



**KATONAI NEMZETBIZTONSÁGI  
SZOLGÁLAT**

---

**XV. évfolyam 4. szám      2017. december**

**SZAKMAI  
SZEMLE**

**ALAPÍTVÁ: 2003**

**BUDAPEST**

**A Katonai Nemzetbiztonsági Szolgálat  
tudományos-szakmai folyóirata**

**Felelős kiadó**

Kovács József altábornagy, főigazgató

**Szerkesztőbizottság**

Elnök:	Dr. Béres János, PhD	vezérőrnagy
Tagok:	Árpád Zoltán	ezredes
	Dr. Fürjes János Norbert, PhD	alezredes
	Dr. Kassai Károly, PhD	ezredes
	Dr. Kenedli Tamás, PhD	ezredes
	Dr. Magyar Sándor, PhD	ezredes
	dr. Sabjanics István	főhadnagy
	Szabó Károly	ezredes
	Tóth Csaba Mihály	alezredes
	Simon László	alezredes
	Dr. Vida Csaba, PhD	alezredes
Felelős szerkesztők:	Dr. Kenedli Tamás, PhD	ezredes
	Simon László	alezredes
Olvasószerkesztő:	Tóth Csaba Mihály	alezredes
Tördelő szerkesztő:	Szabó Beatrix	

**Elérhetőségeink**

Postacím:	Katonai Nemzetbiztonsági Szolgálat Tudományos Tanácsa 1111 Budapest, Bartók Béla u. 24-26. 1502 Budapest, Pf. 117
Telefon:	Dr. Kenedli Tamás 30/738-7925 Simon László 30/999-5205
E-mail:	szakmaiszemle.kontakt@gmail.com
Weblap:	<a href="http://www.knbsz.gov.hu/hu/publikaciok.html">http://www.knbsz.gov.hu/hu/publikaciok.html</a>

**HU ISSN 1785-1181**

---

## TARTALOM

---

### ***NEMZETBIZTONSÁG ELMÉLETE***

- DR. PÁL ISTVÁN  
NAGY-BRITANNIA OPERATÍV HELYZETE 1981-BEN ..... 5

### ***TECHNIKAI RENDSZEREK***

- GULYÁS ATTILA  
KIBERHADVISELÉS ÉSZAK-KOREAI MÓDRA II..... 30
- DR. KOLLÁR CSABA  
A SZERVEZETI INFORMÁCIÓBIZTONSÁGI FOLYAMATOK  
MONITOROZÁSA ÉS A VEZETŐI DÖNTÉS TÁMOGATÁSA  
KULCS TELJESÍTMÉNYMUTATÓK SEGÍTSÉGÉVEL I. .... 43
- DR. MAGYAR SÁNDOR – SIMON LÁSZLÓ  
A TERRORIZMUS ÉS INDIREKT HADVISELÉSE AZ EU  
KIBERTERÉBEN..... 57
- ZÁMBORI RICHÁRD  
MAGYARORSZÁG ÚTJA BYTE-OKKAL VAN KIKÖVEZVE . 69

### ***ALKALMAZOTT NEMZETBIZTONSÁGI-ELHÁRÍTÓ ISMERETEK***

- KOVÁCS KRISZTIÁN  
ALDRICH HAZEN AMES TÖRTÉNETE II. .... 79
- SZIJÁRTÓ LÍVIA  
MAGÁNYOS ELKÖVETŐK AZ INTERNETEN –  
AZ INTERNETES TARTALMAK PSZICHOLÓGIAI  
SZEMPONTÚ ELEMZÉSE ..... 100

### ***FÓRUM***

- DR. GYARAKI RÉKA  
A NYOMOZÓHATÓSÁG ÉS A KATASZTRÓFAVÉDELEM  
FELADATA A KIBERBŰNCSELEKMÉNYEK  
VONATKOZÁSÁBAN ..... 113

DR. LACZÓ JÓZSEF

**AZ ATHÉNI ÁLLAM A TIZENNEGYEDIK  
ALKOTMÁNYMÓDOSÍTÁS UTÁN ..... 128**

E SZÁMUNK TARTALMA..... 150

CONTENTS ..... 151

SZERZŐINK..... 160

E SZÁMUNK LEKTORAI ..... 161

A PUBLIKÁLÁS FELTÉTELEI ..... 162

DR. PÁL ISTVÁN

### NAGY-BRITANNIA OPERATÍV HELYZETE 1981-BEN<sup>1</sup>

---

#### Bevezetés

Takács Dezső rendőr alezredes – aki 1973 és 1979 között a londoni magyar nagykövetség első osztályú, műszaki-tudományos titkáráként a BM-rezidentúrát is irányította<sup>2</sup> – 1981-ben egy közel 70 oldalas dolgozatot írt a korábbi működési területéről. A munkát Károlyi Gyula alezredes dicsérő kritikában részesítette. „*Takács Dezső elvtárs nehéz feladatra vállalkozott akkor, amikor célul tűzte ki, hogy tanulmányt készít Nagy-Britannia rendőri és titkosszolgálati szerveiről. Az anyagot elolvassva az a véleményem alakult ki, hogy a feladatot jól és eredményesen megoldotta*”.<sup>3</sup> *A lektor a brit rendőri és titkosszolgálati szervek mind gyakoribbá váló médiaszereplései mögött a kormányzati megrendeléseit vélte felfedezni, amelynek célja az azt megelőző évtizedek kudarcainak feledtetése, a megtépázott tekintély helyreállítása volt. Károlyi a mű legnagyobb erényének tekintette, hogy a legfontosabb szakirodalmi művekre épült, holott a brit speciális szervekről a CIA-tól eltérően viszonylag kevés hiteles érdeklő írás került nyilvánosságra. Ezt mindenekelőtt azzal magyarázta, hogy a rendkívüli szigorú jogi szabályozás jövőtől a brit titkosszolgálatok tevékenysége évtizedeken keresztül a közvélemény előtt titokban maradt,*<sup>4</sup> például nem robbant ki a Watergate-ügyhöz hasonló botrány.

#### A titokvédelem

*Takács Dezső elengedhetetlennek látta a vonatkozó jogszabály áttekintését, mivel a brit titkosszolgálatok tevékenysége szinte kizárólag az igazságszolgáltatás jóvoltából került nyilvánosságra.*<sup>5</sup> Az első törvényjavaslatot 1889-ben a hadügyminiszter és az admirális első lordja készítette, amely meghatározta a politikai bűncselekmények körét, büntetéssel fenyegetve azokat, akik az állam érdekeit sértő titkos információkat szolgáltatnak ki illetéktelen személyeknek. Az elfogadott normaszöveg két fejezetből állt: az első a kémkedéssel, a második az államtitok védelmével foglalkozott.<sup>6</sup> *Az ezt megelőző időszak során az állami tisztviselők vagy a fegyveres erők tagjai ellen, ha információkat adtak el vagy*

---

<sup>1</sup> A Belügyminisztérium (BM) III/I. Csoportfőnökségének helyzetértékelése alapján

<sup>2</sup> Állambiztonsági Szolgálatok Történeti Levéltára (ÁBTL) – 2. 8. 2. 1 – 469 – Takács Dezső r. alez. – Minősítés. – Budapest, 1979. IV. 9. pp. 11–12.

<sup>3</sup> ÁBTL 4. 1. A – 3006/29 – Nagy-Britannia operatív helyzete. – A brit rendőri és titkosszolgálati szervek története és tevékenysége. (Tanulmány) – BELÜGYMINISZTERIUM III/1. Csoportfőnökség – 67-16-1139/81 – Budapest, 1981. IX. 23. pp. 4–5.

<sup>4</sup> Uo. p. 6.

<sup>5</sup> Uo. p. 7.

<sup>6</sup> Official Secrets Act, 1889. CHAPTER 52. pp. 269–272. – [https://www.nsa.gov/news-features/decclassified-documents/friedman-documents/assets/files/reports-research/FOLDER\\_057/41699539073887.pdf](https://www.nsa.gov/news-features/decclassified-documents/friedman-documents/assets/files/reports-research/FOLDER_057/41699539073887.pdf) (Letöltés ideje: 2017. 04. 01.)

szivárogtattak ki, és más bűncselekmény elkövetése nem volt bizonyítható, a szolgálatból történő elbocsátás volt a legsúlyosabb büntetés. Az 1889-es jogszabály alapján sok állami alkalmazottat állítottak bíróság elé, de mivel az információt átvevő személyt nem fenyegetette büntetéssel, a törvényszegést az esetek többségében nem lehetett bizonyítani. A kormány 1896-ban és 1908-ban kezdeményezte a törvény módosítását az állam tevékenységére vonatkozó adatok hatékonyabb védelmére, de a képviselők ezt elutasították, minthogy ez saját tájékozódásukat is korlátozza. Végül, 1911-ben megszületett az új Államtitok Védelmi Törvény (ÁVT), amely arra volt hivatott, hogy a titkos információk ne kerülhessenek a hírközlő szerveken keresztül a közvélemény elé, de belső konfliktus eseteire is elrettentő fegyvert adott a rendőri szerveknek és a politikai ellenzékkel szemben is fel lehetett használni. Az első világháború alatti tapasztalatok, valamint a Birodalmi Védelmi Törvény /Defence of Realm Act/ hatályon kívül helyezése után 1920-ban módosították a törvényt, majd a kémkedésre és kémkedési kísérletre vonatkozó jogszabályt 1939-ben kiegészítették a hatodik fejezet módosításával.<sup>7</sup>

Az első paragrafus a kémkedéssel foglalkozott, büntetni rendelte azt a személyt, aki átvesz vagy megszerez olyan titkos információkat, amelyek az állam érdekeit vagy biztonságát sértik. A rendelkezés a vádlottat 3-tól 7 évig tartó szabadságvesztéssel fenyegette, ugyanakkor – a tankönyv állításától eltérően – már nem kellett a szóban forgó bűncselekmény elkövetését bizonyítani, a szándék vagy a ráutaló magatartás is büntethetővé vált.<sup>8</sup> A második paragrafus szerint "bűncselekményt követett el az az állami alkalmazott, aki bármilyen rajzot, feljegyzést, tervet, iratot, dokumentumot vagy információt közöl vagy átad arra illetéktelen személynek". Továbbá "az a személy, aki e paragrafusban meghatározott módon, vagy bármilyen más formában információt vesz át". Mindkét tevékenység két évig terjedő börtönnel volt büntethető.<sup>9</sup> Az angol jogászok véleménye szerint a megfogalmazás nagyon általános volt, így kb. 2000 különböző esetre lehetett alkalmazni, miközben az általános jelleg viszont megkönnyítette a rendelkezés kijátszását is. 1970-ben a nigériai brit főkormányzónak a polgárháborúról szóló bizalmas jelentése megjelent a Sunday Telegraph című londoni lapban. A bírósági eljárás nem tudta bizonyítani bűncselekmény elkövetését, így az eljárás Jonathan Aitken újságíró és társai felmentésével végződött.<sup>10</sup> A tanulmány szerint az elhárításnak ugyanilyen komoly presztízsveszteséget okozott az ún. Owen-ügy.<sup>11</sup> Az MI5 először a Labour Party (a brit Munkáspárt) centrumához tartozó David Owen-re gyanakodott,<sup>12</sup> majd Harold Wilson miniszterelnök utasításának megfelelően szoros ellenőrzés alá vonta Will Owen képviselőt, akit hosszas megfigyelést követően, 1970 januárjában a rendőrség letartóztatott. Az MI5

<sup>7</sup> ÁBTL 1981. i.m. pp. 7–8.

<sup>8</sup> Official Secrets Act, 1911. CHAPTER 28/1. p. 3. – [http://www.legislation.gov.uk/ukpga/1911/28/pdfs/ukpga\\_19110028\\_en.pdf](http://www.legislation.gov.uk/ukpga/1911/28/pdfs/ukpga_19110028_en.pdf) –Letöltés ideje: 2017. 04. 01.)

<sup>9</sup> Official Secrets Act (1911.) i.m. CH. 28/2. p. 4.

<sup>10</sup> THOMAS, Rosemund: The British Official Secrets Acts, 1911–1939, In: CHAPMAN, Richard A.–HUNT, Michael (ed.): Open government. A study of the prospects of open government within the limitations of the British political system. Routledge, 1989, London. p. 99.

<sup>11</sup> ÁBTL 1981. i.m. p. 9.

<sup>12</sup> ZEIGLER, Philip: Wilson. The Authorised Life of Lord Wilson of Rievaulx. Weidenfeld & Nicolson, London, 1993. pp. 313–314.

Csehszlovákia javára történő kémkedéssel vádolta a politikust, aki a vizsgálat első részében elismerte, hogy 2300 font jutalomban részesült a Statne Bezpecnost (Állambiztonság, rövidítése: StB) munkatársaitól.<sup>13</sup> A vád végső soron nem azért bukott el, mert Owen ügyvédei tanácsára visszavonta vallomását,<sup>14</sup> hanem azért, mert Jozef Frolik, az egykori csehszlovák hírszerzőtisz, aki vállalta a bíróság előtti vallomástételt, nem találkozott olyan titkos dokumentummal, amely Owen révén jutott az StB birtokába.<sup>15</sup>

A harmadik paragrafus meghatározta a "tiltott hely" fogalmát. E kategóriába bármi beletartozhatott, ha azt az arra illetékes szerv annak minősítette. A törvénycikk értelmében nem csak az a tevékenység számított bűncselekménynek, ami a tiltott helyek ellen irányult, hanem a minősített épületekről szóló információk birtoklását is, ha azok az ellenségnek hasznosak lehetnek.<sup>16</sup> A negyedik paragrafusban büntetéssel fenyegettek mindenkit, aki a törvény bármely paragrafusában meghatározott bűncselekmény elkövetésére bujtott fel, rá ugyanolyan súlyos büntetés volt kiszabható, mint az elkövetőre. Az ötödik és a hatodik paragrafus a bűncselekmények minősítésével foglalkozott: meghatározta a büntett, a főbenjáró büntett /a legsúlyosabb vád/ a vétség fogalmát és alkalmazási körét. A kísérletet ugyanúgy büntetni rendelte, mintha azt elkövették volna. A hetedik paragrafus büntetni rendelte azt, aki olyan személynek ad szállást, aki a törvényben meghatározott bűncselekményt követett el, vagy arra előkészületet tett.<sup>17</sup> Az 1967-es büntető törvény bűnpártolásra vonatkozó paragrafusai szerint az államtitok törvény minősített megsértésében való bűnrészesség maximum tíz év elzárással büntethető. Amennyiben a bűnpártolás elkövetője egy olyan bűncselekményhez nyújt segítséget vagy annak a nyomozását akadályozza, amelyet a törvénykönyv öt évesnél rövidebb börtönbüntetéssel fenyeget, a tettest legfeljebb három évre ítélik.<sup>18</sup> A nyolcadik paragrafus szerint a törvény bármely pontjának alkalmazásához a főállamügyész jóváhagyása volt szükséges. A kilencedik fejezet a házkutatással és letartóztatással kapcsolatos eljárást szabályozta, miszerint az ügyben illetékes bíró, ügyész vagy rendőrfőkapitány jogosult a parancs kiadására, aminek értelmében bármelyik rendőr házkutatást tarthat alapos gyanú esetén, és a minősítéshez nem kell bizonyítékot produkálnia.<sup>19</sup> Az 1920-as törvénymódosítás az első paragrafus értelmében büntetni rendelte azt a személyt, akik színleléssel – egyenruha, hamis igazolvány, stb. felhasználásával – tiltott helyre behatol, egyben büntetni rendelte azt is, aki az ehhez szükséges eszközöket biztosította.<sup>20</sup> A második paragrafus kiegészítése pontosította, hogy mit jelent a külföldi hatalom ügynökével fenntartott kapcsolatot,<sup>21</sup> míg az az ötödik paragrafus elrendelte, hogy a gyanús postai

<sup>13</sup> PINCHER, Chapman: *The Truth About Dirty Tricks from Harold Wilson to Margaret Thatcher*. Sidgwick & Jackson, London, 1991. p. 109–110.

<sup>14</sup> ÁBTL 1981. i.m. p. 10.

<sup>15</sup> ANDREW, Christopher: *The Defence of the Realm*, pp. 541–543.

<sup>16</sup> Official Secrets Act (1911.) i.m. CH. 28/3. pp. 4–5.

<sup>17</sup> Uo. CH. 28/4-7. p. 5.

<sup>18</sup> Criminal Law Act 1967 CHAPTER 58/4. pp. 2–3. –

[http://www.legislation.gov.uk/ukpga/1967/58/pdfs/ukpga\\_19670058\\_en.pdf](http://www.legislation.gov.uk/ukpga/1967/58/pdfs/ukpga_19670058_en.pdf) (Letöltés ideje: 2017. 04. 01.)

<sup>19</sup> Official Secrets Act (1911.) i.m. CH. 28/8-9. pp. 6–7. –

<sup>20</sup> Official Secrets Act, 1920. CHAPTER 75/1. pp. 1–2. –

[http://www.legislation.gov.uk/ukpga/1920/75/pdfs/ukpga\\_19200075\\_en.pdf](http://www.legislation.gov.uk/ukpga/1920/75/pdfs/ukpga_19200075_en.pdf) –(Letöltés ideje: 2017. 04. 01.)

<sup>21</sup> Official Secrets Act (1920.) i.m. CH.75/2. pp. 2–3.

küldeményeket a rendőrség tudomására kell hozni, miközben, aki az utóbbi kategóriába sorolható táviratok, levelek, csomagok eljuttatásában segédkezik, kötelezően bekerül a nyilvántartásba.<sup>22</sup> A hatodik paragrafus ugyanakkor előírta a feljelentési kötelezettséget.<sup>23</sup> Az 1939-es módosítás értelmében büntetendő cselekménnyé vált az államtitkok védelmi törvény esetleges megsértésével kapcsolatos feljelentés elmulasztása és a hatóságok által megkövetelt tájékoztatás elmulasztása. Ezzel egy időben a jogszabály hatálya Észak-Írországra is kiterjedt.<sup>24</sup> *A szerző úgy vélte, hogy a törvény a kormány és a hatalmi szervek vitatható ügyeinek takargatásán túl az elit magánéleti botlásai – pl. John Profumo Minister of Supply (a védelmi utánpótlásért felelős miniszter) ügyében<sup>25</sup> – egyfajta menekülési útvonalként szolgált.<sup>26</sup> A joggyakorlatba bekerült az ún. "Korona Kiváltság" (Royal Prerogative), amely lehetőséget ad a kormánynak bármilyen szintű bíróság birtokában lévő bizonyítékok visszavonására. Akkor alkalmazzák, ha a nyílt tárgyalás az állam érdekeit sértené, például a feltárt bizonyítékok az ország védelmével állnak kapcsolatban, vagy megzavarhatják az ország diplomáciai kapcsolatait. Erről is a főállamügyész dönt, aki a mindenkori miniszterelnök kinevezése alapján a kormány tagjának számít, azaz voltaképp a kormányfő álláspontját képviseli.<sup>27</sup> A törvény alapján az állami alkalmazottaktól teljes titoktartást követeltek egy írásos nyilatkozat formájában, amit az önként távozó vagy nyugállományba vonuló személyekkel is aláíratnak. Ezen túl több olyan rendelkezés is érvényben volt, amely további kötelezettségeket rótt a köztisztviselőkre. A rendelkezések szerint állami hivatalnok – minisztériumok, a Home Office (Belügyminisztérium) és a Ministry of Defence (Védelmi Minisztérium, angol rövidítése: MoD) – alkalmazottai csak hivatali vagy szolgálati érdekből utazhattak a szocialista országokba, ráadásul kötelező volt feletteseiknek jelentést tenni arról, ha utóbbiak diplomataival és más állami beosztású állampolgáraival kapcsolatba kerültek.<sup>28</sup>*

### **Military Intelligence 5 (MI5)**

*Nagy-Britanniában és Észak-Írországból a külső és belső operatív elhárítás és a kémelhárítás funkcióját a mai napig az MI5 végzi. Az angol szakirodalom, az írók és újságírók az idők folyamán újabb nevekké ruházták fel a Szolgálatot; "Defence Intelligence", "Security Service", "Secret Service", amely nevekké a mindennapi gyakorlatban többször lehet találkozni, mint a Szolgálat eredeti nevével. Az MI5 – pontosabban az Admiralty (Admiralitás) és a War Office (a Hadsereg Főparancsnoksága, angol rövidítése: WO) közös felügyeletével a hírszerző*

---

<sup>22</sup> Uo. CH 75/5. pp. 4–5.

<sup>23</sup> Uo. CH 75/6. p. 5.

<sup>24</sup> Official Secrets Act, 1939. CHAPTER 121/1-2. pp. 1–2. – [http://www.legislation.gov.uk/ukpga/1939/121/pdfs/ukpga\\_19390121\\_en.pdf](http://www.legislation.gov.uk/ukpga/1939/121/pdfs/ukpga_19390121_en.pdf) – (Letöltés ideje: 2017. 04. 01.)

<sup>25</sup> The National Archives (TNA) BS 28 – 84 (Records of Defunct Temporary Bodies). Lord Denning's Inquiry into the Profumo Affair: typed copy of report. June 21, 1963. 8–138.

<sup>26</sup> ÁBTL 1981. i.m. pp. 10–11.

<sup>27</sup> Uo. pp. 11–13.

<sup>28</sup> TNA Cabinet Office (CAB) 129/109/1 – Report on the Committee on Security in the Public Service (The Radcliffe Committee). – 16th March 1962. 23–25.



műveletek céljából megalapított Secret Service Bureau (Titkosszolgálati Iroda)<sup>29</sup> – 1909-ben jött létre, ahol az elhárítási részleg vezetésére Vernon Kell százados kapott megbízatást.<sup>30</sup> A War Office alá tartozó Directorate of Military Operations (Védelmi Műveleti Igazgatóság, angol rövidítése: DMO) 1903-tól már működött egy kis létszámú elhárítási csoport, amely kezdetben az MO3, majd 1907-től az MO5 jelzést kapta.<sup>31</sup> 1911-ben ugyanakkor megszületett a mai napig létező, ún. Információk Ellenőrzésével Foglalkozó Bizottság /D–notice Committee/, amely a War Office, az Admiralty és a sajtó képviselőiből áll, és az államtitkok kiszivárogtatásának megakadályozását tekinti fő feladatának. Az újságírók számára kötelező az egyes értesülések publikálhatóságával kapcsolatban a bizottsághoz kell fordulniuk felvilágosításért, aki nem tartja magára nézve kötelezőnek az ellenőrzést vagy a hivatalos álláspontot, büntetőjogilag felelősségre vonják.<sup>32</sup> *A speciális szervek tevékenységének koordinálására az első világháború befejezését követően a védelmi minisztériumban létrehozták a "Katonai Hírszerzés (helyesebben Felderítés) Igazgatóságát". /Directorate of Military Intelligence/. Ez olyan testület megalkotására irányult, amely összhangot teremt a brit speciális szervek tevékenységében, viszont az igazgatóság csak a MoD felhatalmazását élvezte, így "képtelen volt" az MI5 és a Special Branch (a Londoni Rendőrség Különleges Ügyosztálya) tevékenységét koordinálni és a közöttük lévő hatásköri problémákat megoldani. Az 1921-es kormányrendelet megszüntette a Special Branch hatásköri túllépését, ugyanakkor a bizalmas politikai nyomozások lefolytatása kizárólagos jelleggel az MI5-hoz került, amely mindenekelőtt az 1921 óta létező Brit Kommunista Párt, az ipari sztrájkmozgalmak, és a különböző rendszerkritikus politikai mozgalmak és szervezetek operatív ellenőrzésére irányult. A szolgálat ennek érdekében a beszerzéseket preferálta, de ahol ez a módszer valamilyen okból nem volt lehetséges, oda fizetett ügynökséget telepített, amely a szerző értelmezésében az SZT (Szigorúan Titkos) tiszti állományt jelentette. A konspirációhoz kiképzést nem nagyon kaptak; saját leleményességükre támaszkodva kellett helyt állniuk.*<sup>33</sup> Takács alezredes kétséggel helyesen érzékelt, hogy az MI5 komoly informális kapcsolatrendszer alakított ki a sajtó vezetői és képviselői felé, mindenekelőtt a konzervatív újságok jóvoltából iránymutatásaival, negatív kampánnyal segítse elő a baloldalt, a sztrájkmozgalmak lejáratását vagy dezorganizációját. Az irányított sajtópropaganda a szakszervezeti vezetőket vagy éppen a baloldali pártok vezetőit gyakran nevezte a „társadalom megrontóinak, külföldi ügynököknek, vörösöknek”. A Heath-kormány idején is volt rá precedens, hogy az elhúzódoó bányászsztrájk idején a "Red under the bed" (vörösök az ágy alatt) volt a szlogen.<sup>34</sup> *Az MI5 időnként külső missziókra is vállalkozott: 1918-ban az orosz fehérgárdistákat segítette, 1936-ban a spanyol polgárháború alatt ügynököket küldött a nemzetközi brigádokba, hogy kutassák fel a brit baloldali szervezetek tagjait. Tevékenysége kvázi kiterjedt az egész világra, ám ettől függetlenül a Nagy-Britannia háborúba lépése után a német speciális szervek több csapást mértek a*

<sup>29</sup> TNA – War Office (WO) 106/6292/ RC 1245049. Organization of Secret Service. April 28, 1909. 1–9.

<sup>30</sup> ÁBTL 1981. i.m. pp. 14–15.

<sup>31</sup> ANDREW i.m. pp. 4–26.

<sup>32</sup> TNA CAB 129/109/1 – Report on the Committee on Security in the Public Service (The Radcliffe Committee). – 16th March 1962. pp. 34–42.

<sup>33</sup> ÁBTL 1981. i.m. pp. 15–16.

<sup>34</sup> DORRIL, Stephen – RAMSAY, Robin: Smear! Wilson and the Secret State. Grafton, London, 1992. pp. 229–233.

*Szolgálatra, az irattárát is felgyújtották. Az MI5 később eredményesebben vette fel a harcot a német hírszerzéssel szemben. Már a háború előtt különös figyelmet fordítottak a különböző országok rejtjelezett adásainak vételére és megfejtésére, ennek területén komoly eredményeket tulajdoníthattak maguknak. Az első jelentős siker "Ultra Secret" elnevezésű akció volt, amelynek során a brit kódfejtők feltörték a német hadvezetés rádió továbbított, szigorúan titkos utasításait, lehetővé téve a preventív intézkedéseket. Egy másik, kevésbé propagált tevékenységük a német ügynökök visszafordításának titkosszolgálati módszere volt. A "Double – Cross System" (kettősügynök játszma) lényege, hogy a leleplezett hálózatokat az MI5 ellenőrzésével tovább működtették, folyamatosan dezinformációs híranyagokat juttattak a német hadvezetéshez.<sup>35</sup> A tanulmány itt sok tekintetben pontosításra szorul. Az ún. Directorate of Intelligence 1919 tavaszától a brit Belügyminisztérium (Home Office, angol rövidítéssel: HO) közvetlen alárendeltségében működött, míg a Különleges Ügyosztály 1921 ősztől visszakerült a Criminal Investigation Department (Bűnügyi Nyomozó Osztály, angol rövidítése: CID) kötelékébe. Sir Basil Thomson főkapitány-helyettes 1925. évi nyugdíjba vonulásával a hírszerzési igazgatóság megszűnt.<sup>36</sup> A Ministry of Defence ugyanakkor a ma ismert formájában csak 1964 óta létezik.<sup>37</sup> Az MI5 valójában 1931-ben lett a birodalom legfontosabb elhárító szerve,<sup>38</sup> miután a Special Branch hírnevét alaposan megtépázta, hogy 1927-28-ban Charles Jane őrmester és Hubertus van Ginhoven felügyelő politikai szimpátiából bizalmas információkat szivárogtatott ki az 1919-es rendőrsztrájk egyik szószólójaként a testülettől elbocsátott Walter Dale nevű ex-rendőrnek. A volt nyomozó szoros kapcsolatban állt a William Ewer által irányított szovjet kémhálózattal, akiknek mindenekelőtt az MI5 megfigyelői azonosításában segédkezett.<sup>39</sup> Az SZT-tiszt kifejezés az MI5 viszonylatában nem értelmezhető, hiszen az állomány összes tagjának személyazonossága a mai napig minősített információnak számít, a szerző itt minden bizonnyal a korai évek legmegbízhatóbb hálózati embereire – pl. Charles Maxwell Knight – célozott.<sup>40</sup> A brit elhárítás nem küldött ügynököket Spanyolországba, viszont nyilvántartást vezetett a harcok résztvevőiről, megakadályozta a felvételüket a brit hadseregbe.<sup>41</sup> Az Abwehr (a német hírszerzés) kódjait először az MI5-hoz tartozó Radio Security Service (Rádióbiztonsági Szolgálat, angol rövidítése: RSS) törte fel, ám a szóban forgó egység 1941 májusában átkerült a Government Code & Cypher School (Kormányzati Kód-és Rejtjelfejtő Iskola, angol rövidítése: GC&CS keretébe.<sup>42</sup> Az MI5 irattára viszont az angliai csata idején a Luftwaffe bombatalálata folytán égett le, nem arról volt szó, hogy a német hírszerzés felgyújtotta.<sup>43</sup>*

<sup>35</sup> ÁBTL 1981. i.m. pp. 16–17.

<sup>36</sup> WILSON, Ray –ADAMS, Ian: Special Branch. A History: 1883–2006. Biteback Publishing, Ltd. London, 2015. pp. 97–105.

<sup>37</sup> DYLAN, Hugh: Defence Intelligence and the Cold War. Britain's Joint Intelligence Bureau 1945–1964. Oxford University Press, 2014, Oxford. pp. 199–200.

<sup>38</sup> WALTON, Calder: Empire of Secrets. British Intelligence, the Cold War and the Twilight of Empire. Harper Press, London, 2013. pp. 23–24.

<sup>39</sup> TNA KV2/1398 (Security Service) Charles JANE. Personal File 39319/V1. 41–42a

<sup>40</sup> THOMAS, Gordon: A brit titkosszolgálatok világa. J LX Kiadó, Budapest, 2008. pp. 107–110.

<sup>41</sup> BECKETT, Francis: Enemy Within. The Rise and Fall of the British Communist Party. John Murray Ltd. London, 1995. pp. 78–81.

<sup>42</sup> HODGES, Alan: Kódjátzsma. Alan Turing élete. Gabo Kiadó, Budapest, 2015. pp. 398–400.

<sup>43</sup> ANDREW i.m. pp. 230–231.

*Az MI5 feladatai közé tartozott 1) a brit államtitkok megszerzésére irányuló törekvések megghiúsítása. 2) az állam és az államhatalmi szervek zavartalan működésének biztosítása. 3) a politikai nyomozás funkciója. 4) a kémügyekben folytatott nyomozások irányítása. 5) a Londonban lévő diplomáciai testület, mindenekelőtt a Szovjetunió és a szocialista országok követségeinek, valamint a brit kommunista párt és a baloldali mozgalmak ellenőrzése. 6) a volt gyarmati országokban a brit befolyás megőrzése. 7) az ipari, kutatóintézeti, egyetemi és főiskolai elhárítás.*<sup>44</sup>Sir Maxwell-Fyfe konzervatív belügyminiszter 1952-ben kelt bizalmas utasítása az igazgató feladatait a következőképp határozta meg: „Ön, mint a biztonsági szolgálat igazgatója személyesen a belügyminiszternek tartozik felelősséggel. A biztonsági szolgálat azonban nem része a Belügyminisztériumnak. Alkalmanként Önnek joga van közvetlen a miniszterelnökhöz fordulni. A biztonsági szolgálat az ország védelmi erejének része. Feladata; az egész birodalom védelme a külső és a belső veszély ellen, amely bármilyen kísérlet lehet – kémkedés, szabotázs, személyek, vagy szervezetek tevékenysége – amelyet az országból, vagy külföldről irányítanak, és úgy ítéli meg, hogy az állam érdekeit sértő cselekmény. Különös figyelmet szenteljen annak, hogy a biztonsági szolgálat tevékenysége szigorúan a szükséges feladatai ellátására korlátozódjon. Fontos, hogy a biztonsági szolgálat mentes legyen bármilyen jellegű politikai elfogultságtól vagy befolyástól és semmit ne tegyen, ami bármely vonatkozásban azt a látszatot kelti, hogy nem a birodalom érdekeit szolgálja. Tevékenységük a társadalom egyes csoportjai vagy más érdekei ellen nem irányulhat. Vizsgálatot egyetlen államhivatal megbízásából se hajtson végre, hacsak meg nem győződött arról, hogy fontos közérdek forog kockán, ami a birodalom védelmét érinti és a 2. pontban megfogalmazást nyert. Ön és beosztottjai tartsák fenn azt a jól bevált szokást, miszerint a minisztereket és az illetékeseket csak a rájuk tartozó eseményekről tájékoztatják és részletes információkat nem szolgáltatnak ki”.<sup>45</sup>A belügyminiszter ugyan kijelentette, hogy a Szolgálat neki tartozik felelősséggel, csak hogy az MI5 tevékenységét érintő parlamenti interpellációkat mindig a kormányfőhöz, és soha nem hozzá intézik. Az igazgató minden joggal fel van ruházva az operatív tevékenység végzését illetően, teljesen önállóan dönthetett ennek irányairól, miközben a politikai elfogultságtól mentes működést nem mindig sikerült realizálni.<sup>46</sup> *A II. világháború után jelentős átszervezésekre került sor, amely az állomány tekintélyes részének leszerelésével és három igazgatóság megalakításával járt együtt, amelyek alá csoportfőnökségek, osztályok és referatúrák tartoztak. 1./ A Központi Operatív Igazgatóság a Szolgálat operatív munkájának irányításáért és elemzéséért, a belső koordinációért, a számítógépes nyilvántartásért és az információk célba juttatásáért viselte a felelősséget. 2./ A Területi Igazgatóság egységéhez tartozott a fedőszervekben és a legális objektumokban dolgozó operatív állomány. (A fedőszerv alatt az elhárító tevékenység álcázására létrehozott vállalkozások, irodák, a legális objektumok alatt az ellenséges hírszerzők behatolása által fenyegetett összes létesítmény, operatív állomány alatt az ezekbe delegált elhárító tiszti állomány értendő). /"K" ellenőrzés – értsd környezettanulmányozás – figyelés, British Council, stb./ 3./ A Tudományos és Technikai Igazgatóság, élén a főigazgatóval, amely a kémelhárító, a védelmi, a bomlasztó tevékenység elleni, a tudományos, technikai és kiegészítő szolgálati,*

<sup>44</sup> ÁBTL 1981. i.m. pp. 18-20

<sup>45</sup> TNA BS 28/84 Lord Denning's Inquiry into the Profumo Affair: typed copy of report. June, 21, 1963. pp. 143-145.

<sup>46</sup> LEIGH, David: The Wilson Plot. How the Spycatchers and Their American Allies Tried to Overthrow the British Government. Pantheon Books, New York, 1988.

valamint az adminisztratív csoportfőnökségeket foglalta magában. Ebből az első négy osztályokra, az osztályok pedig referatúrákra bomlottak. A Központi Operatív Igazgatóság az MI5 tényleges központja, ahová a kartotékrendszer is tartozik. A nyilvántartó, ahol közel 4 millió emberről tároltak valamilyen szintű információt, őrzi és dolgozza fel a csoportfőnökségekről érkező dossziékat. Ez azonban nem csupán a saját igényeket elégítette ki, hanem szükség esetén a rendőrség speciális osztályainak, a külügyminisztériumnak is a segítségére van. A Központi Igazgatóság munkatársai – többségében újságírók, szociológusok – az operatív úton megszerzett információk értékelését végzik, belső vagy külső felhasználásra. Az első körhöz sorolt anyagok az illetékes igazgatósághoz kerülnek, az utóbbiakkal rendszerint a kormányt vagy a minisztereket tájékoztatják.<sup>47</sup> A szerző a szervezeti egységek angol elnevezésével adós maradt, ugyanis az MI5 a 80-as évek elején nem igazgatóságokból, hanem hat ügyosztályból tevődött össze. Az 'A' Branch volt az Operatív Szolgálat, ide tartoztak a technikusok, a lehallgató személyzet, a gépiró és fordító egység, A4-es jelzéssel figyelőcsoport, és a kísérleti laboratórium. A 'B' Branch volt a személyzeti és belbiztonsági, őrzővédő és pénzügyi részleg, a 'C' Branch a Preventív Biztonsági Ügyosztály, amely a kormányzati szervek titokvédelmével, a pályázók átvilágításával és az állami beszállítók biztonsági intézkedései ellenőrzésével, valamint a szabotázs akciók és terrorcselekmények elleni védekezéssel foglalkozott. Az 'F' Branch (Felforgató Tevékenység Elleni Szolgálat) a Brit Kommunisták Párt elleni vizsgálatokért, a szakszervezetek, a parlamenti képviselők és az egyetemek ellenőrzéséért, a nemzetközi és az északír terrorizmus elhárításáért, illetve az egyéb szélsőbal-és jobboldali szervezetekben működő ügynökhálózat tartásáért volt felelős. A 'K' Branch végezte a kémelhárítási feladatokat, miközben az 'S' Branch (Támogató Szolgálat) üzemeltette az MI5 számítástechnikai részlegét és a nyilvántartást, de a kiképzés és a hivatalos utak szervezése is hozzájuk tartozott.<sup>48</sup> A személyzet utánpótlása először valóban főleg a gyarmati hadsereg és rendfenntartó erők tisztjeiből, főleg az indiai testület egykori tagjaiból érkezett, amit az 1945 utáni változásokkal összhangban – egyrészt a brit rendőrség speciális osztályairól<sup>49</sup> – másrészt az állami intézmények alkalmazottaiból, jogászokból, szociológusokból, pszichológusokból, újságírókból egészítették ki.<sup>50</sup> Az állományba vételi eljárás rendkívül szigorú volt, sokáig csak annak volt esélye, akinek szülei és hozzátartozói is született angolok. Ezen kívül az elvárások között szerepelt legalább két komoly befolyással rendelkező ajánló, aki szavatolhatta a jelölt minden irányú megbízhatóságát.<sup>51</sup> Noha kétségtelen tény, hogy a második világháború utáni időszakban még sokszor a szolgálat tisztjeinek szűkebb vagy tágabb ismeretségi körébe tartozó emberek közül meghívásos alapon gondoskodtak az utánpótlásról, a 80-as években már eltekintettek tőle.<sup>52</sup> A második világháború utáni korszak változásai ugyanakkor alapvetően befolyásolták az MI5 feladatait és tevékenységét. A szocialista tömb létrejöttével a kémelhárítás területén a hangsúly a Szovjetunióra és szövetségeseire helyeződött át, ugyanakkor a gyarmatbirodalom

<sup>47</sup> ÁBTL 1981. i.m. pp. 20-21.

<sup>48</sup> DORRIL, Stephen: The Silent Conspiracy. Inside the Intelligence Services in the 1990's. Heinemann, London, 1993. pp. 475-477.

<sup>49</sup> MACINTYRE, Ben: Kém a csapatban. Kim Philby és a nagy árulás. Gabo Kiadó, Budapest, 2015. pp. 176-189.

<sup>50</sup> RIMINGTON, Stella: Nyílt titok. Az MI5 – a brit kémelhárítás – volt főigazgatójának emlékiratai. Geopen Könyvkiadó, Budapest, 2004. pp. 123-125.

<sup>51</sup> ÁBTL 1981. i.m. pp. 22-23.

<sup>52</sup> THOMAS, 2008. pp. 90-92.

szétesése következtében a tengerentúli feladatkör jelentéktelenné vált. A hidegháború idején három terület változásait volt érdemes kiemelni: a követségi elhárító munka fokozását, a KP és a baloldali szervezetek elleni intézkedéseket, továbbá a brit tudományos és technikai vívmányok védelmére az egyetemeken és kutatóintézeteknél bevezetett operatív elhárítást.<sup>53</sup> Amikor az 50-es években a keletnyugati kapcsolatok igen alacsony szintre zuhantak, brit részről több korlátozó intézkedés született. A Szovjetunió diplomáciai testületének tagjai csak a Foreign Office engedélyével léphettek túl London 30 km-es körzetét,<sup>54</sup> de ugyancsak a brit kormányzathoz fűződött az a diplomáciatörténetben egyedülálló intézkedés, amikor 1971. szeptember 24-én 105 szovjet állampolgárt, köztük 43 diplomatát kiutasítottak a szigetországból.<sup>55</sup> Az MI5 kémelhárítási osztálya eleve a szocialista országok Londonban lévő követségei – egyéb képviseleti szervei ellenőrzésére koncentrálna erőit, ugyanakkor tevékenységének intenzitása mindig szinkronban volt a nemzetközi és a szigetország belpolitikai helyzetével. Amikor az Egyesült Államokban a jobboldali irányzatoknak vagy épp a brit kormányköröknek fűződött érdeke a szocialista országokkal fennálló viszony lazításához vagy megromlásához, az MI5 intézkedéseket hajtott végre a cél érdekében. Az ilyen módszerekhez tartozott a külszolgálatosok aktívabb ellenőrzése és zaklatása, tiltakozó akciók és provokációk szervezése, ellenséges sajtókampány indítása. A kényes évfordulók vagy jeles politikai események alkalmával az emigránsok által szervezett tiltakozás, nagyobb szabású felvonulás általában a Szolgálat kezdeményezésével vagy támogatásával zajlott. A csendes tiltakozás, amely egy konkrét esemény vagy intézkedés ellen szólt, hasonlóképpen ment végbe. Ilyenkor néhány, az MI5 vagy az emigráns szervezetek által fizetett munkanélküli táblákkal vonult fel a követségek előtt, főleg a publicitás végett. A Magyar Népköztársaság (MNK) londoni nagykövetségénél 1970 és 80 között egyszer került sor ilyen csendes tiltakozásra. Ez alkalommal néhány táblát hordozó személy és egy parlamenti képviselő tiltakozott egy magyar állampolgár jogainak megsértése ellen. A Londonban élő feleség felkérésére egy olyan személy érdekében léptek fel, aki kétszer kísérelt meg tiltott határátlépést. Az illető elsőre még felfüggesztett büntetést kapott, ám miután másodszor is elkapták, azt le kellett töltenie. A zaklatás azt jelentette, hogy az MI5 olyan személyeket küldött a nagykövetségre panasszal, bejelentéssel, ajánlkozással, akik provokátorok, degeneráltak, gyengeelméjűek voltak, bár esetenként jó legendával "komoly ajánlattevő" megjelenése is előfordult, aki rendszerint elutasításra talált. Az emigráció vagy az elhárítás időnként fel-felbujtott néhány vállalkozó szellemű egyént, akik az ablakok betörésével vagy rombolással igyekeztek kárt tenni a külképviseleti intézményekben.<sup>56</sup> 1957. október 23-án a forradalom egy éves évfordulója alkalmából az Angliába menekült résztvevők egy csoportja valóban közáport zúdított a magyar követség ablakaira,<sup>57</sup> ám ezt követően már nem fordult elő ilyen esemény. Mindazonáltal, nem zárhatjuk ki, hogy a sokkal vérmesebb

<sup>53</sup> ÁBTL 1981. i.m. pp. 23-24.

<sup>54</sup> DEACON, Richard: 'C'. The Biography of Sir Maurice Oldfield. Head of MI6. Futura Publications Ltd, London, 1985. p. 235.

<sup>55</sup> Magyar Országos Levéltár (MOL) – XIX – J – 1 – j – KÜM – Nagy – Britannia 1971 – 20-as doboz (d.) – 002892/1 – Tárgy: Szovjet – brit viszony alakulása. /105 szovjet állampolgár kiutasítása Nagy - Britanniából/ - London, 1971. X. 8. pp. 1-5.

<sup>56</sup> ÁBTL 1981. i.m. pp. 24–28.

<sup>57</sup> MNL OL – XIX – J – 1 – j – Nagy – Britannia 1945 – 1964 – 5-ös d. – 14.) tétel – 005165 – 367/szig. titk./ - Tárgy: Tiltakozás a konzulátus ablakainak betörése ellen. – London, 1957. X. 24. pp. 1-2.

lengyel és ukrán emigráció már sokkal többször folyamodott hasonló fellépéshez, amelyben az is komoly szerepet játszott, hogy utóbbiak sorsát a mindenkori brit kormányzat mindig is hangsúlyosabban a szívében viselte.<sup>58</sup> Az MI5 a nyugalom megzavarására általában olyan módszereket alkalmazott, mint nyílt demonstratív figyelés, a kiküldöttek és hozzátartozóik megfélemlítése, zavaró éjjeli telefonhívások, lakásbetörések, lopással és károkozással, vagy csak figyelemelterelés érdekében, a szolgálati vagy személyi használatú gépkocsik megrongálása, ellopása, szándékos összetörése, vagy áruházi "lopáson" való tettenérés. Az idegileg kiegyensúlyozatlan, labilis személyiségekre ez negatívan hatott, egy magyar diplomatát hat hónap elteltével haza kellett rendelni. A külképviselet tagjainak tanulmányozására, a zavaró tevékenység megtervezésére és a hatások lemérésére az operatív technikán kívül az MI5 az ügynökséget is használta.<sup>59</sup> A katonai társszerv tapasztalatai azt mutatták, hogy a 70-es évek közepén a magyar diplomatákat nem követte rendszeresen az A4-es csoport, de a szemközti épületből a nagykövetség folyamatos megfigyelés alatt állt.<sup>60</sup>

A brit Kommunista Párt gyengítésére, bomlasztására, zaklatására, tagjainak felderítésére és megfélemlítésére a korábban alkalmazott nyílt és operatív műveleteket a hidegháború kezdetétől adminisztratív intézkedésekkel egészítették ki. 1948-ban Attlee amerikai nyomásra elrendelte, hogy az MI5 igazgatója adatokat gyűjtsön az állami alkalmazásban lévő kommunista párttagokról és szimpatizánsokról, majd az ellenőrzés eredményeképp a kormány úgy döntött, hogy Nagy-Britannia azon állampolgárai, akik baloldali pártnak vagy szervezetnek a tagjai vagy ilyenek tevékenységét támogatják, eszméikkel nyíltan szimpatizálnak, köztintézményekben nem alkalmazhatók. Burgess és Maclean szökését követően, 1956-ban az MI5 újabb szigorítások bevezetését javasolta a kormánynak, végül az ez alapján született rendelkezés nem csak a KP tagjait és szimpatizánsokat, hanem a potenciális társutasokat is kizárta az állami alkalmazás lehetőségéből, ugyanakkor az alkoholizmus, a kábítószer fogyasztás vagy a homoszexualitás is a kizáró okok között szerepelt.<sup>61</sup> Az elfogadott akcióterv nyomán az operatív, bizalmas ellenőrzés nemcsak az egyszerű állampolgárokra, hanem az újságírók, iparmágnások, szakszervezeti vezetők, tudósok, sőt a parlamenti képviselők esetén is érvényesült. A parlament minden egyes először megválasztott tagjáról dossziét állítottak fel azzal a céllal, hogy megakadályozzák a szocialista országok állambiztonsági szerveinek e kategória irányában kifejtett tevékenységét. A képviselők operatív ellenőrzéséről szóló híreket 1971-ben az állambiztonsági jogszabályok felülvizsgálatával foglalkozó Franks Committee is megerősítette. Harold Wilson korábbi Labour miniszterelnök elismerte az operatív ellenőrzésre vonatkozó állításokat, amikor egy képviselő kérdésére adott válaszában kijelentette: „amikor hatalomra kerültünk, természetesen észrevettem, hogy milyen tevékenység folyik a parlament képviselői ellen. Úgy éreztem, a megelőző kormány arra irányuló gyakorlatával szakítani kell, amely a képviselők telefonjai lehallgatását megengedte”. Edward Heath, az akkori konzervatív kormányfő viszont azzal reagált, hogy „nem látom semmi okát annak, hogy a parlament képviselőit mentesíteni kellene a biztonsági ellenőrzés alól”. Az

<sup>58</sup> DORRIL, Stephen: Inside the Covert World of Her Majesty's Secret Intelligence Service. The Free Press, London, 2000. pp. 185–210.

<sup>59</sup> ÁBTL 1981. i.m. pp. 24–28.

<sup>60</sup> MOZSIK Imre: Washingtoni emberünk. Hírszerző voltam Amerikában. MÁS Könyvek, Budapest, 1995. pp. 170–172.

<sup>61</sup> TNA CAB 129/109/1 – 16th March 1962. pp. 13–22.

utóbbi megnyilvánulásokból is kitetszik, hogy az MI5 az államhatalmi és államigazgatási szervekkel kapcsolatos operatív tevékenységét a mindenkori miniszterelnökkel egyeztetni és az említett körökben annak elvi felhatalmazása alapján alkalmazza az operatív eszközöket.<sup>62</sup> A Munkáspárt vezetése az 50-es évek végén 15 parlamenti képviselőjét gyanúsította a kommunista pártban viselt titkos tagsággal, majd a vizsgálat végén a pártközpont sajtóosztályának vezetőjét – Arthur Bax – elbocsátották, mert anyagi ellenszolgáltatásért bizalmas információkat szolgáltatott a szovjet, a román, a bolgár, a csehszlovák – és a magyar<sup>63</sup> – hírszerzésének.<sup>64</sup>

*A második világháború után az MI5 szemében a brit tudományos és technikai vívmányok megóvása, valamint az egyetemek és kutatóintézetek viszonylatában az objektumvédelem vált prioritássá. Tevékenységének fő irányához tartozott az egyetemek és főiskolák tanári karának operatív elhárítása, az intézményekben előforduló szervezkedések, mozgalmak vezetőinek, és tagjainak felderítése és kontrollja, a saját és más speciális szervek káderutánpótlásának biztosítása, a külföldi diákok ellenőrzése, és a köztük végzett tippkutatás, valamint a tanári karban és a hallgatók körében végzett beszervezés. Az MI5 megjelenése az oktatási és kulturális vonalon a diákok és a tanárok között egyaránt vegyes érzelmet váltott ki. A testületek és a hallgatók "zaklatása", a gyakori dekonspirációk sajtó általi publikálása 1957-ben az Egyetemi Tanárok Egyesületének tiltakozásához vezetett. Az egyesület országos gyűlést hívott össze, amelynek egyetlen napirendi pontja volt: a tanári testület milyen álláspontot foglaljon el az MI5 egyetemi tevékenysége ügyében s milyen információkat szolgáltatasson ki a részére. A hosszú és heves vita során a többség elítélte az MI5 működését és az oktatási munkával összeegyeztethetetlennek nyilvánította a hallgatókra vonatkozó adatok kiszolgáltatását. A kiutat British Council (BC) fedőszerveként történő fokozottabb felhasználása jelentette, amely 1934-es megalakulása óta az MI5 és SIS egyik legfontosabb fedőszerveként működött a maga 5000 alkalmazottjával, és 7-8, egyenként 5-10 főből álló területi irodájával, ahol a helyi vezető mindig a Szolgálat embere. A részlegek a szervezőmunkán túl foglalkoztak a külföldi hallgatók és kutatók elhelyezésével, amely tanulmányozásukra és feldolgozásukra is lehetőséget nyújtott. A BC jól összehangolta legális feladatai végzését az operatív célokkal: több ország viszonylatában kiépített hálózati rendszerük volt, amely a konzultáns tanártól a lakóhely tulajdonosig szinte állandóan ellenőrzés alatt tudja tartani a kiválasztott személyeket. Az intézmények vezetői, ha nem is lelkesen, de fegyelmezetten eleget tettek tájékoztatási kötelezettségüknek, amely jóvoltából az együttműködés egyébként rendkívül szorossá vált. Ez látszott például a londoni magyar nagykövetség műszaki-tudományos attaséjának a sheffield-i egyetemen tett látogatásán, ahol a BC körzeti irodájának vezetője is részt vett a meglátogatott tanszék programjában. A tanszékvezető emiatt elnézést kért az attasétól, és megjegyezte: "sajnos, köteles vagyok a külföldiek látogatásáról tájékoztatni a BC körzeti irodáját és ez esetben ragaszkodtak a programban való részvételhez."<sup>65</sup> Takács Dezső a*

<sup>62</sup> ÁBTL 1981. i.m. pp. 28-30.

<sup>63</sup> Állambiztonsági Szolgálatok Történelmi Levéltára (ÁBTL) – 3. 2. 4 – K – 286/1 – "James"(Arthur Bax). – Évkör: 1955–1960. p. 176

<sup>64</sup> ANDREW i.m. pp. 412–415.

<sup>65</sup> ÁBTL 1981. i.m. pp. 30-32. . Az 1934-ben a brit kultúra terjesztésére és a szélsőséges eszmék befolyásának leküzdésére alapították a British Council-t. In DONALDSON, Frances: The British Council: the first fifty years. Jonathan Cape, London, 1934. pp. 5–244.

kutatóintézetekben nem találkozott zaklatással, az egyetemeken tett látogatásai alkalmával azonban a British Council szinte minden esetben figyelemmel kísérte tevékenységét. A valóságban nem a sheffield-i, hanem Nottinghami Egyetemen történt, hogy a British Council körzeti vezetője kezdettől fogva jelen volt a londoni magyar nagykövetség műszaki-tudományos attaséjának programjában.<sup>66</sup> A BC fedése alatt a külföldre utazó brit egyetemi oktatók felkészítést kaphattak a sötétben – az együttműködő partner direkt megközelítése nélkül – folytatott hírszerzésre, adatgyűjtésre vagy kapcsolatépítésre. A BC révén az MI5 beleszólást nyert a meghívásokba, a vendéglőadók kiválasztásába, címek adományozásába vagy a brit tudományos élet különböző társaságainak a tagok kiválasztását illető politikájába. A hallgatók informatori munkára történő bevonása egyéni és csoportos módszerrel történt. Az egyéni tanulmányozás alapján előkészített gyors és fokozatos bevonás mellett gyakran alkalmazták a direkt módszert, amikor 15-20 szelektált hallgatót meghívnak a hadügyminisztérium nevében egy hivatalos beszélgetésre. Ösztöndíj és állásajánlat mellett közlik, hogy rendszeres információkat kell adni néhány társuk politikai tevékenységéről, megnyilvánulásairól és időnként mindenre kiterjedő jelentést kell készíteni a Szolgálat különleges érdeklődése alapján. Az MI5 azért is tulajdonított nagy jelentőséget az operatív ellenőrző munkának, mivel ez lehetőséget adott a korabeli szóhasználat szerint a fellazításra.<sup>67</sup> Nagy-Britannia állami szektorában az egyes objektumok saját biztonsági szolgálattal rendelkeznek, amelyek az MI5 irányításával dolgoznak. Az állami megrendelések teljesítésébe bevont magáncégek /számuk kb. 4-5 ezer/ ellenőrzése a következő formában zajlott. Miután az illetékes minisztérium megkötötte a szerződését a céggel, az MI5 megkapja ennek titkos anyagait és a biztonságra vonatkozó utasítást. A cég védelmi szolgálatának munkatársait speciális tanfolyamokon készítik fel és az MI5 saját forrásaival elvégzi az alkalmazottak ellenőrzését, míg az utóbbi állományában lévő biztonsági tanácsadók megszervezik a vállalatok felügyeletét a biztonságot érintő hibák és mulasztások felderítésére. A szerződések megtiltják, hogy a titkos munkába külföldieket vagy olyan személyeket vonjanak be, akiknek a megbízhatóságában a Szolgálat kételkedik. A biztonsági előírások figyelmen kívül hagyása esetén automatikusan indítványozzák a szerződés felbontását.<sup>68</sup>

### **Secret Intelligence Service (SIS) (Military Intelligence 6)**

*Takács Dezső a brit hírszerzőszolgálat megalakulását 1911-re datálta, amely hivatalosan a Katonai Hírszerző Szolgálat 6. osztályaként /MI6/ jött létre, de a valóságban fegyveres erőktől függetlenül működött, így kapta a "Secret Intelligence Service" (Titkos Hírszerzőszolgálat) elnevezést. A korábbi években a Foreign Office (Külgügyminisztérium), a Gyarmatügyi és Kereskedelmi Minisztérium, valamint a Colonial Office és az India Office végzett titkos információgyűjtést, ám az első hivatalos hírszerző szerv az 1871-ben alakult "Intelligence Branch of the War Office" (a Hadsereg Felderítő Ágazata) volt, amelynek fő feladatát a birodalom katonai védelmével kapcsolatos információk gyűjtése képezte. A katonai hírszerzés a különböző fegyvernemek fejlődésével szakosodott: 1877-ben megalakították a*

<sup>66</sup> MNL OL – XIX – J – 1 – j – Anglia 1975 – 32 –es d. – I – 19 – 004343 – Tárgy: Takács Dezső műszaki – tudományos beosztott beszámoló jelentése. – London, 1975. VII. 4. pp. 1-7.

<sup>67</sup> ÁBTL 1981. i.m. pp. 33-35.

<sup>68</sup> TNA CAB 129/109/1 – 16th March 1962. pp. 28–34.



tengerészeti, 1920-ban a légierő felderítési szolgálatát.<sup>69</sup> Az MI6 a Secret Service Bureau feladatkörének elhatárolása révén, 1910 májusában jött létre az 1923-ig regnáló Sir Mansfield Cumming vezetésével,<sup>70</sup> míg a szárazföldi hadsereg felderítő szolgálata 1873-ban, a Naval Intelligence Department 1887-ben kezdte el önálló működését.<sup>71</sup> A légierő 1918-ban lett önálló fegyverem, azonban saját hírszerző részlegének születéséről nincs megbízható adat, csak annyi bizonyos, hogy 1945-ben már önállóan működött.<sup>72</sup> A szerzőnek abban igaza volt, hogy a különböző szolgálatok és hivatalok koordináció nélkül működtek, a Committee for Imperial Defence (Birodalmi Védelmi Bizottság) nevű tanácsadó testület azonban a Takács Dezső által jelzett időpontnál később, 1904-ben jött létre, hogy a mindenkori miniszterelnök vezetésével rendszeresen meghatározza a hírszerzés legfontosabb feladatainak irányát és összhangot próbált teremteni az ad hoc tevékenységet folytató szolgálatok és irodák között.<sup>73</sup> 1936-tól a hírszerzési koordináció feladatait az e célból létrejött Joint Intelligence Committee (Egyesített Hírszerzési Bizottság) vonta magához.<sup>74</sup> *Az MI6 legfontosabb feladatait a kormány, a kormányhivatalok és minisztériumok számára politikai, gazdasági és katonai titkos információk külképviseltek és ügynökség segítségével történő gyűjtésében, a Nagy-Britannia ellen irányuló kémtevékenységről és titkos akciókról szóló értesülések megszerzésében, valamint Nagy-Britannia érdekeinek titkos eszközök általi védelmezésében határozták meg.*<sup>75</sup> Az 1931-ben elfogadott "három mérföldes szabály" értelmében az SIS csak külföldön tevékenykedhetett,<sup>76</sup> igazgatója csak a mindenkori miniszterelnöknek volt felelős, ugyanakkor az eltérő érdekeiből adódó konfliktusok elkerülése vagy mérséklése végett a brit külügyminisztériumon belül létrehozták a hírszerzési államtitkárságot. Az MI6 tevékenysége kezdetben a Foreign Office önálló szolgálati ágaként működő konzuli hivatalra épült,<sup>77</sup> de a második világháborút követően a diplomáciai fedés lett általános. Igaz, sokszor előfordult, hogy a brit hírszerzés tisztjei egyes nemzetközi vállalatok, bankok vagy kereskedőházak külföldi kirendeltségein töltötték be vezető tisztséget,<sup>78</sup> vagy újságíróként mutatkoztak a nyilvánosság előtt.<sup>79</sup>

A SIS felépítése. A tanulmány szerint 1981-ben a brit hírszerzés négy igazgatóságából, a központi operatív apparátusa négy földrajzi elv alapján működő hivatalból állt. Az 1. sz. igazgatóság a hírszerző és támadólagos elhárító hivatalokat, a 2. sz. igazgatóság a személyügyi, pénzügyi és ellátásügyi hivatalt, a 3. sz.

<sup>69</sup> ÁBTL 1981. i.m. p. 36.

<sup>70</sup> JEFFREY, Keith: MI6. The History of the Secret Intelligence Service. Bloomsbury, London, 2011. pp. 8–22.

<sup>71</sup> HERMAN, Michael: Intelligence power in peace and war. Cambridge University Press, Cambridge, 1996. pp. 16–17.

<sup>72</sup> DYLAN i.m. p. 55.

<sup>73</sup> BUTLER, David – SLOMAN, Anne: British Political Facts 1900–1979. Macmillan Press Ltd. London, 1980. pp. 430–431.

<sup>74</sup> WEST, Nigel: Secret War for the Falklands. The SAS, MI6, and the War Whitehall Nearly Lost. Sphere, London, 2010. pp. 26–27.

<sup>75</sup> ÁBTL 1981. i.m. p. 37.

<sup>76</sup> SMITH, Michael: MI6. The Real James Bonds 1909–1939. Dialogue, London, 2011. 336.

<sup>77</sup> WEST, Nigel: MI6. British Secret Intelligence Operations 1909–45. Panther Books, London, 1985. pp. 56–85.

<sup>78</sup> DORRIL (2000) i.m. pp. 146–148.

<sup>79</sup> CAVENDISH, Anthony: Inside Intelligence. The Revelations of an MI6 Officer. Harper Collins Publishers, London, 1997. pp. 83–117.

igazgatóság az információkat elemző értékeléseket, terveket, prognózisokat készítő, hírszerzést koordináló és a minisztériumokat tájékoztató hivatali foglalta magában, míg a 4. sz. igazgatóság a nyilvántartó hivatal, kiképzési egység, a belső biztonsági osztály és a kutatóintézetek keretként működött.

A központi 1. sz. igazgatóság felépítése Takács ismeretei alapján a következő volt. A D1 hivatal: hírszerző munkát végzett az európai kapitalista országokban, valamint ezek területéről a szocialista országok ellen. A D2 hivatal a közel és középkeleti országokban tevékenykedett, valamint ezek területéről a szocialista országok ellen. A D3 hivatal a Távól-Keleten és Latin-Amerikában volt illetékes, míg a D4 hivatal a Szovjetunió és szocialista országok ellen dolgozott. Az utóbbit a szerző tíz szekcióra osztotta. Az 1. sz. szekció irányítja és szervezi a hírszerző munkát a Szovjetunió, Bulgária, Lengyelország, Csehszlovákia, Magyarország és az NDK ellen. A felsorolt országokban Anglia területéről hírszerző akciókat hajtott végre. A 2-5. sz. szekció szervezte és vezette a Szovjetunió és a szocialista országok elleni harmadik országos hírszerző munkát. A 6. sz. szekció a nemzetközi enyhülés jóvoltából kialakult állami és magánkapcsolatok átfogásán és az ebben rejlő lehetőségek kiaknázásán dolgozott. A 7. sz. szekció a turizmus, a kereskedelmi, tudományos és kulturális utazások és cserék felhasználásával végzett hírszerző, tippkutató és tanulmányozó munkát. A 8. sz. szekció a Szovjetunió és a szocialista országok Nagy-Britanniában tanuló, kutató gyakornokai és aspiránsai között végzett tippkutatást. A 9-10. sz. szekció a hírszerzés és a kémelhárítás periférikus egységeivel tartotta a kapcsolatot. A Szolgáltatón belül további önálló igazgatóságot képez a Rádiófelderítő és Rejtjelfejtő Szolgálat /RRSz/. Az RRSz rádiólehallgatással, táviratok megfejtésével, az ez után szerzett információk elemzésével és feldolgozásával foglalkozik. Telepíthető rádiófelderítő állomásokkal rendelkeznek, amit a világ különböző részein használnak fel és működtetnek. A Rádiófelderítő és Rejtjelfejtő Szolgáltatónak három egysége van. Az 1. sz. egység a gazdasági, kereskedelmi, stb. jellegű táviratok és telexek vételével, megfejtésével és értékelésével, a 2. sz. egység a diplomáciai testületek táviratainak és küldeményeinek vételével, megfejtésével és elemzésével, a 3. sz. egység az ügynöki rádióadások felderítésével, lehallgatásával és megfejtésével foglalkozik.<sup>80</sup> A tényleges felosztás 1978-tól a következő volt: "Directorate of Personnel and Administration" (Személyzeti és Ügyviteli Igazgatóság), "Directorate of Support Services" (Támogatási Igazgatóság), "Directorate of Counterintelligence and Security" (Kémelhárítási és Biztonsági Igazgatóság), "Directorate of Production and Requirements" (Hírszerzési és Elemzési Igazgatóság). Az utóbbi tevékenysége hét, földrajzi terület szerint behatárolt hatáskörű ellenőr alá tartozott – Európa, Szovjet Blokk, Afrika, Közel-Kelet, Távól-Kelet, nyugati félteke – ugyanakkor a legfontosabb szerepet a P1 és P20 közé eső, regionálisan illetékes egységek közül a P4 és a P5 (az európai szocialista országok és a Szovjetunió) játszotta a legfontosabb szerepet.<sup>81</sup> A Rádiófigyelő és Rejtjelfejtő Szolgálat "Government Code and Cypher School" néven már 1922-ben önállósult,<sup>82</sup> 1947-től Government Communications Headquarters lett a hivatalos elnevezés. A szervezet négy igazgatóságból – SIGINT Plans (tervezési), SIGINT Operations and Requirements (műveleti és elemzési), Organization and Establishment (szervezeti és létesítmény fenntartási), valamint

<sup>80</sup> ÁBTL 1981. i.m. pp. 38-43.

<sup>81</sup> DAVIES, Philip, H. J: MI6 and the Machinery of Spying. Frank Cass, London, 2004. pp. 283–289.

<sup>82</sup> HODGES (2015.) i.m. pp. 233–238.

Communications Security (hírközlés-biztonsági) – állt.<sup>83</sup> *Az MI6 központi létszámát a húszas években 20-30 főre becsülték. Az állomány, amelyek nagy része az indai rendőrségtől, valamint különböző katonai alakulatoktól került a SIS kötelékébe – mint pl. Felix Cowgill vagy Valentine Vivian<sup>84</sup> – jogilag szabályozatlan körülmények között dolgozott /pl. nem volt katonai rendfokozat, nyugdíjrendszer, stb./.* *A felvételnél nem volt egységes a követelmény, így a testület sokáig a heterogenitás képét mutatta, ugyanakkor az előrehaladás bizonytalanságai és a nem túl magas fizetés miatt a kvalifikáltabb emberek számára nem tűnt vonzóknak a hírszerzés.<sup>85</sup>* *A második világháborút követően egy bizottság felülvizsgálta az MI6 működését, majd javaslatot tett az átszervezésre. 1946-ban, a békeidőszakra történő átállással egy időben személyi felülvizsgálat történt, így az állomány egy tekintélyes hányada – sokszor kényszerből – leszerelt.<sup>86</sup>* *1964-ben Kim Philby szökése után a belső elhárítás és védelmi részlegből önálló igazgatóság alakult.<sup>87</sup>* *A brit speciális szervek különös jellemzője a maximális konspiráció megvalósítása, ahol a rögeszméig fokozott titoktartásban az SIS járt az élen. Az egykori tisztek egyöntetűen állították, hogy a megszállottságig terjedő titoktartás már bénítóan hatott a SIS operatív tevékenységére. Itt jelennek meg a legkorábban a "Titkos", "Bizalmas", stb. feliratok, amelyek mindenütt ott voltak, s ennek állandóan érvényt is szereztek. Az operatív állomány csak a saját elszigetelt adatait ismerhette, így náluk valósult meg a legtökéletesebben a modern hírszerzés azon elve, hogy a hírszerzők és ügynökök ne ismerjék egymást. A konspiráció sokszor elfedte az eredménytelenséget, vagy legalábbis olyan látszatot formált, mintha a brit hírszerzés körül minden rendben lett volna. Az MI6 a beszervezési jelölteket – feltűnő gondossággal – szakképzettségétől, érdeklődésétől függően valamely brit intézményhez kapcsolta, ahol megszervezte a tanulmányozást, majd eldöntötte, hogy milyen motivációkkal segítheti elő az együttműködést. A jelöltek kutatásában előnyt élveznek azok, akik vezető pozícióban vannak. A tanulmányozás hosszadalmas és sokoldalú, főleg fedőszerveken keresztül zajlik, de minden más lehetőséget felhasználnak. Általános a törekvés, hogy a célszemélyt függő helyzetbe hozzák, például utazásokkal, meghívásokkal, ajándékokkal, címek adományozásával, tiszteletbeli taggá választásokkal, majd a függőségi viszonyba hozott jelöltet érdekeltté teszik a kapcsolat rendszeressé tételében és a kölcsönös bizalom elmélyítésében. Ekkor szorgalmazzák az elsődleges információszerzést. A Szolgálat a hírszerzők kiválasztására és kiképzésére mindig nagy gondot fordított. A jelölteket erkölcsi, értelmi, megbízhatósági és testi (fizikai) tekintetben vizsgálták. A kiválasztottak a London melletti Devonshire-i kémiskolában kapták a kiképzést. Az első két évben általános oktatás folyt hadtudományok, állambiztonsági ismeretek, történelem, kémia, fizika és nagy súllyal testnevelés. A harmadik évben az operatív ismeretek begyakorlása, a titkosírás, rejtjelezés, fotózás megismerése szerepelt a tananyagban, de mindhárom évben intenzív nyelvoktatás zajlott. A felkészítés sokoldalúságára jellemző, hogy többféle sportot /ökölvívás, cselgáncs/ társasági viselkedést, /táncot, kártyavetést/ is tanítottak. A szolgálat ügynökei általában külföldiek, akik eltérő motiváció alapján – elvi meggyőződéstől vagy anyagi juttatások – működnek együtt*

<sup>83</sup> RICHELSON, Jeffrey –BALL, Desmond: *The Ties That Bind, Intelligence Cooperation between the UKUSA Countries – the United Kingdom, the United States of America, Canada, Australia and New Zealand. Boston, 1985. pp. 19–22.*

<sup>84</sup> MACINTYRE i.m. pp. 34–49.

