Kovács László dandártábornok:

A KIBERBIZTONSÁG ÉS A KIBERMŰVELETEK MEGJELENÉSE MAGYARORSZÁG ÚJ NEMZETI BIZTONSÁGI STRATÉGIÁJÁBAN

DOI: 10.35926/HSZ.2020.5.1

ÖSSZEFOGLALÓ: *2020. április végén jelent meg hazánk új Nemzeti Biztonsági Stratégiája, amely a „Biztonságos Magyarország egy változékony világban" önmagában is beszédes címet kapta. A korábbi, 2012-ben megjelent Nemzeti Biztonsági Stratégiát felváltó új dokumentum egy olyan megváltozott biztonsági környezetben határozza meg hazánk biztonsághoz való viszonyát, amelyben az egyik kiemelt terület a kibertér és az abban megjelenő társadalmi és gazdasági folyamatok. Ennek megfelelően érdemes megvizsgálni, hogy a kibertér és annak biztonsági kihívásai hogyan és milyen módon vannak jelen az új stratégiában. A tanulmány e szempontokra fókuszálva hasonlítja össze az új és a régi stratégiát, valamint kitér azokra a következményekre, amelyek – az új stratégiában megjelenő új kibertéri vonatkozások miatt – a kiberbiztonság és a kiberműveletek területén várhatóak mind további jogszabályok megjelenésében, mind pedig szervezeti változásokban.*

KULCSSZAVAK: *biztonság, stratégia, kiberbiztonság, kiberműveletek*

BEVEZETŐ

A biztonságról alkotott felfogásunk és az azzal kapcsolatos percepciónk alapvető változáson ment keresztül az elmúlt közel egy évtizedben. A biztonságpolitikai helyzet Európában, de a világ számos más pontján is negatív irányban változott meg. Ez igaz a kibertérre és az abban megjelenő biztonságra is. A kibertérben az elmúlt években bekövetkezett robbanásszerű fejlődés természetszerűleg magával hozta a kiberbiztonság változásának és annak más biztonsági területekre gyakorolt, sok esetben szintén negatív hatását is.

Ezek a nem mindig pozitív változások indukálták többek között egy új nemzeti biztonsági stratégiai dokumentum elkészítését. 2012-ben született meg hazánk korábbi Nemzeti Biztonsági Stratégiája (NBS 2012),[1] amely az akkori biztonsági környezetet és biztonsági felfogást mutatta be, illetve képezte le, majd ezekre kereste azokat a megoldásokat – stratégiai irányokat –, amelyekkel az akkori kihívások kezelhetők, a veszélyek pedig csökkenthetők voltak.

A kibertér vonatkozásában szükséges hangsúlyozni, hogy a 2012-es Nemzeti Biztonsági Stratégia korszakosnak volt nevezhető, mert ebben a legfelső szintű biztonsági

[1] 1035/2012. (II. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról. Magyar Közlöny 2012/19., 1378–1397. https://2010-2014.kormany.hu/download/f/49/70000/1035_2012_korm_hatarozat.pdf (Letöltés időpontja: 2020. 06. 05.)

dokumentumban szerepel elsőként a kiberbiztonság[2] markáns biztonsági kihívásként megfogalmazva. Ezt megelőzően – bár szakmai oldalról a kétezres évek elejétől természetesen folyamatosan jelen voltak a kibertéri veszélyek és kihívások kezelésének szükségességét bemutató elképzelések és felvetések – azok nem a hivatalos, ágazati stratégiai irányokat legfelsőbb szintről meghatározó dokumentumban, a nemzeti biztonságot meghatározó stratégiában lettek kinyilvánítva.

A 2012-es Nemzeti Biztonsági Stratégia a hazánkat érintő biztonsági fenyegetések, kihívások és azok kezelésének számbavétele, illetve meghatározása során a kiberbiztonságot már mint önálló területet határozza meg. Ugyanakkor a kiber kifejezés összesen csak hat alkalommal szerepelt a dokumentumban. Ezzel szemben az új, 2020-as Nemzeti Biztonsági Stratégiában már 33 alkalommal találkozunk vele különböző kontextusokban. Talán ez a statisztikai szám is igazolja a kiberbiztonság és a kiberműveletek elmúlt időszakban megnövekedett szerepét és jelentőségét.

Jelen írás a két stratégiát kibertéri szempontból elemzi röviden, majd az új stratégiából a közeljövőre vonatkoztatható szükséges jogszabályi és szervezeti változásokról kíván néhány tényezőt felvillantani. A tanulmány mindezeket természetesen a szerző szemszögéből, illetve a szerző számára fontosnak vélt tények mentén teszi meg.[3]

Ez a kép azonban nem lehet és nem is lesz teljes, hiszen az új Nemzeti Biztonsági Stratégia az olyan ágazati stratégiák újradefiniálását is indukálja, mint a Nemzeti Katonai Stratégia és a Nemzeti Kiberbiztonsági Stratégia. Ez utóbbi dokumentumok jelen tanulmány írásakor a kidolgozás fázisában vannak, így azok – kibertérre vonatkozó – megállapításait természetszerűleg még nem tartalmazhatja.

A 2012-ES NEMZETI BIZTONSÁGI STRATÉGIA ÉS A KIBERTÉR

A korábbi Nemzeti Biztonsági Stratégiánk a jelen írás bevezetőjében említettek miatt, azaz pusztán annak a ténynek köszönhetően, miszerint a kibertér[4] és az abban megjelenő kihívások nemzetbiztonsági fenyegetésként lettek megfogalmazva és megjelenítve a dokumentumban, korszakosnak mondható. A 2012-ben kiadott Nemzeti Biztonsági Stratégiánk az első azon legfelső szintű biztonsági stratégiáink sorában, amelyek explicit módon tar-

[2] Meg kell jegyezni – mint azt a későbbiekben látni fogjuk –, hogy a 2012-es Nemzeti Biztonsági Stratégia a kiberbiztonság címszóval jeleníti meg a hazánkat érintő biztonsági fenyegetéseket és kihívásokat, illetve azok kezeléséhez szükséges feladatokat. Lásd NBS 2012: 31. pont. Arra, hogy a stratégia miért kiberbiztonság kifejezéssel fogalmazza meg a fenyegetések számbavétele során ezt a területet, a lehetséges magyarázat az, hogy a kiberbiztonság mint állapot megteremtése volt a cél, illetve az ebben felsorolt feladatok (többek között például kockázatok felmérése, kormányzati koordináció, tudatosság emelése, kritikus infrastruktúrák és kritikus információs infrastruktúrák védelme stb.) szükségesek a megkívánt kiberbiztonsági állapot eléréséhez. A másik magyarázat ennél sokkal prózaibb: számos más olyan területet is, ahol stratégiai szintű biztonsági kihívást azonosított a dokumentum, hasonlóképpen nevezett meg, mint például a pénzügyi biztonság vagy az energiabiztonság.

