsó hétben került sor rendőri jellegű oktatásra. Bár a nyolcadik heti tananyagról is elmondható, hogy ugyan annyi óraszámban oktatták a bilincselést, mint a hatályos afgán törvényeket.

A területeken lévő egységek mind feladatuknak kapták az ott települő rendőri alakulatok valamilyen jellegű képzését. Így történt, hogy a rendőrképzést végzett a már korábban megemlített Tengerészgyalogság, az olasz Carabinierik, és a német Katonai Rendőrség.

2004-ben a Kabulban lévő Könnyű Gyalog Század is feladatul kapta egy, a déli városrészben lévő külvárosi rendőrőrs mentorállását. Ők intézkedéstaktikai/bilincselési képzést tartottak, valamint felkérték az akadémián lévő magyar rendőri kontingenst forgalom-irányítás oktatására.[34]

A civil válságkezelő erők megjelenésével a képzés nagy része a különböző rendőri missziók hatáskörébe került, de az ISAF, és főleg az OEF nem mondott le a felsővezetői szint mentorállásáról. Az ISAF katonákkal, az Egyesült Államok a DynCorp és a Blackwater cégek által fizetett nyugdíjas rendőri szakértőkkel végezte e tevékenységét. A mentorállás során kialakult visszásságokról a következő fejezetben kívánok említést tenni.

2007 végére a CSTC-A felismerte, hogy az országban uralkodó viszonyokat, különös tekintettel a korrupcióra, és a rendőrség tehetetlenségére, nem lehet a központból megoldani, így elindította a már korábban is megemlített vidékfejlesztési programot, az FDD-t.

Az FDD egy eredetileg három éves lefutású programként indult, a tervek szerint a 34 tartomány mind a 365 járása sorra került volna. A cél az AUP képességeinek fokozása volt.

---

[33] *Central Training Center- Kabul, Regional Training Center hét darab*

[34] *A forgalom-irányítási képzés az első ilyen volt Afganisztánban, de az hamar világossá vált, hogy a regnáló közlekedési kultúra mellett egy ilyen oktatás értelmetlen. A gyakorlati tréning három órájában hét koccanásos baleset történt a felügyelt kereszteződésben, ebből hármat ISAF járművek okoztak.*

A terv szerint egy Járási Felmérő Csoport (DART)[35] utazott a fejlesztés alá vont járás rendőri központjába. A csoport alapvetően az OEF állományába tartozó katonákból áll, általában nyolc főből. Hozzájuk csatlakozott az afgán Belügyminisztérium, és a Legfőbb Ügyészség képviselője. A szakértői részt civil rendőri oktatók (a DynCorp cégtől), és lehetőség szerint az EUPOL egy tagja képviselte. Ugyancsak csatlakozott a területileg illetékes PRT képviselője is. Az FDD program szerint a DART egység a helyszínen felméri a teljes rendőri állományt, beosztások, munkakörök, iskolai végzettségek, illetve az épület, gépjármű, és egyéb felszerelések helyzetét. A felmérés két hete után a rendőrség teljes állományát nyolc hetes képzésre viszik a legközelebbi régiós oktatási központba (RTC), és ez idő alatt egy ANCOP egység Kabulból veszi át a napi ügymenetet, a DART irányítása mellett. A nyolc hét alatt végrehajtják a szükséges technikai fejlesztéseket, és az épület modernizálását (alapvető biztonsági és technikai fejlesztések, áramellátás, stb.), és az állomány visszaérkezése után további egy hónap közös munka következik a DART csoporttal. Ezt követően a csoport távozik, és egy újabb hónap múlva visszatér ellenőrizni a rendőrállomás működését. Ezt követően az ellenőrzést a területileg illetékes nemzeti PRT végzi.[36]

Az elgondolás jó volt, az első alkalmakkor sikerekről számoltak be. A nehézséget az okozta, hogy a CSTC-A nem rendelkezett elegendő szakember állománnyal, egy idő után nem tudott rendőrségi szakértőket hozzárendelni a katonai csoportokhoz. Ugyancsak rájöttek, hogy a program során átképzett, ellenőrzött, majd magukra hagyott rendőrök között nem csökkent a korrupció mértéke, és nem javult a munkájuk színvonala sem. Végül az FDD programot anélkül fejezték be 2012-ben[37], hogy végig ért volna mind a 365 járáson.

Az FDD programmal párhuzamosan folyt egy katonai kiképzési program is, a Műveleti Támogató és Összekötő Csoport.[38] Az OMLT leírása nem képezi részét írásomna – lévén katonai képességnövelő program – de annyit érdemes megemlíteni, hogy a programban szereplő alegységek nem csak képezték a gondjaikra bízott afgán zászlóaljakat, de együtt harcoltak velük, irányították azokat a feladatellátás során.

Az FDD program sikertelensége és az OMLT sikeressége nyomán a CSTC-A a Rendőrségi OMLT-k (POMLT) létrehozása mellett döntött. Tanulva az előzőleg elkövetett hibákból, már a program elindítása előtt rendőrségi szakértők közreműködését kérte az EUPOL-tól, és a NATO műveletben részt vevő országoktól. Terveik szerint minden forrást biztosítottak volna, csak a szakember állományt

[35] *DART- District Assessment Reform Team*

[36] *Petty Officer 2nd Class Paul Dillard, "Provincial development added to FDD program," The Enduring Ledger, Combined Security Transition Command-Afghanistan (CSTC-A) Public Affairs, February 2009, p.6.*

[37] *Solar year 1391- Afghan National Police Strategy http://moi.gov.af/en/page/5076*

[38] *Operational Mentoring and Liaison Team OMLT*

kérték közreműködésben. A POMLT végül nem indult el, közreműködők hiányában.

2009 év végére a mind az ISAF mind az OEF belátta, hogy a korábbi út nem járható. Novemberben megalakult a NATO Kiképző Misszió Afganisztán[39] a CSTC-A irányítása alatt. Ennek egyik pillére a Rendőrségi Intézményi Tanácsadó Csoport (PIAT),[40] amely minisztériumi, és felsővezetői szinten működik. A csoport alapvető feladata egy hosszú távú fejlesztési terv, az Egységes Átalakítási Terv[41] kidolgozása. Ennek érdekében elengedhetetlen a koordináció az EUPOL-lal, az IPCB-vel, a GPPT-vel.[42] Ugyancsak elsődleges feladat a Regionális Kiképző Központok, RTC-k fejlesztésének segítése. Fontos programjuk, az írásbeliség fejlesztése és az írástudatlanság felszámolása.

További feladata a PIAT-nak az általa felügyelt szinteken a jogrendiség és bizonyíték alapú rendőrségi eljárások bevezetésének irányítása és felügyelete mind a képzésben, mind a napi munkavégzésben.

Ugyancsak segítik az afgán rendőrség saját nemzeti fejlesztési programját a képzések menedzselésével, és az oktatási programok bevezetésével.[43]

2014. december 31-én az ISAF misszió megszűnt, a helyét a Határozott Támogatás Művelet (RSM)[44] vette át. A névváltoztatás mögött alapvető különbség, hogy 2015. január elsejétől a NATO nem működik közre az afgán biztonsági helyzet stabilitásában, az teljes mértékben az afgán biztonsági erők feladatkörébe került. Ebből adódóan az országban nem harcoló regionális parancsnokságok, hanem tanácsadó központok vannak, amelyek a járőrözés helyett napi egy kijárásos (Level-1) tanácsadást működtetnek felső vezetői (dandár+) szinten. Az elgondolás az, hogy már a képzést is az afgán hatóságok vezessék, a RSM csak felügyeli azt. A jelenleg Mazar-e Sharifban tartózkodó volt magyar nemzeti rangidős tiszt[45] Balogh Péter ezredes szóbeli tájékoztatása szerint a valóságban még mindig egyszerűbb megtartani magát a képzést, és az esetek legnagyobb részében így működik a napi tanácsadás. Ugyancsak elmondta, hogy a jelenleg szolgálatot teljesítő magyar katonák feladata a 3. ANCOP dandár,[46] és a 806. határőrzóna[47] mentorállása.

---

*[39] NATO Training Mission Afghanistan NTM-A*

*[40] Police Institutional Advisory Team PIAT*

*[41] Unified Transition Plan UTP*

*[42] Bár az IPCB maga a koordinálásra létrehozott szerv, az ISAF iratok, mint a koordináció egyik szereplőjét említik*

*[43] RS Security Force Assistance Guide 3.0 p.58-60*

*[44] Resolute Support Mission RSM*

*[45] Senior National Representaive SNR*

*[46] Az északi Balk tartományban települt dandár*

*[47] Az északi területen 2500 km hosszú határ őrzésével megbízott, kb.4000 fős egység*

**Felhasznált Irodalom**:


- Dr. univ. Boda József rendőr ezredes: A rendvédelmi békefenntartás kialakulása, fejlődése, helye és szerepe a XXI. században ; doktori értekezés Zrínyi Miklós Nemzetvédelmi Egyetem Doktori Tanácsa, Budapest, 2007
- Dr. Vida Csaba alezredes PPT előadása "Válságkörzetek és Nemzetközi Békemissziók és Műveletek" 2014
- EUPOL- Introduction Course CN presentation 2008
- ISAF/RSM RS Security Force Assistance Guide 3.0
- Petty Officer 2nd Class Paul Dillard, "Provincial development added to FDD program," The Enduring Ledger, Combined Security Transition Command-Afghanistan (CSTC-A) Public Affairs, February 2009
- Solar year 1391- Afghan National Police Strategy http://moi.gov.af/en/page/5076
- Hughes, Michelle: USIP Special Report 346 The Afghan National Police in 2015 and Beyon 2014.05.
- Islamic Republic of Afghanistan Ministry of Interior Affairs Deputy Minister for Strategy and Policy Department of Strategy : National Police Plan for Solar Years (SY) 1390-1391 2011.04.
- Islamic Republic of Afghanistan Ministry of Interior Affairs Deputy Minister for Strategy and Policy Department of Strategy : Afghan National Police Strategy 2010.12.
- Magyar Honvédség Afganisztán CIMIC kézikönyv 2006
- Magyar Rendőri Kiképző Kontingens: Afgán Misszió 2007 PPT előadás
- Saideman, Stephen és Auerswald, David: Comparing Caveats: Understanding the Sources of National Restrictions upon NATO's Mission in Afghanistan.
- www.honvedelem.hu/cikk/32092/kulcsszo:-bekes-konfliktuskezeles,-vesztesegminimalizalas
- www.unodc.org
- www.eupol-afg.eu
- www.eupol-afg.eu/factsheet
- www.ipcb.worldpress.com

# Nemzetbiztonsági célú rövidhullámú stratégiai COMINT rendszerek elektronikai védelmi megfontolásai

**Kovács Róbert**

**Absztrakt:**

Az 1990-es rendszerváltást követően Magyarországon létrejött demokratikus nemzetbiztonsági szolgálatok struktúrája új keretet adott a magyarországi rádiófelderítő tevékenységnek. A közelmúlt technológiai fejlődése (szélessávú feldolgozás, szoftverrádió technológia, többcsatornás vevőrendszerek) a rövidhullámú felderítésben is új technológiai, szervezési megközelítéseket követelt meg. A stratégiai adatszerző rendszerek egyik legfontosabb jellemzője, hogy az elektronikai védelem eszközeivel hogyan képes az elektronikai támadásokkal szemben fellépni.

A cikk a rövidhullámú sávú adatszerzés sajátosságainak bemutatásával, rövid történeti áttekintést nyújt a jelenlegi magyarországi rádiófelderítés szervezeti rendszerének kialakulásáról és tematikusan vizsgálja a rövidhullámú stratégiai adatszerző rendszer elemeinek (stacioner RH központ, stacioner és mobil RH szenzorok) lehetséges elektronikai védelmi aspektusait.

**Kulcsszavak:** stratégiai, rádiófelderítés, rövidhullámú, elektronikai védelem, nemzetbiztonság

**Abstract:**

After the change of regime in 1990, the new democratic structure of national security services provided a new framework for radio reconnaissance activity in Hungary. The recent technological improvements (wideband proccessing, software radio technology, multi-channel receiver systems) also required a new technological, organizational approaches in shortwave signal intelligence. The key feature of strategic data gathering systems is how to use the measures of electronic protection to act against electronic attacks.

Based on introducing the particularities of data gathering in HF band, this article is intended to provide short historical overview of the current Hungarian radio reconnaissance formations and thematically examines the potential electronic protection aspects of a strategic shortwave data acquisition system components (stationary HF centers, stationary and mobile HF sensors).

**Keywords:** strategical, SIGINT/COMINT, shortwave-high frequency, electronic protection measures, national security

## Bevezetés

A nemzetbiztonsági célú rövidhullámú sávú stratégiai rádiófelderítő rendszerekben alkalmazható elektronikai védelmi lehetőségek nagymértékben függnek a rendszerek sávspecifikus kialakítási lehetőségeitől, fizikai, technológiai sajátosságaitól. A mai magyarországi nemzetbiztonsági célú adatgyűjtéshez kapcsolódó elektronikai védelmi intézkedések meghatározásához szükséges megvizsgálni a rádiófelderítésnek hátteret adó hullámtartományi sajátosságokat, a magyarországi szervezeti berendezkedést, valamint a stratégiai rendszerek elemeinek egyedi jellemzőit, melyek befolyásolják az alkalmazható védelmi módszerek körét. A rövidhullámú stratégiai rádiófelderítő rendszerek jellemzői áttekintésének, a főbb rendszerelemek egyedi vizsgálatának célja annak megválaszolása, hogy elektronikai védelmi szempontból ezen rendszerelemek mutatnak-e olyan sajátosságokat, amelyek meghatározók a rendszer egésze szempontjából.

## 1. Rövidhullámú adatszerzés sajátosságai

### 1.1 Hullámterjedés a rövidhullámú sávban

A földfelszíni adó és vevőberendezések között a rádióhullámok alapvetően két fajta módon terjednek. A Föld felszínének közelében, mint felületi vagy talajhullámok illetve a nagyobb magasságokban az ún. térhullámok útján.

A rövidhullámú (3-30 MHz) tartományba eső elektromágneses hullámok terjedésében jelentős szerepe van a Föld légkörének az atmoszférának. Azon belül is a tropopauza[1] felett kb. 10-11 km-es magasságtól kezdődő sztratoszféra valamint az afölötti, hozzávetőleg 80-800 km-es magasságban elhelyezkedő, ionoszférának nevezett tartományoknak. Jelentőségük annak köszönhető, hogy a Nap ultraibolya és korpuszkuláris sugárzásának[2] valamint egyéb sugárzások (pl. kozmikus háttérsugárzás) hatására a semleges gázmolekulák ionizálódnak, ezáltal elektromos vezetőképességre tesznek szert, így az elektromágneses hullámok ebbe a közegbe érkezve elhajlást szenvednek, ami bizonyos frekvenciatartományban az ionoszférától nagy távolságból szemlélve visszaverődésként (reflexióként) vizsgálható.