<sup>85</sup> ÁBTL 1981. i.m. pp. 44–45.

<sup>86</sup> DORRIL (2000) i.m. pp. 29–30.

<sup>87</sup> DAVIES i.m. pp. 266–267.

a britekkel. Az eredményesebb ügynököket az MI6 a fizetési listáján szerepelteti, mivel véleményük szerint a pénz rendszeres elfogadása növeli a munkára való hajlandóságot. A csak eszmei alapon dolgozó személyek viszont sokszor túlságosan önállóak, amely kereszttezheti az MI6 elképzeléseit. A kizárólag pénz ellenében dolgozó ügynökök, viszont ha választás elé kerülnek, hajlamosak csupán saját érdekeiket nézni, és őszinteségük is vitatható. A SIS jellemzően nem a hozott anyag értéke szerint fizette ügynökeit, hanem a társadalmi, politikai, gazdasági életben betöltött szerepüknek megfelelően jutalmazott. Az összeköttetésben, főként a harmadik világ országaiban, még mindig a nagykövetségi rezidentúra játszotta a főszerepet, de gyakran tartották a találkozót harmadik országban, összekötő ügynökök és beutazók felhasználásával. A célországi vagy harmadik helyszíni találkozókra és az akciókra rendszerint munkaszüneti napokon került sor, utóbbiak előkészítésénél és végrehajtásánál a túlzott óvatosság a jellemző. Az információforgalmazás titkosírással postai úton, vagy tárgyi postaládával történik, de mindez erősen függ az adott országban lévő elhárítás erejétől és aktivitásától. A harmadik világ országaiban a SIS nem kizárólag London politikai és gazdasági befolyásának fenntartásáért, hanem a nyugati világ általános érdekeinek érvényesítéséért is tevékenykedett, ám ez utóbbi szerepében már nem mindenhol tudott helytállni. A volt gyarmati országokban sokszor megosztotta érdekszféráját az Egyesült Államok hírszerzésével, ahol végső soron a CIA teljes egészében átvette a korábban az MI6 által vitt ügyet. A nyugatbarát kormányoknak nyújtott titkos támogatással lehetővé tette a belső ellenséggel történő leszámolást, míg más esetben az ellenzéki pártok vagy csoportok erőszakkal megdönthették a törvényes kormányt.<sup>88</sup> Az MI6 politikai gyilkosságokat, szabotázs-és terrorakciókat is szervezett a nyugtalanság és bizonytalanság fenntartására, ugyanakkor támogatta a felforgató propagandát az egyes országok, pártok, vallási irányzatok közötti ellentétek kiélezésére.<sup>89</sup> A brit hírszerzést már a második világháború óta erős szálak fűzik az Egyesült Államokhoz. A SIS 1940-ben tette meg az első lépést az amerikai speciális szolgálatokkal való együttműködés kiépítése felé, amikor Churchill barátja, William Stephenson kanadai milliomos vezetésével New York-ban megkezdte tevékenységét a "British Security Coordination" (Brit Biztonsági Koordinációs Iroda). A BSC eredetileg az USA-ból Angliába irányuló katonai utánpótlást védelmezte a német diverzánsoktól, viszont az FBI kemény intézkedései megakadályozták, hogy az Abwehr jelentős sikereket tudjon elérni. Stephenson ekkor egy brit mintájú hírszerző szolgálat létrehozására kezdte el rávenni Roosevelt elnököt, amihez az MI6 felajánlotta a segítségét.<sup>90</sup> Az MI6 várokozásán felül jelentős szakmai segítséget nyújtott az Amerikából érkező hírszerzők felkészítéséhez, miközben a tanítványokra gyakorolt befolyásuknak szinte semmi sem szabott határt.<sup>91</sup> Az ismeretekre való kiképzésen túl az amerikaiak bepillantást nyerhettek a SIS operatív ügyeibe és tanulmányozhatták a második világháború idején megfejtett táviratokat. A hidegháború alatt a különböző országokban lévő

<sup>88</sup> ÁBTL 1981. i.m. pp. 45–48. A London melletti Devonshire-i kémiskola valójában Gosport, Fort Monkton-ban volt. In: RICHELSON i.m. p. 16.; A CIA például Iránban vette át MI6 által folytatott műveletet a II. világháborúban. In PRADOS, John: Presidents' Secret Wars. CIA and Pentagon Covert Operations Since World War II. William Morrow and Company Inc. New York, 1986. pp. 91–98.

<sup>89</sup> DORRIL (2000) i.m. pp. 600–652.

<sup>90</sup> DAVIES i.m. pp. 131–134.

<sup>91</sup> WEINER, Tim: A CIA története. Hamvába holt örökség. Gabo Kiadó, Budapest, 2015. pp. 19–24.

küldképviselleteknél is szoros együttműködés valósult meg a brit és az amerikai hírszerzés között. Az MI6 és a brit katonai felderítés ugyancsak rendkívül szerves kapcsolatokat tart fenn az összes NATO tagállam és egy sor másik ország hírszerzésével. Havonta elkészíti és a NATO tagok különleges szolgálatainak átadja a világ helyzetéről szóló általános elemzését, de az észak-atlanti szervezeten belül egyeztetette a többiekkel a Szovjetunió és a szocialista országok ellen irányuló tevékenység irányait és módszereit.<sup>92</sup>

### **Belügyminisztérium**

A Home Office fő feladata a rendőri erők, különös tekintettel a Scotland Yard és a Special Branch irányítása és felügyelete.<sup>93</sup> *A brit Belügyminisztérium vezető testülete a minisztertől eltekintve állandó, a politikusnak öt helyettese van. Ez utóbbiak olyan területekért felelősek, mint a pénzügyi és gazdasági kérdések; az utánpótlás - az eljárások törvényessége - bűnügyi felderítés - panasziroda; út-és közlekedésrendészet; közrend és közbiztonság - felforgató tevékenység megelőzése - tűzrendészet - a rendőrség és a színes bőrűek kapcsolata; anyagi és ruházati ellátás – kiképzés - rendkívüli események koordinálása, a háború esetére szóló mozgósítási tervek; számítógépes egységek - irattárak felügyelete; tudományos-technikai fejlesztések koordinálása. A Home Office négy kutatóintézetet tartott fenn a rendőri munka hatékonyságának javítása érdekében.*<sup>94</sup> A Police Scientific Development Branch (Rendőrségi Tudományos Fejlesztések Csoportja) a saját szakértői és az egyetemi-kutatóintézeti szférából felkért külsős tanácsadók segítségével olyan technikai eljárásokon és műszaki megoldásokon dolgozott, amelyek hozzájárultak a rendfenntartás hatékonyabbá tételéhez, az ujjlenyomatok megőrzésétől a golyóálló mellények fejlesztéséig.<sup>95</sup> A Police Research Services Branch (a Rendőrség Kutatószolgálati Csoportja) a rendfenntartó erők fejlesztési igényeinek felmérését, valamint a kutatók által megtervezett eljárások utólagos értékelését végezte.<sup>96</sup> A Forensic Science Laboratories (Törvényszéki Tudományos Laboratóriumok) – helyesen Forensic Science Service (Törvényszéki Tudományos Szolgálat) csak az 1990-es évek elején lett országos szintű, önálló kormány szerv, amit 2005-től vállalkozói alapon próbált versenyezni a megbízások megszerzéséért. A fejlesztések elmaradása és az alulfinanszírozottság következtében a modell nem vált be, ezért David Cameron akkori miniszterelnök 2010-ben a megszüntetés mellett döntött. A feladatait egyrészt az egyes rendőri erők keretében tevékenykedő laboratóriumok, másrészt a magánszféra vette át.<sup>97</sup> A Directorate of Telecommunications (a Távközlési Igazgatóság) a Home Office, a rendőri erők, a tűzoltóság és az egyéb

---

<sup>92</sup> ÁBTL 1981. i.m. pp. 49–51.

<sup>93</sup> COWLEY, Richard: A History of British Police. From its Earliest Beginnings to the Present Day. Stroud, 2011. pp.147–151.

<sup>94</sup> ÁBTL 1981. i.m. pp. 52-53.

<sup>95</sup> PEPPER, Ian K: Crime Scene Investigation. Methods and Procedures. Open University Press, Maidenhead, 2010. p. 186.

<sup>96</sup> RAWLINGS, Philip: Policing: A Short History. Willan Publishing, Cullompton, 2012. p. 206.

<sup>97</sup> HOUSE OF COMMONS SCIENCE AND TECHNOLOGY COMMITTEE: The Forensic Science Service. Seventh Report Session 2010-12. The Stationary Office Limited, London, 2011. pp. 3–111.

szervezetek közötti rádió-és vezetékes telefonösszeköttetésért, a híradórendszerek üzemeltetéséért volt felelős.<sup>98</sup>

### A Scotland Yard

A II. világháború után a rendőri alakulatokat érintő centralizáció és az összevonások nyomán 1975-ben a Londoni Városi Rendőrséget és a Metropolitan Police szervezetét is beleértve Angliában és Walesben 43 rendőri egység működött.<sup>99</sup> *A 41 fővároson kívüli rendfenntartó erő létszáma 85022 főt tett ki, míg a két londoni rendőrség állományában 21ezren teljesítettek szolgálatot. A megjelölt időszak folyamán Skóciában 8 rendőri egység végezte a rendfenntartást 15373 fős létszámmal. A Scotland Yard szervezeti felépítése nagy vonalakban megegyezett a más országokban szokásos gyakorlattal: a kerületi és területi rendőrőrszobák a rendőrkapitányságokhoz tartoznak, ahol az adminisztrációt, a közlekedésrendészetet, a rádiós személyzetet, a Különleges Ügyosztályt (Special Branch), a bűnügyi nyomozó osztályt és a szabálysértési csoportot helyezték el. Az osztályokat főfelügyelők, a csoportokat felügyelők vezetik. A Metropolitan Police Victoria Street-i központjában – Scotland Yard székház<sup>100</sup> – a legfelső emeleten működött a Special Branch, a brit politikai rendőrség.<sup>101</sup> A 80-as évek első felében London 24 kerületre volt osztva, amihez 189, különböző létszámmal működő őrszoba tartozott. Az egyes kerületek beosztottait a vállukon hordott betűből, és személyazonosságukat a betű alatt elhelyezett számokból lehet azonosítani. Az őrszobák A-tól Z-ig az ABC betűivel vannak jelölve,<sup>102</sup> ennek megfelelően a kerületi betűjelzés ismeretében azonnal megállapítható, hogy az intézkedő rendőr hol teljesít szolgálatot. Az A-tól Z-ig használt válljelzéseken túl az alábbi megkülönböztetéseket alkalmazzák: CO – Commissioner’s Office /Ellenőrzési hivatal/, SC – Special Constables /Különleges rendőri szolgálat/, TD – Traffic Division /Közlekedésrendészet/, AD – Airport Division /Repülőtéri rendészet/. A Scotland Yard technikai fejlődésében jelentős állomás volt, hogy 1964-ben indult a ”Police National Computer Unit” /PNCU/ (Országos Rendőrségi Komputer Központ), amely 3, 5 millió személy anyagát dolgozta fel, vagyis minden 14. állampolgárról rendelkezett valamilyen aktával.<sup>103</sup> A számítógépközpontban a vezetői engedély és gépkocsi nyilvántartó játszotta a legfontosabb szerepet, ugyanakkor a központi adattár az ellopott járművekről és egyéb értékekről, eltűnt és körözés alatt álló személyekről, elítéltekről is naprakészen tudott tájékoztatni.<sup>104</sup> *A szerző ezzel párhuzamosan arra is rámutatott, hogy a bűnözés jellegének változása újabb, különleges feladatokra szakosított egységeket hívtak életre.<sup>105</sup> A ”Flying Squad” (Akcio Osztály) rajtaütésszerű razziákat és operatív akciókat hajt végre,**

<sup>98</sup> WILLIAMS, Chris A: Police Control Systems in Britain, 1775–1975. Manchester University Press, Manchester, 2014. pp. 161–166.

<sup>99</sup> BUTLER–SLOMAN i.m. p. 292.

<sup>100</sup> CATER, Frank – TULLET, Tom: The Sharp End. One Man’s Life with the Flying Squad – From the Krays to Brinks Mat. Grafton Books, London, 1990. pp. 25–26.

<sup>101</sup> ÁBTL 1981. i.m. pp. 53-54.

<sup>102</sup> TNA Metropolitan Police (MEPO) 4/268 – METROPOLITAN POLICE LIST February 1966. pp. 3–9.

<sup>103</sup> ÁBTL 1981. i.m. pp. 54-56.

<sup>104</sup> WILLIAMS i.m. pp. 174–187.

<sup>105</sup> ÁBTL 1981. i.m. pp. 57-58.

mindenekelőtt a fegyveres rablásokkal foglalkozott.<sup>106</sup> A ”Criminal Intelligence Section”<sup>107</sup> (Bűnügyi Hírszerző Részleg) két csoportból állt. Az egyik operatív eszközökkel az aktív bűnözőket ellenőrizte, a másik olyan személyekre megy rá, akik még nem voltak büntetve, de alaposan gyanúsíthatók bünszövetségben való részvétellel, vagy annak irányításával. A ”Regional Crime Squads” (Regionális Bűnügyi Osztág) Takács állításától eltérően nem a terrorizmuscselekmények és a nemzetközi maffia ügyében nyomozott, hanem a brit főváros és annak tágabb környezetében, a körzethatárokon átnyúló bűnügyeket vizsgálta.<sup>108</sup> A ”National Drugs Intelligence Unit” (Országos Kábítószer Felderítő Osztály) a későbbi ”National Criminal Intelligence Service” (Országos Bűnügyi Hírszerző Szolgálat) elődszervezetének volt tekinthető.<sup>109</sup> A ”National Immigration Intelligence Unit” (Országos Bevándorlási Információs Egység) a migrációt ellenőrizte,<sup>110</sup> míg a ”Diplomatic Protection Group” (Diplomáciai Védelmi Csoport) a külképviseleti intézmények egyenruhás biztosítását végezte. A 60-as évek közepétől felgyorsult a brit rendőri erők felfegyverzésének folyamata: ekkor jött létre az ”Special Patrol Group” (Különleges Járőrszolgálat) elnevezésű csapaterős egység, valamint a D11 jelű fegyveres beavatkozó és lőfegyveres kiképző csoport. Az utóbbi jelentősége azért is megnőtt, mivel a DPG mellett a SB, az ”Anti Terrorist Branch” (Terrorellenes Ügyosztály) és a rablási csoport minden tagja fegyverrel lépett szolgálatba.<sup>111</sup>

### **Special Branch (Különleges szolgálat)**

*A Special Branch /SB/ a Scotland Yard egésze keretében működött, de végső soron a Belügyminisztérium közvetlen alárendeltségében állt. A SB az MI5 megbízásából kapcsolódott be az egyes ügyek vizsgálatának utolsó stádiumában, amikor operatív műveleteket, akciókat, letartóztatásokat hajtott végre, bizonyítékokat gyűjtött a bírósági eljárásra, és meg is jelenik a tárgyaláson.<sup>112</sup> A SB, amit 1883-ban alapították az ír nacionalizmus elleni küzdelemre, hivatásos állományának létszáma a 80-as évek elejére kb. 1500 főre volt tehető,<sup>113</sup> miután 1964-ben hatáskörének az egész országra történő kiterjesztésével párhuzamosan jelentős bővítésre került sor. Angliában és Walesben a 41 területi rendőrkapitányság mindegyikénél egy-egy kirendeltség működött, melynek létszáma a körzetük nagyságától és fontosságától függően átlag 8-12 fő. A SB személyzetét saját iskolájában képezte, alapos ellenőrzés után jellemzően azok közül az egyenruhás rendőrök közül válogatott, akik már letöltötték a kétéves próbaidőt és egy idegen*

<sup>106</sup> KIRBY, Dick: The Sweeney. The First Sixty Years of Scotland Yard’s Crimebusting Flying Squad 1919 – 1978. Pen & Sword Books Ltd. Barnsley, 2011. pp. 17–40.

<sup>107</sup> ALLASON, Ruppert: The Branch. A History of the Metropolitan Police Special Branch 1883–1983. Secker & Warburg, London, 1983. p. 166.

<sup>108</sup> SLIPPER, Jack: Slipper of the Yard. Sidgwick & Jackson, London, 1981. p. 112.

<sup>109</sup> DORRIL (1993) i.m. pp. 221–222.

<sup>110</sup> ALLASON i.m. p. 156.

<sup>111</sup> BREWER, John D.– GUELKE, Adrian – HUME, Ian – MOXON-BROWNE, Edward – WILFORD, Rick: The Police, Public Order and the State. St. Martin’s Press. New York, 1988. pp. 13–25.

<sup>112</sup> ÁBTL 1981. i.m. p. 59.

<sup>113</sup> RICHELSON–BALL i.m. pp. 24–25.

nyelvet legalább középfokon ismertek. A feladatkör a megalakulás óta alaposan megváltozott, a parlament legutoljára 1964-ben szabályozta.<sup>114</sup>

1) *A SB volt felelős a királyi család és a kabinet miniszterek védelméért, ahol e célra különlegesen kiképzett nyomozókat alkalmaztak. A külföldi államfők – miniszterek látogatását a FO, vagy más minisztérium megbízásából a "Central Office of Information" (Központi Információs Hivatal) szervezte, amely a programnak és az esetlegesen várható rendzavarásnak megfelelően kérte a SB biztosítását. A Nagy-Britanniába történő beléptetést a SB repülőtéri csoportja végezte el, míg a vidéki utazásokon egy csoport nyugdíjas rendőrtiszt állandó jelleggel kísérte a vendégeket. A helyi biztosítás terén a Branch területi kirendeltsége volt illetékes.*

2) A SB hivatásos állománya foglalkozott a kikötők és a repülőterek ellenőrzésével, amihez nagyszámú informátort alkalmaztak. A terrorcselekmények és gépeltérítések megakadályozása érdekében igen szigorú intézkedéseket vezettek be a repülőtéri ellenőrzés folyamán, ugyanakkor az országba történő beléptetésnél az "Immigration Officer" a SB és az MI5 által összeállított feketekönyvben ellenőrizte, hogy a belépő nincs-e a tiltólistán. A repülőtéri rendészet kamerákon, a kritikusabb helyeknél személyesen figyelték az utasforgalmat és minden gyanús körülményről rádióon tájékoztatták a SB kirendeltségét. 1978. április elsejétől a Scotland Yard a létszámproblémái nyomán a vidéki kikötők ellenőrzésével foglalkozó 39 rendőrtisztet visszarendelte a fővárosba, míg a szóban forgó feladatot átteremtették a helyi erők fokozatosan e célból felkészített egységeihez. A SB ekkor már elsősorban a Heathrow nemzetközi repülőtér biztonságára kívánt összpontosítani, ahol óhatatlanul jelentősen megnőtt a terrorfenyegetettség.<sup>115</sup>

3) *A követségi épületeket és diplomatakat szintén a SB nyílt állománya biztosítja. Fenyegetés vagy várható terrorcselekmény esetére nyílt figyelmet alkalmaztak, rendszerint az objektummal szemben leállított gépkocsiból. A szocialista országok és a "nem baráti országok" követségeinek operatív elhárítását az MI5 végezte.*

4) *A SB kontroll tevékenységének középpontjában akkortájt is a baloldali és jellemzően a színes bőrűekből álló politikai irányzatok, mozgalmak és szervezetek tevékenységének ellenőrzése állt. A megelőző években a terrorakciók elszaporodása és a sorozatos, főleg politikai rendzavarások miatt ismét jelentős létszámnövekedésre került sor, az ír csoport állományát többszörözték, ugyanakkor hatásköre Észak-Írországra is kiterjedt.*<sup>116</sup> A valóságban a brit rendfenntartó erők között különleges helyzetű Royal Ulster Constabulary (Királyi Északír Rendőrség, angol rövidítéssel: RUC) keretében egy megnövelt hatáskörű Special Branch működött, ír terrorizmus elleni harc a fősziqeten a Scotland Yard Különleges Szolgálatának hatáskörébe tartozott.<sup>117</sup>

5) 1973-ig a SB hatáskörébe tartozott a honosítási kérelmek elbírálása és az erkölcsi bizonyítványok kiadása. Ezzel egy külön alosztály foglalkozott, amely a

<sup>114</sup> DORRIL (1993) i.m. pp. 161–165.

<sup>115</sup> TNA Home Office (HO) 287/2465 – POL 74 0766/0002/011 – SPECIAL BRANCH EMPLOYMENT AT SEA AND AIRPORTS – NATIONAL PORTS SCHEME – METROPOLITAN SPECIAL BRANCH INVOLVEMENT. – 25 October 1977. – 17 February 1978.

<sup>116</sup> ÁBTL 1981. i.m. pp. 61–62.

<sup>117</sup> HENNESSEY, Thomas – THOMAS, Claire: Spooks. The Unofficial History of MI5. Amberley Publishing, 2009, Stroud. pp. 577–587.



nyilvántartó áttekintésén túl a célszemély rokonságával, baráti körével, iskolatársaival is elbeszélgetett.<sup>118</sup>

6) A SB naprakészen tartott egy rendkívüli állapotra vonatkozó intézkedési tervet, amely az MI5-al közösen készült, így többek között azon személyek névsorát tartalmazta, akiket háború vagy rendkívüli eset kapcsán órák alatt internálnának, vagy az országból kiutasítanak. Ilyen intézkedésre kétszer, 1914-ben és 1940-ben került sor.<sup>119</sup>

7) 1973-tól a SB látta el a választásokkal kapcsolatos szabálysértések vizsgálatát.

8) A SB országos hálózatának kiépítése után kezdett foglalkozni a kisebb ipari objektumok elhárításával, úgy, hogy de facto az összes jelentősebb magánvállalattal kapcsolatban álltak. A hivatalos kapcsolat szerepét az objektum személyzeti igazgatója és biztonsági vezetője látta el, míg a rendbontó és felforgató elemeket informátorokon keresztül kontrollálták. Sztrájkok alkalmával megszervezték a munkás-és szakszervezeti gyűlések lehallgatását és bizonyítékokat gyűjtenek a sztrájkvezetők elleni eljáráshoz. Szabotázs vagy szabotázsnyíus esetekben a SB nyílt vizsgálatot tart az esemény tisztázására. Az ipari objektumoknál a kémtevékenység elhárítására és a hivatali titkok őrzésére az MI5 hatáskörében volt és maradt.

9) 1964-től a SB fokozta tevékenységét az egyetemeken és a főiskolákon, elsősorban a baloldali beállítottságú tanárok és hallgatók felderítésére és operatív ellenőrzésére. Az információkat főleg sajtófigyeléssel, hivatalos kiadványokból szerezte, de a tömegkommunikációnál jelentősebb az informátorok foglalkoztatása, akiket öt kategóriába soroltak.<sup>120</sup> 1) Alkalmi informátor, akit komolyan semmi nem motivált az együttműködésre, az ügyosztállyal való kapcsolata rendszertelen a szolgálattal, és a mindenki által ismert eseményekről, megnyilvánulásokról ad tájékoztatást. Azok a jobboldali beállítottságú átlagemberek, akik a baloldali beállítottságú személyekről, csoportokról, azok tevékenységéről számoltak be, sokszor egyéni ellenszemből vagy érdeksérelemből. 2) Informátor, aki állandó összekötetésben állt a rendőrséggel, de operatív akcióban nem vesz részt. Az általában ismert dolgokról adott tájékoztatást, nincs beszerelve, és anyagi ellenszolgáltatást sem kap tevékenységéért. 3) Fizetett informátor, akit az ügyosztály egy-egy konkrét ügyben alkalmazott 5-10 fontos díjazás ellenében, legyen szó a keleti blokk követségei elleni tüntetésekről, a tiltakozó mozgalmak felvonulásának megzavarásáról. Sokkal elterjedtebb volt a fizetett informátoroknak az a csoportja, amely az átadott értesülés értékének megfelelő díjazásban részesült. Őket már be is szervezték, miközben együttműködésüket a pénz motiválta. 4) Pressziós informátorok esetén a Special Branch kompromittáló adatokkal rendelkezett, amely alapján büntető eljárást lehetett volna indítani ellenük. Nagyon elterjedt, hogy az informátorok e kategóriáját anyagiakkal ösztönzik aktívabb munkára. 5) Az utolsó kategóriába a különleges szolgálat hivatásos SZT állománya tartozott: ez a 15-20 rendőrtiszt alapos gyanú esetén beépült a célobjektumba és bizonyítékokat szerzett a bírósági eljáráshoz.<sup>121</sup> Az 1980-as évektől a növekvő a korábbi Anti-Terrorism Squad (Terrorellenes Osztag) Anti-Terrorism Branch (Terrorellenes Szolgálat)

<sup>118</sup> TNA MEPO 3/1945 – 35/45/60 – Suggested increase in existing Special Branch Establishment in their forthcoming naturalization enquiries. – 22nd January 1948. 28A–92A

<sup>119</sup> ALLASON i.m. p. 38, 117.

<sup>120</sup> ÁBTL 1981. i.m. pp. 61-62.

<sup>121</sup> ÁBTL 1981. i.m. pp. 63–64.

néven önállósult, végül 2006 októberében a Special Branch és az Anti-Terrorism Branch összeolvastásával létrejött a Counter Terrorist Command (Terrorelhárító Parancsnokság).<sup>122</sup>

A szerző azzal zárta tanulmányát, hogy a brit titkosszolgálatok az anyagi problémák és a birodalom hanyatlása miatt már nem tartoznak a világ élvonalába, igaz, a jó technikai felszereltség, szervezettség, a társadalom fegyelmezettsége növeli az erejüket. *„Hiba volna a sok tapasztalattal és tekintéllyel rendelkező brit speciális és rendőri szervek tevékenységét lebecsülni, de ugyanolyan hibát jelentene az is, ha misztikumokra építve túlbecsülnénk e szervek munkáját és lehetőségeit”*.<sup>123</sup> Takács Dezső azonban nem tudhatott arról, hogy az MI6 1974 folyamán beszervezte az akkor Koppenhágában szolgálatot teljesítő Oleg Gorgyijevszkij KGB alezredest,<sup>124</sup> aki 1985-ben a londoni rezidentúra parancsnokaként figyelmeztette az MI5-öt, hogy a szovjet diplomáták és állampolgárok tevékenységét ellenőrző K4-es alosztály egyik tisztje, Michael Bettaney, felajánlotta szolgálatait Arkagyij Guk korábbi rezidensnek. Bettaney 25 éves fegyházbüntetést kapott, ugyanakkor Gorgyijevszkij a Nyugat-Európában zajló KGB-műveleteket is kompromittálta.<sup>125</sup>

### Utószó

Takács Dezső tanulmánya nem sokkal a détente bukása, az afganisztáni szovjet intervenció utáni konfrontatív időszak terméke, amikor az az észak-atlanti szövetséghez tartozó országok is a mai gyakorlattal összevetve sokkal szélesebb körben titkosították a kormányzat működésével kapcsolatos információkat. A hidegháború lezárása, a Szovjetunió felbomlása, a Varsói Szerződés egykori tagjainak NATO-csatlakozása, valamint az információs forradalom jóvoltából a korábbi állam-és katonai titkok jelentős része okafogyottá vált. Mindezzel párhuzamosan a történészszakma részéről felmerült az igény, hogy a politika-és hadtörténet hírszerzési háttere is megismerhető legyen.<sup>126</sup> Nagy-Britanniában az 1940-es évek végéig a hírszerző-és elhárító szolgálatoknak a létezése is tabutéma volt, de egészen a hidegháború végéig legfeljebb az időről időre kirobbanó kémbostrányok kapcsán találkozhattunk az MI5 vagy az MI6 említésével a brit sajtóban. Az MI5 létezését hivatalosan az 1989. évi Security Service Act (Biztonsági Szolgálati Törvény) ismerte el először egy majdnem félévtizedes előkészítést, illetve hosszas parlamenti vitát követően.<sup>127</sup> Az MI6 működése pedig az 1994-es Intelligence Services Act (Hírszerző Szolgálatokról Szóló Törvény) jóvoltából került önálló jogi alapokra.<sup>128</sup> Valószínű, hogy a Brit Birodalom első védelmi vonalának titokban működő szerveit a pártállami rendszerekre hasonlító titkolózással próbálták megvédeni az ellenséges behatolástól, holott az árulók vagy a meghívással

<sup>122</sup> BLAKE, Christopher – SHELDON, Barrie –STRZELECZKI, Rachael – WILLIAMS, Peter: Policing Terrorism. Learning Matters, London, 2012. pp. 93–94.

<sup>123</sup> ÁBTL 1981. i.m. p. 65.

<sup>124</sup> WEST, Nigel: At Her Majesty's Secret Service. The Chiefs of Britain's Intelligence Agency, MI6. London, Greenhill Books, 2006. pp. 155–156, 205–206.

<sup>125</sup> ANDREW i.m. pp. 714–722.

<sup>126</sup> SIMON László: A titok speciális értelmezése az elmúlt 25 év kihívásainak, kockázatainak és fenyegetéseinek tükrében. Felderítő Szemle, 2016. 3. sz. pp. 78–82.

<sup>127</sup> URBAN, Mark: UK Eyes Alpha. Inside British Intelligence. Faber and Faber, London, 1996. pp. 52–55.

<sup>128</sup> DAVIES i.m. p. 301.

szolgálatokhoz kerülő, felső középosztálybeli fiatalok – pl. Kim Philby, Anthony Blunt – vagy a már hivatásos állományhoz tartozó személyek – pl. George Blake, Michael Bettaney – kerültek ki.

***Felhasznált irodalom:***

- ALLASON, Rupert: *The Branch. A History of the Metropolitan Police Special Branch 1883–1983.* London, 1983, ISBN: 0-436-01165-4.
- ANDREW, Christopher: *The Defence of the Realm. The Authorized History of MI5.* London, 2009, ISBN: 978-0-713-99885-6.
- BECKETT, Francis: *Enemy Within. The Rise and Fall of the British Communist Party.* John Murray Ltd. London, 1995. ISBN: 0719553105
- BLAKE, Christopher – SHELDON, Barrie –STRZELECZKI, Rachael – WILLIAMS, Peter: *Policing Terrorism.* London, 2012, ISBN 978-08-57255-181.
- BREWER, John D.– GUELKE, Adrian – HUME, Ian – MOXON-BROWNE, Edward – WILFORD, Rick: *The Police, Public Order and the State.* New York, 1988, ISBN 0312015658.
- BUTLER, David – SLOMAN, Anne: *British Political Facts 1900–1979.* London, 1980, ISBN 978-0-333-25592-6.
- CAVENDISH, Anthony: *Inside Intelligence. The Revelations of an MI6 Officer.* London, 1997, ISBN 0 00 637 612 6.
- CATER, Frank – TULLET, Tom: *The Sharp End. One Man's Life with the Flying Squad – From the Krays to Brinks Mat.* London, 1990, ISBN 0 586 20641 8.
- COWLEY, Richard: *A History of British Police. From its Earliest Beginnings to the Present Day.* Stroud, 2011, ISBN 978 0 7524 5891 5.
- CHAPMAN, Richard A.– HUNT, Michael (ed.): *Open government. A study of the prospects of open government within the limitations of the British political system.* London, 1989, Routledge. ISBN 0-415-03953.
- DAVIES, Philip H. J: *MI6 and the Machinery of Spying.* London, 2004, ISBN 0-7146-8363-9.
- DEACON, Richard: 'C'. *A Biography of Sir Maurice Oldfield. Head of MI6.* London, 1985, ISBN 0 7088 2878 7.
- DONALDSON, Frances: *The British Council: the first fifty years.* London, 1984, Jonathan Cape. ISBN 0-224-02041-2.
- DORRIL, Stephen – RAMSAY, Robert: *Smear! Wilson and the Secret State.* London, 1992, ISBN 0586 21713 4.
- DORRIL, Stephen: *The Silent Conspiracy. Inside the Intelligence Services in the 1990's.* London, 1993, ISBN 0 434 20162 6.

- DORRIL, Stephen: MI6. Inside the Covert World of Her Majesty's Secret Intelligence Service. *London, 2000, ISBN 0-74432-0379-8.*
- DYLAN, Hugh: Defence Intelligence and the Cold War. Britain's Joint Intelligence Bureau. *Oxford, 2014, ISBN: 978-0-19-965702-5.*
- HERMAN, Michael: Intelligence power in peace and war. *Cambridge, 1996, ISBN 0 521 562317.*
- HENNESSEY, Thomas – THOMAS, Claire: Spooks. The Unofficial History of MI5. *Stroud, 2009, ISBN 978 1 84868 079 1.*
- HODGES, Andrew: Kódjátzsma. *Budapest, 2015, ISBN 978 963 406 011 6.*
- HOUSE OF COMMONS SCIENCE AND TECHNOLOGY COMMITTEE: The Forensic Science Service. Seventh Report Session 2010-12. *London, 2011, IBN 978 0 215 56032 2.*
- JEFFERY, Keith: MI6. The History of the Secret Intelligence Service. *London, 2010, ISBN 978 1 4088 10057.*
- KIRBY, Dick: The Sweeney. The First Sixty Years of Scotland Yard's Crimebusting Flying Squad 1919–1978. *Barnsley, 2011, ISBN 978 1 84884 390 5.*
- LEIGH, David: The Wilson Plot. How the Spycatchers and Their American Allies tried to Overthrow the British Government. *London, 1988, ISBN 0-394-57241-6.*
- MACINTYRE, Ben: Kém a csapatban – Kim Philby és a nagy árulás. Gabo Kiadó, Budapest, 2015. ISBN: 9789636899806
- MOZSIK Imre: Washingtoni emberünk. Hírszerző voltam Amerikában. MÁS Könyvek, Budapest, 1995. ISBN: 9632083458
- PEPPER, Ian K: Crime Scene Investigation. Methods and Procedures. Open University Press, Maidenhead, 2010. ISBN: 978-0-33-523441-7
- PINCHER, Chapman: The Truth About Dirty Tricks from Harold Wilson to Margaret Thatcher. Sidgwick & Jackson, London, 1991. ISBN: 0283060603
- PRADOS, John: Presidents' Secret Wars. CIA and Pentagon Covert Operations Since World War II. *New York, 1986, ISBN 0-688-05384-X.*
- RICHELSON, Jeffrey T. – BALL, Desmond: The Ties That Bind. Intelligence Cooperation between the UKUSA Countries – the United Kingdom, the United States of America, Canada, Australia and New Zealand. *Boston, 1985, ISBN0-04-327092 1.*
- RAWLINGS, Philip: Policing: A Short History. Willan Publishing, Cullompton ISBN 1 903240 26 3
- RIMINGTON, Stella: Nyílt titok. Az MI5 – a brit kémelhárítás – volt főigazgatójának emlékiratai. Geopen Könyvkiadó, Budapest, 2004. ISBN: 0219003733475

- SIMON László: A titok speciális értelmezése az elmúlt 25 év kihívásainak, kockázatainak és fenyegetéseinek tükrében. *Felderítő Szemle*, XV. évf. 1. szám (2016. április) pp. 59-67.
- SLIPPER, Jack: *Slipper of the Yard*. London, 1981, ISBN-0-283-98819-3.
- SMITH, Michael: *The Real James Bonds 1909–1939*. London, 2011, ISBN 978-1-906447-00-7.
- THOMAS, Gordon: *A brit titkosszolgálatok világa*. JLX Kiadó, Budapest, 2008. ISBN: 9789633052778
- URBAN, Mark: *UK Eyes Alpha. Inside British Intelligence*. London, 1996, ISBN 0-571-17689-5.
- WALTON, Calder: *Empire of Secrets. British Intelligence, the Cold War and the Twilight of Empire*. London, 2013, ISBN 978-0-00-745796-0.
- WEINER, Tim: *A CIA története. Hamvába holt örökség*. Budapest, 2015, ISBN 978 963 689 3169.
- WEST, Nigel: *MI6. British Secret Intelligence Operations 1909–45*. London, 1985, ISBN 0-586-06332-3.
- WEST, Nigel: *At Her Majesty's Secret Service. The Chiefs of Britain's Intelligence Agency, MI6*. London, 2006, ISBN-13: 978-1-85367-702-1).
- WEST, Nigel: *Secret War for the Falklands. The SAS, MI6, and the War Whitehall Nearly Lost*. London, 2010, ISBN 978-0-7499-2071-2.
- WILLIAMS, Chris A: *Police Control Systems in Britain, 1775–1975. From parish constable to national computer*. Manchester, 2014, ISBN 978 0 7190 8429 4.
- WILSON, Ray –ADAMS, Ian: *Special Branch. A History: 1883–2006*. London, 2015, ISBN 978-1-84954-910-3
- ZEIGLER, Philip: *Wilson. The Authorised Life of Lord Wilson of Rievaulx*. Weidenfeld & Nicolson, London, 1993. ISBN: 0297812769

GULYÁS ATTILA<sup>1</sup>

### KIBERHADVISELÉS ÉSZAK-KOREAI MÓDRA II.

---

#### *A Lazarus csoport*

A Lazarus csoport neve nem tűnhet ismeretlennek az olvasó előtt, mivel a közelmúlt hírhedt „WannaCry” nevű zsaroló vírus fertőzés kapcsán a sajtóban számos találgatás jelent meg, miszerint az akciót az észak-koreai Lazarus csoport hajtotta végre. A cikk írásának idején azonban az elfogadott általános vélemény szerint Kína áll a támadás mögött. A csoport kétes érdemeit azonban ez nem csökkenti, mivel jelenleg a világ egyik legfelkészültebb és talán a legveszélyesebb csoportjának tekinthető. A szervezet létszámáról, felépítéséről, illetve fizikai tartózkodási helyéről ez idáig nem kerültek nyilvánosságra hivatalosnak tekinthető adatok.

Az amerikai Novetta<sup>2</sup> adatfeldolgozó és elemző, valamint kiberbiztonsággal foglalkozó nagyvállalat, néhány partnerével együttműködve „Blockbuster” néven 2014 decemberében közel egy évig tartó műveletet indított az általuk rendkívül veszélyesnek értékelt Lazarus csoport megismerésének és tevékenységének megszakítása érdekében. Az akciót a Sony Pictures Entertainment (SPE) ellen 2014 novemberében indított kibertámadás motiválta, amelynek keretében a támadó jogtalanul szerzett meg digitális tartalmakat és semmisített meg nagymennyiségű üzleti célú adatot.

A Sony elleni akciót az FBI és az NSA Észak-Koreának tulajdonította. A „Blockbuster” művelet keretében azonban minden hivatalos nyilatkozatot figyelmen kívül hagytak és a pártatlanság érdekében csakis a rendelkezésre álló bizonyítékokat vizsgálták meg és vetették össze a nyílt forrásokból rendelkezésükre álló kártevő mintákkal. Az akció végeztével egyértelmű kapcsolatot mutattak ki a támadás és a Lazarus csoport által használt eszközök és módszerek között. Kiderítették továbbá, hogy a Sony elleni támadásnál használt eszközöket már korábban is használták főleg dél-koreai és amerikai egyesült államokbeli pénzügyi, katonai, repülőgépgyártó és kritikus infrastruktúrákat érintő támadásokban.<sup>3</sup> A Sony elleni akciót a Guardian of Peace (GoP) nevű, addig ismeretlen hacker csoport vállalta magára, azonban a Novetta tanulmánya szerint az állítólagos GoP nyilatkozat csak a figyelmet próbálta elterelni a Lazarus csoportról.

A „Blockbuster” befejezését követően a Lazarus csoporttal kapcsolatban az alábbi megállapításokat tették:

---

<sup>1</sup> A szerző a Honvéd Vezérkar Tudományos Kutatóhely külsős kutatója.

<sup>2</sup> <https://www.novetta.com/our-story/partners> (Letöltés ideje: 2017. 05. 20.)

<sup>3</sup> Novetta: Operation Blockbuster, <https://www.operationblockbuster.com/>, <https://www.operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-Report.pdf>, (Letöltés ideje: 2017. 05. 26.)

A csoport 2009-től működik, tagjai rendkívül jól képzett, felkészült programozók, akik szakterületenként specializálódtak. A programkódokat megosztják egymás között, ám azokat kissé módosítják, hogy az antivírus programok jellemző mintázataik alapján ne deríthessék fel kártevőiket. A csoport programozói közös titkosítási algoritmusokat alkalmaznak, és a programjaikban azonos védelmi megoldásokkal igyekeznek elkerülni a kódok visszafejtését. Kártevők a vezérlő szerverekkel azonos titkosított protokoll alapján kommunikálnak. A feladat végeztével csak rájuk jellemző eljárás alkalmazásával törlik nyomaikat a megfertőzött eszközökről. A csoport olyan erőforrásokkal rendelkezik, amelyek lehetővé teszik a nagy mennyiségű és változatos, egyedileg fejlesztett kártevő elkészítését, és az ezt megelőző, hosszú ideig tartó alapos felderítő, előkészítő munkát. Megfelelő anyagi fedezettel a háttérben képesek hosszú ideig (esetenként hónapokig) tartó elosztott szolgáltatás megtagadásos<sup>4</sup> támadások végrehajtására is. A „Blockbuster” művelet során összevetették a korábbi támadások alkalmával hátrahagyott kártevő programokat és nyomokat a Sony támadásnál használtakkal és ezek alapján felállítottak egy idősort a Lazarus csoporthoz köthető műveletekről.

Ssz	Dátum	Művelet leírása
1.	2007. március 07.	Az elsőgenerációs kártevő kifejlesztése, amely szerepet kapott a későbbiekben az „Operation Flame”, az „Operation 1Mission”, valamint az „Operation troy”, és a „Dark Seoul 2013” műveletekben.
2.	2009. július 04.	Támadás amerikai és dél-koreai weboldalak ellen, amelyekben a MYDOOM és a Dozer kártevőket használták. A kártevő üzenetet hagyott az MBR rekordban ezzel a szöveggel: „ A függetlenség napjának emlékére”
3.	2009-2013. március	„Operation Troy” nagyszabású kiberhírszerzési művelet Dél-Korea ellen, amely 2013-ban a „Dark Seoul” akcióval zárult.
4.	2011. március	A „Ten days of rain” művelet, amelyben a dél-koreai média és pénzügyi, valamint kritikus infrastrukturális intézményeket DDOS módszerrel támadták 10 napon keresztül.
5.	2011. április	DDOS támadás a Nonghyup Bank ellen.
6.	2012.	“Operation 1Mission” művelet kezdete, amely később kapcsolódott a 2013-as „Dark Seoul” művelethez.
7.	2012. június	Egy konzervatív dél-koreai lap bejelentette, hogy egy magát „IsOne”-nak nevező csoport megtámadta, megváltoztatták a weboldalukat (deface) és sikertelenül megpróbálták letörölni a szerverük tartalmát.
8.	2013. március 20.	A „Dark Seoul” támadás során három műsorszóró társaságot, valamint pénzügyi intézményeket, kormányzati szerveket és katonai hálózatokat, valamint egy internet szolgáltatót ért támadás, amelyben megpróbálták a merevlemezeiket helyreállíthatatlanul letörölni. A felelősséget az addig ismeretlen „NewRomantic Cyber Army Team” and „WhoIs Team” vállalta magára. Ez a két csoport is a nyomok alapján a Lazarus csoporthoz köthető.
9.	2014. november 24.	A Sony Entertainment Picture elleni támadás, amelynek keretében adatokat semmisítettek meg és loptak el.

**1. ábra: A Blockbuster művelet keretében összeállított idővonal, a szerző által szerkesztett formában**

<sup>4</sup> Distributed Denial of Service (röviden: DDoS) az elosztott szolgáltatásmegtagadással járó támadás egy informatikai szolgáltatás teljes vagy részleges megbénítása, illetve helyes működési módjától való eltérése.

## A „Dark Seoul” és az „Operation Troy” műveletek

A „Dark Seoul” művelet, az „Operation Troy” néven Dél-Korea ellen irányuló, több évig tartó kiberkémkedési műveletsor utolsó mozzanata volt. A vizsgálat időpontjában a „Dark Seoul” műveletért két különböző csoport vállalta a felelősséget, amelyeket akkor még nem kötöttek a Lazarus csoporthoz. Nem tudjuk, hogy a csoport létezett-e egyáltalán akkor, és a két felelős részleg a Lazarus alárendelt egysége volt-e, vagy éppen belőlük alakult a későbbi Lazarus csoport. A „Blockbuster” jelentés mindenesetre egyértelműen a későbbi Lazarushoz köti a műveletekben használt kártevőket.<sup>5</sup>

Az utóbb „Dark Seoul” néven ismertté vált incidensben Dél-Koreát 2013. március 20-án helyi idő szerint hajnali kettő órakor kibertámadás érte. Hírügynökségek, telekommunikációs cégek, állami szervezetek, és katonai hálózatok, valamint bankok estek áldozatul egy olyan kártevőnek, amely letörölte a számítógépek Master Boot Record-ját (továbbiakban MBR)<sup>6</sup>. A megromlott eszközök és felderített kártevők vizsgálatát követően az elemzők arra a következtetésre jutottak, hogy a támadóknak az akciót megelőzően már volt hozzáférésük a megtámadott rendszerekhez. Az események időrendjét vizsgálva megállapították, hogy rendszerenként egy munkaállomáson keresztül jutottak be a hálózatokba úgy, hogy célirányosan megtévesztő leveleket küldtek az alkalmazottaknak<sup>7</sup>, amelyekben a kártevők letöltéséhez vezető linkeket rejtettek el. A rendszerekbe bejutva a meglévő felhasználói jogosultságuk kiterjesztését követően a patch és update szervereket célozták meg, amelyek alkalmasak voltak arra, hogy a munkaállomásokra adott időben eljuttathassák a kártevő programot. Az akció kezdetét megelőzően néhány perccel a már korábban megnyitott hátsó kapukon keresztül bejuttatták az antivírus update fájlnak álcázott kártevőket a patch és update szerverekre, ahonnan a kártevők eljutottak minden munkaállomásra, ott aztán a már szintén korábban telepített betöltő programok (loaderek) kibontották és indították őket. A kártevők a beépített időzítőnek megfelelően helyi idő szerint 02:00-kor megkezdték az MBR-ok törlését. Ennek a műveletnek a keretében több tízezer számítógép vált – legalább is egy időre – használhatatlanná. A támadás érintette egy közelebből meg nem nevezett bank ATM hálózatát is, napokra lehetetlenné téve az automatakból történő készpénzfelvételt.

A károkozásért két, korábban ismeretlen csoport vállalta a felelősséget. A „New Romanic Army” és a „Whois Hacking Team”. Az előbbihez köthető MBR törlő (wiper) program kódjában és a célrendszerek megváltoztatott (defaced)

---

<sup>5</sup> A szóban forgó akciókat a McAfee Labs elemezte a Dissecting of Operation Troy: Cyber Espionage in South Korea című tanulmányában, lásd: <sup>5</sup>Ryan Sherstobitoff and Itai Liba, McAfee® Labs and James Walter, Office of the CTO: Dissecting Operation Troy: Cyberespionage in South Korea, McAfee Labs, 2013. wp-dissecting-operation-troy.pdf (Letöltés ideje: 2017. 06. 02.)

<sup>6</sup> "Indiana University Indiana University." What is a Master Boot Record (MBR)? Accessed June 09, 2017. <https://kb.iu.edu/d/aijw>. (Letöltés ideje: 2017. 06. 15.) A merevlemez első szektorának elnevezése. Tartalmaz egy MBR nevű programot, valamint a partíciós táblát, amely a partíciók elhelyezkedését tárolja. Az MBR segítségével indul az operációs rendszer, ha megsérül nem indítható az adott lemezzel a rendszer.

<sup>7</sup> Spearphishing



nyilvános weblapjain is számos római korból származó katonai kifejezést hagytak hátra.

Az LG+U internetszolgáltató honlapját a „Whois Hacking Team” változtatta meg és az ehhez a támadáshoz köthető MBR törölő program gyakorlatilag teljesen megegyezett a „New Romanic Army” által használt programmal.

A támadók a megváltoztatott weboldalakon üzeneteket hagytak, amelyek szerint sikerült számos bizalmas banki, illetve személyes információt megszerezniük, majd meghagytak egy dropbox elérhetőséget is, ahol az érdeklődők meggyőződhetnek arról, hogy állításuk megfelel a valóságnak.

A McAfee szakemberei tovább vizsgálva a március 20-án történt pusztítás körülményeit, arra a következtetésre jutottak, hogy az akció nem csupán vandalizmus volt, hanem egy 2009. októbertől tartó kiberkémkedési műveletsorozat záró akciója. A kémkedés egészen a McAfee szakembereinek jelzéséig észrevétlen volt a koreai hatóságok előtt!

A több évig tartó kémakciót az egyik szoftver a forráskódjában gyakran szereplő „Troy”<sup>8</sup> szó miatt „Operation Troy”-nak nevezték el. A McAfee munkatársai vizsgálataik során számos egyedi fejlesztésű trójai programot, ezek különböző verzióit, valamint titkosított félautomata információgyűjtő hálózatokat fedeztek fel, amelyeken keresztül az északi katonai jellegű információkat gyűjtötték a déli szomszéd hadseregéről, műszaki, és technikai fejlesztéseiről. A két műveletben használt eszközök elemzése azt mutatta, hogy egy csoport állt a támadások mögött.

Az „Operation Troy” művelet kezdő lépéseként az észak-koreai hackerek egy dél-koreai katonai közösségi oldalt megfertőztek, majd az úgynevezett „watering hole” módszerrel<sup>9</sup> terjesztették a kémprogramjaikat. Azok, akik ezeket az oldalakat felkeresték, akaratukon kívül, észrevétlenül telepítették gépükre a kémprogramokat. A szoftver képes volt egy elsődleges elemzést készíteni a célszámítógép tartalmáról és azt egy meghatározott pontrendszer szerint rangsorolta, majd felvette a kapcsolatot a vezérlő szerverével és jelentette a gép pontszámát. A kezelők természetesen utasíthatták a programot a könyvtárstruktúra elküldésétől kezdve egyedi fájlok, könyvtárak elküldésére, vagy akár törlésére is. A program meghatározott fájlkiterjesztéseket gyűjtött össze, és ezekben egy előre megadott lista alapján angol és koreai nyelvű katonai jellegű kulcsszavakat keresett. A talált szavak jellege és gyakorisága alapján rangsorolta a gép tartalmát. A kémprogram egyébiránt képes volt a gépen tárolt felhasználóneveket és jelszavakat is megszerezni, valamint a szoftver rendelkezett a már ismert MBR törölő képességgel is, ezért ha a kezelők úgy döntöttek, ennek segítségével indíthatatlanná tehetnék az adott számítógépet, így próbálva eltüntetni a nyomaikat. Önvédelmi célból ezt a program részletet használták abban az esetben is, ha a kártevő úgy érzékelte, hogy megpróbálják elemezni.

Lehetetlen megállapítani, hogy a kémkedés közel négy esztendeje alatt az északiak mennyi és milyen jellegű információhoz fértek hozzá, arra sincs igazán magyarázat, hogy miért azon az adott napon és időben indították a "Dark Seoul" műveletet, hiszen a dél-koreai hatóságok nem fedték fel az akciójukat. Ezekre a kérdésekre a vizsgálat nem tudott választ adni.

---

<sup>8</sup> Trója

<sup>9</sup> watering hole magyarul, itató. Olyan hely, ahová a vadállatok inni járnak. Olyan támadási stratégia, amelyben egy olyan webhelyet fertőznek meg, amelyet sokan felkeresnek és így a fertőzés viszonylag gyorsan terjed.

## A „Blockbuster” hatása

A nyilvánosságra hozott felfedezések nagy károkat okoztak a Lazarus csoportnak, mivel eszközeik egy része kompromittálódott, így ezek pótlására újabb erőforrásokat kellett mozgósítaniuk, ami úgy tűnik már meghaladta a támogatójuk lehetőségeit, vagy valamilyen más okból megvonták tőlük a támogatást, esetleg arra utasították őket, hogy önfenntartók legyenek. A jelek alapján legalább is erre következtetett a Kaspersky Lab's Global Research & Analysis Team-je a „Lazarus under the hood”<sup>10</sup> című elemzésében. A Kaspersky Lab munkatársai ugyanis azt figyelték meg, hogy a csoporton belül létrejött egy általuk Bluenoroff- nak elnevezett csoport, amely kifejezetten pénzügyi intézményeket, bankokat, kaszinókat kezdett el támadni főleg Ázsiában, de próbálkoztak Európában is.

A Bluenoroff csoport tevékenységének ismertetése előtt szót kell ejtenünk a bangladesi Bangladesh Bank ellen elkövetett csalásról, amelyet 2016 februárjában követtek el ismeretlen hackerek, akik internetes csalással 81 millió dollárt tulajdonítottak el a banktól. A történetek rekonstruálása során megállapítást nyert, hogy ismeretlen elkövetők a SWIFT<sup>11</sup> rendszerrel összekapcsolt szerveret feltörve saját számlájukra kívántak utalni több részletben mintegy 900 millió dollárt a Bangladesh Bank Szövetségi Tartalék Bank New Yorki fiókjánál (Federal Reserve Bank of New York) vezetett számlájáról. A szövetségi banknál feltűnt a tranzakció szokatlan mérete és leállították az utalásokat, de így is sikerült a támadóknak 81 millió dollárt megszerezniük.

Az akciót követően több elemzés is napvilágot látott, amelyek szerint az elkövetők a Lazarus csoporthoz köthető hackerek voltak. A megállapítást arra alapozták, hogy a Novetta által már Észak-Koreához kötött kódrészleteket és algoritmusokat fedeztek fel a Bangladesh Bank elleni támadásnál hátrahagyott programokban.<sup>12</sup>

A Kaspersky Lab a bangladesi incidenst követően a korábbi támadásokból származó vírusmintákat felhasználva kártevőfigyelő rendszerén keresztül fokozott figyelemmel kísérte az ilyen jellegű támadásra utaló jeleket, így bukkant rá 2016 augusztusában egy közelebről meg nem nevezett délkelet-ázsiai bank ellen éppen folyamatban lévő támadásra. A Kaspersky Lab munkatársai felvették a kapcsolatot, majd közel egy évig együttműködtek a bank IT szakembereivel abból a célból, hogy

---

<sup>10</sup> Kaspersky Lab's Global Research & Analysis Team. "LAZARUS UNDER THE HOOD." Securelist. April 03, 2017. Accessed May 22, 2017. <https://kas.pr/ix6C> (Letöltés ideje: 2017. 05. 20.)

<sup>11</sup> A Society for Worldwide Interbank Financial Telecommunication (Nemzetközi Bankközi Pénzügyi Telekommunikációs Társaság) és tagjai által működtetett, olyan nemzetközi elektronikus kommunikációs rendszer, amelyen keresztül annak tagjai egymás között bankközi üzenetforgalmat bonyolítanak, és amely rendszer segítségével fizetéseket teljesíthetnek, illetőleg elszámolhatnak egymással. A SWIFT megbízások a bankközi ügyletek fejlett rendezési módja, célja az ügyletek lehető legnagyobb fokú automatizálása és ezzel a lehető legrövidebb idő alatti ügyintézés. Egy banki átutalás klasszikus adatai, mint a feladó és a címzett fél banki azonosítói, az átutalás jogcíme, a szolgáltatási jelzések (átutalási díj, üzenettípus stb.) mind kódolva kerülnek rögzítésre és továbbításra. Például: a bankokat a részükre kiosztott SWIFT-kóddal azonosítják. <https://www.swift.com/about-us/discover-swift>, (Letöltés ideje: 2017. 05. 31)

<sup>12</sup> Shevchenko, Sergei. "BAE Systems Threat Research Blog." Cyber Heist Attribution. January 13, 2016. Accessed May 28, 2017. <http://baesystemsai.blogspot.hu/2016/05/cyber-heist-attribution.html>. (Letöltés ideje: 2017. 05. 28.)

az elkövetők kilétét felderíthessék, a bűncselekményt megszakíthassák, illetve a támadás eszközeit és módszereit mélységében megismerhessék.<sup>13</sup>

A Lazarus (Bluenoroff) csoport felkészültségének és képességeinek reális értékelése érdekében rövidített formában, a technikai részletek mélységekre menő ismertetése nélkül, tekintjük át, mit tapasztaltak az incidens kivizsgálása során.

Először is a vizsgálat megkezdését követően szinte azonnal azt észlelték, hogy a támadók felfedezték az ellenük irányuló nyomozást és megkezdték az árulkodó nyomok helyreállíthatatlan eltüntetését. A sietség miatt azonban nem sikerült mindent megsemmisíteniük és jelentős mennyiségű nyom maradt utánuk, amelyekből majdnem teljes mértékben sikerült az esemény rekonstruálása és a használt eszközök beazonosítása.

### **Kártevők hasonlósága**

A bangladesi támadáshoz hasonlóan a támadók itt is a SWIFT rendszert támadták meg. A SWIFT rendszer működtetői a bangladesi támadást követően javítást adtak ki a szoftverhez. Ez azonban nem rettentette el a Lazarus csoportot, mert a szoftver működését gondosan tanulmányozták és egy úgynevezett patch<sup>14</sup> fájlt készítettek hozzá, amellyel módosították az egyik dinamikus könyvtárt (liboradb.dll), így a beépített plusz védelmet kikerülve ismét képesek voltak a saját programjukkal a SWIFT szoftvert manipulálni. Az eredeti fájlról másolatot készítettek abból a célból, hogy a feladatuk végeztével visszaállíthassák az eredeti állapotot, elkerülve így a módszerük leleplezését. A SWIFT szerveren találtak még egy távoli adminisztrációs eszközt,<sup>15</sup> amely szinte teljesen megegyezett a bangladesi támadásnál használt szoftverrel. Ez a program azonban nem közvetlenül kapcsolódott a C<sub>2</sub>szerverhez<sup>16</sup>, hanem a szegmens egy másik gazdagépével kommunikált, amely átjátszóként szerepelt a kártevő és C<sub>2</sub>szerver között. Ehhez a másik gazdagépen egy saját fejlesztésű célprogramot telepítettek. A kommunikáció ilyen formában történő megvalósításával elkerülték a kompromittált SWIFT szerver gyanúsnak tűnő kommunikációját a külvilág felé, mert úgy számoltak, hogy a helyi kapcsolatok kevésbé tűnnek fel a rendszergazdáknak.

Több más hasonlóság mellett figyelmet érdemelt még az API hívások egyedi módja, valamint a programbetöltő programok (loader) egyedi működése is. Ezek ismertetésére a szakértői vizsgálatok<sup>17</sup> megakadályozására tett lépések bemutatásánál még visszatérünk.

---

<sup>13</sup> Kaspersky Lab's Global Research & Analysis Team. "LAZARUS UNDER THE HOOD." Securelist. April 03, 2017. 4. oldal Accessed May 22, 2017. <https://kas.pr/ix6C> (Letöltés ideje: 2017. 05. 20.)

<sup>14</sup> Hibajavító program, illetve hibajavító csomag.

<sup>15</sup> RAT Remote Administration Tool, lehetővé teszi egy távoli kezelőnek, hogy úgy kezeljen egy rendszert mintha ahhoz fizikai hozzáférése lenne.

<sup>16</sup> Command &Control szerver. A kártevő programot ezen a szerveren keresztül kapja az utasításokat.

<sup>17</sup> Anti Forensic Technics

### Szakértői vizsgálatok eredményei:

- A vizsgálatok során a SWIFT rendszerhez kapcsolódó szerveren kívül a bank más IT rendszerein is fertőzés nyomait találták. A megsemmisített programokat nem sikerült helyreállítaniuk, de találtak ezekre utaló egyedi fájlneveket tartalmazó hivatkozásokat, amelyek megerősítették a kapcsolatot a Bangladesh Bank támadóival.
- A támadók hét hónapon keresztül tartózkodtak benn a bank informatikai rendszerében. Az első nyomok időben egybeestek a bangladesi támadás idejével. Ez arra enged következtetni, hogy egyszerre több bankot is ostrom alá vettek.
- Hasonlóan a bangladesi esethez, a felderített kártevőkben a C:\Windows és a C:\MSO10 könyvtárak fixen kódolva voltak.
- A programokat közvetlenül a támadás előtt fordították, ami arra enged következtetni, hogy célirányosan az adott rendszerhez szabták őket.
- A legtöbb modul szolgáltatásként Rendszergazda, illetve System jogokkal futott.
- A hackereknek nem sikerült mindent terveik szerint végrehajtani, mert a vizsgálat során több alkalmazott programra, rendszerösszeomlásra utaló nyomot azonosítottak.
- A támadók jellemzően munkaidőn túl, illetve munkaszüneti napokon dolgoztak, hogy elkerüljék a lebukást.
- A támadás első fázisában kezdetlegesnek tűnő backdoor (hátsó ajtó) programokat használtak, amelyek esetleges elvesztése nem okozna különösebb kárt számukra. Amennyiben ezen a hátsó ajtón keresztül egy értékes áldozatra bukkantak az egyszerű programot az értékes, titkosított, egyedi fejlesztésű programjukra cserélték.
- Kísérletezés közben hibakeresést végeztek és a Windows Sysinternals Sysmon<sup>18</sup> alkalmazását használták. Szerencsére a Sysmon logfájljait elfelejtették kitörölni így az sok hasznos információval szolgált a vizsgálatot végzőknek. Ezt a hibát a bangladesi támadásnál is elkövették.
- Találtak egy kifejezetten a SWIFT rendszer feltörésére használt programot, amely a már említett bizonyítékok alapján egyértelműen a Lazarus (Bluenoroff) csoportéhoz köthető.
- Rábukkantak egy billentyűzetfigyelő programra, amelyet egy titkosított konténerben tároltak, és amelyet csak egy másik gazdagépről indított jelszóval védett betöltő (loader) program tudott futtatni és a billentyűzetfigyelő program logfájlját is ez az alkalmazás gyűjtötte be és továbbította az átjáró állomáson keresztül a tulajdonosának.
- A támadók előszeretettel a 443-as végű portokat részesítették előnyben (6443,8443,443).

---

<sup>18</sup> Windows Sysinternals System Monitor (Sysmon) egy Windows rendszerszolgáltatás és eszközmeghajtó, amely a telepítést követően a memóriában marad, az újraindításokat követően is, és figyelemmel kíséri valamint rögzíti a Windows eseményeit. Részletes információval szolgál többek között a folyamatok létrehozásáról, a hálózati kapcsolatokról, fájlműveletekről, és a registryben történt változásokról. Technet Microsoft, <https://technet.microsoft.com/en-us/sysinternals/bb545027.aspx> (Letöltés ideje: 2017. 05. 31.)

- A hackerek kísérletezését a SWIFT rendszer adatbázisával 2016 augusztusától több összeomlás is kísérte, amelyeket a program rögzített.
- A támadóknak nem volt vizuális kapcsolatuk a célgépekkel, mindent terminál kapcsolatokon keresztül az átjátszó munkaállomásokat felhasználva intéztek és ennek nyoma maradt a rendszernaplókban.
- A legelső terminál kapcsolatot a bank nyilvános weboldalának otthont adó webszerveren találták. A webszerver és a SWIFT szerver azonos hálózati szegmensbe volt szervezve. Ebből valószínűsíthető, hogy a webszerveren keresztül jutottak be a rendszerbe, ezt fertőzték meg először.

### A támadás időbeni lefolyása

Érdeemes a támadás időbeni lefolyását megvizsgálni ugyanis jól szemlélteti, hogy a hackerek mennyi időt és energiát áldoztak az akcióra. Már ez a körülmény is azt a feltételezést erősíti, hogy nem amatőrökről, nem közönséges bűnözőkről beszélünk, hanem egy nagyon felkészült, stabil háttérrel rendelkező szervezetről.

Ssz.	Dátum	Tevékenység leírása
1.	2015. szeptember 29.	Telepítették a bank nyilvános webszerverét, amelyen keresztül a támadók később bejutottak
2.	2015. december 15-19.	A feltört webszerverről kapcsolatot létesítettek a SWIFT szerverrel
3.	2016. január 08.	A szomszédos gazdagépekre feltelepítették az átjátszó és betöltő szoftvereket.
4.	2016. január 18.	További szoftvereket telepítettek a szomszédos gazdagépekre, amelyekkel a SWIFT rendszert manipuláló szoftvert irányították
5.	2016. január 29.	Megkezdték a SWIFT rendszer tesztelését
6.	2016. február 04.	Elkészült a SWIFT rendszerhez a patch fájl, majd telepítették. Ugyanekkor kezdetét vette a Bangladesh Bank akció
7.	2016. február 29.	A támadók felfüggesztették tevékenységüket.
8.	2016. április 08.	A támadók visszatértek, és billentyűzetfigyelőt telepítettek a SWIFT szerverre.
9.	2016. május	A SWIFT Alliance javítást adott ki a szoftverhez.
10.	2016. július 09-11.	Elkészült az újabb patch fájl, és a támadók tesztelték a működését.
11.	2016. augusztus 04.	A támadók helyreállították a SWIFT rendszerrel megszakadt kapcsolatukat
12.	2016. augusztus 10-12.	Hátsó kapuk sorát telepítették a SWIFT szerverre
13.	2016. augusztus 16-18.	Egy speciális kártevőt juttattak be a SWIFT program memória területébe (dll injection)
14.	2016. augusztus 18-22.	A Kaspersky Lab riasztása, kezdetét veszi az együttműködés a bank IT állományával
15.	2016. augusztus 22-23.	A támadók igyekeztek eltüntetni a nyomaikat

2.ábra: A Kaspersky Lab információi alapján szerkesztette a szerző<sup>19</sup>

<sup>19</sup> Kaspersky Lab's Global Research & Analysis Team. "LAZARUS UNDER THE HOOD." Securelist. April 03, 2017. 10. oldal Accessed May 22, <https://kas.pr/ix6C> (Letöltés ideje: 2017. 05. 20.)

## Szakértői vizsgálat elleni védelmi technikák<sup>20</sup>

A Kaspersky Lab munkatársai vizsgálatuk során számos olyan intézkedés nyomára bukkantak, amelyekkel a támadók megpróbálták megnehezíteni, vagy lehetetlenné tenni a hátrahagyott nyomaik bizonyítékként történő felhasználását. Számos ezek közül csakis a Lazarus (Bluenoroff) csoportra jellemző, így ezek, ha közvetetten is, de az ő bűnösségüket igazolják.

Az első, amely korábban már részben említésre került, az a kártevők különböző felelősségi körébe tartozó hálózati szegmensek közötti megosztása. Az általános gyakorlat szerint a szakértők csak a fertőzött rendszert vizsgálják és így elkerüli figyelmüket a kártevők másik fele, így lényeges információktól esnek el, nem beszélve arról, hogy a támadók újabb akcióját is megkönnyíthetik. A tanulság ebből az, hogy ilyen esetekben a teljes rendszert kell vizsgálni.

A másik tanulság, hogy a fertőzés, vagy az abnormalis tevékenység észlelése esetén nem a cég email szerveréről kell a szakértőkkel konzultációt folytatni, ugyanis a támadók ezt figyelemmel kísérik és idő előtt tudomást szerezhetnek a tervezett vizsgálatról, mint ez történt ebben az esetben is. A hackerek kellően körültekintőek voltak és az IT állomány levelezését folyamatosan figyelemmel kísérték.

Harmadik figyelmet érdemlő védelmi intézkedés részükről a kártevők jelszóval történő védelme. Ennek is egy egészen sajátos módját alkalmazták. Mégpedig azt, hogy a kártevőt egy titkosított fájlkonténerben tárolták, amelyet az installer csak a paraméterként megadott jelszó felhasználásával tudott kibontani.

A negyedik rájuk jellemző módszer az API<sup>21</sup> hívások egyedi módja. A Lazarus csoport programozói a meghívni kívánt eljárás nevét megváltoztatják és egy saját, külön beépített algoritmus alkalmazásával futás közben közvetlenül az eljárás meghívása előtt alakítják vissza az eredeti névre. Például a meghívni kívánt eljárás neve: `GetProcAddress()`, ezt ők `G!e!t!P&r@#c:e>s<A&d@d&r{e#s<s-re` alakítják. Ennek azért van jelentősége, mert egyes kártevő kereső szoftverek a vizsgált program viselkedése alapján próbálják kiszűrni a gyanús programokat. Több tényezőt is mérlegelnek, például honnan és mikor indul a program, van-e látható felülete, milyen API-kat hív meg és így tovább. A sajátos API hívási módszerrel igyekeznek elkerülni, hogy programjuk felhívja magára a figyelmet.

## Betörés a rendszerbe

A bank nyilvános weboldalának szerverét 2015. szeptember 09-én telepítették. Ezt követően megbíztak egy Pentester<sup>22</sup> céget azzal, hogy vizsgálja meg a weboldal, illetve a webszerver biztonságát. A tesztelő számos ellenőrzést hajtott végre, a feltárt

---

<sup>20</sup> Anti-forencics technics: kísérlet a bizonyítékok meglétének mennyiségének, minőségének olyan irányú megváltoztatására, amely megnehezíti, vagy lehetetlenné teszi a bizonyítékok összegyűjtését, illetve felhasználását.