[3] Ez természetszerűleg a téma egyfajta lehatárolását is jelenti. Mind a várható szervezeti, mind a jogszabályi változások esetében jelen írásban elsősorban a katonai terület kerül csak bemutatásra.

[4] A kibertér megfogalmazása számos nemzetközi és hazai szakmai és tudományos diszkussziót generált az elmúlt években. Az értelmezések körüli polémiát egyrészt Munk Sándor foglalta össze tudományos dolgozatában 2018-ban, másrészt Haig Zsolt adott erre az információs műveletekkel kapcsolatos értelmezést szintén 2018-ban. Lásd Munk Sándor: A kibertér fogalmának egyes, az egységes értelmezést biztosító kérdései. Hadtudomány, 2018/1., 113–131. http://real.mtak.hu/77921/1/HT20181_115_133_u.pdf (Letöltés időpontja: 2020. 06. 05.) és Haig Zsolt: Információs műveletek a kibertérben. Dialóg Campus, Budapest, 2018.

talmazzák a kiberbiztonságot. A kibertér és annak biztonsága olyan stratégiai területként jelent meg, amely kihatással volt és azóta is kihatással van a nemzet egésze biztonságáról történő gondolkodásra.

Ez a tény ma már sokkal inkább természetes, mint 2012-ben, hiszen az elmúlt közel egy évtized alatt – többek között a rendkívül dinamikus információtechnológiai fejlődésnek köszönhetően – a társadalmi, gazdasági és kulturális területen bekövetkezett változások miatt a kibertér a biztonság elengedhetetlen dimenziójává vált. Ez azonban a 2010-es évek elején még csak inkább predikció volt, hiszen akkor még csak formálódott az a kibertéri függőség, amely napjainkra oly jellemző. Ugyanakkor éppen emiatt a biztonság ebben a dimenzióban is abszolút módon felértékelődött.

Ahogy a bevezetőben utaltunk rá, a 2012-es Nemzeti Biztonsági Stratégia a klasszikus biztonsági stratégiák felépítését követve megállapította hazánk értékeit és érdekeit, elemezte az azokat fenyegető kihívásokat és veszélyeket, majd leírta azokat a feladatokat, amelyekkel ezekre hazánk eredményesen tud választ adni. A stratégia mindezt nagyon egyértelműen meghatározta annak legelső pontjában: *„[j]elen stratégia rendeltetése, hogy az értékek és érdekek számbavétele, valamint a biztonsági környezet elemzése alapján meghatározza azokat a nemzeti célokat, feladatokat és átfogó kormányzati eszközöket, amelyekkel Magyarország a nemzetközi politikai, biztonsági rendszerben érvényesíteni tudja nemzeti biztonsági érdekeit.”*[5]

A kibertérre vonatkozó kihívásokat és veszélyeket a stratégia a kiberbiztonság címszóval adta meg, amely bár félrevezető lehet, de annak tartalma a – stratégia készítésének, illetve kiadásának idején – meglévő legfontosabb tényezőket sorolta fel. A kiberbiztonság felvezetésénél a stratégia megállapította, hogy *„[a]z állam és a társadalom működése – a gazdaság, a közigazgatás vagy a védelmi szféra mellett számos más területen is – mind meghatározóbb módon a számítástechnikára épül”*.[6] Ez alapjaiban természetesen már akkor sem volt meglepően új és korszakalkotó megállapítás. Ráadásul egy, már ekkor is réginek számító terminológiát, nevezetesen a *számítástechnika* kifejezést használta a dokumentum az infokommunikációs rendszerekre. Ugyanakkor a szövegben már nagyon előremutató utalásokat találunk azokra az összefüggésekre és komplexitásra, amelyek azóta is a legnagyobb kihívást jelentik a területen. A stratégia ezt így fogalmazza meg: *„Egyre sürgetőbb és összetettebb kihívásokkal kell számolnunk az informatikai és telekommunikációs hálózatok, valamint a kapcsolódó kritikus infrastruktúra fizikai és virtuális terében.”*[7]

A stratégia megállapítja, hogy az információ szabad áramlására épülő – és többek között pont emiatt rendkívül gyorsan fejlődő – technika bárki, illetve bármely szervezet számára hozzáférhető, például a terrorszervezetek számára is: *„Fokozott veszélyt jelent, hogy a tudományos és technológiai fejlődés szinte mindenki számára elérhetővé vált eredményeit egyes államok, vagy nem állami – akár terrorista – csoportok arra használhatják, hogy megzavarják az információs és kommunikációs rendszerek, kormányzati gerinchálózatok rendeltetésszerű működését.”*[8]

Ezt követően a dokumentum deklarálja az állam számára talán az egyik legfontosabb feladatot a kibertérrel kapcsolatban, mégpedig azt, hogy a fentiekben felsorolt kibertéri kihívásokat kezelni kell. A stratégia megfogalmazásában: *„A kibertérben világszerte növekvő mértékben jelentkező nemzetbiztonsági, honvédelmi, bűnüldözési és katasztrófavédelmi*

[5] NBS 2012: 1. pont.
[6] Uo. 31. pont.
[7] Uo.
[8] Uo.

vonatkozású kockázatok és fenyegetések kezelésére, a megfelelő szintű kiberbiztonság garantálására, a kibervédelem feladatainak ellátására és a nemzeti kritikus infrastruktúra működésének biztosítására Magyarországnak is készen kell állnia."[9]

Az ennek érdekében szükséges feladatokat a stratégia két nagy csoportra osztotta. Az első csoportba tartoztak azok a feladatok, amelyek a kibertéri – meglévő és potenciális – veszélyek rendszeres felmérését és azok között fontossági sorrend felállítását (priorizálást)[10] jelentik. A stratégia ebbe a csoportba tartozó feladatként határozza meg a védelem hatékonysága szempontjából elengedhetetlen kormányzati koordináció erősítését, valamint a szintén nagyon fontos társadalmi kibertudatosság növelését. Bár csak néhány szóban, de a stratégia utal a nemzetközi együttműködés fontosságára, amely az általunk is említett okok[11] miatt mára már abszolút elengedhetetlenné vált. A feladatok másik nagy csoportja a kritikus információs infrastruktúra védelmére vonatkozik, amelyben a kibervédelemnek kiemelt helyet kell kapnia amellett, hogy itt is hangsúlyosan jelentkezik a nemzetközi együttműködés szükségessége.[12]

A stratégia kitér a Magyar Honvédség (MH) szerepére és feladataira is, amelyet nagyon általánosítva a dokumentum így fogalmaz meg: *„A Magyar Honvédség alapvető feladata, hogy az Alaptörvénnyel összhangban garantálja hazánk biztonságát, valamint hozzájáruljon szövetségeseink kollektív védelméhez."*[13]

Az MH vonatkozásában felsorolt feladatok jórészt valóban csak általánosságok, hiszen az ország szuverenitásának védelmét, illetve a szövetségi kötelezettségvállalásainkból adódó feladat érdekében korszerűen felszerelt, rugalmas, telepíthető és fenntartható haderőt ír le a stratégia.[14]

A dokumentum azonban nem tér ki sem az MH kibertéri védelmi vagy kibertéri műveleti tevékenységére, sem az ezekhez szükséges feladatok, szervezetek és eljárások mikéntjére. Mindezekhez majd a Nemzeti Biztonsági Stratégiára épülő, szintén 2012-ben megjelent Nemzeti Katonai Stratégiában[15] (NKS 2012) kapunk utalásokat. Ebben a hadsereg kiberműveleti képességeinek fejlesztési igénye már megjelenik, hiszen az abban felsorolt veszélyeknél a

---

[9] Uo.