Az ionoszféra ionkoncentrációja a magasság, napszak, évszak, naptevékenységek függvényében időben és térben változó tulajdonságot mutat, azonban ezzel együtt vannak bizonyos – reflektálóképesség szempontjából - viszonylag karakterisztikusabb tulajdonságokat mutató tartományai.

---

[1] *viszonylag stabil állandó hőmérsékletű átmeneti réteg a troposzféra és sztratoszféra között*

[2] *részecske sugárzás, napszél*

Hullámvisszaverő képesség alapján négy ilyen réteget különböztetünk meg, melyek:

- D-réteg (kb. 40-80 km): a Föld Nap által megvilágított oldalán alakul ki, mely így adott földrajzi ponton nappal érvényesül déli maximummal, majd éjszaka megszűnik. Hullámterjedési szempontból alapvetően elnyelő, csillapító tulajdonságokkal bír, elsősorban rövidhullámú sáv alatti (<3 MHz) tartományokban,
- E-réteg vagy Kenelly-Heaviside réteg (kb. 100-160 km): adott földrajzi ponton napfelkelte előtt keletkezik és részben napnyugta után is fennmarad, de lényegesen kisebb elektronkoncentráció mellett. Elegendően nagy elektronsűrűség esetén már képes a rövidhullámú tartomány alsó felébe tartozó hullámok visszatükrözésére,
- F-réteg vagy Appleton-réteg (180-400 km): legnagyobb vastagságú réteg, napnyugta után az elektronkoncentráció csökkenése lényegesen lassabb, mint az alacsonyabb rétegeknél és éjszaka is fennmarad. Minimumát napkeltekor éri el. A nappali intenzív besugárzás hatására az elektronsűrűség magassági maximum értékének két tartománya alakul ki, az alsó 20-300 km-es tartományban az $F_1$ -réteg, míg a magasabb kb. 400 km tartományban az $F_2$-réteg. A rövidhullámú terjedés szempontjából az $F_2$-réteg jelentős reflektáló képességet képvisel.

A felületi hullámok rövidhullámú tartományú terjedését a földfelszín terep elemei valamint a talaj dielektromos állandója[3] jelentősen befolyásolja, ezáltal maximális hatótávolságuk 100-200 km, amely érték a sávtartományon belül a frekvencia növelésével rohamosan csökken.

A földfelszínről kisugárzott térhullámok az ionoszféra reflexiós rétegeiről (megfelelő körülmények között) képesek visszaverődve jelentősen nagyobb, több ezer km-es távolságokat megtenni. A rétegek reflektáló képessége függ a frekvenciától és a beesési szögtől. Általánosan szabályként elmondható, hogy reflexió létrejöttéhez a frekvencia és a beesési szög növekedésével egyre nagyobb ionkoncentráció szükséges. Azt a maximális frekvenciaértéket, amely az ionoszféra adott pillanatnyi állapotában, adott beesési szög mellett még képes reflektálni felső üzemi frekvenciának[4] nevezzük. A D-réteg hasonlóan frekvenciafüggő csillapító hatása miatt az adott terjedési körülményekhez tartozik egy ún. alsó üzemi frekvencia[5] is, amely adott bemeneti jel-zaj viszony mellett a vevővel még vehető. A MUF és LUF közötti használható frekvencia ablak folyamatosan változik, értéke néhány MHz- től akár 20 MHz-ig is terjedhet. Tovább

[3] *dielektromos állandó vagy relatív permittivitás: elektromosan nem vezető anyagok szigetelőképességére jellemző anyagi tulajdonság*

[4] *Maximum Usable Frequency - MUF*

[5] *Lowest Usable High Frequency- LUF*

bonyolítja a terjedési képet, hogy teljesen dielektromos tulajdonságú talajnál a függőlegesen polarizált hullám a talajról nem verődik vissza, ha a beesési szög eléri az ún. Brewster-szöget. A nem teljesen dielektromos tulajdonságú talajnál a visszaverődési tényezőnek ennél az értéknél minimuma van (pszeudo-Brewster szög). A felület mentén párhuzamosan haladó hullám 180°-os fázistolást szenved, emiatt létezik egy olyan minimális kilövési (elevációs) szög érték (kb. 4-5°), amely alatt a sugárzás a teljes tartományban gyakorlatilag megszűnik.

Bizonyos körülmények között azonban a reflektált hullámok a földfelszínről továbbreflektálódva (többszörös visszaverődés), több ugrással, extrém távolságokat (8-12 ezer km) is képesek áthidalni.

A felületi hullámokkal adott pontból már nem-, a térhullámokkal a reflexiós feltételek (ugrások) miatt még nem elérhető földrajzi tartományokat ún. holtzónáknak nevezzük, amelyek kiterjedése a több száz km-es tartományokat is elérheti.

## 1.2 Rövidhullámú összeköttetések jellemzői

A rövidhullámú sáv előző pontban vázolt szofisztikált terjedési tulajdonságai (soktényezős időbeli-, térbeli- nap-, évszak-, frekvencia-, polarizáció-, napfolt- és naptevékenység függősége) a sávtartományra jellemző sajátos összeköttetési csatornák kialakítását követeli meg, illetve teszi lehetővé. Az ionoszférikus terjedésnek köszönhetően, térben és időben folyamatosan változó közegben, időben rendkívül ingadozó vételi körülmények között, a térhullámokkal Föld nagyságrendű távolsági összeköttetések valósíthatók meg az alábbi jellemzőkkel:

- 24 órás összeköttetések megvalósításához több frekvencia használata szükséges
- műsorszórások folyamatos biztosítása ütemezett frekvenciaváltást igényel
- az összeköttetések létrehozásához frekvenciatervezés szükséges
- a sávtartomány sűrű csatorna kiosztású, nagyszámú energia jelenlétével
- az összeköttetések külső zajkörnyezeti feltételei időben és térben folyamatosan változnak
- magas intermodulációs követelmények
- az adásformák tipikus sávszélessége néhány kHz-es tartományú
- néhány helyhez kötött és mobil szolgálat intelligens, kognitív (frekvencia adaptív) rendszereket használ (ALE)[6]
- a legtöbb modulációs sávszélesség meghaladja a korrelációs sávszélességet

[6] *Automatic Link Establishment*

A rövidhullámú sávban a Nemzetközi Rádiószabályzat és a Frekvenciák Nemzeti Felosztási Táblázata (FNFT) szerinti besorolásban a következő jelentősebb tipikus szolgálatok üzemelnek:

Állandóhelyű:
RH állandóhelyű
A3E (AM) és J3E (SSB) adásmódú CB berendezések
Távirányító, távmérő, távjelző és vagyonvédelmi berendezés
Állandóhelyű mozgó:
külügyminisztérium, külképviseletek céljaira, illetve. rendkívüli állapot, szükségállapot, veszélyhelyzet esetén pont-pont típusú összeköttetések adat, beszéd és képátvitelhez

Állandóhelyű műsorszórás:
RH rádió-műsorszórás,
Egyoldalsávos RH rádió-műsorszórás
Tengeri mozgó:
Dunai hajózás RH rádiókommunikációs rendszer
Rádiótelefon üzemű hajóállomások
Légi mozgó:
Levegő-föld (A/G) beszédátviteli és adatátviteli összeköttetés elsősorban nemzetközi és nemzeti polgári légiútvonalakon

Amatőr:
Rövidhullámú amatőrrádiózás
160 m-es amatőrsáv (1,81-2,0 MHz)
80 m-es amatőrsáv (3,5-3,8 MHz)
40 m-es amatőrsáv (7,0-7,1 MHz)
30 m-es amatőrsáv (10,1-10,15 MHz)
20 m-es amatőrsáv (14,0-14,35 MHz)
17 m-es amatőrsáv (18,068-18,168 MHz)
15 m-es amatőrsáv (21,0-21,45 MHz)
Műholdas rövidhullámú amatőrrádiózás

Fentieken túlmenően, a sávban egyéb speciális felhasználások (nemzetközi vész-frekvenciák, speciális vivőfrekvenciák, hiteles frekvenciák és órajelek, ember által lakott űrjárművek kutatási és mentési frekvenciája, egyeztetett kutatási és mentési műveletek, kisteljesítményű eszközök /LPD-k/, ISM berendezések valamint kis hatótávolságú induktív eszközök /SRD-k/ is rendszeresítettek.

## 2. A nemzetbiztonsági célú rövidhullámú elektronikai adatgyűjtés magyarországi környezete

A rövidhullámú stratégiai adatszerző rendszerek elektronikai védelmi lehetőségeinek vizsgálatához szükséges feltérképezni azokat a környezeti változókat, helyi adottságokat, és feltételeket (történelmi adottságok, törvényi környezet, szervezeti struktúra, nemzetközi szerződések földrajzi-geopolitikai adottságok), amelyek keretet adnak egy ilyen rendszer magyarországi működtetésére, illetve meghatározzák az adatgyűjtő rendszer jelenkori elektronikai védelmi lehetőségeit, szükségleteit.

### 2.1 Történelmi előzmények

Ismereteink szerint a nemzeti alapokon működő katonai hírszerzés és elhárítás Magyarországon már a Habsburg monarchia felbomlását követően a monarchia hadseregének korábbi, hasonló rendeltetésű szervezetének felépítése és szabályai alapján jött létre.

Ennek keretein belül rádiófelderítő tevékenységet először 1918-ban végeztek. A hírszerzési célú tevékenység stratégiai, hadműveleti - majd később a II. világháború során - harcászati szinten folyt a Honvéd Vezérkar Hírszerző- és Elhárító VKF-2 Osztályán.

A II. világháborút követően a hírszerzés és elhárítás a Honvédelmi Minisztérium csoportfőnökségek keretében folyt (VI-2. Osztály), majd 1953-tól a MNVK 2. Csoportfőnöksége volt felelős a katonai hírszerzésért.

Ezzel párhuzamosan 1947-től a BM Államrendőrség Államvédelmi Osztályának (ÁVO) megalakulásával, annak keretein belül létrejött egy polgári rádiófelderítő csoport a magyarországi rádióforgalom ellenőrzés személyi és technikai feltételeinek kidolgozására, amely tevékenység 1949-től az akkor létrejövő Államvédelmi Hatóság (ÁVH) operatív technikával foglalkozó II. Főosztályán indult növekedésnek.

Az 1955-ben Moszkvában megrendezett állambiztonsági értekezletet követően az elhárítás a Belügyminisztérium alárendeltségébe került, míg a katonai hírszerzés a Honvédelmi Minisztérium keretein belül folytatta tevékenységét egészen 1990-ig. Ennek megfelelően a magyarországi rövidhullámú rádiófelderítő-rádióelhárító tevékenység is két pilléren érte meg a rendszerváltást.

A demokratikus berendezkedéssel létrejött két polgári – a Nemzetbiztonsági Hivatal (NBH) és az Információs Hivatal (IH) - valamint két katonai – a Katonai Felderítő Hivatal (KFH) és Katonai Biztonsági Hivatal (KBH) - szolgálat szimmetrikussá formálta az elhárítás és hírszerzés polgári és katonai struktúráját.

Az 1996-ban hatályba lépett *a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény (Nbtv.)* ötödik titkosszolgálatként létrehozta az önálló Nemzetbiztonsági Szakszolgálatot (NBSZ), mint a titkos információgyűjtő eszközökkel valamint módszerekkel dolgozó, szolgáltató jellegű operatív-technikai kiszolgáló szakszolgálatot.

Magyarország 1999-es NATO csatlakozásával a rádiófelderítés tevékenysége, mint fogalom, új értelmezési keretrendszerben került elhelyezésre. Illeszkedve a közösségi rendszer *elektronikai hadviselés*[7] fogalomrendszerén belül elfoglalt helyére, az adatforrások (információforrások) NATO-felosztása szerint alapvetően a *rádióelektronikai felderítés*[8] *vagy elektronikai eszközökkel folytatott felderítés és rádiófelderítés*[9], ezen belül a *rádiófelderítés*[10] *vagy kommunikációs felderítés* valamint a *rádiótechnikai felderítés*[11] *vagy elektronikai eszközök felderítése* fogalmi hármasában nyert értelmezést.

Az Nbtv. 2010. évi módosítását követően az NBH jogutódja az Alkotmányvédelmi Hivatal (AH) és NBSZ belügyminiszteri, míg az IH külügyminiszteri irányítás alá került. További változás történt 2012-ben, amikor is a KFH-t és KBH-t egy közös szolgálatba vonták össze Katonai Nemzetbiztonsági Szolgálat- (KNBSZ) néven, továbbá az IH-t KÜM-ből Miniszterelnökség alá rendelték. A változtatások ellenére is a magyar titkosszolgálati rádiófelderítő tevékenység (katonai hírszerzés,[12] polgári technikai hírszerzés[13], valamint hírközlő hálózatok kommunikáció ellenőrzése[14]) továbbra is megtartotta több pilléres struktúráját.

## 2.2 Titkos információgyűjtés és titkos adatszerzés jogszabályi környezete Magyarországon

A titkos információgyűjtés jelenlegi kereteit – a nemzetbiztonsági szolgálatok vonatkozásában az Nbtv. szabályozza, amely az Információs Hivatalt, az Alkotmányvédelmi Hivatalt, a Katonai Nemzetbiztonsági Szolgálatot valamint a Nem-

---

[7] *Electronic Warefare - EW*

[8] *Signal Intelligence - SIGINT*

[9] *Kobolka István: Nemzetbiztonsági alapismeretek, Nemzeti Közszolgálati Egyetem, Budapest, 2013. p.127.]-ben a szerző a „rádiófelderítés" kifejezést a COMINT mellett a SIGINT vonatkozásában is értelmezi*

[10] *Communication Intelligence - COMINT*

[11] *Electronic Intelligence - ELINT*

[12] *Katonai Nemzetbiztonsági Hivatal honlapja, Forrás: http://www.honvedelem.hu/szervezet/knbsz (Letöltve:2015.05.24.)*

[13] *Információs Hivatal honlapja, Forrás: http://www.ih.gov.hu/hivatal_hirszerzes.shtml (Letöltve:2015.05.24.)*

[14] *Nemzetbiztonsági Szakszolgálat honlapja. Forrás: http://www.nbsz.gov.hu/?mid=28 (Letöltve:2015.05.24.)*

zetbiztonsági Szakszolgálatot (együtt: nemzetbiztonsági szolgálatok) nevesíti meg a tevékenység folytatására jogosult szervezetekként. A törvény értelmében a nemzetbiztonsági szolgálatok feladataik teljesítése érdekében titkos információgyűjtést folytathatnak, melyhez speciális eszközöket és módszereket alkalmazhatnak. Ezen szolgálatok főbb feladatai a következők:

A Katonai Nemzetbiztonsági Szolgálat:

- hírszerző, elhárító, védelmi és ellenőrzési feladatok elvégzésével, a nyílt és a titkos információgyűjtés eszközrendszerével működési területén elősegíti Magyarország nemzetbiztonsági érdekeinek érvényesítését, ezáltal közreműködik az ország függetlenségének és törvényes rendjének védelmében;
- megszerzi, elemzi és továbbítja a kormányzati döntésekhez szükséges, a külföldi eredetű, a biztonságpolitika katonai elemét érintő katonapolitikai, hadiipari és katonai információkat;
- biztosítja a Honvéd Vezérkar hadászati-hadműveleti tervező munkájához szükséges információkat, működteti Magyarország katonai felderítő rendszerét.

