

DR. KOVÁCS LÁSZLÓ mk. őrnagy

**EGY KUTATÁS MARGÓJÁRA:
A TERRORIZMUS ELLENI HARC
NEMZETBIZTONSÁGI FELADATAI
MAGYARORSZÁG
INFORMÁCIÓS TÁRSADALMÁNAK
KIÉPÍTÉSE SORÁN**

Jelen írás a 2005 és 2008 között elnyert Magyar Tudományos Akadémia Bolyai János Kutatási Ösztöndíj támogatásával elvégzett munkát mutatja be nagy vonalakban.

This paper outlines my research work which was supported by the Hungarian Academy of Sciences János Bolyai Research Scholarship between 2005 and 2008.

2005 és 2008 között három éves időtartamra elnyertem a Magyar Tudományos Akadémia Bolyai János Kutatási Ösztöndíját. Az Akadémia célja ezzel az ösztöndíjjal „*Tudományos munka megírásának vagy azzal egyenértékű kutatási témában létrehozott alkotás elkészítésének, valamint az MTA doktora cím elnyerésére való felkészülés elősegítése. Pályázat nyújtható be valamennyi tudományterületen, illetőleg tudományágban.*” [1]

Az ösztöndíjra az pályázhat, aki PhD, illetve azzal egyenértékű tudományos fokozattal rendelkezik a pályázat benyújtásakor, a pályázat benyújtási határidejének időpontjáig a 45. életévét még nem töltötte be, kutatásait magyarországi tudományos intézményben (felsőoktatási intézményben, akadémiai kutatóintézetben, egyéb tudományos kutatóhelyen) kívánja végezni, és ehhez az intézmény fogadókészségéről szóló nyilatkozattal rendelkezik, illetve magyar állampolgár.

Az ösztöndíj határozott időre – egy, kettő illetve három évre – pályázható. A pályázat benyújtásához egy kutatási tervet kell készíteni, amelyben a pályázó felvázolja mindazokat a célokat és várható eredményeket, amelyeket az ösztöndíj időszaka alatt el kíván végezni, illetve, amelyet el kíván érni.

Az általam 2005-ben benyújtott kutatómunka címe: A terrorizmus elleni harc nemzetbiztonsági feladatai Magyarország információs társadalmának kiépítése során.

Kutatómunkám előzményei közel 10 évre nyúlnak vissza. A Zrínyi Miklós Nemzetvédelmi Egyetem Elektronikai Hadviselés Tanszéke 1998-ban kezdett kutatásokat az információs társadalom kialakulását, az azt fenyegető veszélyeket, illetve ezek újfajta hadügyi vonatkozásait érintve. A kutatócsoport tagjaként aktívan részt vettem a tudományos kutatásban, illetve az ennek eredményeként megszületett — a Miniszterelnöki Hivatal pályázatán nyertes — tanulmány elkészítésében. Az információs társadalom veszélyforrásai. A kormányzat szerepe a védelem és ellentevékenység műszaki és szervezeti megoldásaiban című tanulmányban [2] azokat a technikai jellegű veszélyforrásokat elemeztem és összegeztem, amely napjainkban, illetve a 21. században az információs társadalom kialakulását, vagy rendeltetészerű működését veszélyeztetik. A tanulmányt egy multimédiás CD-ROM megalkotása, illetve szakmai szimpózium követte, ahol szintén a témában végzett kutatásaink eredményeit ismertettük.

Mindezek után a doktori (PhD) értekezésemben folytattam ezen kérdések egy részének kutatását, amely azokat az új típusú veszélyeket és kihívásokat elemezte, amelyekkel napjainkban — akár a Magyar Köztársaságnak is — az információs társadalom kiépítése során szembe kell néznie. [3]

Az értekezés megírását követően tovább folytattam a kutatásaimat, amelyekben már fókuszáltan a terrorizmus, illetve az információs társadalmat fenyegető veszélyeket közösen, ezeket a tényezőket mintegy újfajta, az eddigieknél sokkal nagyobb kihívásként és veszélyként állítottam a kutatásaim középpontjába. E kutatásaim eredményeit a Verlag és Dashöfer Szakkiadó által kiadott Informatikai biztonság kézikönyvben az Egy informatikai támadás forgatókönyve címmel külön esettanulmányban foglaltam össze 2003-ban. [4]

A terrorizmus újfajta eszközeinek és módszereinek megjelenését az információs társadalomban témát tovább kutatva meghívást kaptam A nemzetközi terrorizmus elleni küzdelem időszerű társadalmi, katonai és rendvédelmi kérdései című tudományos szakmai konferenciára (2004. november 11.), ahol Információs terrorizmus címmel megtartott előadásomban ismertettem az addig elért kutatási eredményeimet.