[10] A priorizálás ezen a területen egyfajta kényszerűség, hiszen az esetlegesen korlátozottan rendelkezésre álló erőforrások elosztását és felhasználását is meghatározza, de egyben az állam szempontjából valódi sorrendiség felállítását is jelentheti. Ez talán a kritikus infrastruktúrák esetében érhető tetten a leglátványosabban. Az ezen a területen felállított megfelelő szempontrendszer alkalmazásával besorolt infrastruktúra-elemek esetén a stratégiai fontosságú rendszerelemektől kezdve lehet felépíteni és megvalósítani a védelmet. Ez nyilvánvalóan szinteket is jelent, és így szintenként – például helyi, regionális, nemzeti szint – valósítható meg a komplex védelem, a különböző szinteken meglévő védelem egymásra épülésével.

[11] A kibertér, illetve annak biztonságának erősítése érdekében a nemzetközi együttműködés több ok miatt is nélkülözhetetlen. A kibertér jellege, azaz a globalitás és a határoknélküliség miatt az olyan területeken, mint az incidenskezelés és a kiberbűnözés elleni tevékenység, csak nemzetközi együttműködésben képzelhető el hatékonyan. A másik ok a kibertérben történő érdekérvényesítés. A kibertér gazdaságban játszott szerepe évről évre exponenciálisan nő. Ennek megfelelően még az olyan nemzetközi szervezetben is, mint az Európai Unió, komoly gazdasági verseny folyik a kibertérben. Ezért például a visegrádi országok közös, a kibertéri gazdasági versenyt szabályozó kérdésekben történő egységes fellépése sokkal hatékonyabb lehet, mint az egyes országok önálló ilyen kezdeményezése. Ugyanez igaz a kibertér védelmére is, hiszen a közös, a védelmet befolyásoló új szabályozási elvek szintén hatékonyabban képviselhetők együtt, mint az egyes tagországok önálló törekvései.

[12] NBS 2012: 31. pont.

[13] Uo. 44. pont.

[14] Uo.

[15] 1656/2012. (XII. 20.) Korm. határozat Magyarország Nemzeti Katonai Stratégiájáról. https://net.jogtar.hu/getpdf?docid=A12H1656.KOR&targetdate=&printTitle=1656/2012.+%28XII.+20.%29+Korm.+hat%C3%A1rozat&getdoc=1 (Letöltés időpontja: 2020. 06. 05.)

kibertér már szintén markánsan jelen van. A katonai stratégia egyik legelőremutatóbb tényezője azonban a hadviselés fogalmi hátterének felülvizsgálatát szorgalmazó pont, amely a következőket tartalmazza: *„A kiberfenyegetésnek a hagyományos fenyegetésektől eltérő jellemzői szükségessé teszik a háborúval kapcsolatos fogalmaink átfogó felülvizsgálatát és adott esetben módosítását."*[16]

Az ebben a pontban megjelenő fenyegetés kifejtésére a stratégiában később kerül sor: *„Ilyen fenyegetést jelent elsősorban a kiber hadviselés, amely anyagi kár okozásában és a közrend megzavarásában potenciálját tekintve egyre kevésbé marad el a hagyományos fegyverektől."*[17] Ahogy ebből az idézetből is látható, a dokumentumban nagyon előremutató módon megjelenik a kiberhadviselés fogalma. Ugyanakkor ezt az előremutató kérdést a stratégia nem viszi végig, hiszen az MH feladatainál ez már nem jelenik meg, mert ott csak a következőket határozza meg: *„A Magyar Honvédség egyik célja a hálózatalapú hadviselés feltételeinek megteremtése. Ennek részeként erősíteni kell a Magyar Honvédség kibervédelmét, amihez koncepcionálisan megalapozott rendszabályok kidolgozása, modern eszközök beszerzése, valamint az állomány megfelelő felkészítése és kiképzése szükséges."*[18]

Ebből azt a következtetést vonhatjuk le, hogy a katonai stratégia bár általánosságban már tartalmazza a kibertéri veszélyeket, illetve az azokban megjelenő potenciális nemzeti biztonságot fenyegető egyik legfontosabb kihívást, és megemlíti annak megjelenését a hadviselésben, de a Nemzeti Biztonsági Stratégia által nyújtott kereteken belül marad, azaz a Magyar Honvédség fejlesztése vonatkozásában csak a kibervédelemre koncentrál.

AZ ÚJ NEMZETI BIZTONSÁGI STRATÉGIA ÉS A KIBERTÉR

Az új, 2020-ban megjelent Nemzeti Biztonsági Stratégia[19] (NBS 2020) a *„Biztonságos Magyarország egy változékony világban"* címet viseli. Így az új stratégia már címében is utal azokra az elmúlt közel egy évtized alatt megjelent biztonsági kihívások okozta helyzetre, amelyben a kihívások alapjaiban alakították át világunkat, és amelyek így ma meghatározó hatással vannak hazánk biztonságára is.[20] A stratégia címe magában hordozza mindazon tényezőket, amelyek a nemzeti biztonság területén a nehezen kiszámítható kihívásokat és azok egymásra is gyakorolt hatásait jelentik.

---

[16] NKS 2012: 33. pont.

[17] Uo. 52. pont.

[18] Uo. 82. pont.

[19] 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról. Magyar Közlöny, 2020/81., 2101–2119. https://magyarkozlony.hu/dokumentumok/6c9e9f4be48fd1bc620655a7f249f81681f8ba67/letoltes (Letöltés időpontja: 2020. 06. 05.)

[20] Ez nyilvánvalóan biztonságpercepciónk változását is magával hozta, ami az Európában a 2010-es évek közepén megnövekedett számú és intenzitású terrortámadásoknak, a Krím félszigetet érintő eseményeknek, majd a kelet-ukrajnai válságnak, de akár az Európát déli irányból érő migrációs nyomásnak is betudható. Ugyanakkor mindehhez – ezekkel párhuzamosan – a kibertéri incidensek, kibertámadások, illetve a nagy nemzetközi visszhangot is kiváltó adatvédelmi ügyek is hozzájárultak. A kibertéri veszélyek ilyen formában és ilyen intenzitással történő megjelenése, illetve azok nyilvánosságot is elérő szintje soha korábban nem volt tapasztalható. Többek között ezeknek az eseményeknek tudható be, hogy már nem csak a kiberbiztonsági szakértők, hanem a politikai és gazdasági döntéshozók is a korábbiaknál jóval nagyobb figyelmet fordítanak erre a területre. Ez igaz a katonai gondolkodás átalakulására is. Hazánk 2012-es Nemzeti Katonai Stratégiája még csak utal a kiberhadviselésre, ugyanakkor ma már természetesnek mondható evolúció figyelhető meg számos ország haderejében, hiszen a kibervédelmi erők mellett egyre több ország hadserege alakít ki olyan kiberműveleti csapatokat, amelyek az offenzív kibertéri műveletekre is alkalmas szervezetek.