Az Információs Hivatal:

- megszerzi, elemzi, értékeli és továbbítja a kormányzati döntésekhez szükséges, a külföldre vonatkozó, illetőleg külföldi eredetű, a nemzet biztonsága érdekében hasznosítható információkat.

Az Alkotmányvédelmi Hivatal:

- felderíti és elhárítja a Magyarország függetlenségét, politikai, gazdasági, védelmi vagy más fontos érdekét sértő vagy veszélyeztető külföldi titkosszolgálati és Magyarország törvényes rendjének törvénytelen eszközökkel történő megváltoztatására vagy megzavarására irányuló leplezett törekvéseket és tevékenységet.

A Nemzetbiztonsági Szakszolgálat:

- a jogszabályok keretei között a titkos információgyűjtés, illetve a titkos adatszerzés eszközeivel és módszereivel – írásbeli megkeresésre – szolgáltatást végez a titkos információgyűjtésre, illetve a titkos adatszerzésre feljogosított szervek titkos információgyűjtő, valamint titkos adatszerző tevékenységéhez;

- a törvény által titkos információgyűjtésre, valamint titkos adatszerzésre feljogosított szervek igényei alapján biztosítja az e tevékenységhez szükséges különleges technikai eszközöket és anyagokat;
- technikai felderítés keretében hírközlő hálózaton folytatott kommunikáció tartalmának megismerését és rögzítését végzi;
- bizonyos eseteket kivéve, a titkos információgyűjtés eszközeit és módszereit saját kezdeményezésre nem alkalmazhatja.

A rádiófelderítés/rádióellenőrzés - mint titkos információgyűjtő és titkos adatszerző tevékenység – megvalósításához a nemzetbiztonsági szolgálatok:

- a nemzetbiztonsági jelleg leplezésével információt gyűjthetnek;
- az információgyűjtést elősegítő információs rendszereket hozhatnak létre és alkalmazhatnak;
- hírközlési rendszerekből és egyéb adattároló eszközökből információkat gyűjthetnek;
- elektronikus hírközlési szolgáltatás útján továbbított kommunikáció tartalmát megismerhetik, az észlelteket technikai eszközzel rögzíthetik;
- számítástechnikai eszköz vagy rendszer útján továbbított, vagy azon tárolt adatokat megismerhetik és azok tartalmát technikai eszközzel rögzíthetik, továbbá felhasználhatják.

Fontos megjegyezni, hogy az Nbtv. alapján a polgári és a katonai titkosszolgálatok a fentiek szerinti „alanyi” jogon élhetnek a titkos információgyűjtés lehetőségével.

Emellett az egyéb ágazati törvények alapján feljogosított további öt szervezet- a Rendőrség[15], a Nemzeti Védelmi Szolgálat[16], a Terrorelhárítási Központ[17], a Nemzeti Adó- és Vámhivatal[18] valamint az Ügyészség[19] - tevékenységi körükhöz kapcsolódó nyomozati cselekmények körében- szintén élhetnek a titkos információgyűjtés és titkos adatszerzés eszközével, azonban ezek az esetek a stratégiai jellegű rövidhullámú felderítés és adatszerzés vonatkozásában – jellegüknél fogva- nem képeznek súlyponti szerepet.

Az NBSZ szolgáltatásai a másik három nemzetbiztonsági szolgálat részére „teljeskörűen” hozzáférhetőek és elérhetők. Tekintettel arra, hogy bár az NBSZ koncentrált titkos információgyűjtő és titkos adatszerző technikai eszköz rend-

[15] *a Rendőrségről szóló 1994. évi XXIV. törvény alapján*
[16] *a Rendőrségről szóló 1994. évi XXIV. törvény alapján*
[17] *a Rendőrségről szóló 1994. évi XXIV. törvény alapján*
[18] *a Nemzeti Adó- és Vámhivatalról szóló 2010. évi CXXII. törvény alapján*
[19] *az ügyészségről szóló 2011. évi CLXIII. törvény alapján*

szer kapacitással bír, a nemzetbiztonsági szolgálatok saját eszközeiket is – a törvényi keretek korlátai között - felhasznál(hat)ják feladataik végrehajtása során.

Magyarországon a nemzetbiztonsági szolgálatok közül az Információs Hivatal és a Nemzetbiztonsági Szakszolgálat rádiófelderítést, a Katonai Nemzetbiztonsági Szolgálat pedig rádióelektronikai felderítést hajt végre törvényi felhatalmazás alapján.

A nemzetbiztonsági célú, rövidhullámú sávtartományú, magyarországi rádiófelderítés szempontjából az 1.1. fejezetben ismertetett jellemzőkkel bíró hullámterjedés elsősorban a nagy távolságban található (külföldi) rövidhullámú rádióforrások jeleinek vételét, rádiólokációs helymeghatározását és a sávtartományban üzemelő pont-pont vagy pont- több pont jellegű kommunikációs összeköttetési rendszerek felderítését és rádióellenőrzését teszi lehetővé, illetve ellenőrzésének ad keretet.

## 3. Stratégiai rövidhullámú COMINT rendszerek elektronikai védelmi lehetőségei

### 3.1. Az elektronikai védelemről általában

A rövidhullámú stratégiai információgyűjtő és adatszerző rendszerek elektronikai védelmi képességének vizsgálatához szükséges áttekinteni az elektronikai védelem fogalomkörét, a harcászati elektronikai konfliktusban elfoglalt szerepét és területeit.

Az elektronikai védelem, mint az elektronikai hadviselés szerves eleme, alapvető rendeltetése az elektromágneses spektrum saját csapatok részéről történő hatékony használatának biztosítása. Mindezt az ellenséges fél elektronikai támogatása és elektronikai ellentevékenysége ellenében szükséges véghezvinnie. Hasonlóképpen, a saját rendszerek, csapatok nem szándékos elektronikai zavaró tevékenységének kiküszöbölése, illetve leküzdése is e védelmi tevékenység feladatát képezi. Olyan aktív és passzív műveletek, módszerek vagy tevékenységi előírások, rendszabályok alkalmazását jelenti, amelyek célja az ellenség felderítő és elektronikai ellentevékenységi hatékonyságának csökkentése, ellehetetlenítése.

A passzív elektronikai védelem azon intézkedéseket tartalmazza, amelyek az ellenség által nem detektálhatóak, így azok főleg taktikai, módszertani és eljárásrendi megfontolásokat tartalmaznak, beleértve a védelmi pajzsok alkalmazását.

Az aktív elektronikai védelem érzékelhető az ellenség által és a védelmet valamilyen speciális berendezés vagy egy adott elektronikai berendezés speciális működtetési módjának alkalmazásával biztosítja.

Az elektronikai védelmi tevékenységek három fő területben csoportosíthatók. Első csoportba azok az intézkedések, aktív tevékenységek tartoznak, amelyek a saját eszközök, rendszerek elektronikai felderítését célzottak megakadá-

lyozni. Az elektronikai felderítő tevékenységen olyan információszerzést megcélzó tevékenységet értünk, amely az infokommunikációs rendszerekben tárolt vagy azokban továbbított adatokhoz való hozzáférést, azok felhasználását célozza meg, másrészről a hatékony támadás elősegítéséhez szükséges célinformációk megszerzését foglalja magában. Az elektronikai felderítésnek számos területe létezik, idetartoznak a különböző sávtartományokra kiterjedő műszeres felderítés[20] különböző szakágai, a képi felderítés[21] valamint a rádióelektronikai felderítés[22]. A felderítés elleni védelem fogalmán belül megkülönböztethetők az elektronikai álcázást biztosító tevékenységek valamint az elektromágneses kisugárzások csökkentését, megakadályozását célzó tevékenységek.

Másik nagy területe az elektronikai védelemnek az elektronikai ellentevékenység (zavarás) elleni védelem, amely körébe a szándékos és nem szándékos zavarok elleni tevékenységek valamint az elektronikai pusztítás elleni védelmet célzó tevékenységek tartoznak.

Harmadik csoportba sorolható az elektronikai ellenőrzés témaköre. Ide olyan technikai és szervezési rendszabályok összessége tartozik, amely feladata a saját eszközrendszer elektronikai védelmi állapotának folyamatos vizsgálata, a védelmi intézkedések, rendszabályok betartásának és hatékonyságának nyomon követése, a saját rendszer ellenség szempontjából történő vizsgálata, tesztelése.

A három nagy terület a módszer, jelleg, tartomány alapján számos részterületekre bontható[23], melyek alapján lehetséges egy adott objektum/rendszer elektronikai védelmi lehetőségének vizsgálata.

## 3.2 Rövidhullámú stratégiai adatszerző rendszerek elektronikai védelmi áruló jegyei

Az elektronikai védelmen belül az elektronikai felderítés elleni tevékenység hatékony tervezéséhez szükséges megvizsgálni a védendő rendszereink azon tulajdonságait (áruló jegyeit), amelyek az ellenség felderítő tevékenysége szempontjából jelentőséggel bírnak. Az áruló jegyek ismeretében kidolgozható a védelmi eljárás vagy az adott objektumra vonatkozó felderítés elleni rendszabályok összessége.

Stratégiai adatszerző rendszerek esetében áruló jegyeknek a rendszer elemeinek, technikai eszközeinek működésére jellemző olyan sajátosságait, jellegzetességeit értjük, amelyek az ellenség számára lehetővé teszik, hogy elemzésükkel a rendszer elemei felderíthetővé váljanak. A rendszer elemeinek mozgására, összetartozására, csoportosítására utaló jellemzőket hadműveleti-harcászati áruló jelekként azonosítjuk, míg az eszközrendszer védettségére, zavarállóságára, ren-

[20] *Measurement and signature intelligence - MASINT*

[21] *Imagery Intelligence - IMINT*

[22] *Signal Intelligence - SIGINT*

[23] *lásd 4.2, 4.3. és 4.4 fejezetek*

deltetésére, típusára, hovatartozására vonatkozó jegyeket technikai jegyekként tartjuk nyilván:

Adatszerző rendszerek hadműveleti-harcászati áruló jelek:

- épületek/objektumok mennyisége;
- épületek/objektumok földrajzi elhelyezkedése;
- épületek/objektumok nagysága;
- épületek/objektumok külső megjelenési formája;
- épületek/objektumok egymáshoz viszonyított elhelyezkedése;
- épületek/objektumok körleteinek mérete.

Adatszerző rendszerek technikai jellegű áruló jelek:

- a kibocsátott és visszavert jelek
    - térbeli alakja (irányítottság, méretek);
    - belső struktúrája (vivőfrekvencia, modulációs mód, modulációs tartalom, moduláció minősége);
    - a sugárzó eszközök;
    - üzemi frekvenciája;
    - frekvencia stabilitása;
    - frekvencia váltogatása (zavarás hatására);
    - harmonikus sugárzása;
    - sávon kívüli sugárzása;
    - vivőelnyomása;
- az antenna berendezések
    - külső geometriai méretei (alak, felépítés);
    - iránykarakterisztikák;
    - a tér figyelési módja (forgatás, lengetés);
- az információ továbbítás
    - módja (adásmód, üzemmód);
    - sávszélesség jellemzők;
    - egyidejű csatornák száma;
    - időosztásos csatornák képzése.

Az áruló jegyek ismeretében teljes kép alkotható a védendő rendszerről és kidolgozhatók azok az eljárások, rendszabályok, amelyek megakadályozzák vagy csökkentik az ellenség vagy saját eszközeink rendszerünk zavartatására irányuló képességét.

A rövidhullámú adatszerzés szempontjából fontos megemlíteni, hogy a nemzetbiztonsági célú tevékenység passzív rádiófelderítő eszközökkel valósul meg. A szenzorok és központ közötti – a megszerzett adatok továbbítására vagy az adatszerzés irányítására szolgáló –összeköttetések – pl. rádiós megvalósítás esetén tartalmazhatnak aktív elemeket. Passzív rendszerelemek esetén a fenti felsoro-

lásból a kibocsátott és visszavert jelek valamint a sugárzó eszközök jellemzői, mint áruló jelek nem rendelkeznek relevanciával.

## 3.3. Stratégiai rövidhullámú ellenőrző központok elektronikai védelmi lehetőségei

Egy stratégiai COMINT központ nagyon hasonlatos vizsgálati feltételeket mutat egy egyéb, hétköznapibb funkcionalitású felhasználással, mint például, vállalati számítógép központ vagy általános informatikai rendszerek központi elemeinek elhelyezése.

Az elektronikai védelmi módszerek jelentős köre a stratégiai COMINT központ általános (irodai) jellegű környezetben (épület, akár lakott, urbánus terület) történő elhelyezhetőség miatt békeidőben nem értelmezhető a központ esetében. A jelentősebbeket említve nem értelmezhetők a vizsgálatban a hidroakusztikai-, akusztikai felderítés elleni rejtés módszerei, a szándékos zavarok elleni védelem zavar hatékonyság csökkentő azon eljárásai, amelyek alapvetően duplex összeköttetések (elsősorban híradó) védelmi eszközeiként hatékonyak. Specialitásuk miatt nem értelmezhetőek továbbá a rádiólokációs- és rádiórelé rendszereknél alkalmazható zavarvédelmi eljárások és szervezési- illetve technikai módszerek sem. Hasonlóképpen kívül esnek a vizsgálhatóság körén azok az eljárások, amelyek valamilyen módon az eszközrendszer elemeinek térben és/vagy időben történő elkülönítésével operálnak, illetve amelyek az ellenség azonnali megsemmisítésén alapszanak (nemzetbiztonsági rendszer, békeidejű használati feltételek).

A központ teljesen passzív (csak jelfeldolgozás folyik, nincs kisugárzott kommunikációja) jellege valamint általános épületben elhelyezhetősége (nincs külső, felismerhető azonosíthatósági jegye, épület nagyságrendű helyigény) értelmezhetőek, azonban nem vagy csak nagyon korlátozottan alkalmazhatóak az elektronikai rejtés aktív elemei, az optikai rejtés álcahálós- vagy fényforrás manipulációs módszerei, a rádiólokációs felderítés elleni rejtés valamint a rádió- és rádiótechnikai felderítés elleni tevékenység egyes aktív elemei. Általánosságban kijelenthető, hogy stratégiai központok esetében még békeidőn kívül sem alkalmazhatóak az objektum különböző hullámtartományú (látható fény, lézer, infravörös) rejtését csak korlátozott ideig biztosítani képes füst- és köd generáló eszközök. Ez utóbbiak elsősorban kisebb objektumok, tárgyak, mobil eszközök harcászati szinten, konfliktus közepette történő védelme során lehetnek hatékonyak. Külön kockázati tényezőként említhető az elektromágneses impulzusok elleni védelem korlátozottsága, mivel az impulzus nagyságára vonatkozó ismeretek hiánya nem teszi lehetővé a szükséges védelmi módszer és eszköz optimális meghatározását. A központ elhelyezését biztosító objektum (épület) vonatkozásában – technológiai szempontból - lehetőség van elektromágneses árnyékolás (pl. falakon fémadalékos bevonatok vagy a központ teljeskörű, Faraday-kalicka

elvű, fémlemezzel történő burkolása) alkalmazására. Ezek a módszerek információbiztonsági kisugárzási (TEMPEST)[24] szempontból az elektromágneses hullámok vonatkozásában az előírt - mintegy 100 dB értékű- csillapítást képesek biztosítani, azonban az elektromágneses impulzusok elleni védelmi képességük nem ismert.