Ezeket az előzményeket figyelembe véve írtam meg pályázatomat a Bolyai Ösztöndíjra. A pályázatban megfogalmaztam az ösztöndíj időszaka

alatt tervezett kutatások célkitűzéseit. Célom volt feltárni azokat a kritikus pontokat, amelyeken keresztül a terrorizmus potenciálisan veszélyezteti a 21. század társadalmának egy részét vagy akár annak egészét. Mindezeket túl további célként jelöltem meg, hogy feltárjam és elemezzem azokat az eszközöket és eljárásokat, amelyeket a Magyar Köztársaság esetében terrorista csoportok vagy személyek hazánk információs infrastruktúrája, vagy információs rendszerei ellen alkalmazhatnak, majd ezt követően meghatározom azokat a lehetséges információs technikai eszközöket, eljárásokat valamint szervezeti megoldásokat, amelyekkel eredményesen fel lehet készülni, vagy amelyekkel védekezni lehet e támadások ellen.

Kutatómunkám végső célja az volt, hogy tudományos kutatásokkal igazolt kiinduló alapot — a legsérülékenyebb infrastruktúrák megjelölését, a potenciálisan támadható szervezetek, vagy technikai eszközök feltárását, a civil információs társadalmat leginkább fenyegető terrorista támadásokat, illetve mindezek ellen való védekezés módszereit, eljárásait felsorolva — szolgáltatassak egy olyan társadalmi együttműködés kialakításához, amelybe a kormányzati és önkormányzati szervek, illetve a gazdasági tevékenységet folytató vállalatok, valamint a civil szervezetek felkészülhetnek arra, hogy együtt, közösen csökkentsék a lehető legminimálisabbra az információs kor terrorizmusának veszélyeit, illetve közösen készüljenek fel egy esetlegesen bekövetkező ilyen támadás következményeinek minimalizálására, felszámolására.

Ugyanakkor célom volt az elért kutatási eredmények egyetemi jegyzetekbe, illetve tananyagba való átültetése és megjelentetése is.

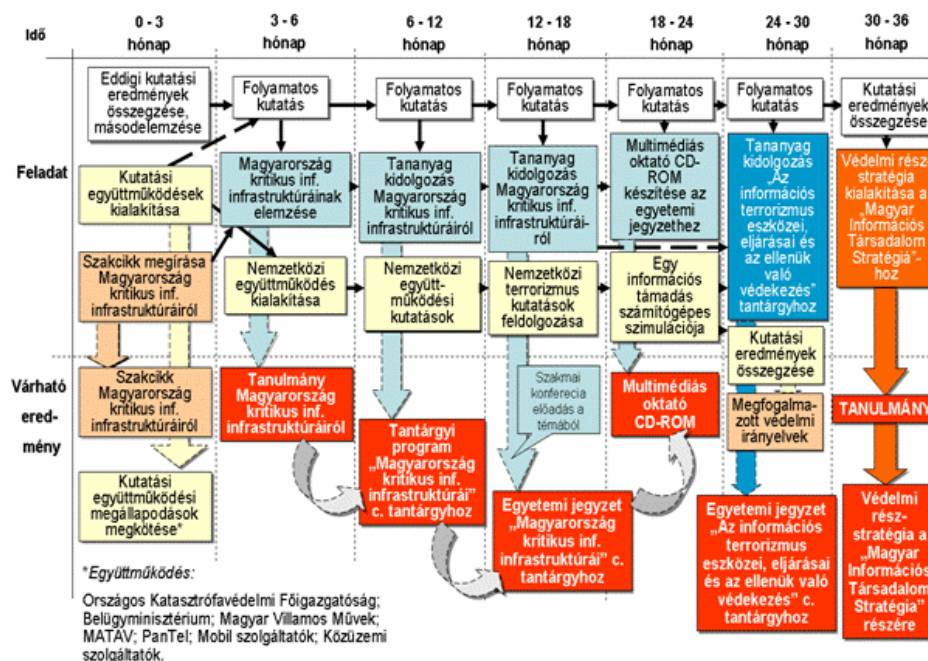
A tervezett kutatómunka módszerei a következők voltak:

- folyamatos szakirodalmi kutatás;
- kutatások másodelemzése;
- kritikai adaptáció;
- szimuláció;
- szintézis;
- hatáselemzés;
- tudományos szakmai konferenciák, szakmai viták során az eredmények szakmai megmértetése.