<sup>21</sup> API Application Programming Interface. Esetünkben a Windows rendszer statikus és dinamikus könyvtáraiban (dll fájlokban) tárolt eljárásai, amelyeket más programok meghívhatnak. Előnye, hogy a nyilvánosságra hozott eljárás hívási formák betartásával feladatokat hajthatunk végre anélkül, hogy a belső működéssel foglalkoznunk kellene. Lényegesen lerövidíti a programozási időt és programozási nyelv független.

<sup>22</sup> Penetration Tester rövidítve: Pentester, behatolás tesztelő, ellenőrző

hiányosságokat javította, az ellenőrzés során feltelepített egy C99 shell<sup>23</sup> elnevezésű PHP nyelven írt kártevő programot, azzal a céllal, hogy tesztelje a védelmi rendszer működését. A teszt befejeztével ezt letörölte. A vizsgálat valószínűsíti, hogy a bank rendszerébe történő betörés ennek a kártevőnek a felhasználásával történt. Az elemzők nem tartották lehetetlennek, hogy a feltöltött shellt már eleve manipulálta a Lazarus csoport így az a telepítéskor értesítette őket és a segítségével a szerver felett át tudták venni a hatalmat. Ez azonban csak feltételezés. Az bebizonyosodott, hogy a tesztelő szakember jó szándéka kétségtelen, ennek ellenére a Lazarus csoport valamilyen módon vissza tudott élni ezzel a programmal és bejutott a webszerverre úgy, hogy ezt a tesztelők nem vették észre.

## Európai áldozatok

A Kaspersky Lab munkatársai a már említett incidenseket követően továbbra is figyelték a bankok elleni támadásoknál használt kártevők felbukkanását. Így szembesültek azzal, hogy 2017 januárjában több európai pénzintézményt is támadás ért. A cég munkatársai biztonságos úton felvették a kapcsolatot az érintett bankok IT személyzetével és sikerült elérniük, hogy a rendszereket leállítsák és a merevlemezekről képfájlokat készíthessenek. Ezek elemzése során számos olyan kártevőt sikerült azonosítaniuk, amelyekről már korábban sikerült bizonyítani, hogy a Lazarus (Bluenoroff) csoporthoz köthetők.

Az alábbiakban az egyik lengyelországi bank elleni támadást kívánom nagyvonalakban, a technikai részletek nélkül bemutatni. Az akció több szempontból is érdekes, és mint látni fogjuk számos tanulsággal szolgálhat.

A lengyelországi bank esetében az első gazdagép úgy fertőződött meg, hogy valaki az operációs rendszerrel együtt települő Internet Explorerrel meglátogatta a Lengyel Pénzügyi Felügyelet hivatalos honlapját<sup>24</sup>, amelyet már előzőleg egy ártalmas javascripttel megfertőztek a támadók. Az IE cache-ben tárolt fájl alapján rekonstruálni lehetett a weboldalon elhelyezett ártalmas kódot. Ez a script egy ugyancsak megfertőzött szerverről letöltött egy speciális módon összeállított „swf” kiterjesztésű flash fájl volt, amely a Flash Player hibáját kihasználva egy ugyancsak megfertőzött másik szerverről letöltötte a kártevők első csoportját. Érdekes, hogy a flash fájlban és a támadásban érintett többi kártevőben is az elemzők gyenge orosz helyesírású szövegeket és utasításokat találtak, amiből arra következtettek, hogy a hackerek megpróbálták az oroszokra terelni a gyanút. Fokozni kívánták a gyanút azzal, hogy a programokat egy orosz fejlesztésű Enigma nevű szoftverrel tömörítették.

Az első gép megfertőzése után tovább haladtak, és megfertőzték a backup szervert és még további két gazdagépet. A hackerek tevékenységének elemzése során megállapították, hogy eddig ismeretlen módon sikerült az először megtámadott gazdagépen a hálózat legmagasabb felhasználói jogát megszerezniük, és ennek birtokában már gyakorlatilag minden további gazdagépen teljes hozzáféréssel bírtak. A vizsgálatot végzők megállapították, hogy a Lazarus (Bluenoroff) csoportra

---

<sup>23</sup> A C99 shell egy PHP nyelven írt kártevő, amely felkerülve a webszerverre hátsó ajtót nyit a támadóknak és lehetővé teszi, hogy azok a PHP-t futtató account jogosultságával átvegyék a szerver feletti irányítást.

Keane, Justin C. Klein: PHP Malware C99 Shell. "Mad Irish . net." Mad Irish, Accessed June 01, 2017. <http://www.madirish.net/241>. (Letöltés ideje: 2017. 05. 20.)

<sup>24</sup> [https://www.knf.gov.pl/opracowania/sektor\\_bankowy/index.html](https://www.knf.gov.pl/opracowania/sektor_bankowy/index.html) (2017.05.20.)

jellemzően a kártevőket ugyanazokba a könyvtárakba másolták, mint korábban a bangladesi bank támadásának esetében. A hálózati forgalom elemzése és néhány titkosított konfigurációs fájl visszafejtése után sikerült további négy C<sub>2</sub> szervert is azonosítaniuk. Sajnos a jelszavak hiányában csak a titkosított fájlok egy részét sikerült visszafejteniük így nem sikerült minden kártevőt azonosítaniuk, illetve elemezniük. A szakértők tanulságként megállapították, hogy amennyiben a felhasználók számítógépére telepítették volna a flash playerhez kiadott aktuális frissítéseket, a fertőzési kísérlet nem járt volna sikerrel.

### **További áldozatok**

A lengyelországi támadást is az úgynevezett „watering hole” támadások közé sorolják. Az egyébként is veszélyes támadási mód súlyát növelte, hogy egy állami weboldal esett a támadók áldozatául. A Kaspersky Lab munkatársai ebben az irányban folytatva tovább a vizsgálatot még további országokat találtak, ahol a támadók hasonló taktikát követve próbálták bejutni az egyes bankok rendszerébe. A teljesség igénye nélkül: Oroszországi Föderáció, Ausztrália, India, Nigéria, Peru, Mexikó, Uruguay.

A Kaspersky Lab tapasztalati alapján nem csak a bankok kerültek a Lazarus csoport célkeresztjébe, hanem számos egyéb más pénzügyi intézmény is, így például tőzsdék, fizetésre használatos virtuális eszköz<sup>25</sup> előállító cégek, kaszinók.

### **Összegzés**

Írásomban igyekeztem az elektronikus sajtóban megjelent publikációk alapján bemutatni Észak-Korea feltételezett kiberstratégiáját, és annak megvalósítására alkalmazható szervezeti egységeit. Nagyvonalakban betekintést kapott az olvasó a kiberstruktúrák felépítésébe és ezek működésébe, majd bemutatásra került néhány érdeklődésre számot tartó művelet, amelyek megfelelően illusztrálták, az ország kiberképességeit. A műveletek elemzése során igazolást nyert, hogy az állami támogatással foglalkozott hackerek célirányosan, esetenként hosszú éveken keresztül készítenek elő egy-egy műveletet, majd ezeket nem ritkán további éveken keresztül folytatják, amíg céljukat el nem érik vagy le nem lepleződnek. Az időközben okozott károk sok esetben gyakorlatilag felbecsülhetetlenek. A bemutatott események jól szemléltetik, hogy az olyan apró biztonsági hiányosságokat kihasználva, mint amilyen egy szoftverfrissítés elmulasztása, milyen óriási károkat képesek okozni az ártó szándékú szakemberek.

Véleményem szerint a Koreai Népi Demokratikus Köztársaság várhatóan nem fog változtatni eddigi stratégiáján, és folytatja majd az alacsony intenzitású, háborús küszöb alatti műveleteit, elsősorban déli szomszédja és az Egyesült Államok, valamint a világ pénzügyi rendszerei ellen. Nagy valószínűséggel nagyobb mértékben és hatékonyabban vonja bele a kibererőit ezekbe a műveletekbe, hiszen láthatóan viszonylag alacsony befektetés mellett nagy hatású műveleteket indíthat úgy, hogy ugyanakkor a saját csapatai ellen nem áll fenn hasonló támadás esélye. Ezzel a stratégiával jelentős anyagi forrásokat köt le ellenségeitől azzal, hogy

---

<sup>25</sup> Angolul: cryptocurrency. Két alapvető kritériuma van. Olyan fizetőeszköz, amely titkosítást használ, a tranzakciók lebonyolítására, és az új egységek létrehozására. Ilyenek például a Bitcoin, Ethereum, Litecoin, Monero stb...



folyamatos védekezésre kényszeríti őket, ugyanakkor az ellene hozott szankciók vajmi kevés hatással vannak a saját országára. Ez a gyakorlatilag büntetlen, folyamatos provokáció felbátoríthatja a vezetést és elképzelhető olyan forгатókönyv, amikor a viszonylagosan kismértékű károkozásról áttérnek a jelentősebb, nagyobb károkat okozó műveletek szervezésére. Ilyenek lehetnek a kritikus infrastruktúrák, atomerőművek, vagy más stratégiaiul fontos létesítmények elleni támadások. A sikeres támadások emberéleteket, vagy nagy anyagi károkat is okozhatnak. Ez még abban az esetben is előfordulhat, ha eredetileg nem ez volt a szándékuk, de a művelet során elveszítik az irányítást a folyamatok felett.

A jövőben, amennyiben nem történik valamiféle éles fordulat az ország politikai életében, vagy a nemzetközi biztonságpolitikai helyzetben számítani kell arra, hogy Észak-Korea kiberharcosai még sok fejtörést okozhatnak az IT szakembereknek szerte a világban.

#### ***Felhasznált irodalom:***

- HARMAT Árpád Péter: "Korea kettészakadásának története." Tortenelemcikkek.hu. 2015. 06. 20. <http://tortenelemcikkek.hu/node/372>. (Letöltés ideje: 2017. 05. 21.)
- CHA, Victor – James Andrew Lewis: North Korea's Cyber Capabilities. North Korea's Cyber Capabilities Center for Strategic and International Studies. 2014. 12. 18, <https://www.csis.org/programs/korea-chair/north-koreas-cyber-capabilities>. (Letöltés ideje: 2017. 05. 20.)
- Novetta: Operation „Blockbuster”, <https://www.operation”Blockbuster”.com/>, <https://www.operation”Blockbuster”.com/wp-content/uploads/2016/02/Operation-”Blockbuster”-Report.pdf>, (Letöltés ideje: 2017. 05. 20.)
- Kaspersky Lab's Global Research & Analysis Team: LAZARUS UNDER THE HOOD. Securelist. 2017.04.03. <https://kas.pr/ix6C> (Letöltés ideje: 2017. 05. 20.)
- The global provider of secure financial messaging services, <https://www.swift.com/about-us/discover-swift> (Letöltés ideje: 2017. 05. 20.)
- Windows Sysinternals System Monitor (Sysmon), Technet Microsoft, <https://technet.microsoft.com/en-us/sysinternals/bb545027.aspx> (Letöltés ideje: 2017. 05. 31.)
- KEANE, Justin C. Klein: PHP Malware C99 Shell. "Mad Irish . net." Mad Irish, <http://www.madirish.net/241>. (Letöltés ideje: 2017. 05. 20.)
- KNF – Komisja Nadzoru Finansowego, [https://www.knf.gov.pl/opracowania/sektor\\_bankowy/index.html](https://www.knf.gov.pl/opracowania/sektor_bankowy/index.html) (Letöltés ideje: 2017. 05. 20.)
- Ryan Sherstobitoff and Itai Liba, McAfee® Labs and James Walter, Office of the CTO: Dissecting Operation Troy: Cyberespionage in South Korea, McAfee Labs, 2013. <https://www.mcafee.com/error->

pages/404.aspx?url=https://www.mcafee.com/kr/resources/white-papers/wp-dissecting-operation-troy.pdf (Letöltés ideje: 2017. 05. 21.)

- "Indiana University Indiana University Indiana University." What is a Master Boot Record (MBR)? Accessed June 09, 2017. <https://kb.iu.edu/d/aijw>. (Letöltés ideje: 2017. 05. 20.)
- Shevchenko, Sergei. "BAE Systems Threat Research Blog." Cyber Heist Attribution. 2016.01.13. <http://baesystemsai.blogspot.hu/2016/05/cyber-heist-attribution.html> (Letöltés ideje: 2017. 05. 20.)
- "North Korea's Cyber Operations: Strategy and Responses." North Korea's Cyber Operations: Strategy and Responses Center for Strategic and International Studies. November 23, 2015. <https://www.csis.org/events/north-korea%E2%80%99s-cyber-operations-strategy-and-responses> (Letöltés ideje: 2017. 05. 20.)
- "What Do We Know About Past North Korean Cyber Attacks and their Capabilities?" What Do We Know About Past North Korean Cyber Attacks and their Capabilities? Center for Strategic and International Studies, <https://www.csis.org/analysis/what-do-we-know-about-past-north-korean-cyber-attacks-and-their-capabilities>. (Letöltés ideje: 2017. 05. 20.)

**A SZERVEZETI INFORMÁCIÓBIZTONSÁGI FOLYAMATOK  
MONITOROZÁSA ÉS A VEZETŐI DÖNTÉS TÁMOGATÁSA KULCS  
TELJESÍTMÉNYMUTATÓK SEGÍTSÉGÉVEL I.**

*Az információbiztonság rendszerelméleti megközelítése*

---

**Bevezetés**

Manapság már axiómaként fogadjuk el, hogy a XXI. század erőforrásai között az adatok és az információk kiemelkedő szerepet töltenek be. Az üzleti, szervezeti folyamatok elképzelhetetlenek a megfelelő időben, megfelelő helyen, megfelelő mennyiségben, megfelelő szinten és minőségben, illetve kellő relevanciaszint mellett rendelkezésre álló adatok és információk nélkül. Az adatok, információk felértékelődésével párhuzamosan megnövekedett azoknak a kibertámadásoknak a száma, amelyek célja többek között a szervezeti adatok megszerzése, zavarkeltés az adatfolyamban, illetve az adatfolyam akadályozása, az adatok módosítása/manipulálása. Annak érdekében, hogy a szervezeteknél minimalizálni lehessen az eredményes támadások számát, szükség van a szervezeti, különösen a(z információ)biztonsági folyamatok monitorozására. A folyamatok monitorozása lehetőséget ad a vezetői döntések támogatására is, mivel az ellenőrzési (monitorozási) pontokról származó adatok és információk révén olyan kulcsmutatószámok képezhetők, amelyek könnyen áttekinthetővé teszik a szervezet, mint rendszer nem csak információbiztonsági folyamatait.

**A szervezet, mint rendszer**

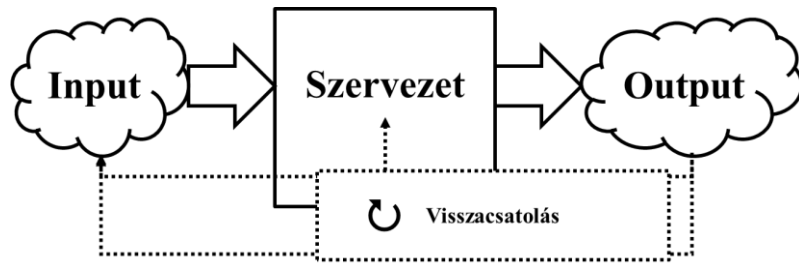
A rendszerre megalkotott és általánosan elfogadott definíció nincs<sup>1</sup>, tanulmányomban Zvikli<sup>2</sup> definícióját fogadom el, mely szerint „A rendszer különféle tulajdonságú elemek (összetevők) meghatározott módon rendezett halmaza, amelyek egymással jól definiálható relációkkal kapcsolódnak és ezáltal az egészre kiterjedő olyan egységet alkotnak, amely egység az adott célok elérését, az azokhoz szükséges funkciók elvégzését biztosítja a környezetéhez is illesztve, integrált egészként”. A rendszer egyszerű értelmezésénél<sup>3</sup> megkülönböztetünk inputot, outputot és magát a rendszert (tanulmányom fókuszában szervezetet), ugyanakkor hiányzik a visszacsatolás, a rendszer által előállított outputok értékelése, így ezzel kiegészítve közlöm az 1. ábrát.

---

<sup>1</sup> KINDLER József – KISS István: Rendszerelmélet. Válogatott tanulmányok. Budapest, Közgazdasági és Jogi Könyvkiadó, 1971.

<sup>2</sup> ZVIKLI Sándor: Rendszerelemzés 1. Győr: Széchenyi István Egyetem, 2009:6.

<sup>3</sup> POKORÁDI László: Rendszerek és folyamatok modellezése. Debrecen, Campus Kiadó, 2008.



**1. ábra: A rendszer értelmezése az input, output, visszacsatolás segítségével**  
(saját szerkesztés)

Megjegyzem, hogy az elsősorban műszaki megközelítésű rendszerelméleti szakirodalom megkülönböztet negatív és pozitív visszacsatolást. Zvikli<sup>4</sup> megfogalmazásában a negatív visszacsatolás „a rendszer működésére előírt, elvárt kimenetek betartására szabályoz, azaz bizonyos dinamikus egyensúlyi állapotot kíván fenntartani”, a pozitív visszacsatolás pedig „nem az eredeti egyensúlyi állapot fenntartása az irányítás célja, hanem – megteremtve ezáltal egy újabb egyensúlyi állapot létrehozatalának feltételeit – éppenséggel attól való eltávolodás”.

Tanulmányomban a rendszerre úgy tekintek, mint egy, vagy több szempont alapján a környezetből leválasztott és körülhatárolt dologra. A szempont(ka)t a lehető legtágabban lehet értelmezni, s ez alapján megkülönböztethetők többek között az alábbi rendszerek:

- (marketing) információs rendszer
- a vállalat, szervezet, mint rendszer
- az emberi szervezet, mint rendszer
- egészségügyi rendszer
- gazdasági rendszer
- jogrendszer
- mezőgazdasági rendszer
- oktatási rendszer
- pénzügyi rendszer
- szociális ellátó rendszer
- társadalmi rendszer
- vállalatirányítási rendszer
- stb...

### ***Input és output***

A rendszer bemenetét nevezzük inputnak, kimenetét pedig outputnak. Egymáshoz kapcsolódó rendszerek esetében az egyik rendszer outputja lehet (de nem minden esetben) egy másik rendszer inputja, kapcsolódásuk valamilyen rendszerinterfészen keresztül történik. Egy rendszernek lehet egy-több inputja és egy-több outputja.

---

<sup>4</sup> ZVIKLI Sándor: Rendszerelmélet 1. Győr: Széchenyi István Egyetem, 2009 p. 54.

## ***Erőforrások***

Gyakorlati tapasztalati úton feltételezhető, hogy a rendszer nem önállóan működik, hanem interakciót folytat részint a környezetével, részint a környezetében levő egyéb rendszerekkel. Az interakciók során olyan input-output folyamatok zajlanak, amelyekben többek között az alábbi erőforrások cserélődnek egymással:

- anyag
- energia
- információ (tapasztalat, tudás)
- pénz
- humán erőforrás

A rendszereknek természetesen vannak/lehetnek saját belső erőforrásaik is. Ezek közé tartozhat többek között:

- idő (ami valamely tevékenység elvégzéséhez szükséges)
- humán erőforrás (a szervezet munkavállalói)
- know how, innováció
- stb...

## ***Az erőforrások értéke***

Az erőforrások értéke számos tényezőtől függhet. Az érték gazdaságfilozófiai és tapasztalati meghatározásában a környezet és a rendszer egyaránt részt vehet. A közgazdaságtanban az érték fogalmának és természetének meghatározásával többek között Jevons<sup>5</sup>, Menger<sup>6</sup> és Walras<sup>7</sup> foglalkozott. Meglátásuk szerint a javak mértéke azok hasznosságától függ (szubjektív ítélet), ellentétben Ricardoval<sup>8</sup>, aki úgy gondolta, hogy a javak értéke és az ára az előállításukhoz szükséges munka mennyiségének a függvénye. A fontosabb, fentebb nevezett külső erőforrások értékének meghatározása során felmerülő kérdések:

- anyag
  - Mennyibe kerül az előállítása, illetve nyersanyagok esetében a kitermelése/bányászata?
  - Az előállítása során milyen technológiákat kell használni?
  - Ezek a technológiák milyen hatással vannak a bioszférára?
  - Az anyag élő (növény, gomba, állat), halott (pl.: levágott állat, bútorlapnak feldolgozott fa), vagy élettelen (pl.: vas, gépelem, vegyi anyag, víz)?
- energia
  - Véges, vagy megújuló?
  - Előállításának és a fogyasztóhoz (értsd: az azt felhasználó rendszerhez) juttatásának mennyi a költsége?
  - Környetkímélő, vagy környezetszennyező?

---

<sup>5</sup> JEVONS, William Stanley: Money and the Mechanism of Exchange. New York, Okitoks Press, 2017., illetve The Theory of Political Economy. Basingstone, Palgrave Macmillan, 2013.

<sup>6</sup> MENGER, Carl: Principles of Economics. Auburn, Ludwig von Mises Institute, 2007.

<sup>7</sup> WALRAS, Léon: Elements of Pure Economics. Abingdon, Routledge, 2010.

<sup>8</sup> ICARDO, David: The Principles of Political Economy and Taxation. London, J. M. Dent & Sons Ltd., 2004.

- Kiváltható más energiával (alternatív megoldások)?
- Felhasználása milyen kárt jelent a bioszférának?
- Felhasználása milyen technikai, technológiai megoldások révén valósítható meg?
- információ
  - Mikor keletkezett?
  - Ki számára releváns?
  - Mennyi az értéke, s mitől függ ez?
  - Milyen az avulási ideje/mértéke?
  - Hogyan dolgozható fel tudássá?
  - Beépíthető a rendszer működésébe? (pl.: tudásalapú szervezet)
- pénz
  - Milyen célra van rá szüksége a rendszernek?
  - Milyen számítások révén határozzák meg a szükséges mennyiséget?
  - Kiváltható? (pl.: barter)
  - Helyettesíthető?
  - Értékálló, vagy folyamatosan inflálódik?
- humánerőforrás
  - Mi a végzettsége?
  - Milyen tapasztalatokkal rendelkezik?
  - Milyen az egészségi állapota?
  - Beszél nyelveket?
  - Tud csapatban dolgozni, vagy inkább magányos harcos?
  - Mennyire fogadja el a változásokat?
  - Milyen gyorsan tud változni?
  - Mennyire elkötelezett a szervezet (és értékrendje), mint rendszer iránt?
  - Fizetése hányszorosa termeli ki egy hónap alatt?

#### *Az erőforrások paraméterei*

Az erőforrásokat értékelésük (értékük megállapítása) mellett különböző paraméterekkel is le lehet írni. Az erőforrások paramétereinek leírása segítheti – többek között – az érték, a tárolási, raktározási körülmények, a felhasználás módjának, az interakciók milyenségének a meghatározását is. Számtalan paraméter létezik, néhány ezek közül:

- avulás, romlás, meghibásodás mértéke, várható ideje
- szubjektív megítélés (pl.: szép, jó, kellemes, hasznos)
- fizikai-kémiai jellemzők:
  - halmazállapot
  - tömeg
  - sűrűség
  - olvadáspont, forráspont
  - tárolhatóság (pl.: energia tárolhatósága)
  - fizikai kiterjedés
  - hőmérséklet
- ár

Az erőforrások paramétereinek egy része nem tekinthető állandónak, hiszen az őt körbe vevő környezet (ilyen aspektusból egy erőforrás is tekinthető rendszernek) folyamatosan változtatja/változtathatja azt (pl.: ár, hőmérséklet).

### *Az erőforrások kezelése*

A rendszerbe érkező erőforrásokat a rendszer saját és/vagy bérelt erőforrásai segítségével "kezelésbe veszi". Ez alatt általában a következő tevékenységeket értjük:

- átereszt magán: a rendszer alapvetően nem változtat semmit a beérkező erőforráson, azt nagyon rövid időn belül kibocsátja magából
- raktározza: a beérkező erőforrást bizonyos ideig a rendszer tárolja, tehát az erőforrás időbeli paraméterén változtat. A gyakorlatban a raktározás feladata az erőforrás megóvása a kedvezőtlen behatásoktól.
- szállítja: a rendszer az erőforrást eljuttatja egyik pontból a másikba. Eközben rendszerint bizonyos idő eltelik, ami kritikus is lehet (pl.: az e-mail a többszörös biztonsági védelemnek köszönhetően csak késéssel jut el a címzetthez). Itt is fontos feladat az erőforrás megóvása a kedvezőtlen behatásoktól. Az erőforrás megóvása más erőforrások bevonása segítségével valósítható meg.
- feldolgozza: a beérkező erőforrás a feldolgozás után eredeti formájában rendszerint már nem áll rendelkezésre, s az esetek jelentős részében a feldolgozás nem visszafordítható folyamat.
- átalakítja: az erőforrás valamilyen transzformáción megy keresztül (pl.: a villamos áram egy gépet hajt meg, így a villamos energiából mozgási és hőenergia keletkezik).
- komplex tevékenység: a fentiek egy részének együttes alkalmazása a rendszeren belül.

### *A rendszer értéke*

A rendszer értéke számos aspektusból vizsgálható. Pénzügyi értelemben egy szervezet, mint rendszer estében lehet beszélni többek között a tulajdonában levő álló- és forgóeszközökről, pénzeszközökről, tudásról (pl.: know how, innováció), illetve goodwillről is. Ez utóbbi – magyar fordításban kb. jó hírnév – a környezet véleményét is tükrözi az adott szervezetről. A goodwill a szervezet és környezete közötti interakciók (pl.: károsanyag kibocsátás, jó ügyek támogatása, green technology alkalmazása) révén folyamatosan alakul, s hatást gyakorol a szervezet által gyártott termékek forgalmára, így bevételére és profitjára.

Gazdasági és filozófiai értelemben egyaránt kérdéses lehet, hogy mit kell (helyesen és etikusan) tenni a rendszer avulásakor, meghibásodásakor. Az egyik álláspont szerint pontosan ki lehet számolni, hogy megéri-e pl. egy gépet javítani, vagy helyette inkább újat érdemes venni. Külön figyelmet érdemel, hogy a termékek jelentős részénél a terméktervezés és design része a szándékos avulás. A termelésből kivont gép rendszerint komoly terhet ró a környezetére, melynek mértékével sajnos még nem kellő komolysággal foglalkoznak. A leselejtezett gépek szakszerű újrahasznosítása mindenképp indokolt. A másik álláspont szerint nem feltétlenül gazdasági megfontolás egy gép megtartása, sokkal inkább ökológiai döntés. Erről többek között Gerken<sup>9</sup> (1993) is írt a 2000-es évek metatrendjeinek vonatkozásában: a menedzserekből ökológusok lesznek.

A rendszer értéke az interakciók számával és milyenségével is jellemezhető. A környezetével, illetve a környezetében levő rendszerekkel való hasznos interakciók révén a rendszer felértékelődik (fontossá válik a vele interakcionálók számára),

---

<sup>9</sup> GERKEN, Gerd: A 2000. év trendjei. Budapest, Akadémiai Kiadó, 1993, p.494

fontos tagja lesz a gazdasági-társadalmi folyamatoknak. Ha csökken egy rendszer értéke, akkor a rendszert felügyelő, vagy azzal foglalkozó szakembereknek megoldást kell találni ennek megállítására. Ez történhet belső erőforrások átcsoportosításával (pl.: vállalatok újraszervezése), vagy külső erőforrások bevonásával. Makrorendszerek esetében – ilyen pl. a gazdasági, az egészségügyi, vagy a pénzügyi rendszer – rendszerint kormányzati beavatkozás szükséges értékcsökkenés esetén (pl.: új törvényeket hoznak, állami szinten fejlesztéseket támogatnak).

A tudásalapú gazdaságban a rendszer értéke a benne felhalmozott és felhasznált tudás mértékével is leírható. Elsősorban nem az információ az érték (mivel az rendszerint rendelkezésre áll), hanem az a szervezeti intelligencia, ami révén a vállalat, mint rendszer az információkból és adatokból hasznos és hasznosítható tudást, tapasztalatot, bölcsességet képez. A szervezeti intelligencia teszi a szervezeti tudást értékké.

### ***Rendszer és alrendszer***

A fentiekben számos példán keresztül láthattuk, hogy bármi lehet rendszer, amit a környezetétől valamilyen szabály alapján elhatárolunk. A rendszereknek szinte kivétel nélkül van alrendszere, s az alrendszernek al-alrendszere, és így tovább. Hogy mit tekintünk rendszernek, s mit alrendszernek, az tőlünk függ. Két rendszer interakciója során nem feltétlenül rendszer-rendszer interakciónál. Elképzelhető rendszer-alrendszer, illetve alrendszer-alrendszer kapcsolódása is.

### ***Rendszer egymáshoz kapcsolódása és a folyamatok***

A rendszer – ahogy arra már többször utaltam – más rendszerekhez és alrendszerekhez kapcsolódik, így részévé válik különböző folyamatoknak. Számatalan folyamat létezik, többek között:

- gyártási/termelési folyamat
- kereskedelmi/eladási folyamat
- beszerzési folyamat
- pénzügyi folyamat
- szállítási folyamat
- a munkaerőkiválasztás folyamata
- a károsanyag-kibocsátás mérésének a folyamata
- az információ átadásának (kommunikáció) folyamata
- stb.

A rendszer legáltalánosabb értelemben vett piacképességét, s bizonyos aspektusban a már korábban tárgyalt értékét az is meghatározza, hogy (1) a többi rendszerhez sorosan és/vagy párhuzamosan és/vagy vegyesen kapcsolódik, illetve (2) ha kiesik a folyamatból, akkor mi történik magával a folyamattal, illetve a többi rendszerrel. A párhuzamosan történő kapcsolódás rendszerint azt jelenti, hogy a rendszer osztozik az inputokban és/vagy a hozzá kapcsolódó rendszerek az outputjaiban. Egy gazdasági példával szemléltetve: egy vállalatnak van több vevője. A vállalatnak, mint rendszernek több outputja van, s az egyes outputok végén egy-egy vevő jelenik meg. A vevői igények a csatlakozás révén visszahatnak a rendszer működésére (mennyit, mikorra, mennyiért, stb. termeljen).



Az információs társadalom hálózati (pókhálós) modelljében az egyes rendszerek (ezek lehetnek pl.: emberek, nonprofit szervezetek, állami szervezetek, vállalatok) számos síkon és aspektusban kapcsolódnak úgy egymáshoz, hogy a kommunikációt az információmegosztás révén tartják folyamatosan fenn. A (kommunikációs) kapcsolatok szövevényes hálójában a szereplőktől alapvetően tisztességes viselkedést várnak el a többiek, de ez az érdeke az adott szereplőnek, mint rendszernek is.

### ***Visszacsatolások***

A visszacsatolások elsődleges feladata tanulmányom fókuszában az, hogy a kimenetekkel (output) kapcsolatban a szervezet információkat szerezzen. A visszacsatolás és annak tartalmi elemzése segítségével következtetni lehet arra, hogy a szervezet a bemeneteken megjelenő inputokkal mit csinált (pl.: feldolgozta, raktározta – lásd fentebb), az input-output között milyen minőségi/mennyiségi változás történt, mik azok a visszacsatolásban megjelenő adatok/információk, melyek miatt szükség van a rendszer, s a benne levő folyamatok átszervezésére, vagy legalábbis módosítására. A visszacsatolás nem csak a bemenet-kimenet relációjában, hanem a rendszeren belül is értelmezhető. Ilyenkor a rendszeren belüli folyamatoknál, az alrendszerek egymáshoz kapcsolódásánál, a belső input-outputoknál, illetve a rendszerinterfészek területén vizsgáljuk meg a visszacsatolást. A visszacsatolás harmadik értelmezésekor – ez különösen a mutatószámok és -indexek képzésekor jelenik majd meg – az inputokon mért adatok (pl.: e-mail-ek száma egy óra alatt), s az outputokon mért adatok (pl.: vírusirtó rendszer által átvizsgált, s fertőzött e-mail-ek száma) összevetése révén következtetnek a rendszer hatékonyságára. Bár a később tárgyalt KPI<sup>10</sup>-ok esetében a rendszer által adott időszakon belül fogadott e-mailek száma is tekinthető KPI-nak, a biztonságot illetően sokkal több információval szolgál az, ha tudjuk, hogy a rendszer a beérkező e-mailek átvizsgálása után mennyit talált vírusosnak, s e kettő hányadosával jellemezzük a rendszer működését.

A visszacsatolásnál szinte valamennyi tudományterületen megkülönböztetnek pozitív és negatív visszacsatolást. A pozitív visszacsatolásnak felerősítő, a negatívnak csillapító hatása van. Szervezeti szinten ez úgy is értelmezhető, hogy mivel a mutatószámok elemzése révén világossá vált, hogy megnövekedett a biztonsági incidensek száma, ezért szigorúbb intézkedéseket kell bevezetni annak érdekében, hogy az incidensek számát csökkenteni lehessen. Az intézkedéseket rendszerint a megfelelő vezetői döntéssel párhuzamosan hozzák meg. Az input-output folyamatok és a visszacsatolás elemzése során arra is lehetőség van, hogy a rendszer értékét (különösen reagálását a környezeti hatásokra, illetve adaptív képességét) határozzuk meg, illetve az intézkedések hatásvizsgálata révén a vezetői döntés megfelelésségét is értékelni lehet. Amikor a rendszer adaptív képességét,

---

<sup>10</sup> KPI (Key Performance Indicator), magyarul kulcs-teljesítménymutató. A KPI feladata, hogy számszerűsítve mutassa meg, hogy mennyire hatékonyan kezeli a vállalat a kulcsfontosságú üzleti célokat. Tanulmányaimban ezt a megközelítést kívánom bemutatni a(z információ)biztonság területén. Véleményem szerint a(z információ) biztonsági folyamatok mérföldköveinél elhelyezett mérőpontok segítségével nem csak a rendszer állapotát lehet nyomon követni, hanem az adatok és az információk feldolgozása révén a nem műszaki-informatikai vezetők is olyan átfogó képet kapnak, ami alapján megalapozottabb, s így hatékonyabb döntéseket tudnak hozni.

illetve a vezetői döntést vetjük össze, akkor abból a feltevésből indulunk ki, hogy a rendszer (szervezeti értelmezésben) nem lehet független a vezetőtől, aki a rendszerrel, annak működéséről, folyamatairól, erőforrásairól rendelkezésre álló adatok és információk alapján „(finom)hangolja” azt. A rendszer hangolásában (általánosságban: fejlesztésében, folyamatainak újraszervezésében, stb.) tud nagy segítséget nyújtani a KPI módszertana.

### **A(z információ)biztonság és az adatérték értelmezései**

A biztonság természetét<sup>11</sup> az egyének, a csoportok (ide tartoznak a szervezetek is), a nemzetállamok, illetve a nemzetközi rendszerek/szervezetek szintjén lehet értelmezni. Supan<sup>12</sup> hat biztonsági aspektust nevez meg, úgymint: személyi biztonság, információbiztonság, műveleti biztonság, környezeti biztonság, hírnév biztonság, fizikai biztonság. A biztonságról alkotott ismereteink Brooks<sup>13</sup> szerint a kriminológia, a létesítményüzemeltetés, a nyomozás, a kockázatkezelés, az üzletfolytonosság-menedzsment, az iparbiztonság, a fizikai biztonság, a védelem, a biztonságmenedzsment, a biztonságtechnika, a jog, illetve a tűzvédelem kategóriákban jelennek meg a legmarkánsabban. A szakirodalom<sup>14</sup> a biztonság megközelítései közül a korábban már bemutatott rendszer-megközelítést megfelelőnek tartja, s számos előnyét nevezi meg, úgymint:

- egyszerűbb és hatékonyabb a kommunikáció a közös szó- és fogalomhasználatnak köszönhetően
- segítséget nyújt a biztonsági program architektúrájának meghatározásához
- felhívja a figyelmet a rendszertervezési elvekre a felsővezetői támogatás kialakítása érdekében
- az átlagtól/megszokottól való eltérést egy közös gondolati alap (filozófia) révén értelmezik
- elősegíti és támogatja a kommunikációt a hagyományos és funkcionális határokon keresztül
- előmozdítja a biztonsági menedzsment szempontjait a már kiforrott elképzelések elfogadása révén
- rugalmasságot biztosít az egyébként merev keretek között
- lehetővé teszi a megbízhatóságot, a karbantarthatóságot és a szükséges frissítések kezelését
- alapot szolgáltat a meglévő rendszerekhez tartozó hézagok elemzéséhez
- támogatja a teljesítményt és a hatékony forráselosztást
- támogatást nyújt a (felső)vezetésnek

A(z információ)biztonság (köz)gazdasági értelmezésénél többféle aspektust célszerű ismertetni. A digitális korban az adatok, információk, s a belőlük képzett

---

<sup>11</sup> ROTHSCHILD, Emma: What Is Security? Daedalus, Vol. 124, No. 3, The Quest for World Order, Summer, 1995.

<sup>12</sup> SUPAN, Joel Jesus M.: The art and science of security. Bloomington, Trafford Publishing, 2012.

<sup>13</sup> BROOKS, David J. (2009): What is security: definition through knowledge categorisation. Security journal 23 (3), 2009.

<sup>14</sup> Pl.: SMITH, Clifton L. – BROOKS, David J.: Security science. The Theory and Practice of Security. Amsterdam, Elsevier.

tudás, tapasztalat, bölcsesség a modern szervezetek, mint tanulószervezetek számára gyakran a pénznel is többet érő erőforrás. A szervezet, mint rendszer bemutatásánál már utaltam az inputok értékére, s két klasszikus közgazdasági megközelítést mutattam be (hasznosság, előállításához szükséges munka). Egy 2017 elején összegzett saját kutatás<sup>15</sup> egyik kérdésénél arra voltam kíváncsi, hogy mennyire alkalmasak az adatok és az információk értékének megállapítására az alábbi módszerek/modellek (mellettük az alkalmazott ötfokú Likert-skálán adott osztályzat átlaga szerepel, kiemelve a két legnagyobb átlagosztályzatot):

- az adatok idősoros megközelítése (az adatot nem önmagában, hanem a többi adattal együtt időrendiségében vizsgálom meg): 3,04
- az adatok megosztás szerinti megközelítése (megosztás = hányan tudnak róla): 3,32
- az adatok ráfordítás szerinti megközelítése (mennyibe került az adat előállítása): 3,52
- az adatok adott időpontban (jelenérték) szerinti megközelítése (pl.: részvényvásárlásnál az adat értéke az adott pillanatban): **3,71**
- az adatok pszichológiai megközelítése (milyen emlékeim fűződnek hozzá): 3
- az adatok címzettje szerinti megközelítés (egy tőzsdei adat mást ér egy utcaseprőnek és mást egy tőzsdei spekulánsnak): 3,52
- szükségesség elve szerinti megközelítés (minél kevesebben tudják, annál többet ér az azt ismerőknek): 3,16
- elveszett haszon elve szerinti megközelítés (mennyivel több hasznot tudnánk realizálni akkor, ha az adat rendelkezésre állna): **3,92**

Látható, hogy a megkérdezett szakértők szerint az elveszett haszon, illetve az adatok jelenértéke szerinti megközelítése kapta a legmagasabb átlagosztályzatot. Ez a két megközelítés ismerős a vállalati/szervezeti vezetők számára is, így amikor az információbiztonság kulcsmutatószámaihoz kapcsolódó fejlesztések/beruházások anyagi fedezetéről esik szó, akkor a nevezett megközelítések eredményesen használhatóak fel az argumentálás során.

### A szervezetek folyamatai

A szervezetek működésében számos folyamatot tudunk megkülönböztetni, mint pl.: pénzügyi, gazdasági, gyártási, beszerzési, értékesítési, reklám, informatikai, biztonsági, kommunikációs, s külön terület foglalkozik a változások, átalakulások, átszervezések, krízisek folyamatszintű kezelésével. A szervezeti folyamatokat – elsősorban a gyártási és a menedzsment folyamatokat – különböző vállalatszervezési és vállalatirányítási rendszerek támogatják, melyek egy, vagy több területre fókuszálnak. A témának gazdag hazai<sup>16</sup> és nemzetközi<sup>17</sup> szakirodalma van, többek

<sup>15</sup> KOLLÁR Csaba: Szakértői megkérdezés – kutatási jelentés. Budapest, PREMA Consulting, 2017.

<sup>16</sup> Pl.: WOMACK, James P. – JONES, Daniel T.: Lean szemlélet - A veszteségmentes, jól működő vállalat alapja. Budapest, HVG Könyvek kiadó, 2009., vagy RIES, Eric: Lean startup - Hogyan tegyük ötleteinket sikeressé és fenntarthatóvá? Budapest, HVG Könyvek kiadó, 2013., illetve NARUSAWA, Toshiko – SHOOK, John: Kaizen Expressz - Alapismertetek a lean utazáshoz. LEI Magyarországi Egyesülete, 2015.

<sup>17</sup> Pl.: OSTERWALDER, Alexander: Business Model Generation: A Handbook for Visionaries, Game Changers, and Challengers. New Jersey, John Wiley and Sons, 2010., vagy

között a Lean, a Kaizen, CRM, illetve a Canvas területén, így tanulmányomban csak a biztonsági folyamatokkal foglalkozom.

### *A szervezetek biztonsági folyamatai*

A biztonsági folyamatok megalkotásánál Steinklauber<sup>18</sup> 4 lépést azonosít: (1) kockázatmenedzsment folyamata, (2) biztonság-tervezési folyamat, (3) biztonsági végrehajtási folyamat, (4) ellenőrzési folyamat. A biztonsági folyamatokat a szervezeteknél alapvetően két kategóriába sorolhatjuk: (1) az adott folyamat (pl.: gyártás) biztonsági követelményei, (2) a szervezet általános, vagy részterületi működésének biztonsági kérdései (pl.: beléptetőrendszer, információbiztonság, kritikus infrastruktúra biztonsága). Az adott folyamathoz kapcsolódó, illetve a szervezeti működést érintő biztonsági követelmények célja, hogy a folyamatban meghatározott mérőföldköveknél biztonsági ellenőrzési (mérő)pontokat iktatnak be, s az így szerzett adatok ellenőrzése, feldolgozása, kiértékelése, stb. után az adott folyamat a korábban meghatározott következő lépések/stációk szerint halad tovább, illetve a továbballadás előtt, vagy azzal időben párhuzamosan a folyamatban, vagy annak valamely elemében korrekciót, javítást hajtanak végre.

A folyamatok menedzselése során is megjelenik a biztonság, ahogy arról Bayuk<sup>19</sup> is ír. Meglátása szerint egy hatékony biztonsági menedzsment folyamat hat alfolyamatot tartalmaz:

#### 1. Irányelvek

- a szabályozás/szabályok területe, amelyik a létesítményekre, rendszerekre és a felhasználókra egyaránt vonatkozik
- a biztonsági menedzsment folyamata és az alfolyamatok leírása
- az alfolyamatoknál a felelősök és a felelősség kérdése
- minimális követelmények az összes rendszer/alrendszer biztonságos konfigurálásához
- a szabályok megsértésének következményei és az alkalmazandó büntetések
- a felhasználó felelősségi nyilatkozata az általa használt adat(bázis)ok, információk és eszközök vonatkozásában.

#### 2. Tudatosság

- a biztonságtudatosságot és elköteleződést minden vezetési szinten és a szervezet minden területén támogatják

---

GRAHAM, Julia – KAYE, David – ROTHSTEIN, Philip Jan: A Risk Management Approach to Business Continuity: Aligning Business Continuity with Corporate Governance. Brookfield, Rothstein Associates Inc., 2006., illetve WILLIAMS, David S.: Connected CRM: Implementing a Data-Driven, Customer-Centric Business Strategy. New Jersey, Wiley, 2014.

<sup>18</sup> STEINKLAUBER, Kirk: Security Process for the implementation of a Company's extranet network. SANS Institute, 2003. <https://www.sans.org/reading-room/whitepapers/policyissues/security-process-implementation-companys-extranet-network-1115> (Letöltés ideje: 2017. 12. 22.)

<sup>19</sup> BAYUK, Jennifer L.: Security through process management. <https://csrc.nist.gov/csrc/media/publications/conference-paper/1996/10/22/proceedings-of-the-19th-niscc-1996/documents/paper015/bayuk.pdf> (Letöltés ideje: 2017. 12. 22.)

- megtanítják a munkavállalókat a biztonsági szabályokra és biztonságtudatos magatartásra, valamint arra, hogy betartsák ezeket a szabályokat
- rámutat az információbiztonsági szabályok megsértéséből eredő üzleti kockázatokra, s ezeket kiemelten kezeli
- a szervezet valamennyi munkatársa, illetve a szervezet, mint rendszer input és output folyamataiban résztvevő érintettek biztonságátudatosságával is foglalkozik
- megállapítja a felelősséget.

### 3. Hozzáférés

- a hozzáférést igénylő személyek azonosítása
- a rendszerszintű hozzáféréshez szükséges engedélyezési eljárások
- automatikus azonosítás a belépéssel egy időben (a belépés lehet a fizikai belépés valamely terembe, majd az itt végzett tevékenységek naplózása alapján a teljes tevékenység, mint folyamat ismertté válik)
- a feladatok felosztása az engedélyezés és a hitelesítés között
- a hozzáférési környezetek elkülönítése különálló munkakörökhöz.

### 4. Monitoring

- a rendszer biztonsági profiljainak konfigurálása
- a rendszer biztonsági naplójának (logfile) rendszeres áttekintése
- a biztonsági riasztások kiváltó okainak azonosítása.

### 5. Megfelelőség

- a rendszer műszaki felépítése támogatja a szükséges biztonsági funkciókat
- a megfelelés fenntartásához szükséges erőforrások rendelkezésre állnak
- a biztonsági események/incidensek során olyan biztonsági rést azonosítottak, amelyekkel a biztonsági szabályzatok már foglalkoztak
- a rutin biztonsági ellenőrzések vagy biztonsági felülvizsgálatok korábban észrevétlen kockázatokat fednek fel
- biztonsági események/incidensek esetén a munkatársak jelentik azt az illetékes kollégának.

### 6. Stratégia

- olyan kockázatbecslési módszerek kifejlesztése, amelyek számszerűsítik a működési kockázatok szintjét az új termékekben
- a szervezet biztonságos és kiszámítható működése érdekében a biztonsági fejlesztések és megoldások költsége szerepel a pénzügyi stratégiában és az éves pénzügyi terv tételei között
- új biztonsági szolgáltatások és termékek felülvizsgálata és tesztelése.

Bár elvárás lenne, a hivatkozott tanulmány nem nevez meg konkrét mérőpontokat egyik al folyamat bemutatásánál sem, egyedül a monitoring és a stratégia alrendszereknél látunk utalást a mérés fontosságára.

Egy rendszer általános biztonsági leírásánál általában hét lépést különböztetünk meg:

1. A rendszer **célja**, a tárolt adatok és információk fajtái, a nyújtott alkalmazások és szolgáltatások, valamint az ezekkel szemben támasztott biztonsági követelmények;
2. A rendszert használó **felhasználók** kategóriái, a számukra adott jogosultságok, valamint azoknak az információknak a fajtái, amelyekhez hozzá tudnak férni;
3. A felhasználók **hitelesítése**;
4. A **hozzáférés módja** azokhoz az adatokhoz és információkhoz, amit a rendszer tárol;
5. Milyen **hozzáférést** biztosít a rendszer **más rendszerekben** tárolt információkhoz, például fájl- vagy adatbázis-kiszolgálókhoz, valamint milyen módon támogatja ezek kezelését;
6. Ki és hogyan **kezeli** a rendszert (adminisztrátor, rendszergazda) helyi, illetve távoli hozzáférés segítségével;
7. A rendszer felügyeletéhez és működtetéséhez szükséges **mérőpontok és mérések**, beleértve a tűzfalakat, vírusirtó vagy egyéb kártevővédelmi mechanizmusokat, illetve a naplózást.

A(z) elektronikus információ)biztonsági vezető feladata a fentiek alapján az, hogy a(z) információ)biztonsági folyamatok megalkotása és/vagy számbavétele során meghatározza és/vagy azonosítsa azokat a mérőpontokat, amelyeknél a szervezet (információ)biztonsága, illetve a működés, fenntartás, üzemeltetés számára az elemzéshez, kiértékeléshez, beavatkozáshoz szükséges adatok nyerhetők. A szervezetek jelentős része a(z) információ)biztonság területén nem saját fejlesztésű szoftvereket és alkalmazásokat használ, hanem lehetőségei és erőforrásai ismeretében szerzett be korábban, vagy szerez be a (közel)jövőben a rendszer biztonságát támogató alkalmazásokat különböző beszállítóktól.

A szervezetek klasszikus mechanikai és elektronikus vagyónvédelmi megoldásai<sup>20</sup> között is megjelennek már azok a lehetőségek, amelyek szükség szerinti beavatkozás mellett az adatelemzéshez/bányászathoz kínálnak adatokat. Ilyen adat lehet pl.: a nem a szervezet állományába tartozó látogatók száma naponta/hetente/havonta, a munkavállalók belépése/kilépése a szobákból/helyiségekből (mikor léptek be/ki, mennyi időt töltöttek ott), a műszak végén nyitva hagyott ablakok száma, az egy év alatt elveszett belépőkártyák száma, a video felügyeleti rendszerek eszközeinek meghibásodása adott időszak alatt, a tűzjelző és egyéb biztonsági rendszerek hibás riasztásainak száma adott időszak alatt. Az információbiztonság területén megjelenő mérésre alkalmas adatokkal a kulcs teljesítménymutatók bemutatásánál foglalkozom. Gyakorlatilag bármit meg tudunk mérni<sup>21</sup>, hiszen rendszerint nagyon sok adat áll rendelkezésünkre. Ugyanakkor a vezetői döntéseket támogató elemzésről csak akkor lehet érdemben beszélni, ha a mérési nyers adatokat fel is dolgozzuk, például big data analitika módszereivel<sup>22</sup>.

---

<sup>20</sup> BEREK Lajos: Biztonságtechnika. Budapest, Nemzeti Közszolgálati Egyetem, 2014.

<sup>21</sup> HUBBARD, Douglas W.: Mérjük meg bármit. Budapest, Akadémiai Kiadó, 2011.

<sup>22</sup> MAYER-SCHÖNBERGER, Viktor – CUKIER, Kenneth: Big Data. Forradalmi módszer, amely megváltoztatja a munkánkat, gondolkodásunkat és egész életünket. Budapest, HVG Könyvek, 2014.

## Záró gondolatok

Szinte valamennyi rendszernél – különösen a szervezeti aspektusban – meg lehet különböztetni magát a rendszert, a környezetét, illetve a környezetéből származó (input), illetve oda áramló (output) dolgokat, s rendszerint a visszacsatolást is. Az inputok, mint erőforrások értékelésénél többféle szempontot vehetünk figyelembe (hasznosság, előállítás), s pont az adatok és információk leltározása és értékének megállapítása miatt válik fontossá azok védelme is. Szakértők (elektronikus információbiztonsági szakemberek/vezetők) körében végzett felmérésem<sup>23</sup> alapján megállapítottam, hogy az adatok és információk értékénél leggyakrabban az elveszett haszon elve, illetve az adatok jelenértéke szerinti megközelítés a legmegfelelőbb. Ez a két megközelítés ismerős a vállalati/szervezeti vezetők számára is. Ennek a jelentőségét abban látom, hogy közel azonos fogalmi keretben tud beszélni informatikus, biztonsági szakember és vállalatvezető a szervezeti (információ)biztonság témájában az adatok értéke és azok elvesztése miatti károk vonatkozásában, s ennek alapján könnyebben lehet ész érvek mentén anyagi és humán erőforrásokat mozgósítani a szervezeti (információ)biztonság érdekében.

Az adatok és információk értéke mellett lehet beszélni a rendszer értékéről is, mely többek között az általa végzett input-output folyamatokban, a materiális vagyonában, hírnevében, a környezetre kifejtett hatásában, a környezettel, s a többi rendszerrel való interakcióinak számában és minőségében, valamint az általa termelt, felhalmozott és felhasznált tudásban fejezhető ki. A szervezet, mint rendszer működésének leírásánál is nagyon fontos szerepet kap a visszacsatolás értelmezése, mivel következtetni lehet belőle arra, hogy a rendszer milyen transzformációt hajt végre az inputokkal, de abban is segít, hogy a rendszer működésében annak vezetői szükség esetén változtatásokat hajtsanak végre. A rendszeren belül meg lehet különböztetni alrendszereket, amelyek egymáshoz kapcsolódása révén vázolhatók fel a szervezet, mint rendszer folyamatai, így a(z információ)biztonság folyamatai is. A biztonsági menedzsment folyamata hat alfolyamatot tartalmaz: irányelvek, tudatosság, hozzáférés, monitoring, megfelelőség és stratégia. A hivatkozott forrást (BAYUK, Jennifer L.: Security through process management) megfelelőnek gondolom, mivel a monitoring és a stratégia területén utal a mérésre, bár meglátásom szerint a mérést, illetve annak komolyabb kielemezését még jobban a fókuszba kellett volna helyeznie. Tanulmányom első részét azzal a gondolattal zárom, hogy a legtöbb biztonsági és informatikai rendszernél – különösen a rendszert működtető, felügyelő, monitorozó, védő szoftvereknek és alkalmazásoknak köszönhetően – rendelkezésre állnak azok a mérőpontok, illetve a mérőpontokon keresztül kinyerhetőek azok a mérési- illetve a rendszer működését és állapotát leíró adatok, amelyek révén olyan teljesítménymutatók (KPI-ok) képezhetőek, amik hatékonyan képesek támogatni a vezetői döntéseket.

---

<sup>23</sup> Nevezet kutatás két csoport véleményét vizsgálta hasonló kérdésekkel: (1) kommunikációs szakemberek, illetve (2) elektronikus információbiztonsági szakemberek/vezetők. Jelen tanulmányomban csak az utóbbi csoport véleményét ismertetem.

### ***Felhasznált irodalom:***

- BAYUK, Jennifer L.: Security through process management. <https://csrc.nist.gov/csrc/media/publications/conference-paper/1996/10/22/proceedings-of-the-19th-nissc-1996/documents/paper015/bayuk.pdf> (Letöltés ideje: 2017. 12. 22.)
- BEREK Lajos: Biztonságtechnika. Budapest, Nemzeti Közszerológati Egyetem, 2014.
- BROOKS, David J. (2009): What is security: definition through knowledge categorisation. Security journal 23 (3), 2009.
- GERKEN, Gerd: A 2000. év trendjei. Budapest, Akadémiai Kiadó, 1993.
- HUBBARD, Douglas W.: Mérjünk meg bármit. Budapest, Akadémiai Kiadó, 2011.
- KINDLER József – KISS István: Rendszerelmélet. Válogatott tanulmányok. Budapest, Közgazdasági és Jogi Könyvkiadó, 1971.
- MAYER-SCHÖNBERGER, Viktor – CUKIER, Kenneth: Big Data. Forradalmi módszer, amely megváltoztatja a munkánkat, gondolkodásunkat és egész életünket. Budapest, HVG Könyvek, 2014.
- POKORÁDI László: Rendszerek és folyamatok modellezése. Debrecen, Campus Kiadó, 2008.
- ROTHSCHILD, Emma: What Is Security? Daedalus, Vol. 124, No. 3, The Quest for World Order, Summer, 1995.
- SMITH, Clifton L. – BROOKS, David J.: Security science. The Theory and Practice of Security. Amsterdam, Elsevier.
- STEINKLAUBER, Kirk: Security Process for the implementation of a Company's extranet network. SANS Institute, 2003. <https://www.sans.org/reading-room/whitepapers/policyissues/security-process-implementation-company-extranet-network-1115> (Letöltés ideje: 2017. 12. 22.)
- SUPAN, Joel Jesus M.: The art and science of security. Bloomington, Trafford Publishing, 2012.
- VASVÁRI György: Vállalati (szervezeti) kockázatmenedzsment. Budapest, Információs Társadalomért Alapítvány, 2008.
- ZVIKLI Sándor: Rendszerelemzés 1. Győr: Széchenyi István Egyetem, 2009.



## A TERRORIZMUS ÉS INDIREKT HADVISELÉSE AZ EU KIBERTERÉBEN

---

### Bevezetés<sup>1</sup>

Az információs technológia fejlődése jelentős hatással van a mindennapi életre. A kibertérben verseny alakult ki a hírek mielőbbi megjelenítéséért. Ugyanakkor a könnyen befolyásolható olvasókat a valóságtartalom ellenőrzése nélkül tájékoztatják. A társadalom befolyásolása vallási, politikai, üzleti és egyéb szempontból valós veszélyeket is rejt magában. A közelmúlt eseményei megmutatták, hogy akár országok választási rendszereire is lehet külső hatást kifejteni, azonban ezen tevékenységek bizonyítása nagyon nehéz, sokszor lehetetlen feladat.

A személyes, vállalati adatok sértetlenségének, bizalmasságának, rendelkezésre állásának biztosítása komoly kihívást jelent, amelyet a napvilágra kerülő számítógépes programokkal elkövetett támadások jól alátámasztanak.

Az infokommunikáció fejlődésével az új technológiák egyre kifinomultabb lehetőségeket adnak a rejtett kommunikáció, az internetalapú hangkommunikáció, közösségi hálózatok, okos eszközök területén. Kihívásként jelentkezik, hogy a pont-pont közötti információcsere már nem egyértelműen azonosítható. A felhőszolgáltatások elterjedése új tárházát hozta elő a védendő információ rejtésének.

A világhálón a tartalmak szinte bárhol publikálhatók és elérhetők, ezért a terrorista szervezetek ezt felhasználva nyíltan és rejtve is képesek toborzásokra, különféle támadási technikák népszerűsítésére, ideológiájuk, propaganda videóik széles körben történő terjesztésére, elektronikus pénzeszközök használatával adományok gyűjtésére, továbbá kiemelve az egyik legfontosabb területet, a félelemkeltésre.

A kibertér napjainkban mint önálló hadszínteret kell figyelembe venni<sup>2</sup>, amely egy speciális műveleti környezetként értelmezhető, ahol elkövetői körben növekvő számban jelennek meg a magukat dzsihadistáknak valló harcosokból álló közösségek. A kibertér azonban olyan sajátos hadszíntér, amelyben a terrorizmus elleni fellépésnek is megvannak a szabályai.

---

<sup>1</sup> A tanulmány előzményeként a kibertérre befolyással bíró terrorizmus közvetett hatásaival foglalkoztak a szerzők. Bővebben: SIMON László – MAGYAR Sándor: A terrorizmus és indirekt hatása a kibertérben. Nemzetbiztonsági Szemle 2017. 3. sz. <https://www.uni-nke.hu/document/uni-nke-hu/nemzetbiztonsagi-szemle-2017-3-1.original.pdf> (Letöltés ideje: 2017. 12. 15.)

<sup>2</sup> NATO: Warsaw Summit Communiqué 70-71 pont, [http://www.nato.int/cps/en/natohq/official\\_texts\\_133169.htm#cyber](http://www.nato.int/cps/en/natohq/official_texts_133169.htm#cyber) (Letöltés ideje: 2017. 11. 31.)

## A terrorizmus hadviselésének hadikultúrája és a hálózatok

A különböző fegyveres terrorista csoportok a politikai és katonai céljaik eléréséhez képessé váltak a világ teljes lakosságának megszólítására. Ez nem azt jelenti, hogy az ISIS vagy hasonló szervezetek az információt hadműveletekre alapozva használják fegyverként, de mégis tudatosságot kell feltételezni. A hagyományos műveleteik támogatására egyre jobban és eredményesebben használják fel az információs technológiák adta lehetőséget. A tapasztalatok dinamikus beépítése az alkalmazott műveletekbe, valamint annak széleskörű megjelenítése, propagálása mind a kibetér többretű kihasználását tükrözi. Ez túlmutat a hagyományos információs támadások (1. ábra) összefüggésein. Az információtechnológia „soft” és „hard” típusú alkalmazása<sup>3</sup> mellett a terrorista szervezetek Európa közlekedési, turisztikai pontjainak, illetve jelképeinek közvetlen támadásával a különböző társadalmi, szociális és kulturális hálózataira is hatást gyakoroltak. A beszláni iskola, a moszkvai színház, a brüsszeli és a londoni metró, vagy a török, a spanyol, a német, illetve a francia fegyveres támadások, de még a szinte kinyomozhatatlan, feltételezett iszlamisták által elkövetett (akár magyarországi<sup>4</sup>) hekkertámadások is a szokásainkat és az életünket, a maslow-i értelemben vett emberi alapszükségleteket<sup>5</sup> célozták. Amíg a terroristák az ideológiai, de leginkább az információs fölény kialakítására törekuszenek, addig módszereikben az emberekre, mint „objektumokra”, célpontokra tekintenek. A hálózatok segítségével ezen „objektumok” tudatának befolyásolása, megnyerése, illetve megfélemlítése lőfegyverek nélkül is halálos következményekkel járhatnak. Az agresszióra a demokratikus államok – kultúrájukra jellemzően – bűnügyi felfogással, esetenként szociális érzékenységgel és humanitárius segítségnyújtással igyekeztek válaszolni. A közösségi hálózatokban tudatosan vizualizált visszavisszatérő fenyegetés pedig a szubjektív biztonságérzetünket<sup>6</sup> folyamatosan negatív tartományban tartotta. Értékelésünk szerint az egyéni és a társadalmi döntéseinket ebből adódóan nem a ráció, hanem a stressz és a félelem határozta meg. A vallási (iszlám) indíttatású terrorizmusként<sup>7</sup> jelölt törekvés politikai akaratának rákényszerítése a „nem muszlim ellenségre” pedig a fegyveres terror új dimenzióját hozta létre.

<sup>3</sup> HAIG Zsolt: Internet terrorizmus. Nemzetvédelmi Egyetemi Közlemények, 2007. 2. sz. pp. 81-93.,

<sup>4</sup> Origo.hu: Iszlám fanatikus támadhatta meg az Óbudai Egyetem honlapját, <http://www.origo.hu/techbazis/20150519-isis-izsalm-allam-hacker-tamadas-hackertamadas.html> (Letöltés ideje: 2017.12.15.)

<sup>5</sup> Maslow az emberi alapszükségletek alapján felállított egy piramist. Az alsó szinten a fizikai szükségletek, majd a biztonság és védelem, felette helyezkedik el a szeretet és összetartás, amit az önbecsülés követ. A legfelső szinten pedig az önmegvalósítás áll.

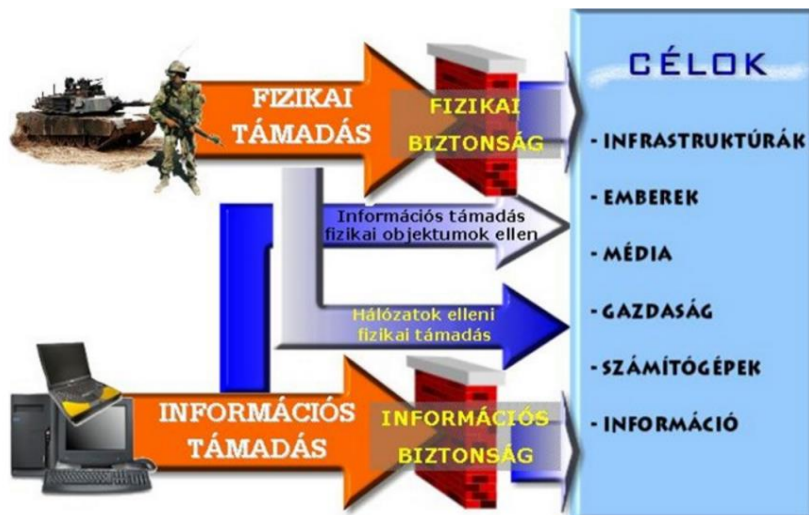
<sup>6</sup> A szubjektív biztonságérzetünket az eltérő környezeti hatások különböző módon, egymást erősítve illetve gyengítve befolyásolhatják. Ulrich Beck szerint a posztmodern emberi életút folyamatos, individuális választások alapján alakul, ami magában rejt a rizikót, magasabb stresszhelyzetet teremtve a 21. századi embernek. In: TÓTH Péter - HORVÁTH Helga: A szubjektív biztonságérzetet befolyásoló tényezők Magyarországon. [http://kgk.sze.hu/images/dokumentumok/kautzkiadvany2014/TothP\\_HorvathH.pdf](http://kgk.sze.hu/images/dokumentumok/kautzkiadvany2014/TothP_HorvathH.pdf) (Letöltés ideje: 2017. 12. 15.)

<sup>7</sup> RESPERGER István: Az aszimmetrikus hadviselés és a terrorizmus jellemzői. Hadtudomány 2010/4. pp. 68-77.

A terrorizmus elleni műveletekben való európai katonai részvétel és annak lakossági támogatása folyamatosan bővíti a terrorfenyegetettséget. A gerilla hadviselés elveinek mentén szerveződő és az új technológiai környezet felhasználásával közvetített műveletek pedig tömegessé és személyessé teszik a terrorizmus pusztító, tudatformáló hatásait. Az új típusú gerilla hadviselés technológiai támogatottsága folyamatosan növekszik, amely ellen a hatékony fellépés egyre komplexebb. A terrorista szervezetek céljaik elérése érdekében hibrid hadviselés-jellegű műveleteket alkalmaznak, a hagyományos és az információs műveletek – egyes, nem teljes körű – eszköztárával kombinálva.

A Magyar Honvédség 2014-ben kiadott információs műveletek doktrínája<sup>8</sup> például – a NATO AJP-3.10 doktrínában<sup>9</sup> foglaltakkal megegyezően – az alábbi információs műveleteket sorolja fel:

- Lélektani műveletek (Psychological Operations – PSYOPS)
- Megjelenés, viselkedés, arculat (Presence, Posture, Profile – PPP)
- Műveleti biztonság (Operational Security – OPSEC)
- Információbiztonság (Information Security)
- Megtévesztés (Deception)
- Elektronikai hadviselés (Electronic Warfare – EW)
- Fizikai megsemmisítés (Physical Destruction – PD)
- Kulcsfontosságú vezetőkkel való érintkezés (Key Leaders Engagement – KLE)
- Műveletek számítógépes hálózatokkal (Computer Network Operations – CNO)
- Civil-katonai kapcsolatok (CIMIC).



1. ábra: Információs támadás<sup>10</sup>

<sup>8</sup> Ált/57 Információs Műveletek Doktrína 1. kiadás, a Magyar Honvédség kiadványa 2014.

<sup>9</sup> AJP 3-10. Allied Joint Doctrine for Information Operations pp. 1-3. <http://info.publicintelligence.net/NATO-IO.pdf> (Letöltés ideje: 2017. 12. 15.)

<sup>10</sup> Forrás: KOVÁCS László: Kiberterrorizmus, (2008. 03. 19.) ZMNE, <http://slideplayer.hu/slide/5656918/> (Letöltés ideje: 2017. 12. 15.)

A saját állammal nem rendelkező népi felkelők, szakadárok, de még a terrorista csoportok tevékenysége is folyamatosan jelen van az emberiség fejlődésében. A félelemkeltés, mint a terrorizmus egyik eszköze a világháló elterjedésével újabb, hatékonyabb lehetőséget, terjesztési formát kapott. Az információs társadalmak korában és a multipoláris világhatalmi rendszerben a „megszállók”, a „hódítók” vagy egy „zsarnoki rend” elleni fegyveres fellépés vagy azok közvetlen „államépítő” hatásainak kérdésköre jog-, állam- és társadalomelméleti problémákat jelent. A tudatunkat befolyásoló közvetett hatások miatt viszont egyre szélesedő – a technológiai vizsgálatokon túlmutató – információelméleti problémakörrel kell számolni<sup>11</sup>. Az említett mozgalmak fegyveres tevékenységét a hadtudomány gerilla hadviselésként értelmezi. A különböző csoportok létezését és aktivitását azonban csak egyes államok segítő szándéka, illetve más országok ellenszenvé, ellenségképe alapján értelmez. Egyes népi mozgalmak, bár önálló identitással nem rendelkeztek, mégis jól leírható politikai, társadalmi, kulturális és katonai igénnyel léptek fel, amely eredményeként például az önálló Koszovó megszületett. A több állam által elismert köztársaság jelenlegi államfője, Hashim Thaçi például az USA által korábban terrorszervezetként nyilvántartott Koszovói Felszabadítási Hadsereg (UÇK) vezetője volt.<sup>12</sup>

A továbbiakban mégsem ezt a politika- és jogelméleti szempontok alapján is érdekes összefüggéseket vizsgálnánk, hanem a küzdelem fegyveres oldalát. A hatalmi erőszak összefüggéseinek ezen témakörében, a magyar katonai gondolkodók közül Kovács Jenő és követői<sup>13</sup> három jól elkülöníthető – társadalomelméleti alapokat is szem előtt tartó – kulturális felfogás szerint folytatták, illetve folytatják vizsgálataikat. Az európai terrorizmus és gyökerei az elmélet alapján a gerilla hadviselés hadikultúrájával jellemezhető. A vele szemben fellépő társadalmak fegyveres küzdelme a mozgáscentrikus, illetve az anyagcentrikus hadviselési hadikultúra. A hadikultúrák és az információs, illetve infokommunikációs rendszerek közötti kapcsolat elemzését Ács Tibor 2005-ben alapozta meg. A hadtörténész kiemelte<sup>14</sup>, hogy a technológiai haladás következtében megjelenő új fegyverekre, illetve rendszerekre a katonai kultúrák egyszerre pozitívan és negatívan is reagálhatnak.

