Kovács László [1]

A tudomány rögös útján: a múlt és a jövő kutatása

Inspiráció, amely a tudomány rögös útján elindít

Katonai főiskolás hallgatóként, készülve a nagybetűs életre és nem utolsósorban a katonatiszti hivatásra M. Szabó Miklós altábornaggyal, aki akkor még vezérőrnagyi rendfokozatot viselt, a Bolyai János Katonai Műszaki Főiskolán (a továbbiakban: Főiskola) találkoztam először. Máig maradandó élményem ebből az időszakból ez egyik fordított nap, nevezetesen az a hallgatók számára különösen fontos nap, amikor az oktatók helyett ők kapják meg, ha csak néhány órára is, azt a megtisztelő lehetőséget, hogy „vezessék" az adott intézményt. Ezen a tavaszi napon M. Szabó Miklós tábornok, a Főiskola parancsnoka vezetőtársaival és kollégáival olyan – mai szóhasználattal élve *standup* – előadást tartott, amely során az intézmény jelen lévő hallgatói gurultak a nevetéstől. Ez nemcsak hogy szokatlan volt, hanem korábban teljesen elképzelhetetlennek tűnt. Évekkel, sőt évtizedekkel később, már én is tábornokként, felidéztem Miklósnak (csak így lehetett szólítani, ugyanis megfenyegetett, ha altábornagy úrnak szólítom, akkor soha többé nem áll velem szóba) ezt az esetet, és Miklós a legapróbb részletekig emlékezett az említett fordított napra, valamint nagy sikerű fellépésükre, sőt még ki is javította az emlékezetemet, amelyben néhány részlet már homályba veszett.

M. Szabó Miklós egyénisége, tábornoki tartása, a szó legjobb értelmében vett tudóshoz méltó precizitása a későbbiek során is meghatározó volt számomra. Miklós akadémikusként, ráadásul a hadtudományok kiemelkedő tudósaként olyan ikont jelenített meg, akit valóban példaképnek tekintett számos fiatal kutató, köztük én is. Miklós közismerten fanyar humora szintén legendás volt. Egyik elhíresült humoros mondása pont a tudomány rögös útjára lépő, ott az első lépéseket még csak megtevő fiatal kutatók irányában hangzott el gyakran.

[1] Dandártábornok; egyetemi tanár, NKE HHK Elektronikai Hadviselés Tanszék; kibervédelmi haderőnemi szemlélő, Magyar Honvédség Parancsnoksága; az MTA doktora.

A PhD- avagy doktori védést épphogy csak túlélt fiatal tudóspalánták, akik úgy érezték, hogy már letettek valamit a tudomány asztalára, a védés után a következő útravalót kapták Miklóstól:

> „Szép volt, gratulálok ifjú kolléga, de nehogy azt higgye, hogy ez az út vége. Ez a tudományok és a tudományos kutatások útján csak az első lépés, az első lépcsőfok. A következő állomás az akadémiai doktori cím, majd az akadémiai tagság!"

Bevallom őszintén, ez a mondata engem is elgondolkodtatott kissé, és akkor azt gondoltam, hogy sem érdemes nem vagyok rá, sem képes, és talán soha nem is fogom elérni az akadémiai doktori címet.

A sors kegyeltjeként azonban azt kell mondanom, hogy bár nem kevés munkával és küzdelemmel, de végül is sikerült elérni az MTA doktora címet, ráadásul MTA-doktori értekezésem védése során a bírálóbizottság elnöke M. Szabó Miklós akadémikus úr volt. Megtiszteltetés volt mellette ülni az MTA IX. Gazdaság- és Jogtudományok Osztályának ülésein, amelyek rendszerint az Akadémia Elnöki Tanácstermében voltak. Nagyon jó volt látni és érezni is, hogy a hadtudomány akadémikusa nemcsak népszerű az akadémikusok körében, hanem érezhető tisztelet is övezi.

A következő meghatározó találkozás M. Szabó Miklóssal már egyetemi hallgató koromban volt 1997-ben. Miklós ekkor már a Zrínyi Miklós Nemzetvédelmi Egyetem rektora volt. Rektorként nemcsak az egyetem ügyeit igazgatta, hanem a hadtörténelem neves kutatójaként oktatott is. Oktatási tevékenysége meghatározó élmény volt számomra. Miklós hadtörténelem-órát tartott nekünk, és természetesen legfőbb kutatási témája volt az aktuális tananyag. Ez nem más volt, mint a II. világháború, illetve az azt megelőző időszak magyar királyi Honvédségének légiereje.