A központ objektumának védelmére hatékonyan alkalmazhatók az elektronikai álcázás területén a külső megjelenési jegyek elkerülése, az akusztikai álcázás, valamint az elektromágneses árnyékolás eszközrendszere. Urbánus környezetben történő elhelyezéssel a műholdas felderítést kivéve jól alkalmazhatók a környezeti elemek, objektumok védő-, árnyékoló tulajdonságán alapuló rejtési lehetőségek, míg a műholdas felderítés ellen biztonságos védelmet egy más kockázati megközelítésű, földfelszín alatti központ kialakítás biztosíthat. A rendszabály alapú megközelítések jelentős mértékben alkalmazhatóak a szándékos és nem szándékos kisugárzások elleni védelem területén is. A zavar eredetének és hovatartozásának meghatározásával, a vevőrendszer lehetőségekhez képesti finomhangolásával, elektromágneses kompatibilitási szabvány előírásoknak megfelelő vagy azokon esetleg akár túlmutató jellemzőkkel rendelkező eszközök fejlesztésével és alkalmazásával biztosíthatók a zavarvédettség feltételei. Elektronikai pusztítás elleni védelem területén a stratégiai központ esetében szintén széles körben alkalmazhatók mindazon technológiai eszközök, alkatrészek (pl.: szikraközök, árnyékoló anyagok, túlfeszültség levezetők, nemlineáris feszültségvédelmi elemek, stb.), amelyek képesek megakadályozni a nagy energiájú rádiófrekvenciás források sugárzott jeleinek objektumba való bejutását.

## 3.4. Stacioner telepítésű rövidhullámú ellenőrző szenzorok elektronikai védelmi lehetőségei

A szenzorok feladata a sávtartományban található adások, forgalmazások vétele, a sugárforrás helyzetének iránymérése, valamint a vett jelek további feldolgozásra történő továbbítása valamilyen csatornán (rádiós, vezetékes, optikai) a központhoz. A vett jelek az antennákról vagy diszkrét vevőkre kerülnek vagy teljessávú digitalizálást követően jutnak a feldolgozó központba. A szenzorok emiatt alapvetően különböző polarizációjú szélessávú- vagy keskenysávú vevőantennából, iránymérő antenná(k)ból vagy antennarendszerekből állnak.

A rövidhullámú stacioner telepítésű szenzorok sajátossága, hogy a térszelektivitás biztosítása céljából a gyakorlatban több típusú és elrendezésű antennákból álló antennamezővel rendelkeznek. A sáv tartomány 10-től 100 méterig terjedő hullámhosszából adódóan az antennák fizikai mérete általában jelentős, egyes esetekben a több tíz méteres terjedelmet is elérik. Méretükből adódóan

[24] *Az amerikai Nemzeti Biztonsági Ügynökség (NSA - National Security Agency) által specifikált, az információ szivárgását gátló normarendszer*

jelentős méretű, (általában fém) tartóoszlop és feszítő rendszer kialakítását igénylik. Az antennák elkülönítésének figyelembevételével kialakított antennamező területe a néhány négyzetkilométert is elérheti. Az antennamező elemeitől a rádiófrekvenciás jelek (a talpponti digitalizálást kivéve) kábeleken jutnak be a konténerben vagy kisebb épületben elhelyezett vevőkhöz, melyek hangolása, programozása távvezérelt módon az akár több száz kilométerre található stacioner felderítő központból történik.

Ennek megfelelően elektronikai védelmi szempontból a szenzornak négy funkcionális eleme különböztethető meg, melyek:

- vételi antennák, iránymérő antennák a tartószerkezettel*;*
- antennák és konténer(épület) közötti összeköttetés (rádiófrekvenciás kábel, optikai kábel, elektromos tápkábel) *;*
- konténer(épület) az elhelyezet vételi eszközökkel*;*
- összeköttetési csatorna a szenzor konténer(épület) és stacioner felderítő központ között (rádiós, vezetékes, optikai) .

A rövidhullámú stacioner szenzorok földrajzi elhelyezése rádióvételi szempontból alacsony háttérzajú, ipari létesítményektől mentes, általában természeti környezetben lehetséges, ezáltal városi-, nagyvárosi telepítésük nem ideális. A vételi viszonyokat pozitívan befolyásolja az antenna talajszerkezete, nedvességtartama, ezért gyakori a rövidhullámú szenzorok lápos, ingoványos, esetleg mocsaras területeken történő kialakítása.

A stacioner adatszerző központhoz képest a jelentős számosságú, méretű és kiterjedtségű antennarendszerrel és vevőeszközzel rendelkező stacioner szenzorok elektronikai védelmi szempontból érzékenyebb képet mutatnak.

A nem értelmezhető védelmi módok nagyrészt hasonlóságot mutatnak a stacioner adatszerző központ jellemzőivel. Ugyanakkor, kiemelhető azonban néhány elem, amelyek a szenzoroknál értelmet nyernek, illetve valamilyen mértékben alkalmazhatók. Ilyenek például a elektromágneses árnyékolás alkalmazása, ami zavartatási szempontból szükséges pl. a konténer(épület) esetében, azonban az antennák, mint elektromágneses jelátalakító eszközök esetében semmilyen formában nem alkalmazható illetve funkcionalitásában gátolná az antennák működését. Míg a központoknál nem értelmezhető az ellenség által zavarással lefogott elektronikai eszközök helyettesítése, addig a „vadonban”, nagy területen telepített stacioner szenzor esetében az elektronikai eszközök széttelepítése bizonyos korlátok között értelmet nyerhet. Tekintettel, hogy a szenzor rendelkezik valamilyen szintű vételi eszközzel, ezeknél – ha nem is rádiólokációs berendezéseknél használt értelemben – értelmezhető és elméletileg alkalmazhatók a vevő eszköz minőségi mutatóira vonatkozó javítási módszerek (pl.: szelektivitás, dinamikatartomány, antenna oldalnyaláb jellemzőinek javítása). Hasonlóképpen, a nem szándékos zavarok védelmi lehetőségeként használhatóvá válnak az elektronikai eszközök üzemi szektorainak kisugárzási és vételi

viszonyok alapján történő elosztása, csoportosítása is. Ez utóbbi az elektronikai ellenőrzés területén, az előírások betartásának területén, valamint a mért EM jellemzők műszaki normákkal történő összehasonlítása esetében is különbözőséget mutat az adatszerző központokhoz képest.

A nagyméretű vételi elemek (antennák, tartószerkezetek) jelenléte miatt, elektronikai rejtés tekintetében - mint passzív módszer - jelentőséghez jut az eszközök áruló jeleinek megszüntetése és rádiólokátor zavarása, azonban a méretek miatt esetenként csak korlátozott mértékben kivitelezhetők és hatékonyságuk is kérdőjeles. A kiterjedt antenna méretek miatt az optikai rejtés területén is nagyobb kihívásokkal szembesülünk és a terep rejtő tulajdonságai is kevésbé használhatók ki.

A szenzorok esetében kulcsponti kérdés a központtal magvalósított összeköttetési csatorna fajtája. Rádióösszeköttetés esetén aktív elem lép a képbe, ami felderíthetőség területén emeli a kockázati tényezőt és kiszélesíti a szükséges elektronikai védelmi módszerek körét. Minden tényezőt figyelembe véve a talpponti digitalizálás és optikai kábeles összeköttetések alkalmazása nagymértékben növeli a felderítő rendszer zavarvédettségét.

## 3.5. Mobil telepítésű rövidhullámú ellenőrző szenzorok elektronikai védelmi lehetőségei

A mobil telepítésű szenzorok feladatai azonosak a stacioner kivitelű állomásokéval, azonban alkalmazási módjuk, eszközrendszerük eltér attól. Legfontosabb sajátosságuk, hogy önjáróak, gyorsan telepíthetőek, elsőrendű alkalmazási sajátosságuk a mozgékonyságuk. Ebből adódóan valamilyen terepjáró képességű hordozó jármű felépítménye biztosít helyet a vevő eszközöknek.

Az antennák a felépítményen fixen vagy a telepített gépjármű közelében önálló telepítéssel kerülnek elhelyezésre. Az egység saját tápellátással kell rendelkezzen, ami a gépjármű saját generátoráról vagy az az mellett működtetett vontatható áramforrásról üzemel.

A mobilan telepíthető antennák mérete jelentősen kisebb a stacioner állomásnál alkalmazottaktól. Eltérően a stacioner állomástól a mobil állomások nem rendelkeznek kiterjedt antennaparkkal, az egyszerre üzemeltett iránymérő vagy vételi antennák száma a néhány darabot éri el. A korlátozott, de célzott felhasználás sajátossága, hogy alkalmazásában, kivitelében, méretében, felhasználásának jellegében, felderítési célpontként nagy hasonlóságot mutat az egyéb harcászati eszközökkel (harckocsi, szállítójármű, stb.). Ebből a tulajdonságaiból adódóan az elektronikai védelmi aspektusai is jelentősen elmozdulnak a harctéri mobil szárazföldi egységek jegyeinek irányába.

Kritikus eleme a szenzornak, hogy mobilitásából adódóan összeköttetése a stacioner központtal – egyedi eseteket leszámítva - kizárólag rádiós úton valósul meg.

Az elektronikai álcázás szükségességével párhuzamosan a mobil szenzor esetében megjelennek a különböző hullámtartományokban (optikai, lézer, infravörös) alkalmazható terep, napszak, optikai forma kihasználását alkalmazó álcázási lehetőségek és előtérbe kerülhetnek a passzív elektronikai rejtés elemei, mint a lokátor zavarás, elektrooptikai felderítés elleni álcázás és akusztikai álcázás szükségessége is. A gépjármű felépítmény anyagi tulajdonságai szükségessé teszik a mágneses mérésen alapuló felderítés elleni rejtés és a rádiólokációs felderítés elleni rejtés módszereinek alkalmazását. A stacioner szenzorhoz képest jelentős különbség mutatkozik a szándékos és nem szándékos zavarok elleni védelem alkalmazásában. A füst- és ködkibocsátó eszköz alkalmazása békeidőben nem rendelkezik relevanciával, azonban a mobil eszközök esetében, konfliktus időszakában kiemelt jelentőséggel bírhatnak.

Mobil állomás esetében a zavarvédelem érdekében az átjátszó állomás, az antenna helyzetének megváltoztatása, esetleges tartalék mobil egység alkalmazása is lehetőség. A központi egységgel való kapcsolattartásban helye és szerepe is lehet olyan, bonyolultabb modulációs módok alkalmazásának, melyek az információt továbbító elektronikai eszközök manőverező képességének kihasználásán alapulnak. Az elektromágneses kompatibilitás (EMC) biztosításában - tartalék egység rendelkezésre állása esetén - alkalmas módszer lehet az elektronikai eszközök széttelepítésének alkalmazása is.

## Összegzés

A nemzetbiztonsági célú rövidhullámú stratégiai rádiófelderítés elektronikai védelmi lehetőségeinek vizsgálatához bemutatásra kerültek a rövidhullámú sávú rádióellenőrző tevékenység sajátosságai.

A nemzetbiztonsági célú rádiófelderítés magyarországi szervezeti evolúciójának eredményeként a SIGINT/COMINT tevékenység ma egy olyan szervezeti keretrendszerben működik, amelyben a komplex stratégiai adatgyűjtés nem, csak az egyes szervezetek (IH, KNBSZ, NBSZ) törvényi feladatkörébe illeszkedő rádiófelderítő és rádiótechnikai felderítő tevékenységek vannak jelen.

A rövidhullámú stratégiai adatszerző központ esetében a mai technológiai és infrastrukturális jellemzők (informatikai alapú jelfeldolgozás, tényleges rádióvételi eszköz nem funkcionál a központban, elhelyezése gyakorlatilag „bárhol”, irodaépületben is lehet sajátos külső jegyek nélkül, illetve a helyhez kötöttség) az elektronikai védelmi aspektusokat jelentősen leszűkítik.

A stacioner szenzorok, bár szintén helyhez kötött kivitelezésűek, de telepítésük a központtal ellentétben kifejezetten nem urbánus környezetben ideális. A szenzor telepítési környezete, kiterjedt méretű és terjedelmű vevő és iránymérő antennarendszere, valamint tényleges rádióvétel jelenléte ez esetben is sajátos elektronikai védelmi lehetőségeket enged meg, illetve tesz szükségessé.

A mobil szenzorok méretükben, kivitelükben, alkalmazásuk jellegében elektronikai védelmi szempontból nagyon hasonlatos kezelést igényelnek az egyéb harcászati jellegű csapategységekkel.

Fontos megjegyezni, hogy míg a stratégiai központ önmagában alkalmazásakor rendelkezésre állnak hatékony álcázási, rejtési lehetőségek, a helyzet nagymértékben megváltozik, amennyiben a feldolgozó központhoz – annak követlen közelében - rövidhullámú vételi és iránymérő antennák, kiterjedtebb antenna rendszerek csatlakoznak.

Összességében megállapítható, hogy a stratégiai felderítő rendszer elemeinek tematikus elektronikai védelmi vizsgálatával megállapíthatóvá váltak az egyes elemeknél alkalmazható, vagy kevésbé hatékony védelmi intézkedések köre.

A vizsgálat eredményeként létrejött táblázatos áttekintés lehetőséget biztosít egy adott létező vagy még tervezés alatt álló rövidhullámú stratégiai adatszerző rendszer elektronikai védelmi lehetőségeinek vizsgálatára, illetve további kutatás alapján egy elektronikai védelmi követelményrendszer megalkotására.