A terrorizmus elleni küzdelemben részt vevők eltérő motivációval ugyan, de folyamatosan igyekeztek bevonni a civil lakosságot. Ennek következményeként a politikai célok megvalósításának legfőbb rendszerei a globális hálózatok lettek. „A kibertámadásokkal szembeni ellenálló képesség Unió-szerte történő előmozdítása

---

<sup>11</sup> Ezt a kijelentésünket még akkor is fenntartjuk, ha a közvetett hatások tekintetében nem csak az információra helyezünk a hangsúlyt. A hidegháború idején például az atomfegyverek *fizikai bevetésének lehetősége* miatt szinte minden nap a világ végére „kellett gondolni”! A nukleáris fenyegetés – az általunk vázolt biztonság- és információelméleti szempontok szerint – a legsötétebb és legáltalánosabb agresszió körébe sorolható be.

<sup>12</sup> DELAUNEY. Guy: Kosovo's Hashim Thaci: From guerrilla leader to president. BBC News 2016. <http://www.bbc.com/news/world-europe-35984823> (Letöltés ideje: 2017. 12. 31.)

<sup>13</sup> HAIG Zsolt: Információ, Társadalom, Biztonság, NKE Szolgáltató Kft, 2015. pp. 93-122.

<sup>14</sup> ÁCS Tibor: A hadikultúra történetéhez In: Hadtudomány, XV. évf. 2. sz. 2005. pp. 15-26.

*érdekében az állami hatóságoknak és a magánszektornak egyaránt ki kell fejleszteniük a szükséges képességeket és hatékonyan együtt kell működniük.”<sup>15</sup>*

A kibertér a meggyőzés és az agresszió közvetlen és közvetett célpontjává vált. Az indirekt hadviselés az információból fegyvert kovácsolt<sup>16</sup>. Ez annak ellenére kijelenthető, hogy 2013-ban, a NATO értekezlet előtt Thomas Rid az információ fizikai természetére utalva kizárta ennek lehetőségét. Rid kijelentése szerint hagyományos módon a programok, vagyis a kódok az élet kioltására alkalmatlanok. Ezzel szemben az információ útján átadott fenyegetés nemcsak ideológiai vagy politikai, de katonai (fizikai) értelemben is valósnak tekinthető, ahogy a CIA korábbi igazgatója, Leon Panetta már 2011-ben megfogalmazta: „...a következő Pearl Harbor egy kibertámadás lehet...”. A „szemben álló felek” közül pedig mind a hekkerek, mind a terroriszervezetek napi rendszerességgel jelentenek be különböző céllal támadó műveleteket, még ha azok megvalósítása eddig a kijelentés szintjén is maradt. (Az ISIS például 2015-től gyilkos kibertámadásokra készül többek között Európában is.<sup>17</sup>) Az elszenvedett vagy lehetséges fizikai hatások mellett nagyobb figyelmet kell fordítani más elemekre is, amelyek elsősorban az információkon keresztül közvetetten, az egyén tudatára és biztonságérzetére hatnak. Így a fizikai fenyegetés bekövetkezésének magas valószínűsége, illetve tömeges megvalósításának lehetősége halálos félelmet jelent.

### **A terror direkt és indirekt hatása Európára**

A kibertérben az elektronikus információs rendszerek ellen, vagy azokat felhasználva elkövetett bűncselekmények száma növekszik. A világhálón nem lehet markánsan elkülöníteni a civil és az állami szervezetek, a rendvédelmi erők stb. területét. Az információs társadalom „idegrendszerét”<sup>18</sup> állami, vállalati és magán hálózatok alkotják. Tapasztalataink szerint kijelenthető, hogy az emberek szociális hálózával kiegészítve minden olyan törekvés, amely az eszközeink passzív védelmére irányult, eddig kudarcot vallott. Nem lehet teljesen zárttá tenni a meglévő, de még a kiépítendő rendszereinket sem. A kapcsolatok megszakítása, az erőforrások kiiktatása, a „villanykapcsoló ellenőrzése” csak a hálózat technikai részének megszűnését, illetve megszakítását eredményezi, nem pedig annak megóvását. A felhasználók jelenléte miatt pedig mindig lesznek olyanok, akik bizonyos előnyökre akarnak szert tenni, és ezért időről-időre nyitottá teszik a fizikailag zártnak és biztonságosnak tekinthető rendszereket. Ezen összefüggő társadalmi és technikai hálózatok így kimeríthetetlen forrásokat jelentenek.

A politika- és jogelméleti megközelítés szerint ezek a személyek bűnözőknek tekinthetők. A bűnelkövetők, köztük a terroristák a nyilvánosságot kerülve, rejtve szerveződnek. A terroristák esetében a hálózati célpontok és a célok elérése mutathat ugyan egyezést, de maga a cél teljesen elkülönül. A terrorral fenyegető személy vagy csoport lehet bűnöző, de társadalomelméleti szempontok alapján akár

<sup>15</sup> Az Európai Unió kiberbiztonsági stratégiája. <http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A52013JC0001> (Letöltés ideje: 2017. 12. 31.)

<sup>16</sup> SIMON László: Az információ mint fegyver? Szakmai Szemle. 2016. 1. sz. pp. 34-60.

<sup>17</sup> SMEJKÁL Péter: Halálos kibertámadásokra készül az Iszlám Állam (2015. 11. 17), <http://www.origo.hu/techbazis/20151117-islam-allam-halalos-kibertamadas-felkeszules-nagy-britannia-terrorizmus-parizs-tamadas.html> (Letöltés ideje: 2017. 12. 15.)

<sup>18</sup> SIMON László: Az információ mint fegyver? Szakmai Szemle. 2016. 1. sz. pp. 34-60.

népfelkelő vagy partizán is. A legfőbb kihívást értékelésünk szerint az jelenti, hogy amíg a célpontokat elérő elkövetők egyik része igyekszik a virtuális tér nyújtotta azonosíthatatlanság álarca mögött maradni, addig a másik része büszkén hirdeti saját vagy mások által elkövetett cselekményeit úgy, hogy az még nagyobb nyilvánosságot kapjon. A politikai és vallási indíttatású terror esetében a tudatosan használt „információs műveletek” a gazdasági, a közigazgatási, a szociális, az oktatási, a közösségi, illetve a közlekedési hálózatok közös pontjainak közvetlen támadása mellett a média felhasználásával megdöbbentő fenyegetettségünket<sup>19</sup>.

A támadás bárhol és bármikor érhet bennünket. Az említett rendszereket kiszolgáló infokommunikációs és információs hálózatokon keresztül már most is szinte korlátlan méretekben képesek felderíteni és megszólitani a potenciális ellenségeiket, az áldozataikat, de még a szövetségeseiket is. Ebben a felfogásban a második „elkövetői csoport” esetében a politikai célok elérésének fő ereje az információban és annak megosztásában van. A hagyományos fegyveres akciók mellett a „közvetett műveletekkel” kombinált csapásokat, illetve terrorakciókat preferálják. Annak ellenére, hogy David Galula már 1964-ben megfogalmazott négy törvénye<sup>20</sup> szerint a terrorizmus elleni küzdelem alapját a helyi lakosság megnyerése, a jól működő hatékony kormányzás kialakítása, a biztonság fenntartása haderő alkalmazásával, valamint a fegyveres felkelők fő erőinek szétverése vagy kiszorítása jelentheti az érintett területről, Európában mégsem tudunk megnyugtató sikereket felmutatni.

Az eddig alkalmazott hagyományos katonai műveletek nem oldhatják fel az Európát érő agresszió és félelem kérdéskörének ellentmondásait.<sup>21</sup> Egyszerre biztonságban lenni és egyéni szabadságjogainkat érvényre juttatni a fokozódó morális kérdések miatt egyre nehezebb. Ez esetenként egymást kizáró törekvéseket is jelenthet. Például a magyar katonákat 2016-ig csak az országon kívül vethették be terroristák ellen. Jelenleg a terrorizmus elleni küzdelemben a fegyveres erők a légi csapások elsődlegességét, valamint az ellenség „lefejező csapásait” tartja műveleteinek középpontjában.<sup>22</sup> A terrorizmus legyőzésben ez a felfogás értékelésünk szerint csak egy jól körülhatárolt földrajzi hadszíntéren értelmezhető. A korábban említett mozgáscentrikus hadikultúrában a győzelem feltétele a direkt műveletek, továbbá azok fokozása a TÉR, az IDŐ és az ERŐ dimenzióiban. Leegyszerűsítve, itt az információ reálisan csak a mozgékonytámasztó szolgáló eszközöket, illetve módszereket támogatja. Az anyagcentrikus hadikultúra pedig a TÉR, IDŐ és ERŐ fokozása mellett már az INFORMÁCIÓ dimenziójának jelentőségét is mérlegeli. Például az embargós, a befolyásoló, a pszichológiai, valamint a katonai-civil együttműködésre irányuló műveletek végrehajtásánál

---

<sup>19</sup> RESPERGER István: Kis háborúk nagy hatással: a XXI. század fegyveres konfliktusai, a terrorizmus és az aszimmetrikus hadviselés jellemzői. Felderítő Szemle 2013/1 pp. 200-230.

<sup>20</sup> GALULA, David: Counterinsurgency Warfare (1964), pp. 61-73., <http://ready4itall.org/wp-content/uploads/2013/05/Counterinsurgency-Warfare-Theory-and-Practice.pdf> (Letöltés ideje: 2017. 12. 15.)

<sup>21</sup> BOLGÁR Judit – SZTERNÁK Nóra – SZTERNÁK György: A terrorizmussal kapcsolatos kutatások legújabb eredményei. Felderítő Szemle 2005. 4. sz. pp. 5-60.

<sup>22</sup> RESPERGER István: Forrongó világ, nemzetbiztonsági kihívások 2030-ig, (2015. 11. 17.). [http://uni-nke.hu/uploads/media\\_items/12-resperger-istvan.original.pdf](http://uni-nke.hu/uploads/media_items/12-resperger-istvan.original.pdf) (Letöltés ideje: 2017. 12. 15.)

racionálisan kerül alkalmazásra. De továbbra is csak a támogató szerepet töltheti be. A hagyományos hadviselésben az anyagi erőforrások és a mozgékonytárat jelentő hadi eszközök birtokában tehát az információ elsősorban az ütközetek megvívásához szükséges információk főlény elérését szolgálja. A korábbiakban tárgyalt speciális stratégiai kommunikáció az indirekt hadviselés<sup>23</sup> kiegészítő módszere.

A megértést és a megoldásokat szolgáló információk, valamint a döntéseket támogató tudás szinte korlátlanul állnak mind az állami, mind a nem állami szereplők, így a laikus lakosság rendelkezésére is. A világunkban jelenleg is folyó fegyveres küzdelmek valós vagy annak vélt céljainak modern felfogású, racionális labirintusában ugyanakkor, valljuk be, egyre inkább elveszünk. A korábban kényelmünket, komfortunkat, valamint szabadságunkat, illetve biztonságunkat garantáló hálózatok miatt rendre bajba kerülhetünk. A hálózatokat kihasználó bűnözők és ellenséges szándékú emberek nemcsak bosszúságot, de jelentős erkölcsi, anyagi és egyéb károkat okozhatnak. Az arctalanul programokkal, vírusokkal végrehajtott támadások mára az utolsó felhasználókat is elérték, minden újonnan fejlesztett és folyamatosan frissített biztonsági alkalmazások és rendszabályok ellenére. Az infokommunikációs rendszerekben továbbított adatok, hírek a megnyugtató helyett csak fokozzák a félelemérzetünket. Korunk egyik jelentős kihívása az információs társadalmak új biztonságfelfogásának kérdésköre egyre növekvő biztonsági kockázatokra és fenyegetésekre mutat rá. Egyetértve Haig Zsolttal<sup>24</sup>, az „összehangolt információs támadások és az ellenük való védelem komplexitásában” lehet csak kezelni az „információ, az infokommunikációs technológia, a társadalom és a biztonság összefüggéseit”.

A komplex védelem – pontosabban kibervédelem – feladatainak értelmezése Kassai Károly véleménye szerint „az eddigi elektronikus információbiztonsági követelmények és eljárásrend erőforrások szerinti továbbfejlesztését jelenti.” Az „erőforrások szerinti” kifejezés a közigazgatási gyakorlatban inkább az „alulfinanszírozás” szalonképesebb megfogalmazása, a valóság azonban ettől eltérhet, mert gyakori eset, hogy a napjainkban jellemző, egyre gyorsuló információs igények és szolgáltatások kiszolgálását nem pontosan kialakított, illetett megoldások szolgálják, vagy a védelmi mechanizmusok nem illeszkednek az adott kommunikációs szolgáltatásokhoz.<sup>25</sup>

Az említett közvetett és közvetlen erőszakra adott válaszok alapján eddig azt tapasztalhattuk, hogy az iraki, az afganisztáni, de még az ukrainai válság kezelése során sem működhetek teljesen eredményesen a hagyományos hadviselés eszközei, illetve módszerei. A válság sújtotta területeken a fegyveres harcok lezárása és a katonai erők kivonása után, a béke fenntartására hivatott katonai és nem katonai szereplők, nem voltak képesek jól működő államokat kialakítani, illetve hátrahagyni. A hozzá szükséges hálózatokat még ma sem tudják teljesen megvédeni. Az új, mesterségesen kialakított társadalmakat rendre gerilla típusú támadások érik. A

---

<sup>23</sup> FORGÁCS Balázs: Napjaink hadikultúrái. (A hadviselés elmélete és fejlődési tendenciái a modern korban). ZMNE PhD értekezés (2009), [http://uni-nke.hu/downloads/konyvtar/digitgy/phd/2009/forgacs\\_balazs.pdf](http://uni-nke.hu/downloads/konyvtar/digitgy/phd/2009/forgacs_balazs.pdf) (Letöltés ideje: 2017. 12. 15.)

<sup>24</sup> HAIG Zsolt: Információ, Társadalom, Biztonság, NKE Szolgáltató Kft., 2015. pp. 93-122.

<sup>25</sup> KASSAI Károly: Kiberveszély és a Magyar Honvédség, Hadmérnök, 2012. VII. évf. 4. sz. p. 137.

bennünket érő fenyegetések, a világban folytatott nemzetközi, illetve ad hoc válságkezelő katonai műveletek, valamint az ISIS terrorszervezetének tevékenysége kapcsán az információ fegyverré vált.<sup>26</sup>

Az ISIS területén Szíriában folytatott katonai műveletek révén egyre csökken az általuk ellenőrzés alatt álló terület, de a szakértők ennek ellenére a növekvő intenzitású gerilla hadviselésre, és az erőszak szétterjedésére figyelmeztetnek<sup>27</sup>. A szíriai hadszíntértől távol eső területeken ezek a fegyveres műveletek csak az elmúlt két évben közvetve több mint háromszáz európai polgár halálát okozták. Madrid, London, Párizs, Brüsszel, Nizza, Berlin – a nemzetközi turizmus és az európai kulturális emlékek központjaiként – a terrorizmus, illetve a radikális fegyveresek közvetett támadásainak új színterévé vált. Ezzel párhuzamosan, kultúránk számára eddig látszólag érthetetlen módon, a támadásokat követően nem jelenhető ki, hogy csökkenne az ISIS európai támogatóinak, illetve követőinek köre. Az elektronikus propaganda-kiadványaikkal, a videó-üzeneteikkel, illetve a közösségi médiában megosztott toborzó és megfélemlítő tevékenységükkel folyamatosan népszerűsíteni tudták politikai szándékukat. A közvetett, valamint közvetlen módon megtámadott és megfélemlített ártatlan áldozatok száma pedig folyamatosan nő. A gerilla hadviselés a XXI. században az ISIS tevékenysége kapcsán egy információ-centrikus és hálózat központú (2. ábra) hadviselési hadikultúrává fejlődött.<sup>28</sup>



2. ábra: A gerilla hadviselés (saját szerkesztés<sup>29</sup>)

A terroristák a célok eléréséhez a hagyományos, katonai jellegű műveleteikben – mivel anyagi forrásaik szűkösek – csak a célzott ERŐ és az INFORMÁCIÓ

<sup>26</sup> SIMON László: Az információ mint fegyver? Szakmai Szemle 2016. 1. sz. pp. 34-60.

<sup>27</sup> CIA: Az Iszlám Állam félelmetes és rugalmasan alkalmazkodik, MTI (2016. 06. 16.), <http://www.origo.hu/nagyvilag/20160616-cia-isis-izlam-allam-erosebb-mint-az-alkaida.html> (Letöltés ideje: 2017. 12. 15.)

<sup>28</sup> SIMON László: Az információ mint fegyver? Szakmai Szemle 2016. 1. sz. pp. 34-60.

<sup>29</sup> Forrás: SIMON László: Az információ mint fegyver? Szakmai Szemle 2016. 1. sz. pp. 34-60.



dimenziójában képesek támadásaikat fenntartani. Az erőszak legitimitációját a virtuális térhez kapcsolódó lakosság támogatásával, a magányos elkövetők megnyerésével még bővíteni is tudták. A civil és hálózati célpontok támadása kapcsán a hagyományos TÉR kiegészült a kibertér dimenziójával. Értékelésünk szerint pontosan az erőszak verbális, vizuális, illetve virtuális jellemzői miatt került hátrányba ezen a területen a hagyományos hadviselés hadikultúrája. Az IDŐben folyamatosan és rendszertelenül, ugyanakkor intenzíven, valamint impulzívan megjelenített indirekt fenyegetések a kibertÉRben (amelyen az elektronikus és ahhoz kapcsolódó hálózatok összességét értjük) a szemben álló felek és azok támogatóinál ellentétes hatást eredményeztek.<sup>30</sup>

A terrorizmus elleni erőfeszítések esetében a hagyományos fegyveres műveletek mellett a kibertér is egyre hangsúlyosabban jelenik meg mind a támogató, mind az önálló műveletek végrehajtásának színtereként. Ez a tendencia tudatos felkészülést követel meg a védelmi képességek kialakítása területén is. A hibrid hadviselés, az információs műveletek korában az egykor kiszolgáló támogató területek, mint a híradás és az informatikai üzemeltetés szerepe felértékelődik. A kibertér (angolul: Cyber Intelligence – CYBINT) a nyílt forrású hírszerzés (angolul: Open Source Intelligence – OSINT), a kibertámadás (angolul: Computer Network Attack – CNA) területek fejlődése szükségessé teszik a gondolkodásmódbeli változást. Az említett területek jelentős fejlesztése esetében a kibervédelmi képességek szerepét ki kell hangsúlyozni.

Az „e-társadalomban” a digitális jólét által nyújtott előnyöknek azonban van sötét oldala is. A szervezetek, egyének függősége az elektronikus rendszerekhez, a sorra előbukkanó sérülékenységek megmutatják a célpontok gyenge pontjait, amelyet a terrorszervezetek jól képzett támadói képesek kihasználni. A védelem ezen esetekben nem csak az informatikai üzemeltető, kibervédelmi szakemberek felelőssége, hanem a felhasználóké is.<sup>31</sup>

Az informatikai, kibervédelmi terület támogató szerepe hatékonyan közrejátszik napjaink támadásainak elhárításában, a védelem első lépcsőjébe helyezi az informatikai üzemeltetési feladatot – különös tekintettel az elektronikus információbiztonsági eszközök tekintetében – 7/24 rendelkezésre állással.<sup>32</sup>

Napjainkban sok esetben nehezíti a kibertérben folytatott védelmet, hogy hiányoznak informatikusok (a piaci és az állami szektorban egyaránt), ezáltal ezen

---

<sup>30</sup> A hagyományos hadviselésben az információs és a fizikai támadás egységesen jelenik meg, egymást erősítve, minél pontosabban és egyre kevesebb civil áldozatra törekedve. Amennyiben például növelem a közdelem terét, beleértve a kibertérét is, a véges erőforrások miatt törvényszerűen csökken a hatékonyság, illetve a pontosság. Növekedhet az elszennvedett veszteség és emelkedhet a civil áldozatok száma is. Ez a „háterszög”, a támogatókat negatívan befolyásolhatja. Ezzel szemben a gerilla hadviselést folytatók ezen TÉR növelésével bővítik az elérhető célpontokat, egyre több támogatót szereznek, és újabb erőforrásokat képesek bevonni.

<sup>31</sup> Lásd még KRASZNAI Csaba: A magyar elektronikus közigazgatás biztonsága. ZMNE előadás (2008. 07. 07.) [http://krasznay.hu/presentation/mhtt\\_ekozig\\_krasznay.ppt](http://krasznay.hu/presentation/mhtt_ekozig_krasznay.ppt) (Letöltés ideje: 2017. 12. 31.)

<sup>32</sup> Bővebben: HAIG Zsolt: Információ, Társadalom, Biztonság, NKE Szolgáltató Kft., 2015. pp. 93-122.

humán erőforrás-szegmens tekintetében a szükséges bérköltségek még mindig növekednek.<sup>33</sup>

### **Következtetés**

Az elektronikus információs rendszerek mindamelllett, hogy hatékonyan támogatják életünket, egyre nagyobb részben vállalnak szerepet a mindennapjainkban. Egyre gyakrabban bebizonyosodik, hogy ezen rendszerek a hardver- és szoftverkomponenseik tekintetében sebezhetőek. A megjelenő programozási és kódolási hibák kihasználása egy hekker számára rutinfeladatnak számíthat, melyek a felhasználói biztonság tudatosság hiányában rendkívül könnyen támadhatóvá válnak.

A hálózatok elleni támadások folyamatosan csökkentették a hagyományos hadikultúrák küzdelmének hatásait a terrorizmussal szemben. A terrorszervezetek által folytatott információ- és hálózatcentrikus hadviseléssel szemben „forradalmi gondolkodásra” van szükség. A globalizáció modern, de sérülékeny intézményi hálózatainak védelme kiemelt állami feladat marad a jövőben is. A fentiek alapján a kritikus infrastruktúrák mellett a közösségi és az internetes kapcsolatok biztonságának növelésével tovább kell csökkenteni a terrorizmus célpontjainak, ártatlan áldozatainak számát.

A kibertérben a halálos fenyegetések ellenére egyelőre csak közvetett támadásokkal kell számolnunk. Ahhoz, hogy a védekezést megszervezhessük, pontosan kell meghatározni a biztonságos működésre alkalmas programokat, eszközöket, módszereket és a védelmi erők körét. Ebben a bonyolult rendszerben a tradicionális állami szereplők (rendőrség, honvédség, nemzetbiztonsági szolgálatok), hatékony fellépésük mellett a lakosság egyéni szerepvállalására is szükség van. A kibertér fizikai és logikai részei mellett egyre hangsúlyosabb „kognitív térben” nem állhatnak mindig rendőrök, titkosszolgák, katonák vagy akár informatikusok a felhasználók mellett. A személyes védelmünk érdekében ezen hivatásrendek csak helyes döntések, megfelelő eljárások alkalmazását javasolhatják. Éppen ezért a jelenlegi technológiai környezetben – a már alkalmazott lokális katonai és nem katonai együttműködések, a jogi szabályozottságon túl – az egyének, valamint a felhasználói csoportok biztonságfelfogásában is jelentős változásokra lesz szükség.

A terrorizmus elleni széleskörű fellépés megvalósítása során figyelembe kell venni, hogy az egyének szintjén az erőszak és az agresszió ellenszere nem a szociális érzékenység és az önámítás („velem ez nem történhet meg”), hanem a tudatos és hiteles kommunikáció. Az egyének valósidejű tájékozottságának növelése, illetve biztonság tudatosságuk fejlesztése elengedhetetlen közös érdek.

---

<sup>33</sup> HABÓK Lilla: Mennyit keres az informatikus? Íme a 2017-es számok!  
<https://www.hwsz.hu/hirek/57000/hays-salary-guide-fizetes-berek-bertargyalas-hr-fejlesztok-2017.html> (Letöltés ideje: 2017. 12. 31.)

### ***Felhasznált irodalom:***

- Ács Tibor: A hadikultúra történetéhez In: Hadtudomány, XV. évf. 2. sz. 2005. pp. 15-26. ISSN 1215-4121
- AJP 3-10. Allied Joint Doctrine for Information Operations pp. 1-3. <http://info.publicintelligence.net/NATO-IO.pdf> (Letöltés ideje: 2017. 12. 15.)
- Ált/57 Információs Műveletek Doktrína 1. kiadás, a Magyar Honvédség kiadványa 2014.
- BOLGÁR Judit – SZTERNÁK Nóra – SZTERNÁK György: A terrorizmussal kapcsolatos kutatások legújabb eredményei, Felderítő Szemle 2005. 4. sz. pp. 5-60. ISSN 1588-242X
- DELAUNEY. Guy: Kosovo's Hashim Thaci: From guerrilla leader to president. BBC News (2016. 04. 08.) <http://www.bbc.com/news/world-europe-35984823> (Letöltés ideje: 2017. 12. 31.)
- FORGÁCS Balázs: Napjaink hadikultúrái. (A hadviselés elmélete és fejlődési tendenciái a modern korban). ZMNE PhD értekezés (2009), [http://uni-nke.hu/downloads/konyvtar/digitgy/phd/2009/forgacs\\_balazs.pdf](http://uni-nke.hu/downloads/konyvtar/digitgy/phd/2009/forgacs_balazs.pdf) (letöltve: 2016. 12. 15.)
- GALULA, David: Counterinsurgency Warfare (1964), pp. 61-73., <http://ready4itall.org/wp-content/uploads/2013/05/Counterinsurgency-Warfare-Theory-and-Practice.pdf> (Letöltés ideje: 2017. 12. 15.)
- HABÓK Lilla: Mennyit keres az informatikus? Íme a 2017-es számok! <https://www.hsw.hu/hirek/57000/hays-salary-guide-fizetes-berek-bertargyalas-hr-fejlesztok-2017.html> (Letöltés ideje: 2017. 12. 31.)
- HAIG Zsolt: Információ, Társadalom, Biztonság, NKE Szolgáltató Kft, 2015. pp. 93-122. ISBN 978 615 5527 08 1
- HAIG Zsolt: Internet terrorizmus, Nemzetvédelmi Egyetemi Közlemények, 2007. 2. sz. pp. 81-93., ISSN 1417 7323
- KOVÁCS László: Kiberterrorizmus, (2008. 03. 19.) ZMNE, <http://slideplayer.hu/slide/5656918/> (Letöltés ideje: 2017. 12. 15.)
- KRASZNAI Csaba: A magyar elektronikus közigazgatás biztonsága. ZMNE előadás (2008. 07. 07.) [http://krasznay.hu/presentation/mhtt\\_ekozig\\_krasznay.ppt](http://krasznay.hu/presentation/mhtt_ekozig_krasznay.ppt) (Letöltés ideje: 2017. 12. 31.)
- RESPERGER István: Az aszimmetrikus hadviselés és a terrorizmus jellemzői In: Hadtudomány2010/4. pp. 68-77.
- RESPERGER István: Forrongó világ, nemzetbiztonsági kihívások 2030-ig, (2015. 11. 17.), [http://uni-nke.hu/uploads/media\\_items/12-resperger-istvan.original.pdf](http://uni-nke.hu/uploads/media_items/12-resperger-istvan.original.pdf) (Letöltés ideje: 2017. 12. 15.)
- RESPERGER István: Kis háborúk nagy hatással: a XXI. század fegyveres konfliktusai, a terrorizmus és az aszimmetrikus hadviselés jellemzői. Felderítő Szemle 2013/1 pp. 200-230. ISSN 1588-242X

- SIMON László – MAGYAR Sándor: A terrorizmus és indirekt hatása a kiberterében. Nemzetbiztonsági Szemle 2017. 3. sz. <https://www.uni-nke.hu/document/uni-nke-hu/nemzetbiztonsagi-szemle-2017-3-1.original.pdf> (Letöltés ideje: 2017. 12. 15.)
- SIMON László: A fokozódó terrorizmus Európában és annak hatása a katonai tömegrendezvények biztosítására. Szakmai Szemle, 2015. 2. sz. pp 145-162. ISSN 1785-1181
- SIMON László: Az információ mint fegyver? Szakmai Szemle, 2016. 1. sz. pp. 34-60. ISSN 1785-1181
- SMEJKÁL Péter: Halálos kibertámadásokra készül az Iszlám Állam (2015. 11. 17), <http://www.origo.hu/techbazis/20151117-islam-allam-halalos-kibertamadas-felkeszules-nagy-britannia-terrorizmus-parizs-tamadas.html> (Letöltés ideje: 2017. 12. 15.)
- Sz.n.: CIA: Az Iszlám Állam félelmetes és rugalmasan alkalmazkodik, MTI (2016. 06. 16.), <http://www.origo.hu/nagyvilag/20160616-cia-isis-islam-allam-erosebb-mint-az-al-kaida.html> (Letöltés ideje: 2017. 12. 15.)
- Sz.n.: Iszlám fanatikus támadhatta meg az Óbudai Egyetem honlapját, [www.origo.hu](http://www.origo.hu) <http://www.origo.hu/techbazis/20150519-isis-islam-allam-hacker-tamadas-hackertamadas.html> (Letöltés ideje: 2017.12.15.)
- Sz.n.: NATO: Warsaw Summit Communiqué 70-71 pont, [http://www.nato.int/cps/en/natohq/official\\_texts\\_133169.htm#cyber](http://www.nato.int/cps/en/natohq/official_texts_133169.htm#cyber) (Letöltés ideje: 2017. 11. 31.)
- Sz.n.: Az Európai Unió kiberbiztonsági stratégiája. <http://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A52013JC0001> (Letöltés ideje: 2017. 12. 31.)
- TÓTH Péter – HORVÁTH Helga: A szubjektív biztonságérzetet befolyásoló tényezők Magyarországon, 2014, [http://kgk.sze.hu/images/dokumentumok/kautzkiadvany2014/TothP\\_HorvathH.pdf](http://kgk.sze.hu/images/dokumentumok/kautzkiadvany2014/TothP_HorvathH.pdf) (Letöltés ideje: 2017. 12. 15.)

### Bevezetés

Az ezredfordulót követően valami örökre megváltozott a világban. Távoli földrészek történései karnyújtásnyira kerültek, a világ minden eseménye elérhető a nappalinkban, egymástól elszakadt családok óceánokat átívelő napi kapcsolatban állhatnak, gyakorlatilag ingyen. Divatosan azt mondjuk, hogy globalizáció van. Megszűnik a hagyományos posta, a hagyományos levelezés, a hagyományos verbális kommunikáció, a hagyományos vezetés-irányítási rendszer bizonyos elemei, a hagyományos „minden”. Az informatika robbanásszerű térhódítása megállíthatatlan. Az emberiség fejlődésének történetében nincs még két olyan egymást követő évtized (különösen nem évszázad), amely annyira különböző egymástól, mint az 1990-es, a 2000-es és a 2010-es évek. Azt lehet mondani, hogy szinte évtizedenként egy-egy új generáció fejlődik tovább az informatika legtöbb területén. És valóban, talán nem véletlenül, a sávszélességek vonatkozásában így is hívják a képességeket, hogy 3. generáció, 4. generáció.

Az első internetes közösségi oldalak még csak nem is nagykorúak, de mára tömegeknek vált elképzelhetlenné nélkülük az élet, sőt, mindennapjaink bizonyos területein alapvető kommunikációs platformmá avanzáltak. A világ egyik vezető közösségi média szolgáltatása a 2004-es alapítását követő 8 évben több mint 1 milliárd felhasználót ért el. Az ezt követő 2012-es tőzsdei megjelenése óta eltelt 5 évben ezt megduplázta, és kezdi kiterjeszteni a tevékenységét további szolgáltatási körökre annak érdekében, hogy gyorsabbá, egyszerűbbé, olcsóbbá tegye a felhasználóinak az életét, ezáltal átvéve olyan területeket, ahol az ott már meglévő piaci szereplők alapvető és súlyos hátrányból indulnak a „hozzáférés”, a fogyasztók elérése és megszólítása tekintetében. Mindezzel párhuzamosan az internet is közelebb került az emberekhez azáltal, hogy olyan mobil eszközök jelentek meg, amelyekkel „állandó”, online kapcsolatban állhat az egész emberiség. Képzeljük el, hogy a mai fogyasztói társadalmak korában mit ér az, ha meg tudunk szólítani 2.000.000.000, azaz két milliárd embert egyidőben.

Természetesen ez a jelenség magában hordozza számtalan sok újszerű lehetőség, igény megfogalmazódását, kibontakozását is, amelyek mindegyikének alapfeltétele az internethez való kapcsolódási képesség.

Az Európai Unió (EU) ezt a potenciált ismerte fel, amikor zászlajára tűzte a Digitális Európa képét és – lévén eredendően gazdasági társulás – megcélozta a Digitális Egységes Piac létrehozását, amely megvalósításához koncepcionális stratégiát dolgozott ki.

Összefoglaló esszémben azt kívánom bemutatni, hogy ebben a legújabb, az egész világunk arculatát befolyásoló folyamatban Magyarország, mint állam, hol találta meg a helyét és milyen módon csatlakozik az események fő sodrához.

## Az internet hálózatának kezdetei

1957-ben, a hidegháború kezdetén, a Szovjetunió pályára állította az első mesterséges holdat a világűrben, a Szeptnyikot, amire válaszul az Egyesült Államok létrehozta a Védelmi Minisztérium gondozásában a Fejlett Kutatási Projektek Ügynökségét (Advanced Research Projects Agency), az ARPA-t. Az ARPA 1966-ra megalkotta a világ első számítógépek közötti hálózati kapcsolat tervét, az ARPANET-et<sup>1</sup>. Az ezt követő évek fejlesztői munkájának eredményeként az ARPANET megvalósult és a tudomány nevében előbb egyetemek munkaállomásait kapcsolta egy hálózatba, majd több hálózat közötti kapcsolat feltételeit teremtette meg. 1983-ban az ARPANET két részre vált, és létrejött a MILNET (amerikai katonai hálózat, a későbbi DDN, a Defense Network része)<sup>2</sup> és a ma ismert polgári felhasználású internet. Ez utóbbi, a tudomány úttörő munkássága révén, az amerikai tudományos élet, illetve az oktatás fejlesztése érdekében létrehozott és az Amerikai Egyesült Államokat behálózó, jellemzően egyetemeket összekötő, National Science Foundation Network (NSFNET)<sup>3</sup> keretében fejlődött tovább, ezzel háttérbe szorítva az „anyahálózatot”, az ARPANET-et, amelyet végül 1989-ben le is kapcsoltak.

Korunk internetje, a World Wide Web (WWW) 1989-ben, a svájci CERN (Európai Nukleáris Kutatási Szervezet) kutatója, Tim Berners-Lee és kollégái munkájának köszönhetően jött létre azáltal, hogy megalkották azokat a definíciókat és protokollokat, amelyek közös alapokra helyezték a hálózatba, hálózatokba kötött számítógépek kommunikációját. Az így létrejött hálózatban a HTTP (HyperText Transfer Protocol) segítségével kommunikáló számítógépek URL (Uniform Resource Locator)-címek alapján értek el a HTML (HyperText Markup Language) nyelvben programozott oldalakat, illetve egymást. Az ehhez a rendszerhez tervezett és általuk létrehozott, 1992-ben megjelent szöveges böngésző gyorsan kedveltté vált. Egy évvel később, ezt a protokollt használva, az amerikai Marc Andreessen és csapata megalkotta az első grafikus böngészőt, a Mosaic-ot, amelyet követően 1994-ben útjára engedték az első világszerte ismert web böngészőt, a Netscape Navigator-t, amelynek köszönhetően a '90-es évek második felére már milliók használták<sup>4</sup> a WWW-t, azaz a világhálót. 20 évvel később majdnem 4 milliárdnyian<sup>5</sup>.

## Gazdasági világválság, átértékelt kölcsönhatások, új irány

Már az EU 2000-ben elfogadott lisszaboni stratégiája is megfogalmazott olyan irányokat a közös európai politika számára, amelyeknek fontos szerepük volt abban, hogy a 21. század kihívásait az EU tagállamai egységes látásmóddal értékeljék. Annak ellenére, hogy az olyan elveket, mint a versenyképesség, az oktatás fontossága, az innováció vagy a hosszú távú fenntarthatóság egységes és széleskörű konszenzus övezte, a 2000-2010 közötti időszakra megfogalmazott irányelvek

---

<sup>1</sup> FEATHERLY, Kevin: ARPANET United States Defense Program, <https://www.britannica.com/topic/ARPANET> (Letöltés ideje: 2018. 01. 08.)

<sup>2</sup> MILNET, <https://www.techopedia.com/definition/27932/milnet> (Letöltés ideje: 2018. 01. 08.)

<sup>3</sup> NSFNET, <http://www.tech-faq.com/nsfnet.html> (Letöltés ideje: 2018. 01. 08.)

<sup>4</sup> World Wide Web, <https://www.britannica.com/topic/World-Wide-Web> (Letöltés ideje: 2018.01.09.)

<sup>5</sup> Internet World Stats, <http://www.internetworldstats.com/stats.htm> (Letöltés ideje: 2018. 01. 12.)

inkább voltak teoretikusak, mint gyakorlatiasak<sup>6</sup>. Azon túl, hogy nem tudták tökéletes összhangban, egy irányba mozdítani a szervezetet, a 2008-as gazdasági recesszió különösen felkészületlenül és cselekvésképtelenül érte a tagállamokat. Közelebről megvizsgálva a 2000-es éveket látható, hogy az informatika, az internet, a mobilkommunikáció és a mobilalkalmazások dömpingje még gyerekcipőben járt és csak az évtized végére terjedt el végérvényesen a mindennapjainkban. A világ figyelmét a 2001. szeptember 11-ei terrorcselekmény<sup>7</sup>, az afganisztáni, majd iraki események kötötték le.

Ezért amikor az Európai Bizottság 2010-ben elkészítette a következő, 2010-2020 közötti időszakra vonatkozó lisszaboni stratégiai tervét, már figyelembe vette a korábbi évek tapasztalatait, a válság hatásának elemeit, illetve az informatika forradalmát, ezért bár hasonló elvek mentén, de feladatorientáltabban fektették le az elérendő célokat.

Megfogalmazták az intelligens-, a fenntartható- és az inkluzív növekedés kívánalmait, mint prioritásokat a következő évtizedre. Konkrét célokat tűztek ki, mint például a 20-64 éves korosztály foglalkoztatásának a 75%-ra emelése, a kutatás-fejlesztésre fordított összeg az EU GDP-arányos 3%-ra emelése, a megújuló energiaforrások arányának 20%-ra emelése, a 30-34 év közötti uniós állampolgárok felsőfokú iskolázottságának a 40%-ra emelése, illetve a társadalom perifériáján élők számának legalább 20 millió fővel való csökkentése<sup>8</sup>.

A célok eléréséhez vezető, a prioritások mentén elvégzendő feladatokat az alábbi fő irányvonalakban, kiemelt kezdeményezésekben határozták meg. Az intelligens növekedéshez A Digitális Menetrend (Digital Agenda for Europe), Az Innovatív Unió és a Mozgásban az ifjúság (Youth on the move) nevű kezdeményezések járulnak hozzá. A fenntartható növekedés alapjait az erőforrás-hatékony Európa és a globalizációs kornak megfelelő iparpolitika adja. Az inkluzív növekedéshez pedig a munkahelyek és a készségek optimalizálásának a terve, illetve egy szegénység elleni európai platform kialakítása szükséges. A terv javaslatára értelmében a tagállamoknak le kellett bontaniuk az uniós célkitűzéseket nemzeti célkitűzésekre.

### **Digitális Magyarország az uniós stratégia tükrében**

Az EU 2020 stratégiában megfogalmazódó kiemelt kezdeményezések meghatározó alapelemei többek között a kis- és középvállalkozások (KKV) térnyerése, az innováció, a gyors, mindenki számára hozzáférhető internet és az egységes európai piac megerősítése, bizonyos szempontból a tagállamok szorosabb együttműködése, mondhatni az Unión belüli mindennemű interoperabilitás.

Amikor Jean-Claude Juncker, az Európai Bizottság jelenlegi elnöke 2014. július 15-ei strasbourgi elnökjelölti beszédében kiemelte a Digitális Egységpiac

---

<sup>6</sup> Vértess: a lisszaboni stratégiai célok jók, az eszközök elégtelenek, [http://hvg.hu/gazdasag/20090525\\_GKI-konferencia\\_Vertes\\_lisszaboni\\_Eu](http://hvg.hu/gazdasag/20090525_GKI-konferencia_Vertes_lisszaboni_Eu), (Letöltés ideje: 2018. 01. 12.)

<sup>7</sup> Az afganisztáni lett az USA történetének leghosszabb háborúja, [www.origo.hu/nagyvilag/20100608-az-afganisztani-lett-az-usa-tortenetek-leghosszabb-haboruja.html](http://www.origo.hu/nagyvilag/20100608-az-afganisztani-lett-az-usa-tortenetek-leghosszabb-haboruja.html), (Letöltés ideje: 2018. 01. 26.)

<sup>8</sup> EUROPE 2020 Strategy, <https://www.finance-ni.gov.uk/articles/europe-2020-strategy> (Letöltés: 2018. 01. 12.)

(Digital Single Market)<sup>9</sup> jelentőségét, akkor Magyarországon már hatályban volt a Nemzeti Infokommunikációs Stratégia 2014-2020 (NIS)<sup>10</sup> elnevezésű dokumentum, amely egyben az az EU 2020 Stratégiában szereplő Digitális Menetrendben meghatározott célok eléréséhez szükséges feladatok nemzeti szintre adaptálása is. A NIS célja, „*hogy koherens képet adjon a magyar információs társadalom jelenlegi viszonyairól, és ez alapján a 2014-20-as uniós tervezési ciklussal egybeeső időtávra meghatározza az infokommunikációs területre vonatkozó fejlesztési irányokat, közpolitikai, szabályozási és támogatási teendőket, és számba vegye az ezek megvalósításához szükséges eszközöket/erőforrásokat.*”<sup>11</sup> A hazai stratégiában megfogalmazott célok eléréséhez a Nemzeti Fejlesztési Minisztérium kidolgozta a 2014 decemberében elfogadott „Zöld Könyvet”, amely részleteiben határozta meg a fejlesztési irányokat, az elvárt tevékenységeket.<sup>12</sup>

A NIS négy nagy pilléren nyugszik, amelyek közül a legfontosabb a Digitális infrastruktúra. A Digitális infrastruktúra az a hírközlési infrastruktúra, amely lehetővé teszi a digitális szolgáltatást és annak igénybevételét a hálózat teljes szegmensében. Az erre épülő további pillérek a Digitális Kompetenciák, a Digitális Gazdaság és a Digitális Állam, ahol a kompetenciák kialakulása jellemzően a lakosság oktatásával elérhető fejlesztéssel valósítható meg, míg a gazdaság és állam területein jellemzően az elektronikus szolgáltatások létrehozásán és fejlesztésén van a hangsúly.

Az EU 2020 stratégiában megjelenő Digitális Menetrendben foglaltak nemzeti vetülete egyben a Nemzeti Infokommunikációs Stratégiában megfogalmazottak végső célja is, a Digitális Magyarország.

### **Úton 2020 digitális Európája felé**

A Digitális Magyarország megvalósítása digitalizálás<sup>13</sup> útján, a NIS-ben megfogalmazott pillérekhez hasonló, releváns alapokon nyugszik.<sup>14</sup> Első lépésként megteremti az ország egészét lefedő szupergyors internetet eléréshez szükséges infrastruktúrát. Ez a tervek szerint 2018 év végéig megvalósul. Második lépésként a digitális közösség- és gazdaságfejlesztéssel megteremti azt a környezeti hátteret, kiemelten a KKV-k körében, amellyel igénybe vehetőek az elektronikus szolgáltatások, ezáltal hozzájárulva Magyarország Unión belüli gazdasági versenyképességéhez. A harmadik tevékenységi kör az e-közszolgáltatások

---

<sup>9</sup> A New Start for Europe: My Agenda for Jobs, Growth, Fairness and Democratic Change, - [https://ec.europa.eu/commission/sites/beta-political/files/juncker-political-guidelines-speech\\_en.pdf](https://ec.europa.eu/commission/sites/beta-political/files/juncker-political-guidelines-speech_en.pdf) (Letöltés ideje: 2018. 01. 12.)

<sup>10</sup> Nemzeti Infokommunikációs Stratégia 2014-2020, [http://www.nisz.hu/sites/default/files/u1/nemzeti\\_infokommunikacios\\_strategia\\_2014\\_2020.pdf](http://www.nisz.hu/sites/default/files/u1/nemzeti_infokommunikacios_strategia_2014_2020.pdf) p. 10., (Letöltés ideje: 2018. 01. 12.)

<sup>11</sup> Nemzeti Infokommunikációs Stratégia 2014-2020, [http://www.nisz.hu/sites/default/files/u1/nemzeti\\_infokommunikacios\\_strategia\\_2014\\_2020.pdf](http://www.nisz.hu/sites/default/files/u1/nemzeti_infokommunikacios_strategia_2014_2020.pdf) p. 10., (Letöltés ideje: 2018. 01. 12.)

<sup>12</sup> „Zöld könyv”, <http://digitalismagyarorszag.kormany.hu/download/f/35/e0000/Z%C3%B6ld%20K%C3%B6nyv.pdf>, (Letöltés ideje: 2018. 01. 12.)

<sup>13</sup> Digitalizálás – amelynek során főként egy más hordozón már megjelent művet (szöveget, képet, hangot) számítógéppel olvasható, kódolt formába alakítunk át., <http://elmenyor.hu/digitalizalas-tisztazzuk-az-alapokat>, (Letöltés: 2018. 01. 26.)

<sup>14</sup> Digitális Magyarország, <http://digitalismagyarorszag.kormany.hu/digitalis-magyarorszag>, (Letöltés ideje: 2018. 01. 12.)



bevezetése, amellyel az államigazgatási feladatrendszert racionalizálja. Végezetül kiemelt hangsúlyt fektet a digitális készségek megteremtésére úgy a köznevelésben, mint a felsőoktatásban és a hátrányos helyzetű célcsoportok vonatkozásában, amelynek alapja a lakosság digitális Európába illesztése és ezáltal Magyarország versenyképességének megőrzése.

### **A magyarországi feladatrendszer**

Hazánkban a Digitális Menetrenddel és a Digitális Magyarországgal összefüggésben keletkező mindennemű feladatot a Miniszterelnöki Kabinetirodához tartozó Digitális Jólét Program koordinálja. A Program folyamatosan készíti elő és terjeszti fel azokat a stratégiákat, amelyek az EU által megfogalmazott digitális célok eléréséhez szükségesek. A 2016-os évben elkészült a Digitális Gyermekvédelmi Stratégia, a Digitális Exportfejlesztési Stratégia és a Digitális Oktatási Stratégia. A 2017-es évben a tevékenység lendületet váltott, kibővítésre került és elkészült a Digitális Jólét Program 2.0 (DJP2.0) terve, amely az EU stratégiákkal szoros összhangban, az addig elért eredményeket figyelembe véve további irányokat határozott meg. A stratégiai dokumentum folytatja azt a törekvést, miszerint a Digitális Európában a Digitális Magyarországot minél előnyösebb helyzetbe kívánja hozni azáltal, hogy a digitalizáció folyamatában Magyarországot több szegmensben is lépéselőnyhöz juttatja. Ennek megfelelően már 2017 májusában elhangzott, hogy több százmilliárd forintos digitalizációs fejlesztés zajlik, amelynek keretén belül halad a Szupergyors Internet Program és a mobilszolgáltatók is elérték a teljes 4G lefedettséget. A lefedettség kapcsán megalakult a magyarországi 5G Koalíció (5GK), amelynek célja, hogy Magyarországot az 5G fejlesztés és a regionális tesztelesek egyik európai központjává emelje. Az elnökség összetétele<sup>15</sup> arra enged következtetni, hogy a vezető piaci szereplők, a tudományos háttérbázis és a kormányzati szervek jelenléte, valamint közös munkája teremti meg a feltételét annak, hogy Magyarország optimális helyzetből nézhessen szembe a kihívásokkal, továbbá, hogy jó versenyhelyzetbe kerüljön.

A DJP2.0 keretében kidolgozás alatt állnak a digitális kompetenciák, és azok hosszú távú fejlesztési és mérési lehetőségei. Folyamatban van a különböző ágazatok digitális átalakítási stratégiáinak a kidolgozása is. Tekintettel arra, hogy a gazdasági fejlődés alapja a digitális világban is a szakképzett munkaerő, (amiből értékelésem szerint hiány mutatkozik), ezért kiemelt figyelmet kap a Digitális Munkaerő Program<sup>16</sup> végrehajtása. Mindezekon túlmenően készül Digitális Agrár Stratégia, Digitális Egészségipari-fejlesztési Stratégia és Digitális Sport Stratégia

---

<sup>15</sup> Az 5GK elnökségi tagjai: Deutsch Tamás, a Digitális Jólét Program miniszterelnöki biztosa; Király István, a Vodafone Vállalati Szolgáltatások Üzletág vezérigazgató-helyettese; Jakab Roland, az Ericsson Magyarország Kft. ügyvezető igazgatója (egyben az IVSZ digitális transzformációért felelős alelnöke); Kaszás Zoltán, a T-Systems vezérigazgatója; Jakab László BME Villamosmérnöki és Informatikai Karának dékánja; Major Gábor, az IVSZ főtitkára és Dr. Parragh László, a Magyar Kereskedelmi és Ipari Kamara elnöke.

<sup>16</sup> A Digitális Munkaerő Program az IVSZ kezelésében lévő megoldási javaslat az informatikus és digitális szakember hiány kezelésére <http://ivsz.hu/wp-content/uploads/2016/09/ivsz-digitalis-munkaero-program.pdf>, (Letöltés ideje: 2018. 01. 12.)

2.0<sup>17</sup> A teljes közigazgatás digitalizációját támogató továbbképzési programok is elindításra kerültek. Magyarország tehát halad az EU által kijelölt úton.

### **Aktuális helyzet számokban**

A továbbképzési programok kapcsán megjegyzést érdemel, hogy a Nemzeti Fejlesztési Minisztérium megbízásából a Kormányzati Informatikai Fejlesztési Ügynökség 2015-ben megrendelt egy összefoglaló tanulmányt a BellResearch kutató cégtől. „A hazai informatikus- és IT-mérnökképzés helyzetének, problémáinak, gátló tényezőinek vizsgálata”<sup>18</sup> címmel, amely rendkívül részletes tanulmány megállapította, hogy a hazai munkaerő-piacon 22 ezer üres informatikai állás van, amely üres pozíciók közvetett multiplikátor hatásai összesen 72 ezer munkavállalónak adhatnának munkát a nemzetgazdaságban. Tekintettel arra, hogy a NIS-ben leírtak alapján a magyar GDP mintegy 12%-át adja az IKT<sup>19</sup>-szektor, amely szektorban a nevezett tanulmány szerint 122 ezren dolgoztak, illetve további 40 ezren az ágazaton kívüli informatikai munkakörben tevékenykedtek, ezért látható, hogy a 22 ezres hiány az összesen 72 ezer fő felvételére képes munkahelyteremtő potenciállal már önmagában is igen jelentős GDP arányt, illetve növekedést eredményezne.

A tanulmány azon túl, hogy részletesen kitér az okokra is, feltárja a problémákat (oktatás hiányosságai, versenyszféra elszívó ereje stb.), egyértelműen megalapozza az IVSZ által megfogalmazott, és a Digitális Munkaerő Program jelentőségét növelő megállapítást: „Az informatikusok és magasan képzett digitális szakemberek hiánya ezért nemcsak a magyar IKT szektor, hanem a teljes digitális gazdaság, s így áttételesen a nemzetgazdaság további fejlődésének is a legfőbb akadály.”<sup>20</sup>

### **Digitális Európa 2020-ban, avagy sok még a tennivaló**

A fentiekén túl, az informatikus és IT-szakemberhiány kérdésköre a jövőben még kritikusabb lesz, mert a Digitális Európa képe nem csak a Digitális Egységpiac létrejöttét jelenti, hanem további megvalósítandó célok összessége, amelyek első lépcsője az egyébként is erős európai ipar továbbfejlesztése.

Az EU 2016. április 16-án bemutatta az Európa Digitális Ipara<sup>21</sup> tervét, amelyben azokra az a már meglévő nemzeti kezdeményezésekre alapozza az európai digitális ipart, mint a németországi Industrie 4.0, a szlovák és holland Smart Industry, az olasz Fabbrica Intelligente, vagy francia Nouvelle France Industrielle. A digitális ipari átállás az előzetes felmérések alapján, tekintettel az újabbnál-újabb

<sup>17</sup> <http://www.kormany.hu/hu/miniszterelnoki-kabinetiroda/digitalis-jolet-program/hirek/digitalis-jolet-program-2-0-attores-a-digitalis-fejleszteseekben> (Letöltés ideje: 2018. 01. 12.)

<sup>18</sup> <http://ivsz.hu/wp-content/uploads/2016/03/a-hazai-informatikus-es-it-mernokkepzes-helyzetenek-problemainak-gatlo-tenyezoinek-vizsgalata.pdf> 4. oldal (Letöltés ideje: 2018. 01. 26.)

<sup>19</sup> IKT–ICT Information and Communication Technologies, Információs és kommunikációtechnológia, azokat a technológiákat jelenti, amelyek információkhoz való hozzáférést biztosítanak telekommunikációs eszközökön keresztül., <https://techterms.com/definition/ict>, (Letöltés ideje: 2018. 01. 26.)

<sup>20</sup> Digitális Munkaerő Program <http://ivsz.hu/digitalis-munkaero-program/> (Letöltés ideje: 2018. 01. 12.)

<sup>21</sup> Digitising European Industry, <https://ec.europa.eu/digital-single-market/en/policies/digitising-european-industry> (Letöltés ideje: 2018. 01. 13.)

technológiai vívmányok megjelenésére is, évi 110 milliárd EUR<sup>22</sup> többletbevételt jelentene az első 5 évben az EU-nak. A megvalósításhoz 50 milliárd EUR áll rendelkezésre, amely fedezi az Európai Felhő (European Cloud Initiative) létrejöttét szorgalmazó terv végrehajtását is.

Napjaink egyik szignifikáns jelensége az IoT (Internet of Things – minden „dolog” ami az internetre csatlakozik). Manapság már nem csak számítógépek és mobiltelefonok csatlakoznak, hanem órák, TV-k, hűtőszekrények, lakások, autók stb. Ahhoz, hogy az internetre csatlakozó „dolgokat” kezelni tudjuk, mind nagyobb számolási kapacitású számítógépekre, memóriára és tárhelyre van szükség. Különösen igaz ez akkor, ha olyan rendszerekről beszélünk, mint az M2M (Machine to Machine – gép a géppel), ahol előre programozott módon, automatizált folyamatok, akciók-reakciók játszódnak le gépek között, de akkor is igaz, amikor a virtuális fizetési rendszer alapját adó blockchain<sup>23</sup> technológia használata van folyamatban. Az EU számítása szerint 2020-ra 25 milliárd<sup>24</sup> eszköz fog csatlakozni egyszerre a netre és évi 2 Zeta-Byte<sup>25</sup> forgalmat fog bonyolítani.

Az EU felismerte, hogy a digitális forradalomhoz való igazodás csak gyors adatkapcsolattal rendelkező szuperszámítógépek és kvantumszámítógépek felhő-alapú tárolási kapacitásával valósítható meg, mert ez az egyetlen módszer, ami garantálja, hogy az Európai Egységpiac valóban egységes, a kontinens bármelyik pontjáról irányítható és működőképes legyen. Ennek megfelelően, a kvantum számítástechnika és annak fejlesztése is prioritást élvez, és stratégiai fontossággal bír.

A számolási sebesség, a tárhely-kapacitás és a nagyadat<sup>26</sup> problematikája mellett az EU kiemelten kezeli a kiberbiztonság és az 5G adatkapcsolat kiépítésének kérdését is, illetve felismerte, hogy a digitális ipar megteremtésének előfeltétele a digitális kormányzás (e-Government), ezért kiadta az EU eGovernment Action Plan 2016-2020 elnevezésű dokumentumot, amelyben már a 2016-2017-es évekre is megfogalmazott elérendő célokat. Ennek a tervnek a fő célja, hogy az EU tagállamaiban a közügyek intézése digitálisan történjen, ezáltal közelebb hozva a tagállamok állampolgárait és vállalkozásait egymáshoz, így előmozdítva az egységes digitális piac létrejöttét, ami a várakozások szerint évi több száz milliárd euró<sup>27</sup> bevételi többletet jelentene az EU-nak.

---

<sup>22</sup> [http://europa.eu/rapid/press-release\\_MEMO-16-1409\\_en.htm](http://europa.eu/rapid/press-release_MEMO-16-1409_en.htm) (Letöltés ideje: 2018. 01. 13.)

<sup>23</sup> Blockchain – A blockchain alapvetően egy felhasználók közötti megosztott, visszamenőleg megmásíthatatlan digitális főkönyv, ha úgy tetszik, egy adatbázis, amely minden felhasználó előtt egységes, aktuális tranzakciós listát tartalmaz., <https://www.pwc.com/hu/hu/sajtoszoba/2017/blockchain.html>, (Letöltés ideje: 2018. 01. 26.)

<sup>24</sup> High Performance Computing, <https://ec.europa.eu/digital-single-market/en/high-performance-computing> (Letöltés ideje: 2018. 01. 13.)

<sup>25</sup> 1 Zeta-Byte, az 1 milliárd Terra-Byte-tal egyenlő

<sup>26</sup> Big Data – A „Big Data” a cégek, az intelligens hálózatok, a magánszektor és az egyéni felhasználók által világszerte és napi szinten előállított óriási adatmennyiséget jelenti. <https://www.it-services.hu/hirek/mi-az-a-big-data/> (Letöltés ideje: 2018. 01. 13.). Bővebben: ILLÉS Noémi: A NAGY ADAT; A nagy adat nemzetbiztonsági aspektusai. Budapest, Szakmai Szemle, 2016. 4. sz. pp. 101-135. ISSN 1785-1181

<sup>27</sup> Európai digitális egységes piaci stratégia <http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52015DC0192&from=EN> (Letöltés ideje: 2018. 01. 13.)

## Következtetések

A fejlesztés közben megfogalmazódnak ugyanakkor bizonyos aggályok a digitális világ sebezhetőségét illetően. Gyakorta lehet hallani a különböző kibertámadásokról, vagy kísérletekről, illetve egyre többször és mind szélesebb körben hívják fel a lakosság figyelmét a következetes internethasználatra. Vitathatatlan, hogy az európai lakosság ezirányú képzése elengedhetetlen és maga az EU is a kibervédelemmel szoros együttműködésben tervezi megvalósítani a digitális világot. Nem beszélve arról, hogy a jogi szabályozás rendszerének is le kell követnie az eseményeket.

Ezzel együtt is azonban meg kell állapítani, hogy a Digitális Európa nem csak a gazdaság viszonylatában biztosít kiemelkedő lehetőségeket, hanem többek között a biztonsági szektorban is. Egy digitalizált keretrendszer létrehozása után, ahol a keretrendszer a digitális infrastruktúrára épülő digitális államigazgatás meglétét jelenti, már folyamatosan lehet a különböző automatizált rendszereket integrálni. Egy digitális országban a kereskedelem, a bankszektor, a közlekedés, az oktatás, az egészségügy, stb. minden szegmensét egy rendszerbe lehet kötni, ami kiemelt lehetőséget biztosít a rendvédelmi és titkosszolgálati szervezeteknek arra, hogy minden szempontból növeljék az ország biztonságát.

Ahhoz azonban, hogy az ebben rejlő potenciált optimálisan kihasználjuk, minél előbb meg kell határozni a rendvédelmi és titkosszolgálati szervezeteknek a súlypontokat, kiemelt területeket, amelyek megteremtéséhez létre kell hozni a feltételeket, előkészíteni a jogi szabályozást és mellérendelni a finansziális tervezést. Gyakorlatilag nem csak az államigazgatásnak kell az EU Digitális Menetrendjébe beilleszkedni, de a manapság konstans terrorfenyegetettség miatt a biztonságért felelős szervezeteknek is.

Európa nagyléptekkel halad a digitalizáció útján, mint az egyetlen úton, ami a jövőbe vezet. Az irányt illetően annyira biztosak vagyunk, hogy 2014-ben létre is jött a DigitalEurope<sup>28</sup> nevű non-profit szervezet, amely az európai digitális technológiában érdekelt cégeket tömöríti annak érdekében, hogy Európát a világ vezető gazdasági hatalmává emelje.

Jelenleg 60 olyan cég áll szoros kapcsolatban (például az Apple, az Amazon, a Canon, a Cisco, a Dell, a HP, az Intel, a Lenovo, vagy a Samsung), tehát a világ minden tájáról a legnagyobbak, és 37 kereskedelmi szövetség, köztük a fent nevezett magyar IVSZ is tagja a szervezetnek, tehát karnyújtásnyira van minden segítség, legyen az technológiai probléma vagy üzleti kérdés.

A mindent átölelő stratégiai tervezés és végrehajtás megkezdődött. Az elmaradott földrészek mellett lesz a bolygón végre egy digitális kontinens is. Már csak a kvantumszámítógépek hálózatában életre kelt mesterséges intelligencia irányította automata M2M rendszerek és szenzorai hiányoznak, és akkor csak remélhetjük, hogy érteni fogjuk, hogy mi vesz minket körül 20 év múlva.

---

<sup>28</sup> <http://www.digitaleurope.org/About-Us> (Letöltés ideje: 2018.01.13.)

### ***Felhasznált irodalom:***

- A New Start for Europe: My Agenda for Jobs, Growth, Fairness and Democratic Change, [https://ec.europa.eu/commission/sites/beta-political/files/juncker-political-guidelines-speech\\_en.pdf](https://ec.europa.eu/commission/sites/beta-political/files/juncker-political-guidelines-speech_en.pdf) (Letöltés ideje: 2018. 01. 12.)
- ILLÉS Noémi: A NAGY ADAT; A nagy adat nemzetbiztonsági aspektusai. Budapest, Szakmai Szemle, 2016. 4. sz. pp. 101-135. ISSN 1785-1181
- Digitális Magyarország, <http://digitalismagyarorszag.kormany.hu/digitalis-magyarorszag>, (Letöltés ideje: 2018.01.12.)
- Digitális Munkaerő Program <http://ivsz.hu/digitalis-munkaero-program/> (Letöltés ideje: 2018.01.12.)
- Digitising European Industry, <https://ec.europa.eu/digital-single-market/en/policies/digitising-european-industry> (Letöltés ideje: 2018.01.13.)
- Európai digitális egységes piaci stratégia <http://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52015DC0192&from=EN> (Letöltés ideje: 2018.01.13.)
- EUROPE 2020 Strategy, <https://www.finance-ni.gov.uk/articles/europe-2020-strategy> (Letöltés: 2018.01.12.)
- FEATHERLY, Kevin: ARPANET United States Defense Program, <https://www.britannica.com/topic/ARPANET> (Letöltés ideje: 2018.01.08.)
- High Performance Computing, <https://ec.europa.eu/digital-single-market/en/high-performance-computing> (Letöltés ideje: 2018.01.13.)
- Internet World Stats, <http://www.internetworldstats.com/stats.htm> (Letöltés ideje: 2018. január 12.)
- MILNET, <https://www.techopedia.com/definition/27932/milnet> (Letöltés ideje: 2018.01.08.)
- Nemzeti Infokommunikációs Stratégia 2014-2020, [http://www.nisz.hu/sites/default/files/u1/nemzeti\\_infokommunikacios\\_strategia\\_2014\\_2020.pdf](http://www.nisz.hu/sites/default/files/u1/nemzeti_infokommunikacios_strategia_2014_2020.pdf) p. 10., (Letöltés ideje: 2018.01.12.)
- NSFNET, <http://www.tech-faq.com/nsfnet.html> (Letöltés ideje: 2018.01.08.)
- Vértés: a liszaboni stratégiai célok jók, az eszközök elégtelenek, [http://hvg.hu/gazdasag/20090525\\_GKI-konferencia\\_Vertes\\_lisszaboni\\_Eu](http://hvg.hu/gazdasag/20090525_GKI-konferencia_Vertes_lisszaboni_Eu), (Letöltés ideje: 2018.01.12.)
- World Wide Web, <https://www.britannica.com/topic/World-Wide-Web> (Letöltés ideje: 2018.01.09.)
- Zöld könyv, <http://digitalismagyarorszag.kormany.hu/download/f/35/e0000/Z%C3%B6ld%20K%C3%B6nyv.pdf>, (Letöltés ideje: 2018.01.12.)
- <http://www.digitaleurope.org/About-Us> (Letöltés ideje: 2018.01.13.)

- [http://europa.eu/rapid/press-release\\_MEMO-16-1409\\_en.htm](http://europa.eu/rapid/press-release_MEMO-16-1409_en.htm) (Letöltés ideje: 2018.01.13.)
- <http://ivs.hu/wp-content/uploads/2016/03/a-hazai-informatikus-es-it-mernokkepzes-helyzetenek-problemainak-gatlo-tenyezoinek-vizsgalata.pdf> (Letöltés ideje: 2018. 01. 12.)
- <http://www.kormany.hu/hu/miniszterelnoki-kabinetiroda/digitalis-jolet-program/hirek/digitalis-jolet-program-2-0-attores-a-digitalis-fejleszteseekben> (Letöltés ideje: 2018.01.12.)
- <https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/> (Letöltés ideje: 2018.01.10.)
- <https://www.pwc.com/hu/hu/sajtoszoba/2017/blockchain.html>, (Letöltés ideje: 2018.01.26.)
- <https://techterms.com/definition/ict> (Letöltés ideje: 2018.01.26.)

KOVÁCS KRISZTIÁN

**ALDRICH HAZEN AMES TÖRTÉNETE II.**

---

Az első részben megismerhettük Ames személyét, élettörténetét, titkosszolgálati pályafutását és kémkedésének motivációját. A történet érdekes részletekkel szolgált Magyarország érintettségére is, hiszen Amesnek lehetett szerepe egy magyar katonai hírszerző lebuktatásában, illetve hozzá kötődik az egyik legsikeresebb magyar katonai hírszerző művelet dekonspirációját végrehajtó orosz GRU ezredes elárulása is.

**Róma**

Ames, főnökei javaslatára elvállalt egy római beosztást. Rick és Rosario 1986 júliusában Rómába utazott, ahol Ames alosztályvezetői pozícióba került (Enemy Target Branch). Feladatuk a szovjet és kelet-európai, illetve a kínai és észak-koreai vonatkozású műveletek végzése volt. Hozzáférésrel rendelkezett az ügynökök adataihoz, a tervezett találkozókhoz és a jelentésekhez. Részt vett az Állomás heti értekezletein, ahol a tervezett és meglévő ügynökök dolgait átbeszélték, koordinálta a kettős ügynök műveleteket a katonai szolgálatokkal és hírszerzési jelentéseket kapott a világ eseményeiről. Bár az új beosztás közel sem jelentett széleskörű hozzáférést a CIA műveletekhez, a KGB sosem kérte, hogy ezen változtasson. Több kollégája is úgy nyilatkozott később az FBI-nak, hogy Ames rendszeresen érdeklődött nem az ő területéhez tartozó munkákról is.<sup>1</sup>

Munkavégzésében többé-kevésbé a washingtoni mintát követte. Az összekötője Aleksey Khrenkov szovjet diplomata lett. Khrenkov – ellentétben a korábbi kapcsolattartójával – megtiszteltetésnek érezte az Amessel való találkozókat és ezt rendszeresen fel is emlegette.

Arról nincs információ, hogy Khrenkov a KGB mélyfedésben lévő tisztje lett volna, a CIA nem rendelkezett róla adattal korábról. A táskacserék visszatértek, Ames rendszeresen átadta a római Állomás táviratforgalmazását és cserébe pénzt, vodkát és szovjet követségi kiadványokat kapott. Már Bogotában megszervezték, hogy Khrenkov diplomata beosztásban lesz Rómában, találkozhatnak a különböző összejöveteleken, partikon és könnyed csevegést folytathatnak. Aztán valamelyikük meghívja a másikat egy italra, vagy ebédre. Ez meg is történt, így Amesnek volt fedősztorija, hogy miért találkozik Khrenkovval, és mindenki más azt hitte, hogy hivatalos együttműködés leple alatt Ames tanulmányozást folytat. Aztán, ahogy már Chuvakhinnál kialakult, Ames megírta a jelentéseket – helyesebben, volt, hogy írt jelentést – a találkozókról, úgy mint csekély értékű kapcsolat, korlátozott

---

<sup>1</sup> Az illetéktelen érdeklődés a kémkedés egy újabb indikátora volt, de ezzel sem foglalkozott senki, nem jelentették.

információszerző lehetőséggel, de folyamatosan lebegtetve, hogy talán lehet belőle beszerzés is<sup>2</sup>.