Ugyanakkor Miklós nemcsak a történések és azok összefüggéseinek átadására törekedett, hanem nagyon gyakran kitért azokra a tudományos kutatási módszerekre is, amelyeket ő is alkalmazott kutatásai során.

A tudományos kutatás rögös, azaz néhol egészen sima, néhol azonban különösen nehezen járható útján nagyon sok segítséget adnak az olyan példaképek, mint amilyet M. Szabó Miklós jelentett.

Ez a fajta inspiráció elengedhetetlenül szükséges nemcsak a tudományos kutatásokkal még csak ismerkedő doktorandusz vagy fiatal kutató, hanem már a tudományos fokozattal rendelkező vagy akár tudományos cím birtokosa számára is. Ebben az inspirációban kiemelkedő szerepet játszanak az olyan intézményesített ösztönzők is, mint amilyet például a Magyar Tudományos Akadémia Bolyai János Kutatási Ösztöndíja jelent. M. Szabó Miklós hosszú éveken keresztül a Bolyai-ösztöndíj kuratóriumi

tagjaként, illetve az MTA Doktori Tanácsának társelnökeként nagyon sokat tett az ösztöndíj népszerűsítéséért, illetve azért, hogy a hadtudomány területéről megfelelően magas színvonalú kutatási terveket támogassanak.

Úton a jövő felé, avagy lehet-e a jövőt kutatni a múlt ismerete nélkül?

Tudományos kutatómunkám során a doktori (PhD-) fokozat megszerzése után közvetlenül a kiberbiztonság technikai kihívásait, az infokommunikációs rendszereket és eszközöket fenyegető veszélyeket, valamint az ellenük való védekezés lehetséges módszereit vizsgáltam.

Akkori kutatásaim fő fókuszában a nemzeti biztonság és annak legmagasabb szintre történő növelésének lehetséges módjai álltak, az említett kibertechnikai kérdések vizsgálatával. Ennek során olyan problémákat vizsgáltam, mint a kiberterrorizmus vagy a kiberhadviselés. Elnyerve az MTA Bolyai János Kutatási Ösztöndíjat kiemelt kutatásokat folytathattam a terrorizmus kibertéri megjelenésével összefüggésben. Ennek során több olyan tudományos probléma merült fel, amely nemcsak itthon, de a nemzetközi kutatások során is kiemelt figyelmet kapott. Az olyan kérdések többek között, mint a terrorizmus és az információtechnológia kapcsolatának vizsgálata vagy azoknak az eszközöknek és megoldásoknak az azonosítása, amelyekkel a terrorizmus a kibertérben hatékonyan tud terrorakciókat tervezni, szervezni és kivitelezni, mindegyike önmagában is hatalmas és szerteágazó téma.[2]

Ezeknek a tudományos életben akkor még meglehetősen szokatlan területeknek a kutatására több kollégával együttesen vállalkoztunk. A kutató kollégák jelentős része M. Szabó Miklós szellemi örökségét hordozta, hiszen sokan közülünk a Zrínyi Miklós Nemzetvédelmi Egyetem vagy a korábbi Zrínyi Miklós Katonai Akadémia berkeiben tanulták, látták, érezték és nem utolsósorban tették magukévá a tudomány iránti alázatot és elkötelezettséget.

A kibertér biztonságának hazai kutatása már a 2000-es évek legelején elkezdődött. Bár ez a téma és benne a terrorizmus kutatása a fentieknek megfelelően rendkívül új elem volt a tudományos kutatási területek között, ugyanakkor hatalmas és kíváncsi érdeklődés is övezte. Ez az érdeklődés többek között annak is volt köszönhető, hogy a kibertér és benne a terrorizmus szerepének kutatása során szerzett eredményeket rendszeresen publikáltuk. A kutatások kitértek

[2] Kovács 2006.

azoknak a tevékenységeknek a vizsgálatára, amelyeket a terrorista szervezetek az interneten vagy az alkalmazott információtechnológia felhasználásával végezhettek.