**Felhasznált Irodalom**:


- A nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény.
- A polgári célra használható frekvenciasávok felhasználási szabályainak megállapításáról szóló 2/2013. (I. 7.) NMHH rendelet.
- Balajti I. – Vass S.: Elektronikai védelem. Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem, J-1435. 2000. p. 9
- Dobák Imre: A nemzetbiztonság általános elmélete, Nemzeti Közszolgálati Egyetem, 2014. p.252.
- Frater M. – Ryan M.: Communications Electronic Warfare and the Digitised Battlefield, 2001. http://army.gov.au/Our-future/LWSC/Our-publications/Working-Papers/~/media/Files/Our%20future/LWSC%20Publications/WP/pdfs/wp116-Comms%20EW%20and%20Digitised%20Battlefield_Michael%20Frater_Michael%20Ryan.pdf (Letöltve: 2015.05.24)
- Haig Zsolt: Információ társadalom biztonság, NKE Szolgáltató Kft., p.143. ISBN 978-615-5527-08-1
- Haig Zsolt-Kovács László-Ványa László-Vass Sándor: Elektronikai hadviselés, Nemzeti Közszolgálati Egyetem, Budapest, 2014. ISBN 978-615-5305-87-0
- Haig Zsolt-Várhegyi István: A cybertér és a cyberhadviselés értelmezése, Hadtudomány, 2008. elektronikus lapszám http://www.zmne.hu/kulso/mhtt/hadtudomany/2008_e_2.pdf (Letöltve: 2015.05.24.)

- Kobolka István: Nemzetbiztonsági alapismeretek, Nemzeti Közszolgálati Egyetem, Budapest, 2013. p.127. ISBN 978-615-5344-32-9
- Magyar Honvédség Összhaderőnemi elektronikai hadviselés doktrína. Honvédelmi Minisztérium, Honvéd Vezérkar, Felderítő Csoportfőnökség, Budapest, 2004.
- Molnár Béla, Turi-Kovács Attila: Rádió hullámterjedés és hálózattervezés, Közlekedés- és
- Nemzetbiztonsági Szakszolgálat honlapja http://www.nbsz.gov.hu/?mid=28
- Postaügyi Minisztérium, Budapest, 1969.
- Rothammel Karl: Antenna könyv, Műszaki Könyvkiadó, Budapest, 1977.

# A digitális PMR-ek szerepe a szervezett bűnözésben és a kiscsoportos direkt kommunikációban

**Balog Károly**[1]

**Absztrakt:**

Napjainkban az engedélyhez kötött és engedély nélkül is üzemeltethető PMR[2] rádiótechnológia a mobiltelefonoknál már megtapasztalt paradigmaváltáson megy keresztül. Újfajta digitális PMR rendszerek és egyedi készülékek kezdenek elterjedni a gyakorlatban, melyek frekvenciaengedélyhez nem kötött változatai ráadásul olcsók, bárki számára hozzáférhetők, és mozgásuk sem korlátozott. Cikkemben megvizsgálom az ilyen típusú kommunikáció jelentőségét és alkalmazási lehetőségeit, majd a jelenleg forgalomban lévő eszközök típusait és képességeit tekintem át. Megvizsgálom a piaci trendeket, az új vagy egyedi technológiákat.

**Abstract:**

In these days, both the licensed and license-free PMR radio technology is going through massive paradigm shift as formerly seen at mobile phone technologies. In fact, the new digital PMR systems and individual devices are spreading in practice, which the license-free versions moreover cheap, easily accessible for everyone and not limited in their movements. My article will examine the importance of this type of communication and application possibilities and the types and capabilities of the devices currently on the market is reviewed. I analyze market trends, new or specific technologies.

[1] *Nemzeti Közszolgálati Egyetem, másodéves doktorandusz, bkarika07@gmail.com*

[2] *PMR: Professional / Private Mobile Radio - professzionális / magán mobil rádió: A felhasználók által saját maguknak nyújtott zártkörű rádióalkalmazások gyűjtőneve*

## 1. Bevezetés

A nemzetbiztonsági rádiófelderítés új célterületei között szerepelnek napjainkban a PMR eszközök újfajta digitális változatai, annak eredményeként, hogy az engedélyhez kötött és engedély nélkül is üzemeltethető analóg PMR rádiótechnológia a mobiltelefonoknál már megtapasztalt paradigmaváltáson megy keresztül. A neves európai, amerikai és japán gyártók szabványos digitális rendszerei és készülékei egyre jobban kezdenek elterjedni a gyakorlatban, de jelentős népszerűségnek örvendenek a kínai cégek olcsó, de a szabványok kereteit gyakran átlépő készülékei is. A frekvenciaengedélyhez nem kötött kézirádiók, a 90-es évekbeli kialakulásuk óta töretlen népszerűségnek örvendenek: olcsók, bárki számára hozzáférhetők, és mozgásuk sem korlátozott. Új típusú digitális változataik a professzionális rendszerekhez hasonló megoldásokat tartalmaznak, azonban azoknál olcsóbban és bárki számára hozzáférhetően, Mivel az ilyen eszközök teljes mértékben kikerülhetik a hagyományos távközlési infrastruktúrákat, felderítésük és ellenőrzésük kizárólag rádiós úton, a rádiófelderítés eszközrendszerével történhet. Éppen ezért ezeket a rádiókat bűnözők és terroristák is előszeretettel alkalmazzák kommunikációra, a távközlés ellenőrzés tudatos elkerülése céljából. Mindezek mellett pedig alternatívát képezhetnek a speciális katonai vagy kiscsoportos speciális műveleti kommunikáció területén is. Szegényebb, infrastruktúra hiányos országokban, konfliktus (szükség kommunikáció), vagy természeti katasztrófa sújtotta területeken is (vészhelyzeti kommunikáció), előléphetnek elsődleges kapcsolattartó eszközzé.

Kutatási témámban a modern rádiófelderítés eszköz- és elméletrendszerével, ezen belül az ilyen eszközök felderítési ellenőrzési lehetőségeivel foglalkozom részletesebben. Cikkemben megvizsgálom az ilyen típusú kommunikáció jelentőségét és alkalmazási lehetőségeit, majd a jelenleg forgalomban lévő eszközök típusait és képességeit tekintem át. Megvizsgálom a piaci trendeket, az új vagy egyedi technológiákat.

## 2. A COMINT[3] célterületének változása a nemzetközi szervezett bűnözés kapcsán

A COMINT alkalmazásának célterületei igen szerteágazóak. A leghagyományosabb COMINT célpontok a katonai és diplomáciai üzenetek voltak. Az 1960-as évektől azonban a fokozódó világkereskedelmi növekedés miatt egyre inkább előtérbe került a gazdasági jellegű, valamint a tudományos-technikai fejlesztésekre irányuló kommunikációs felderítés. A COMINT legújabb célpontjai közé tartozik napjainkban a kábítószer kereskedelem, a pénzmosás, és

[3] *COMINT: Communications Intelleigence - Rádiófelderítés*

a nemzetközi terrorizmus valamint a nemzetközi szervezett bűnözés. Ezen új célpontok természetesen új kommunikációs módok (fokozottabb) elterjedését is magukkal hozták, amelyek legfőbb erőfeszítései a sikerességük érdekében arra irányulnak, hogy a hagyományosan ellenőrizhető és ismert kommunikációs formákat valamilyen módon tudatosan elkerüljék, illetve a kommunikáció során az identitásuk minél kevésbé legyen ellenőrizhető. Ez a tendencia feltárt a nemzetközi szakirodalomban[4], így hazánkban is egyre jellemzőbb[5].

Ha megértjük a bűnügyi szervezetek szerkezetét kiderül, hogy a szervezett bűnözés alapvető (kulcsfontosságú) sérülékenységi pontja a kommunikációban rejlik[6], mivel a bűnözéshez azonnali és hatékony kommunikáció szükséges tevékenysége lebonyolításához. Grabosky és Smith[7] megállapították, hogy négyféle alapvető tevékenység során használják a kommunikációt: - bűncselekmények tervezésére és koordinálására, - a tiltott áruk v. termékek marketingjére és forgalmazására, - a szervezeti struktúra fenntartására, valamint - a rendőrségi nyomozás akadályozása céljából. A fenti tevékenységek hatékony kivitelezéséhez különféle kommunikációs formákat használnak, és mindig keresik a fenti funkcióknak megfelelő legalkalmasabb és legbiztonságosabb módszereket, a kommunikációs technológia legújabb megoldásait messzemenően kihasználva.

Ezek egy része a hagyományos rádiózás analóg, de újabban digitális és ez által kevésbé lehallgatható formái irányába mutatnak, míg más részük a hagyományos LI[8] által ellenőrizhető kommunikációs formákon belül egy IP alapú (sub) kommunikációs formát valósítanak meg, melyhez annak szolgáltatótól való elkülönülése okán az LI által egyelőre nem lehet hozzáférni[9].

A témám tekintetében megállapíthatom, hogy a fenti bűnözői kommunikációs célok közül a PMR rádiók leghatékonyabban a bűncselekmények kivitelezése koordinálása során alkalmazhatóak, ahol ugyan olyan előnyökkel rendelkeznek, mint amivel a rendvédelmi szervek esetében is: gyors

---

*[4] Jackson, B. A., Chalk, P., Cragin, R. K., Newsome, B., Parachini, J. V., Rosenau, W., Temple, M. (2007), Breaching the Fortress Wall: Understanding Terrorist Efforts to Overcome Defensive Technologies. Santa Monica: RAND Corporation.*

*[5] Balog Károly: A PMR rádiózás kialakulása, fejlődése, jelentősége napjaink hírközlésében, Társadalom és Honvédelem, 2013. XVII. évf. 3.-4. szám, pp. 97-115.*

*[6] Malkin, S. (2007). Social Networks of Organized Crime: Towards a Communication Approach. Proceedings of the National Communication Association 93rd Annual Convention, November 15: Chicago.*

*[7] Grabosky, P., & Smith, R. (1999). Crime in the Digital Age: Controlling Telecommunications and Cyberspace Illegalities. The FBI Law Enforcement Bulletin, July.*

*[8] LI: Lawful Interception – törvényes ellenőrzés (A távközlési rendszerek törvényes lehallgatása)*

*[9] Kovács Zoltán: Felhő alapú rendszerek törvényes ellenőrzési problémái, Hadmérnök, VIII. évf. 1. szám, 2013. március http://hadmernok.hu/2013_1_kovacsz.pdf (2013. 09. 25.)*

hívásfelépülés, pont-multipont csoportkommunikáció, megbízható rendelkezésre állás (elkülönült rendszer), és direkt kommunikáció esetén a távközlési infrastruktúra (tudatos bűnözői szempontú) kikerülése, illetve (szükséghelyzeti) szükségtelensége. A digitális rádiók esetében ehhez adódik hozzá a relatív jó lehallgatás elleni védettség is, valamint olyan új szolgáltatások megjelenése melyek még hatékonyabbá teszik ezeket az eszközöket.

A fent említett tendenciák hazánkban és a környező országokban egyaránt éreztetik hatásukat. Azaz IP alapú esetben olyan új típusú potenciális adatforrások jelentek meg, mint a -mobil cellás földi (2-3-4 G) és -mobil műholdas kommunikációs rendszerek IP alapú (ezeken belül a különféle elkülönült: Viber, Skype, stb.) kommunikációs formák, és természetesen az általam kutatott PMR kommunikáció különféle főleg digitális típusai és fajtái. Természetesen a polgári nemzetbiztonsági feladatkörben ezek ellenőrzése adott rendszereknél a törvényes ellenőrzés eszközével is kivitelezhető, azonban bizonyos kommunikációs formák kizárólag a COMINT eszközével vonhatók ellenőrzés alá.[10].

## 3. Az élő és tárolt kommunikáció viszonya a COMINT tevékenységéhez és a PMR ellenőrzéshez

A kommunikációs formák technikai értelembe alapvetően 2 féle típusba sorolhatóak: élő kommunikáció és tárolt kommunikáció típusába. Az első forma pl. a telefonbeszélgetés, de ide tartozik a PMR rádiók beszédkommunikációja is. Itt alapvetően a fogadó (az üzenet vevője) azonnal megkapja, (on-line / valós időben) veszi (értelmezi) az üzenetet, amelyik így nincs rögzítve és nyilvántartva a tartalom szempontjából[11], miután a kommunikáció, azaz a beszélgetés befejeződik. Ezzel szemben a tárolt kommunikáció esetében az üzenet, az átvitel során egy vagy több helyen pl. szervereken, számítástechnikai eszközökön rögzítésre kerül, amelyet ezután a szolgáltató elérhetővé tesz a címzett részére, aki ezt letölti, így a saját eszközön is tárolva van. Ilyen üzenetek pl. az e-mail, az SMS, a hangposta, a különféle chat programok azonnali üzenetküldő alkalmazások, VoIp telefon adatcsomagok. Tehát ez utóbbiaknál már akkor rögzítésre kerül az üzenet, mielőtt a címzett ezt megkapná[12].

A fenti gondolatment alapján a PMR eszközök rádiók az élő kommunikáció csoportján belül azért is különlegesek, mivel zártkörű (saját maguknak nyújtott)

---

*[10] Balog Károly: Digitális PMR rendszerek összehasonlítása I., Hadmérnök, IX. évf. 3. szám. 2014. szeptember http://www.hadmernok.hu/143_08_balogk.pdf (2014. 09. 30)*

*[11] Természetesen a kommunikáció kísérő adatait, azaz a meta adatokat / beszélgetés kezdetét végét, a kommunikáló feleket, stb. /, tárolják a számlázási információk miatt*

*[12] Dr Peter Bell - Mitchell Congram: Communication Interception Technology (CIT) and Its Use in the Fight against Transnational Organised Crime (TOC), International Journal of Science Research, 2014. Vol. 2, No. 1.*

szolgáltatás okán nincsenek számlázási adatok, így ehhez kapcsolódó meta adatok sem, kivéve, ha biztonsági okokból ezek mégis rögzítésre kerülnek (pl. diszpécser típusú rendszereknél). A direkt kommunikáció esetén pedig nincs is rá mód, hogy ilyen adatokat rögzítsünk, kivéve akkor, ha egy passzív rádiófelderítő eszközt működtetünk kifejezetten ezzel a céllal.

A kutatási témám szempontjából azonban van némi átfedés a hagyományos rádiózás digitális változatai és az IP alapú kommunikáció (tárolt formái) között. A legtöbb ilyen digitális PMR szabvány ugyanis átjátszón keresztüli, vagy trönkölt működésmódja során képes egyelőre még csak alacsony sebességű IP alapú (adat) kommunikációra, a legújabb tendenciák alapján azonban szélessávú PMR rendszerek bevezetését is tervezik. Ez utóbbiak, pl. a kialakulóban lévő LTE[13] hálózatokat használnák hordozó közegként, szimbiózist alkotva azokkal. Az ilyen IP alapon kommunikáló PMR rendszerek esetében szintén felvetődik az LI gondolata, azonban ezekre egyelőre nem léteznek kidolgozott LI szabványok.

A fenti gondolatmenetből látható az egyébként is közismert tendencia, hogy minden az un. all IP vagy Nextgen hálózatok irányába mutat, a PMR kommunikáció tekintetében is. Így az IP alapú hálózatok oldaláról történő ellenőrzés lehetőségének vizsgálata is fontos lehet, de le kell szögezni, hogy a direkt kommunikációt folytató eszközök esetében ez akkor sem vezet eredményre. Kutatásaim során az IP alapú ellenőrzési lehetőségekkel nem foglalkozom.