A CIA adattárában csupán 3 távirat volt Khrenkovról, vagyis a többi találkozóról készült jelentésben kb. annyi lehetett, hogy „találkoztam Khrenkovval, de nem mondott semmi jelentésre érdemes dolgot”. Ames ugyanazzal a dilemmával nézett szembe, mint Washingtonban, úgy kell jelentenie, hogy fenntarthassa a kapcsolatot, de úgy is, hogy ne hívja fel magára a figyelmet. Persze szerencséje volt, az Állomás vezetését nem nagyon érdekelte az ügy. Néhányan azonban elkezdtek gyanakodni, hogy Ames titkolózik. Egy munkatársa le is ellenőrizte az adatbázist és megállapította, hogy Ames bizony nem mindig írt jelentést. A szabálytalansággal kapcsolatos észrevételeiket azonban továbbra sem jelentették, azok megmaradtak munkahelyi pletykának<sup>3</sup>.

A kapcsolatot évente ellenőrizte a tartótiszt, Mechulayev Moszkvából, akivel még 1985. decemberben, Bogotában került kapcsolatba. Egy autós felvételt követően Khrenkov egy szovjet „K” lakásra<sup>4</sup> vitte Amest, ahol Mechulayev várta és 3-4 órában átbeszélték az elmúlt és a következő időszakot<sup>5</sup>.

A római találkozók során Ames egy új finanszírozási megállapodást kötött a szovjetekkel. 1985 végén két millió dollárt kapott összegben, azonban Ames szeretett volna havi fizetést is, így végül úgy állapodtak meg, hogy havonta 10.000, illetve találkozóként 20-50.000 USD-t kap. 1988 novemberében, a fia születése alkalmából pedig további bónuszt kapott. Mivel a szovjetek mindig készpénzben fizettek, Amesnek problémát jelentett a pénz eredetének legalizálása. A megoldás érdekében nyitott két számlát a Credit Suisse Banknál Zürichben, egyiket a saját, másikat az anyósa nevére, amelyen ő megbízottként szerepelt, és rendszeresen odautazott befizetni a készpénzt, mely összesen 950.000 USD-t tett ki. Ezeket az utakat nem jelentette be munkahelyén, ezzel ismételten megsértve a CIA szabályzóit. Az utakra mindig magával vitte Rosariot, mivel a kedvenc helye volt a város. Ames vásárolt egy használt Jaguárt, amivel keresztülvetve az Alpokon, James Bondnak érezte magát.

Olaszországban Amesék sok pénzt költöttek, amit a munkatársak észre is vettek. Számtalan európai utazáson vettek részt, így többek között Svájcban, az Egyesült Királyságban, az NSZK-ban. Egyik kollégája azt is tudta, hogy a telefonszámlája 5.000 USD volt havonta. A biztonsági tiszt készítet is egy feljegyzést a római Iroda vezetőjének a költségekről és italozásról, azonban az a

---

<sup>2</sup> A rendszer hibáját mutatja az is, hogy hagyták Amest találkozgatni egy csekély értékű kapcsolattal. Az ügynök legfontosabb tulajdonsága az információszerző képessége, hozzáférése az információhoz. Ha ez nincs, akkor felesleges kockázatvállalás, idő, energiabefektetés minden találkozó.

<sup>3</sup> Az állomány biztonsági tudatossága nem volt megfelelő szintű, úgy gondolhatták, hogy Ames viselkedése, az elkövetett szabálytalanságok nem rájuk tartoznak, pedig itt nem egy egyszerű munkahelyi kihágásról volt szó.

<sup>4</sup> Konspirált lakás, amely valamilyen fedésben működött, a KGB tulajdonában volt és titkos találkozókra használták.

<sup>5</sup> Itt már nem a követségre vitték be, mint Bogotában, hanem igyekeztek konspirálni a találkozót. Ames lelki konfliktusát jól mutatja, hogy minden találkozó alkalmával teljesen lerészegedett.



legenda, hogy Rosario örökölt, elosztott minden biztonsági aggodalmat a vezetői részéről. Ezek a momentumok pedig nem jelentek meg a személyi és biztonsági gyűjtőjében sem.

Ames munkája középszerű és gyenge szint között ingadozott Rómában. A négy értékeléséből az első kettő pozitívan nyilatkozott a vezetői képességeiről, de a megjegyzésben szerepelt, hogy többet kellene dolgoznia új kapcsolatok kialakításán. A másodikban a vezetője azt írta, hogy nincs folyamatban lévő ügye, tevékenysége ötletszerű. Ez egy erős kritikai értékelés volt. Az utolsó értékelésében, amit már egy másik vezető írt, a tevékenységét következtetlenségnek nevezte és képességein alulinak. Amessel kapcsolatban úgy érezték, hogy a GS14 besorolás a végállomás, beleszürkült, középszerű műveleti tiszt lett. A teljesítményét jelentősen befolyásolta a nagymértékű alkoholfüggősége, de ennek nyoma sem volt a hivatalos iratokban. 1986 és 1988 között hetente többször került ittas állapotba. 1987-ben, mivel nem léptették elő, még erőteljesebben kezdett el inni. Történt olyan eset, hogy Ames visszatért egy találkozóról Khrenkovval, de olyan részeg volt, hogy képtelen volt jelentést írni. Máskor a követség fogadásán rúgott be annyira, hogy egy helyi kórházban ébredt fel. Szóbeli figyelmeztetést kapott, semmilyen más következménye nem volt cselekedeteinek. Az alkoholproblémái miatt Rosarioval is megromlott a kapcsolata, rendszeresen veszekedtek.

A pénzügyi jelentései most is későn készültek el, de erről minden előjárója tudott, konfrontálódtak is vele ezért. Ames úgy próbálta feloldani a konfliktust, hogy lezárta a pénzkeretét és saját pénzből fizette a munkájával járó költségeket, majd azokat megtérítette a CIA-val. Az új főnöke viszont újraindította a pénzkeretét.

A teljesítménye és alkoholizmusa ellenére a két éves kiküldetést a főnöke meghosszabbították még egy évvel, 1989. júliusig.

Hazatérése előtt a KGB tájékoztatta őt a hírigényéről. Ennek egyik fele a CIA szovjet műveletei voltak, másik része pedig a lehetséges kettős ügynökök – a szovjetek által beszervezhető CIA tisztviselők – felkutatása. Kidolgozták a kapcsolattartási tervet is, ami szerint megjelölt időpontban találkoznak majd a következő évben, illetve tárgyi postaládák<sup>6</sup> használatát iktatták be. Tartói azt is javasolták, hogy évente egyszer találkozzanak az Egyesült Államokon kívül, Bogotában, minden december az első kedden<sup>7</sup>. Második lehetőségként pedig Bécset jelölték meg. 1987. július 20-án Amesék visszatértek Washingtonba<sup>8</sup>.

### **Amerika, Róma után**

Amesék 1989 júliusában elhagyták Rómát, elmentek nyaralni, majd a svájci számlákról kivett pénzből házat vásároltak Észak-Arlingtonban. A magánéleti dolgok rendezése után, Ames 1989. szeptemberben jelentkezett szolgálatra, és a munkatársai megrökönyödésére a Szovjet és Kelet-Európai Osztályra került vissza, az Európai Alosztály vezetői beosztásába. Ebben a beosztásban hozzáférése volt minden ügryhöz és ügynökhöz, akit a CIA foglalkoztatott a szovjet és a kelet-európai területen, az európai hadszíntéren, ami miatt a KGB kiemelt érdeklődésére tartott számot. Ames későbbi elmondása szerint, ha gyanakodtak volna rá a CIA-nál, ez lett volna az utolsó hely, ahová beosztásba helyezik.

<sup>6</sup> A természetes környezethez igazodó rejtkehely, melyben az ügynök és tartója dokumentumot, adathordozót, pénzt stb. helyez el a másik fél részére.

<sup>7</sup> Előre egyeztetett harmadik országos találkozó, amely bevett módszer a hírszerzésben.

<sup>8</sup> Itt már látszik, hogy a szovjetek igyekeztek elvinni a kapcsolattartást mély konspirációba, a felesleges kommunikáció – találkozók megbeszélése – kiiktatásával.

A kelet-európai politikai változások következtében néhány hónap után – 1990 januárjában – Ames a Csehszlovák Műveleti Alosztályhoz került főnöki beosztásba, így kevesebb hozzáférése volt a KGB számára értékes ügyekhez. A kommunista kormány bukását követően érdektelennek tartotta ezt a beosztást, és kérte a főnökét, hogy ismét olyan beosztásba kerülhessen, ahol szovjet ügyekkel foglalkozhat. A főnöke arcátlanok találta a kérést, és megígérte, hogy visszatérnek rá, de ez sosem történt meg. Ehelyett mást neveztek ki az alosztályvezetői posztra, így Amest megint áthelyezték, ezúttal az Előmeneteli Bizottságba. Itt, bár teljesen el volt szeparálva a műveletektől – *legfeljebb régi ismerősein keresztül juthatott egy-két információhoz* – de hozzáférése lett a CIA előmenetellel érintett állományának a személyügyi gyűjtőihez. Vallomásában később azt mondta, hogy ezeket az adatokat nem adta át a szovjeteknek.

A bizottság két hónapig működött, majd Ames az Elhárító Központ Elemző Részlegére ment egy év váltási rendben. A munkája elemzések készítése volt a KGB vonatkozásában, így hozzáférést kapott a CIA, a hadsereg elhárítói és az FBI műveleteihez. Ezeket az információkat időről-időre átadta a KGB-nek, kompromittálva az egész programot. Hozzáfért továbbá a régebbi hidegháborús anyagokhoz is, amit szintén átadott. A vezénylése lejártát követően tért vissza a Szovjet és Kelet-Európai Osztályhoz egy rövid időre. A KGB Munkacsoporthoz vezényelték, ahol a feladata a CIA és KGB, illetve annak 1991-es megszűnését követően a hírszerző jogutód, az SZVR jövőbeni stratégiai együttműködésének kidolgozása volt. Ebben az időben a KGB-re már nem ellenségként tekintettek, sokkal inkább partnerszolgálatként, és Ames ennek megfelelően dolgozott ki anyagokat. Itt sem sok időt töltött, majd a Kábítószer Ellenes Központba helyezték.

Ames hozzáféréseit továbbra sem korlátozták, a Kábítószer Ellenes Központ vezetői nem kaptak semmilyen utasítást – pl. a számítógép hozzáférése változatlan maradt –, majd 1993 őszén a számítógépes rendszer korszerűsítése után még ki is terjesztették a jogosultságát. Ames floppyra töltötte le az anyagokat, olyanokat is, amelyek nem igazán tartoztak a munkaköréhez. Hozzáfért a világ eseményeiről tudósító táviratokhoz, ebben az orosz és európai politikai, gazdasági eseményekről szólókhoz is. Az FBI és a CIA adatai szerint, nem volt személyes találkozó Ames és az oroszok között 1993 novembere és az 1994 februári letartóztatása között, és nem volt lehetősége sem átadni az információkat.

Mielőtt Rómából visszatért az Egyesült Államokba 1989 nyarán, a tartótisztjeivel kidolgoztak egy kapcsolattartási tervet, amely szerint két tárgyi postaládát telepítettek Washingtonban, illetve harmadik országos találkozókat egyeztettek le. A tárgyi postaládák egyike egy híd alatt volt<sup>9</sup>, a csomagot egy fekete zsákba kellett csomagolni, mintha szemét lenne. A tárgyi postaláda töltés jele egy krétajelzés volt egy Georgetown-i (valódi) postaládán<sup>10</sup>. A KGB ugyanígy jelzett, ha pénzt és utasításokat helyeztek el.

Az eljárás jól működött bár csak néhányszor alkalmazták egy évben. Hátránya volt a megközelítésben rejlő kockázat és az elhelyezhető dokumentáció korlátozott mennyisége. A rendszert évente felülvizsgálták a dél-amerikai vagy európai

---

<sup>9</sup> Robert Hanssen szintén híd alatti postaládát használt.

<sup>10</sup> Konspirált kapcsolattartás során az ügynök és tartója a közterületeken elhelyezett jelzésekkel üzennek, üzenhetnek egymásnak. Ezek a jelzések nem feltűnőek, pl. egy krétajelzés egy falon. Így értesíthetik egymást, a postaláda töltéséről, ürítéséről.

találkozók során. A találkozók rendjében is voltak problémák, mivel Ames részint italozási szokása, részint hanyagsága okán nem mindig volt ott időben.

A későbbi nyomozás során találtak egy levelet Ames számítógépén, amit 1992. júniusban írt. Ebben közölte tartóisztjével, hogy „azonnal szükségem van pénzre. Ahogy többször említettem már, igyekszem jól befektetni a pénzt, de a jórészt elviszik a kiadások. Most készpénzre van szükségem egy nagyon szorító helyzetben. El kellett adnom a zürichi letéti jegyeket és részvényeket, hogy betömjem a lyukakat. Annyi készpénzre van szükségem amennyit gondolnak, úgy vélem a tárgyi postaládába 100.000 USD beleférhet”. Amesnek sok problémája volt ezzel a személytelen kommunikációval, mivel korlátozta az átadott anyagmennyiséget és a kapott pénzt is.

1993. március 9-én gépelt egy levelet a számítógépén: „Minden rendben van, nincs jele annak, hogy gyanakodnának”. A levélben részletezte még a morált a szervezeti egységénél, a személyi változásokat, és a költségvetésüket, illetve néhány minősített adatot is leírt.

1993. november 1-jén Ames Bogotába utazott személyes találkozóra, ahol kapott egy nagyobb összeget, illetve új kommunikációs tervet 1994-re, amely a Washingtonban telepített új jelzőhelyek és tárgyi postaládák elhelyezkedését is tartalmazta. A váltások februárban, márciusban, májusban, augusztusban, és szeptemberben voltak. 1994. novemberre terveztek személyes találkozót Caracasba, Venezuelába, vagy Quitoba, Ecuadorba.

1992 és 1993 között a Kábítószér Ellenes Központnál Ames több szolgálati utat is tett a tengerentúlra Moszkvába, és Törökországba. Utóbbi országba egy konferenciára utazott és magával vitte személyes laptopját minősített adatokkal. A főnöke, aki vele utazott, kérte, hogy játszhasson a gépén, melyet Ames megengedett. A CIA szabályozói tiltják, hogy minősített adatokat tároljanak saját laptopon, de Ames ezzel nem törődött. Visszatérés után jelentette a főnök az eseményt a CIA-nak és FBI-nak is. Úgy nyilatkozott, hogy mindent elborított a minősített dokumentum a gépen, sőt látta a Vlad könyvtárat is, de nem nyitotta meg.

Ames a tengerentúli utazásai során biztonságos helyre – mely a kézitáskája, vagy a számítógép-táskája volt – rakta a dokumentumokat. A pénzt ugyanígy szállította, kihasználva hogy amerikai hivatalos személyként utazott, és nem a terrorista profilnak felelt meg, így valószínűtlen volt, hogy a csomagját átnézzék a 9/11 előtti időszakban.

### **A nyomozás utolsó évei**

A Szovjet és Kelet-Európai Osztályon létrehoztak egy csoportot – amely jellemzően a korábbi évek vizsgálatában részt vevőkből álltak – Backroom néven. Ez az elhárító csoport azon dolgozott, hogy stabilan tudja foglalkoztatni a szovjet és néhány kelet európai forrását, akik révén meg lehet fejteni az 1985-86-ban tapasztalt különös eseményeket. Napi megbeszélések voltak, a jelentéseket megosztották egymással, a forrásokat koordináltan kezelték. A források számának növekedésével nőtt a Backroom létszáma is. A helyiség a pincének egy félreeső részén volt, zárt ajtók mögött. Ha más akart bemenni, addig nem nyitottak ajtót, amíg el nem pakoltak mindent az asztalról. Ezt a szabályt, bár nem foglalták az Osztály működési

szabályzatába, mindenki betartotta, kivéve egy embert, Aldrich Amest, aki a római kiküldetése után, egy reggel kopogás nélkül nyitott be az irodába.

A Backroom kezelte az Osztály legfontosabb forrásait, ami miatt a többiekkel való viszonyukban időnként konfliktusok jelentek meg. A többiek ugyanis azzal szembesültek, hogy a látókörbe került személyek eltűntek a Backroomban és többet nem hallottak róluk. Ez bizonyos feszültséget szült, mert úgy érezték a vizsgálócsoporthoz kívüli dolgozók, hogy nem bízik bennük a szervezet.

Az Osztálynak természetesen voltak kudarcai is. Egyik ilyen ügyük, a GT Prologue nagyon sok fejfájást okozott. 1988 júniusában kezdődött, amikor Aleksandr Vasilyevich Zhomov, a KGB belső elhárítási tisztje megközelítette Jack Downingot, a Moszkva Állomás törzsfőnökét a leningrádi HÉV-en. Zhomov nem azonosította magát, csak egy borítékot adott át és eltűnt. A borítékban KGB dokumentumok voltak és egy fecni, amire azt írták, hogy a személy a KGB 2. Igazgatóságáról<sup>11</sup> van, amely a CIA Állomások ellen dolgozik. Az ismeretlen egy későbbi, biztonságosabb körülmények közötti beszélgetésre tett javaslatot. Közölte, hogy el akarja hagyni a Szovjetuniót, ezért segítené a CIA-t. Az átadott dokumentumok között volt egy, amely kapcsolódott a 85-ös veszteségek nyomozásához. Az elemzés a CIA 1984-1986. évi moszkvai működéséről szólt és arra a következtetésre jutott, hogy a rossz eljárás miatt sikerült olyan sok ügynököt felderíteni. Ez az újabb jelzés, ami a CIA hibáját hangsúlyozta, felébresztette a gyanút az ismeretlen ellen. A moszkvai Állomás azonban hallani sem akart erről mondván, hogy nem akarják elijeszteni az új tippszemélyüket, hiszen a kérdéssor bizalmatlanságot mutat. Zhomov-val nem is folytattak interjút, így figyelmen kívül hagyták azt az alapelvet, hogy a jelentkezőnek először is bizonyítania kell őszinteségét, megbízhatóságát, értékét. Végül – más források által – Zhomov-ról kiderült, hogy dezinformálni akarta a CIA-t. Soha nem vette igénybe a kimenekítést, arra hivatkozva, hogy az túl kockázatos. Megszakadt vele a kapcsolat, az eredmény pedig annyi volt, hogy a CIA fizetett egy nagyobb összeget Zhomov-nak, ami a KGB számláját gazdagította, megmutatták neki az eljárásukat az ügynök kivonásával/kimenekítésével kapcsolatban, adtak neki amerikai útlevelet, tehát végeredményben kijátszotta őket. A végső következtetés pedig az lett, hogy a CIA-t megtévesztették.

1989. november elején olyan esemény történt, amelynek akkor még nem érzékelték a fontosságát, mégis ez jelentette az igazi áttörést. A Szovjet és Kelet-Európai Osztály egyik munkatársa, Diana Worthen (*aki Amesék esküvőjén is ott volt*) megkereste Sandy Grimest – a könyv egyik szerzőjét – és aggodalmas bejelentést tett. Worthen ugyanabban az időszakban volt Mexikóban, mint Ames, együtt dolgoztak a szovjet részlegen, barátok lettek és így hamarosan Rosario Casas Dupuy, a columbiai nagykövetség kulturális attaséjával is szoros kapcsolatba került.

Diana és Amesék barátsága a kiküldetést követően is megmaradt. Amesék 1986-ban Rómába mentek és ez időszak alatt Diana küldött apró dolgokat Rosarionak, amelyek ott nem voltak kaphatóak, viszonzásul azonban egészen drága ajándékokat kapott (pl. Gucci sál). Amikor Amesék visszatértek Washingtonba, az életvitelük gyökeresen megváltozott. Mielőtt elmentek, egy szerény, bérelt lakásban

---

<sup>11</sup> Politikai elhárítás

laktak észak Virginiában és Amesnek egy régi Volvoja volt. Visszatérésüket követően egy hatalmas házat vásároltak Észak Arlington elegáns részén, amiért Diana elmondása szerint 540.000 USD-t fizettek készpénzben. A házat magas költségen fel is újították, illetve Ames vett egy Jaguárt, feleségének pedig egy Honda Accordot. Diana-nak feltűnt a hatalmas költségek – hiszen látta, hogy Rosarionak Mexikóban nem volt semmije, hónapról-hónapra élt a fizetéséből – és rá is kérdezett a pénz eredetére, de nem kapott választ.

Sandy fontosnak ítélte az információt, és Dianat főnökéhez, Redmondhoz irányította, ráirányítva a figyelmet, hogy Ames tudott minden ügyről ami dekonspirálódott, volt hozzáférése és most már pénze is. A részlegvezetőnek azonban nem állt így össze a kép, nem is igazán akart vele foglalkozni, mert más dolog volt, ezért Jeanne-hez – a könyv másik szerzőjéhez – irányította Dianat.

Diana zaklatottan kereste meg Jeanne-t, aki azonban éppen Agee ügyben volt elfoglalva, annak a végjátéka előtt álltak, így nem tudott foglalkozni az információval és Dan Payne-hez, a Belbiztonsági Iroda munkatársához irányította a nőt.

Diana nem adta fel, megkereste Dan Payne-t, és negyedjére is elmondta, amit tudott. Bár Dan is elfoglalt volt más dolgaival, de azért előzetes nyomozás<sup>12</sup> keretében átnézte Ames Biztonsági Gyűjtőjét és Személyi Gyűjtőjét, amelyekről viszont úgy vélte, hogy nem tartalmaztak semmilyen, elhárítási szempontból releváns információt, annak ellenére, hogy szerepeltek benne Ames korábbi ittas vezetés miatti ügyei. A dokumentumok szerint az 1970-es években berúgott egy munkahelyi karácsonyi partin, ami abban az időben teljesen normális viselkedés volt a CIA-nál. A karácsonyi partik délután kezdődtek és inkább az italnak volt nagy szerepe, nem az ételnek. A Biztonsági Részleg ellenőrizte a kijáratokat, és aki részegen akart távozni, azt inkább hazavitték. A Személyi Gyűjtő adatai szerint meglehetősen régen, 1986-ban volt utoljára Amesnek poligráf teszthez. Ezt követően Dan elolvasta Rosario műveleti – 201-es – gyűjtőjét. Diana szerint Rosario támogató ügynökként dolgozott a CIA-nak Mexikóvárosban, a lakását találkozóhelyként használták a CIA tiszték, illetve jelentett azon személyekről, akikkel munkája során találkozott. Dan észrevételezte azt is, hogy Rosario egy politikai kötődésekkel bíró családból érkezett Kolumbiából, az apja a Liberális Párt korábbi vezetője volt. Rosario kinevezése Kolumbia mexikói nagykövetségére a kolumbiai elnök által történt.

Dan elment az Arlington Megyei Bíróságra, hogy ellenőrizhesse Ames jelzalog bejegyzését az új házon, de nem talált semmit. Szintén nem talált semmilyen hitelfelvételre utaló adatot.

Ellenőrizte a bankszámla információkat is és három érdekes tranzakciót talált:

- 1985. október 18. – 15.660 USD befizetés;
- 1986. február 18. – 13.500 USD befizetés;
- 1989. augusztus 1. – 22.107 ITL (olasz lira) váltás.

Az adatokkal nem igazán tudtak mit kezdeni, azokat csatolták az addigi anyagokhoz és a vizsgálat megrekedt. 1990. januárban a nyomozó két hónapos

---

<sup>12</sup> Az előzetes nyomozás – a közvélekedésben nyomozásnak nevezett munkafolyamatot megelőző, jellemzően adatpontosító tevékenység. A magyar állambiztonsági szolgálatok előzetes ellenőrzésként használták a fogalmat, amelynek tartalma: „a bűncselekményre utaló elsődleges információk, jelzések adatpontosító, kiegészítő munkafolyamata. Célja az információ valószínűsítése.” – Állambiztonsági értelmező kiegészítő, <http://osaarchivum.org/files/fa/357/szotar.CEwin.htm>, (Letöltés ideje: 2017.07.11.)

képzésre ment, senki nem vette át az ügyet. Amikor visszatért, más ügyekkel volt elfoglalva, illetve 1990 júniusában Európába küldték.

Dan 1990 decemberében tért vissza az Ames-ügyhöz és kérte a Belbiztonsági Irodát, hogy ellenőrizték Ames háttérét, amelynek része volt a poligráf vizsgálat is. 1991 januárjáig halasztódott az ügy feltárása, mert a dolgozók öt éves periódusokban voltak beosztva és a soron kívüli vizsgálat felkeltette volna Ames gyanúját. Dan tett egy javaslatot, hogy a belbiztonsági vizsgálat fókuszáljon Ames anyagi helyzetére, életvitelére.

1991. januárban ismét ellenőrizték a számlákat a Northwest Federal Credit Unionnál, de nem találtak semmit. Később kiderült, hogy Dan olyan hónapot választott ki szerencsétlenül, amikor nem volt utalás. Ellenőrizték Ames CIA-számláját is, ami szintén nem mutatott gyanús eltérést, sőt, amit találtak, az hamis biztonságérzetet keltve Ames mellett szólt, mivel 25.000 USD kölcsönt vett fel a Jaguárra és azt a fizetéséből rendszeresen törlesztette. Más bankoktól nem kérték le az adatokat, később azt állítva, hogy nem tudták, hogy az engedélyük más intézményekre is vonatkozik<sup>13</sup>.

A CIA nyomozócsoport gondolkozott rajta, hogy egy pénzügyi szakértőt is bevonjon a vizsgálatba egy másik igazgatóságról, vagy az FBI-tól, de végül arra jutottak, hogy egy külsős nem értheti meg a Műveleti Igazgatóság működését, szervezeti kultúráját, valamint problémát okozott számukra, hogy milyen módon és alapon vonhatná ellenőrzés alá a CIA alkalmazottakat. Úgy gondolták, hogy nincs itt az ideje, hogy az FBI nyomozást indítson<sup>14</sup>.

Ames a személyi biztonsági kérdőívet 1991. január 22-én kapta meg, márciusban adta vissza. A belbiztonság 1991. április 12-én fejezte be a vizsgálatát, amely megállapította Ames anyagi gyarapodását, de a referencia személyek azt egyöntetűen a feleség kolumbiai családjához kötötték. Amesről a vélemények egy része pozitív volt, megbíztak benne, azt hogy néha berúgott, nem tartották biztonsági kockázatnak. A meghallgatottak között azonban voltak olyanok is, akik szerint lehetséges, hogy Ames kém volt, Rómában figyelmet érdemlő szovjet kapcsolatai voltak, akiktől nagyon sok hívást kapott. Többször megszegte a rezsimszabályokat, nyitva hagyta a páncélját, otthon írta a jelentéseket, 9-10 óra előtt nem ért be az irodába munkakezdésre, hetente legalább egyszer leittasodott ebéddidőben. Amikor azonban megkérték ezeket a munkatársakat, hogy kétségeiket, észrevételeiket a vizsgálat során nyíltan is vállalják fel, inkább visszakoztak.

A CIA belbiztonsági nyomozása semmi újat nem hozott, amit addig ne tudtak volna. Így a nyomozó nem gondolta, hogy folytatnia kellene, vagy az előjárójával konzultálnia kellene. Szerinte a további interjúk gyanúsak lettek volna Ames számára és egyébként sem keletkezett elhárító szempontból releváns adat.

---

<sup>13</sup> Hogy miért csak egy vagy néhány hónapot választott a nyomozó, azt nem lehet tudni, de mindenképpen érdekesebb lett volna hosszabb időszakra lekérni a bankszámla adatokat, lehetőség szerint minden pénzintézetből.

<sup>14</sup> A helyzet tipikusan az, amikor egy zárt közösség „beleszorul” a saját igazságába. A nyomozások során érdemes egy olyan kontrollszemélyt/szervezetet alkalmazni, aki/ami külsős, tehát nem él együtt az ügygel, így megőrizheti objektivitását.

Amest április közepén vették poligráf vizsgálat alá úgy, hogy a vizsgálónak nem adták oda a készült jelentéseket, csak egy részét, sőt, a személyes körülményeivel kapcsolatban felderített aktuális információk még bele sem kerülhettek a gyűjtőjébe. A poligráf vizsgálat során először meginterjúvolták Amest, aki magától elmondott bizonyos adatokat a pénzügyi helyzetére vonatkozóan, illetve könnyedén válaszolt az anyagi helyzetét firtató felszínes kérdésekre, elismerte vagyonát és az anyósától származónak mondta a pénzt, a vizsgáló pedig nem firtatta tovább a témát. Megkérdezték, hogy titkol-e pénzügyi problémát, amire nemmel válaszolt és nem mutatott zavarjelet. A részletekbe azonban nem mentek bele a vizsgálók, mert úgy gondolták, hogy egy rutinjelzésnek az nem kell hogy részét képezze. Ames egyébként készült a kérdésre, készítettett egy ajándékozó levelet, amit anyósa írt alá, de ezt soha senki nem kérte, kérdezte.

Ames szintén nem mutatott reakciót, amikor megkérdezték, hogy dolgozott-e külföldi titkosszolgálatnak. Amikor azonban arról kérdezték, hogy van-e kapcsolata külföldi személlyel, akkor hazugságjelet produkált. Több óra múlva is zavarjelet adott a kérdésre, és a vizsgáló a protokollt követve abbahagyta a tesztet és kérte Amest, hogy néhány nap múlva ismételjék meg a vizsgálatot. Négy nap múlva Ames visszatért és egy másik vizsgálónál minden kérdést megválaszolt zavarjel nélkül. Ames úgy magyarázta, hogy számos embernek be lett mutatva Kolumbiában, amikor családlátogatáson voltak és nem tudja, hogy közülük kik dolgoznak a kolumbiai titkosszolgálatnál. A vizsgáló elfogadta ezt a magyarázatot, így Ames pozitív eredményt kapott. Annyit jegyeztek csak fel, hogy az együttműködés alacsonyabb szintű volt, mint az első vizsgálat alatt. Nem voltak további kérdések a pénzügyi helyzetére vonatkozóan és Ames sikerrel teljesítette a tesztet. Az első vizsgáló megjegyzése szerint nem kém, de a pénzügyi helyzetével kapcsolatban felmerülnek kétségek.

1991. júliusban Bogotából, az ottani irodavezetőtől kértek információt a Rosario családdal kapcsolatban. Egy bő hónappal később kapták a választ, hogy a család valóban vagyonos és politikai kapcsolatokkal rendelkezik. Anyagi helyzetüket jellemezte, hogy több millió dollár értékű földet adományoztak a bogotai stadion építéséhez. Ezen felül ingatlanfejlesztéssel foglalkoztak, illetve egy fagylaltláncot is tulajdonoltak.

Ames későbbi elmondása szerint, nem érezte zavarónak az 1991-es vizsgálatot, hiszen időszerű volt, de sokkal aprólékosabb, részletesebb vizsgálatot várt. Elmondása szerint soha nem kapott kiképzést a KGB-től/SZVR-től, bár azt tanácsolták neki, legyen nyugodt, nincs mitől félnie. A későbbi vizsgálatok szerint az 1986-os és 1991-es poligráf vizsgálatok nem megfelelően voltak végrehajtva, mert a vizsgáló nem teremtett megfelelő pszichológiai helyzetet vizsgálatához – a vizsgálók egy baráti felállásban vizsgálták – és nem készültek fel rendesen.

A tény, hogy 1991-ben teljesítette a poligráfot, a nyomozó csoport gyanúja lankadt. A sikeres poligráf és a bogotai háttér ismeretében a belbiztonság lezárta az ellenőrzést.

### **A nyomozás új életre kel**

1991-ben Jeanne, a nyugdíjazása előtt újra nekikezdett az 1985-ös veszteségek átvizsgálásának és a munkához csatlakozott az FBI Műveleti Igazgatóság Szovjet Részlege. Két fő FBI és négy fő CIA tisztviselővel megalakították az Elhárító

Központ Különleges Nyomozó Egységet.<sup>15</sup> Az irodájuk az Elhárító Központ közepén volt, ami nem biztosított túl nagy zártságot. Jeanne meglehetősen kicsi irodája jelentett valamiféle diszkréciót, ott lehetett bizalmas megbeszéléseket tartani. A számítógépek nem voltak a CIA központi hálózatra csatlakoztatva, azok külön hálózatban működtek.

Először kérték a belbiztonságot, hogy adjanak egy listát azokról a személyekről, akik ismerhették az 1985-ös vesztesség személyeit. A lista 198 személyt tartalmazott. Ezekből Jeanne és Sandy le tudta válogatni azokat, akik valójában távol voltak – hiszen ismerték az akkori Szovjet és Kelet-Európai Osztály állományát – illetve le tudták válogatni a Jelentési Csoport<sup>16</sup> állományát, mivel ők nem ismerhették az ügynököket. Így sikerült kb. 160 főre redukálni a listát. Ez még mindig túl nagy létszám volt, ezért valamiképpen priorizálni kellett a személyeket. Jeanne és Sandy kizárta azokat is, akik szerintük – *szubjektív döntés alapján* – nem lehettek az árulók. Ezt követően egy 10 fős bizottság szavazott az összes benmaradóról. Mindenkinek ki kellett választania 5-6 személyt, akinek a körülményei, további vizsgálódást igényelt. Ezeket az embereket pedig sorba kellett állítaniuk aszerint, kivel kapcsolatban legerősebb az aggodalmuk. Amikor a listák elkészültek, pontozták őket. Hat pontot kapott a legelső helyen álló és az utána következők mindig eggyel kevesebbet. Ezután összeadták a számokat, amelynek eredményeként Richard Ames került az élre 21 ponttal, akit egyébként egyedül Sandy sorolt első helyre. A vizsgálat ezt követően a 15 pontnál többet kapó személyekre koncentrált. Az FBI és a CIA tagjai teljesen más sorrendet állítottak fel, mivel az előbbieket nem ismerték a személyek hátterét. Később a négy CIA-s újra szavazott és Ames megint a legtöbb pontot kapta.

Kikérték a belbiztonságtól a 160 fő gyűjtőit is, illetve azok listáját, akik 1985 eleje óta nem voltak poligráf vizsgálaton. Az ő vizsgálatukat kezdeményezték is, de sokan elmentek már nyugdíjba, leszereltek, vagy éppen tengeren túli szolgálaton voltak, így őket nem lehetett kikérdezni.

A pontozásos listán szereplőknek átnézték a biztonsági gyűjtőjét és a személyügyi gyűjtőjét is. Ezen túlmenően az Ügynökség pszichológusa áttekintette az egészségügyi anyagokat, amibe a nyomozócsoport nem nézhetett bele. Az anyag tartalmazta a pszichológia teszt eredményeket is, így ezeket össze tudták vetni a Slammer Project kutatással<sup>17</sup>. Az összehasonlítás nem hozott eredményt Amessel kapcsolatban, habár néhány érdekes részlet kiderült róla. Az 1967-es pszichológiai vizsgálaton, amikor a Career Training Programba jelentkezett, úgy jellemezték, mint féltékeny, önbizalomhiányos személy és nem kapott erős ajánlást. Egy évvel későbbi vizsgálaton változásokat detektáltak nála, miszerint képessé vált elrejtetni gondolatait, felvenni egy maszkot, szerepet játszani.

Elkezdtek átnézni a dekonspirálódott ügyeket is. Korábban az FBI csak az ügyek összefoglalóit ismerhette meg, most teljes betekintési jogosultságot kaptak, illetve ők is megnyitották aktáikat a CIA számára.

---

<sup>15</sup> Special Investigation Unit of Counterintelligence Center

<sup>16</sup> Reports Group

<sup>17</sup> Ez a projekt vizsgálta azokat az amerikai állampolgárokat, akik kémkedésért voltak elítélve. Velük a börtönbe pszichológiai mélyinterjúkat készítettek és felállították a pszichológia profiljukat.



Összeállítottak egy listát azokról a KGB tisztekről, akiknek tudomása lehetett a CIA-ba való behatolásról, egyrészt mert 1985-ben kulcsbeosztásban voltak, másrészt mert rendelkeztek megfelelő angol nyelvtudással. Ez a lista 60-70 nevet tartalmazott, akiknek kigyűjtötték az előléptetéseit, külföldi utakat, külszolgálatukat, fedőneveiket annak reményében, hogy külföldi utazásaikat össze tudják vetni a CIA tisztviselők utazásával – amibe az NSA is sokat segített – és találhatnak közös eseményt. Persze erre kevés esély volt, hiszen a KGB és SZVR tisztjei rendszerint fedőnévvel utazgattak, amit az amerikaiak nem ismertek. A szerencse mégis melléjük állt. Az Amessel korábban találkozó szovjetek egyike a valódi nevén utazott Bogotába és teljes bizonyossággal megállapítható volt, hogy egyazon időben mindketten ott tartózkodtak. Ames ezt az utazását nem titkolta el, annak idején úgy indokolta, hogy az anyósának kellett segítenie. Természetesen ez az egybeesés nem bizonyított semmit.

Az ebben az időszakban végbemenő világpolitikai változások a titkosszolgálati szférára és így a CIA műveleti tevékenységére is kihatással voltak. A KGB megszűnt és az utódszervezettel kezdett kialakulni egy barátságosabb viszony, ezért redukálták az Állomások orosz célpontok elleni tevékenységének intenzitását. Az volt az utasítás, hogyha egy önkéntes jelentkezik, akkor „cash and carry”<sup>18</sup> alapon számoltassák be, aztán búcsúzzanak el tőle. A hosszú távú kapcsolattartást nem bátorították és a menedékkérelmeket figyelmen kívül kellett hagyni. Az üzenet egyértelmű volt: a KGB/SZVR/GRU/FSZB tisztek elleni műveleti tevékenység nem volt többé karrierépítő szegmens. Az intézkedésnek számos következménye volt, amelyek közül az egyik látványos mellényúlás Vasili Mitrokhin esete volt. A férfiak KGB irattárában dolgozott, ahonnan rendkívül nagy mennyiségű dokumentumot csempészett ki. Ezzel kétszer jelentkezett az amerikaiaknál, de elutasítása miatt a briteknél kötött ki és részükre adta át az aranybányának tekinthető iratanyagot.<sup>19</sup>

A csoport 1970-ig visszamenőleg átnézte azokat a jelentéseket, amelyekben egy esetleges CIA beépülésről jelentett a forrás. Munkájuk Ezek nem vezettek eredményre, jellemzően értelmetlen információk voltak, mivel az ügynököknek nem volt direkt hozzáférésük az adatokhoz, csak elbeszélések alapján adtak tájékoztatást. Megkezdtek az átállt ügynökök meghallgatását is, de ez sem hozott kézzelfogható eredményt.

Elkezdődött azon CIA alkalmazottak körének kikérdezése, akik 1985-ben kulcsbeosztásban voltak. Ez a projekt zavarta az FBI-t, mert ők az interjúkat nyomozati cselekményként értelmezték, tulajdonképpen kihallgatásnak, amihez a CIA-nak nem volt joga. Jeanne és Sandy megígérték, ha valamelyik interjúban bűncselekményre utaló közlés hangzik el, ők elhagyják a termet és az FBI folytatja a meghallgatást. Végül megindultak az interjúk, ahol minden személy ugyanazt a kérdéseket kapta: Ki fogadta a minősített táviratokat reggelente? Kinek, melyik páncélhoz volt hozzáférése? Lehet-e hallani a beszélgetéseket a munkaállomások között? Tapasztaltak-e valamiféle biztonsági szabálysértést munkájuk során?

---

<sup>18</sup> fizess és vidd – vagyis fizessék ki az ügynököt és engedjék útjára

<sup>19</sup> Christopher ANDREW – Vasilij MITROHIN: A Mitrohin-archivum, Tálatum, Budapest, 2000, ISBN: 9636450765

Mintegy 40 főt hallgattak meg, vagyis nem volt túl diszkrét a vizsgálat. Ebből következően joggal számolhattak azzal, hogy a két útlevelel<sup>20</sup> rendelkező Ames Kolumbiába szökik, ha elkezd gyanakodni. A meghallgatott személyeket úgy válogatták össze, hogy köztük voltak a pontozásos lista tagjai, illetve olyan személyek is, akik abszolút gyanún felül álltak. Ennek köszönhetően a kívülállók nem gyanakodtak, rutinvizsgálatnak tekintették az interjúkat. Két dologra derült fény: egyik, hogy Ames nyilatkozata szerint egy éjszaka nyitva felejtette a páncélját, ami dokumentálva is volt a biztonsági gyűjtőjében, mint szabályszegés. Azt mondta, hogy a páncélban volt egy lista, ami több olyan ügyet tartalmazott, ami dekonspirálódott, illetve a csoportja összes páncéljának a kódja is ott volt. A nyilatkozat természetes volt tőle, hiszen erre kérdeztek rá, illetve ez fel volt jegyezve a gyűjtőjében. Azonban a meghallgatás során, oda nem illően megint felhozta a témát, ami már kissé erőltetett volt, mintha azt akarná elhitetni, hogy valaki az ő páncéljából lopta ki az adatokat. Másik furcsa dolog volt a reakciója arra a kérdésre, hogy: Ha elárulná a CIA titkait a KGB-nek, hogyan csinálná? Elárulná-e a személyazonosságát? Egyszeri vagy folyamatos kapcsolattartást preferálna? Befolyásolná-e a tudat, hogy rendszeres poligráf vizsgálaton kell részt vennie? Eredetileg a kérdéssorozat célja az volt, hogy újabb ötleteket adjon lehetséges forgatókönyvekről, a másodlagos cél pedig megmutatni az FBI kollégáknak, hogyan gondolkodik egy CIA tisztviselő. A meghallgatottak többsége beleélte magát a szerepbe és a képzeletük végtelen variációjával jöttek elő, amelyek azonban saját tapasztalataikhoz kötődtek. Egyikőjük azt mondta, hogy egy szubszaharai fővárosba menne, ahol az orosz nagykövetség előtt a helyi szolgálatnak van egy megfigyelő pontja. Mivel ő ázsiai típus, senki nem foglalkozna azzal, ha bemegy a követségre. Egy másik személy, aki korábban a Távol-Keleten dolgozott, ismerte az akkor ott szolgáló KGB tisztet. A személy jó benyomást keltett, intelligens volt, művelt és nem részeges, mint akkoriban olyannyira jellemző volt. A meghallgatott tudta, hogy megint külszolgálaton van, így őt kereste volna meg a korábbi jó kapcsolatuk miatt. Vagyis jellemzően az eddigi munkatapasztalataikat használták fel, hogy kidolgozzák az oroszokkal való kapcsolatfelvételt.

Ames válasza azonban eltért mindenkiétől. Általában nagyon jól kommunikált, amikor gyors döntéseket kellett hoznia, most viszont lassú volt és hezitált. Olyan dolgokat mondott, fűzött össze, amelyeket már csinált, és amelyeket még nem. Számára – a többiekkel ellentétben – ez nem játék volt. Olyat mondott például, hogy ő a tengerentúlon dolgozott, miközben Washingtonban közvetlen kapcsolata volt a Szovjet Nagykövetséggel<sup>21</sup>. Nyilatkozata szerint őt a poligráf nem rettentené el. Az utolsó kérdés, amit kérdeztek: Mit gondol, mi történt 1985-ben? Néhányan azt mondták, hogy szerintük behatolás történt a CIA-hoz, néhányuk szerint technikai probléma volt, illetve egyesek szerint egyéb okok miatt következett be a veszteség. Ames Howardot említette, illetve retorikai kérdést tett fel, hogy mennyire lehet véletlen egybeesés az egész dolog?<sup>22</sup>

---

<sup>20</sup> Az amerikaiak számára is van lehetőség két útlevelet birtokolni, aminek biztonsági okai vannak.

<sup>21</sup> Tehát Ames nem csak a munkatapasztalataira épített, hanem új, kitalált módszereket, eljárásokat is előadott.

<sup>22</sup> Vagyis nem erősítette az ismeretlen beépített személy gyanúját, és ezzel a nyomozás folytatásának szükségességét.

## Ames kerül a fókuszba

Az idő előrehaladtával egyre inkább Ames került a középpontba, de igazából nem köthető egy konkrét történéshez, időponthoz ennek bekövetkezése. Az is igaz, hogy valójában más gyanúsított sosem volt és inkább Ames irányította magára a figyelmet.

1992 augusztusára elkészítették azt a táblázatot, amelyben feltüntették, hogy Ames mikor, hol volt beosztásban, hol végzett műveleti munkát. Ez a mintegy 500 oldalas dokumentum fontos szerepet játszott az ügy felderítésében.

A dokumentum adatait a biztonsági és a személyi gyűjtőből vették, illetve naplózták a CIA elektronikus fájljait évekre visszamenőleg, Ames igazi és fedőneveire is visszakeresve. Az állomány a Műveleti Igazgatóságon fedőnévvel is rendelkezett, sok irat így jelent meg az Ügynökség iratforgalmában. Ekképpen az emberek elvileg nem ismerhették meg egymást, a gyakorlatban persze az igazgatóságon belül mindenki tudta a többiek fedőnevét.

Több ezer dokumentumot gyűjtöttek össze, ami magába foglalta az Ameshez köthető, illetve minden további személy – akinek kereszt-, középső vagy vezetéknevében szerepelt az Ames szó – dokumentumait, valamint minden hivatkozást Ames településre Iowában, az Ügynökség Ames nevű épületére Rosslynban, Virginiában. Ezeket kronológiai sorrendbe tették és átvizsgálták, amivel ismét hónapok teltek el.

Egy másik nagy adatblokk volt, amely Ames regisztrációs kártyájához volt köthető. Mindenkinnek volt ilyen kártyája, amit a belépésnél és távozásnál le kellett húzni. Ezt az adathalmazt évekre visszamenőleg gyűjtötte be a Belbiztonsági Iroda, de az értékelése szintén hónapokat vett igénybe. Eredményeképpen képet kaptak Ames napi életritmusáról, szokásairól. Ritkán járt időben dolgozni, ritkán túlórázott és még ritkábban dolgozott szombaton. Sandy balszerencséjére Ames erős dohányos volt és mivel az utolsó években már nem lehetett az épületben dohányozni, így a legtöbb mozgást a bejáratnál az épület előtti cigarettaszünet indukálta.

A mozgási mintában figyelemreméltó adat keletkezett az FBI számára. Nyilvánvaló volt, hogy Ames nem szeretett korán kelni és nem ért be időben, azonban volt a mintában eltérés, amikor fél nyolcra ment dolgozni. Az FBI nyomozás megállapította, hogy a KGB érintkezések – tárgyi postaláda töltés-ürítés, jelzés elhelyezése, olvasása – mindig korán reggel, ezeken a napokon történt.

Megvizsgálták Ames személyi gyűjtőjében a teljesítményértékeléseket, különös tekintettel az 1984-1985-ös évekre. Ezekben voltak utalások – konkrét, részletes adatok nélkül – két szovjet diplomatára, akik abban az időben szolgáltak Washingtonban és akikkel Amesnek engedélyezett kapcsolata volt.

Ames napi tevékenységének teljes feltérképezésével egyidejűleg folyt anyagi helyzetének vizsgálata is. Mindez erős vezetői nyomás alatt zajlott, mivel úgy érezték, nem halad elég gyorsan a munka. Lekérték a bankszámla forgalmi adatokat, hitelkártya információkat, és bár rendelkeztek engedéllyel (National Security Letter, *a külső engedélyhez nem kötött adatok gyűjtésére adott felhatalmazás, úgymint*

*híváslista, banki adatok*) az akkori törvényi rendelkezések szerint a brókercégeknek nem volt kötelező adatot szolgáltatni, illetve – *a még nálunk is ismerősen csengő nevű vagyongazdálkodó cégek, mint* – a Merrill Lynche és a Morgan Stanley sem nem volt hajlandó információt kiadni.

Nem tudták begyűjteni a külföldi számlákkal kapcsolatos tranzakciós adatokat sem, bár tudták, hogy Amesnek volt olasz számlája, de rendelkezett betétszámlával Svájcban a Credit Suisse-nél, illetve feltételezések szerint Kolumbiában is volt banki terméke. Az adatok feldolgozása unalmas és fárasztó volt, mivel nemcsak havi kivonatokat kaptak, hanem minden egyes sikeres, sikertelen tranzakcióról, törölt csekkről, betétekről, hitelkártya tranzakciókról szóló adatot. Egy idő után világossá vált, hogy Ames hatalmas összegeket mozgatott.

Ezt követően az adatokat összevetették Ames műveleti tevékenységének kronológiájával. Az utazásokat, a napi rutintól eltérő tevékenységeket, számítógép és alkatrészek vásárlását és egyéb, nagyobb összegű tranzakciókat keresték.

1992. augusztusra sikerült kimutatni érdekes összefüggéseket a Chuvakhinnal – a legelső összekötője Amesnek Washingtonban – történt találkozók és a banki tranzakciók között:

- 1985. május 17. – Ames Chuvakhinnal ebédel,
- 1985. május 18. – Ames befizet 9.000 USD-t;
- 1985. július 5. – Ames Chuvakhinnal ebédel,
- 1985. július 5. – Ames befizet 5.000 USD-t;
- 1985. július 31. – Ames Chuvakhinnal ebédel,
- 1985. július 31. – Ames befizet 8.500 USD-t.

A találat rendkívül felvillanyozta a csoportot, Sandy úgy fogalmazott: „Nem kell rakétamérnöknek lenni ahhoz, hogy lássuk, Rick egy istenverte orosz kém”. Ames akkori fizetése nem érte el az évi 70.000 USD-t.

Később, a nyomozás során több összefüggést is kimutattak az orosz kapcsolattartás és a pénzmozgások között, de 1992 őszén még nem látták a teljes képet, így a felfedezés ellenére sem volt még mindig mindenki számára egyértelmű a korreláció, nem tartották azt bizonyító erejűnek.

Kérték az FBI-t, hogy adatbázisukban gyűjtsenek ki minden kontaktot Ames és Chuvakhin között és nézzék át a szovjet követség lehallgatási anyagát is. Ez utóbbit azonban az FBI visszautasította, arra hivatkozva, hogy ezt csak hivatalos nyomozás elrendelése esetén tehetik meg.

Nem sokkal később kész volt a pénzügyi háttér feltérképezése. 1985. és 1991. között Ames teljes befolyó összege több mint egymillió dollár volt, azonosítatlan forrásokból. Pontosan: 1.326.310 USD

Innentől kezdve már nem volt hihető magyarázat, hogy a családtól kapta Ames a pénzt. Mégis, a CIA nem értesítette hivatalosan az FBI-t és nem kezdeményezett nyomozást<sup>23</sup>.

---

<sup>23</sup> A szabályozók szerint az FBI nem kezdeményezett nyomozást a CIA-nál, csak akkor, ha a hírszerző szolgálat erre felkérte. Ezért fordulhatott elő, hogy bár több FBI tisztviselő is dolgozott az Ames ügyön, hivatalos nyomozás nem indult a CIA értesítéséig.

1992 októberében újabb mozaik került a helyére, mert megtudták, hogy a tengeren túli utalások nagy része Ames zürichi számlájáról érkezett.

A CIA 1993. januárban kezdte el tájékoztatni az FBI-t és más hivatalos szervezetet, és megkezdődött az ügy átadása az FBI-nak. 1993. márciusban az egyesített nyomozócsoport leadta az utolsó jelentését, a PLAYACTOR/SKYLIGHT jelentést. A jelentés egy elemzés volt az 1985-86-os veszteségekről és a KGB azon törekvéseiről, hogy eltereljük a figyelmet a beépített személyről a CIA-nál. A jelentés szerint 30 db CIA és FBI művelet dekonspirálódott, vagy szakadt meg gyanús körülmények között a két évben. A jelentés következtetései:

– biztosan beépült a KGB a CIA-ba, a disszidens Edward Lee Howarddal hozzávetőleg egy időben. Valószínűleg 1985. júliusban kezdte el szivárogtatni az adatokat, vagy korábban. A KGB ezt követően kezdte el felfedni az ügynököket.

– A „vakond” a CIA Központ alárendeltségében dolgozott olyan beosztásban, amelyben hozzáfért a szovjet ügynökök adataihoz. A Szovjet és Kelet-Európai Osztály állományában dolgozott, vagy valamilyen elhárító beosztásban. Itt volt egy 40 fős felsorolás a lehetséges árulókról, illetve 5 fő volt kiemelve, élen Amessel, mivel az FBI nem akarta magát kényszerpályára állítani azzal, hogy csak Ames után nyomozhat, hanem látókörben akarta tartani a többi lehetséges gyanúsítottat is<sup>24</sup>.

### **Az FBI átveszi a nyomozást**

1993. május 12-én az FBI washingtoni belvárosi irodája megnyitotta a „Nightmover” fedőnevű nyomozását, amit aztán kihelyeztek a város egy lepukkantnak számító részében lévő Irodához, a Buzzard’s Pointra.

A nyomozáshoz főügyészi és igazságügyi miniszteri engedéllyel minden nyomozati eszközt használhattak<sup>25</sup>. De ellenőrizték a postaforgalmat is, illetve a gépjárművébe nyomkövetőt szereltek.

Az FBI nem figyelte folyamatosan Amest, mivel az állomány nem volt felkészülve erre. A képzett célszemély, ha észreveszi őket, az egész nyomozás megbukik, hiszen elhagyhatja az országot, vagy abbahagy minden bűnös tevékenységet. Az FBI ezt nem akarta, így a telefon cellainformációt használták Ames mozgásának lekövetésére.

Az FBI Les Wiser Jr.-t jelölte ki az ügygazdának, akinek – a CIA megítélése szerint – egyébként nem volt túl sok elhárító tapasztalata. Nyitott volt a CIA felé, és józan gondolkodású, így természetes volt számára, hogy segítséget kér a CIA-tól, amikor szüksége volt rá<sup>26</sup>.

---

<sup>24</sup> A kémelhárítási nyomozásban is célszerű verziókat felállítani és akár több szálon, párhuzamosan kell végezni a nyomozati tevékenységet. Valószínűleg az FBI is ezért jelölt meg több lehetőséget, hiszen még más elkövetők is látókörben voltak, pl. Edward Lee Howard. Másfelől, mind minden bűncselekmény esetén, nem elégséges, ha a nyomozók tudják ki és hogyan követte azt el, a cselekményt bizonyítani is kell.

<sup>25</sup> A külső engedélyhez kötött titkos információgyűjtés eszközeit is: lehallgatás, titkos kutatás, beépülés, stb., pl. Ames irodájának (CIA objektumban!) és lakásának megfigyelését.

<sup>26</sup> Eléggé rosszindulatú személyeskedő megjegyzés, ami a CIA-FBI kapcsolatra – ahogy a könyvből érzékelhető – eléggé jellemző volt. Ismereteim szerint az FBI Akadémián egy hétig tart az elhárító modul a 20 hetes alapképzés során, tehát nem túl sok. Azonban, ha

A „Nightmover” gyorsan és hatékonyan haladt, az FBI rendelkezésére álló teljes eszköztár felhasználásával. A CIA ehhez támogatást nyújtott, mint például amikor nyomkövetőt kellett szerelni Ames kocsjára, azt a CIA segítségével titkos akció keretében vonták ki. Amest meghívták egy kábítószer bűnözési konferenciára az FBI központjába a főnökével együtt. Aztán megkérték Edgert, a főnököt, hogy úgy intézze, Ames vigye őket, tudván, hogy az szeret segítőkésznek mutatkozni parancsnokainál. A konferencia ideje alatt pedig megszerelték az autót. Eleinte az FBI nem szervezett túl szoros együttműködést a CIA-val. Ennek voltak hátulütői, hiszen pl. a megfigyelés során, amikor Ames bement egy CIA objektumba, a figyelőcsoport be akarta vonni az őrséget, persze sikertelenül. A konfliktus elsimítása érdekében a CIA Elhárító Központ tájékoztatta a biztonsági őrséget, hogy egy közös gyakorlat folyik a két szervezet között és az FBI csak imitálta a titkos együttműködésbe való felkérését.

A legbonyolultabb és ezért legidőigényesebb feladat volt Ames irodájának és házának titkos kutatása és betechnikázása. Először is a főnökén keresztül egy új irodába költöztették, amely megfelelt az FBI kívánásainak. Ezt követően beengedték az FBI szakembereit az éjszaka folyamán, hogy végrehajtsák a beépülést, persze ehhez – megfelelő legendával – teljesen ki kellett üríteni az épületet. Megszerezték a kombinációt ahhoz az épületrészhez, ahol Ames irodája volt<sup>27</sup> és jelen voltak, amíg az FBI beépült, annak érdekében, hogy a biztonsági őrség megjelenését kezeljék, hiszen a munka órákig tartott. 1993. június 25-én titkos kutatást hajtottak végre az irodájában, ahol 144 minősített dokumentumot találtak, amelyek nem kapcsolódtak a munkájához<sup>28</sup>.

Természetesen másnap mindenki ment dolgozni, mintha semmi sem történt volna. Miután a kamerákat beszerelték, kidolgozták a csapdát, ami során Amest dokumentálhatják, hogy minősített dokumentumokat tulajdonít el. Kiválasztottak egy iratot, ami érdekelhette a célszemélyt, és amelynek kikerülése, kompromittálódása nem volt nagy veszteség, kár a kormányzat számára. Ennek a másolatát Ames főnökén keresztül juttatták el hozzá, abban reménykedve, hogy majd levágja a minősítést róla és elrakja, vagy csinál vele valamit. Sajnos ez nem jött be, Ames átfutotta a dokumentumot és berakta a kimenő postába.

1993. szeptember 15-én Ames kukájának átvizsgálása során találtak egy jegyzetdarabot, amelyet Ames saját kezével írt. A feljegyzés egy titkos találkozóról szólt Bogotában, október 1-jére. Szeptember 29-én a feleségével folytatott telefonbeszélgetésben azt mondta Ames, hogy a találkozót törölték, majd le is mondta repülőjegy foglalását.

Október 9-én titkos kutatást hajtottak végre a házában, ahol megtalálták Ames feljegyzéseit egy caracasi találkozóról az SZVR-es tartójával. Egy másikon egy tárgyi postaláda jelzőhely adatai voltak a 37. és R utca kereszteződésében, illetve

---

úgy nézzük, hogy FBI elsősorban bűnügyi nyomozó hatóság és a képzése során nem elhárító műveleti tiszteket képez, hanem kémügyek nyomozására (ami az elhárító tevékenységnek csak egy része) készíti fel az állományát, már érthetőbb a kurzus hossza.

<sup>27</sup> Erről nem tudhatott senki, miért kell egy másik részlegnek a kód.

<sup>28</sup> Érdekes részlete ez az amerikai titkosszolgálatok működésének és viszonyának, amely során az egyik ilyen szervezet meghívta a partnerszolgálatot, hogy az ő objektumában hajtson végre műveleti tevékenységet.

további adatok Ames és a KGB kapcsolatára (titkos kommunikáció, minősített CIA művelet, titkos kapcsolatok adatai, és korábbi fizetési adatok).

Október 12-én Ames közölte a feleségével, hogy reggel korábban indul, mert a jelzést ki kell raknia. Az FBI követte és meg is találták a jelzést (függőleges vonal) ami délutánra eltűnt.

Október vége felé egy beszélgetésben Ames felesége aggodalmaskodott egy bogotai út miatt, hogy a határon nehogy gond legyen a nagy összegű készpénzből. November 1-jén Ames elutazott Bogotába, ahol kétszer is találkozott az SZVR-es tartójával. Novembertől kezdve a letartóztatásáig Ames megfigyelés alatt állt, de nem sikerült dokumentálni egyetlen találkozót sem az orosz tisztekkel<sup>29</sup>.

1994 elején azonban Ames Moszkvába utazott volna egy konferenciára és az FBI nem akarta törölni az utat, nehogy felkeltsék Ames gyanakvását, ezért a letartóztatás mellett döntöttek.

Ismételten bevonták közvetlen munkahelyi vezetőjét, akivel külföldi útra indultak volna. 1994. február 21-én – egy munkaszüneti napon – megkérte megint Edgert, hogy utasítsa Amest, menjen be munkahelyére és válaszoljon meg egy, az utazásukkal kapcsolatos táviratot. Ames amikor elhagyta a házát, a sarkon várta az FBI és letartóztatta, incidens nélkül<sup>30</sup>.

A gyanúsítottakat külön kezelték és hallgatták ki, azonban csak az asszony mondott néhány dolgot, Ames nem akart beszélni. Egészen az utolsó pillanatig, a letartóztatásáig Ames öntelt módon viselkedett, soha nem gondolta, hogy elkaphatják, ezért nem is titkolta túlságosan a tevékenységét.

#### **Az Ames ügy következményei**

A letartóztatást követően az FBI megfogalmazott egy sajtóközleményt, úgy tálalva az ügyet, mintha ők egyedül csinálták volna, a CIA pedig csak a háttérben kiegészítő feladatokat végzett. Emiatt a CIA készített egy saját közleményt, amit meg az FBI nem fogadott el. Végül a főügyész az FBI verzióját adta ki, a CIA meg kiadta a sajátját. Egy FBI ügynök szerint, a központjukban úgy érezték, mintha tört dőfték volna a CIA-ba, akik egyébként is magukra vonták a Szenátus haragját. A nyomozás, ami Ames leleplezéséhez vezetett, évekig tartott, azonban a Kongresszust senki nem tájékoztatta menet közben és ez a mulasztás politikai szinten óriási felháborodást váltott ki. A nyomozás során az FBI és a CIA között kialakult ideiglenes jó viszony egy pillanat alatt elillant, ahogy a felsővezetők próbáltak elugrani a Kongresszusi kritikák elől, a másokra hárítva a felelősséget.

Természetesen belső vizsgálat is indult a CIA-nál, de a vizsgálóbizottság vezetőinek fogalmuk sem volt a Műveleti Igazgatóságon folyó munkáról, pláne nem a kémelhárítás műveleti tevékenységről. Mindenkit meghallgattak, aki részt vett a nyomozásban, majd ezt jegyzőkönyvezték és visszaadták átolvasásra. Persze a jegyzőkönyvekben nem az volt, ami elhangzott az interjúban, a pontatlanságok mellett

---

<sup>29</sup> Azért az látszik, hogy Ames „igyekezett mindent elkövetni”, hogy lebukjon. Tulajdonképpen semennyire nem törődött a konspirációval és ez lett a végzete.

<sup>30</sup> Az őrizetbe vételt/elfogást célszerű kontrolált körülmények között végrehajtani, mert ezzel csökkenthetik a bizonytalansági faktorokat, a váratlan események bekövetkezésének esélyét.

valótlan tényállítások is megjelentek. Végül a jelentésüket a nyomozócsoport tagjaival közösen véglegesítették, ami így nem tett említést a CIA vezetésének hibáiról, a Kongresszus tájékoztatásának elmulasztásáról.

Másik hiba volt, hogy az FBI és a CIA nem kötött együttműködési megállapodást – *ebben a feladatokat és felelősségi területeket konkretizálhatták volna* –, aminek hiányát az érintettek erősen megérezték, amikor a felelősség hátrításról volt szó.

A CIA főigazgató március 24-i levelében javasolta, hogy azokat, akik Ames főnökei voltak, továbbá munkájának ellenőrzéséért, vagy a nyomozás vezetéséért feleltek, ne lehessen előléptetni, kinevezni, jutalmazni a vizsgálat végéig, és a CIA-nál szigorú rezsimszabályokat kell bevezetni.

Az tény, hogy a CIA Elhárító Központ a nyomozás utolsó két évében több jelentéstervezetet is felterjesztett a Szenátus Hírszerzési Bizottságnak<sup>31</sup> és a Kongresszusi Hírszerző Bizottságnak<sup>32</sup> címezve, azonban ezek egyike sem jutott túl a CIA vezetésén. A letartóztatás másnapján a CIA és az FBI vezetőit berendelték a Capitol Hillre, hogy adjanak magyarázatot a mulasztásra. A meghallgatások, amelyek során azt kérték számon a CIA-n, hogy miért tartott ilyen sokáig a nyomozás, nem túl kellemes hangvételben folytak. A bizottságok számon kérték a CIA tisztviselőkön, hogy miért gondolták azt, hogy képesek levezetni egy elhárító nyomozást.

Mindkét bizottság elkészítette a jelentését, amelyek megállapításai – főleg a kongresszusi – elég vegyesek voltak. Egy ilyen elmarasztaló megjegyzés szerint nem kaptak tájékoztatást megfelelő időben a CIA nyomozásáról. Ez vélhetőleg azon vezetői álláspontnak volt köszönhető, amely szerint ha időben tudnak mindenről, hamarabb megoldódott volna az ügy. A valóságban azonban a CIA felső vezetése írásban és szóban is kapott tájékoztatást, de onnan nem jutott tovább az információ.

A Szenátus Hírszerző Bizottságának jelentése többek között az alábbi megállapításokat tette:

– Egy CIA tiszt kilenc évig tartó kémkedése, amit nem vettek észre, rendszerhibára utal. Ennek összetevője a bürokrácia, amely toleráns volt személyi és szakmai hibákkal, fegyelmezetlenséggel. A biztonsági tudatosság hiánya és a rendszer szervezeti kultúrája, amely nem volt hajlandó és képes szembesülni a hibákkal, az ámulással. Ebből következően a rendszert meg kell változtatni, a CIA nem szenvedhet több bizalomvesztést, alkalmassá kell tenni az alapfeladatára, ki kell küszöbölni azokat a rendszerhibákat, amelyeket az Ames ügy feltárt. A bizottság jogalkotási intézkedéseket tett a hiányosságok orvoslására és koordinációt követeltek meg az FBI-jal elhárítási kérdésekben. A nyomozati jogkörrel rendelkező hatóságokat felhatalmazták, hogy hozzáférjenek azok pénzügyi és utazási adataihoz, akik minősített információkat kezelnek.

– A változások bevezetéséhez azonban kell a CIA főigazgató, a beosztott vezetők és a teljes állomány akarata. Nagyon fontos a vezetői felelősség megállapítása, és a

---

<sup>31</sup> Select Senate Committee on Intelligence

<sup>32</sup> House Permanent Select Committee on Intelligence



döntéshozók elszámoltathatósága. *Az ügy kapcsán 11 fő felelősségrevonása történt meg, de egyiket sem bocsájították el, nem fokozták le, nem függesztették fel, nem helyezték át. R. James Woolsey főigazgató fegyelmi intézkedései elégtelenek voltak, ő pedig december 28-án lemondott.*

– A CIA elhárító funkciója gyenge és eredendően hibás. A belső és külső jelentések sorozata ellenére – amelyek jelezték a régóta fennálló szervezeti kultúrával kapcsolatos problémákat az elhárító funkcióval kapcsolatban<sup>33</sup> – sem sikerült kiküszöbölni a hibákat. Az elhárító beosztás, tevékenység alacsony megbecsültséget kapott a CIA-nál, így nem vonzott magas kvalitású tisztviselőket. A felelősség (hatáskör) felosztása nem volt egyértelmű az Irodák között, az elhárítási információ nem volt megfelelően megosztva a CIA részlegei között, a CIA nem volt hajlandó megosztani az elhárítási információkat az FBI-jal.

– Az elhárítás rossz állapota az Angleton időszak egyik következménye. James Angleton 1954 és 1974 között az elhárító szakterület vezetője volt a CIA-nál (majd nyugdíjazták) és meg volt győződve, hogy a KGB beépült az Ügynökségbe. Ezért gyanakodott minden szovjet ügynökre és minden CIA tisztviselőre, aki ügynököt szervezett. Ennek eredményeként sorba rúgták ki a CIA tisztviselőket mindenféle objektív vizsgálat nélkül. Így az elhárító tevékenységet elbizonytalanította, leépítette, főleg a Szovjet és Kelet Európai Osztályon, amely a fő felelőse volt a CIA elhárító tevékenységének.

– A külföldi ügynökök beszerzése túlságosan hangsúlyossá vált, miközben nem törődtek az elhárítási aggodalmakkal, érdekekkel. Több tisztviselő azért akart a területre kerülni, mert az elismerés és előléptetés a beszerzésekkel együtt jött, nem pedig a műveleti munkák során történő problémafelismerésen, információszerezésen volt a hangsúly. A CIA közösségben pedig kialakult egy elit kép saját magával kapcsolatban, ami képtelenné tette őket, hogy felfedezzenek egy kémeket maguk között.

– A CIA főigazgató vizsgálja felül a stratégiát az elhárító tevékenység vonatkozásában. A Műveleti Igazgatóság elhárítási területén növelni kell a hatékonyságot, aminek érdekében ki kell dolgozni az előmeneteli rendet, annak követelményeit és az ösztönzőket. Az elhárítók számára biztosítani kell a hozzáférést a külföldi hírszerző műveletekhez.

– Ahogy az Ames ügy bizonyította, a CIA Műveleti Igazgatóság hajlamos tagadni, elutasítani, figyelmen kívül hagyni az állomány alkalmasságára vonatkozó problémákat. Ames karrierjének kezdetétől több alkalmatlanságára utaló jel is volt, ami alapján az előjárói felülvizsgálhatták volna foglalkoztatását. Ezek a gondok: az alkoholizmus, a rezsím szabályok figyelmen kívül hagyása, és az adminisztrációs kötelezettségek – minősített irat kezelése – megszegése. A munkahelyi vezetői érzékelték a személyi és szakmai hiányosságait, de ezeket nem dokumentálták és a kiküszöbölésére nem tettek erőfeszítéseket. A túlzott alkoholfogyasztást és a házasságon kívüli kapcsolatot – beszervezett ügynökkel folytatott szexuális viszonyt – a munka részének tekintették, nem pedig indikátornak, hogy gond van.