A stratégia már a bevezetőjében nagyon röviden összefoglalja azokat a kihívásokat és veszélyeket, amelyek a legmarkánsabbak napjainkban, de amelyek egyben a leggyorsabban változnak, így azok – ahogy a stratégia címe is utal rá – valóban egy változékony világot is jelentenek. A dokumentum ezt a következőképpen fogalmazza meg: *„Az új kihívások alapja a formálódó, többpólusú világrend, a nemzetközi szereplők kapcsolatait befolyásoló szabályok átalakítására való törekvés, a biztonsági kihívások változó arculata, továbbá az olyan globális kihívások, mint a klíma- és a demográfiai változások felgyorsulása, az ezzel szorosan összefüggő illegális és tömeges migráció, a természeti erőforrások kimerítése, végül pedig a technológiai forradalom társadalomformáló hatásai."*[21]

A fenti idézetből – amely egyben a stratégia bevezetője is – kitűnik, hogy napjainkban a technológiai fejlődés, illetve az abból származtatható kihívások nem hagyhatók figyelmen kívül, amikor a nemzet egészének biztonságáról gondolkodunk. Ahogy később a stratégia többször is utal rá, ennek egyik igen hangsúlyos elemét képezik a kibertérben jelentkező kihívások, majd az azokra adandó lehetséges válaszok megtalálása.

A stratégia felépítése követi a hagyományos nemzeti biztonsági stratégia – mint az adott nemzet biztonságról alkotott dokumentumainak legmagasabb szintű eleme – ma már klasszikusnak mondható felépítését.

A stratégia a kibertér vonatkozásában hazánk alapvető érdekeként a következőket azonosítja: *„A forradalmi technológiák fejlesztése stratégiai fontosságú kérdés. Hazánk biztonsága megkívánja, hogy a kulcsfontosságú területeken – mint például a kibervédelem, a mesterséges intelligencia, az autonóm rendszerek, a biotechnológia – kiemelt figyelmet fordítsunk a kutatás-fejlesztésre és annak védelmi összetevőjére."*[22]

A stratégia azonosítja azokat a kiemelt biztonsági kockázatokat, amelyek hazánk esetében a legfontosabbaknak tekinthetőek. Ezeken belül a kibertérrel kapcsolatosan a stratégia a következőket állapítja meg kiemelt kockázatokként: *„…jelentős károkat okozó kibertámadások a kormányzati informatikai rendszerek, az E-közigazgatás, a közműszolgáltatók, a stratégiai vállalatok, a létfontosságú infrastruktúra egyéb elemei és más, a társadalom működésében fontos szervezetek számítógépes hálózatai ellen..."*[23]

A stratégiát továbbelemezve eljutunk az egyik legfontosabb, és nyugodtan kijelenthetjük, hogy a kibertéri műveletek vonatkozásában valóban paradigmaváltó kitételhez, amely a következő: *„Magyarország a fizikai biztonságot veszélyeztető vagy jelentős anyagi károk okozására képes kiberképességeket fegyvernek, alkalmazásukat fegyveres agressziónak tekinti, amelyre a fizikai térben megvalósuló válaszadás is lehetséges."*[24]

A korábbi visszafogott biztonságpolitikai értékelésekkel szemben itt már látható a kibertérből érkező fenyegetések valódi realitása. Korábban nem, vagy csak részben volt látható a hazai biztonságpolitikai gondolkodásban a kibertéri veszélyek ilyenfajta felértékelődése. Ugyanakkor annak kijelentése, hogy Magyarország egyrészt a fenyegető kiberképességeket fegyvernek tekinti, illetve a Magyarországot érő kibertéri támadások elérhetik azt a küszöböt, amikor fizikai válaszcsapások is elképzelhetők, valódi új irányt és

[21] NBS 2020: 1. pont.
[22] Uo. 106. pont.
[23] Uo. 124. b.
[24] Uo. 101. pont.

nagyon markáns véleményeltolódást jelez.[25] Ezek nagyon pozitív változásként értékelhető kitételek a stratégiában. Markáns megállapítások, amelyek még egy közvetett eredményt is magukkal hozhatnak. A kibertéri támadásokra történő potenciális fizikai válaszok megjelenítése ugyanis biztonság- vagy védelempolitikai szemszögből nézve elrettentést is jelenthet. Ugyanakkor az esetleges kibertéri támadásokra történő fizikai válaszadás mellett szükséges lehet a kibertéri válaszcsapás lehetőségének a megjelenítése is. Ez is hozzájárul az elrettentés kialakításához, mivel: *„…[e]bben a kontextusban a kiberelrettentés nem jelent mást, mint egyrészt olyan kibervédelmi megoldások kialakítását az adott országban, amelyek áttörése nem, vagy csak komoly erőforrások segítségével lehetséges, másrészről olyan kibertámadó képességek kiépítését és felmutatását,*[26] *amelyek egy adott ellenséges kibertámadásra válaszul alkalmazhatók a támadóval szemben."*[27]

A kiberelrettentést már számos ország alkalmazta a közelmúltban kiadott stratégiáiban. Az egyik ilyen az Amerikai Egyesült Államok Nemzeti Védelmi Doktrínája, amellyel párhuzamosan mindezt megtaláljuk az ország Védelmi Minisztériuma által kiadott kiberbiztonsági stratégiában is: *„A fokozódó fenyegetés, amellyel szembenézünk, szükségessé teszi, hogy a Védelmi Minisztérium hozzájáruljon egy átfogó kiberelrettentési stratégia kidolgozásához és végrehajtásához, annak érdekében, hogy megakadályozza a legfontosabb állami és nem állami szereplőket az amerikai érdekek elleni kibertámadások elkövetésében."*[28]

Az azonban nyilvánvaló, hogy egy kibertéri támadásra – legyen az a fizikai biztonságot veszélyeztető vagy jelentős anyagi károkat okozó – adandó válasz előtt elsőként bizonyítani kell a kibertámadás tényét, illetve meg kell nevezni az elkövetőt. Ez rögtön magával hozza az attribúció kérdését, amely legalább olyan összetett és bonyolult problémakör, mint maguknak a kibertámadásoknak a technikai visszafejtése az elkövetőkig. Mindezekből következően az attribúciónak, azaz az elkövető megnevezésének legalább két összetevőjével kell számolni.[29] Az első a technikai attribúció, amely során nagyon pontos és alapos adatgyűjtés szükséges ahhoz, hogy az elkövető személye valóban bizonyítható legyen. Erre utal maga a stratégia szövege is: *„A kiberműveletek sokszor nehezen bizonyítható attribúciójára, az elkövető azonosítására, megnevezésére való tekintettel*

---

[25] A kiberbiztonsággal foglalkozó szakemberek és szervezetek több mint egy évtizede folyamatosan hangsúlyozzák annak a veszélyét, hogy a kibertérből érkező potenciális támadások nemcsak az információs rendszerekre, hanem közvetve az állam működésére is komoly, esetenként súlyos fenyegetést jelentenek. Így a súlyos kibertámadásokra adandó fizikai válaszok megjelenése a Nemzeti Biztonsági Stratégiában megnyugvással töltheti el a kiberbiztonsági szakembereket. Ugyanakkor mindez már nemcsak szűk kiberszakmai, hanem tágabb értelemben vett és szélesebb kontextusban megjelenő biztonságpolitikai és védelempolitikai kérdéssé is vált egyben.