## 4. A PMR rendszerek távközlésben betöltött szerepe, típusai, szabványai

A PMR rendszerek alapvető funkciója az azonnali beszédkommunikáció megvalósítása két vagy több felhasználó között egy csoporton belül. A modernebb digitális rendszereknél már megjelenik a lehetőség a kissebességű adatátvitelre: szöveges információk, egyedi jelzések (vészjelzés, helyzetinformációk, stb.) formájában. A PMR piac a rádiózás speciális szegmensét jelenti. Pont-többpont átviteli módja kifejezetten alkalmas egy szervezeten belüli hatékony kommunikáció elősegítésére, de ha szükséges pont-pont összeköttetés is megvalósítható. Az egyes szervezetek funkciója, a megvalósított szolgáltatások köre, az engedélyezési feltételek jelentősen differenciálják az egyes PMR hálózatokat, melyek egyben az ilyen rendszerek flexibilitását, és skálázhatóságát is jelentik. A PMR rendszerek típusait 3 fő csoportba sorolhatjuk. A direkt kommunikáció két vagy több azonos frekvencián működő terminál között jöhet létre (1. ábra bal oldala). Ebben a kategóriában megkülönböztetnek engedély nélkül üzemeltethető kis hatótávolságú max. 500mW teljesítményű eszközöket, valamint frekvenciaengedélyhez kötött nagyobb teljesítményű csoportot

[13] *LTE: Long Term Evolution, 4. generációs mobil cellás átviteli technológia*


**1.** ábra Direkt kommunikáció és diszpécser típusú rendszer[14]

Ha nagyobb területi lefedettség szükséges, átjátszót alkalmaznak a hatótávolság növelésére. Ekkor a kommunikáció a PMR terminálok között nem direkt módon, hanem az átjátszó állomáson keresztül jön létre (1. ábra jobb oldala) ezek az un. helyszíni vagy diszpécser típusú rendszerek, melyek nagyon elterjedtek a gyakorlatban. Egyre jellemzőbb, hogy ez utóbbiak valamilyen IP alapú hálózathoz is kapcsolódnak, mellyel jelentősen kibővíthető a terülreti lefedettség illetve a PMR hálózatok beszéd és adatkapcsolata más vezetéknélküli és vezetékes rendszerek felé is kiterjeszthető. A harmadik kategória a trönkölt rendszerek csoportja, melyek méretük és szolgáltatásaik alapján leginkább a vezetéknélküli mobilhálózatokhoz hasonlítanak.

Mindhárom fenti típus megtalálható az újfajta digitális szabványcsoportok kínálatában, melyekből az európai szabványok mellett amerikai, japán, és kínai változatok is léteznek más névvel, de teljesen hasonló technikai megoldásokkal. A digitális PMR szabványkategóriának két nagy csoportja létezik, melyeket alapvetően a csatorna hozzáférési technika alapján lehet elkülöníteni, és amely egyben a csatorna sávszélességet is meghatározza. Így a gyakorlatban TDMA[15] alapú szélessávú (12,5-25 kHz), valamint FDMA[16] alapú keskenysávú (6,25-12,5 kHz) technológia csoportokat különböztetnek meg a szabványokban és a szakirodalmakban egyaránt (1. táblázat). Európában, és Amerikában a DMR és a dPMR (USA-ban NXDN) szabványok a legelterjedtebbek a kereskedelmi szektorban, de a kormányzati és rendvédelmi szférában a TETRA és a P25 a mérvadó rendszerek. Természetesen nem hivatalosan bármilyen típusú és szabványú készülékeket be lehet szerezni és üzemeltetni a világ bármely pontján, az engedélyhez nem kötött vagy amatőr sávokban, illetve illegálisan az engedélyhez kötött, de kevéssé használt frekvencia-tartományokban is.

[14] *http://www.icom.co.jp/world/idas/dpmr/whats_dpmr/ (2013.01.15.)*

[15] *TDMA: Time Division Multiple Access – időosztásos többszörös hozzáférési (rádiócsatorna megosztási) technika*

[16] *FDMA: Frequency Division Multiple Access – frekvenciaosztásos többszörös hozzáférési eljárás*

| FDMA alapú | TDMA alapú |
|---|---|
| dPMR[17], TS 102-490, TS 102-658 (EU) | DMR[18] (EU) /2 időréses/ |
| NXDN (USA) | PDT[19] (Kínai) /2 időréses/ |
| DCR[20], ARIB[21] standard T-98 (Japán) | |
| ARIB standard T-102 (Japán) | |
| P25[22] (1 fázis TIA-102) (USA) | P25 (2. fázis) (USA) /2 időréses/ |
| Tetrapol[23] (Francia) | TETRA[24] (EU) /4 időréses/ |
| D-Star[25] (Japán amatőr) | |

**1. táblázat.** A jelenlegi elterjedtebb digitális PMR rádiószabványok

A kínai készülékek ráadásul nagyon olcsók és szinte az összes típusú (nem csak kínai szabványú) készülék közvetlenül megrendelhető az internetről is, így szinte bárki számára egyszerűen hozzáférhetőek. Ezek között nagyon sok készülék olyan az eredeti szabványoktól eltérő tulajdonságokkal is rendelkezik pl. engedély-nélküli sávú készülékek, melyek jóval nagyobb adóteljesítményre képesek, mint a megengedett 500mW. Így 1-5W teljesítménnyel az adótávolság jelentősen megnövelhető, még épületen belüli alkalmazások esetén is. A rádiók gyakorlatilag gyárilag programozottak, így out of box megoldást kínálnak a legegyszerűbb közvetlen (direkt) kommunikáció alkalmazására, de természetesen némi

[17] *dPMR: Digital Professional Mobile Radio – Amely a hagyományos 12,5 kHz-es analóg csatornát két 6,25 kHz-sávszélességű digitális rádiócsatornával váltja ki.*

[18] *DMR: Digital Mobile Radio – Amely a hagyományos 12,5 kHz-es analóg csatornát, 12,5 kHz-sávszélességű két időréses TDMA (időosztásos) digitális rádiócsatornával váltja ki.*

[19] *PDT: Professional Digital Trunking – 2 időréses DMR-hez hasonló trönkölt rendszer*

[20] *DCR: Digital Convenience Radio – az európai dPMR alapján készült Japán digitális rádiószabvány*

[21] *ARIB: Association of Radio Industries and Business – Japán Üzleti és Ipari Rádió Társaság, a DCR kidolgozója*

[22] *P25: Project 25 – az APCO (Association of Public Safety Communications Officials International) kezdeményezésére a TIA (Telecommunications Industry Association) által kidolgozott nyílt rádiószabvány, melyet a TETRA-hoz hasonló célokkal hoztak létre amerikában, de Kanadában és Ausztráliában is használt.*

[23] *Tetrapol: A tetrától eltérő francia trönkölt szabvány*

[24] *TETRA: Terrestrial Trunked Radio – európai trönkölt rádiószabvány*

[25] *D-Star – Digital Smart Technologies for Amateur Radio, a Japán rádióamatőr szövetség (JARL) szabványa*

szakértelemmel egyszerűen át is programozhatóak. Természetesen a nevesebb gyártók professzionális típusaiért jelentős árat kell fizetni, amihez a kiegészítő titkosítás és egyéb tartozékok megvétele (töltők, tokok, külső antennák, stb.) is plusz árat jelen. A szervezett bűnözés számára azonban ezek sem hozzáférhetetlenek. A legolcsóbb és szerintem még megfelelően megbízható kommunikációs alternatívát mégis az olcsó kínai készülékek csoportja jelentheti az illegális, vagy a relatív biztonságosabb digitális kommunikációt választó felhasználók részére egyaránt.

## 4. A digitális PMR rádiók piaca

A Research and Markets[26] piackutatásai alapján a legmarkánsabb trend jelenleg a digitális piacon az LMR-PMR hálózatok LTE hálózatokhoz történő kapcsolódásának kialakítása. Igen dinamikusan növekvő piacról van szó, amelynek a 2013 évi összes bevétele 10,57 milliárd dollár volt, az analóg rendszereket is beleszámítva. Az egyes szabványkategóriák sorrendje a digitális szegmensben a következő volt, a részesedésük arányában: a TETRA rendszer vezet, utána az amerikai P-25 következik, majd a dPMR/NXDN, a DMR és végül a Tetrapol zárja a mezőnyt. A legnagyobb piaci részesedést a következő négy cég könyvelte el 2013-ban: A Motorola Solutions Inc., a Harris Corporation, a Raytheon Company, valamint a Thales Group. Ezek mellett azonban még számos gyártó készülékei és rendszerei (EMC, Hytera, Radio Active, Selex Elsag, Vertex Standard, ICOM, JVC-Kenwood, ) találhatók meg a piacon, és igen feljövőben vannak a kevésbé neves kínai gyártók is (Beifeng, Wintec, stb.) a szegmensben, olcsó alternatívát kínálva a nevesebb gyártók termékeinek. A következőkben áttekintem néhány gyártó termékeit és egyedi megoldásait, amelyek összességében jól reprezentálják a piacon lévő tendenciákat és trendeket és megfelelő kitekintésre adnak lehetőséget.

Harris cég a 2. legsikeresebb a Motorola mögött, melynek Momentum DMR rádiócsaládja egymásra épülő típusokból áll, melyek a típusszám növekedésével egyre fejlettebb képességekkel és egyre bővülő funkciókkal rendelkeznek. A 2. ábrán a baloldali kijelző nélküli legolcsóbb típus HDP-100 ára a programozástól függően (direkt, átjátszón keresztüli, vagy trönkölt működés) 1000-1200 dollár körül van tartozékokkal együtt. A középső HDP-150 ennek színes kijelzővel és billentyűzettel ellátott változata, 1100-1300 dolláros áron. A jobboldali HDP-250 pedig napjaink egyik legkisebb DMR rádiója, amellyel csak a Hytera cég hasonlóan kisméretű és képességű modellje versenyezhet. A HDP-250 belépő ára 1400 dollár, ami 1700 dollárnál fejeződik be. A legnagyobb típus a katonai szabványoknak is megfelel. A cég átjátszóállomást is kínál 50W-os kivitelben

[26] *http://www.researchandmarkets.com/reports/3001313/land-mobile-radio-lmr-systems- tetra-project#adaptive*

2900 dollárért, azonban ha diszpécser típusú rendszert akarunk üzemeltetni, ehhez még meg kell vásárolni a dipatcher szoftvert a kiegészítőkkel ami még plusz 4000-5000 dollár egy 25 rádiós rendszerre.


HDP-100 HDP-150 HDP-250

**2.** ábra A Harris cég kézi DMR típusai [27]

A rádiók a digitális átvitel mellett a hagyományos analóg üzemmódban is működhetnek. Rendelkeznek beépített GPS-el, képesek csoport és egyéni hívásokra, a készülékek távolról monitorozhatók vészhelyzet esetén. Mindhárom típushoz vásárolható titkosító (AES 256) kiegészítés, ami plusz 300 dollárba kerül.

A Kenwood európai kínálatában átlagos készülékek találhatóak ezek NXDN (NEXEDGE) szabványúak, Ambe2+ beszédkódolóval, analóg és digitális üzemmódra alkalmasak. A 3. ábrán, a baloldalon látható N-330 azonban un. ATEX minősítésű veszélyes környezetben (robbanás, gáz, éghető por) történő használatra készült különleges rádió. a NX-300 egy átlagos NXDN típus, míg a TK-340 egy legegyszerűbb engedély nélküli sávú, dPMR szabványú 16 csatornás készülék, amelyik az analóg üzemmódban beszédspekrum-fordítós (Voice Inversion Scrambler) típusú egyszerű beszédtitkosítást alkalmaz.

Az NX200-300 /NEXEDGE/ típusú rádiók mindegyike kiegészíthető 256 bites AES/DES (KWD-AES/DES21), illetve egy gyengébb 56 bites DES (KWD-DE21) panelba illeszthető titkosító modullal (3. ábra jobb oldala). Mind a 256 bites mind az 56 bites modul (Encryption Module), 1024 kulcs tárolására képes, melyek kulcsfeltöltő szoftverrel változtathatóak. Az ilyen titkosító modulok hivatalos beszerzés során export-engedély kötelesek adott országokban, így csak a megfelelő engedélyek alapján lehet megvásárolni és kivinni őket.

[27] *http://pspc.harris.com/media/ComwlthofVAMomentumCatalog8009D_tcm42-21635.pdf (2015.01.15.)*


NX-330EXE NX-300GE TK-3401DE KWD-DE/AE-21 titkosító modul

**3.** ábra A Kenwood cég kézi NXDN és dPMR típusai és titkosító moduljai [28]

Vannak a piacon olyan egyedinek számító megoldások is mint a kínai Hytera cég kiscsoportos kommunikációra pl. bevetési csoportok kommunikációjára szánt professzionális megoldása, amelyik egy hátizsákban hordozható átjátszó-állomás (RD96X) és egy intelligens diszpécser állomás és alkalmazás segítségével egy bevetési csoport minden típusú kommunikációs igényét kiszolgálja, még épületen belüli alkalmazás esetén is (4. ábra). Egy konzol 8 csatornát kezel, és lehetőség van az állomások helyzetkövetésére útvonaluk kirajzolására, rejtett pl. vibrációs hívására, hangrögzítésre és visszajátszásra az összes rádió egymás közötti és külső hálózatba irányuló vagy onnan fogadott hívások esetében. Az összes rögzítményben keresni lehet idő és rádióazonosító szerint is. Lehetséges a kompromittálódott készülékek tiltása, illetve rejtett behallgatás a rádió környezetébe mikrofonján keresztül. A cég gyártja a világ legkeskenyebb és legkisebb méretű teljes értékű DMR rádióját az X1e típust (4. ábra bal oldal)

Az 5. ábrán a cég legújabb kommerciális típusú PD3 sorozatú DMR rádiói láthatóak, amelyek hagyományos mobiltelefon méretűek, USB-ről tölthetők. Az UHF sávú készülékekben semmi különleges nincs, 256 csatorna tárolására képesek, 1,5W ill. 3W kimenő teljesítményt biztosítanak, analóg üzemmódra is képesek, 64 karakteres üzenetek küldhetők vele, és 4 programozható gombbal rendelkeznek. A kreatív antenna kialakításnak köszönhetően kompakt méretűek, és egyedi formatervezésükkel kitűnnek társaik közül.