Ugyanakkor, és itt következik a címben megfogalmazott „múlt ismerete nélkül nincs jövő" filozófia esetünkre történő alkalmazása, a több évtizedre vagy akár évszázadra visszatekintő hagyományos terrorizmus vizsgálata, valamint az ezekből a vizsgálatokból levonható következtetések létkérdésként merültek fel már a kibertéri terrorizmus vizsgálata megkezdésének idején is. Az nagyon gyorsan világossá vált számunkra, hogy anélkül, hogy megértenénk a terrorizmus mozgatórugóit, összefüggéseit, szervezeteit, valamint eddigi tevékenységét, a jövőbeni – a kibertérben vagy azon keresztül végzett – ilyen tevékenységek nem vizsgálhatók. Így hát igyekeztünk a régmúlt és a közelmúlt terrorcselekményeit, illetve magát a terrorizmust is történelmi távlatokban vizsgálni.

A múlt kutatása és a jövő vizsgálata tehát összekapcsolódott, és össze is kellett, hogy kapcsolódjon. Ezen még az sem változtatott, hogy olyan forradalmian új területet vizsgáltunk, mint a kibertér, illetve annak biztonsága.

2001. szeptember 11-e, amely nyugodtan kijelenthetjük, világméretű sokkot jelentett az addig ismert, a II. világháborút követő, többnyire békében élő nyugati világ számára, ismét bizonyította a fentiekben megfogalmazott múlt és jövő kapcsolatát leíró kijelentésünket.

Szeptember 11. után a terrorizmus sajnálatos módon újra a mindennapok részévé vált. Így a kutatásaink értelemszerűen még inkább összekapcsolódtak a hagyományos terrorizmus, illetve a nemzetközi terrorszervezetek kutatásával. Igyekeztünk a hagyományos terrorizmus esetleges kibertérre történő kivetüléseit feltárni. Mindezek mellett azt is vizsgáltuk, hogy egy potenciális, a kibertérben vagy azon keresztül elkövetett terrortámadás milyen következményekkel és milyen hatásokkal járna. Ennek érdekében olyan területeket is vizsgálat alá vontunk, mint az információtechnológia és az általa okozott jelentős mértékű függőségünk, amely a kritikus, más szóval létfontosságú infrastruktúráinkban és információs infrastruktúráinkban érhető tetten leginkább.

Mindezen kutatások egyik szekunder eredménye a kiberterrorizmus hazai definíciójának megalkotása volt, építve természetesen a már meglévő meghatározásokra. Közvetlenül az említett 2001-es terrortámadások után már születtek ilyen meghatározások, amelyeket azonban elsősorban az Egyesült Államokból, ottani szemszögből fogalmaztak meg. Az amerikai Szövetségi Nyomozó Iroda (Federal Bureau of Investigation, FBI) kibervédelmi részlegét korábban több éven keresztül vezető Keith Lourdeau a következő megállapítást tette 2004-ben:

> „A kiberterrorizmus olyan bűncselekmény, amelyet számítógépekkel és telekommunikációs lehetőségekkel úgy hajtanak végre, hogy rombolják és/vagy megzavarják a szolgáltatások működését, zavart és bizonytalanságot keltve ezzel a lakosságban. Ezen akciók célja a kormányzat vagy a lakosság erőszakos befolyásolása a szervezet egyéni politikai, társadalmi vagy ideológiai céljai érdekében."[3]

Korábban, rögtön 2001. szeptember 11-e után hasonló megfogalmazást alkotott Dorothy Denning professzor, aki a következőkben foglalta össze a kiberterrorizmust: „A kiberterrorizmus számítógépalapú támadást vagy fenyegetést jelent, amelynek célja, hogy megfélemlítsék vagy kikényszerítsék a kormányok vagy a társadalmak részéről az adott terrorszervezet politikai, vallási vagy ideológiai céljainak elérését."[4]