[26] Ez a felmutatás történhet indirekt módon úgy is, hogy a kiberbiztonsági stratégiába bekerül az elrettentés mint fogalom.

[27] Kovács László: Kiberbiztonság és -stratégia. Dialóg Campus, Budapest, 2018.

[28] The DoD Cyber Strategy. The Department of Defense, Washington, 17. 04. 2015., 10. https://archive.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf (Letöltés időpontja: 2020. 06. 05.)

[29] Az attribúcióval kapcsolatban a NATO Kibertér Műveleti Doktrínája szintén több meghatározó lépésről tesz említést (nem véletlenül az anonimitás címszó alatt), amelyek között csak az egyik a technikai kérdések bizonyítása, de emellett szükségesnek ítéli a több forrásból származó információk, a hagyományos forenzikus eljárás és más egyéb eljárások alkalmazását is az elkövetők kilétének felfedéséhez, illetve azok személyének bizonyításához. Ugyanakkor a doktrína azt is hozzáteszi, hogy attribúció hiányában, azaz, ha nincs megnevezve a támadó, akkor nő a politikai kockázat, illetve csökken a válaszreakciók lehetősége. Természetesen a nem megalapozott attribúció ugyanilyen veszélyeket hordoz magában. Lásd AJP 3.20 – Allied Joint Doctrine for Cyberspace Operations. Edition A Version 1. 2.4. NATO Standardization Office, 2020.

a válaszlépések különösen körültekintő, eseti elbírálást igényelnek az érintett kormányzati szervezek bevonásával."[30]

Az attribúció másik összetevője a politikai vagy diplomáciai attribúció, amely a technikai vizsgálatok eredményeire építve, politikai és/vagy diplomáciai eszközökkel nevezi meg a támadót. Ugyanakkor hangsúlyozni kell, hogy amennyiben egy kibertámadásra a fizikai térben adandó válasz lehetőségként felmerül, az valóban nagy körültekintést igényel ebben a korántsem könnyű döntési körben.

A stratégiában foglalt nemzeti biztonságot erősítő célok elérése érdekében a dokumentum számos átfogó feladatot és eszközt határoz meg. Ezek a feladatok nyilvánvalóan akkor hajthatók végre hatékonyan, amennyiben pontos képünk van arról, hogy a kibertérben milyen kockázatok és fenyegetések vannak jelen, ezek közül melyek a legfontosabbak, és melyek azok, amelyek kezelésének elmaradása a nemzeti biztonsági célok megvalósítását közvetlenül is befolyásolhatják. Ennek megfelelően a stratégia által meghatározott feladatok közé nagyon markánsan bekerült a kibertéri kockázatok kezelése is. A stratégia ezzel kapcsolatban a következőket fogalmazza meg: *„A kibertérben jelentkező kihívások, kockázatok és fenyegetések kezelésére, a megfelelő szintű kiberbiztonság garantálására, a kibervédelmi feladatok ellátására, a nemzeti létfontosságú információs infrastruktúra zavartalan működésének biztosítására Magyarországnak készen kell állnia."*[31]

Azt szintén megfogalmazza a stratégia, hogy mindezeket hogyan lehet kivitelezni, azaz milyen kiinduló feltételei vannak a fentiek sikeres végrehajtásának: *„Elsődleges feladat a kibertérben ténylegesen jelentkező vagy potenciális kihívások, kockázatok és fenyegetések azonosítása és nyomon követése, a kormányzati koordináció erősítése, a kibertér jogi szabályozásának fejlesztése, a felhasználók biztonságtudatos viselkedésének elősegítése, a kormányzati infokommunikációs rendszerek, a nemzeti létfontosságú információs infrastruktúra, a minősített információk és a nemzeti adatvagyon védelmének erősítése, valamint a kiberbiztonsággal kapcsolatos nemzetközi együttműködés bővítése."*[32]

Az átfogó stratégiai feladatok és eszközök között megjelenik a katonai területen szükséges tennivalók felsorolása is: *„A katonai kibervédelmet növekvő mértékben alkalmassá kell tenni a haderő kinetikus műveleteinek kibertérbeli támogatására, ki kell alakítani a kiberműveletekben alkalmazható offenzív képességeket. Ennek érdekében fejleszteni kell a Magyar Honvédség kibervédelmi és kiberműveleti erőit."*[33]

Nagyon fontos a fenti idézetben foglalt katonai kiberműveleti erők fejlesztése, amely magában kell foglalja az offenzív, tehát a támadó kiberképességek fejlesztését is. Ez komoly előrelépés ahhoz képest, hogy sokáig még szakmai körökben is csak nagyon óvatosan fogalmazódott meg a támadó kiberképességek fejlesztésének igénye. Biztonságpolitikai oldalon pedig nagyon sokáig tabunak számított ez a fajta – egyébként sok esetben kicsit paradox

[30] NBS 2020: 101. pont.
[31] Uo. 159. pont.
[32] Uo.
[33] Uo.

módon éppen a – védelmet szolgáló tevékenység,[34] illetve az ahhoz szükséges képességek kialakítása.