[28] *http://www.kenwood.eu/comm/digital/portable/NX-230EXE/ (2015.01.15.) http://www.kenwood.eu/comm/digital/portable/NX-300GE/ (2015.01.15.) http://www.kenwood.eu/comm/license_free/TK-3401DE/ (2015.01.15.)*


**4.** ábra A Hytera cég kiscsoportos bevetési rendszere és elemei[29]


**5.** ábra A Hytera cég PD36X és PD35X típusú DMR rádiója[30]

[29] *http://www.hytera.com/productResources.htm?columnId=416&proId=259&resourceType=2#page-index (2013.01.20.)*

[30] *http://www.hytera.com/productResources.htm?columnId=416&proId=2493&resourceType=2#page-index (2015.01.15.)*

A cég élenjár mind a professzionális mind az engedély nélküli készülékek területén, így 2014. november 24-én jelentették be, hogy forgalomba hozzák a világ első engedély nélküli sávban működő (Tier I. kategóriájú) DMR készülékeit[31]. Az új típusok az 5. ábrán látható tokozásban, de eltérő rádiós paraméterekkel és típusszámmal kerülnek forgalomba. Ezek a PD355LF és a PD365LF típusok, míg ezek mellett megjelent egy hagyományos kivitelű (tokozású) PD505LF típusú készülék is. A rádiók az európában elfogadott 446,0 -446,2 MHz-es frekvenciatartományban működnek, mind analóg mind a digitális átvitelnél 500 mW teljesítménnyel és 12,5 kHz-es csatorna sávszélességgel. AMBE+2 beszédkódolóval, 2000/ 1500 mAh kapacitású akkumulátorral kb. 12/16 órás működésre képes (5/5/90 másodperces[32]) használati ciklusidő mellett. A két kisebb 160, illetve a nagyobb 260 grammos, rádiók 32 csatorna tárolására képesek, IP54 kategóriájú por és vízállósággal rendelkeznek.[33]

A DMR szabványú eszközök a TETRA-hoz hasonló biztonság mellett, jóval kedvezőbb árfekvésű rendszerek kialakítását teszik lehetővé, így valós alternatívát képviselnek a digitális migráció kapcsán az analóg rendszerek leváltása során. A cég 2014. októberi bejelentése során közölték, hogy a közeli Cseh Köztársaságban Breclav, Znojmo és Blansko városokban a cég DMR Tier II. típusú rendszerei kerülnek kiépítésre a helyi rendőrség számára.[34] Az RD985 típusú átjátszókból és a professzionális kivitelű 60db PD785G típusú kézi, valamint az 14 db MD785G típusú mobil rádiókból álló flotta kerül alkalmazásra. A készülékek beépített GPS-el rendelkeznek, így kültéri esetben nyomon követhető a készülékek tartózkodási helye a diszpécser állomáson. A rádiókészülékek kültéri helyzetkövetése természetesen már régóta nem jelent technikai problémát, azonban a rádiók digitalizálódása a digitális formájú helyzetadatok közlését nagymértékben leegyszerűsíti, valamint beszédinformációval párhuzamos automatikus átvitelét is lehetővé teszi. Hazánkban is számos helyen működnek már DMR szabványú hálózatok és rendszerek a Tier 2 engedélyköteles kategóriában.

Vannak azonban a piacon olyan különleges megoldások is, mint az angol PMR Products nevű cég SafetyNet Locator nevű megoldása. Ez lehetővé teszi egy adott helyszínen, a rendszerben lévő PMR rádiók nem csak kültéri, de beltéri

---

[31] *DMR handhelds for digital PMR446 radio, (Latest News) http://www.hytera-mobilfunk.com/news-events/latest-news/details/dmr-handhelds-for-digital-pmr446-radio/browse/1/bPid/1033/ (2015. 01. 15.)*

[32] *5/5/90: 5 másodperc adás, 5 másodperc vétel és 90 másodperc szünet ciklusú igénybevétellel számolva*

[33] *Hytera presents: The world's first DMR handheld radios for digital PMR446 http://www.dmrtier1.com/fileadmin/user_upload/Downloads/90PD_DMRTIER1_Fly_ENG_v02_web.pdf (2015. 01. 15.)*

[34] *City police builds on radio technology from Hytera (Latest News) http://www.hytera-mobilfunk.com/news-events/latest-news/details/city-police-builds-on-radio-technology-from-hytera/browse/1/bPid/1033/ (2015. 01. 20.)*

helyzetkövetését is az adminisztrátorok számára. Kültéri esetben a rádió pontos GPS pozíciója kerül ábrázolásra a térképen, mely többféle formátumú lehet, még beltéri tartózkodás esetén egy megadott területet lefedő tartózkodási zónán belüli jelenléte. Azaz egy épület (objektum) több zónára van felosztva az alapterület tekintetében, és az egyes zónákon belüli tartózkodás ismert, de azon belül a pontos pozíció nem. A rendszer technikailag úgy működik, hogy a rádiókészülékekhez egy speciális vevőt kell csatlakoztatni, amelyik vagy külső modul vagy beépített a készülékbe. A speciális vevő a zónákban megadott pozícióban elhelyezett jeladók (bacon) jeleit veszi, amelyek az adott zóna referencia számát sugározzák. A jeladók beépített akkumulátorral 2-5 évig működnek önállóan, de természetesen hálózati energiával is üzemelhetnek. Távolról menedzselhetőek (programozhatóak, pl, hogy milyen típusú rádióval működjenek együtt), és elhelyezésüknek meg kell felelni a védelmi és biztonsági előírásoknak. Minél nagyobb számú bacon van a rendszerben annál pontosabb a helyzetinformáció. A jeladó és a PMR-be épített dekóder IEEE 802.15.4 ZigBee protokollon keresztül kommunikálnak a 2,4-2,5 GHz-es sávban. A jeladó 15 mS-os csomagokat küld, majd 1-20 másodpecig készenlétben van. A jeladótól kapott zóna információt a PMR rádiók a hagyományos rádiócsatornán küldik vissza rövid adat üzenet formájában egy központi dekódernek, amelyik egy rádiómodem vagy fix telepítésű rádió. Ez dekódolja a visszaküldött adatokat és az audió információt. A SafetyNet Locator térképén vagy sematikus ábráján jelenítik meg a pozícióadatokat (zóna) és a rádiók egyéb kiegészítő, pl. állapot (vészjelzés, stb.) információit, míg a hangadatokat egy hagyományos diszpécseralkalmazás kezelheti. Ez utóbbi természetesen az összes itt megszokott funkciót betölti, azaz hangrögzítésre képes, szöveges üzenetek küldhet/fogadhat, és az állapot információk ugyanúgy megjelennek, mint a térképen. A rádiók pozíció adatai szöveges vagy audió üzenet formájában kiküldhetők a többi felhasználó részére is, pl vészhelyzet esetén.

A cég megoldása többféle digitális PMR szabvánnyal (TETRA, DMR, NEXEDGE) is képes együttműködni, de ezen felül DECT telefonok, személyhívók és SRD eszközök kezelésére is képes. A 6. ábrán a Hytera cég PD780 típusú DMR rádiójának külső vevője, az x1p/e rádió belső vevője, illetve a jobb oldalon a rendszer jeladói láthatók kétféle kivitelben. A rendszer alkalmazása ideális lehet börtönökben de akár veszélyes ipari vagy egyéb nagy biztonságot igénylő helyszíneken egyaránt.

És végül, de nem utolsó sorban bemutatok két kínai készüléket a low-end dPMR DMR/PDT kategóriából, amelyekhez egyszerűen hozzáférhet bárki internetes megrendelés útján. A TCB TM208 egy dPMR szabványú készülék, 1-4 W kimenő teljesítménnyel rendelkezik és mindössze 50 dollárba kerül. A másik típus TCB TM218 egy TDMA két időréses DMR szabványú készülék, amelyik a kínai PDT szabványt is tudja kezelni. Ennek az ára duplája az előzőnek, azaz 100 dollárba kerül. A két készülék a 7. ábrán látható. A tokozásuk meglehetősen hasonló az interneten rendelhető többi ilyen kategóriájú készülékhez. A high-end (pl. Harris) és a low-end szintek készülékei nyilván eltérő kategóriát képviselnek, de a

minőségkülönbségnél a mintegy tízszeres az árkülönbség jóval nagyobb, a kínai készülékek javára. A 6. ábrán látható PD780 típusú Hytera készüléket is meg lehet rendelni az interneten, amelyik az 500 dolláros árfekvésével a középkategóriát képviseli, legalábbis az ár tekintetében mindenképpen.


**6.** ábra A Hytera PD780 külső illetve x1e/p belső jeladó vevője és bacon jeladói[35]


**7.** ábra TCB TM208 és TM218 típusú digitális PMR rádiók[36]

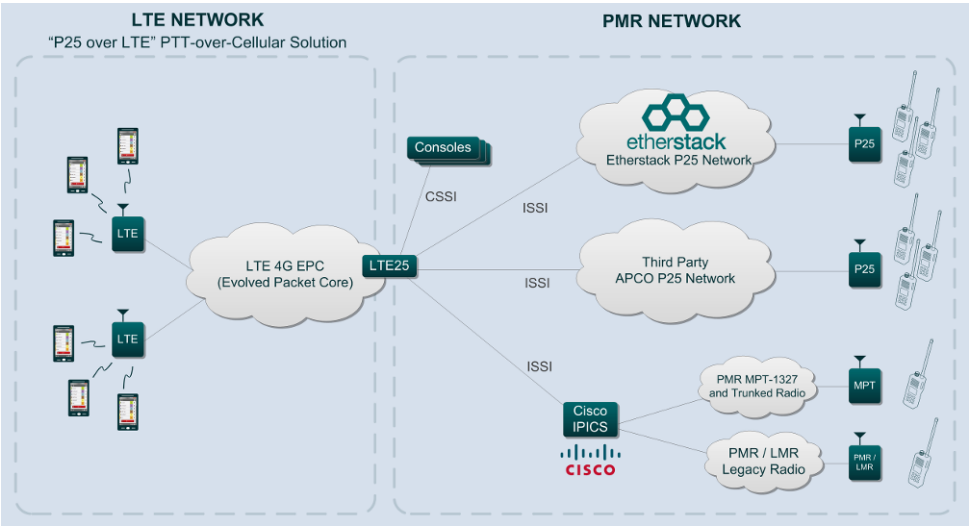
## 5. A PMR-LTE integráció

A piac legújabb és legdinamikusabban fejlődő trendje, a különféle LMR-PMR hálózatok LTE hálózatokhoz történő kapcsolódásának kialakítása. Erre már több

[35] *http://pmr-products.com/PMR-Products/SafetyNet-Locator/ (2015.01.15.)*

[36] *http://1017904.en.makepolo.com/products/Police-professional-Digital-two-way-radio-p25406432.html (2015.01.15.)*

cég is dolgozott ki megoldásokat, melyek közül az Etherstack cég PMR over LTE megoldását ismertetem. A cég PMR-LTE Softswitch megoldásai hidat képeznek az LTE hálózatok és a meglévő PMR hálózatok push-to-talk megoldásai között 8. ábra. A hagyományos rádiós készülékek tökéletesen kommunikálni tudnak és együttműködnek az LTE hálózathoz kapcsolódó Androidos készülékekkel, a különböző gyártójú hálózatokon keresztül is. A rendszerben az adott PMR szabvány valamennyi funkciója és szolgáltatása rendelkezésre áll az LTE környezetben is, beleértve az összes típusú beszédhívást és adatszolgáltatásokat is. A softswitch megoldásnál nem alkalmaznak jel-átkódolást a rendszerben, így nem romlik sem a beszédminőség, sem a kapcsolat felépítési idő.




**8.** ábra Az Etherstack Push-to talk PMR over LTE megoldása[37]

Ennek érdekében az Androidos eszközön az adott PMR szabvány beszéddekódolóját futtatják (TETRA, P25, DMR, dPMR, NXDN, stb.). Az átkódolás nélkül megoldható továbbá az eszközök közötti végponti titkosítása (LTE-PMR), akár OTAR[38] funkció alkalmazása mellett is. A megoldás egy nagy rendelkezésre állású, korlátozott földrajzi területen működő katasztrófa utáni helyreállítási pontot kínál (DRN - Disaster Recovery Node), a hálózat üzemeltetési központok (NOC- Network Operation Centre) tartalék kommunikációjára, annak működésképtelensége esetén. A 9. ábra bal oldalán látható a rendszer Windows alapú Blue Force Tracking (saját erő követő) desktop GIS (Geographic Information System – Térinformatikai rendszer) alkalmazása, amelyik a Google

[37] *http://www.etherstack.com/eu/images/ES_LTE25_diagram.png (2015.01.15.)*

[38] *OTAR: Over The Air Rekeying – Azaz a rádiócsatornán keresztüli kulcs-csere, a titkosítás megváltoztatására.*

Earth alkalmazásba is beépül. Ezen egyaránt nyomon követhető az LTE és PMR készülékek helyzete valós időben, valamint egyedileg hívhatók készülékek illetve hívócsoportok is. Megoldható az automatikus járműkövetés (AVL[39]) a járművek sebesség, hely és állapot információinak lekérésével. A 9. ábra jobb oldali képén a rendszer Androidos kliens alkalmazása látható, az egyes hozzákapcsolódó hívócsoportok listájával. A készülék egy kereskedelmi forgalmú technikai feltételeknek megfelelő eszköz lehet. Az androidos telefonon egyszerre több hívócsoport kommunikációja is figyelemmel kísérhető, valamint csoporthívás is kezdeményezhető.


**9.** ábra PMR over LTE Blue Force Tracking és Android kliens alkalmazás [40]

## 6. A PMR eszközök felderítésének metodikai megfontolásai

A COMINT tevékenység folytatható stratégiai és taktikai szinten is, azonban a hagyományos COMINT felfogás szerinti stratégiai ellenőrzés a PMR eszközök felderítése kapcsán nem értelmezhető, hiszen egy adott korlátos földrajzi helyszínen van lehetőség az eszközök detektálására, különösen kisteljesítményű engedély nélkül üzemeltethető direkt módú eszközök esetén. Így ebben az esetben inkább csak taktikai alkalmazásról beszélhetünk. A szakirodalomban ezt szokták működési zónának (területnek) nevezni. Szűrő-kutató jelleggel lehetséges végezni rádiófelderítést pl. a pillanatnyi veszélyeztetettség megállapítására, egy személy, objektum védelme érdekében, vagy általános témaorientált felderítés végrehajtása céljából. Azonban a polgári rádiófelderítés igen sokszor célirányos

[39] *AVL: Automatic Vehicle Location*

[40] *http://www.etherstack.com/eu/pdf/ES-PMRLTE-AndroidClient-EU.pdf (2015.01.15.)*

információtartalom (adott forrásból, adott személytől származó) felderítésére, és ellenőrzésére is alkalmazott eszköz a törvényes keretek között (azaz meghatározott az adatforrás). Ennek kivitelezése egy adott ismeretlen környezetben az „elektronikai helyzet" előzetes feltérképezésével (felderítési alapadatok), majd ennek ismeretében a konkrét taktikai célok pontosabb realizálásával történhet. Ezt a feladatot fogalmazhatnánk úgy is, hogy egy adott környezetben új kisugárzások detektálása adott technikai és tartalmi szempontok szerint[41], jelen esetben a digitális vagy analóg PMR eszközöknek technikai, valamint a műveleti igényeknek egyaránt megfelelő tartalmi paraméterekkel.