Ugyanakkor ebben az időben a kiberteret érintő hazai kutatások sok esetben nemcsak hogy újnak számítottak a tudományos világban, hanem sokszor egyfajta útkeresést is jelentettek. Nem volt ez másként a kiberterrorizmus területének vizsgálata során sem. Akkoriban hívtuk ezt információs terrorizmusnak vagy félig angol terminológiával élve *cyber* terrorizmusnak is. Az ekkor született kiberterrorizmus megfogalmazásom természetszerűleg magán viseli mindezeket az útkereséssel járó bizonytalanságokat, hiszen ekkor még kissé következetlen módon az alábbi meghatározást adtam a kiberterrorizmusra: „Az információs terrorizmus definíciószerűen megfogalmazva: a cybertámadásokat és a hagyományos terrortámadásokat egyszerre alkalmazó olyan terrortevékenység, amely az információs infrastruktúrákat felhasználva, a kritikus információs infrastruktúra elleni támadásokkal próbálja meg célját elérni."[5]

A témában végzett vizsgálatainkból már akkor is és azt követően is számos következtetést vontunk le. Elsőként a terrorszervezetek és az információtechnológia kapcsolatának feltérképezése és leírása indukálta ezeket a következtetéseket. Megállapítottuk, hogy nagyon jól tipizálhatóak és el is különíthetőek azok a tevékenységek, amelyek során a terrorszervezetek a különböző információtechnológiai eszközöket és rendszereket használják. Olyan tevékenységeket azonosítottunk, mint például a propaganda, a potenciális terrorista tagok radikalizálása, illetve toborzása. Megállapítottuk, hogy a terrorszervezetek mindezek mellett ezeket a rendszereket adatszerzésre, titkosított kommunikációra, az akciók összehangolására és természetesen a hagyományos terrortevékenységek bemutatására és azok

[3] FBI 2004.
[4] Denning 2001.
[5] Kovács 2008: 11.

hatásainak fokozására használják. Ugyanakkor ezek az akciók két jól elkülöníthető tevékenységi csoportba oszthatók, amelyek alapján két típusú terrorszervezetet különböztettünk meg. Az egyik csoportba az ún. puha típusú kiberterroristákat soroltuk, akik legfőbb jellemzője, hogy közvetlenül nem az infokommunikációs rendszereket támadják, hanem azokat hagyományos akcióik elkövetése érdekében eszközként használják (például a már említett kommunikációra, adatszerzésre vagy akcióik összehangolására). A másik csoportot azok a terrorszervezetek alkotják, amelyek elsősorban az internetet, a kritikus információs infrastruktúrákat, illetve azok egyes elemeit tekintik pusztítandó célpontnak. Ennek megfelelően ezt a csoportot *hard,* azaz kemény jelzővel illettük.[6]

Kutatások a biztonságosabb jövőért

Ahogy talán a fentiekben bemutatott kiberterrorizmus esetében látható, a 21. század új technológiája, azaz az információtechnológia számos olyan területre hatással volt és jelenleg is van, amely első ránézésre nem evidens. Ez, ahogy a társadalom egészére, úgy a hadtudományra is igaz. A hadtudomány és a katonai műszaki tudomány területén végzett, M. Szabó Miklós által is inspirált kutatásaink kitértek azoknak a kérdéseknek a vizsgálatára is, amelyek az információtechnológia hadtudományra gyakorolt hatásainak elemzéseit jelentették. Ezen kutatásaink során a cél a biztonság, alapvetően a nemzeti biztonság megteremtése, annak növelése és fenntartása volt. Ezen kutatások során az elektronikus hírközlés eszközeitől kezdve a virtuális valóság katonai alkalmazásáig számos területet górcső alá vettünk.[7]

Az elektronika és az elektrotechnika azonban már jóval az információtechnológia 20. század végi megjelenése előtt tiszteletét tette a hadviselésben, hiszen a 19. század második felében a Marconi-féle rádió volt az első olyan vezeték nélküli híradást biztosító eszköz, amely teljes egészében átalakította a harctéri kommunikációt. Ezt követően már az 1905-ös japán–orosz háborúban megjelent a hadviselő felek részéről az igény, hogy a rádióeszközöket használó ellenség kommunikációját lehallgassák, vagy akár annak működését meg is akadályozzák.[8]

Ettől az időszaktól kezdve beszélhetünk elektronikai hadviselésről. Bár, ahogy láthatjuk, az elektronikai hadviselés nem új eljárás, mégis az elektronika és a legutóbbi időkben az ezzel párhuzamosan ezekben az eszközökben is alkalmazott