A CIA főigazgató gondoskodik róla, hogy mikor egyértelmű jelek vannak valakinek az alkalmatlanságára, azokat dokumentálják és vegyék figyelembe a

<sup>33</sup> A hírszerző szemlélettel működtetett elhárító tevékenység nem tudott megfelelően működni. A két titkosszolgálati szakág különböző szervezeti kultúrával rendelkezik, amely működésük alapvető mozgatórugója ezért nem lehet egyiket a másikra erőltetni.

kinevezésnél, beosztásba helyezésnél, előléptetésnél, és ha olyan súlyú, akkor meg kell szakítani az érintett foglalkoztatását.

– Vizsgálják felül a CIA személyi értékelési rendszerét, hogy jobban megfeleljen az egyéni teljesítmény megítélésére. Vizsgálják felül az adminisztrációs kötelezettségeket és szankciókat. Vizsgálják felül a műveleti eljárásrendet, hogy biztosítva legyen a megfelelő ellenőrzés, irányítás, koordináció és dokumentáció.

– A CIA hibát követett el, amikor 1986-ban vizsgálandó kezdett és nem az FBI-t értesítette. Egy bizottsági tag megjegyzése szerint, „nyomozni kellett volna, nem tanulmányozgatni”. A CIA elemzői azt várták, hogy maguktól történjenek a dolgok, hátha új információk kerülnek felszínre. Folytatták az elemzés-értékelést, de nem volt világosan meghatározott cél, eljárásrend, elképzelés, hogy hogyan járjanak az ügy végére. Az FBI hivatalosan 1986 októberében lett beavatva, de a két szervezet külön-külön végezte a vizsgálatot. Mialatt az FBI és a CIA munkacsoportok rendszeresen cseréltek információt, soha nem végeztek szisztematikus értékelést együtt. Senkiben nem merült fel, hogy az FBI nyomozóit bízzák meg a vizsgálatokkal, holott nyilvánvaló volt, hogy a CIA képtelen felelősségre vonni az alkalmazottait. A CIA-nak a jövőben tájékoztatnia kell az FBI-t a kompromittálódott esetekben, az FBI-nak pedig nyomozati támogatást kell nyújtania.

– A CIA főigazgatója gondoskodjon róla, hogy minden alkalmazott, aki elhárító beosztásba kerül, rendelkezzen megfelelő kiképzéssel, tapasztalattal, és felügyelettel, ami biztosítja, hogy ismerik és tudják alkalmazni a nyomozati jogköröket. A CIA vezetése gondoskodjon róla, hogy a megfelelő elemző és műveleti erőforrások rendelkezésére álljanak az elhárító ügyeknek. Az elhárítási ügyek rendszeresen kerüljenek referálásra a vezetői szintekre is.

– Az FBI főigazgató biztosítsa a megfelelő erőforrásokat a CIA és más szövetségi szervezetek elhárítási ügyeihez. Tekintsék át az FBI eljárásrendjét az elhárítási ügyekben, határozzák meg, milyen alapinformációk szükségesek egy nyomozás megindításához.

– A CIA főigazgatója dolgozzon ki eljárásrendet, hogy amikor egy alkalmazott kémügy gyanúsítottjává válik, a minősített adatokhoz való hozzáférése kerüljön felülvizsgálatra. A CIA főigazgatója gondoskodjon a beléptetési szabályok felülvizsgálatáról, ki, mit vihet ki vagy be az objektumba, legyen véletlenszerű teljes ellenőrzés, váratlan időben és helyen. Vizsgálják felül a rezsimszabályokat, a számítógépes rendszerbiztonságot, növeljék, erősítsék a biztonsági tudatosságot, kiemelt figyelemmel a need to know elvére (*a „szükséges tudni elv” a NATO-nak is információbiztonsági alapelve, miszerint mindenki csak ahhoz az információhoz férjen hozzá – de ahhoz igen – amely a munkája végzéséhez szükséges*).

Amest 1994. április 28-án életfogytiglanra ítélték, felesége 63 hónap börtönbüntetést kapott.

### ***Felhasznált irodalom:***

- An Assessment of the Aldrich H. Ames espionage case and its implications for U.S. Intelligence, Report prepared by the Staff of the Select Committee on Intelligence United States Senate, U.S. Government Printing Office 84-046 Washington, 1994.
- BELOVAI István, Fedőneve: Scorpion, Budapest, 1988, ISBN: 9635506724, magánkiadás
- BÖRCsök András ezredes – Dr. VIDA Csaba mk. alezredes: A nemzetbiztonsági szolgálatok rendszere (Nemzetközi gyakorlat a nemzetbiztonsági rendszer kialakítására) Nemzetbiztonsági Szemle 2014. II. évfolyam I. szám pp. 63-100.
- Circle of Treason: A CIA account of traitor Aldrich Ames and the men he betrayed – Sandra Grimes and Jeanne Vertefeuille, ISBN 978-1-61251-305-8, 2012 Naval Institute Press
- KOVÁCS Krisztián: Az amerikai katonai elhárítás külföldön végzett műveleti tevékenységének sajátosságai a Conrad kémügy tükrében, Szakmai Szemle, Katonai Nemzetbiztonsági Szolgálat, 2015/1. pp. 35-64.
- LOWENTHAL, Mark M.: Intelligence From Secrets to Policy ISBN: 1483307786 Published 2014.
- MCCARGAR, James: A short course in the secret war, Madison Books, 2001, első kiadás 1963, ISBN 978-1-5683-3179-9.
- Spycraft: The Secret History of the CIA's Spytechs, from Communism to Al-Qaeda, Robert Wallace, H. Keith Melton, Henry R. Schlesinger, ISBN 978-0-525-94980-0, 2009.
- [https://en.wikipedia.org/wiki/Central\\_Intelligence\\_Agency](https://en.wikipedia.org/wiki/Central_Intelligence_Agency)
- <http://osaarchivum.org/>
- <https://nsarchive.wordpress.com>
- <https://archive.org/>

### **Bevezető**

2011-ben Norvégiában Anders Behring Breivik két merényletben összesen 77 embert ölt meg, ezzel Európa történelmének egyik legnagyobb tömeggyilkosává vált. A támadó az ún. magányos farkasok közé tartozik, tettét egyedül hajtotta végre. Breivik radikális nézeteket vallott, elítélte a multikulturalizmust és a migrációt. Az ilyen típusú szélsőségesek mellett ma Európában az iszlám fundamentalizmus motiválta magányos elkövetők jelentik a legnagyobb veszélyt. Az Iszlám Állam közel-keleti veszteségei miatt a harcokban résztvevő dzsihádisták nagy számban jelenhetnek meg kontinensünkön.<sup>1</sup> A nizzai, a berlini vagy éppen a barcelonai merényletek bizonyítják, hogy a támadások már nemcsak gépfegyverekkel vagy robbanóeszközökkel hajthatók végre; a gázolósos elkövetési mód esetében az előkészületek teljes mértékben rejtve maradhatnak.<sup>2</sup>

A 21. században a magányos elkövetők már az interneten radikalizálódnak, esetleg ott teremtenek kapcsolatot más szélsőséges csoportokkal. Az elmúlt években több magányos elkövető kapcsán is bizonyítást nyert, hogy a merénylő a támadás kitervelése során szélsőséges gondolatokat tartalmazó kiadványokat tett közzé az interneten, illetve nyilvánosan vállalta tervét.<sup>3</sup> Emiatt a radikális tartalmú honlapok és a közösségi oldalak a védelmi szektor látókörébe kerültek. A magányos elkövetők potenciális számának növekedése és az elkövetési mód megváltozása miatt a hagyományos nemzetbiztonsági feladatok mellett szükség van új típusú eljárásokra is, melyek segíthetik a szakembereket a tervezett támadások időbeni felderítésében. A tanulmány amellet érvel, hogy a magányos elkövetők többsége meghatározható pszichés jellemzőkkel bír, illetve, hogy ezek a jellemzők pszichológiai eszközökkel azonosíthatók. A 21. században az internet az egyik legfőbb terepe mind a radikális

---

<sup>1</sup> Az Iszlám Állam magányos elkövetői célba vehetik Európát. frissujsag.ro, 2017.03.29. <http://www.frissujsag.ro/az-islam-allam-maganyos-elkovetoi-celba-vehetik-europat/> (Letöltés ideje: 2017. 09. 15.)

<sup>2</sup> 2015 és 2017 között összesen 132-en veszítették életüket ún. rammingmerényletben Európában. A legtöbb halálos áldozattal járó gázolósos támadás Nizzában történt ünnepi felvonulás közben, a 86 halott mellett majdnem 500-an szereztek komoly sérüléseket. A berlini karácsonyi vásáron végrehajtott támadásban 12-en haltak meg, míg a Barcelonában 2017 nyarán egy kisteherautó hajtott a tömegbe, megölve ezzel 13 embert. Forrás: TÁLAS P. – SZENTE-VARGA M.: A 2017. augusztusi spanyolországi terrortámadásokról. 2017.08.21. SVKK, Elemzések 2017/18. [http://archiv.netk.uni-nke.hu/uploads/media\\_items/svkk-elemzesek-2017-18-a-2017-augusztusi-spanyolorszagi-terrortamadasokrol-talas-p-szente-varga-m-1.original.pdf](http://archiv.netk.uni-nke.hu/uploads/media_items/svkk-elemzesek-2017-18-a-2017-augusztusi-spanyolorszagi-terrortamadasokrol-talas-p-szente-varga-m-1.original.pdf) (Letöltés ideje: 2017. 09. 15.)

<sup>3</sup> ld. az Európai Unió Internet Referral Unit nevű szervezet működését. EU Internet Referral Unit–Year one report. Forrás: <https://www.europol.europa.eu/publications-documents/eu-internet-referral-unit-year-one-report-highlights> (Letöltés ideje: 2017. 09. 15.)

csoportok és személyek működésének, mind az őket célzó felderítésnek.<sup>4</sup> A pszichológiai szempontú tartalomelemzés kvalitatív és kvantitatív módszerekkel is hozzájárulhat a magányos elkövetők esetleges internetes jelenlétének kiszűréséhez és a tervezett támadások megakadályozásához.

### A magányos elkövetők tipológiája

A bevezetőben említett Breivik típusú magányos elkövetők általában nem kapcsolódnak semmilyen radikális szervezethez, azonban a muszlim terrrorszervezetek által ösztönzött gázolások merényletek elkövetői már egy szélsőséges eszme parancsára cselekszenek. Hankiss Ágnes mellett érvel, hogy az Iszlám Állam által inspirált merénylők kevésbé tekinthetők magányosnak, mivel mind anyagi, mind operatív támogatást kaptak az előkészületek során.<sup>5</sup> A Magyar Időkben megjelent cikkében a nyilvános titkosszolgálati információk alapján arra a következtetésre jut, hogy az európai merényleteket az Iszlám Állam operatív emberei tervezték meg, akik közvetlen kapcsolatban voltak a terrrorszervezettel. A muszlim terrrorszervezetek már 2006 óta propagálják a magányos elkövetést, először az al-Kaida jelentetett meg támadásra buzdító írásokat az Inspire magazinban. 2014 szeptemberében az Iszlám Állam tett közzé felhívást a hívek számára, hogy harcoljanak minden lehetséges helyen, míg a Mujahideen Secrets nevű internetes felület kifejezetten magányos elkövetők számára készült.<sup>6</sup>

A fentiekből is látszik, hogy meg kell különböztetni a Breivik-típusú magányos farkasokat a muszlim terrrorszervezetek által inspirált elkövetőktől, mivel mind a kivitelezésben, mind a motivációs háttér tekintetében eltérések mutatkoznak.

Ma az alábbi magányos elkövetéssel kapcsolatos elméletek terjedtek el tudományos körökben:

A *vezető nélküli ellenállás (leaderless resistance)* modell<sup>7</sup> azt állítja, hogy a szélsőséges csoportok kommunikációs csatornákon keresztül ösztönzik a híveiket terrortámadások elkövetésére. Ebben az esetben a merényletet elkövető egyén számára az adott csoport csak az ideológiai alapot nyújtja, de más módon nem kötődik hozzá. A modell szerint nehéz felderíteni ezeket az elkövetőket, mivel nem tagjai a szélsőséges csoportnak, csupán szimpatizánsai. Ahogy a korábbiakból kiderült, a muszlim terrrorszervezetek használnak hasonló technikát. Az Iszlám Állam számtalan alkalommal szólította fel híveit merényletek elkövetésére (nyugati célpontok ellen), többek között a 2016-os ramadán idején: Abu Mohammed al-Adnani, az ISIS akkori szóvivője hangüzenetben azt mondta, *“a ramadán a*

---

<sup>4</sup> EU Internet Referral Unit–Year one report. Forrás: <https://www.europol.europa.eu/publications-documents/eu-internet-referral-unit-year-one-report-highlights> (Letöltés ideje: 2017. 09. 15.)

<sup>5</sup> HANKISS Á.: „Égesd el őket!” Európai terror – A magányos elkövető legendája. Magyar Idők, 2017. július 1. Forrás: <http://magyaridok.hu/lugas/egesd-el-oket-1872439/> (Letöltés ideje: 2017. 09. 15.)

<sup>6</sup> Uo.

<sup>7</sup> BATES R. A. (2012): Dancing with wolves. Today’s lone wolf terrorists. The Journal of Public and Professional Sociology. Vol. 4. Is. 1., 2012., pp. 1-14.

*megszállás és a szent háború, a dzsihád hónapja. Isten akaratával a világon mindenhol tegyétek ezt a hónapot a hitetlenek számára a szenvedés hónapjává”.*<sup>8</sup>

Egy másik nemzetközi elmélet szerint megkülönböztethetünk **káoszvezérelt és karrierista magányos elkövetőket**.<sup>9</sup> Az első típusú merénylők számára a minél nagyobb károkozás és sajtóérdeklődés a cél, míg a karrieristák politikai célokért küzdenek, ezért kisebb határfokú, de rendszeres támadássorozatot indítanak. A káoszvezérelt elkövetők közül kerülnek ki gyakran az öngyilkos merénylők, míg a második típusba tartozók magas önbecsüléssel rendelkeznek, és minden egyes sikeres merénylet után tovább nő a magabiztosságuk.

A magányos elkövetési mód egy másik közismert elmélete szerint<sup>10</sup> a merénylőknek négy típusát lehet megkülönböztetni:

- **„loner”** – A fogalom magyar jelentése: magányos ember. A loner típusú elkövető nem tagja egy radikális szervezetnek sem, azonban a merénylet kivitelezésekor egy szélsőséges eszmével legitimálja a cselekedeteit. Az általa elismert radikális csoportot interneten keresztül figyelemmel kíséri, passzív módon figyeli tevékenységét, propagandakiadványait, azonban nem lép kapcsolatba a tagokkal. A radikalizálódás mellett a loner általában valamilyen pszichológiai vagy szociális zavarban szenved (pl. elszegényedés, magány), így inkább ezek a tényezők okozzák a destruktív viselkedést (a radikalizálódás is már egy tünet). Többségük nyíltan vállalja szélsőséges nézeteit, illetve a támadási szándékot is, így könnyen kerülnek a hatóságok látókörébe. A mentális zavar miatt azonban nehezen állapítható meg, hogy milyen valószínűséggel követnek el merényletet.
- **„lone wolf”** – A kifejezés magyar jelentése magányos farkas. Ez a típus egyedül hajt végre terrorcselekményeket, azonban kapcsolatot tart fent legalább egy radikális csoporttal. A lone wolf az interneten kommunikál más magányos elkövetővel és radikális csoporttagokkal is, azonban arról általában kevés információ derül ki, hogy részt vett-e terrorista kiképzésben. Összességében a lone wolf típusú elkövető tette mögött egy szélsőséges csoport áll, melynek tagjai buzdítással vagy közvetett irányítással hatással voltak az elkövetőre.
- **„lone wolf pack”** – A kifejezés a magányos farkasok laza szerveződésére utal. Az ebbe a típusba tartozó személyek kis létszámú csoportban működnek, szélsőséges ideológiát követnek, de nem tagjai egy nagyobb terrorszervezetnek sem. Fennállásuk csak az adott támadás kivitelezéséig tart, és náluk is a fő kommunikációs csatorna – akár más csoportokkal is – az internet.
- **„loner attacker”** – A szó magyarul magányos támadót jelent. Ezek az elkövetők egyedül hajtják végre merényletet, azonban egy terrorszervezet

---

<sup>8</sup> Üzent az Iszlám Állam: Tegyétek szenvedéssé a hitetleneknek a ramadánt. hirado.hu, 2016.05.22., <http://www.hirado.hu/2016/05/22/uzent-az-islam-allam-tegyetek-szenvedesse-a-hitetleneknek-a-ramadant/> (Letöltés ideje: 2017. 09. 15.)

<sup>9</sup> BATES i.m.

<sup>10</sup> PANTUCCI R. (2011): A typology of lone wolves: Preliminary analysis of lone islamist terrorists, International Centre for the Study of Radicalisation and Political Violence, London, March 2011.

fizikai és anyagi támogatásával. A támadáshoz szükséges eszközöket – fegyvereket, pénzt –, a fő instrukciókat az adott szervezet vezetője biztosítja.

A magányos merénylőkkel kapcsolatos *négydimenziós elmélet*<sup>11</sup> szerint az elkövetési módot négy tényező határozza meg: a radikalizálódás mértéke, a motiváció, a kivitelezés és a kockázattudatosság. A radikalizálódás mértékéhez hozzátartozik az azt meghatározó befolyásoló tényező definiálása is (pl. az egyén saját érdeklődése, illetve a szocializációs és külső környezeti hatások megléte). A modell szerint az egyéni motiváció alapján megkülönböztethetünk egoista és altruista merénylőt. Az előbbi számára a merénylet elkövetése a saját felsőbbrendűségének igazolása, magát a társadalom elé képzele, és általában szélsőséges ideológiákkal kapcsolatos irodalomból, internetes honlapokról építi fel saját eszmerendszerét. Az altruista elkövetőt egy magasabb cél motiválja, többségük öngyilkos merényletet hajt végre. A harmadik dimenzió, a kivitelezés lényegében megegyezik a korábban említett káoszvezérelt és karrierista terrorista elkövetési módjával. A kockázattudatosság a veszélyforrások felmérését, azok elkerülésére tett erőfeszítéseket és a várható végkimenetellel kapcsolatos valószínűségek kiszámolását jelenti.

Egy Psychology Today nevű (internetes) szaklapban megjelent elemzésben<sup>12</sup> idézett kutatások szerint a magányos elkövetők esetében gyakoribb a mentális zavar megléte, mint egy terrorszervezet tagjainál. A mentális zavar önmagában azonban nem okoz erőszakos hajlamot, azonban a betegség kombinálva a személyes frusztrációval és a szélsőséges politikai, vallási vagy ideológiai nézetekkel már elvezethet egy potenciális támadás végrehajtásáig. A magányos farkasok főként kényszeres, szorongásos zavarban szenvednek, illetve gyakori a depresszív kórkép megjelenése is.

### **Szélsőséges tartalmak az interneten**

Hazánkban Somogyi Ábel esete hívta fel a figyelmet a magányos farkasok jelentette veszélyre. A férfit 2010-ben azzal vádolták, hogy 22 diákot akart megölni az ELTE jogi karán, mely tervéről internetes blogjában számolt be. A 2010-es elfogásáig Somogyi Ábel sportlövész klubba járt, fegyvertartási engedélyt szerzett és dicsőítette az iskolai mészárlásokat. Ez az eset rávilágított az internet szerepére a magányos elkövetők felderítésében, mivel a labilis mentális állapotú férfi sok időt töltött az interneten, blogjában rendszeresen tett közzé fenyegető verseket, iskolai mészárlásokkal foglalkozó tartalmakat. A novellák és versek istentagadóak, blaszfémiát és a gyilkolás eszményítését tartalmazzák.<sup>13</sup>

---

<sup>11</sup> BATES i.m.

<sup>12</sup> PERSAUD R. – BRUGGEN P.: Atrocity in the city of Nice: An act of clinical insanity? Psychology Today, 2016. július 18. Forrás: <https://www.psychologytoday.com/blog/slightly-blightly/201607/atrocity-in-the-city-nice-act-clinical-insanity> (Letöltés ideje: 2017. 09. 15.)

<sup>13</sup> „Én vagyok isten” Heteken belül gyilkolt volna S. Ábel. Hetek, 2010.02.19. Forrás: [http://www.hetek.hu/hatter/201002/en\\_vagyok\\_isten](http://www.hetek.hu/hatter/201002/en_vagyok_isten) (Letöltés ideje: 2017. 09. 15.)

Az Europol már 2014-ben<sup>14</sup> felhívta a figyelmet arra, hogy a szélsőséges személyek és csoportok internetes tevékenysége egyre nagyobb fenyegetést jelent. Az iOCTA (Internet Organised Crime Threat Assessment) című dokumentum a kiberkockázatok bemutatása során külön kiemeli a muszlim terrorizmus és a magányos farkasok internetes jelenlétét. A szélsőséges szervezetek és egyének anonimitásuk megőrzése mellett könnyen ismerkedhetnek meg más radikális eszmékkel, személyekkel, illetve a támadások megtervezése és kivitelezése is lehetővé vált a webes felületeken.

Az Europol jelentése szerint a hatóságoknak erre a problémára preventív intézkedésekkel kell reagálni, melybe beletartozik az online jelenlét növelése, olyan kommunikációs programok támogatása, melyek fejlesztik a biztonságos és tudatos internetes magatartást, illetve a hatóságok fókuszpontjának ráirányítása a proaktív, hírszerzésen alapuló eljárásokra. Az uniós jelentés külön fejezetet szentel az ún. kiberpszichológiának, mely az internet által befolyásolt emberi viselkedést vizsgálja. A hálózati kapcsolatok felderítése és a szereplők tevékenységének elemzése segítségével azonosítani lehet az online és az offline viselkedés közötti különbséget, illetve meghatározni az internetes tevékenység alapján a valós életben várható magatartást.

Az internetes szélsőséges tartalmak elemzéséhez azonban szükség van olyan empirikus módszerekre, melyek segítségével megbízhatóan vizsgálhatók az adott anyagok. A tanulmány amellettt érvel, hogy a pszichológiai szempontú tartalomelemzés hozzájárul a szélsőséges internetes tevékenység jobb megértéséhez.

### **A tartalomelemzés fogalma**

A tartalomelemzés interdiszciplináris módszer, mivel több tudományterületen is használható, alapvetően a közlemények meghatározott célú elemzését jelenti.<sup>15</sup> A tartalomelemzés két fő szakaszból áll: az első lépés a közlemény kódolása, majd ezután következik az interpretáció, mely a kódolt tartalmakban rejlő rejtett összefüggések feltárását jelenti.<sup>16</sup>

A tartalomelemzés segítségével tehát az adott dokumentumból mögöttes tartalmak kinyerésére van lehetőség, illetve nagy mennyiségű kvalitatív információ kezelhető reprezentációra való redukálására.<sup>17</sup> A kutatók általában írásos dokumentumokat, videófelvevételeket, művészeti alkotásokat, illetve fényképeket vizsgálnak, az elemzés során az üzenetek speciális jellemzőit igyekeznek feltárni. A kutatási kérdés szempontjából a vizsgált tartalmakat két szinten lehet elemezni: a felszíni struktúra és a mögöttes meghúzódó látens tartalom szintjén.<sup>18</sup>

---

<sup>14</sup> The internet organised crime threat assessment (iOCTA), European Police Office, 2014.

<sup>15</sup> ANTAL L.: A tartalomelemzés alapjai (Gyorsuló idő), Magvető Kiadó, 1976.

<sup>16</sup> Uo.

<sup>17</sup> SMITH C. P.: Content analysis and narrative analysis. In REIS H. T. – JUDD C. M.: Handbook of research methods in social and personality psychology, pp. 313-335. Cambridge University Press, New York, 2000.

<sup>18</sup> BERG B.: Qualitative research methods for the social sciences, Fourth edition. Allyn & Bacon, A Pearsons Education Company, Needham, Massachusetts, 2001.



A tartalomelemzésnek alapvetően két típusa létezik:<sup>19</sup> a kvantitatív elemzés során a szavakat előre meghatározott módon kategóriákba soroljuk, majd a találati gyakoriság alapján következtetéseket vonunk le. A szakértők ezt a módszert helyettesítő tartalomelemzésnek hívják. A vizsgálati eszköz ebben az esetben nomotetikus<sup>20</sup>, mivel a kutató egy előzetes vizsgálat során besorolja a szavakat egy adott kategóriába. A kvalitatív megközelítés ezzel szemben nem fogadja el azt a nézetet, hogy a szavakat egységes kódokba lehetne rendezni. A kvalitatív elveket valló hagyomány a korrelációs módszert használja, mely során egy adott szövegben az egymás környezetét jelentő szavak együtt előfordulásából lehet következtetéseket levonni a szöveg jelentéstartalmára vonatkozóan.

### **Kvantitatív tartalomelemző eljárások**

A korszerű tartalomelemző szoftverek kvantitatív módon elemzik a vizsgált szövegeket, ahol az empirikus kutatás alapja egy előzetes kategóriarendszer használata. Ezek a programok a szöveg nyelvi-strukturális tulajdonságainak adnak adekvát pszichológiai jelentést.<sup>21</sup>

Egy 2005-ös kutatás<sup>22</sup> a Las Vertikum nevű szoftver<sup>23</sup> működésén keresztül szemlélteti a kvantitatív tartalomelemzést. A kutatás élettörténeti elbeszéléseket vizsgált, ahol a tagadásra és az énrre vonatkozó nyelvi markerek gyakoriságát vetették össze a vizsgálati személyek által kitöltött személyiségtesztekkel. Az eredmények szerint a tagadó szavak gyakorisága összefügg az energizáltság és a teljesítményvágy hiányával, a hiányérzettel és az akadályozottsággal, míg a szelfre mutató kifejezések magas száma összefüggött a depresszív és szuicid állapottal, a frusztráció és szorongás okozta maladaptív megküzdési módokkal. Az idézett vizsgálat tehát kimutatta, hogy a szógyakoriságból következtetni lehet az egyén mentális állapotára.

A kvantitatív tartalomelemzés egyik legismertebb szakértője James W. Pennebaker, amerikai szociálpszichológus. A kutató által kidolgozott elmélet alapfeltevése, hogy az egyén hétköznapi kommunikációjából következtetni lehet

---

<sup>19</sup> LÁSZLÓ J. (2011): A tudományos narratív pszichológiai tartalomelemzés és a pszichológiai tartalomelemzés hagyományai. *Pszichológia* (2011), 31. évf., 1. szám, pp. 3-15.

<sup>20</sup> nomotetikus: (görög)Törvényszerű. Törvényszerű megismerésre törekvő, ezen alapuló (pl. tudomány) Tudományos és Köznyelvi Szavak Magyar Értelmező Szótára <http://meszotar.hu> (Letöltés ideje: 2017. 09. 15.)

<sup>21</sup> LÁSZLÓ J. (2005): A narratív pszichológiai tartalomelemzés, *Magyar Tudomány*, 2005/11. p. 1366.

<sup>22</sup> HARGITAI R., NASZÓDI M., KIS B., NAGY L., BÓNA A., LÁSZLÓ J. (2005): A depresszív dinamika nyelvi jegyei az énelbeszélésekben. A LAS-Vertikum tagadás és szelf-referencia moduljai. *Pszichológia*, 2005. 2., pp. 181-199.

<sup>23</sup> A magyar nyelvű tartalomelemző szoftverek létrehozása komoly nehézségbe ütközik a nyelvi sajátosságok miatt: a képzők, jelek és ragok számtalan szóvariációt eredményeznek, így az angol nyelvű programokban működő szólisták nálunk nem megvalósíthatók. Ennek kiküszöbölésére például a LAS-Vertikum LINTAG nevű kódoló programja a szavak szerkezetét (más szóval morfológiáját) elemzi, így a szöveg szavait morfémmákra bontja, és azokat vizsgálja. Ezzel a módszerrel lehetővé vált a magyar nyelvű szoftverek használata a nagy szövegtörzsekben található nyelvi jellegzetességek azonosítására. ld. Hargitai és mtsi, 2005.

annak szociális státuszára, korára, motivációjára, vagy akár a nemére is.<sup>24</sup> A szövegben rejlő számtani és szemantikai jellemzők felfedik az elbeszélő pszichológiai és társadalmi tulajdonságait. Pennebaker abból indul ki, hogy a mondatok összetétele, a szóhasználat és a nyelvtani sajátosságok (a szöveg stílusa) kvantitatív módon vizsgálhatók. Pennebaker munkatársaival kidolgozta a LIWC (Linguistic Inquiry and Word Count) nevű programot, mely alkalmas nagy kiterjedésű szövegek elemzésére. A szoftver közel 80 nyelvtani és számtalan pszichológiai és tematikus kategóriát kezel, illetve a szöveg elemeit a megfelelő kategóriákba rendezi. A LIWC meghatározza, hogy a szöveg elemei milyen kategóriákba tartoznak: a dimenziók hierarchikusan rendeződnek, mivel egy szó több kategóriában is megjelenhet. A program felismeri a nyelvtani formákat (igék, névmások, névelők, stb.), pszichológiai folyamatokat (pozitív, negatív érzelmek, kognitív állapotok, stb.), időre, térre vonatkozó szavakat és az alapstatisztikai jellemzőket is mint a nem, foglalkozás, életkor. A szoftver a szöveg stílusát is vizsgálja a nyelvtani és stilisztikai alakzatok azonosításának segítségével, illetve lehetőség van saját kategóriák kialakítására is.<sup>25</sup> A program legújabb, 2015-ös verziója már kezeli az internetes szlengeket is, így alkalmas a közösségi oldalak (Facebook, Twitter) szövegeinek elemzésére is.<sup>26</sup>

A LIWC számos kutatásban eredményesen működött; 2003-ban Mehl és Pennebaker tanulmányukban<sup>27</sup> azt vizsgálták, hogy miként változtatta meg a 2001-es amerikai terrortámadás a szociális interakciókat. A vizsgált személyek beszélgetéseit egy speciális eszközzel rögzítették, majd elemezték a merénylet előtti és utáni interakciók közötti különbséget. (A terrortámadás előtti minta eredetileg egy másik kutatáshoz készült.) Az elemzés során az derült ki, hogy közvetlenül a támadás után megnőtt a személyes diádikus<sup>28</sup> interakciók száma, csökkentek a csoportos kapcsolatok és a mobiltelefonos beszélgetések is. A kutatás rámutat arra, hogy a tartalomelemzéssel azonosítani lehet a szociális viselkedésben bekövetkező változásokat nagy stressz hatására.

### A kvalitatív tartalomelemzés

A kvalitatív tartalomelemzés hasonlóan a kvantitatív eljárásokhoz meghatározott elemzési szabályokat követ, de nem előzetes kategóriarendszer alapján rendezi a szöveg elemeit. Az elemzési egységek így nem előre meghatározottak, hanem az elemzés során alakulnak ki. Az intuitív módon kialakult elemzési egységek azonban már számszerűsíthetők, így kvantitatív eszközökkel

---

<sup>24</sup> PENNEBAKER, J.W. – MEHL, M.R. – NIEDERHOFFER, K.G.: Psychological aspects of natural language use: Our words, our selves. *Annual Reviews Psychology*, 2003., 54. pp. 547-577.

<sup>25</sup> Uo.

<sup>26</sup> PENNEBAKER, J.W. – BOYD, R.L. – JORDAN, K. – BLACKBURN, K.: The development and psychometric properties of LIWC2015. Austin, TX: University of Texas at Austin.

<sup>27</sup> MEHL M.R. – PENNEBAKER J.W. (2003): The social dynamics of a cultural upheaval: Social interactions surrounding September 11, 2001. *Psychological Science*, Vol. 14., Nr. 6., November 2003.

<sup>28</sup> diádikus: kettős, két ember párosára vonatkozó. Idegen Szavak Szótára, <http://idegen-szavak-szotara.hu> (Letöltés ideje: 2017. 09. 15.)

mérhetővé lehet tenni az adott szöveget. A kvalitatív tartalomelemzés komplex eljárás, mely alapvetően hét lépésből áll.<sup>29</sup>

- Az első lépés minden esetben a konkrét kutatási kérdés meghatározása. A kutató meghatározza a témakört, a vizsgálandó változókat, melyeket a kérdésfelvetés fogja meghatározni.
- A kutatói kérdés elméleti keretbe való ágyazása a második lépés. A kutató tisztázza a vizsgálat alapjául szolgáló elméletet, ennek megfelelően értelmezi és elemzi az eredményeket.
- A harmadik lépés a kutatási terv és módszerek megfogalmazása. A kutató itt meghatározza, hogy leíró, feltáró, korrelációs vagy ok-okozati vizsgálati eszközöket használ-e. Az empirikus kutatásokban alapvetően az utóbbi kettőt használják, azonban a leíró és feltáró jellegű vizsgálatok is hasznos adatokkal szolgálnak az adott témáról.
- A negyedik lépés a mintavételi stratégia és a vizsgálati alanyok meghatározása. Ezen a szinten szükséges annak bizonyítása, hogy az adott mintanagyság elegendő a kutatási kérdés megválaszolásához. Olyan esetben, amikor csak kényelmi mintavétel lehetséges, az eredmények általánosítását fenntartásokkal kell kezelni.
- Az ötödik lépés az adatgyűjtési és elemzési módszerek meghatározása, mely során a kutató konkretizálja az eljárásokat, a kvantitatív és kvalitatív elemeket. Kvalitatív tartalomelemzésnél a kategóriaalkotás általában induktív módon történik.
- A hatodik lépés az eredmények bemutatása az előzetesen meghatározott kutatási kérdések mentén. A kutatás során kapott eredményeket a vizsgálatot végző személy köteles részletesen bemutatni a tanulmány végén.
- A kvalitatív tartalomelemző kutatás végén – hasonlóan más empirikus vizsgálatokhoz – a kutató összegzi az eredményeket és következtetéseket von le az addig leírtakból. A vizsgált tartalmak a sztenderdizált tesztekkel szemben nem megismételhetőek, így az objektivitás ezekben az esetekben nem értelmezhető.

### **Internetes tartalmak elemzése a gyakorlatban**

A cikk amellett érvel, hogy a fenti tartalomelemző technikák segítségével elemezni lehet azokat az internetes tartalmakat, melyek összefüggésbe hozhatók a potenciális magányos elkövetőkkel. A nemzetközi és hazai szakirodalom áttekintése során főként a terrorista csoportok tevékenységét érintő kutatások kerültek látókörbe, ezek közül is kiemelten az arab nyelvű weboldalak vizsgálata. Az IntelCenter nevű terrorizmussal foglalkozó civil cég 2005-ben összegyűjtötte az akkor nyilvánosan elérhető dzsihádisták videófelvételeket. Az FBI egyik szakembere egy tanulmányban<sup>30</sup> megvizsgálta ezeket a tartalmakat, és arra jutott, hogy a

<sup>29</sup> MAYRING P.: Qualitative content analysis: theoretical foundation, basic procedures and software solution. Klagenfurt, Ausztria, 2014.

<sup>30</sup> REID E. (2009): Analysis of Jihadi Extremist Groups' Videos, Forensic Science Communications, 2009 július, Vol. 11., Nr. 3. Letöltés ideje innen (2013. október 11.): [http://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/july2009/index.htm/research\\_tech/2009\\_07\\_research01.htm](http://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/july2009/index.htm/research_tech/2009_07_research01.htm) (Letöltés

felvételek két típusba sorolhatók: a terrorcselekmények bemutatása a megfélemlítést szolgálják, míg a propaganda célú, illetve vezetői videók kommunikációs célokra készültek.

Egy 2013-as kutatás<sup>31</sup> olyan arab nyelvű fórumokat vizsgált, ahol radikális személyek kommunikáltak egymással. A kutatók a pozitív és negatív hangvételű hozzászólások jelenlétét vizsgálták, és arra jutottak, hogy a radikális arab honlapokon megjelenő személyek kommunikációjukra jellemző a vallásos szavak túlsúlya, illetve az ellenséges érzelmeket és indulatokat mutató kifejezések jelenléte.

Az online szélsőséges oldalak figyelése – ahogy a fentiekből is kiderül – már a 2000-es években kiemeltté vált a védelmi szektorban. Egy 2003-as kutatás<sup>32</sup> eredményei azt mutatják, hogy a való életben elszigetelt, magányos személyek könnyebben radikalizálódnak az internet segítségével, mivel ők fogékonyabbak a multimédiás tartalmakra. A szélsőséges tartalmakkal bíró honlapok és fórumok összegyűjtik ezeket az egyéneket, így ezek monitorozása kiemelt hatósági feladat.

A potenciális magányos elkövetők internetes tevékenységére reflektálva az Europol 2017-ben megvizsgálta az Iszlám Állam üzemeltetett Dabiq nevű internetes magazin említését a Twitter-felhasználók körében.<sup>33</sup> A kutatók a magazinnal kapcsolatos hozzászólásokat csoportosították a hangvételük, a felhasználói profil terrorizmushoz való kötődése és a muszlim valláshoz való kapcsolódás szerint. Az eredmények szerint a Dabiq-kal kapcsolatos bejegyzéseket közzétevő profilok egy részét a Twitter a megjelenés után felfüggesztette. A tartalom vizsgálata után kijelenthető, hogy azok a felhasználók kerültek felfüggesztésre, akik a hozzászólásaik alapján szimpatizáltak az Iszlám Állam eszméivel. A kutatás megállapításai szerint a vizsgált Dabiq-kiadvány terjesztését célzó bejegyzések olyan profilokon jelentek meg, melyek kevés követővel rendelkeztek és rövid ideje működtek. Az előbbieket alapján feltételezhető, hogy a Twitter tartalomlemező kontrollja eredményesen szűri ki a radikális elemeket.

2015-ben az Europol – reflektálva a digitális forradalomra és a terrorizmus online terjedésére – létrehozott egy internetes felügyelő szervezet (Internet Referral Unit – EU IRU)<sup>34</sup>, melynek célja a szélsőséges tartalmak azonosítása és az azokhoz köthető feladatok koordinálása a társszervekkel. Az egység lényegében a nyílt forrású tartalmak monitorozásával és elemzésével foglalkozik, továbbá a terrorizmus mellett figyel a illegális migrációval kapcsolatos tartalmakat is. Az IRU 2016-ban

---

ideje: 2017. 09. 15.)

<sup>31</sup> CHALOTRON T. – ELLMAN J. (2013): Affect analysis of radical contents on Web forums using SentiWordNet. *International Journal of Innovation, Management and Technology*, Vol. 4., No. 1., February 2013, pp. 122-124.

<sup>32</sup> GERSTENFELD P. B. – GRANT D. R. – CHIANG C-P. (2003): Hate online: A content analysis of extremist internet sites. *Analyses of Social Issues and Public Policy*. Vol. 3., No. 1., 2003. pp. 29-44.

<sup>33</sup> GRINNEL D. – MACDONALD S. – MAIR D. (2017): The response of, and on, Twitter to the release of Dabiq Issue 15. Europol Public Information. 1st European Counter Terrorism Centre (ECTC) conference on online terrorist propaganda, 10-11 April 2017, at Europol Headquarters, The Hague.

<sup>34</sup> EU Internet Referral Unit–Year one report. Forrás: <https://www.europol.europa.eu/publications-documents/eu-internet-referral-unit-year-one-report-highlights> (Letöltés ideje: 2017. 09. 15.)

több, mint 70 olyan platformot elemezett, ahol szélsőséges tartalmak jelentek meg. Az egység a felderítés és az elemzés után értesíti a honlap üzemeltetőjét, aki dönt a tartalom eltávolításáról. Az IRU célja, hogy feltárja azokat a mechanizmusokat, mely alapján fellelhető a terrorista online propaganda. Az elmúlt évek európai terrortámadásai rávilágítottak arra, hogy szükséges az internetalapú kommunikáció elemzése, így az IRU feladatának tekinti a tagállamok ilyen irányú munkájának támogatását is, mind technológiai, mind szakmai fejlesztéssel. Az IRU nagy hangsúlyt fektet a preventív intézkedésekre is, az online tartalmak elemzésével és az online propaganda trendjeinek vizsgálatával segíti a tervezett merényletek megelőzését.

### **Összegzett következtetések**

A tanulmány a magányos elkövetők jelentette biztonsági kockázatra reflektál. A fentiek szerint a magányos terrortámadások valószínűsége nőtt Európában; a szélsőséges nézetek – mint a radikális bevándorlás-ellenesség vagy az iszlám fundamentalizmus – követői az interneten radikalizálódnak, illetve teremtenek kapcsolatot más szélsőségesekkel. A magányos elkövetők felderítése nehézségekbe ütközik két okból. Az új típusú, ún. rammingmerényletekhez nem szükséges speciális eszközök beszerzése, így az előkészületek gyakran rejtve maradnak, emellett a magányos elkövetők nem aktív tagjai terrorszervezeteknek, ezért nem kerülnek a hatóságok látókörébe.

A magányos elkövetők általában politikai indíttatásból követnek el támadást, tevékenységük ideológiai hátterét valamilyen radikális eszme adja. A merényletek mögött gyakran áll személyes sérelem vagy motiváció, így a célpontok kiválasztása személyes okokból történik. Habár a magányos elkövetőkkel kapcsolatban nem lehet egységes definíciót alkotni, általánosságban elmondható róluk, hogy valamilyen vélt vagy valós sérelem miatt radikalizálódtak. A hatóságok számára a radikalizálódási folyamat azonosítható a legkönnyebben, hiszen többségük az interneten tájékozódik: szélsőséges tartalmú honlapokon, illetve radikális csoportok közösségi oldalain. A fentiek miatt célszerű az ilyen típusú weboldalak figyelése, mivel a szélsőséges gondolatok azonosítása hozzájárulhat a tervezett merénylet felderítéséhez.<sup>35</sup>

A tanulmányban idézett kutatások szerint a tartalomelemzés segítségével azonosítani lehet azokat a radikális elemeket, melyek elvezethetik a hatóságokat a potenciális elkövetőkhöz. A kvantitatív szövegelemzés segítségével ki lehet szűrni azokat a hozzászólásokat, illetve bejegyzéseket, melyek fenyegető üzeneteket tartalmaznak. A kvantitatív tartalomelemző szoftverek nagy mennyiségű adatokat képesek kezelni rövid idő alatt, így akár fórumok, közösségi oldalak elemzésére is alkalmazhatók. A terrorelhárítás számára az ilyen típusú tartalomelemzés azért hasznos, mert segítségével azonosítani lehet azokat a személyeket, akikkel a felderítésnek és az értékelő-elemző egységeknek kiemelten foglalkozni kell.

---

<sup>35</sup> Id. Somogyi Ábel esetét, aki az ELTE jogi karán tanult, és egy blogoldalon 22 egyetemi társának megölésével fenyegetőzött. Az ő esetében a bíróság bizonyítottan látta a gyilkolási szándékot, így két és fél év börtönbüntetést kapott. Az esetről ld. Két és fél évet kapott S. Ábel, de most már tényleg. Index.hu., 2015.06.23. [http://index.hu/belfold/2015/06/23/s.abel\\_elte\\_lovoldozes\\_elokeszulet/#](http://index.hu/belfold/2015/06/23/s.abel_elte_lovoldozes_elokeszulet/#) (Letöltés ideje: 2017. 09. 15.)

A potenciálisan radikális személyek kiszűrése mellett a pszichológiai szempontú tartalomelemzés alkalmas arra is, hogy meghatározza azokat a lélektani aspektusokat, melyekre a hatóságoknak külön figyelmet kell fordítani a radikális személyek felderítése során. A szélsőséges személyek internetes tartalmainak elemzése, illetve tevékenységük folyamatos monitorozása lehetőséget ad arra, hogy egy esetleges merénylet már az előkészületi szakaszban lelepleződjön. A kvalitatív tartalomelemzés segítségével kevésbé objektív módon, de részletesebben fel lehet tárni a magányos farkasok szöveges tartalmai mögött húzódo rejtett pszichés elemeket. A tanulmány amellett érvel, hogy mind a kvantitatív, mind a kvalitatív tartalomelemző eljárások segíthetik a terrorelhárítás munkáját: az előbbi inkább a felderítés során, míg az utóbbi módszerek az elemző-értékelő munkát könnyíthetik meg.

#### ***Felhasznált irodalom:***

- ANTAL L.: A tartalomelemzés alapjai (Gyorsuló idő), Magvető Kiadó, 1976.
- Az Iszlám Állam magányos elkövetői célba vehetik Európát. frissujsag.ro, 2017.03.29. <http://www.frissujsag.ro/az-islam-allam-maganyos-elkovetoi-celba-vehetik-europat/> (Letöltés ideje: 2017. 09. 15.)
- BATES R. A.: Dancing with wolves. Today's lone wolf terrorists. The Journal of Public and Professional Sociology. Vol. 4. Is. 1., 2012., pp. 1-14.
- BERG B.: Qualitative research methods for the social sciences, Fourth edition. Allyn & Bacon, A Pearsons Education Company, Needham, Massachusetts, 2001.
- CHALOTRON T. – ELLMAN J. (2013): Affect analysis of radical contents on Web forums using SentiWordNet. International Journal of Innovation, Management and Technology, Vol. 4., No. 1., February 2013, pp. 122-124.
- „Én vagyok isten” Heteken belül gyilkolt volna S. Ábel. Hetek, 2010.02.19. Forrás: [http://www.hetek.hu/hatter/201002/en\\_vagyok\\_isten](http://www.hetek.hu/hatter/201002/en_vagyok_isten) (Letöltés ideje: 2017. 09. 15.)
- EU Internet Referral Unit–Year one report. Forrás (2017.10.21.): <https://www.europol.europa.eu/publications-documents/eu-internet-referral-unit-year-one-report-highlights>. (Letöltés ideje: 2017. 09. 15.)
- GERSTENFELD P. B. – GRANT D. R. – CHIANG C-P. (2003): Hate online: A content analysis of extremist internet sites. Analyses of Social Issues and Public Policy. Vol. 3., No. 1., 2003. pp. 29-44.
- GRINNEL D. – MACDONALD S. – MAIR D. (2017): The response of, and on, Twitter to the release of Dabiq Issue 15. Europol Public Information. 1st European Counter Terrorism Centre (ECTC) conference on online terrorist propaganda, 10-11 April 2017, at Europol Headquarters, The Hague.

- HANKISS Á.: „Égesd el őket!” Európai terror – A magányos elkövető legendája. Magyar Idők, 2017. július 1. Forrás (2017.12.07.): <http://magyaridok.hu/lugas/egesd-el-oket-1872439/> (Letöltés ideje: 2017. 09. 15.)
- HARGITAI R., NASZÓDI M., KIS B., NAGY L., BÓNA A., LÁSZLÓ J. (2005): A depresszív dinamika nyelvi jegyei az énelbeszélésekben. A LAS-Vertikum tagadás és szelf-referencia moduljai. Pszichológia, 2005. 2., pp. 181-199.
- Két és fél évet kapott S. Ábel, de most már tényleg. Index.hu., 2015.06.23. [http://index.hu/belfold/2015/06/23/s.abel\\_elte\\_lovoldozes\\_elokeszulet/#](http://index.hu/belfold/2015/06/23/s.abel_elte_lovoldozes_elokeszulet/#) (Letöltés ideje: 2017. 09. 15.)
- LÁSZLÓ J.: A tudományos narratív pszichológiai tartalomelemzés és a pszichológiai tartalomelemzés hagyományai. Pszichológia (2011), 31. évf., 1. szám, pp. 3-15.
- LÁSZLÓ J.: A narratív pszichológiai tartalomelemzés, Magyar Tudomány, 2005/11. p. 1366.
- MAYRING P.: Qualitative content analysis: theoretical foundation, basic procedures and software solution. Klagenfurt, Ausztria, 2014.
- MEHL M.R. – PENNEBAKER J.W. (2003): The social dynamics of a cultural upheaval: Social interactions surrounding September 11, 2001. Psychological Science, Vol. 14., Nr. 6., November 2003.
- PANTUCCI R. (2011): A typology of lone wolves: Preliminary analysis of lone islamist terrorists, International Centre for the Study of Radicalisation and Political Violence, London, March 2011.
- PENNEBAKER, J.W. – MEHL, M.R. – NIEDERHOFFER, K.G. (2003): Psychological aspects of natural language use: Our words, our selves. Annual Reviews Psychology, 2003., 54. pp. 547-577.
- PENNEBAKER, J. W. – BOYD, R. L. – JORDAN, K. – BLACKBURN, K. (2015). The development and psychometric properties of LIWC2015. Austin, TX: University of Texas at Austin.
- PERSAUD R. – BRUGGEN P.: Atrocity in the city of Nice: An act of clinical insanity? Psychology Today, 2016. július 18. Forrás (2017.10.21.): <https://www.psychologytoday.com/blog/slightly-blightly/201607/atrocity-in-the-city-nice-act-clinical-insanity> (Letöltés ideje: 2017. 09. 15.)
- REID E. (2009): Analysis of Jihadi Extremist Groups' Videos, Forensic Science Communications, 2009 július, Vol. 11., Nr. 3. Forrás (2013.10.11.): [http://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/july2009/index.htm/research\\_tech/2009\\_07\\_research01.htm](http://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/july2009/index.htm/research_tech/2009_07_research01.htm) (Letöltés ideje: 2017. 09. 15.)
- SMITH C. P.: Content analysis and narrative analysis. In REIS H. T., JUDD C. M.: Handbook of research methods in social and personality psychology. (313-335. old.) Cambridge University Press, New York, 2000.

- TÁLAS P. – SZENTE-VARGA M.: A 2017. augusztusi spanyolországi terrortámadásokról. 2017.08.21. SVKK, Elemzések 2017/18. Forrás (2017.12.07.): [http://archiv.netk.uni-nke.hu/uploads/media\\_items/svkk-elemzesek-2017-18-a-2017-augusztusi-spanyolorszagi-terrortamadasokrol-talas-p-szente-varga-m-1.original.pdf](http://archiv.netk.uni-nke.hu/uploads/media_items/svkk-elemzesek-2017-18-a-2017-augusztusi-spanyolorszagi-terrortamadasokrol-talas-p-szente-varga-m-1.original.pdf) (Letöltés ideje: 2017. 09. 15.)
- The internet organised crime threat assessment (iOCTA), European Police Office, 2014. Forrás (2017.12.12.): <https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017> (Letöltés ideje: 2017. 09. 15.)
- Üzent az Iszlám Állam: Tegyétek szenvedéssé a hitetleneknek a ramadánt. hirado.hu, 2016.05.22., <http://www.hirado.hu/2016/05/22/uzent-az-islam-allam-tegyetek-szenvedesse-a-hitetleneknek-a-ramadant/> (Letöltés ideje: 2017. 09. 15.)



DR. GYARAKI RÉKA

**A NYOMOZÓHATÓSÁG ÉS A KATASZTRÓFAVÉDELEM FELADATA A KIBERBŰNCSELEKMÉNYEK VONATKOZÁSÁBAN<sup>1</sup>**

---

**Bevezetés**

Az informatika fejlődése magával hozta a bűnözés megváltozását és a hagyományos bűnelkövetési módok mellett, vagy sok esetben azok helyett, az információs rendszerek felhasználásával elkövetett deliktumok szaporodtak el. Ezen bűncselekmények közvetlen célja már nem kizárólag az anyagi haszonszerzés, hanem az elektronikus rendszerekben tárolt adatok megszerzése, azok hozzáférhetetlenné tétele, az azokkal történő visszaélés és károkozás. Ezen célok akár külön-külön vagy együttes megvalósulása miatt lassan kezd elmosódni a határ a kiberbűnözés<sup>2</sup>, a kibertámadás és a kiberhadviselés között, akkor, amikor az információs rendszerben tárolt (szenzitív) adatok megszerzésével, azok mindenki számára megismerhetővé tételével már nemcsak egy deliktum valósul meg, hanem ezáltal idegen kormányoknak, szervezeteknek okozott kár, az irántuk lévő bizalom elvesztése, ellehetetlenítése, akár az alkotmányos rendszerbe vetett bizalom megrendítése a cél.

Ahogy a tanulmány címe is mutatja, azokat a szervezeteket kívánom bemutatni, amelyek feladataik szempontjából összefonódnak, ugyanakkor mégis az adott probléma felmerülése kapcsán más és más módszerrel történő végrehajtást vár el tőlük a jogalkotó és a felügyeleti szervük, a Belügyminisztérium. Ezen két hazai szervezet működését a hatáskör és illetékesség szempontjából úgy szeretném bemutatni, hogy kifejezetten az elektronikus információs rendszer elleni jogellenes cselekmény bekövetkezése esetén történő összefonódásukat és az együttműködésük szükségességét vizsgálom majd meg.

A két szervezet – a rendőrség és a BM Országos Katasztrófavédelmi Főigazgatóság (a továbbiakban: BM OKF) közötti, a kibertérben elkövetett jogellenes cselekményekre fókuszálva, többek között az elmúlt időszakban – így hazánkban is – bekövetkezett kibertámadások miatt fontosnak éreztem, hogy a szervezetek közötti együttműködést – különösen a jogszabályban meghatározott kötelezettségeiket és feladataikat – megvizsgáljam és a közös kapcsolódási pontokat megkeressem.

---

<sup>1</sup> A mű a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosítószámú, „A jó kormányzást megalapozó közszolgálat-fejlesztés” elnevezésű kiemelt projekt keretében működtetett *Ludovika Kiemelt Kutatóműhely* keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült.

<sup>2</sup> A kiberbűnözés, mint kifejezés ma már általánosan elfogadott fogalom. A külföldi szakirodalomban a cybercrime, cyberkriminalitát (német), la cybercriminalité (francia) használják. Magyarországon mind a KR NNI Kiberbűnözés elleni Főosztálya, mind pedig a Nemzeti Közszolgálati Egyetem Rendészettudományi Kar Kiberbűnözés elleni Tanszéke is ezt a kifejezést használja, ezért én is ennél a fogalomnál maradok a tanulmányban.

A tanulmányban végig kívánom vezetni, hogy:

1. a kiberbűncselekmény és a kibertámadás között milyen összefüggés van;
2. a kiberbűncselekmény elleni küzdelem során milyen feladata van a rendőrségnek valamint a BM OKF-nek;
3. a katasztrófavédelem szerepe és helyzete, valamint a katasztrófavédelmi szervek együttműködése más hatóságokkal.

A tanulmány első részében ismertetem azokat a feladatokat, amelyek a nyomozószervekre: a rendőrségre és az BM OKF hárul napjaink kiberfenyegetései miatt, majd pedig a két szerv közös feladatainak, illetve szükséges kapcsolódási pontjainak ismertetése következik a kibertámadások és kiberbűncselekmények megelőzése, felderítése és bekövetkezését követően a károk, veszélyek elhárítása, enyhítése vonatkozásában.

A szervezetek feladatainak ismertetése előtt szükséges annak meghatározása, hogy mit is értünk kiberbűncselekmény (cyber crime) alatt és milyen rendszer alapján lehet meghatározni a deliktumot, egyáltalán lehetséges-e egységes fogalomban meghatározni azt?

Az elmúlt időszakban végzett kutatások alapján három csoportba sorolom a kibercselekményeket:

1. Amikor a hagyományosnak nevezhető bűncselekményt az internet segítségével követik el. Ilyenek a különböző hirdetési, illetve aukciós oldalakon a nem létező vagy nem a meghirdetett minőségű termékek, szolgáltatások kínálása eladásra vagy bérletre. Ezáltal megvalósul a csalás vagy közokirathamisítás, piramisjáték szervezése stb, de akár az „okoseszközök” elterjedése révén a lopás vagy rablás bűncselekménye is megvalósul.
2. Amikor önmagát az információs rendszert használják fel deliktum elkövetésére, vagy az információs rendszerben tárolt adatok, illetve a rendszer integritását sértő vagy veszélyeztető jogellenes cselekménnyel valósul meg a bűncselekmény. Ilyenek az információs rendszer felhasználásával elkövetett csalás, az információs rendszerben tárolt adatok megsértése, felhasználása stb.
3. Amikor az elkövető jogellenes cselekménye támadást valósít meg úgy, hogy azok a kritikus infrastruktúrák információs rendszerei ellen irányulnak és amelyek sokszor találmányra, a leggyengébb védelemmel ellátott berendezések ellen történnek.

## **1. Fogalmi meghatározások**

### ***1.1. A (kiber)bűncselekmények***

A jog meghatározza, hogy mit is értünk bűncselekmény alatt. A hatályos Büntető Törvénykönyv<sup>3</sup> (Btk.) szerint az a szándékos vagy – ha a törvény a gondatlan elkövetést is bünteti – gondatlanságból elkövetett cselekmény, amely veszélyes a társadalomra, és amelyre a törvény büntetés kiszabását rendeli<sup>4</sup>.

---

<sup>3</sup> A Büntető Törvénykönyvről szóló 2012. évi C. törvény

<sup>4</sup> Btk. 4.§ (1) bekezdés

A Btk. valamennyi törvényi tényállást meghatároz, ugyanakkor az, hogy mit is ért számítástechnikai környezetben elkövetett bűncselekmény alatt, azt nem tette meg a jogalkotó. Persze felmerül a kérdés, hogy ennek van-e relevanciája?

Álláspontom szerint, bizonyos mértékig szükséges, hogy rendelkezzen, ha más nem, a nyomozóhatóság a felderíthetőség miatt egy olyan pontos fogalommal, ami a nyomozási taktika kiválasztását elősegíti.

Amennyiben megelégszünk azzal, hogy minden olyan jogellenes cselekmény, amelyben az elkövetés eszközeként információs rendszer szerepel, akkor szinte valamennyi bűnelkövető kiberbűnöző is egyben, hiszen majdnem mindenki rendelkezik valamilyen eszközzel, amelynek működése összefüggésben van az internettel.

A hazai jogi szabályozás a számítástechnikai bűncselekményeket a büntető kódexünkben nem egy fejezet alatt tárgyalja, hanem sok esetben a törvényi tényálláson belül, mint elkövetési magatartást emeli ki az információs rendszerben alkalmazott kifejezésekkel, illetve a törvény indoklásában utal a 2001-es Számítástechnikai Bűnözésről szóló Egyezményben vállalt kötelezettségünkre.

A kiberbűncselekmények kategóriái:

- I. „Klasszikus cybercrime”: adathalászat, kibertámadások, internetes csalások, on-line banking csalások
- II. Gyermek online szexuális kizsákmányolása: gyermekpornográfia, egyéb (szexuális zsarolás, beszerzés), nemi élet szabadsága és nemi erkölcs elleni bűncselekmények
- III. Bankkártyabűnözés

A kiberbűncselekmény fogalma valamennyi tényállásból és a fenti kategóriákból összegezve az alábbiak szerint határozható meg. Informatikai eszközök és/vagy rendszerek segítségével, vagy informatikai eszközök és hálózatok ellen elkövetett bűncselekmények, amelyek célja általában az anyagi haszonszerzés, továbbá kapcsolódó következménye a rendszerben tárolt adatok megszerzése, hozzáférhetővé tétele vagy éppen a jogosultak számára hozzáférhetetlenné tétele. Külön kategóriát képeznek azok a számítógéphez kapcsolódó bűncselekmények, amelyeket a törvény más tényállás alapján büntetni rendel, de ebben a részben azzal külön nem kívánok foglalkozni.

### **1.2. A kibertámadás**

A kibertámadás fogalmát egy HM utasítás határozza meg. Ez alapján kibertámadásnak minősül a kibertéren keresztül történő támadás, melynek célja egy információs környezet vagy infrastruktúra üzemelésének megszakítása, kikapcsolása, megsemmisítése, felügyeleti jogának megszerzése, a kezelt adat integritásának megsemmisítése, vagy a felügyelet alatt álló adat megszerzése<sup>5</sup>.

Ahogy az utasításból is kiolvasható, a kibertámadás valamilyen információs infrastruktúra elleni támadás, amelynek célja az abban tárolt adatok megszerzése, magának a rendszernek a megsemmisítése, kikapcsolása.

---

<sup>5</sup> A Magyar Honvédség Kibervédelmi Szakmai Koncepciójának kiadásáról szóló 60/2013. (IX. 30.) HM utasítás

A kiberbűncselekmények jellemzőit tekintve és az általam meghatározott fogalomból valamint a kibertámadás jogszabályi fogalmát kielemezve megállapítható, hogy a két jogellenes tevékenység összefügg, azok sok helyen kapcsolódnak.

Egy általam felállított tézis, miszerint minden kibertámadás bűncselekmény, ugyanakkor nem minden kiberbűncselekmény kibertámadás, a fentiek alapján megállja a helyét.

Kibertámadások fajtái<sup>6</sup>:

- illetéktelen hozzáférés az információkhoz,
- illetéktelen adatbevitel,
- rosszindulatú szoftverek bevitel,
- információk környezetszennyezés.

## **2. A rendvédelmi feladatokat ellátó szervezetek**

### **2.1. Rendőrség**

Magyarország közbiztonságáért, a rendvédelmi, bűnüldözési és bűnmegelőzési feladatok ellátásáért a belügyminiszter irányítása alá tartozó rendőrség felelős. A rendőrség feladatait elsősorban a Rendőrségről szóló 1994. évi XXXIV. törvény (Rtv.) szabályozza, de munkájuk során tekintettel kell lenniük a Büntetőeljárásról szóló 1998. évi XIX. törvényre (Be.), a Büntető Törvénykönyvről szóló 2012. évi C. törvényre (Btk.), illetve a rendőrség hatásköréről és illetékességéről szóló 25/2013. (VI. 24.) BM rendeletrre, amely a rendőrség szervezeti tagozódását hivatott szabályozni. Ezen jogszabályokon kívül a nyomozóhatóság a belügyminiszter irányítása alá tartozó nyomozó hatóságok nyomozásának részletes szabályairól és a nyomozási cselekmények jegyzőkönyv helyett más módon való rögzítésének szabályairól szóló 23/2003 (VI. 24.) BM-IM közös rendelet és további belső utasítások alapján látja el feladatait.

A rendőrség a feladatait az Alaptörvényben meghatározott jogok és kötelezettségek szem előtt tartása mellett végzi, mindeközben védi az állampolgárok biztonságát és a gondoskodik a törvények betartásáról és betartatásáról. A rendőrség feladata talán az egyik legösszetettebb, hiszen a bűnmegelőzési és bűnüldözési tevékenységen túl államigazgatási és rendészeti feladatkörrel is rendelkezik.

Minden büntetőeljárás megindításánál az első lépés a hatáskör és illetékesség vizsgálata, amely alapján az az arra jogosult szerv az elkövetés helye, jellege, az elkövetett kár mértéke alapján folytatja le a vizsgálatot. Az illetékesség kérdésében az elkövetés helyének megállapítása a fő szempont. Azaz az illetékesség alatt a földrajzi, területi meghatározást értjük. A 25/2013. (IV. 24.) BM rendelet 3. §-a alapján *a nyomozás lefolytatására az a nyomozó hatóság illetékes, amelynek illetékességi területén a bűncselekményt – sorozat-bűncselekmények esetén a bűncselekmények többségét – elkövették*. Amennyiben az elkövetés helye nem állapítható meg, vagy pedig a cselekmény jellegéből adódóan több hatóság lenne jogosult lefolytatni az eljárást, akkor a megelőzés elve érvényesül, vagyis ott fogják az ügyet kivizsgálni, ahol korábban intézkedtek.

---

<sup>6</sup> HAIG Zsolt – VÁRHEGYI István: Hadviselés az információs hadszíntéren, Zrínyi Kiadó Budapest 2005., p. 230.

Az illetékesség esetében megkülönböztettünk általános, kiemelt és kivételes illetékességet, aminek meghatározása fontos.

Általános illetékességű nyomozó hatóságok a rendőrkapitányságok, kiemelt illetékességű szervek a megyei rendőr-főkapitányságok, a Budapesti Rendőr-főkapitányság, valamint a Készenléti Rendőrség Nemzeti Nyomozó Iroda és a Repülőtéri Rendőr Igazgatóság.

A hatáskör és illetékesség kérdésével különösen szükséges a kibercselekmény esetében foglalkozni, mert vitatott, hogy a számítástechnikai környezetben elkövetett bűncselekmények esetében mi tekintendő az elkövetés helyének.

Első gondolatra sokakban az a válasz fogalmazódik meg, hogy ott követik el a kibercselekményeket, ahol maga az eszköz található. Ugyanakkor ma, amikor már az asztali számítógépek helyett laptopokat, tableteket és okostelefonokat használunk, amelyek mozgatható, helyváltoztatható egyszerű, már nem ennyire evidens a válasz. A határon átnyúló bűnözés joghatósági kérdéseire a nemzetközi jogban kereshetünk választ, hiszen a belső jogi szabályozás nem képes mindenre választ adni.

Létezik az illetékesség megállapítására olyan nézőpont<sup>7</sup> is, mely szerint az elkövetés helye ott van, ahol maga a kibertérben elkövetett jogellenes cselekmény ténylegesen megvalósul.

A fentiek értelmezése alapján azt gondolom, hogy a kibertér esetében – bár az nem egy egységesen meghatározott terület, tér – is megállapítható, hogy melyik nyomozószerv jogosult eljárni.

*A nyomozó hatóság a hatáskörét és az illetékességét hivatalból vizsgálja<sup>8</sup>, amennyiben valamelyik hiányát észleli, akkor átteszi a hatáskörrel és illetékességgel rendelkező nyomozó hatósághoz vagy ügyészhez<sup>9</sup>.*

## **2.2. Készenléti Rendőrség Nemzeti Nyomozóiroda (NNI)**

A 25/2013. (IV. 24.) BM rendelet 2. számú melléklete alapján a Készenléti Rendőrség Nemzeti Nyomozóiroda hatáskörébe tartoznak – a teljesség igénye nélkül – a következő számítástechnikai környezetben elkövetett bűncselekmények:

- a nemi élet szabadsága és a nemi erkölcs elleni bűncselekmények,
- nukleáris létesítmény üzemeltetésével visszaélés büntette<sup>10</sup>,
- atomenergia alkalmazásával visszaélés büntette<sup>11</sup>,
- az állam elleni bűncselekmények<sup>12</sup>,
- az igazságszolgáltatás elleni bűncselekmények<sup>13</sup>,
- háborús uszítás büntette<sup>14</sup>,

<sup>7</sup> A Magyar Kriminológiai Társaság Kriminológia és Bűnügyi Tudományok PhD szekció Konferenciája „Új kutatási területek a kriminológiában” című konferenciája 2016. október 14-én az ELTE ÁJK-n az Informatika és bűnözés szekció előadóinak vitaindító témája.

<sup>8</sup> A Rendőrség nyomozó hatóságainak hatásköréről és illetékességéről szóló 25/2013. (IV. 24.) BM rendelet 4.§ (1) bekezdése

<sup>9</sup> 25/2013 (IV.24) BM rendelet 4.§ (2) bekezdése

<sup>10</sup> Btk. 251.§

<sup>11</sup> Btk.252.§

<sup>12</sup> Btk. XXIV. fejezet

<sup>13</sup> Btk. XXVI. fejezet

- különösen jelentős kárt okozó csalás büntette, ha annak elkövetője a Btk. 459. § (1) bekezdés 1. pontjában meghatározott bűnszervezet vezetője vagy annak tagja<sup>15</sup>,
- különösen jelentős vagyoni hátrányt okozó gazdasági csalás büntette, ha annak elkövetője a Btk. 459. § (1) bekezdés 1. pontjában meghatározott bűnszervezet vezetője vagy annak tagja<sup>16</sup>,
- különösen jelentős kárt okozó információs rendszer felhasználásával elkövetett csalás, ha annak elkövetője a Btk. 459. § (1) bekezdés 1. pontjában meghatározott bűnszervezet vezetője vagy annak tagja<sup>17</sup>,
- pénzhamisítás előkészülete, ha az NNI kizárólagos hatáskörébe tartozó bűncselekmény elkövetésére irányul<sup>18</sup>,
- pénzmosás<sup>19</sup>,
- tiltott adatszerzés és az információs rendszer elleni bűncselekmények<sup>20</sup>,
- fedett nyomozó vagy a bűnüldöző hatósággal, illetve titkosszolgálattal titkosan együttműködő személy kilétének vagy tevékenységének megállapítása céljából elkövetett tiltott adatszerzés büntette<sup>21</sup>,
- közérdekű üzem ellen elkövetett információs rendszer vagy adat megsértése büntette<sup>22</sup>,
- közérdekű üzem ellen elkövetett információs rendszer védelmét biztosító technikai intézkedés kijátszásának vétsége<sup>23</sup>.

A Készenléti Rendőrség Nemzeti Nyomozó Iroda Kiberbűnözés Elleni Főosztály – 2017. január 01-je óta – három osztályra tagolódik. Az egyik osztály végzi a hatáskörükbe tartozó, vagy magukhoz vont bűncselekmények nyílt nyomozását – így a kihallgatásokat és a Be.-ben felsorolt eljárási cselekményeket. A másik osztály a kiberbűncselekmények felderítését végzi a Be., valamint az Rtv. alapján.

A harmadik osztály a Forenzikus Osztály, amely feladata nemcsak a szervezetükön belüli, hanem más, hazai rendőri szervnek történő szakértői tevékenység elvégzése, támogatása, valamint egyéb bűncselekmény során keletkezett adatok, evidenciák mentése, értékelése, elemzése úgy, hogy azok bizonyítékként felhasználhatóak legyenek a bírósági eljárásban.