A stratégia látszólag általánosságban fogalmazza meg a Magyar Honvédség fejlesztését: *„A Magyar Honvédségnek jól felszerelt és jól kiképzett erőkkel, valamint rugalmas, hatékonyan alkalmazható, telepíthető és fenntartható, a szükséges mértékben interoperábilis képességekkel kell rendelkeznie, a mennyiségi mellett a minőségi mutatók javítására törekedve."*[35] A meghatározott fejlesztés azonban már magában foglalja többek között a hibrid fenyegetések elleni felkészülést is, valamint ezzel összefüggésben meghatározza azokat a műveleti tereket is, ahol az MH-nak alkalmazásra alkalmasnak kell lennie. Ilyen műveleti tér a hagyományos szárazföld és levegő mellett az új dimenzióként megjelent kibertér[36] is: *„A haderőt úgy kell fejleszteni, hogy képes legyen hatásokat kiváltani a hazánk szempontjából releváns összes műveleti térben: a szárazföldön, a levegőben és a kibertérben egyaránt."*[37]

Nagyon fontos elemként került be a stratégiába a kibervédelemhez szükséges kutatás-fejlesztés hazai bázisú kiépítésének és fenntartásának feladata: *„Elengedhetetlen a nemzeti kibervédelmi képességek hazai bázisú kutatás-fejlesztéssel megalapozott erősítése, a korszerű technikai eszközök biztosítása. A kibervédelmi feladatok összetettsége miatt partnerséget kell kialakítani az állami és a magánszektor szereplői, az oktatási és a tudományos intézmények és az egyéni felhasználók között."*[38]

A hatékony védelem a kibertér jellege miatt nemzetközi együttműködés[39] nélkül nem működik. Ennek megfelelően a stratégia ezen a területen a következőket határozza meg: *„A kibertérrel kapcsolatos kihívások hatékony kezelése nemzetközi együttműködés nélkül elképzelhetetlen. Aktívan részt veszünk a globális kibertérben való felelős viselkedést szabályozó normák*

---

[34] A paradoxon itt abból adódik, hogy számos esetben a támadás az egyetlen hatékony megoldás a kibervédelem eszköztárában. Természetszerűleg az attribúciónál tárgyalt módon ebben az esetben is igaz az a vitathatatlan tény, amely a potenciális támadó meghatározásának bizonytalanságát jelenti. Ez nem más, mint az, hogy hogyan tudjuk eldönteni, hogy ki és mikor fog majd a jövőben megtámadni minket a kibertérben. Hiszen a védelmünk akkor lesz a leghatékonyabb, ha a támadást még azelőtt megakadályozzuk – például egy általunk a potenciális támadó információs és számítógépes rendszereit célzó támadással –, hogy a saját rendszereink irányába a támadás megindult volna.

[35] NBS 2020: 135. pont.

[36] A NATO 2016-ban nyilvánította a kiberteret a „műveletek" terévé (domain of operations) a varsói csúcsértekezleten. Lásd Warsaw Summit Communiqué – Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8–9 July 2016. NATO E-Library, 09. 07. 2016. www.nato.int/cps/en/natohq/official_texts_133169.htm (Letöltés időpontja: 2020. 05. 11.) Hazánkban a kibertér műveleti térré való elismerését a Honvédelmi törvény (Hvt.) 2018-as módosításában megjelent meghatározás jelentette: „…műveleti terület: a műveleti tervben meghatározott és kijelölt földrajzi terület és a felette levő légtér, továbbá a kibertér…" Lásd 2011. évi CXIII. törvény a honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről. 80. § 22. pont. https://net.jogtar.hu/jogszabaly?docid=a1100113.tv (Letöltés időpontja: 2020. 06. 05.)

[37] NBS 2020: 135. pont.

[38] Uo. 160. pont.

[39] A nemzetközi kibervédelmi együttműködés természetesen nem volt példa nélküli eddig sem. Az EU és a NATO keretében történő kibervédelmi együttműködés mellett talán kevésbé ismert, de nagyon fontos az olyan regionális együttműködés, mint például a Közép-európai Kiberbiztonsági Platform (Central European Cyber Security Platform, CECSP). Ezt a fórumot cseh–osztrák kezdeményezésre 2013-ban, Magyarország, Lengyelország és Szlovákia támogatásával és együttműködésével hozták létre. A platform egyik legfontosabb célja a szomszédos országok intenzív együttműködésének kialakítása a kiberbiztonság területén, amely magában foglalja az információcserét, a kiberfenyegetések és a potenciális kibertámadások területén megjelenő tudás, valamint a jó gyakorlatok megosztását. Lásd Nemzeti Kibervédelmi Intézet – Nemzetközi kapcsolatok. https://nki.gov.hu/intezet/tartalom/nemzetkozi-kapcsolatok/ (Letöltés időpontja: 2020. 05. 15.)

és a globális kiberbiztonság fokozására szolgáló bizalomerősítő intézkedések kidolgozására és végrehajtására irányuló nemzetközi erőfeszítésekben."[40]

Mindezeket összefoglalva: a kibertér, a kiberbiztonság és a kiberműveletek megjelenése az új Nemzeti Biztonsági Stratégiában nemcsak azok statisztikailag nagyobb számú megjelenése miatt hangsúlyos, hanem azok fontos üzenete, illetve az így megjelenő feladatok miatt is.

Az egyik leghangsúlyosabb rész kétségkívül a kibertámadásokra adható potenciális fizikai válaszok taglalása, amely a fenti megállapítások okán egyrészt az elrettentést, másrészt a terület felértékelődött fontosságát is jelenti.

AZ ÚJ NEMZETI BIZTONSÁGI STRATÉGIA KIBERTÉRI SZABÁLYZÓKRA ÉS SZERVEZETEKRE GYAKOROLT VÁRHATÓ HATÁSAI

Az új Nemzeti Biztonsági Stratégiában a fentiekben részletezett módon markánsan, számos területre hatást gyakorolva jelenik meg a kibertér és annak számos kihívása. Ezeknek a kihívásoknak a kezelése mind jogszabályi, mind szervezeti változtatásokkal és az azokban foglalt fejlesztésekkel, valamint a kibertérre hatást gyakorolni képes, a különböző szinteken megjelenő képességnövekedéssel kell együtt járnia.

Minderről maga a stratégia is rendelkezik a következő módon: *„A biztonság egyes részterületeiért felelős állami szervezeteknek a Magyarország Nemzeti Biztonsági Stratégiában megfogalmazott iránymutatásokkal összhangban kell megalkotniuk és felülvizsgálniuk a tevékenységükre vonatkozó szakági szabályzókat, különös tekintettel a nemzeti katonai, a rendészeti, a nemzetbiztonsági, a terrorelhárítási, a katasztrófavédelmi, a kiberbiztonsági és a migrációs területekre."*[41]

A fentiekből kitűnik, hogy a jogszabályi változásokat maga a stratégia is explicit módon indukálja, de nem feledkezhetünk meg a honvédelmi törvény – a stratégia előtt nem sokkal megjelent – változásáról,[42] illetve az abban a kibertéri műveletek egyes szabályait meghatározó, újonnan a törvénybe bekerült feladatokról sem, hiszen azok mintegy előszelei voltak a stratégia által kért jogszabályi változásoknak.

Ennek megfelelően ezen a helyen is célszerű kis kitérőt tennünk ezekre a változásokra, hiszen a honvédelmi törvény (Hvt.) igen markáns változásokat hozott ezen a téren is 2020. január 1-jétől. Bár ez a törvény időben kissé megelőzte az új nemzeti biztonsági stratégiánkat, mégis az abban foglaltak filozófiájukat tekintve összhangban vannak a stratégiában a kibertérre megfogalmazott egyes kitételekkel.