Eben az esetben a szűrő-kutató jellegű felderítés természetesen nem a tömeges ellenőrzés érdekében történik, hanem az adott rádiós szub-környezet feltérképezése okán (felderítési alapadatok – azaz jelen esetben ismert adók spektrumképeinek, frekvenciájának, technikai adatainak előzetes megismerése érdekében), amelyből annak ismerete után, a konkrét céltartalom (aktuális felderítési adat) könnyebben és célirányosabban, technikai megoldások és emberi közreműködés segítségével kiszűrhető. Így itt a stratégia jelzőt nem a nagy volumenű tömeges vagy totális ellenőrzés szinonimájaként értem.

A fenti metódus végrehajtására a rádió-monitoring eszközök elhelyezkedése mobilitása szempontjából a szakirodalom különféle típusokat különböztet meg:[42]

1. Stacionárius eszközök (épületben fixen telepítve),
2. Mobil eszközök (földi, légi vizi, hordozóeszközökre telepített),
3. Hordozható eszközök (amelyek egy adott ideiglenes helyszínen a telepítés után használhatóak),
4. Kézi eszközök (nyílt vagy rejtett kivitelben, az operátor szabad mozgása közbeni alkalmazásra).

A hagyományos felderítő eszközök a digitális PMR rádiók jeleinek detektálására alkalmasak, azonban a felderítési adatok (beszéd vagy adatátvitel) információjának kinyerésére önmagukban nem képesek ezen új szabványok esetében. Így ennek megoldása szükséges, akár eltérő típusú és beszédkódolású szabványok esetében, a valós idejűség szempontját is figyelem bevéve.

## 7. Összegzett következtetések

A PMR rendszerek, rádiók alkalmazása ideális megoldás a kiscsoportos ponttöbbpont kommunikációra, így a szervezett bűnözés és a terrorizmus ilyen típusú kommunikációs igényeinek megvalósítására is. A direkt módú (átjátszó nélküli),

[41] *Anatoly Rembovsky, Alexander Ashikhmin, Vladimir Kozmin, Sergey Smolskiy: Radio Monitoring, Problems, Methods, and Equipment, Springer 2009*

[42] *Rembovsky et all 2009*

de akár az egyedi pl. hordozható átjátszón keresztüli (lásd a Hytera hátizsákos átjátszóját) megoldások egyaránt kikerülhetik a hagyományos távközlési infrastruktúrákat, így ellenőrzésük kizárólag rádiófelderítéssel valósítható meg.

Ezen felül egyedi megoldásokkal a legkülönlegesebb piaci igényeket is kielégítik, az engedély nélkül alkalmazható legkisebb kategóriától, egészen a legnagyobb trönkölt rendszerekig bezárólag. A piaci felmérések szerint jelentős mértékű növekedés várható a digitális rádiók elterjedésében, amit az olcsó kínai készülékek tömeges megjelenése csak tovább fog erősíteni, főleg az általam vizsgált engedélyhez nem kötött eszközök vonatkozásában. Látható, hogy egy professzionális titkosító modul jóval többe kerül mint a legolcsóbb rádiók ára, így ebben a szegmensben nem valószínű ezek alkalmazása, de a felsőbb szegmensekben is meggondolásra készteti a döntéshozókat. Azonban a digitális átvitel miatt a hagyományos felderítő eszközökkel még ezek alkalmazása nélkül sem nyerhető vissza az átvitt beszédinformáció, ahogyan ezt egy korábbi cikkemben[43] elméleti síkon kifejtettem. Jelen cikk utolsó részében ismertetett metodika szerinti eljárással a viszonylag korlátos frekvencia tartományokban működő rádiók felderíthetőek, és akár iránymérés is végezhető rajtuk a hagyományos eszközökkel. Azonban egy olyan eszköz megalkotása, és alkalmazási feltételeinek, körülményeinek kidolgozása is szükséges, amely a fenti rendszerekből a digitális átvitelű beszéd valamint az egyéb járulékos adatátviteli (műveleti) információkat is megfelelően képes kinyerni és felderítési adatokká konvertálni. Ehhez a megfelelő technikai megoldások kidolgozása vagy adaptálása szükséges a berendezésekben, melyek egy része különálló technológiaként már rendelkezésre áll. Ezek egy készülékbe integrálásával egy komplex, adott esetben átkonfigurálható eszköz létrehozásával az ilyen rádiók és rendszerek ellenőrzése lehetővé válik.

[43] *Balog Károly: Digitális PMR rendszerek összehasonlítása I., Hadmérnök, IX. évf. 3. szám. 2014. szeptember http://www.hadmernok.hu/143_08_balogk.pdf (2014. 09. 30)*

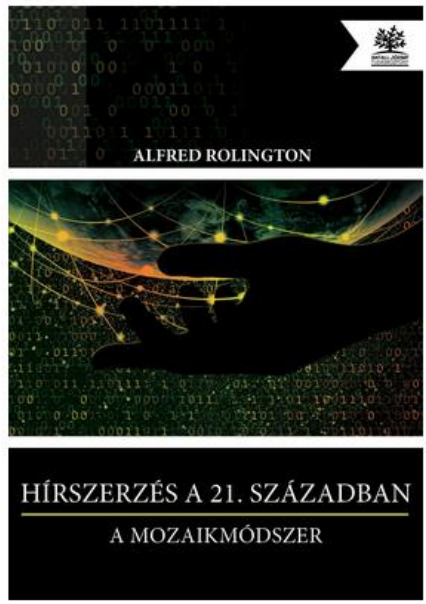
**Felhasznált szakirodalom**


- Anatoly Rembovsky, Alexander Ashikhmin, Vladimir Kozmin, Sergey Smolskiy: Radio Monitoring, Problems, Methods, and Equipment, Springer 2009
- Balog Károly: A PMR rádiózás kialakulása, fejlődése, jelentősége napjaink hírközlésében, Társadalom és Honvédelem, 2013. XVII. évf. 3.-4. szám, pp. 97-115.
- Balog Károly: Digitális PMR rendszerek összehasonlítása I., Hadmérnök, IX. évf. 3. szám. 2014. szeptember
- http://www.hadmernok.hu/143_08_balogk.pdf (2014. 09. 30).
- Grabosky, P., & Smith, R. (1999). Crime in the Digital Age: Controlling Telecommunications and Cyberspace Illegalities. The FBI Law Enforcement Bulletin, July.
- Jackson, B. A., Chalk, P., Cragin, R. K., Newsome, B., Parachini, J. V., Rosenau, W., … Temple, M. (2007), Breaching the Fortress Wall: Understanding Terrorist Efforts to Overcome Defensive Technologies. Santa Monica: RAND Corporation
- Kovács Zoltán: Felhő alapú rendszerek törvényes ellenőrzési problémái, Hadmérnök, VIII. évf. 1. szám, 2013. március, http://hadmernok.hu/2013_1_kovacsz.pdf (letöltve: 2013. 09. 25.).
- Malkin, S. (2007). Social Networks of Organized Crime: Towards a Communication Approach. Proceedings of the National Communication Association 93rd Annual Convention, November 15: Chicago.
- Dr Peter Bell - Mitchell Congram: Communication Interception Technology (CIT) and Its Use in the Fight against Transnational Organised Crime (TOC), International Journal of Science Research, 2014. Vol. 2, No. 1. http://www.macrothink.org/journal/index.php/ijssr/article/download/4089/3821. ()

# Könyvismertető
# - Alfred Rolington: Hírszerzés a 21. században, A mozaikmódszer c. könyvéről

**Dr. Dobák Imre**

Alfred Rolington – Hírszerzés a 21. században – A mozaikmódszer (Magyar kiadás. Antall József Tudásközpont 2015, Fordította: Szabó Mihály 2014, ISBN 978-963-87486-3-8, Eredeti mű: Alfred Rolington: Strategic Intelligence in the 21st Century: The Mosaic Method, Oxford University Press) című könyvéről




2013-ban jelent meg az Oxford University Press kiadásában Alfred Rolington: Strategic Intelligence in the 21st Century: The Mosaic Method című munkája, amely fordítását követően 2015-től, az Antall József Tudásközpont kiadásában már magyar nyelven is elérhető az olvasók számára. Alfred Rollington - mint a könyv bevezetőjéből is kitűnik - kiadói munkája kapcsán régóta foglalkozik a hírszerzés tevékenységét és folyamatait érintő változások, vagy akár a stratégiai elemzések kérdéskörével. Mindezen ismeretei tükröződnek vissza a hírszerzés terén új szemléletet bemutató, az ún. mozaikmódszert középpontba helyező könyvében, amelyhez a R. James Woolsey, a CIA (1993-1995 között) volt igazgatója írt előszót.

A könyv szerzője a titkosszolgálati – hírszerzési tevékenységeit jól ismerő szakértők véleményét kikérve ismerteti gondolatait a 21. századi hírszerzésről. Mindezt a múlt egyes biztonsági aspektusainak ismertetésén, a változó környezet jelentette fenyegetettség, és a jelenlegi stratégiai gondolkodás bemutatásán keresztül teszi. A bevezetőben a hírszerzés szemszögéből tekinti át jelenlegi világunkat, és világít rá a technikai fejlődés, az információs, valamint a biztonságpolitikai környezet számos összefüggésére.

A szakirodalmakban ma már gyakran említett alaptétel, hogy a hírközlés változása alapvetően átformálta a hírszerzés jelentőségét és lehetőségeit. Ennek a gondolatkörnek elméleti jellegű, modelleket felvázoló átültetésére ezidáig azonban kevés, hitelesnek tekinthető szakirodalmat találhattunk. Ebben új Rolington műve, megfogalmazva, hogy a „kommunikációs forradalom mélyen érintette a hírszerzési ciklus tradicionális elemeit" (p.13) is. Mindennek hatásai a tömeges méretekben rendelkezésre álló információk feldolgozásának, elemzésének lehetőségeiben is megmutatkoznak. Értelmezhető szakmai érvei mentén újfajta elemzési megközelítés szükségessét veti fel, amely közvetve hatással lehet a mögöttes nemzetbiztonsági, rendvédelmi, katonai szervezetek struktúrájára is, hiszen napjainkban már határokon átnyúló, mindenki számára hozzáférhető és folyamatosan változó információs folyamatokról beszélhetünk.

A. Rolington, már könyve bevezetőjében felhívja a figyelmet a tradicionális hírszerzési ciklus és tervezési modell kiváltásának szükségességére és javasolja a hírszerző szolgálatok, rendfenntartó szervek, valamint kereskedelmi szervezetek számára korszerű, az infokommunikációs környezetnek megfelelő modellek megalkotását. Mint kifejti, új struktúrákat kell kialakítani, amelyek szereplői műveleti képességeik és függetlenségük megtartása és javítása mellett mélyebben és folyamatosabban kell, hogy egymáshoz kapcsolódjanak (p.18.). Ezen gondolat mentén számos példát, rendkívül értékes, elgondolkodtató szakmai felvetést ismerhetünk meg, látva hogy a hierarchikus struktúrák átértékelése számos ország hírszerző, rendőri, és egyéb, biztonsági feladatköreit felölelő szervezetében már megkezdődtek. Példáin keresztül a „nyugati titkosszolgálati" szféra stratégiai folyamataiba kaphat rövid betekintést az olvasó, látva azok pozitív és negatív oldalait egyaránt.

Amellett, hogy bátran felveti a hírszerzés átalakuló jelenségének sajátosságait, javaslatokat, új szemléletmód kialakításának szükségességét fogalmazza meg. Munkájában kitér a főbb tradicionális hírszerzési adatgyűjtés és tervezés fajtáira, áttekinti a ciklikus, a szcenáriós és a mozaik hírszerzési módszereket, azok jelentőségét, hatékonyságát. Rendkívül értékes része a munkának, hogy a hírszerzés tág értelmezése révén a hagyományos hírszerzés mellett kitér a gadasági hírszerzés, vagy akár a hírszerzés és a rendvédelem kérdésköreire is. A technológiák okozta változások és hatásaik visszatérő gondolatként jelennek meg könyvének több fejezetében is, amelyek az olvasó számára is jól jelzik, hogy a hírszerzés

képességei (pl. adatgyűjtési eszközrendszerek) folyamatos fejlődésen mennek keresztül, előrevetítve az elemzési tevékenység szükséges módosulását is.

A mozaikmódszer lényegével a könyv utolsó részében ismerkedhet meg az olvasó, amely mint információszerzés és elemzés egysége a ma már konzervatívnak tekinthető hírszerési ciklus leértékelődését vetíti előre. Az elmúlt évtizedek biztonságpolitikai változásai mellett robbanásszerű technikai - technológiai változás ment végbe környezetünkben. Megváltozott az információk mennyisége, típusa, elérhetősége, így új és újabb hatások érték az információgyűjtés és elemzés területét is. Századunkban az új típusú fenyegetések és az életünket egyre nagyobb mértékben meghatározó modern technikai eszközök folyamatosan alakítják a biztonsági környezetünket, amelyek vonatkozásában az elektronikus formában megjelenő adatok és információk a különféle veszélyek előrejelzési lehetőségeit is magukban hordozhatják.

A szerző felveti a régi piramis típusú struktúra helyett a hálózati szervezési struktúra hatékonyságát, környezethez való „alkalmazkodási" képességét, a kollektivitás kérdését, figyelembe véve az elektronikusan egyre inkább globalizálódó környezetünkből adódó kihívásokat. A korábbi elméletek mellett a hatékonyság és eredményesség mentén, mint újfajta megközelítés a több forrásból származó információk mintegy koncentrált elemzését helyezi a középpontba, mozaikmódszerét új hírszerzési modellbe (stratégiai hírszerzés - posztmodern módszer) építve.

A könyv által felvállalt kérdésköröket tekintve a szerző arányaiban is megtalálta a szükséges egyensúlyt az egyes témakörök között, kellő terjedelmet szentelve a történeti és elméleti kérdéseknek, az új geopolitikai hírszerzési helyzet bemutatásának, és a munka egyik legfontosabb részeként megjelenő paradigmaváltást felvető részeknek. Mindezen fejezetek egymásra épülve nyitják fel a hírszerzés elvi – elméleti kérdései iránt az érdeklődők szemét. Az egyes fejezeteket olvasva számos fogalom tisztulhat le előttünk, megismerhetjük a hírszerzési modellek jelentőségét, vagy akár ráeszmélhetünk a szervezetek közötti együttműködések fokozott szükségességére is.

A könyv szakkönyv, amely magyar nyelvű fordítását a szakszavak és megfogalmazások korrekt, értelmezhető, szakmailag hiteles megjelenése tesz teljessé. A könyv összességében elgondolkodtat a hagyományosnak tekintett modellek és folyamatok átértékelésének szükségességéről, és új hírszerzési modellt felvázolva körvonalazza a stratégiai hírszerzés napjainkban egyre meghatározóbb jelentőségét. Ajánlható nemcsak szakembereknek, hanem a témakör iránt érdeklődők széles körének. Értékes, új gondolataival az oktatási célok mentén is szerepet kaphat.