Az NNI feladatait a fent említett BM rendelet alapján a következőkben lehet röviden meghatározni:

- büntetőeljárás lefolytatása,
- operatív felderítés,
- forenzikus tevékenység,
- OSINT jelentések, elemzések készítése,
- monitorozás,

<sup>14</sup> Btk. 331. §

<sup>15</sup> Btk. 373. § (6) bekezdés a) pont

<sup>16</sup> Btk. 374. § (6) bekezdés a) pont

<sup>17</sup> Btk. 375. § (4) bekezdés a) pont

<sup>18</sup> Btk. 389. § (3) bekezdés

<sup>19</sup> Btk. XL. fejezet

<sup>20</sup> Btk. XLIII. fejezet

<sup>21</sup> Btk. 422. § (2) bekezdés

<sup>22</sup> Btk. 423. § (3) bekezdés

<sup>23</sup> Btk. 424. §

- rendezvénybiztosítás,
- hazai együttműködés,
- nemzetközi együttműködés,
- szakirányítás, segítségnyújtás,
- a rendőri és igazságszolgáltatás egyéb területein dolgozók (ügyészek, bírók) oktatása.

### **2.3. Budapesti Rendőr-főkapitányság**

A Budapesti Rendőr-főkapitányság Korrupciós és Gazdasági Bűnözés Elleni Főosztály Pénzhamisítás és Csúcstechnológiai Bűnözés Elleni Osztály Csúcstechnológiai Bűnözés Elleni Alosztály foglalkozik a főváros területén elkövetett kiberbűncselekményekkel.

Az általános szabály szerint minden olyan deliktum esetében, amelynek tárgya vagy eszköze informatikai berendezés vagy információs rendszer, és amennyiben nem éri el az elkövetési érték az 50 millió forintot, vagy egyéb minősítő körülmény nem merül fel, úgy az illetékességgel rendelkező kerületi rendőrkapitányság jogosult eljárni Budapest területén elkövetett jogellenes cselekmények esetén.

### **2.4. Nemzeti Adó- és Vámhivatal (NAV)**

A Nemzeti Adó- és Vámhivatal feladatai a klasszikus adó- és illetékkiszabások mellett büntetőeljárások lefolytatása. A NAV Bűnügyi Főigazgatóság Központi Nyomozó Főosztály Informatiótechnológiai Osztály (NNI ITO) feladata a különböző informatikai eszköz felhasználásával elkövetett jogellenes cselekmény nyomozása. A Főigazgatóság hatáskörébe tartozik az egymilliárd forintot meghaladó értékre üzletszerűen, vagy bünszövetségben elkövetett bűncselekmények, a bűnszervezetben elkövetett bűncselekmények, valamint az olyan bűncselekmények nyomozása, amelyeket az elkövető személye, vagy az elkövetés körülményei, illetve a bűncselekmény társadalomra való veszélyességének kiemelkedő foka miatt a Bűnügyi Főigazgatóság hatáskörébe vont, illetve utalt bűncselekmények nyomozása. A NAV hatáskörébe a következő bűncselekmények nyomozása tartozik<sup>24</sup>:

- nemzetközi gazdasági tilalom megszegése (Btk. 327. §),
- nemzetközi gazdasági tilalom megszegése feljelentésének elmulasztása (Btk. 328. §),
- haditechnikai termékkel vagy szolgáltatással visszaélés (Btk. 329. §),
- kettős felhasználású termékkel visszaélés (Btk. 330. §),
- orgazdaság, ha vámellenőrzés alól elvont nem közösségi árura vagy jövedéki adózás alól elvont termékre követik el (Btk. 379. §),
- bitorlás (Btk. 384. §),
- szerzői vagy szerzői joghoz kapcsolódó jogok megsértése (Btk. 385. §),
- védelmet biztosító műszaki intézkedés kijátszása (Btk. 386. §),
- jogkezelési adat meghamisítása (Btk. 387. §),
- iparjogvédelmi jogok megsértése (Btk. 388. §),
- társadalombiztosítási, szociális vagy más jóléti juttatással visszaélés (Btk. 395. §),

<sup>24</sup> forrás: <https://www.nav.gov.hu/nav/bunugy/buncselekmenyek/buncselekmenyek.html>  
(Letöltés ideje: 2017. 06. 20.)

- költségvetési csalás (Btk. 396. §),
- költségvetési csaláshoz kapcsolódó felügyeleti vagy ellenőrzési kötelezettség elmulasztása (Btk. 397. §),
- jövedékkal visszaélés elősegítése (Btk. 398. §),
- számvitel rendjének megsértése (Btk. 403. §),
- csődbűncselekmény (Btk. 404. §),
- engedély nélküli nemzetközi kereskedelmi tevékenység (Btk. 406. §),
- versenytárs utánzása (Btk. 419. §),

továbbá a felsorolt bűncselekményekkel összefüggésben elkövetett:

- közokirat-hamisítás (Btk. 342-343. §),
- hamis magánokirat felhasználása (Btk. 345. §),
- egyedi azonosító jellel visszaélés (Btk. 347. §),
- bélyeghamisítás (Btk. 391. §),
- pénzmosás (Btk. 399-400. §),
- és a pénzmosással kapcsolatos bejelentési kötelezettség elmulasztása (Btk. 401. §).

Az említett bűncselekmények közül a hagyományos kiberbűncselekmény a szerzői vagy szerzői joghoz kapcsolódó jogok megsértésének bűncselekménye, amely csak 2011. január 01-je óta tartozik kizárólag a NAV hatáskörébe, azt megelőzően a rendőrség is hatáskörrel rendelkezett ezen deliktum nyomozásában. A szerzői vagy szerzői joghoz kapcsolódó jogok bűncselekménye során az NNI ITO feladata internetes monitorozás, azon belül a jogsértések feltárása, a jogsértés módjának meghatározása, továbbá az okozott vagyoni hátrány meghatározása, a jogsértő azonosítása, a Btk. 77. §-a alapján a jogsértő adat eltávolítására tett indítvány és annak ellenőrzése.

### 3. BM Országos Katasztrófavédelmi Főigazgatóság (BM OKF)

Magyarországon a BM OKF feladatát a köztudatban a tüzesetekre, a balesetek esetén történő mentésre, valamint az egyéb veszélyek elhárítására szűkítették. Pedig tevékenységük nemcsak a fizikai biztonságra, hanem a kibertérből érkező fenyegetések és támadások elhárítására és megelőzésére, a kritikus infrastruktúra (vagy ahogy a magyar jogi szabályozás is nevezi: létfontosságú rendszerelemek) védelmére, az iparbiztonságra is kiterjed.

A BM OKF feladatai miatt leginkább a Kibervédelmi Intézettel történő kapcsolattartást látja el, amelynek keretében a létfontosságú rendszerek elleni incidensek bejelentését, továbbá az aktív együttműködés egyéb formáit végzi.

A kritikus infrastruktúrák azonosításáról és kijelölésükről, illetve ezek védelmi fejlesztéseinek szükségességéről szóló 2008/114/EK tanácsi Irányelv 2008-ban jelent meg. Magyarországon a „Zöld Könyv”<sup>25</sup> megjelenése (2007) után 2010-ben kapott új lendületet a hazai létfontosságú rendszerek és létesítmények védelmével kapcsolatos szabályozások kidolgozása. A „Zöld Könyv” szerint *„az infrastruktúrák folyamatos működése, kockázati tényezőkkel szembeni ellenálló képességének növelése a lakosság, az infrastruktúra tulajdonosok, üzemeltetők, valamint a*

<sup>25</sup> „Zöld könyv”,

<http://digitalismagyarorszag.kormany.hu/download/f/35/e0000/Z%C3%B6ld%20K%C3%B6nyv.pdf>, (Letöltés ideje: 2017. 06. 20.)



*gazdaság szereplőinek és az állam számára egyaránt kiemelt fontossággal bír, a biztonságos működést elősegítő környezet és intézkedések ezért értéket képviselnek.*<sup>26</sup>

A kritikus infrastruktúrákkal kapcsolatosak a 2013. március 1. napján hatályba lépett létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvényben, valamint a hozzá kapcsolódó 65/2013. (III. 8.) általános végrehajtási kormányrendeletben meghatározott védelmi feladatok. A jogszabály célja egyrészt a létfontosságú rendszer elemek azonosítása, másrészt a kijelölés megtörténte után a megfelelő szintű – humán, fizikai és informatikai – védelem biztosítása

A létfontosságú rendszer elemek fogalma alatt a hazai jogi szabályozás az alábbi definíciót adja meg: *„a.....meghatározott ágazatok valamelyikébe tartozó eszköz, létesítmény vagy rendszer olyan rendszer elem, amely elengedhetetlen a létfontosságú társadalmi feladatok ellátásához – így különösen az egészségügyhöz, a lakosság személy- és vagyonbiztonságához, a gazdasági és szociális közszolgáltatások biztosításához –, és amelynek kiesése e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna”,<sup>27</sup> ...*

A létfontosságú rendszer elem védelmének meghatározása, ami többek között a BM OKF feladata: *„a létfontosságú rendszer elem funkciójának, folyamatos működésének és sértetlenségének biztosítását célzó, a fenyegetettség, a kockázat, a sebezhetőség enyhítésére vagy semlegesítésére irányuló valamennyi tevékenység.”<sup>28</sup>*

A BM OKF Országos Iparbiztonsági Főfelügyelőség tevékenységi körén belül kiemelt helyet foglal el a kritikus infrastruktúra védelmi szakterület, melynek egyik fő tevékenysége a jogalkotási és szabályozási feladatok végrehajtása.

A létfontosságú rendszer elemeket érő fenyegetések<sup>29</sup>:

- természeti csapások,
- műszaki/technikai hibák, zavarok, amelyek a működésük közben lépne fel,
- emberi mulasztások,
- terrorizmus,
- ipari kémkedés,
- szabotázs.

A fent felsoroltakon kívül, akár azokhoz kapcsolódóan, a kiberbűnözés, így a zsarolóvírusok, a kiberterrorizmus és a különböző hackertámadások, valamint a rendszereik nem megfelelő üzemeltetése, felügyelete, a belső szabályozás hiánya, illetve azok kijátszása is veszélyezteti a kritikus információs infrastruktúrát.

A BM OKF feladata többek között az, hogy koordinálja a kritikus infrastruktúrák védelmével kapcsolatos hálózatbiztonsági intézkedéseket, valamint végzi a hálózatbiztonsággal kapcsolatos események elemzését, és azok értékelését is.

<sup>26</sup> 1249/2010. (XI. 19.) Korm. határozat 1. melléklete – a nemzeti kritikus infrastruktúrák védelmének célja és alkalmazási köre

<sup>27</sup> A létfontosságú rendszer elemek védelméről szóló 2012. évi CLXVI. törvény (Lrtv.) – Értelmező rendelkezések 1. § f) pontja

<sup>28</sup> Lrtv. 1. § e) pontja

<sup>29</sup> [http://kok.katasztrofavedelem.hu/letoltes/document/document\\_218.pdf](http://kok.katasztrofavedelem.hu/letoltes/document/document_218.pdf) (Letöltés ideje: 2017. 06. 20.)

### **3.1. Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központ (LRLIBEK)**

A BM OKF szervezetén belül működő Létfontosságú Rendszerek és Létesítmények Informatikai Biztonsági Eseménykezelő Központja – az állam és önkormányzat által üzemeltetett létfontosságú rendszerek és létesítmények kivételével – ellátja a nemzeti létfontosságú rendszerek és létesítmények védelmével kapcsolatos hálózatbiztonsági tevékenységet.

Az LRLIBEK feladat- és hatáskörét a 185/2015. (VII. 13.) Korm. rendelet a kormányzati eseménykezelő központ és az eseménykezelő központok feladat- és hatásköréről, valamint a biztonsági események kezelésének, a biztonsági események műszaki vizsgálatának és a sérülékenységvizsgálat lefolytatásának szabályairól, továbbá az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról szóló 187/2015. (VII. 13.) Korm. rendelet szabályozza.

A Hatóság az eseménykezeléssel kapcsolatban – a vonatkozó szabályozás, de különösen a 2013. évi L. törvény (Ibtv.) alapján – a következő feladatokat látja el:

- a szervezetekkel való kapcsolattartás a bejelentett biztonsági események fogadására, valamint azok kezeléséhez szükséges intézkedések megtétele és koordinációja (20. § c.),
- a magyar kibertér rendszeres biztonsági helyzetértékelésének elvégzése (20. § d.),
- folyamatosan elérhető 24 órás ügyelet működtetése (20. § e.),
- a biztonsági események kivizsgálásának támogatása, amely során elvégezheti a biztonsági események adatainak műszaki vizsgálatát, amelyhez adatokat és az adatokhoz elektronikus hozzáférést kérhet (20. § f.),
- azonnali figyelmeztetések közzététele a kritikus hálózatbiztonsági fenyegetettségekről, ezek magyar nyelvű megjelenítése (20. § i.),
- hazai információbiztonsági és kibervédelmi gyakorlatokat tervezhet, szervezhet, gyakorlatokon vehet részt (20. § k.),
- nemzetközi információbiztonsági és kibervédelmi gyakorlatokat tervezhet, szervezhet, gyakorlatokon vehet részt (20. § l.),
- együttműködik a hatósággal, továbbá, szükség szerint, a biztonsági esemény kezelése tekintetében érintett szervezetekkel (20. § m.).

A fentiekén túl az eseménykezeléssel kapcsolatos feladataik a 185/2015. Korm. rendelet szerint:

- a tudomására jutott biztonsági eseményekről az érintettek haladéktalan értesítése (4. § a.),
- biztonsági eseményekről nyilvántartás vezetése (személyes adatokat nem tartalmaz, a megtett intézkedések és azok eredménye kerül rögzítésre) (4. § b.),
- az érintettek számára a biztonsági események kezelése során szakmai támogatás nyújtása (4. § c.),
- az elektronikus információs rendszereket veszélyeztető sérülékenységekkel és fenyegető kockázatokkal összefüggésben az üzemeltetők, a hatóságok és az eseménykezelő központok tájékoztatása (5. § (2) bek. b.),

- évente jelentés készítése a tevékenységéről az irányító miniszter részére (5. § (3) bek. c.),
- (nem kötelező érvényű) állásfoglalások, ajánlások kiadása (5. § (4) bek. a.),
- a biztonsági események kezelésére irányuló tájékoztató tartása (5. § (4) bek. b.),
- részvétel az információbiztonság tudatosításáért felelős intézmények tudatosítási programjában (5. § (4) bek. b.),
- szakértői-oktatói tevékenység végzése (5. § (4) bek. b.),
- információtechnológiai, hálózatbiztonsági, és biztonságiesemény-kezelési együttműködési fórum működtetése (5. § (4) bek. c.).

Az előzőekben felsorolt feladatokra figyelemmel a következőkben a tanulmány címében kiemelt két szervezet, azaz a rendőrség és a katasztrófavédelem kapcsolatát vizsgálom, amelyet leginkább a felsorolt feladataik alapján a kritikus infrastruktúrákat érő kibertámadásokban lehet a legjobban érzékeltetni.

Az 512/2013. (XII. 29.) Korm. rendelet alapján a BM OKF az egyes rendvédelmi szervek létfontosságú rendszerei és létesítményei azonosításáról, kijelöléséről és védelméről szóló jogszabály alapján a rendvédelmi szervek kijelölt infrastruktúrájának védelmével kapcsolatban lát el feladatokat, illetve kijelölő hatóságként jár el.

#### 4. További vonatkozó jogszabályok<sup>30</sup>

Az információs rendszerek elleni támadások fogalmánál már megjelenik annak értelmezése, hogy a kibercselekmények és a kibertámadások nem választhatók el egymástól, így ebben a fejezetben az egymással összekapcsolódó jogi szabályozást tekintem át, amelynek a legutolsó momentum a kibercselekményekre vonatkozó büntetőjogi tényállást tartalmazó Btk. rendelkezéseinek ismertetése.

A Btk. alapján három tényállást vizsgáltam meg:

- a 323. §: a közérdekű üzem működésének megzavarása,
- a 314-316. §: terrorcselekmény és
- a 424. §: az információs rendszer védelmét biztosító technikai intézkedés kijátszása.

##### ***Közérdekű üzem működésének megzavarása***

*323. § (1) Aki közérdekű üzem működését jelentős mértékben megzavarja, büntetett miatt egy évtől öt évig terjedő szabadságvesztéssel büntetendő.*

A közmű meghatározása: olyan termelő, vagy szolgáltató üzemek, amelyek a lakosság, továbbá az ipar, a mezőgazdaság, a szolgáltató tevékenység kiterjedt körét vízzel, elektromos, gáz-, gőz-, vagy hőenergiával látja el<sup>31</sup>. Továbbá a közösségi közlekedési üzem, amely a tömeges közlekedés lebonyolítására alkalmas, a használok széles köre által igénybe vehető közlekedési eszközök üzeme. A

<sup>30</sup> Kizárólag a rendőrség hatáskörébe tartozó bűncselekményekkel foglalkozom, így a Nemzeti Adó-és Vámhivatalt érintő deliktumok ebben a tanulmányban nem szerepelnek. A továbbiakban ezért kizárólag a Rendőrség fogalma szerepel.

<sup>31</sup> KERESZTY Béla – MARÁZ Vilmosné – NAGY Ferenc – VIDA Mihály: A magyar büntetőjog különös része, Korona Kiadó, Budapest, 2004. p. 457.

tényállást kell alkalmazni az elektronikus hírközlő hálózatokra is, továbbá az egyetemes postai szolgáltató közérdekű feladatainak teljesítése érdekében üzemeltetett logisztikai, pénzforgalmi és informatikai központok és üzemekre is.

A bűncselekményt nyitott törvényi tényállásnak lehet nevezni, hiszen a törvényalkotó nem határozza meg benne az elkövetési magatartást, így elkövethető szándékosan, tévessel vagy éppen mulasztással is. A deliktum a fent felsorolt közműhálózatba okozott bármilyen zavarral már bekövetkezett az eredmény. A bűncselekmény elkövetője tettesként bárki lehet.

### ***Terrorcselekmény***

**314. § (1)** *Aki abból a célból, hogy*

*a) állami szervet, más államot vagy nemzetközi szervezetet arra kényszerítsen, hogy valamit tegyen, ne tegyen vagy eltűnjön,*

*b) a lakosságot megfélemlítse,*

*c) más állam alkotmányos, társadalmi vagy gazdasági rendjét megváltoztassa vagy megzavarja, illetve nemzetközi szervezet működését megzavarja,*

*a (4) bekezdésben meghatározott személy elleni erőszakos, közveszélyt okozó vagy fegyverrel kapcsolatos bűncselekményt követ el, ...*

*(2) Az (1) bekezdés szerint büntetendő, aki az a) pontban meghatározott célból*

*a) jelentős anyagi javakat kerít hatalmába, és azok sértetlenül hagyását vagy visszaadását állami szervhez vagy nemzetközi szervezethez intézett követelés teljesítésétől teszi függővé, vagy*

*b) terrorista csoportot szervez.*

...

*(4) E § alkalmazásában személy elleni erőszakos, közveszélyt okozó vagy fegyverrel kapcsolatos bűncselekmény*

...

*c) a közlekedés biztonsága elleni bűncselekmény [232. § (1)-(2) bekezdés], a vasúti, légi vagy vízi közlekedés veszélyeztetése [233. § (1)-(2) bekezdés],*

*d) a radioaktív anyaggal visszaélés [250. § (1)-(2) bekezdés],*

*f) a jármű hatalomba kerítése [320. § (1)-(2) bekezdés], a közveszély okozása [322. § (1)-(3) bekezdés], a közérdekű üzem működésének megzavarása [323. § (1)-(3) bekezdés], a robbanóanyaggal vagy robbantószerrel visszaélés [324. § (1)-(2) bekezdés], a lőfegyverrel vagy lőszerrel visszaélés [325. § (1)-(3) bekezdés],*

*g) a nemzetközi szerződés által tiltott fegyverrel visszaélés [326. § (1)-(5) bekezdés], a haditechnikai termékkel vagy szolgáltatással visszaélés [329. § (1)-(3) bekezdés], a kettős felhasználású termékkel visszaélés [330. § (1)-(2) bekezdés],*

*h) a rablás és a rongálás,*

*i) az információs rendszer vagy adat megsértése*

**315. § (1)** *Aki a 314. § (1) vagy (2) bekezdésében meghatározott büntett elkövetésére felhív, ajánlkozik, vállalkozik, a közös elkövetésben megállapodik, vagy az elkövetés elősegítése céljából az ehhez szükséges vagy ezt könnyítő feltételeket biztosítja...*<sup>32</sup>

---

<sup>32</sup> net.jogtar.hu

A terrorcselekmény jogi tárgya az állami szervek, más államok, a nemzetközi szervezetek zavartalan, kényszertől mentes működéséhez, a lakosság megfélemlítéstől mentes életviteléhez fűződő társadalmi érdek.<sup>33</sup>

Az elkövetési magatartás a tényállás alapján a tűrésre kötelezés, megfélemlítés, alkotmányos rend megváltoztatása, nemzetközi szervezet működésének megzavarása, anyagi javak hatalomba kerítése és azok sértetlenül hagyását vagy visszaadását állami szervhez vagy nemzetközi szervezethez intézett követelés teljesítésétől teszi függővé<sup>34</sup>. A szakirodalom ennél a bűncselekménynél meghatároz egy cél-, illetve eszközcselekményt is. Az eszközcselekménye a jelentős anyagi javak hatalomba kerítése, amely nem feltétlenül jelenti a jogellenes birtokbavételt és a rendelkezési jog gyakorlását. A kibertérből érkező fenyegetések<sup>35</sup> – értve ezalatt a zsarolóvírus kritikus információs infrastruktúrához történő eljuttatását – már teljes mértékben kimeríti a terrorcselekmény fogalmát. Mivel a törvény az előkészületet is bünteti, így már akkor önmagában csak azzal elköveti valaki a cselekményt, hogy akár egy adott Kibervédelmi Intézet információs rendszerének sérülékenységét ismerve, arra célzottan elkészíti a programvírust, de ugyanúgy az is elköveti a jogellenes cselekményt, aki – bár nem tudva a sérülékenységekről – az általa megírt rosszindulatú programot megír, ami egy adott, létfontosságú rendszer elem működését veszélyezteti, vagy abban zavart okoz.

## 5. Összegzés

A BM OKF hatósági jogkörében eljárva ellenőrzi a biztonsági szintekre vonatkozó követelmények teljesülését,<sup>36</sup> ellenőrzését, kockázatelemzését és kivizsgálja a különböző biztonsági eseményekkel kapcsolatos bejelentéseket, ennek megfelelően együttműködik a hatóságokkal (többek között az Eseménykezelő Központtal, amely felé az incidenst jelenti).

Egy bekövetkezett támadás esetén – szükséges mértékben – mindkét szervezetnek van feladata.

A kritikus információs infrastruktúrák működésével kapcsolatos szabályozás, biztonsági szintjének besorolása, az annak kezelésére jogosult személyek kijelölése stb. a BM OKF hatáskörébe tartozik. Éppen ezért egy információs rendszert érő támadás – súlyos biztonsági esemény bekövetkezése<sup>37</sup> – vagy akár „csak” annak kísérlete esetén az ő feladatuk többek között a további hatóságok – így a GovCert, Alkotmányvédelmi Hivatal, Rendőrség – értesítése és a szükséges intézkedés és tájékoztatás megtétele.

---

<sup>33</sup> BLASKÓ Béla– HAUTZINGER Zoltán– MADAI Sándor – PALLAGI Anikó – POLT Péter – SCHUBAUER László: Büntetőjog különös rész II. Rejtjel Kiadó, Budapest 2015. p. 16.

<sup>34</sup> Btk. 314.§ (1) és (2) bekezdés

<sup>35</sup> Az Ibtv 1. § 16. pontja meghatározza, hogy mit is jelent a fenyegetés: olyan lehetséges művelet vagy esemény, amely sértheti az elektronikus információs rendszer vagy az elektronikus információs rendszer elemi védetségét, biztonságát, továbbá olyan mulasztásos cselekmény, amely sértheti az elektronikus információs rendszer védetségét, biztonságát.

<sup>36</sup> Ibtv. 9. § (1) bek.: A kockázatokkal arányos, költséghatékony védelem kialakítása érdekében a szervezetet az elektronikus információs rendszerek védelmére való felkészültsége alapján a szervezetnek biztonsági szintekbe kell sorolni a jogszabályban meghatározott szempontok szerint.

<sup>37</sup> Ibtv. 1. § 41/a. pontja

Súlyos biztonsági esemény „*olyan informatikai esemény, amely bekövetkezése esetén az állami működés szempontjából kritikus adat bizalmassága, sértetlensége vagy rendelkezésre állása sérülhet, emberi életek kerülhetnek közvetlen veszélybe, személyi sérülések nagy számban következhetnek be, súlyos bizalomvesztés következhet be az állammal vagy az érintett szervezettel szemben, alapvető emberi, vagy a társadalom működése szempontjából kiemelt jogok sérülhetnek.*”

Mivel az említett két bűncselekmény nyomozása (is), a további bűncselekmények megakadályozása, az elkövető kézre kerítése a rendőrség, ezen belül a hatáskörre vonatkozó utasítás alapján a Készenléti Rendőrség Nemzeti Nyomozóiroda hatáskörébe tartozik, így azok bekövetkezése esetén a rendszer működéséről, a kialakult veszélyhelyzetről a legteljesebb információval ők rendelkeznek.

### **5.1. Egyéb közös feladatok elvégzése**

Egy bekövetkezett kibertámadás során a létfontosságú rendszerelemek információs rendszereiben keletkezett problémák befolyással lehetnek az adott rendszer elem más területére, például a berendezések funkciójára. Egy ilyen súlyos biztonsági esemény veszélyezteti az érintett kritikus infrastruktúra működésének folytonosságát, amely katasztrófához vezethetne.

A támadás következtében bekövetkezett zavar elhárítása ugyanakkor nem kizárólag a Katasztrófavédelem feladata. A lakosság létfenntartását, egészségét, biztonságát szolgáló ideiglenes intézkedések és cselekvések – így akár a vízművek elleni támadás, amely következtében nincs, vagy nem megfelelő az ivóvízellátás, a napi adag pótlásának eljuttatása – mind a katasztrófavédelem, mind a rendőrség, mind pedig a honvédelem feladata.

### **Felhasznált irodalom:**

- HAIG Zsolt – VÁRHEGYI István: Hadviselés az információs hadszíntéren, Zrínyi Kiadó Budapest 2005.
- KERESZTY Béla – MARÁZ Vilmosné – NAGY Ferenc – VIDA Mihály: A magyar büntetőjog különös része, Korona Kiadó, Budapest, 2004.
- BLASKÓ Béla– HAUZINGER Zoltán– MADAI Sándor – PALLAGI Anikó – POLT Péter – SCHUBAUER László: Büntetőjog különös rész II. Rejtjel Kiadó, Budapest 2015.
- <https://www.nav.gov.hu/nav/bunugy/buncselekmenyek/buncselekmenyek.html> (Letöltés ideje: 2017. 06. 20.)
- [http://kok.katasztrofavedelem.hu/letoltes/document/document\\_218.pdf](http://kok.katasztrofavedelem.hu/letoltes/document/document_218.pdf) (Letöltés ideje: 2017. 06. 20.)
- <http://digitalismagyarorszag.kormany.hu/download/f/35/e0000/Z%C3%B6ld%20K%C3%B6nyv.pdf>, (Letöltés ideje: 2017. 06. 20.)

***Felhasznált jogszabályok:***

- A Büntető Törvénykönyvről szóló 2012. évi C. törvény
- A büntetőeljárásról szóló 1998. évi XIX. törvény törvény
- Az állami és az önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény
- A létfontosságú rendszerelemek védelméről szóló 2012. évi CLXVI. törvény
- 25/2013. (IV. 24.) BM rendelet a Rendőrség nyomozó hatóságainak hatásköréről és illetékességéről
- 60/2013 (IX. 30.) HM utasítás a Magyar Honvédség Kibervédelmi Szakmai Konceptiójának Kiadásáról

**AZ ATHÉNI ÁLLAM A TIZENNEGYEDIK ALKOTMÁNYMÓDOSÍTÁS  
UTÁN<sup>1</sup>**

---

*„A vizsgálódás nélküli élet  
nem emberhez méltó élet”<sup>2</sup>*

**Előzetes megfontolások**

Az állam autoritásának normatív megjelenési formája a jogi norma. A jogi norma alkalmazása pedig az állam autoritásának érvényesülési módja, az állam egy működési formája. Amikor a jogról beszélünk, az államról is szólnunk, de más olvasatban, más horizonton. Az athéni állam a peloponnészoszi háborúban elszenvedett vereséggel és az utána következő „közjátékkal” Arisztotelész tanúsága szerint a tizenegyedik alkotmánymódosítással jutott el abba az állapotába, amely a szövegtörzshöz keletkezése idején is érvényes és hatályos. Ez az alkotmány maradt érvényben Róma hódításáig. Arisztotelész így ír az alkotmányreform sorozatról: „XLI. Ezek a dolgok már a későbbi időkben történtek, a nép viszont, amint a helyzet ura lett, megteremtette a most is meglévő alkotmányt, Pythodoros archósága idején... a nép pedig jogosnak látta, hogy a maga vegye kezébe a kormányzást azon az alapon, hogy a maga erejéből valósította meg a visszatérést. Ez volt az átalakulások sorában szám szerint a tizenegyedik. Az első átalakulást az ősi dolgokhoz képest Ión és a vele lévők letelepedése jelentette. Akkor oszlottak ugyanis először együttesen négy phylére és állították a phylobasileusokat. A második, s ezután az első olyan, amelynek alkotmányos jellege volt, az, mely Thészeus alatt következett be, s mely egy kissé eltért a királyságtól. Ezután a Drakón alatti, amelyben először foglalták írásba a törvényeket. A harmadik a pártharcok utáni, Solón alatt létrejött átalakulás, ezzel vette kezdetét a demokrácia. A negyedik Peisistratos tyrannisa. Az ötödik a tyrannosok bukása után Kleisthenés alkotmánya, amely Solónénál demokratikusabb volt. A hatodik a perzsa háborúk utáni, amikor az Areiospagos tanácsa állott az élen. A hetedik az ez után következő, amely felé Aristeidész mutatott és amit Ephialtés valósított meg azzal, hogy feloszlatta az Areopagiták tanácsát. Ekkor történt, hogy a város a legtöbb hibát követte el a népvézerek miatt a tengeri hatalom birtokában. A nyolcadik volt a négyszázak hatalomba helyezése, és az ez utáni, a kilencedik pedig ismét a demokrácia. A tizedik a harmincak és a tízek kényuralma. A tizenegyedik a Phyléből és Peiraieusból való hazatérése utáni rend, amely azóta is érvényben van mind mostanig, s amely szüntelen gyarapítja a tömeg hatalmát. A nép ugyanis mindenek urává magamagát

---

<sup>1</sup> Az írás Az államelmélet alapkérdései II konferencián (NKA Államtudományi és Közigazgatási Kar 2017. november 22-23.) elhangzott előadás tanulmányformára szerkesztett változata. A tanulmány a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosító számú, A jó kormányzást megalapozó közszolgálat-fejlesztés című kiemelt projekt Ludovika Kiemelt Kutatóműhely Programjának Államelméleti alap kutatás 2016-2018 (2016/86 NKE-AKFI) elnevezésű alprogramjának keretében a Nemzeti Közszolgálati Egyetem megbízásából készült.

<sup>2</sup> PLATÓN: Szókratész védőbeszéde. In Platón: Euthüphrón, Szókratész védőbeszéde, Kritón. Fordította a jegyzeteket és a kommentárt írta GELENCZEY-MIHÁLTZ Alirán (Kritón) és MOGYORÓDI Emese (Euthüphrón, Szókratész védőbeszéde). In Platón összes művei kommentárokkal. Budapest, 2005, Atlantisz, 38a7-8. pp. 103-104.



tette meg, és mindent szavazások és törvényszékek útján intéz, márpedig itt a nép az úr, minthogy a tanács jogkörébe tartozó ítélezések is a népre szállottak át.”<sup>3</sup>

Témám szempontjából fontos, hogy az alkotmányozás nem egyszeri aktus volt, hanem egy elhúzódó folyamat, amely feltételezhetően Szókratész perének idejére fejeződött be, annak minden vonatkozásával. Szókratész perének rekonstrukciója interdiszciplináris megközelítést igényel. A kutatási folyamatot egy úgynevezett „elmetérképen” rögzítem, amelynek lényege, hogy a kapcsolódási vonalak és pontok, ágak jól láthatóak és vizuálisan is jelzik a munkám állapotát, irányát és következő szükséges lépéseket is.<sup>4</sup> Az interdiszciplináris megközelítéshez külön módszertani eljárást dolgoztam ki, amelyet a „síkok módszerének” nevezek. A módszer lényege, hogy az „elmetérképen” rögzített információkat tudományterületek, ezen belül információ-csoportok szerint rendezem, amely, mint rendszerelemek, a gondolatilag konstruált térben analitikus síkokat jelölnek ki. A síkok egymásra vonatkoztatásából, illetve kapcsolódásaiból jön létre a probléma megoldására szolgáló elméleti hipotézis.

### **A vizsgált alkotmányreform szervezési elvei**

Úgy tűnik, hogy a tizenegyedik alkotmányreform több elvet és eljárást követett. Az így feltárt elvek között szűkítést alkalmaztam és azokat emeltem ki, amelyek az *aszbeia* bűncselekményével nehézség nélkül kapcsolatba hozhatók és vonatkoztathatók Szókratész perére. Ez a két szempont, mint tükrözési tengely is értelmezhető, ha matematikai szempontot alkalmazok a módszer kidolgozásánál. Az alkotmányreform során az általam vizsgált területen hat konstitutív, a szabályozás tartalmait is meghatározó elv érvényesült. Az elvek az államellenes bűncselekmények vonatkozásában kapcsolódtak az *aszbeia* cselekmény-együtteshez és esetköréhez. Ezt azért kell hangsúlyozni, mivel az *aszbeia* törvényi tényállására nem található pontos leírások, de Szókratész i.e. 399. évben megtörtént perének rekonstrukciója fontos felismerésekkel szolgál a kutatás számára, s egyúttal bővíti az *aszbeia* esetkörét is. Az alkotmányreform szervezési elvei a következők sorjában kifejtve az alábbiak:

#### ***Amnesztia***

A felejtés elve. A politika- és jogtörténetben ezt a törvényt szokás Európa első amnesztiatörvényének nevezni. Ennek azonban már volt előzménye Szólón alkotmányreformja idején, mivel a közkegyelem és az amnesztia fogalmai még nem válnak el élesen. Szólón „Először közkegyelmet hirdetett: a gyilkosok és a hazaárulók kivételével minden athéni polgár hazatérhetett”.<sup>5</sup> Lehet, hogy nem volt olyan sok embert érintő, mint a tizenegyedik alkotmányreform során meghozott törvény, de legalább ennyire meghatározó volt, és a *szeiszakhteia* (teherlerázás) együttes alkalmazásával legalább ennyire jelentős, és szintén átformálta egy korszak politikai és jogi felfogását. A felejtés elvének, mint az i. e. 403. évi amnesztia-

<sup>3</sup> ARISZTOTELÉSZ: Az athéni állam. Pseudo-Xenophón: Az athéni állam. Ford. RITOÓK Zsigmond. A bevezetést írta SARKADY János. Budapest, 1954, Akadémiai Kiadó, XVII. 1., 2., 4. LVII.2- 4. pp. 115 – 117.

<sup>4</sup> Vö. LACZÓ József: Az athéni állam és Szókratész pere. Budapest, 2017, Kézirat.

<sup>5</sup> HORVÁTH Pál (szerk.): Egyetemes jogtörténet. Budapest, 2005, Nemzeti Tankönyvkiadó, p. 48.

törvénynek, több pragmatikus indoka volt az állam szempontjából. A hivatalnokokra, hivatalokra és a bíróságokra nehezedő ilyen mennyiségű ügyterhet e törvény nélkül nem lehetett volna törvényesen, racionálisan és békeséget teremtő módon rendezni. Függetlenül attól, hogy már Drakón korlátozta a vérbosszú intézményét a szándékos emberölés esetére,<sup>6</sup> a folyamatot nem lehetett volna kezelni és mederben tartani, mert minden családnak volt sérelme és polgárháborús elszámolni valója. A „felejtés” hiányában a „mindenki harca mindenki ellen” állapota vált volna tartóssá, és ez, mint tudjuk, újra és újra megsemmisítette volna az államrendet. Ekkor ugyanis még érvényben volt az a Szólón alkotta törvény,<sup>7</sup> hogy aki belharc esetén nem áll egyik párt mellé sem, az bárki kerül hatalomra, felelősségre vonja. Ebben álláspontom szerint sokan érintettek lehettek, de Szókratész mindenképpen, mint azt Platón szövegekörpuszából levezethetjük. Szókratész azt állítja, hogy „sem a népgyűlés ügyeire, vagy egyáltalán a városbeli tisztségekre, politikai szervezkedésekre” nem gyakorolt hatást, „mert úgy ítélt meg, valójában tisztességesebb vagyok, semhogy életben maradhassak, ha erre az útra térek”.<sup>8</sup>

### *A jogrendszer revíziója*

A jogrendszer revíziója esetében lényegében a Kleiszthenész és Ephialtész által intézményesített mérsékelt demokráciája *restitúciója* volt a kitűzött cél. A vizsgált terület, amely az *aszabeia* és Szókratész pere szempontjából érdekessé teszi a revízió elvét, az összes *pszefizma* (néphatározat) hatályon kívül helyezését jelentette. Többek között a Diopethész a jós által javasolt és a nevét viselő *pszefizma* hatályon kívül helyezése jelentette a kiemelt momentumot. Mogyoródi Emese szerint „kiemelendő, hogy Plutarkhosznál (Párhuzamos életrajzok, Periklész 32.) fennmaradt az utalás egy Diopethész jós által beterjesztett népgyűlési határozatra, amely szerint Athénban fel kellett jelenteni azokat, „akik nem gyakorolják a vallást, nem hisznek istenekben, vagy égi jelenségekről szóló tanokat hirdetnek” (*ta theia mé nomizontasz é logusz peri tón metarszión poiuntasz*), amely Anaxagorasz személyén keresztül Periklész ellen irányult volna. Ezt a népgyűlési határozatot azonban a legkésőbb a demokrata hatalomváltást követő amnesztia idején (Kr. e. 403) érvénytelenítették, tehát efféléért senkit nem lehetett törvényesen bevádolni”.<sup>9</sup> Eszerint az *aszabeia* bűncselekménye a közvélekedésen, a bírák esküjén és meggyőződésén alapult, azaz feltételezésem szerint előítéletes szerkezetű volt. Ehhez tekintetbe kell venni két dolgot. Egyfelől azt a tendenciát, hogy Athénban a vallás per se közügynek, azaz politikainak számított, így feltételezhető, hogy az *aszabeia*-vádak mögött általában politikai koncepciók állnak. Másfelől azt a tényt, hogy Szókratész perének tárgyalását megelőző napon volt a Déloszba induló hajó „felkoszorúzása” és kultikus ünnepe beszédekkel. Ehhez tudni kell, hogy az ünnepséget és Szókratész *anakriszisz* eljárását és tárgyalását is az *arkhón baszileosz* vezette. „Platón szerint (6) Apollón papja a tárgyalás előtti napon koszorúzta meg hivatalosan az útra (ettől az időponttól számított a kivégzési tilalom) és 30 nap

---

<sup>6</sup> I. m. uo.

<sup>7</sup> I. m. uo.

<sup>8</sup> Platón: Szókratész védőbeszéde. 36 c.

<sup>9</sup> MOGYORÓDI Emese Szókratész védőbeszédéhez fűzött 40. lábjegyzete. I. m. pp. 71-72.

múlva tért vissza.”<sup>10</sup> Az a tény, hogy Szókratész tárgyalását megelőző napon ilyen vallási-politikai esemény történt, nem a jóindulatról árulkodik, hanem arról, hogy a vád előzetes politikai koncepción alapult. Az ítélkező testület esküdtbíróság jellegéből következően ennek fontos szerepe volt, hiszen a bírák az előítéletes közegből kerültek véletlenszerűen kiválasztásra, döntésük előtt pedig egymással nem konzultáltak.

### *A vallás hangsúlyainak megváltozása*

A vallás hangsúlyainak megváltozása nem csak a vallási átélés elmélyülését jelenti, amely által a társas lélek számára lehetővé válik a politikai kudarcból következő trauma feldolgozása. A hangsúly megváltozása irányváltást jelentett a kultuszban, amely Apollón felé tolódott el. Feltételezésem szerint az athéni polgárok, bár nem kifejezetten, de elégedetlenek voltak Pallaszt Athénével, aki mint a várost oltalmazó istenség „nem adott elégséges védelmet” a spártaiak és szövetségesei ellen viselt háborúban. Ebben a vonatkozásban Thészeusz hajóján Délosz-szigetére menni, azaz szakrális ünnep keretében Apollón születési helyére utazni, komoly konfliktust jelentett a bevett közösségi kultusszal és annak értelmezésével, szakralitásával. Ez feltételezhetően igaz Szókratészre is, aki a Védőbeszédben hivatkozott jóslat alapján egyedi és bensőséges viszonyt képzelt Apollón istennel. Ám ezt a viszonyt olyan módon és összefüggésben értelmezte, ami szemben állhatott a közösségi felfogással, amelyet az athéniak hivatalosnak és elfogadottnak tekintettek. Hasonló konfliktust mutat az athéni állam elemzése a közösségi és az egyéni nevelés gyakorlata között. Ebben a vonatkozásban elegendő Platón Menón című dialógusából felidézni Szókratész és Anütosz vitáját: „XXXV. Szókratész: Nicsak Menónom, úgy látszik Anütosz felhúzta magát! Nem csoda, ha egyszer azt hiszi, hogy valami rosszat mondtam ezekről az emberekről, aztán saját magáról meg azt képzelem, hogy ő is közéjük tartozik.”<sup>11</sup> Ez az elv a szofistákkal szemben alkalmazott eljárást is bevezeti.

### *A szofisták kiűzése*

A szofisták kiűzése az alkotmányreform előtt, második generációjuk kiszorítása és korlátozása a közéletben Szókratészt is érintette. A konfliktusban a közösségi nevelés és az egyéni nevelés módjai közötti törésvonal fejeződött ki. Az alkotmányreform során a szofistákat mindenképpen korlátozni kívánták, nemcsak a nevelés vonatkozásában, hanem más területeken is. Ráadásul a szofisták szolgáltatásait csak a tehetősek, legfőképpen az arisztokraták fizethették meg, így emiatt sem voltak kívánatosak a továbbiakban. Szókratész a nevelés területén, mintegy „szofista pótlékot” jelenthetett a hatalom szemében. Másfelől a közvélekedés szerint Szókratész maga is szofista volt, mint második generációs tanítványra tekintettek rá. A nevelésnek pedig az a formája, amelyet képviselt az erény tanítása vonatkozásában mindenképpen szemben állt a közösségi nevelés eszméjével és gyakorlatával. In *Platón összes művei kommentárokkal*. Az athéni

---

<sup>10</sup> HORVÁTH Barna: A génusz pere Szókratész – Johanna. Máriabesnyő – Gödöllő, 2003, Attraktor Kiadó, 13. A felkoszorúzási ünnepséget illetően lásd Platón: Phaidón. 95 a3. 88.58a.

<sup>11</sup> PLATÓN: Menón. In Platón összes művei kommentárokkal. Fordította, a jegyzeteket és az utószót írta BÁRÁNY István. Budapest, 2013, Atlantisz, 95 a3. p. 88.

átlagpolgár számára agresszívként megjelenő, irritációkat keltő módszere, az *elenkhosz* pedig kifejezetten ellenségeket szerzett számára.

### ***Az arisztokraták politikai tevékenységének korlátozása***

Alkotmányreform során követett alapvető elv volt az arisztokraták politikai tevékenységének korlátozása. Szókratész vonatkozásában a szofista tevékenység és az arisztokrata restauráció lehetősége sajátosan összeforrott, különös tekintettel arra a módra, ahogyan karizmatikus kisugárzásának hatására tanítványokként maga köré gyűjtötte az arisztokrata ifjakat. Szókratész tanítványi köréhez tartozott Kritiasz és Alkibiadész is. Szókratész és az arisztokrata ifjából álló tanítványi köre, mind a restauráció lehetősége, mind a nevelés, mind a szofisták vonatkozásában törésvonalat és konfliktust jelzett a hatalommal. Ehhez járult még a vallás, a közösségi és egyéni nevelés ügyében fennálló konfliktus, amely Anütosz demokrata és Szókratész arisztokrata köre között állt fenn. Ezt a konfliktust jelzi az idézett szöveghely is a Menón című dialógusban.<sup>12</sup> Ezért Szókratész léte biztonsági kockázatot jelentett a demokraták számára, likvidálását államérdeknek és a közjó védelmének tekintették.

### ***Az írásreform***

Az írásreform fontos elv és toposz volt a tizenegyedik alkotmánymódosítás során. A ión írásmód átvétele szükségképpen a törvények új írásmódban való alkotását és újraalkotását tette szükségessé.<sup>13</sup>

Az alkotmányreform bemutatott szervezési elvei és tényei alapján a görög jog életét fogom megvizsgálni a tizenegyedik athéni alkotmányreform következtében előállott helyzetben. A továbbiakban három Platón által írt dialógus, mint eredeti szöveggörpusz alapján, három pertípus elemzésével teszek kísérletet a restituált állam működésének bemutatására a peres gyakorlatban. A dialógusokat ebből a szempontból a filozófiatörténet és klasszika filológia tudomásom szerint még nem vizsgálta.

### ***A diké idia pertípusa***

Az első pertípusról, melynek *diké idia* az elnevezése, Platón Euthüphrón című dialógusában egy jogesetet kapcsán olvashatunk. A feltételezett beszélgetés Szókratész és Euthüphrón között i. e. 399 *Munükhion*<sup>14</sup> havában történik, amely az április-május hónapnak felel meg Szókratész perének *anakriszisz* eljárási szakaszában. Ez a drámai időpont Horvát Barna felfogása szerint a nevezetes „délsozi hajó” útjára alapozott kombináció.<sup>15</sup> A *thargélia* aratási ünnep, és mint tudjuk Athénban az aratás május-június hónapra esett. A *Thargelosz* jelentette az edényt és a benne sütött első szent kenyeret, s egyúttal a zsenge áldozatot is jelképezte. Ennek az ünnepnek a megtartása és intenzitása a tizenegyedik

<sup>12</sup> PLATÓN: Menón. 89e., 95a., pp. 76-87.

<sup>13</sup> HEGYI Dolores – KERTÉSZ István – NÉMETH György – SARKADY János (szerk.): A görög történelem a kezdetektől kr. e. 30-ig. Budapest, 1999, Osiris Kiadó, p. 219.; valamint NÉMETH György (szerk.): A görög történelem. Szöveggyűjtemény. Budapest, 2003, Osiris Kiadó.

<sup>14</sup> HORVÁTH Barna: i. m. p. 12.

<sup>15</sup> Uo.

alkotmánymódosítás után még hangsúlyosabbá vált. A *thargélia* szakrális aratási ünnep, vélhetően emiatt halasztódik Szókratész halála közel egy hónapot. Erre tekintettel Szókratész kivégzésének időpontját az ünnep végét, a hajó visszaérkezését követő napra teszem. A következtetést Platón Kritón című dialógusára alapozom.<sup>16</sup> Szókratész és Euthüphrón beszélgetésének helyszíne az *arkhón baszileosz* hivatala előtt, a *baszileosz sztoa* ligetben történt, amely szent helynek minősül, mivel a kultuszért felelős személy hivatalát övezte. Pauszaniász szerint a hivatal jobbra az első épület, ha *Keramikosz* felől lépünk az *Agorára*.<sup>17</sup> Az *arkhón baszileosz* hatásköre és illetékessége a szentélyek és kultuszok felügyelete, a vallással kapcsolatos peres ügyek, az áldozatbemutató kötelezettségének elmulasztása, a misztériumok profanizálása és a gyilkossági perek vonatkozásában volt. Ezek közül néhányban elnökölt a bíróságon, de a gyilkosságok vonatkozásában az *anakriszisz* eljárás az ő felügyelete és vezetése alatt folyt. Szókratész esetében a tárgyalást is ő vezette.<sup>18</sup> Bár Euthüphrón személyével Platón dialógusain kívül nem találkozunk, azonban történelmileg valós személy lehetett.<sup>19</sup> Platón a nevét viselő Euthüphrón című dialógusban említi meg először, mint a Proszpalté démosz tagját, aki jós, a vallási dolgok és a bölcsesség szakértője.<sup>20</sup>

### *Az Euthüpron gondolatmenet*<sup>21 22</sup>

Euthüphrón és Szókratész találkoznak az *arkhón baszileosz* csarnoka előtt.<sup>23</sup> Szókratész tartózkodásának jogcíme, hogy az *arkhón baszileosz* beidézte őt meghallgatásra. Ez feltehetőleg a második találkozása a hivatalnokkal. Euthüphrón ügye magánper, vádat szándékozik emelni az apja ellen emberölés jogcímén.<sup>24</sup> Euthüphrón szerint a megtorlatlan gyilkosság beszennyezi a várost, és azt a személyt is, aki vele egy fedél alatt él. Szókratész beszélgetőpartnere azt állítja, birtokában van a tudás arról, hogy mi az isteni és mi az istentelen.<sup>25</sup> Szókratész megőrül a tanítónak.<sup>26</sup> A dialógusban Euthüphrón először a fogalmat azzal a példával határozza meg, hogy Zeusz is megtorolta Kronosz tettét Uranossal szemben. Az emberek önellentmondásban vannak, amikor helytelenítik azt, amit tenni akar, azt tudniillik,

<sup>16</sup> PLATÓN: Kritón. 44a. p. 158.

<sup>17</sup> PLATÓN: Euthüphrón. 15. lábjegyzet. Pauszaniász: Görögország leírása I. 3. p. 1.

<sup>18</sup> ARISZTOTELESZ: Az athéni állam. LVII.2- 4.,pp. 116 – 117.

<sup>19</sup> PLATÓN: Euthüphrón 4 a5, Mogyoródi Emese 7. lábjegyzete. p. 15.

<sup>20</sup> I. m. p. 17.

<sup>21</sup> Vö. i. m. pp. 7-13.

<sup>22</sup> I. m. 2a – 16a.

<sup>23</sup> A közöttük zajló beszélgetés fikció, mert az idézési szabályok alapján így ebben a formában nem találkozhattak egymással. Szókratész a szent helyekről történő kitiltás hatálya alatt áll, miaszmában „szenved”, ezért „fertőző” a környezetére nézve. [A dialógust fiktívnek gondolom. Az idézési szabályok alapján így ebben a formában nem találkozhattak egymással. Szókratész kitiltás hatálya alatt van a szent helyekről és miaszmában „szenved”, „fertőző” a környezetére nézve. Öt évvel ezelőtti lehet csak az a tényállás, amely alapján Euthüphrón vádat készül emelni az apja ellen.]

<sup>24</sup> PLATÓN: Euthüphrón. 2a-4b. A tényállás, amely alapján Euthüphrón vádat készül emelni az apja ellen, feltehetően öt évvel korábbi lehet.

<sup>25</sup> I. m. 4b-4e.

<sup>26</sup> I. m. 4e-5c.

hogy megvádolja az apját.<sup>27</sup> Szókratész ekkor rámutat arra, hogy a definíciónak általánosan érvényesnek kell lennie.<sup>28</sup> A dialógusban kifejtett érvelésment:

1. *definíció:* „Ami kedves az istenek előtt, az istenes, ami pedig nem kedves, istentelen.” Az istenes és az istentelen ellentétben állnak egymással. Euthüphrón megjegyzi, hogy istenek vitatkoznak a jó és a rossz kérdésében.<sup>29</sup> Szókratész szerint a meghatározás nem kielégítő, az egyes isteneknek más kedves.<sup>30</sup> Euthüphrón ekkor javítja az 1. definíciót. Eszerint létezik olyan erkölcsi kérdés, amelyben minden isten egyetért: a jogtalanság elkövetőjét meg kell büntetni. Szókratész ellenvetése az, hogy nem elvi, hanem konkrét ügyről vitáznak.<sup>31</sup> Módosul a definíció: „Az istenes az, amit minden isten kedvel, az ellentéte pedig, amit minden isten gyűlöl, istentelen.”<sup>32</sup> A definíció megcáfolásra kerül, a hordozott és a hordozó, a látott és látó példáján. Ha valamivel történik valami, akkor az oknak prioritása van a történéshez viszonyítva, amiből analógiával az következik, hogy egy kedvelt dolgot nem azért kedvelnek, mert az sokak által kedvelt, hanem azért kedvelik, mert az önmagában kedvelt.<sup>33</sup> Ha pedig ez igaz, akkor az istenes nem lehet azonos a sokak által kedvelttel.<sup>34</sup> Szókratész egy *aporiával* bizonyítja, hogy Euthüphrón kudarcot vallott a meghatározás kísérletével.<sup>35</sup>

2. *definíció:* Szókratész rávezeti Euthüphrón, hogy a nem (genus) és a megkülönböztető jegy (differentia specifica) mentén határozza meg az istenes fogalmát. Ezért először a nem és a faj (species) viszonyát elemzi a félelem és a szégyen példájával. Az istenes fogalmának a meghatározásához az igazságosság erényét javasolja, s megállapítja, hogy az istenes a fajhoz, míg az igazságosság a nemhez tartozik.<sup>36</sup> A kérdés az, hogy az istenes-species hogyan különíthető el az az igazságosság többi fajtájától, hogyan határozható meg fajfogalomként. Szókratész a páros-páratlan szám analógiájának segítségével találja meg a megkülönböztető jegyet. Szókratész formálisan helyesnek tartja Euthüphrón azon meghatározását, hogy az istenes az a része az igazságosságnak, amelyik az istenek gondozásával áll kapcsolatban.<sup>37</sup> Azonban a lovak gondozásának analógiájával megmutatja, hogy a javasolt megkülönböztető jegy, a „gondozás” elfogadhatatlan, mert az emberek istenes tettei jobbá teszik az isteneket. Euthüphrón nem ezt akarja állítani,<sup>38</sup> és a megkülönböztető jegyet „szolgálatra” cseréli. Eszerint az istenes az a fajtája az igazságosságnak, amelyik az istenek szolgálata. Ekkor Szókratész a mesterségek analógiájával rávezeti, kell lenni egy műnek vagy munkának, amire az istenek tevékenysége utal és minket, mint teljesítési segédeket alkalmaznak. Euthüphrón azt állítja, mindenkinél jobban tudja, hogy ez sok szép dolog. Azonban a szolgálat fogalma meghatározatlan marad, és így a definíció hiányos lesz.<sup>39</sup>

---

<sup>27</sup> I. m. 5d-6a.

<sup>28</sup> I. m. 6a-6e.

<sup>29</sup> I. m. 6a-7e.

<sup>30</sup> I. m. 7e-8b.

<sup>31</sup> I. m. 8b-9e.

<sup>32</sup> I. m. 9c-9e.

<sup>33</sup> I. m. 9e-10c.

<sup>34</sup> I. m. 10d-11b.

<sup>35</sup> I. m. 11b – 11e.

<sup>36</sup> I. m. 11e – 12d.

<sup>37</sup> I. m. 12d – 12e.

<sup>38</sup> I. m. 12e – 13d.

<sup>39</sup> I. m. 13d – 14b.

3. *definíció*: Euthüphrón zavarba jön, újabb definíciót ad. Az istenes lényegét az istenekhez való imádkozás és a nekik nyújtott áldozás szakértelme adja. Szókratész pontosítja: a helyes kérés és a nekik való helyes adás tudománya az istenes,<sup>40</sup> mert a helyes kérésre nekünk van szükségünk, a helyes adásra az isteneknek van szükségük. Az istenes fogalma eszerint cserekereskedelemként határozható meg. Euthüphrón felháborodik azon, hogy az istenek hasznot húznak belőlünk. Felsorolja, hogy a hagyományos görög vallás szerint, mi jár az isteneknek: tisztelet, megbecsülés, dicsőség. Szókratész arra következtet, hogy az istenes nem az, ami hasznos vagy kedves számukra, hanem az, ami az istenek dicsőségére szolgál. Euthüphrón kijelenti, ami kedves az istenek számára az istenes,<sup>41</sup> s ezzel visszakanyarodnak az első definícióhoz: Az istenes, ami az isteneknek kedves. Az istenes és a kedves nem lehet ugyanaz. Két lehetőség adott: vagy az istenes és az isteneknek kedves nem ugyanaz, vagy ha ugyanaz, akkor a jelenlegi definíció helytelen.<sup>42</sup> Az elsőhöz visszakanyarodó harmadik definíció *aporia*hoz vezet. Szókratész javaslata, vizsgálódjanak újra.<sup>43</sup>

### ***Euthüpron „hozott” jogesete***

„Különben a megölt ember bérmunkásom volt, és amikor Naxoszon műveltük a földet, ott dolgozott napszámban nálunk. Mármost egyszer jól lerészegedett, aztán feldühödött az egyik szolgánkra, és elvágta a torkát. Erre az apám kezét-lábát összekötözve belökte egy gödörbe, és ide küldetett valakit a vallási tanácsadóhoz, hogy megtudakolja tőle, mi a teendő. Eközben a megkötözöttel egyáltalán nem törődött, gondolván, hogy mivel gyilkos, mit sem számít, ha akár meghalna is – ami be is következett. Mert az éhségtől, a hidegtől, és a kötelékeitől elgyötörve elpusztult, mielőtt a hírnök visszaérkezett volna a tanácsadótól. Nos, persze hogy haragszik rám az apám az egész rokonsággal egyetemben, hiszen egy gyilkos miatt vádoló gyilkossággal az apámat, pedig szerintük nem is ő ölte meg őt, de ha megölte volna is, akkor is, mivel az elhunyt maga is gyilkos volt, az ilyennel nem kell törődni – hiszen istentelen dolog, hogy egy fiú gyilkossággal vádolja az apját.”<sup>44</sup> A dialógusban tárgyalt jogeset mai fogalmaink szerint az eshetőleges szándékkal elkövetett szándékos emberölés törvényi tényállásának felel meg. Egy ilyen visszavetített minősítéssel azonban a következők miatt félreértjük az athéni jogot.

Első olvasatra egyértelműnek tűnik, hogy a jogeset, bármilyen furcsa is, a *diké idia* per típusához tartozik, tehát magánper, az eljárást az *arkhón baszileosz* előtt kell megindítani. Arisztotelész leírása szerint, az előzetes vizsgálat az *anakriszisz* eljárás keretében történik, az ügy az eljárás eredményétől függően kerül a megfelelő bírói fórum elé.<sup>45</sup> „Az emberölési vagy megsebesítési perek, ha a gyilkosság vagy a megsebzés előre megfontolt szándékkal történt, az *Areioszpagos* elé tartoznak, úgyszintén a mérgezés, ha halált okoz, továbbá a gyújtogatás; egyedül ezekben ítélik az *Areioszpagosz* tanácsa. A vétlen esetben való gyilkolás és gyilkossági szándék felett, továbbá az olyan ügyben, ha valaki rabszolgát, metoikoszt vagy idegent ölt meg a *Palladion* bírái ítélik. Ha valaki elismeri, hogy ölt, de azt

<sup>40</sup> I. m. 14b – 15b.

<sup>41</sup> I. m. 14d – 15b.

<sup>42</sup> I. m. 15b – 15c.

<sup>43</sup> I. m. 15c – 16a.

<sup>44</sup> I. m. 4c4 – e.

<sup>45</sup> ARISZTOTELÉSZ: i. m. LVII. 3. p. 115.

állítja, hogy eljárása nem ütközik törvénybe, mint például, ha felesége elcsábítóját tetten érte, vagy ha a harcban nem ismert fel valakit, vagy a versenyen küzdelem közben történt – az ilyen felett a *Delphinionban* ítélik; aki száműzetésben van megbocsátható gyilkosságért, és megvádolják, hogy valakit megölt vagy megsebzett, a felett *Phreatos* csarnokában ítélik, ő pedig egy lehorgonyzott hajón védekezik.<sup>46</sup> Arisztotelész leírásából egyértelműen kiderül, hogy az athéni állam jogában ennél a pertípusnál, az emberölés eseteiben milyen körültekintően szabályozott és differenciált a lefolytatott vizsgálat, melynek során különbséget tesznek az emberölés szándékos, gondatlan, véletlen alakzatai között.<sup>47</sup>

A dialógusban előadott jogeset értelmezését, a dialógus valóságosságát illetően több probléma is adódik. (a) Szókratész és Euthüphrón nem találkozhat egymással szent helyen, mert Szókratész a szent helyekről való kitiltás hatálya alatt van, és mint ilyen *miaszmában* szenved, amely „fertőző” lehet Euthüphrónra nézve. (b) A dialógus létrejöttét nehezíti az is, hogy Euthüphrón megszegi az idézési szabályokat, amelyek az *diké idia* és a *graphé timétosz* esetében megegyeznek.<sup>48</sup> „Az attikai perjog értelmében az idézés úgy történt, hogy a felperes, illetőleg a vádló egy vagy két tanú kíséretében felkereste ellenfelét és őt a kereset, illetőleg a vád jogalapjának megjelölése mellett felhívta arra, hogy meghatározott napon az illetékes hatóság előtt jelenjen meg a keresetlevél, illetőleg a vádindítvány átvétele végett. Az idézésnek legalább négy nappal kellett az utóbbi napot megelőznie. Az idézést követte a keresetlevélnek, illetőleg a vádindítványnak az illetékes hatóságnál való benyújtása.”<sup>49</sup> Euthüphrónnak a saját apját előzetesen idéznie kellett volna nyilvános helyen, majd a tanúkkal együtt megjelenni a *baszileosz sztoában*. Euthüphrón azonban egyedül van. Erre tekintettel pedig, az ő eljárás indítása nem hatályos, és nem törvény szerint való. (c) Szókratész arra hivatkozik, hogy őt az *arkhón baszileosz* idézte be.<sup>50</sup> Ebből az következik, hogy Szókratész már átesett az első meghallgatáson, átvette a vádindítványt és az *anakriszisz* eljárás folyamatban van, így ez már a második találkozója. Ebben az esetben csak rá kellene mutatnia Melétoszra, hogy ott van, ő az, és nem kellene elmesélni, hogy milyen a vádlója. „Magam nem igen ismerem az illetőt, Euthüphrón: úgy tűnik, hogy valami ismeretlen ifjú. Mindenesetre, ha jól tudom, Melétosznak hívják. A Pitthosz démoszból származik, egy bizonyos egyenes hajú, alig serkenő szakállú, sasorrú pitthoszi Melétosz, ha ez mond valamit.”<sup>51</sup> (d) Ezen túlmenően van még egy további súlyos probléma a találkozó valóságosságát illetően. Erre a dialógus fordítója, Mogyoródi Emese hívja fel a figyelmünket: „Naxosz a Küklaszok legnagyobb szigete, Parosztól Keletre fekszik. Euthüphrón és apja feltehetőleg telepesként (*klérukhosz*) éltek itt és művelték a földet. Komoly fejtörésre adott okot a tény, hogy Athén Naxoszt 404-ben (tehát az Euthüphrón drámai ideje, azaz 399 előtt öt évvel) elvesztette. Platón tehát vagy szándékosan él az anakronizmussal, hogy jelezze, a dialógus fikatív, vagy azt kell feltételeznünk, hogy Euthüphrón öt évet várt apja beperlésével. Úgy tűnik azonban, hogy a dialógus nem lehet fikatív, mert a történet ehhez túlságosan komplikált és különleges. Euthüphrón késlekedését viszont nem

---

<sup>46</sup> I. m. LVII. 3. pp. 115-117.

<sup>47</sup> Vö. LACZÓ József: Szándékos, gondatlan, véletlen emberölés megítélése Athénban. Budapest, 2017, Kézirat.

<sup>48</sup> HORVÁTH Barna: i. m. p. 14.

<sup>49</sup> Uo.

<sup>50</sup> PLATÓN: Euthüphrón. 2a – 4 b. p. 7.

<sup>51</sup> I. m. 2 b 8-12. p. 16.



okozhatták a Burnet által említett történeti, illetve törvénykezési körülmények (vö. Allen 1970, 21.). Hoeber (1958, 97. ) szerint a késlekedés megvilágítja Euthüphrón jellemét (és jól illik apja idős korához): az évek múlásával az orphikus szektákhoz közel álló fiúban növekszik az aggodalom apja és a maga túlvilági sorsával kapcsolatban, ezért minden óvintézkedést megtesz, hogy mielőtt még késő lenne, megtisztítsa magát és az apját minden megelőzőleg elkövetett vétektől.”<sup>52</sup> A túlságosan komplikált jogeset tántorítja el Mogyoródi Emesét, hogy kimondja, a dialógus fikatív. „Úgy tűnik azonban, hogy a dialógus nem lehet fikatív, mert a történet ehhez túlságosan komplikált és különleges”<sup>53</sup> Ezzel kapcsolatban, jogászi nézőpontból, azt kell mondanunk, hogy a jogtudományi oktatásban használatos büntetőjogi jogesetgyűjtemények általában bonyolult és komplikált jogeseteket tartalmaznak. De persze vannak bennük olyanok is, amelyek a jogesetgyűjtemény összeállítójának fantáziáját dicsérik. Platón fantáziájával pedig nem vagyunk ok nélkül elfogultak. Így álláspontunk szerint az ügy, amely egy komplett *diké idia* pertípust rejt, valóságos lehet, a dialógus azonban az említett okok miatt fikatív.<sup>54</sup>

### A graphé timétosz pertípusa

A Szókratész védőbeszéde című dialógus egy *graphé timétosz* pertípust tartalmaz. A dialógus három beszédre tagolódik, amelyek a pertípus következőképpen foglalható össze. Az *első* beszéd a bűnösség kérdését vizsgálja. Szókratész először az ellene felhozott régi vádakát cáfolja. Az ellene irányuló rágalmak alaptalanok, mert nem természetfilozófus és nem is szofista. A vádak eredete a jóslat miatt lehetséges. A jóslat értelmének vizsgálata során az államférfiak, költők, kézművesek vizsgálata. A vizsgálat eredménye a rágalomhadjárat lett. A jóslat értelme egyenlő Szókratész küldetésével. Tevékenységét utánozzák az ifjak, további ellenségek keletkeznek. Ez vezetett Melétosz vádjához.<sup>55</sup> Az új vádak cáfolata következik. Melétosz soha nem törődött az ifjakkal, és téved abban, hogy ki teszi jobbakká őket. Második tévedése, lehetséges-e szándékosan ártani valakinek. Az istenek tiszteletének hiánya vonatkozásában a vád alapjában véve ellentmondásos szerkezetű. A vád értelmezése, hogy az istenekkel szembeni tiszteletlenségre tanítja az ifjakat Szókratész. A benyújtott vádirat önellentmondásos és ennek konklúziója is levonja Szókratész.<sup>56</sup> A Szókratész által választott életmód szégyenletes és esztelen, mert életveszélyes. A válaszban Szókratész az istenfélelmét bizonyítja. A helyes felől közelítve, hogy a kötelesség mindig előbbre való, mint az élet. A halálfélelem nem riasztja el küldetése gyakorlásától, amely a jóslaton alapul. A hasznos felőli megfontolások: Vádloi nem árthatnak neki és isteni küldetése Athén javát szolgálja. Ellenvetés, hogy Szókratésznek részt kellett volna venni a politikában. Szókratész válasza, hogy tevékenysége az ifjakra üdvös, a *daimóni* jelzés akadályozta a nyilvános politizálását. A második ellenvetés, hogy a tisztességes politizálás lehetetlen Athénban. Ezért Szókratész az egyes emberrel való beszélgetés határain belül marad, amiből azonban nem zár ki senkit. Az ifjakra való hatása pedig egyenesen üdvös.<sup>57</sup> Szókratész nem fog esdekeln a bírákhoz, mert méltatlan volna

<sup>52</sup> I. m. 10. lábjegyzet p. 20.

<sup>53</sup> Uo.

<sup>54</sup> LACZÓ József: Egy férfi, aki nem volt ott. Budapest, 2017, Kézirat

<sup>55</sup> PLATÓN: Szókratész védőbeszéde. 17a – 24b2.

<sup>56</sup> I. m. 24b3 – 28b2.