6 Haig–Kovács–Ványa 2011.
7 Kovács–Tózsa 2014.
8 Kovács 2017.

információtechnológia rohamos fejlődése azt igényelte, hogy időről időre ezt a területet is tudományos kutatásoknak vessük alá.[9]

Addig amíg az elektronikai hadviselés többnyire azt az elektromágneses spektrumot használja, amely fizikailag jól körülírható, addig a kibertéri műveletek dimenziója, azaz a kibertér esetében ez nem ilyen egyszerű. A kibertér nem minden esetben fogható meg kézzel, és nem mindig írható körül sem fizikailag, sem földrajzilag, hiszen virtuális, számítógépek és hálózati eszközök által létrehozott térről beszélünk. (Most tekintsünk el attól az egyébként fontos ténytől, hogy az említett számítógépek viszont a fizikai térben helyezkednek el.) Ráadásul a két terület, azaz az elektromágneses spektrumban végzett műveletek és a kibertéri műveletek sok esetben jelentős konvergenciát mutatnak. Nyugodtan kijelenthetjük, hogy a hagyományos hadviselés, benne az említett elektronikai hadviseléssel kilép a megszokott fizikai dimenziókból (szárazföld, levegő, tenger, űr), és a kibertéri tevékenységek egész sorát alkalmazza katonai célokra. A kibertér és a hagyományos dimenziókban folyó elektronikai hadviselési és elektronikai felderítési tevékenységek elemzése során már a 2010-es évek elején arra a megállapításra jutottunk, hogy a kibertér lesz a hadviselés következő dimenziója.[10]

Ugyanakkor mind az elektronikai hadviselés, mind a kibertéri műveletek esetében arra a megállapításra jutottak a kutatások, hogy ezeknek a technológiáknak az alkalmazása nem csak a hadseregek privilégiuma. Mivel az információtechnológia, így különösen az információ szabad – és tegyük rögtön hozzá, sok esetben kontrollálatlan, sőt esetenként felelőtlen – áramlása lehetővé teszi, hogy bárki hozzáférjen ahhoz a technológiához, amelyet ártó szándékkal a társadalom ellen, illetve annak korábban már említett legfontosabb, kritikus (létfontosságú) rendszerei ellen fel tud használni, így ez súlyos nemzetbiztonsági kockázatokat jelent.

2010-ben *Digitális Mohács* címmel olyan forgatókönyvben összegeztük ebben a témában a kutatásainkat, amely arra kívánta felhívni a figyelmet, hogy az információtechnológia ártó szándékú felhasználása milyen károkat okozhat egy olyan fejlett információs infrastruktúrájú ország esetében, mint Magyarország. Maga a *Digitális Mohács* szcenárió gondolatkísérlet volt, elképzelt eseményeket és azok egymásra és az országra (lakosság, gazdaság, politika) gyakorolt hatásait vázoltuk fel úgy, hogy abban Magyarország kritikus infrastruktúrái és kritikus információs infrastruktúrái ellen elkövetett különböző támadási módszereket mutattunk be azok következményeinek elemzésével együtt. A tanulmány egyik legfontosabb következtetése, és ha tetszik, figyelmeztetése az volt, hogy a biztonság

[9] Németh 2014.
[10] Haig–Kovács–Ványa 2011.

érdekében a kormányzatilag felügyelt koordinált védekezés elengedhetetlen a bemutatott rosszindulatú tevékenységekkel szemben.[11]

Maga a fenti forgatókönyvből született tudományos publikáció, illetve az abból levonható következtetések már egyértelműsítették, hogy bár rendkívül fiatal terület a kibertér és annak biztonsága, mégis a tudományos kutatások eredményeit a gyakorlatban is felhasználható olyan nemzeti stratégia vagy stratégiák kidolgozása szükséges, amelyek mentén valóban megvalósítható a már említett célkitűzés: a magasabb szintű nemzeti biztonság elérése.