A honvédelmi törvényt az Országgyűlés 2019 végén módosította, amely módosítások 2020. január 1-jétől léptek hatályba. Jelen írás témájának szempontjából az egyik legfontosabb változás a törvényben a kibertér igen markáns megjelenése volt. A Hvt. e módosítást követően előírja, hogy a kormánynak hazánk védelmi felkészültsége biztosításának céljából meg kell határoznia mindazokat a feladatokat, amelyek a kibertéri műveletekhez, a kibervédelemhez, a kibertámadások megelőzéséhez és a kibertéri felkészüléshez szükségesek. A törvény mindezek mellett meghatározza mindazokat a szabályokat, amelyek ezeknek a feladatoknak a végrehajtásához szükségesek. A törvény azt is meghatározza, hogy ezek a feladatok és

[40] NBS 2020: 162. pont.

[41] Uo. 178. pont.

[42] 2011. évi CXIII. törvény a honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről.

esetleges műveletek egyes esetekben kivételes döntéshozatali mechanizmusokat jelentenek, azaz a kormánynak külön döntést kell hoznia róluk.[43] A Hvt.-be számos, a Magyar Honvédségre vonatkozó kiberrelációjú pont is bekerült. Az egyik ilyen, a kibertér vonatkozásában mindeddig hiányzó kitétel az, hogy a Magyar Honvédség a kibertérben műveleteket hajthat végre. Mindezeket nyilvánvalóan fegyverhasználati jog nélkül teheti meg.[44] A Hvt. értelmében a fegyverhasználat nélkül ellátható műveletek: *„…a Magyarország biztonságát, honvédelmi érdekeit sértő, veszélyeztető, katonai jellegű kibertér műveletek, kibertérre ható cselekmények vagy kibertámadások elleni fellépés, illetve az ezekkel összefüggő szövetségesi, illetve nemzetközi együttműködési keretben megvalósuló feladatok.'*[45] Így ez a pont felhatalmazást ad és megteremti a lehetőségét, hogy az MH a kibertérben is műveleteket hajtson végre, illetve az azzal összefüggő – például felkészülés, támadások megszakítása – kibertéri feladatokat egyáltalán folytasson.

Mindezekkel összhangban a törvény számos feladatot is meghatároz a Magyar Honvédség részére. Ezeknek megfelelően az MH-nak folyamatosan biztosítania kell a honvédelmi szervezetek, gyakorlatok és műveletek kibertérből érkező fenyegetésekkel és támadásokkal szembeni védelmét.[46] A védelem mellett a honvédelmi szervezeteket érő kibertámadások esetén az esetleges támadást az MH kibertér műveleti erőinek meg kell szakítaniuk, illetve amennyiben a kibertámadások olyan súlyosak, hogy azok Magyarország biztonságát fenyegetik, akkor a támadó rendszerekkel szemben katonai kibertéri műveletekkel kell fellépnie.[47] Ezek a jogi megfogalmazások és az azok mentén megvalósítandó feladatok önmagukban is hatalmas előrelépést jelentenek, és komoly felhatalmazást is adnak a katonai kibertér műveleti erők számára. Nyilvánvalóan ez a felhatalmazás és az az alapján végzett kiberműveletek a védelmet szolgálják, és nem jelentenek olyan jogalapot, amely alapján nem védelmi jellegű kibertámadások lennének kivitelezhetőek.[48] A feladatok mellé a Hvt.-be bekerült még egy további, szintén előremutató pont is, amely egy, a honvédelmi miniszter által kijelölt kibervédelmi ügyeletes parancsnoki funkció beiktatását határozza meg. Ez a kibervédelmi ügyeletes parancsnok rendelheti el – külön döntések alapján – a fentiekben említett támadások megszakítását, valamint az említett támadó rendszerekkel szembeni katonai kibertér műveletek megindítását. Természetesen a törvény meghatározza azokat az eseteket is, amikor ezek a kibertér műveleti tevékenységek elrendelhetők, illetve végrehajthatók, de mindezek csak a kormány külön döntése alapján indulhatnak meg.

---

[43] Hvt. 21. § (1) o) pont.

[44] Ennek vonatkozásában azonban felmerül a kérdés, hogy a kibertérben mi minősül fegyvernek. Egy adott kibertéri művelet végrehajtásához használt szoftver vagy informatikai eljárás fegyvernek minősülhet-e, amennyiben az offenzív célokat szolgál? Ezekre a kérdésekre azonban a nemzetközi jog ma még nem tud adekvát és megfelelő válaszokat adni.

[45] Hvt. 36. § (2) g) pont.

[46] Hvt. 62/A. § * (1) bek.

[47] Mindezeket a Hvt. a következőképpen tartalmazza: „A Honvédség katonai kibertér műveleti erői jogszabályban meghatározottak szerint folyamatosan ellátják a) a honvédelmi szervezetek, gyakorlatok, műveletek kibertérből érkező fenyegetésekkel és támadásokkal szembeni védelmét, az arra történő felkészülést és a kapcsolódó biztonsági feladatokat, b) az a) pont szerinti feladatokkal összefüggésben a folyamatban lévő, kibertérből érkező támadás megszakításához szükséges intézkedések végrehajtását, vagy annak kezdeményezését, valamint c) külön döntés szerint a Magyarország biztonságát, honvédelmi érdekeit, vagy szövetségesi kötelezettségeit sértő vagy fenyegető rendszerekkel szembeni katonai kibertér műveleti fellépést." Lásd Uo.

[48] Ezt támasztja alá a törvény szövege is, amely rögzíti: „...az alkalmazott intézkedésnek a folyamatban lévő támadással arányosnak kell lennie és törekedni kell arra, hogy az a támadás megszakításán túli eredményre, sérelemre ne vezessen..." Lásd Hvt. 62/A. § * (3) b) pont.

Ilyen esetek például a nemzetközi műveletek alkalmával, honvédelmi veszélyhelyzet idején vagy különleges jogrendben lehetségesek.[49]

Visszatérve az új Nemzeti Biztonsági Stratégiára, illetve az abban megfogalmazottakra, természetesen további – ágazati – stratégiai és szervezeti változások szükségesek. A védelempolitikát alapvetően meghatározó, az NBS-re épülő egyik legfontosabb ágazati stratégia a Nemzeti Katonai Stratégia (NKS), amelynek szintén meg kell újulnia. Az NKS-nek az új Nemzeti Biztonsági Stratégiával harmonizáló átalakítása jelenleg folyamatban van, az még nem jelent meg, így jelen tanulmány írásakor nem hivatkozható. Ugyanakkor általánosságban néhány, a kibertérrel összefüggő kérdés már felvázolható ezzel a stratégiával kapcsolatosan is.

Az új Nemzeti Katonai Stratégia elkészítése során a már meglévő, illetve a kialakítandó kiberképességek és azok hatékony alkalmazása érdekében ki kell térni mindazokra a műveleti terekre, amelyekben a kiberműveletek hatékonyan tudják támogatni a Magyar Honvédség alaprendeltetésből adódó katonai műveleteit. Ez nyilvánvalóan a kibertér mellett a fizikai dimenziókat is érinti, mert a konkrét kiberműveletek integrálása mind a szárazföldi, mind a légierő műveleteibe szükséges a háborús, de akár az olyan időszakokban vagy konfliktusokban is, amelyek még nem érik el a háborús küszöböt. Ugyanígy fontos a kiberműveletek különleges műveleti erők feladatrendszerébe történő integrálása, hiszen a háborús küszöb alatti konfliktusok időszakában a különleges műveleti erők játsszák az egyik legfontosabb katonai erőt.