<sup>57</sup> I. m. 28b3 – 34b5.

magához, a bírákhoz és egész Athénhoz is. Nem volna jogszerű és nem volna istenfélő sem.<sup>58</sup> A második beszéd a büntetést értelmezi. A szavazás értékelése és elvi ellenindítvány érdem szerinti megtétele. Szókratész a város jötevője és nincs vagyona. Ezért megérdemli, hogy állami eljárásban részesüljön. Gyakorlati ellenindítvány: Szókratész nem érdemel büntetést, de a lehetőségeket számba veszi. A száműzetés nem opció. A börtönbüntetés sem elfogadható lehetőség a számára. Ha a bíróság ragaszkodik a büntetéshez egy *mina* pénzbírságot javasol, amit meg tud fizetni. Az összeget barátai kérésére felemeli harminc *minára*.<sup>59</sup> A harmadik beszédben<sup>60</sup> végső reflexiókat fogalmaz meg és elbúcsúzik. Megvilágítja a halál értelmét halálára szavazók tak, a halál jelentősége Szókratész számára. A halálra szavazóknak felelőssége van, és Szókratész összeveti vádlóival magát. Szókratész jósol. Azoknak, akik a felmentésre szavaztak értékeli a *daimóni* jelzés elmaradását. Megvizsgálja a halálra vonatkozó nézeteket. Szókratész búcsújában kifejti, hogy bízik az isteni gondviselésben és a bírakra bízza a fiait.<sup>61</sup>

A tanulmányhoz csatolt Melléklet sematikus ábrázolja Szókratész perének a statikáját és dinamikáját. A per dinamikájának az alapja a hasonló módon lefolytatott *aszebeia* perek statikája.<sup>62</sup> Szókratész perét négy részre, a II. részt A és B alrészre osztom. A részek és alrészek további szakaszokra oszthatók a per tényleges menetének megfelelően. A Szókratész elleni per lefolyása az athéni peres eljárási szabályai alapján rekonstruálható. A huszonhárom pont egy folyamatára, amely Szókratész perének dinamikáját mutatja be. Az első részt politikai szakasznak nevezem, amely a peloponnészoszi háborút a spártai békediktátummal zárja le. A demokrata restauráció alkotmányreformmal kezdődik, amely a római hódításig hatályban marad és Arisztotelész szerint a tizenegyedik. A jogi reformból az amnesztia törvény emelkedik ki, amelynek Szolón reformjainál vannak előzményei. Fontos az összes *pszefizma* hatályon kívül helyezése, közöttük a Diopithész-féle is.

A közvetlen Szókratész elleni politikai koncepciót „Délia-tervnek” nevezem, és az idézés jelenti a fordulót, amely átvezet a II. Rész A) alrészébe. Ez az *anakriszisz* eljárás egy meghatározott szakaszát, az előzetes eljárást jelenti. Az előzetes eljárásban az *arkhón basszileosz* eldönti, hogy lesz-e egyáltalán per. Feltételezésem szerint az eljárásnak ebben a szakaszban nyújtják be a vádiratot, ekkor történik a vádirat formai vizsgálata az illetékes közhivatalnok részéről. A tartami vizsgálat már egy újabb szintlépés, amelynek a következménye a vádirat átadása és az *arkhón* kihirdeti a kitiltás hatályát Szókratészre és átadja a vádirat egy példányát. A felek többször is megfordulhatnak szükség szerint ebben a szakaszban az *arkhón basszileosz* előtt, amelynek során az felhívja Szókratészt a kötelezettségére, hogy írásbeli védekezést, *apológiát* kell előterjesztenie a törvény szerint.

---

<sup>58</sup> I. m. 4b6 – 35d9.

<sup>59</sup> I. m. 35 e1 – 38b10.

<sup>60</sup> Itt meg kell jegyeznem, hogy a harmadik beszédet fiktívnek tartom, amelyet Platón mintegy hozzágondolt a perhez. Itt persze nem beszédről, hanem beszélgetésről van szó. A perrend nem engedte meg az elítélt beszédét. Az arkhón az ítélet írásba foglalásával foglalatoskodik, nem adta meg a vádnak a szót, pedig mindig ők szólnak először. Beszéd a bémáról hangozhat el, mért idővel. A bírák nagy része már az oboloszaiért megy.

<sup>61</sup> I. m. 38c1 – 42a5.

<sup>62</sup> LACZÓ József: Az aszebeia-istentelenségi perek statikája és dinamikája. Budapest, 2017, Kézirat.

A B) alszakaszba való átfordulás az apológia benyújtása és az eskü kivétele jelenti a felektől, hogy csak az ügygel szorosan összefüggő tényeket hivatkozzák. Ebben a szakaszban már eldöntötték, hogy a pert megindítják. A tárgyalás előkészítése érdekében az *arkhónnak*, a *teszmothészekhez* kell fordulnia. A tárgyalás kitézésére harminc nap áll rendelkezésre. A bíróság hozzárendelése és a bíróság megszervezése fordítja az ügyet a III. részbe, amely a tárgyalási szakaszt jelenti. A tárgyalás megkezdése előtt a kultuszért felelős *arkhón* füstáldozatot és imát végez a *miszama* és az egyéb szokásos dolgok miatt. A tárgyalás megnyitása előtt megtörténik a tíz bíró kiválasztása, akik segítő feladatokat látnak el a tárgyalás során. A tárgyalás megnyitása, akkor történik, amikor a *herold* a felek nevét kikiáltja a jelenlévők felé. A tárgyalás az irat jegyzők általi felolvasásával kezdődik meg. Ezután fordul át a per menete az írásbeli szakaszból a szóbeli szakaszba, a vádbeszéd, a *szünégorosz* Anütosz beszéde következik, majd Szókratész első beszéde hangzik el. A beszédek után a 14. szakaszban Szókratész bűnösségéről dönt a bíróság. Majd ezután következik az úgynevezett becslési eljárás, de előtte a vádlónak büntetést indítványozó *timétosz* beszéde és Szókratész *antitimészisz* rész is tartalmazó második beszéde hangzik el. A becslési döntés után az *arkhón* kimondja a határozatot, amely ellen kifogást lehet előterjeszteni, ami ebben az esetben nem történt meg. A bíróság feloszlik, az *arkhón baszileosz* írásba foglalja az ítéletet. Ekkor ajánlja fel Kritón az első óvadékot, hogy az elítélt az idő elérkezéséig szabadlábon legyen. Ez a státusz és a *miaszma* miatt elutasításra kerül. Feltételezésem szerint a köztisztviselő szakrális elemmel, füstáldozattal és imával zárja be a pert. A bírák a négy bíró felügyelete mellett átveszik az *oboloszokat*. Néhányan esetleg beszélgetnek Szókratésszel, aki a tizenegyeket a helyszínen várja. Fontos tény, hogy a bíróság előtti beszéd a *bémán* hangozhat, mért idővel, bírósági döntéssel. Ekkor fordul Szókratész ügye a végrehajtási szakaszba, amely a IV. része az eljárásnak. Kritón, kezessége és óvadéka alapján Szókratészt barátai látogathatják a börtönben, azzal az ígérettel, hogy Szókratész nem szökik meg. A kezességet Kritón vállalja. A börtönbeli tevékenység I. vonatkozása a szökés lehetőségének megvizsgálása egy hipotetikus *graphé paranomón* keretében. A Börtönbeli tevékenység II. Vizsgálódás a lélekről, és Szókratész írásai, amelyről Platón Phaidón című dialógusa tudósít. A következő szakaszt az ítélet végrehajtásának előkészítése, a *teszmothészek* döntése és a halál nemének a megállapítása jelenti. Az utolsó szakasz a halál tényének megállapítása, a hagyaték és az iratok sorsáról való rendelkezés. Meléoszt tíz százalék illeti abból az egy *minából*, amely Szókratész vagyona. Valamint Xantippétól szpéthoszi Aiszkhinész megveszi Szókratész hagyatékát az iratokkal.

Természetesen kritikai elemzés alá kell venni Platón, Xenophón, Arisztophanész, Arisztotelész, és a másodlagos irodalom írásait is. A megarai emigráció idején többen írtak Szókratész vonatkozásában Apológiát: „Minden valószínűség szerint ugyanis hitelt adhatunk Diogenész Laertiosz idevonatkozó tudósításának, miszerint Platón más Szókratész követőkkel egyetemben a pert követően Megarába távozott, Eukleidészhez (Diogenész Laertiosz III. 6. vö. II. 106) és egy ideig nem is tért vissza. Ha azonban a számonkérésnek nem feltétlenül abban a formában kell bekövetkeznie, ahogyan azt Szókratész maga gyakorolta, akkor ideszámíthatjuk az ún. „Szókratikus beszédeket” (Szókratikai logoi), amely

műfajnak számos gyakorlója akadt Szókratész halálát követően. (Aiszkhinész, Antiszthenész, Xenophón stb.)<sup>63</sup>

A Szókratész-per rekonstrukciójának pontossága, tudományos egzaktusa a rendelkezésre álló források értelmezésétől nagymértékben függ. Ezzel összefüggésben két problémát kell megvizsgálni: a halálbüntetés kiszabását javasoló vádindítvány és az ellenindítvány szempontjait, illetve a bírák létszámára vonatkozó fejtegetést. Ami a *timéosz* – *antitimészisz* problémáját illeti, a következőre problémára kell felhívni a figyelmet. „Egy ilyen per (ún. *graphé timéosz*) esetében, ahol a törvény nem határozta meg a kiszabható büntetést, a vádló maga tett erre javaslatot a vádirat benyújtásával együtt. A bíróság a vádlott védőbeszédének elhangzása után szavazott róla, hogy a benyújtott vádakban egyáltalán bűnösnek találja-e vagy sem. A szavazás eredményét kihírdették, majd a vádlottnak a törvény értelmében javaslatot kellett tennie a saját büntetésére (*antitimészisz*), amely általában nyilvánvalóan valami enyhébb alternatívát jelentett a vádló által indítványozotthoz képest. A vádlottnak magának viszont nem volt ajánlatos az előterjesztettnél sokkal enyhébb alternatív büntetést kérnie, mert ilyen esetben a bírának joguk és kötelességük volt elfogadni a vád által indítványozott büntetést. Harmadik lehetőség nem volt.”<sup>64</sup> A vádlók elkövettek egy jogi hibát. Ha igazából Szókratész eltávolítása lett volna csupán az igazi céljuk, akkor nem halálbüntetést, hanem csak száműzetést kellett volna indítványozniuk. Ebben az esetben a bíróság adott ellenindítványok mellett Szókratészt száműzi és Szókratész számára a halálbüntetést csak saját indítványa esetében szabhatott volna ki. Ebből két következtetést lehet levonni. Vagy ténylegesen meg akarták ölni Szókratészt és a halálos indítványt valósnak és akartnak kell feltételeznünk, vagy pedig ebben a kérdésben nem gondolkodtak helyesen és tudniuk kellett volna, hogy Szókratész nem fog sem elszökni az eljárás elől, sem könyörögni nem fog az enyhébb büntetésért, valamint a Börtönből sem fog megszökni akármennyire unszolják őt barátai és tanítványai. Viszont biztosra veszem, hogy száműzetési indítvány esetén a „megarai emigráció” megvalósult volna az „enyhébb” indítvány esetén is. A bíróság nem tud egyebet tenni, mint a két indítványból választ, hogy melyik felel meg a mérlegelés után az bíróság felfogása szerinti igazságosságának.

A másik problémát a bíróság létszámának a meghatározása jelenti. Horváth Barna ötszázegy tagú bíróságról beszél, ami azonban Szókratész perében fogalmilag kizárt. Ez annak ellenére állítható, hogy az ötszázegy létszám Arisztotelész szövegéből származik. Ezzel szemben bizonyosak lehetünk abban, hogy Szókratész perében az egyenlőségi szabály érvényben volt. A szabály miatt 500 főt kell tételünk, de mindenképpen páros számú bírósági tanácsot kell elgondolnunk, Platón szövegkorpusza alapján: „XXV Hogy ne haragudjak a történetekért, athéni férfiak, hogy bűnösnek ítéltetek, arra számos okom van. Legfőképpen, mert nem ért váratlanul az eredmény, sőt sokkal inkább csodálkozom a szavazatok számán, mindkét oldalon. Mert ugyan nem gondoltam volna, hogy ilyen kevés szavazaton múlik majd a döntés, hanem sokkal többet vártam. Lám úgy látszik, ha csupán harminccal több esett volna a másik oldalra, most fel volnék mentve.”<sup>65</sup> A dialógus fordítója is ezt a gondolatmenetet támogatja: „Nem tudjuk egészen bizonyosan,

---

<sup>63</sup> I. m. 135. lábjegyzet, p. 107.

<sup>64</sup> I. m. 111. lábjegyzet, p. 99.

<sup>65</sup> I. m. 35 e – 36 a – a7.

pontosan hány emberből állt a bíróság, mely a perben ítélkezett, mert a 6000 esküdtbírából ebben az időszakban ennél kisebb, de néhány száztól több ezerig terjedő létszámú testületek ülészetek. Mindenesetre egy ilyen per esetében a korban általában ötszáz emberből állt a bírósági testület (később felemelték ötszázegyre) Ebből következne, hogy 280-an szavaztak Szókratész bűnösségére és 220-an ártatlansága mellett. (Egyenlő szavazat esetén a vádlottat felmentették.)<sup>66</sup> Természetesen később a létszámot páratlan számúra kellett emelni, de akkor az egyenlőségi szabályt is hatályon kívül kellett helyezni. Tovább erősíti ezt az álláspontot Diogenész Laertiosz tudósítása a témában. „Ugyancsak igen vitatott kérdés, vajon elfogadható-e Diogenész Laertiosz tudósítása, miszerint nyolcvannal többen szavaztak volna Szókratész halálára, mint ahányan az első szavazáson egyáltalán bűnösnek ítélték. (Diogenész Laertiosz II. 142.) Ez – egyébként Burnet Kalkulációjával ellentétben (vö. Burnet 1924, 161.) – a 360 *contra* 140 arányt adná a második szavazásra. Az adatot a legtöbben minden további nélkül elfogadják, noha Diogenész Laertioszé az egyetlen erre vonatkozó tudósítás – több mint hatszáz évvel Szókratész halálát követően.”<sup>67</sup>

Horváth Barna szerint Szókratész pere iskolapélda, annak ellenére, hogy az adatok hiányosak.<sup>68</sup> A bizonytalansági tényezők felvetése mellett biztosnak tűnő kiindulópontokat állít. Szerinte nem kételkedhetünk abban, hogy a pert i. e. 399. évben tárgyalta az athéni esküdtbíróóság 501 tagú tanácsa. Azonban ha ezt a szöveghelyet együtt tekintjük az egyenlő szavazati arány felmentő ítéletet jelentő regulájával, komoly gondban vagyunk. Az 501 tagú bírósági tanács tételezése még négy alkalommal fordul elő a vonatkozó szövegekben Horváth Barna esetében. Először úgy védtem Horváth Barna álláspontját, hogy az *anakriszisz* eljárást vezető *arkhón baszileoszt*, mint nem szavazó bírót számolta az ötszázhoz, aki a tárgyalást elnökként is vezeti, és így kapta az 501 bírót. Amikor azonban az egyenlőségi szabályt idézi a vádlott felmentésére, akkor ez a védelem gyengülni látszik, és az 500 tag válik elfogadhatóvá. A páratlan számú tanács esetében az egyenlő szavazati arány fogalmilag kizárt, ha feltesszük, hogy teljes a tanács és minden bíró leadja a szavazatát. Az 501 tag ellentétes a szövegekkel a szavazatok összeszámlálása miatt is.<sup>69</sup> Ezért vagy azt az álláspontot tartjuk fenn, hogy 501 tagot számlálunk, ahol is az elnök nem szavazó bíró, de fontos döntéseket hoz a per kezdete előtti eljárásban. Az előkészítő eljárást is és a tárgyalást is ő vezeti. Az ítéletnek írásba foglalásáig és Szókratésznek a 11-ek részére való átadásáig tényleges, akár „tanácsvezetői” bírói státusza van. Vagy azt az álláspontot képviseljük, hogy a szavazati arány 280 ellene és 220 mellette, nem pedig 281 ellene.<sup>70</sup> Ezzel a megoldással jöhet ki csak a Szókratész által is „elfogadott” 30 szavazat különbség aránya, amely elfogadott a szakirodalomban.<sup>71</sup> Horváth Barna 501 tagra vonatkozó kijelentése és a szavazati arány számítása az egyenlőségi szabállyal együtt olvasva egyszerre nem teljesülhet.<sup>72</sup> Azt a megoldást tartjuk valószínűnek, hogy az 501 főt

---

<sup>66</sup> I. m. 112. lábjegyzet, p. 100.

<sup>67</sup> I. m. 129. lábjegyzet, p. 105.

<sup>68</sup> HORVÁTH Barna: i. m. p. 11.

<sup>69</sup> PLATÓN: Szókratész védőbeszéde.36a7.

<sup>70</sup> HORVÁTH Barna: i. m. p. 54.

<sup>71</sup> PLATÓN: Szókratész védőbeszéde.36a.

<sup>72</sup> I. m. 112. lábjegyzet.

az egyenlőségi szabály feladása után vezették be, amit Arisztotelésznél található szöveghely bizonyít.<sup>73</sup>

### A graphé paranomón pertípusa

A Kritón című dialógus<sup>74</sup> egy *graphé paranomón* pertípust tartalmaz. Kritón meglátogatja Szókratészt a börtönben, hogy közölje, a szent hajó megérkezett. Másnap meg kell Szókratésznek halnia.<sup>75</sup> Szókratész álmot látott, mely szerint nem másnap, hanem a következő napon kell meghalnia.<sup>76</sup> Kritón menekülésre biztatja Szókratészt, mivel tart tőle, hogy az emberek megvetik, hogy fukarságból mulasztották el megmentését. Szókratész arra inti, hogy Kritón ne törődjön a sokaság véleményével, mert az sem jót, sem igazán rosszat nem tud cselekedni, mert azt teszi, ami eszébe jut.<sup>77</sup> Kritón amellet érvel, hogy meg kell szöknie Szókratésznek. Ne tartson a barátokra váró megtorlástól, mert mindenki kész az áldozatra.<sup>78</sup> Szókratész jól tenné, ha nem okozna ellenségeinek örömet, gyermekeinek fájdalmat.<sup>79</sup> Szókratész válasza, hogy mindig arra az évrre hallgatott, ami a leghelyesebbnek tűnt a számára, most sem akar másképpen cselekedni. Nem a sokaságra kell hallgatni, hanem annak a véleményére, aki szakértője a kérdésnek.<sup>80</sup> Nem csak a testi dolgokat, hanem a lelkieket illetően is a szakértőre kell figyelni, aki érti, mi árt, és mi használ a léleknek.<sup>81</sup> Nem azt fontoljuk meg, mit mondanak mások, hanem mit mond a szakértő, aki ért az igazsághoz és az igazságtalansághoz. A tömeg megölheti az embert, de nem az élet a legfontosabb, hanem a jó élet.<sup>82</sup> Igazságos-e elmenekülni a börtönből, amit meg kell vizsgálni?<sup>83</sup> Szókratész szerint, aki helyes elvek szerint akar élni, soha senkivel nem szabad igazságtalanságot elkövetnie akkor, sem ha igazságtalanságot szenved el. Ha az ember tudja, mi az igazságos nem szabad a legjobb belátása ellen cselekednie.<sup>84</sup> Szókratész szerint azt kell megvizsgálni, igazságtalanságot követne-e el, ha elmenekülne a börtönből a város engedélye nélkül. Mi lenne, ha elé állnának a város törvényei és megkérdeznék, miért akarja őket elpusztítani. Egyetlen város sem maradhat meg törvények nélkül. Miért akarod lábbal tiporni a törvényt, amely úgy rendelkezik, hogy a meghozott ítéleteknek érvényeseknek kell lenniük.<sup>85</sup> Mivel vádolsz bennünket, hogy el akarsz pusztítani. Mi vagyunk a szülőid, felnevelőid. Az igazságosság dolgában nem vagyunk egyenlők. Ha mi elpusztítunk, te nem teheted ezt meg velünk. Ha igazságtalanok voltunk veled, nem felelhetsz igazságtalansággal, és közben nem jelentheted ki, hogy igazságosan cselekszel.<sup>86</sup> Apádnál, anyádnál, minden felmenődnél szentebb a haza. Bármit meg kell tennünk, amit a város

<sup>73</sup> ARISZTOTELESZ: Az athéni állam. LVII. p. 117.

<sup>74</sup> PLATÓN: Kritón. 153. A dialógus összefoglalásához Gelenczey-Miháltz Alirán vázlatát vettük alapul.

<sup>75</sup> PLATÓN: Kritón:43a – d.

<sup>76</sup> I. m. 43d – 44b.

<sup>77</sup> I. m. 44d – 45c.

<sup>78</sup> I. m. 44d – 46a.

<sup>79</sup> I. m. 45c – 46a.

<sup>80</sup> I. m. 46a – 47a.

<sup>81</sup> I. m. 47a – d.

<sup>82</sup> I. m. 47d – 48b.

<sup>83</sup> I. m.48b – 49a.

<sup>84</sup> I. m. 49a – e.

<sup>85</sup> I. m. 49e – 50c.

<sup>86</sup> I. m. 50c – 51b.

parancsol, vagy ha nem, meg kell győznünk, hogy merre van az igazság.<sup>87</sup> A törvények mindenki számára választási lehetőséget adnak. Vagy engedelmeskedünk nekik, vagy meg kell győznünk, ha valamiről rosszul rendelkeztek. Van egy harmadik út a polgárok számára. Ha nem tetszenek a város törvényei, mindenkinek jogában áll, családjával, vagyonával együtt kivándorolni.<sup>88</sup> Szókratész nem hagyta el a várost, mert tetszett a város törvényes rendje. Hiszen kinek tetszene egy város annak törvényei nélkül.<sup>89</sup> Milyen lenne az élete máshol. Földönfutó idegen lenne. Semmivé válnának az elveid, amit hirdettél. Nem beszélhetnél az igazságról, a törvények tiszteletéről és az igazságról, ha lábbal tipornád azokat, ha a város ítéletét kijátszva megszöknél. Nem élhetnél így tovább.<sup>90</sup> Mindenképpen jobb és méltóbb, ha meghalnál. Az ottani bírák elé állnál, mert igazságtalanságot szenvedve mentél el innen, de te magad nem követtél el igazságtalanságot. Ne vegyen rá Kritón a szökésre.

Athénban a tizenegyedik alkotmánymódosítást követően, a törvényalkotás az i. e. 5. században kialakult gyakorlatnak megfelelően rögzült. A népgyűlés már nem kezdeményezett törvényeket.<sup>91</sup> A törvényjavaslatokat a *Bulé*, az ötszázak tanácsa készítette elő és terjesztette a népgyűlés elé. Az *Ekklészia*, a népgyűlés megtárgyalta a javaslatot és döntött. Ha a népgyűlés a javaslatot elfogadta, hogy a kérdésben szükséges törvényt alkotni, akkor a *Héliia* egy külön tanácsa megvitatta a törvényjavaslatot. A külön bírósági tanács görög neve *Nomothetai*, amely a törvényt felülvizsgáló bírósági tanácsot jelentette. Tagjai a 6000 fős esküdtbírószámból sorsolással kerültek ki. A 600 tagú külön bírósági tanács a törvényjavaslatot megszövegezte és az ismét a népgyűlés elé került. Népgyűlési jóváhagyás után a bírósági tanács megvitatta, és ha elfogadta, akkor ilyen módon hatályos joggá vált. Ez volt a törvényalkotás alapesete és ún. „rendes menete”. A bonyodalom ott kezdődött, ha valamely jogterület újraszabályozásra egy meglévő törvény esetében került sor, akár módosítás, akár a teljes törvény hatályon kívül helyezésével. Ebben az esetben a régi törvény mellé egy védőt kellett rendelni, akinek a feladata a hatályos és érvényes törvény védelme volt. A javaslatot tévő pedig opponálta a régi törvényt és az indítványának megfelelően a törvény módosítását, vagy hatályon kívül helyezését képviselte. Abban az esetben, ha az erre szervezett külön bíróság a régi törvényt a javaslatnak megfelelően „elítélte”, ekkor kezdődhetett az ötszázak tanácsában a törvény javaslatának, vagy a módosítás betervezésének előkészítése. Ha ez megtörtént, akkor kerülhetett a népgyűlés elé a javaslat és a fentiekben jelzett módon történt az eljárás. Ephialtész i. e. 462-461 évi *arkhónsága* idején vezette be a *graphé paranomón* eljárást, amelyet alkotmányvédelmi eszközként is értékelhetünk. „Ephialtész az *Areiosz pagosztól* megvonta azt a jogot is, hogy a népgyűlés által elfogadott törvényeket jóváhagyja vagy elutasítsa. Így, a törvényhozó hatalom letéteményese a népgyűlés és az ötszázak tanácsa lett.”<sup>92</sup> Ezt kiegészíthetjük azzal, hogy a *nomothetész* bírósági tanácsával a törvényhozó hatalom gyakorlása három intézmény között oszlott meg. Nem véletlen, hogy az *arkhón* a városszéli viskójába

---

<sup>87</sup> I. m. 51c – 52a.

<sup>88</sup> I. m. 51c – 53a.

<sup>89</sup> I. m. 52a – 53a.

<sup>90</sup> I. m. 53a – 54b.

<sup>91</sup> KAJTÁR István – HERGER Csabáné: Egyetemes állam és jogtörténet. Budapest, 2013, Dialóg Campus Kiadó, p. 32.

<sup>92</sup> I. m. p. 31.

menet egy éjszaka meggyilkolták,<sup>93</sup> mielőtt az *arkhóni* idejét teljesen kitöltötte volna. „Az alkotmányos rendet a *graphé* (közvád) egyik speciális formája, az ún. *graphé paranomón* (törvénytelenesség elleni vádirat) intézménye védte. A nem jogerős törvény esetén a *Héliia* elé került. A népgyűlés tagjai a törvényjavaslatok előterjesztését minden bizonnyal jól meggondolták, mert ha a *Héliia* az ilyen előzetes normakontroll során a törvényhely jogellenességét állapította meg, az előterjesztőt bírsággal vagy halálbüntetéssel sújtották. Ha viszont a *graphé paranomón* alaptalannak bizonyult, a kifogásolót büntették meg.”<sup>94</sup> Egyfelől a törvénytelenesség elleni vádirat benyújtása előtt az illetékes *arkhón*nak le kellett folytatnia az *anakriszisz* eljárást és az ügyet, amennyiben arra érdemesnek tartotta a *héliia* különbírósa elé nem a *nomothetész* 600 tagú tanácsa elé került, amely a javaslat felett döntött. Ha a vádlónak adott igazat, akkor is, ha a bevádoltat nem találta vétkesnek az indítvány vonatkozásában, implikált egy következő *anakriszisz* eljárást, az illetékes *arkhón* előtt, aki az eljárás után már a „rendes” *héliia* tanácsa elé utalta az ügyet, amely a szokásos kétmozzanatú eljárása során először a bűnösség kérdésében, majd a becslési eljárásban a büntetés kiszabásáról döntött. Ezért tekintem én a *graphé paranomón*t a harmadik pertípusnak, amely kettős arculatú: egyfelől az alkotmányvédelem, másfelől a vétkes személy megbüntetése a funkciója. Az egyik per implikálja a másikat ezért „szíami” pernek nevezem ezt az eljárásmodot, és egyben a harmadik pertípust vélem benne felfedezni.

A Kritón című dialógus helyes interpretációja szempontjából döntő felismerés, hogy Platón a *graphé paranomón* eljáráshoz igazodva fejt ki Szókratész álláspontját. A gondolatkísérlet formájában lefolytatott eljárásban Kritón a törvényt vádló szerepét kapja, Szókratészre pedig a szerző a törvények védelmének képviselőjét bízta. A dialógus drámai ideje i. e. 399. július/augusztus hónap, amely a déloszi hajó útjára felépített kombináció.<sup>95</sup> Szókratészt a börtönben meglátogatja öreg gyermekkori barátja és démosztárs, hogy közölje, vele a déloszi hajó rövidesen megérkezik és Szókratésznek meg kell halnia. Menekülésre próbálja rávenni. Szókratész erre válaszolja, hogy beszéljék meg a kérést, szabad-e igazságtalanságot elkövetnie. Mi lenne, kérdezi Szókratész, ha szökés közben eléje állnának a város törvényei. Ekkor kezdődik a „hipotetikus” *graphé paranomón* eljárás. Kritón, mint vádló, Szókratész, mint védő között. A törvények érve, hogy a meghozott ítéleteknek érvényeseknek kell lenniük.<sup>96</sup> Mi a vádad ellenünk kérdezhetnék a törvények? A törvények nevében Szókratész érvel is: Mi voltunk a szülőid és felnevelőid. Nem vagyunk egyenlők. Ha mi akarunk elpusztítani te nem, teheted meg ezt velünk. Ha te igazságtalansággal vádolsz minket, akkor sem cselekedhetsz igazságtalanul.<sup>97</sup> Tudnod kell, hogy anyádnál és apádnál előrébb való a haza. Mindent meg kell tenned amit, parancsol a haza. Ha ezekkel nem értesz egyet, akkor meg kell győznöd minket arról, hogy merre található az igazság.<sup>98</sup> Az elképzelt *graphé paranomón* eljárásban a törvények további érveket hoznak fel. Mindenki választhat, hogy engedelmeskedik a törvényeknek, vagy meg kell győznie, ha valamiben rosszul rendelkezünk. Ha ez valakinek nem tetszik, mindenkinek joga

---

<sup>93</sup> I. m. p. 31.

<sup>94</sup> I. m. p. 31.

<sup>95</sup> HORVÁTH Barna: i. m.pp. 12-13.

<sup>96</sup> PLATÓN: Kritón. 50 c

<sup>97</sup> I. m. 50 c – 51 b.

<sup>98</sup> I. m. 51 b – 51 c.



van egész családjával, vagyonával elmenni.<sup>99</sup> A törvények érvei szerint Szókratész nem hagyta el a várost, csak ha katonai feladatot teljesített.<sup>100</sup> A törvények rákérdéznek, milyen lenne az életed Szókratész, ha a döntésünk után hagynád el Athént, a város akarata ellenére. Hogyan tudnál máshol erényes életet élni és hirdethetnéd-e amit eddig mindtál az igazságról, ha te magad lábbal tipornád az igazságot. Milyen lenne az életed mindezek után.<sup>101</sup> Ha így cselekednél, inkább halj meg. Így alvilági bíráid előtt megállhatnál, hogy nem követtél el igazságtalanságot.<sup>102</sup> Szókratészt ez a gondolatmenet meggyőzi arról, hogy az elképzelt eljárás során a törvények érvényben és hatályban maradnak, míg Kritón összeomlik az érvek súlya alatt és nem tud mit felhozni ellene. Valóságos *graphé paranómón* esetében Kritón képzeletbeli másik eljárása a szíami per eljárása szerint a valóságban halálbüntetést kapna.

### Összegzés

Írásom csak a külső tárgyi látszat szerint szól túlsúlyosan a jogról. A dialógusok elemzése során végig az államról beszéltem, de más dialektusban. A konferencia téziseiben felvetett kérdésekre az egyik lehetséges válasz az, hogy az államtudományt a jogtudomány művelése nélkül kielégítően nem lehetséges tanulmányozni, mert a *démiurgosz* „kísérti meg a lelket”. Az egyetem csak felsőoktatási intézmény lenne nem pedig *universitas*. Álláspontom szerint a tétel megfordítása is igaz. Mindezekre tekintettel igazat kell adnunk Szókratésznek és ügyvédként is hasonló módon „védtem volna”, mert igaz a mondása: „A vizsgálódás nélküli élet nem emberhez méltó élet”<sup>103</sup>

---

<sup>99</sup> I. m. 51 c – 52 a.

<sup>100</sup> I. m. 52 a – 53 a.

<sup>101</sup> I. m. 53 a – 54 b.

<sup>102</sup> I. m. 54 b – 54 d.

<sup>103</sup> PLATÓN: Szókratész védőbeszéde. 38 a7-8. pp. 103-104.

***Felhasznált irodalom:***

- ARISZTOTELÉSZ: Az athéni állam. Pseudo-Xenophón: Az athéni állam. Ford. RITOÓK Zsigmond. A bevezetést írta SARKADY János. Budapest, 1954, Akadémiai Kiadó, XVII. 1., 2., 4.. LVII.2- 4. pp. 115 – 117.
- HEGYI Dolores – KERTÉSZ István – NÉMETH György – SARKADY János (szerk.): A görög történelem a kezdetektől kr. e. 30-ig. Budapest, 1999, Osiris Kiadó.
- HORVÁTH Barna: A génusz pere Szókratész – Johanna. Máriabesnyő – Gödöllő, 2003, Attraktor Kiadó.
- HORVÁTH Pál (szerk.): Egyetemes jogtörténet. Budapest, 2005, Nemzeti Tankönyvkiadó.
- KAJTÁR István – HERGER Csabáné: Egyetemes állam és jogtörténet. Budapest, 2013, Dialóg Campus Kiadó.
- LACZÓ József: Az athéni állam és Szókratész pere. Budapest, 2017, Kézirat.
- LACZÓ József: Az aszebeia-istentelenségi perek statikája és dinamikája. Budapest, 2017, Kézirat.
- LACZÓ József: Egy férfi, aki nem volt ott. Budapest, 2017, Kézirat
- PLATÓN: Szókratész védőbeszéde. In Platón: Euthüphrón, Szókratész védőbeszéde, Kritón. Fordította a jegyzeteket és a kommentárt írta GELENCZEY-MIHÁLTZ Alirán (Kritón) és MOGYORÓDI Emese (Euthüphrón, Szókratész védőbeszéde). In Platón összes művei kommentárokkal. Budapest, 2005, Atlantisz, 38a7-8. pp. 103-104.



## **SZÓKRATÉSZ PERE (ATHÉN - I.E. 399.)**

### **I. RÉSZ: A POLITIKAI (1 - 3. SZAKASZ)**

**1. A PELOPONNÉSZOSZI HÁBORÚ VÉGE,  
BÉKEKÖTÉS (404)**

**2. DEMOKRATA RESTAURÁCIÓ,  
AMNESZTIA - ALKOTMÁNYREFORM (403)**

**3. HATALMI STABILIZÁCIÓ, „DÉLIA-TERV”  
(IDÉZÉS 399)**

### **II. RÉSZ: ANAKRISZISZ (4 - 8)**

#### **A. ELŐZETES ELJÁRÁS (4 - 6)**

**4. GRAPHÉ - VÁDRAT BENYÚJTÁSA, FORMAI VIZSGÁLAT**

**5. TARTALMI VIZSGÁLAT, VÁDIRAT ÁTADÁSA (KITILTÁS)**

**6. A FELEK AZ ARKHÓN BASZILEUSZ ELŐTT,  
FELHÍVÁS AZ APOLÓGIÁRA**

#### **B. ELŐKÉSZÍTŐ ELJÁRÁS (7 - 8)**

**7. A TÁRGYALÁS ELŐKÉSZÍTÉSE, APOLÓGIA,  
30 NAP A KITŰZÉSRE**

**8. A BÍRÓSÁG MEGSZERVEZÉSE, THESZMOTHÉSZEK**

### **III. RÉSZ: A TÁRGYALÁS (9 - 18)**

**9. SZAKRÁLIS TEVÉKENYSÉG, FÜSTÁLDOZAT - IMA**

- 10. A TÁRGYALÁS MEGSZERVEZÉSE, 10 BÍRÓ**
- 11. A TÁRGYALÁS MEGNYITÁSA, A HEROLD  
KIKIÁLTJA AZ ÜGYET**
- 12. A TÁRGYALÁS MEGKEZDÉSE, JEGYZŐK I  
RATFELOLVASÁSAI**
- 13. SZÓBELI TÁRGYALÁSI SZAKASZ, A VÁD - SZÓKRATÉSZ  
ELSŐ BESZÉDE**
- 14. A BÍRÓSÁG DÖNTÉSE SZÓKRATÉSZ BÜNÖSSÉGÉRŐL**
- 15. BECSLÉSI ELJÁRÁS, TIMÉTOSZ – ANTTIMÉSZISZ,  
MÁSODIK BESZÉD**
- 16. BECSLÉSI DÖNTÉS, AZ ARKHÓN HATÁROZATOT HIRDET,  
KIFOGÁS**
- 17. AZ ÍTÉLET ÍRÁSBA FOGLALÁSA, ÓVADÉK FELAJÁNLÁSA**
- 18. VÉLT SZAKRÁLIS ELEM, FÜSTÁLDOZAT, HÁLAIMA**

**IV. RÉSZ: VÉGREHAJTÁS (19 - 23)**

- 19. SZÓKRATÉSZ A BÖRTÖNBEN, ÓVADÉK ÉS KEZESSÉG**
- 20. BÖRTÖNBELI TEVÉKENYSÉG, I. A SZÖKÉS LEHETŐSÉGE  
(KRITÓN)**
- 21. BÖRTÖNBELI TEVÉKENYSÉG, II. A LÉLEKRŐL, ÍRÁSOK  
(PHAIDÓN)**
- 22. VÉGREHAJTÁS ELŐKÉSZÍTÉSE, ARKHÓNOK  
DÖNTÉSE - HALÁL NEME**
- 23. A HALÁL MEGÁLLAPÍTÁSA,  
A HAGYATÉK – IRATOK SORSA**

**DR. LACZÓ JÓZSEF**



---

## E SZÁMUNK TARTALMA

---

DR. PÁL ISTVÁN

### **NAGY-BRITANNIA OPERATÍV HELYZETE 1981-BEN**

A Belügyminisztérium (BM) III/1. Csoportfőnökség Személyzeti és Kiképzési Osztályának égisze alatt készült utolsó, Nagy-Britannia operatív helyzetét elemző tanulmány történelmi perspektívába helyezi a brit titkosszolgálatok fejlődését, valamint – a pártállami korszak utolsó két évtizedének egyfajta minimális jogszerűsége irányuló törekvésének jegyében – bemutatja az államtitkok védelmének törvényi háttérét. A tanulmányban mindvégig hangsúlyos marad a brit (polgári) hírszerző és elhárító szervek felépítésének és funkcióinak bemutatása, amely az intézkedési jogkör nyomán az egyenruhás rendőrségre is kiterjed, azonban a tényleges operatív helyzetről, a szolgálatok módszertanáról keveset olvashatunk. A Magyar Néphadsereg Vezérkara 2-es Csoportfőnöksége (MNVK 2) által írt tankönyvektől eltérően a brit fegyveres erők védelmi és felderítő szolgálatairól csak történelmi előzményként esik szó, miközben a mű – a lektori elismerés ellenére is – sok tekintetben pontatlan. A törvény paragrafusainak fordítása különösen sok kívánnivalót hagy maga után, ezért azt korrigált formában közöljük.

**Kulcsszavak:** Nagy-Britannia, hírszerzés, elhárítás, operatív helyzet.

GULYÁS ATTILA

### **KIBERHADVISELÉS ÉSZAK-KOREAI MÓDRA II.**

A Koreai Népi Demokratikus Köztársaság kiberstratégiája, és a kiberhadviselésben érintett szervezeti a tanulmány első részben már bemutatásra kerültek. A következő részben az ország fejlett kiberképességeinek demonstrálása céljából megismerkedhetünk a híres-hírhedt „Lazarus” csoporttal, illetve annak tevékenységével, valamint néhány olyan nagy nemzetközi visszhangot kiváltó művelettel, amelyeket a szakértők Észak-Koreához, illetve ehhez a hacker csoporthoz kötnek. A bemutatásra kerülő műveletek részleteinek megismerését követően valószínűleg az olvasó is osztja majd azt a széles körben elterjedt nézetet, amely szerint a Koreai Népi Demokratikus Köztársaság a kiberhadviselő országok élmezőnyébe tartozik.

**Kulcsszavak:** Észak-Korea, Koreai Népi Demokratikus Köztársaság, Lazarus, kibertámadás, Novetta, Blockbuster, Operation Flame, Operation 1.Mission, Operation troy, Dark Seoul 2013, MYDOOM, Dozer, Operation Troy, Ten days of rain, NewRomantic Cyber Army, Whols Hacking Team, Bluenoroff, SWIFT, Sony

---

## CONTENTS

---

ISTVÁN PÁL DR.

### **THE OPERATIVE SITUATION IN GREAT-BRITAIN IN 1981**

The Intelligence Directorate of the Hungarian Ministry of Internal Affairs had the last operative manual written on Great-Britain in 1981. The thesis of Dezso Takacs former scientific attaché deputed to London presented the British Secret State from a broad, but superficial perspective, often making more or less serious mistakes. Police Lieutenant-Colonel Takacs endeavored to be legalistic by the citation of the Official Secrets Act of 1911; however, even the translation proved to be largely inaccurate. Likewise, the operative situation that determines the intelligence activities is barely mentioned in the passages. The British Military intelligence structure is also missing from the picture.

**Keywords:** Great-Britain, intelligence, counter-intelligence, operative situation

ATTILA GULYÁS

### **CYBERWARFARE IN A NORTH-KOREAN WAY**

The cyber strategy of the Democratic People's Republic of Korea and the organizations involved in cyber warfare have been introduced in the first part of the study. In this part, in order to introduce the cyber capability of the country the Lazarus group and its activity is presented. Operations, which are linked to the hacker group and North-Korea are introduced. After getting familiar with the details of the massive attacks, the reader is also likely to share the opinion that the Democratic People's Republic of Korea belongs among the top cyberwarfare countries.

**Keywords:** North Korea, Democratic People's Republic of Korea, cyber attack, Lazarus, Novetta, Blockbuster, operation, Flame, Operation IMission, Operation troy, Dark Seoul 2013, MYDOOM, Dozer, Operation Troy, Ten days of rain, ewRomantic Cyber Army, Whols Hacking Team, Bluenoroff, §WIFT, Sony

DR. KOLLÁR CSABA

**A SZERVEZETI INFORMÁCIÓBIZTONSÁGI FOLYAMATOK MONITOROZÁSA ÉS A VEZETŐI DÖNTÉS TÁMOGATÁSA KULCS TELJESÍTMÉNYMUTATÓK SEGÍTSÉGÉVEL 1.**

***AZ INFORMÁCIÓBIZTONSÁG RENDSZERELMÉLETI MEGKÖZELÍTÉSE***

Tanulmányom első részének a célja, hogy teoretikus, illetve kutatási források feldolgozása révén bemutassa a szervezetek megközelítései közül a rendszerelvű megközelítést. Feltételezem ugyanis, hogy a rendszerelvű megközelítés segítségével megalapozható a szervezeti fókusz, ami révén rá lehet mutatni a(z információ)biztonsági folyamatok monitorozásának fontosságára, valamint a vezetői döntés támogatására. Ennek értelmében foglalkozom a rendszer be- és kimeneteivel (inputok és outputok), az erőforrásokkal, az erőforrások értékével, valamint állandó és változó paramétereivel. Külön részben mutatom be, hogy a szervezet, mint rendszer hogyan kezeli az erőforrásokat, milyen elvek szerint adható meg egy rendszer értéke, a rendszerek hogyan kapcsolódnak egymáshoz, illetve, hogy a rendszerben milyen visszacsatolások lehetnek. A rendszerelvű megközelítés után a(z információ)biztonság és az adatérték értelmezéseivel, valamint a szervezetek biztonsági folyamataival foglalkozom.

**Kulcsszavak:** szervezeti folyamatok, monitorozás, döntéstámogatás, teljesítménymutatók, KPI

DR. MAGYAR SÁNDOR – SIMON LÁSZLÓ

**A TERRORIZMUS ÉS INDIREKT HADVISELÉSE AZ EU KIBERTERÉBEN**

A szerzők általános rendszerszintű látásmóddal közelítik meg a terrorista cselekmények hatását, kifejezetten Európa kiberterére koncentrálva. Induktív módon európai esetekből kiindulva történik általános következtetések levonása. Az Iszlám Állam szervezete azzal fenyeget, hogy halálos kimenetelű kibertámadásokat tervez a jövőben. A terroristák új dimenzióban támadják az egyének biztonságát. A fegyveres harcuk során a gerillákhoz hasonlóan az információt helyezik a műveleteik központjába. A média szerint a terroristák harcában az információ és a kommunikáció egyszerre lehet halálos és nem halálos fegyver is. A cikk összegzése szerint az internetet fenyegetésre használó arctalan bűnözők csak indirekt módon ölthetnek ki életet. Az áldozatok védelmét az államok ugyan garantálhatják, de a kibertér felhasználói maguk is tudják növelni a biztonságérzetüket. Az információközpontú hadviselés korában a megoldást a biztonságtudatos gondolkodás és a hiteles kommunikáció jelenti.

**Kulcsszavak:** terrorizmus, kibertámadás, gerilla hadviselés, információs környezet, információ- és hálózat-centrikus hadviselés hadikultúrája



CSABA KOLLÁR DR.

**MONITORING ORGANIZATIONAL INFORMATION SECURITY PROCESSES AND SUPPORTING LEADERS' DECISION-MAKING THROUGH KEY PERFORMANCE INDICATORS 1.**  
***SYSTEM-THEORETICAL APPROACH TO INFORMATION SECURITY***

By analysing theoretical and research sources, the first part of the study aims to describe the system-based approach in order to support the organisational focus and highlight the importance of monitoring (information) security processes, as well as to prepare for the chapters about management decisions. Accordingly, the study looks into the outputs and inputs of a system, the resources and their value, and the constant and variable parameters. A separate chapter introduces how an organisation, as a system, deals with resources; what principles help to define the value of a system; how the systems are interrelated and the possible feedback types. Following the system-based approach, the study focuses on the definition of information security and data value and security processions.

**Keywords:** organizational processes, monitoring, decision support, performance indicators, KPI

SÁNDOR MAGYAR DR. – LÁSZLÓ SIMON

**THE INDIRECT WARFARE OF TERRORISM IN THE CYBERSPACE OF EU**

The authors approach the effects of terrorist attacks aimed at the cyberspace of Europe from a systematic point of view. Beginning with European cases general conclusions are made by using inductive research. According to ISIS' threat, 'fatal' cyber-attacks are planned for the future. The terrorists attack the security of individuals in a new dimension. During their armed conflict, they place information in the center of operations just like guerrillas. In the opinion of the media, information and communication can and can't be a deadly weapon at the same time in a terrorist war. According to the conclusion of the article faceless criminals using the Internet to carry out online threats, can take someone's life only in an indirect way. Although, the protection of the victims is guaranteed by the state, in cyberspace users are also able to increase their own security. The solution is conscious thinking and authentic communication in the era of information-centric warfare.

**Kulcsszavak:** terrorism, cyber-attack, guerrilla warfare, information environment, war culture of information- and network- centric warfare

ZÁMBORI RICHÁRD

### MAGYARORSZÁG ÚTJA BYTE-OKKAL VAN KIKÖVEZVE

Korunk informatikai fejlődése és a mindent behálózó internet jelensége magában hordozza azt a potenciált, amit kihasználva az Európai Unió lépéselőnyre tehet szert a vezető gazdasági hatalmak versenyében. Ennek érdekében a stratégiai tervezésben megjelentek olyan elemek, amelyek lépésről-lépésre haladva meghatározzák azokat az elérendő célokat, amelyek egymásra épüléséből létre jöhet a Digitális Európa. A Digitális Európának természetesen része a Digitális Magyarország is, amelynek a megteremtéséhez megkezdődtek a munkálatok.

**Kulcsszavak:** Digitális Európa, Digitális Magyarország, Digitális Menetrend, digitalizáció

KOVÁCS KRISZTIÁN

### HAZEN AMES TÖRTÉNETE II.

A tanulmány nyílt dokumentumok alapján mutatja Aldrich Hazen Ames volt titkosszolgálati tiszt kémtevékenységét és ezen keresztül azt, hogy az amerikai Központi Hírszerző Ügynökség (CIA) hogyan integrálta az elhárító tevékenységet a hírszerző szervezet struktúrájába. Bepillantást nyerhetünk a CIA vizsgálati eljárásrendjébe, megismerkedhetünk a szervezeti kultúrával, amelynek diszharmóniája az alkalmazott elhárító tevékenységgel, súlyos következményekkel járt. Az Ames kémügy adalékokkal szolgál a magyar katonai hírszerzés tevékenységével kapcsolatban is.

**Kulcsszavak:** elhárítás, hírszerzés, CIA, nemzetbiztonsági rendszer, Clyde Lee Conrad, Belovai István

RICHÁRD ZÁMBORI

### **PATH OF HUNGARY IS PAVED WITH BYTES**

The IT developmet of our age and the phenomenon of encompassing internet carries the potential which can be exploited by European Union to gain advantage in the competition of the world's leading economical powers. In order to do so, certain elements showed up in strategic planning that determine desired goals step by step to achieve and to create Digital Europe. Digital Hungary is obviously part of Digital Europe therefore the works have begun.

**Keywords:** Digital Europe, Digital Hungary, Digital Agenda for Europe, digitalization

KRISZTIÁN KOVÁCS

### **THE STORY OF ALDRICH HAZEN AMES, PART I.**

The study, based on open source documents, introduces the espionage activity of Aldrich Hazen Ames former intelligence officer and through his activity how the Central Intelligence Agency integrated counterintelligence activity into the structure of an intelligence agency. We can get an insight into the operational procedures and get familiar with the organizational culture, which was in disharmony with the applied counterintelligence activity. This however had serious results. The Ames case serves with interesting addition to the Hungarian military intelligence activity as well.

**Keywords:** counterintelligence, intelligence, Central Intelligence Agency (CIA), Clyde Lee Conrad, István Belovai

SZIJÁRTÓ LÍVIA

## MAGÁNYOS ELKÖVETŐK AZ INTERNETEN – AZ INTERNETES TARTALMAK PSZICHOLÓGIAI SZEMPONTÚ ELEMZÉSE

Napjainkban a magányos elkövetők megjelenése potenciális fenyegetés Európára nézve. Az ún. magányos farkasok általában egyedül radikalizálódnak – habár gyakran kapnak közvetett vagy közvetlen támogatást szélsőséges szervezetektől –, illetve a tervezett támadás előkészületei és kivitelezése során sem tartanak fent közvetlen kapcsolatot más személyekkel, csoportokkal. A személyüket érintő felderítő munka nagy hangsúlyt fektet az internetes jelenlétre, mivel a magányos elkövetők többsége aktív tagja webes fórumoknak, illetve egy részük blogot is vezet. A tartalomelemző módszerek segítségével lehetővé vált ezeknek az oldalaknak a monitorozása és pszichológiai szempontú elemzése. A tartalomelemző eljárások használata során ki lehet szűrni a radikális tartalmakat, továbbá adott esetben meghatározni a fenyegetés valós szintjét. A nemzetközi kutatásokban és a hivatásos szervek munkájában is egyre nagyobb teret nyer a tartalomelemzés mint interdiszciplináris módszer.

**Kulcsszavak:** magányos elkövetők, internetes tartalmak, felderítés, pszichológiai szempontú tartalomelemzés

DR. GYARAKI RÉKA

## A NYOMOZÓHATÓSÁG ÉS A KATASZTRÓFAVÉDELLEM FELADATA A KIBERBŰNCSELEKMÉNYEK VONATKOZÁSÁBAN

A kiberbűnözés az egyik leggyorsabban terjedő és talán az egyik legveszélyesebb bűncselekmény, amely komoly kihívásokat állít a nyomozóhatóságok és a kibervédelemmel és kiberbiztonsággal foglalkozó hatóság, így az Országos Katasztrófavédelmi Főigazgatóság elé.

A tanulmány célja, hogy a két szervezet feladatai és hatásköre tekintetében bebizonyítsam, hogy közös együttműködésük a kiberbűnözés a kiberfenyegetés ellen elengedhetetlen. A büntetőjogi tényállások – a terrorcselekmény, valamint a közérdekű üzem megzavarása – esetében a nyomozóhatóság eljárásában elengedhetetlen szerepe van a katasztrófavédelmi hatóságnak, mint ahogyan egy bekövetkezett kibertámadás esetén a károk elhárítása sem kizárólag a katasztrófavédelem feladata, hanem a rendőrség segítsége és fellépése is szükséges lehet egy esetlegesen bekövetkező veszélyhelyzet elhárítása érdekében.

**Kulcsszavak:** rendőrség, katasztrófavédelem, kibertámadás, terrorcselekmény, közérdekű üzem, kiberbűncselekmény

LÍVIA SZIJÁRTÓ

#### **LONE PERPETRATORS ON THE INTERNET – PSYCHOLOGICAL ANALYSIS OF THE INTERNET CONTENTS**

Nowadays the appearance of the lone-actor offenders is a potential threat to Europe. The so-called lone wolves usually radicalize alone – with often receiving indirect or direct support from extremist organizations – usually they are not in contact with other radical people or groups during the preparation and execution of their planned attack. Intelligence services have paid very close attention to online presence of lone actors, as most of them are active members of web forums and some of them even write blogs. These contents can be monitored and analysed with content analysis methods. With using these methods radical contents can be filtered out and if necessary the level of threat can be determined. Content analysis as an interdisciplinary method, which plays an increasingly important role in the international research and work of the intelligence services.

**Keywords:** lonely offenders, internet contents, intelligence, psychological content analysis

RÉKA GYARAKI DR.

#### **TASKS OF THE INVESTIGATIVE AUTHORITIES AND DISASTER MANAGEMENT REGARDING CYBERCRIME**

One of today's fastest expanding and probably the most dangerous criminal offences is cybercrime, which poses a challenge for the investigative bodies that handle cybercrimes – including the National Directorate General for Disaster Management. The goal of this study is to prove that the cooperation of these two authorities in fighting cybercrime and cyber threat is a must.

In criminal offences – such as terrorist acts or disturbance of public utility – the disaster management authority plays a crucial role in the procedure of the investigative authority, just as in the case of a cyber attack the aftermath is not solely the task of disaster prevention, but the help and presence of an investigative authority may also be necessary to overcome an eventual emergency.

**Keywords:** police, disaster management, cyber attack, terrorist offence, public utility, cybercrim

DR. LACZÓ JÓZSEF

## AZ ATHÉNI ÁLLAM A TIZENNEGYEDIK ALKOTMÁNYMÓDOSÍTÁS UTÁN

Tézisem szerint Szókratész tevékenysége biztonsági kockázatot jelentett a restituálódó athéni államnak. A magatartása és konfliktusa a közösséggel és az állam szerveivel, intézményeivel, tisztségviselőivel szemben többrétű, az állam integritására való kockázatként jelent meg. Az amnesztiatörvény felejtést és feloldozást hozott az i. e. 403. év előtti cselekményekre, de a filozófus ezután sem változtatott magatartásán. Cselekedetei ezért *aszebeia* perhez vezettek. A tisztségviselők, a bíróság mellett a *szükophanták* és a büntetés-végrehajtási szervek ily módon való fellépése az állam érdeke volt. Ennek bizonyítása interdiszciplináris kutatáson alapuló érvekkel és a „síkok módszerével” történt meg. Szókratész belviszály esetén egyik fél mellé sem állt, sőt, bírálta törvénytelen eljárásaikat. Lehetetlennek tartotta a közösségi életben való részvételét, mert ő tisztességesebb volt, mint a többiek. Az istenségtől kapott feladatként értelmezte a magatartását, megrögzötten, még akkor is, ha többször meg kell halnia. A tilalom ellenére az amnesztiatörvény előtti cselekedetekre hivatkozik az eljárás során, és hogy nem szabad a közélet színterére lépni, mert a közösség jogtalankodik. A jogszabályi revízió üresen hagyta az *aszebeia* törvényi tényállását, de az előítéletet nem tudta hatályon kívül helyezni. A vallás hangsúlyának eltolódásai, Szókratészre nézve, súlyos következményekkel jártak. A közösség úgy érezte, nem tiszteli a város isteneit, ahogyan a közösség, helyette valami új istenséget hoz be, amely népgyűlési hatáskör lenne. Apollón istennel tételezett személyes kapcsolata és a tőle származtatott önbeteljesítő jóslat, feladat és az ebből vállalt életmód szintén közösségi konfliktust generált. Szókratész a társas lélek szemében szofistának minősült, és módszere folytatása és alkalmazása az arisztokrata ifjak által jelentős állambiztonsági kockázatot jelentett. Ez módosította a közösségi nevelés eszményképét a szofisták és Szókratész egyéni nevelési elvei irányába, amelyre a jövő és a kibontakozás akadályát jelentő biztonsági kockázatként tekintett az athéni közösség amely érzelmi állapotát tekintve a vizsgált időszakban, túlfűtött volt. Nem volt szüksége bögölyre, hogy felébressze. Szókratész a közösség szemében centrális hazugságban van, mert nem igaz az állítása, hogy soha nem foglalkozott természetfilozófiával. Mindezekért a közösség Szókratészt „istentelennel” tételezte. Az állam, a tisztségviselők és a *szükophanták* révén, folyamatosan figyelemmel kísérte őt haláláig. Mindez nem jelenti azt, hogy Szókratészt nem szerethetjük születésének 2500. évfordulója előtt 13 évvel.

**Kulcsszavak:** Szókratész pere, athéni állam, alkotmánymódosítás, amnesztia, állambiztonsági kockázatok, *aszebeia* – istentelenség, kitiltás, esküdtbíróság, állami besúgók – *szükophanták*

JÓZSEF LACZÓ DR.

**THE ATHENIAN STATE AFTER THE FOURTEENTH  
CONSTITUTIONAL AMENDMENT**

As per my thesis, Socrates was a security liability to the restituting state of Athens. His conduct, conflicts with the community, as well as state officials were corrosive to the integrity of the state on multiple levels. The amnesty law diminished awareness and provided absolution for his actions before 403 b.c., but even after the verdict, the philosopher did not change his behavior. His actions therefore have led to asebeia proceedings. The strong reaction of officials; the court, sycophants and law enforcement was in the interest of the state. I have provided proof of this with arguments based on interdisciplinary research and the "method of planes". In events of internal strife, Socrates chose to be impartial, moreover, judged the unlawful conduct of officials. He thought himself utterly unable to participate in communal activities, because he was more decent than his peers. He considered his demeanour a duty from the deity, to the extent that he would have been willing to die multiple deaths because of it. Regardless of the ban, he referenced his pre-amnesty actions during the proceedings, as well as his thoughts that one should not appear on the public stage because of the public's deep disregard of the structurally logical word of law. The legislation revision has left the asebeia law without enforceable content, but could not tame the prejudice of the public. The shifts of the emphases of religion had dire consequences for Socrates. The community felt like he did not respect the deities of the city, but instead introduced a new deity, which would have been in the jurisdiction of the assembly. His reckoned personal connection with Apollo, the self-fulfilling prophecy credited to him, the mission and the lifestyle derived from this connection have also led to public conflicts. Socrates was perceived a sophist by the collective. Continuation and implementation of his method by the young of Athens was a cumulative state-wide security risk. This brought the paragon of communal education closer to the particular schooling disciplines of the sophists and Socrates, which effect also cumulated, and manifested in the perception of the people of Athens - whose emotional state could be described as exalted - as a security risk and obstacle for their future and development. Socrates did not need a gadfly to be upset. In the community's eyes he was in a central lie, because his statement of him never having practiced natural philosophy has been proven false. For these reasons, the community labeled him "godless". The state, through officials and sycophants, monitored him until his death. But, all this does not mean that we cannot admire him 13 years before the 2500th anniversary of his birth.

**Keywords:** trial of Socrates, Athenian State, constitutional amendment, amnesty, state security risks, *asebeia* (impiety/godlessness), ban, jury, state informers - sycophants)

---

## SZERZŐINK

---

<b>Gulyás Attila</b>	ny. alezredes
<b>Dr. Gyaraki Réka</b>	őrnagy, Nemzeti Közszolgálati Egyetem Rendészettudományi Kar Magánbiztonsági és Önkormányzati Rendészeti Tanszék, tanársegéd
<b>Kovács Krisztián</b>	alezredes, a KNBSZ munkatársa
<b>Dr. Laczó József</b>	Eötvös Lóránd Tudományegyetem Állam- és Jogtudományi Doktori Iskola doktorandusz hallgató
<b>Dr. Pál István</b>	PhD, Eötvös Lóránd Tudományegyetem Történelemtudományi Doktori Iskola témavezető
<b>Szijártó Livia</b>	Nemzeti Közszolgálati Egyetem Hadtudományi Doktori iskola doktorjelölt
<b>Zámbori Richárd</b>	százados, szakértő
<b>Dr. Kollár Csaba</b>	PhD, Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola témavezető
<b>Dr. Magyar Sándor</b>	ezredes, PhD, NKE NBI Katonai Nemzetbiztonsági Tanszék, adjunktus, a KNBSZ munkatársa
<b>Simon László</b>	alezredes, NKE NBI Katonai Nemzetbiztonsági Tanszék és a KNBSZ munkatársa



---

## E SZÁMUNKAT LEKTORÁLTÁK

---

<b>Árpád Zoltán</b>	ezredes, a KNBSZ munkatársa
<b>Prof. em. Dr. Bolgár Judit</b>	ny. ezredes, CSc, Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar, egyetemi tanár
<b>Fülöp Imre</b>	ezredes, a KNBSZ munkatársa
<b>Dr. Fürjes János Norbert</b>	alezredes, PhD NKE NBI Katonai Nemzetbiztonsági Tanszék és a KNBSZ munkatársa
<b>Dr. Hódos László</b>	százados, a KNBSZ munkatársa
<b>Dr. Kassai Károly</b>	ezredes, PhD, a KNBSZ munkatársa
<b>Dr. Kenedli Tamás</b>	ezredes, PhD, NKE NBI Katonai Nemzetbiztonsági Tanszék és a KNBSZ munkatársa
<b>Prof. Dr. Cs. Kiss Lajos</b>	CSc, a tudományok kandidátusa, az NKE Államtudományi és Közigazgatástudományi Kar, kutatóprofesszor
<b>Dr. Magyar Sándor</b>	ezredes, PhD, NKE NBI Katonai Nemzetbiztonsági Tanszék, adjunktus, a KNBSZ munkatársa
<b>Dr. Sabjanics István</b>	főhadnagy, PPKE JÁK Nemzetközi Közjog Tanszék, tudományos segédmunkatárs, a KNBSZ munkatársa
<b>Simon László</b>	alezredes, NKE NBI Katonai Nemzetbiztonsági Tanszék és a KNBSZ munkatársa
<b>Szabó Károly</b>	ezredes, NKE NBI Katonai Nemzetbiztonsági Tanszék és a KNBSZ munkatársa
<b>Tóth Csaba Mihály</b>	alezredes, a KNBSZ munkatársa

## A SZAKMAI SZEMLÉBEN TÖRTÉNŐ PUBLIKÁLÁS FELTÉTELEI

### Az írásművekkel szemben támasztott követelmények

#### *Etikai követelmények:*

- az írásmű másol, ebben a formájában még nem jelent meg;
- a szerző(k) kizárólagos szellemi tulajdona, melyet szerzői nyilatkozat aláírásával igazol(nak);
- korrekt, visszakereshető hivatkozásokkal ellátott;
- bibliográfiával ellátott (amely tartalmazza a hivatkozott irodalom jegyzékét, az internetes anyagok jegyzékét a letöltés idejével együtt);
- a szerző(k) saját véleményét is tükrözheti, mely értelemszerűen nem mindig egyezik meg a Szolgálat álláspontjával.

#### *Tartalmi követelmények:*

- a folyóiratokban – jellegével összhangban – a honvédelemmel, azon belül elsősorban a hadtudománnyal, nemzetbiztonsággal, hírszerzéssel, felderítéssel, katonai biztonsággal és a biztonságpolitikával kapcsolatos tudományos igényű kérdéseket feldolgozó és elemző írásokat – tanulmányokat, cikkeket és más tudományos területetémáit, anyagait – jelentjük meg;
- az írásmű legyen logikus, áttekinthető, tartalmilag összefüggő és jól tagolt;
- a témával kapcsolatos saját koncepció megfogalmazása legyen érthető, a következtetések pedig megalapozottak, érvekkel, adatokkal alátámasztottak legyenek.

#### *Formai követelmények*(és a kapcsolódó információk):

- a szerzői kéziratok terjedelme lehetőleg ne haladja meg az egy szerzői ívet (40 ezer karakter, illetve 20-21 gépelt oldal); a kéziratot elektronikus formában Times New Roman 12 pontos betűvel, másfeles sortávolsággal írva, a képeket és ábrákat feldolgozható (.jpg vagy .tif) formátumban kérjük megküldeni;
- lehetőség van a kézirat interneten történő megküldésére is, a [szakmaiszemle.kontakt@gmail.com](mailto:szakmaiszemle.kontakt@gmail.com) e-mail címen. A kézirathoz kérjük mellékelni a szerző vagy szerzők nevét, rendfokozatát, beosztását vagy munkakörét, állandó lakcímét, telefonon és interneten történő elérhetőségét;
- a közlésre elfogadott írásokért – a szerzői nyilatkozattal létrejött megállapodás figyelembe vételével – szerzői honorárium fizethető;
- a kéziratokat a Szerkesztőbizottság minden esetben lektoráltatja. A kiadványban megjelentetni kívánt írásokat a Szolgálat kompetens, tudományos fokozattal rendelkező munkatársai vagy más szakértők lektorálják;
- a Szerkesztőbizottság – a lektori vélemények figyelembevételével – fenntartja a jogot, hogy a megjelenésre alkalmatlannak ítélt kéziratokat – indokolás nélkül – nem közli. Az ilyen írásokat nem küldi vissza és nem őrzi meg;

- a kiadványban bárki publikálhat, akinek az írását a Szerkesztőbizottság az etikai, tartalmi és formai követelmények alapján, kiadványban történő megjelenítésre, valamint az interneten történő közzétételre alkalmasnak tartja. A közlésre nem került kéziratot csak az adott naptári év végéig őrizzük meg, de a szerző kérésére azt visszaadjuk;
- a közleményhez „Absztraktot/Rezümét” kell mellékelni, maximum 10–12 sorban, magyar és angol nyelven;
- a közleményhez 3–5 kulcsszó megadása szükséges, magyar és angol nyelven;
- az írás angol nyelvű címét is kérjük megküldeni.

#### ***Tudományos közleményekkel szemben támasztott formai követelmények***

A folyóirat kizárólag az MSZ ISO 960 szabvány alapján készített hivatkozásokkal ellátott tanulmányt, cikket jelentet meg.

*A közleményhez szükséges megadni, mellékelni:*

A SZERZŐ, SZERZŐK NEVE (rendfokozata)  
 AZ ÍRÁS CÍME (magyarul, angolul)  
 ABSZTRAKT/REZÜMÉ (magyarul, angolul)  
 KULCSSZAVAK (magyarul, angolul)  
 SZERZŐI NYILATKOZAT

#### ***Bibliográfiai hivatkozás***

A társadalomtudományokban a megszokott számozott hivatkozást az idézések jegyzetben<sup>1</sup> módszerrel kérjük alkalmazni.

Abban az esetben, ha a szerző nem ezt a módszert alkalmazza, a kéziratot lektorálás nélkül visszaküldjük átdolgozásra!

#### ***Idézetek jegyzetben***

A szövegen belüli idézést követően felső indexként megadott sorszámok jegyzetekre utalnak, melyeket a szövegbeli megjelenésük sorrendjében kell közölni. Ezek a jegyzetek tartalmazhatják az idézéseket.

#### ***Első idézés***

*Ha az idézések jegyzetben vannak megadva, egy dokumentumra vonatkozó első idézésnek tartalmaznia kell az idézés és a bibliográfiai hivatkozások külön jegyzékében levő kapcsolódó tétel pontos megfeleltetéséhez szükséges adatokat. Az első idézésnek tartalmazni kell: legalább a szerző(k) nevét és a teljes címet úgy, ahogy azok a bibliográfiai hivatkozásokban meg vannak adva, továbbá az idézett rész oldalszámát, ha az szükséges.*

---

<sup>1</sup> Bibliográfiai hivatkozások. Magyar Szabvány, MSZ ISO 690. pp. 19-20.

Példák:

TARJÁN G. Gábor: A terrorizmus, p. 4.  
KECSKEMÉTI Klára: A mediterrán térség és az Európai Unió, Európai Tükör, 2010. május XV. évfolyam 5. szám p. 38.  
J. Nagy László: Mit kell tudni Algériáról?, Kossuth Kiadó, Budapest, 1987. p. 46-47.  
PRYCE, Paul: France's Long War: Operation Barkhane, <http://natoconcil.ca/frances-long-war-operation-barkhane/> (Letöltés ideje: 2015.02.24.),  
Global Trend 2020: Mappingthe Global Future, <http://www.foia.cia.gov/2020/2020.pdf> (Letöltés ideje: 2012.08.21.),

### ***Bibliográfiai hivatkozások jegyzéke***

A bibliográfiai hivatkozások jegyzékében a hivatkozásokat az első adatelem betűrendjében kérjük megadni.<sup>2</sup>

Példák:

ÁCS Tibor: A reformkor hadikultúrájáról, *Budapest, 2005, Zrínyi Kiadó. ISBN 963 9276 45 6*  
BEREK Lajos: A hadtudományi kutatómunka alapjai, In: SZILÁGYI Tivadar (szerk.): Szemelvények, Budapest, 1994, Zrínyi Miklós Katonai Akadémia. pp. 31–50.  
KOVÁCS Jenő: Az új magyar hadtudomány gyökerei, fejlődésének szemléleti problémái, In: Új Honvédségi Szemle, 1993. 47. évf. 6. sz. pp. 1–7. ISSN 1216-7436  
Global Trend 2020: Mappingthe Global Future, <http://www.foia.cia.gov/2020/2020.pdf> (Letöltés ideje: 2012.08.21.),

### ***Ábra, vázlat, térkép, diagram, egyéb melléklettel szembeni követelmények:***

- az ábra, vázlat címe;
- az ábra, vázlat forrás (vagy: Szerkesztette: ...);
- az ábra, vázlat sorszáma (pl. 1. ábra.);
- idegen nyelvű ábra, vázlat esetén lehetőség szerint magyar nyelvű jelmagyarázat.

### ***Rövidítések, idegen kifejezésekkel kapcsolatos követelmények:***

- az idegen kifejezéseket, rövidítéseket magyarul és eredeti idegen nyelven kell az írásműben az első alkalommal feloldani lábjegyzetben;

Példa:

- WFP – (World Food Program – ENSZ Világélelmezési Programja).

**SZERKESZTŐBIZOTTSÁG**

---

<sup>2</sup> Bibliográfiai hivatkozások. Magyar Szabvány, MSZ ISO 690. p. 18.