Ugyanakkor ennek a stratégiának az elkészítése számos más terület vizsgálatát is igényelte. Ennek oka abban keresendő, hogy a fentiekben említett módon a kibertér és a gyakran azzal azonosított internet mindennapjaink részévé vált, és át is alakította a 21. század számos társadalmi és gazdasági folyamatát. Ezek a változások a kommunikációtól kezdődően a politikán, a kultúrán, a gazdaságon át a hadügyig minden területre igazak. Ez az átalakulás azonban paradox módon még mélyebb függőséget okozott az információtechnológiától. Ennek megfelelően ma már elengedhetetlen, hogy az említett társadalmi és gazdasági folyamatokat lehetővé tevő információtechnológiai eszközök és rendszerek zavartalanul és biztonságosan működjenek. Így az ezen rendszerek és eszközök alkotta kibertér biztonsága elsődleges fontosságúvá vált.[12]

Ennek a biztonságnak a megteremtése érdekében tehát nemzeti stratégiát kell alkotni. E munka során azonosítani kell azokat a veszélyforrásokat, amelyek a kibertérben nemzetbiztonsági kockázatként jelentkeznek a digitális ökoszisztémával rendelkező országok, így hazánk esetében is. Természetesen már ma is léteznek a különböző országokban olyan stratégiák vagy stratégiai elképzelések, amelyek az ezekre a kockázatokra adandó válaszokat tartalmazzák. Ezek többsége azonban többnyire statikus dokumentum, amely nem képes válaszokat adni a kibertér dinamizmusa miatti gyorsan bekövetkező változások mindegyikére. Ennek megfelelően olyan stratégiára van szükség, amely dinamikusan és adaptívan alkalmazható megváltozott világukban, és amely figyelembe veszi az olyan tényezőket is, mint például a kiberhadviselés vagy akár a kiberelrettentés.

Ehhez az olyan nagyhatalmak, mint az Egyesült Államok, Kína vagy Oroszország kibertérhez való viszonyának, illetve az olyan nemzetközi szövetségek, mint az Európai Unió és a NATO, valamint számos európai ország kiberbiztonságról alkotott stratégiai elképzeléseinek kutatása alapján azok szerkezeti és tartalmi elemei elemzése után a javaslatok megszülettek.[13]

[11] Kovács–Krasznay 2010.
[12] Kovács 2018a.
[13] Kovács 2018b.

A múlt és a jövő kutatása tehát, építkezve az M. Szabó Miklóstól is kapott inspirációval végzett tudományos kutatásokra, valóban biztonságosabb világ felépítéséhez járulhat hozzá.

Felhasznált irodalom

Denning, Dorothy E. (2001): Is Cyber Terror Next? *Items.ssrc.org,* 2001. november 1. Online: https://items.ssrc.org/after-september-11/is-cyber-terror-next

FBI (2004): *Testimony of Keith Lourdeau, Deputy Assistant Director, Cyber Division, FBI Before the Senate Judiciary Subcommittee on Terrorism, Technology, and Homeland Security.* Online: https://www2.fbi.gov/congress/congress04/lourdeau022404.htm

Haig Zsolt – Kovács László – Ványa László (2011): Az elektronikai hadviselés, a SIGINT és a cyberhadviselés kapcsolata. *Felderítő Szemle,* 10(1–2), 183–209.

Kovács László (2006): Az információs terrorizmus eszköztára. *Hadmérnök,* 2006/különszám (Robothadviselés 6. Tudományos szakmai konferencia, 2006. november 22.). Online: www.hadmernok.hu/kulonszamok/robothadviseles6/kovacs_rw6.html

Kovács László (2008): Az információs terrorizmus elleni tevékenység kormányzati feladatai. *Hadmérnök,* 3(2), 138–148.

Kovács László (2017): Az elektronikai hadviselés jelene és lehetséges jövője. *Hadmérnök,* 12(1), 213–232.

Kovács László (2018a): *A kibertér védelme.* Budapest: Dialóg Campus.

Kovács László (2018b): *Kiberbiztonság és -stratégia.* Budapest: Dialóg Campus.

Kovács László – Krasznay Csaba (2010): Digitális Mohács: Egy kibertámadási forgatókönyv Magyarország ellen. *Nemzet és Biztonság,* 3(1), 44–56. Online: www.nemzetesbiztonsag.hu/cikkek/kovacs_laszlo__krasznay_csaba-digitalis_mohacs_.pdf

Kovács László – Tózsa István szerk. (2014): *Az infokommunikációs technológia hatása a hadtudományokra.* Budapest: Nemzeti Közszolgálati Egyetem.

Németh András szerk. (2014): *Elektronikai hadviselés.* Budapest: Nemzeti Közszolgálati Egyetem.