A kutatómunka műveleteit és időbeli elosztását mutatja be az 1. számú ábra. Miután elnyertem az ösztöndíjat a benyújtott tervet szem előtt tartva elkezdtem, illetve az előzményeket is figyelembe véve, folytattam a kutatómunkát. Az ösztöndíj három éve alatt lehetőségem volt megvizsgálni

azokat a kritikus pontokat, amelyeken keresztül a terrorizmus potenciálisan veszélyezteti a 21. század társadalmát.

Munkám során feltártam, majd elemeztem azokat az eszközöket és eljárásokat, amelyeket a Magyar Köztársaság esetében terrorista csoportok vagy személyek hazánk információs infrastruktúrája, vagy információs rendszerei ellen alkalmazhatnak. Magyarország információs infrastruktúrájának vizsgálata során meghatároztam azokat a rendszereket, amelyek hazánk kritikus információs infrastruktúráinak tekinthetők.



1. ábra
A kutatómunka műveletei és időbeli elosztása

Elemézve a potenciális — az információs térből érkező — veszélyeket, ezeket összevetve a feltárt kritikus információs rendszerekkel, javaslatot tettem olyan kormányzati lépések megtételére, amelyek lehetővé teszik a felkészülést a kritikus információs infrastruktúrák lehető legmagasabb szintű védelme megteremtése érdekében.

E javasolt kormányzati feladatok a következők (ezeket természetesen publikálásra kerültek):

- meg kell határozni a kritikus információs infrastruktúra hazai fogalmát;
- az ágazati kritikus infrastruktúrák mellett meg kell határozni azokat az elemeket, amelyek kritikus információs infrastruktúráként jelentkeznek;
- fel kell tárni a hazai a kritikus információs infrastruktúrákat fenyegető konkrét veszélyeket;
- elemezni kell, hogy a feltárt veszélyforrások közül, melyik és milyen mértékben érinti a meghatározott kritikus információs infrastruktúrákat, illetve azok egyes elemeit;
- konkrét szimulációkat kell tervezni és szervezni az információs infrastruktúrák körében, amelyek alapján fel lehet tárni azokat a pontokat, kulcsfontosságú elemeket, amelyek a gazdaság, a társadalom és a kormányzat szempontjából létfontosságúak;
- meg kell határozni, és fel kell térképezni a hazai információs infrastruktúrák egymásra, illetve a kritikus infrastruktúrákra gyakorolt közvetlen és közvetett hatásait;
- meg kell határozni, és fel kell térképezni a hazai információs infrastruktúrák környező országok infrastruktúráira gyakorolt hatását;¹
- a kormányzati koordináló szerv feladatait és résztvevőit ki kell egészíteni a kritikus információs infrastruktúra tulajdonosainak, üzemeltetőinek, illetve a hazai CERT-ek képviselőivel;
- meg kell vizsgálni, hogy alkalmas-e egy esetleges terrortámadás esetén a hazai információs és kommunikációs infrastruktúra a riasztás és a jelzés, majd a vészhelyzeti kommunikáció menedzselésére;
- a tudatos és biztonságos internet-, illetve infokommunikációs eszközhasználatának oktatása, az erre való lakossági felkészítés az eddiginél hatékonyabb és nagyobb szerepet kell, hogy kapjon. [5]

Kutatómunkám során formális és informális kapcsolatokat alakítottam ki hazai és nemzetközi — a kritikus infrastruktúrák és kritikus információs infrastruktúrák védelme területén dolgozó — szervezetekkel, kutató intézetekkel és kutatókkal (pl. EU ENISA, NATO SPS, MeH EKK, OKF, Rendőrség, BMGE, ITTK, SZTAKI). E kapcsolatok révén többször tartottam előadásokat, szakmai vitákat a témában különböző szervezeteknél, kutató-

¹ Ezt a feladatot előírja az Európai Bizottság 9403/08-as, az európai kritikus infrastruktúra azonosításáról és megjelöléséről, és azok védelmének növeléséről szóló határozata is. [16]

helyeken, egyetemeken. Többek között e kapcsolatok tették lehetővé, hogy a 2007 novemberében megrendezett Robothadviselés 7. tudományos konferencia egyik szervezőjeként, az információbiztonsággal foglalkozó hazai vezető szakembereket előadások megtartására kérjük fel.

Kutatási eredményeimet folyamatosan — számosat a párhuzamos kutatásokat folytató kollégáimmal közösen — publikáltam. Ennek eredményeként megjelent 5 cikk szerkesztett könyvben, 3 cikk tudományos folyóiratban, 8 cikk különböző konferencia kiadványokban. Kutatásaim eredményeire alapozva elkészítettem kettő egyetemi jegyzetet — Kritikus információs infrastruktúrák [6]; valamint Az információs terrorizmus eszköztára [7] címmel —, illetve egy multimédiás oktató CD-ROM-ot a Kritikus információs infrastruktúrák egyetemi jegyzethez.

A jegyzetek a ZMNE új gyakorlatának megfelelően CD-n, elektronikusan jelennek meg. Ezekben a jegyzetekben természetesen jelen vannak a publikációkban ismertetett tények, vizsgálati és kutatási eredmények.

A kritikus információs infrastruktúrák, illetve a cyberterrorizmus iránt élénk és egyre fokozódó médiaérdeklődés tapasztalható, amely során több nyilatkozatot, interjút, valamint cikkekhez szakértői véleményt kértek a kutatásaimmal kapcsolatban (pl. HVG online, [Origo], Hír TV, MR1 Kosuth Rádió).

Kutatásaim eredményeit megjelentettem és beépítettem az egyetemi oktatásba és a doktori képzésbe is. Az egyetemi (MSc) oktatásban két új tantárgyat indítottam Védelmi vezetéstechnikai rendszerek védelmének szervezése, és Számítógépes hálózati támadások címmel.

A doktori képzésben két új tantárgy tematikáját dolgoztam ki Információs terrorizmus, valamint Kritikus információs infrastruktúrák címmel, amelyeket a ZMNE Katonai Műszaki Doktori Iskola befogadott, és amelyeknek oktatását megkezdtem.

Összességében elmondhatom, hogy a kutatásaim során elért eredmények — az információs veszélyek feltárása, Magyarország kritikus információs infrastruktúráinak meghatározása, és javaslatok a kormányzati feladatok végrehajtására —, illetve a különböző fórumokon tartott előadások, bemutatók és konferenciarendezés, a megjelentetett publikációk, egyetemi jegyzetek, ha szerény mértékben is, de hozzájárultak ahhoz, hogy az információbiztonság terén meghatározó elméleti és gyakorlati ismeretekkel megalapozott kutató- és oktató hely jöjjön létre a Nemzetvédelmi Egyetemen.

Természetesen e munkához kollégáim, kutató és oktató társaim igen nagy segítsége és párhuzamos kutatómunkája is kellett, akiknek ehelyütt is köszönetet kell mondanom.

Külön köszönetet kívánok mondani a Magyar Tudományos Akadémiának, amiért a Bolyai János Kutatási Ösztöndíjjal lehetővé tették kutatómunkám elvégzését!

Felhasznált irodalom

- [1] Az MTA Bolyai János Kutatási Ösztöndíj pályázati felhívása.
<http://mta.hu/index.php?id=504> (2009.02.15.)
- [2] Prof. Dr. Makkay Imre mk. ezds.–Dr. Seebauer Imre–Dr. Haig Zsolt–
Dr. Vass Sándor–Ványa László–Kovács László: Az információs
társadalom veszélyforrásai. A kormányzat szerepe a védelem és
ellentevékenység műszaki és szervezeti megoldásaiban. Tanulmány
a Miniszterelnöki Hivatal számára, Budapest, 2002.
- [3] Kovács László: Az elektronikai felderítés korszerű eszközei, rendszerei
és azok alkalmazhatósága a Magyar Honvédségben. Doktori (PhD)
értekezés. ZMNE, Budapest, 2004.
- [4] Kovács László: Egy informatikai támadás forgatókönyve
(esettanulmány). Az informatikai biztonság kézikönyve. Verlag
Dashöfer Szakkiadó Kft. és T. Bt. Budapest, 2003. 3. rész 6.1. fejezet.
1-25. oldal. ISBN 963 9313 12 2
- [5] Kovács László: Az információs terrorizmus elleni tevékenység
kormányzati feladatai. HADMÉRNÖK on-line tudományos lap,
2008. június, ISSN 1788-1919
http://www.zmne.hu/hadmernok/2008_2_kovacsl.php
- [6] Kovács László: Kritikus információs infrastruktúrák, Egyetemi jegyzet.
ZMNE, 2007.
- [7] Kovács László: Az információs terrorizmus eszköztára.
Egyetemi jegyzet. ZMNE, Budapest, 2008.