Itt szintén szükség van egy kis kitérőre, amely az információs műveletek területét jelenti. Napjainkban – békeidőben – az egyik legnagyobb kihívást a különböző információs műveleti elemek alkalmazása jelenti számos helyen a világban. Ezeken belül számos kibertéri tevékenységet is tetten érhetünk a politikai döntések befolyásolásától kezdve a lakosság befolyásolásán át a gazdasági célú és az azt befolyásolni kívánó kiberkémkedésig. Ugyanakkor, bár általában az információs műveletekről mint új elemekről beszélünk, az információs műveletek doktrinális háttere meglehetősen hosszú múltra tekint vissza, amelyben világosan nyomon követhető e műveletek fejlődéstörténete. A korai, 1990-es évek második felét jelentő, ma már klasszikusnak számító információs műveletektől, amelyek még alapvetően katonai tevékenységek koordinált alkalmazásában határozták meg ezeket a műveleteket, eljutunk a 2010-es évek második feléig, amikor a cél már a befolyásolás. Ráadásul ma már az információs műveletek egyik leghatékonyabb kivitelező eszközévé váltak a kibertérben működő szolgáltatások. Ezeken keresztül – nyilván sok esetben azokat manipulálva – lehet az információs műveletek célcsoportjait elérni. Ezek a célcsoportok ma már elsősorban nem katonai, hanem sokkal inkább a lakossági, a politikai vagy gazdasági szereplők.

Az információs műveletek egyik legfontosabb filozófiai alapja az abban foglalt különböző elemek koordinált és hatásaikban egymást kiegészítő vagy azokat erősítő tervezése és alkalmazása. Mindezek katonai alkalmazása azt is feltételezi, hogy már a műveletervezés időszakában, de különösen a műveletek végrehajtásakor az információs műveleteket a parancsnok céljainak végrehajtása érdekében koordináltan tervezik és hajtják végre.[50] Ehhez szükséges egy olyan szervezeti keret, amely alkalmas erre a koordinációs feladatra. Mivel a kiberműveletek az információs műveletek szerves részét képezik, ezért ennek a koordinációs

[49] Hvt. 62/A. § (6) bek.
[50] Haig: i. m.

szervezetnek alkalmasnak kell lennie a kiberműveletek többi információs műveletekkel történő koordinálására is.[51]

Mindezeknek megfelelően az új katonai stratégiának az információs műveletek és a kiberműveletek kölcsönhatásait, azok katonai műveletekben betöltött szerepét is vizsgálnia kell.

A következő ágazati stratégia, amelynek szükségszerűen meg kell újulnia, az a Nemzeti Kiberbiztonsági Stratégia. Hazánk korábbi Nemzeti Kiberbiztonsági Stratégiája[52] 2013-ban született, így azt az információtechnológia hatalmas sebességű változásait is figyelembe véve már az elmúlt években célszerű lett volna felülvizsgálni. Ugyanakkor ez csak részben történt meg, hiszen bár elkészült 2018 végére a Nemzeti Hálózat és Információbiztonsági Stratégia,[53] de az mégsem fedi le teljes egészében a nemzeti kiberbiztonság minden fontos (stratégiai) kérdését.

Az új Nemzeti Kiberbiztonsági Stratégiának építenie kell azokra a stratégiai célokra, amelyeket az új Nemzeti Biztonsági Stratégia meghatározott. Ezzel kapcsolatban számos feladatot tudunk azonosítani, amelyek közül sok közvetlenül, több azonban csak közvetve következtethető ki a Nemzeti Biztonsági Stratégiában megfogalmazottakból. Ezek közül talán az egyik legmarkánsabb a súlyos kibertámadásokra adandó fizikai támadások összefüggésének kezelése lehet, hiszen ebben az esetben a kiber- és a fizikai tér, illetve az abban lévő tevékenységek összehangolt szabályozását – stratégiai értelemben azok stratégiai együttműködési alapjainak megteremtését – kell elvégezni. Ugyanakkor az új kiberbiztonsági stratégiának legalább ekkora figyelmet kell szentelnie az NBS-ben is kihívásként említett mesterséges intelligencia, valamint az autonóm rendszerek miatt szükséges kibervédelmi kérdéseknek. Az új kiberstratégiának kezelnie kell a kiberműveletek, ezen belül is a katonai kiberműveletek kérdését is.

A jogszabályi és doktrinális változásokon túl az új Nemzeti Biztonsági Stratégiának és az abban foglalt kibertéri hatásoknak számos szervezeti változást is kell indukálniuk.

---

[51] A jelenlegi doktrinális háttér ezt még nem támasztja alá teljes egészében, hiszen a jelenlegi hazai, a NATO, de még az Amerikai Egyesült Államok információs műveleti doktrínája is a hagyományos információs műveleti elemekkel számol, úgymint műveleti biztonság, katonai megtévesztés, lélektani műveletek, elektronikai hadviselés és számítógép-hálózati műveletek. Ugyanakkor ma már – a fentieknek megfelelően – az információs műveletek sokkal inkább befolyásolást jelennek, semmint konkrét katonai tevékenységet (amely befolyásolás ráadásul már békeidőszakban is megvalósul). Ez a befolyásolás a kibertéren, az abban megvalósuló szolgáltatásokon keresztül nagyon hatékonyan érhető el, amiből az is következik, hogy a kiberműveletek egyre inkább az információs műveletek részét képezik. A kérdés másik olvasata az a klasszikus információs műveleti elem, a számítógép-hálózati műveletek egyre nagyobb térnyerését jelenti. Ez azt is jelenti, hogy ezeket a műveleteket összefoglaló néven kiberműveleteknek hívjuk, amelyek célja – az információs műveletek céljait támogatva – a szemben álló fél vezetési rendszereinek akadályozása, az információs fölény kivívása, majd annak vezetési fölénnyé való váltása.

[52] 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról. http://njt.hu/cgi_bin/njt_doc.cgi?docid=159530.238845 (Letöltés időpontja: 2020. 06. 05.)

[53] Ez a stratégia szintén kormányhatározat – 1838/2018. (XII. 28.) Korm. határozat – formájában jelent meg. Ugyanakkor érdemes arra felhívni a figyelmet, hogy nagyon sok ország ezeket a stratégiáit nemcsak hazai, hanem nemzetközi szinten is publikálja, általában angol nyelven téve azokat elérhetővé a nemzetközi közösség számára. Ezek a stratégiák sok esetben az adott ország politikai vezetésének kinyilatkoztatásai is, így azon kívül, hogy az adott ország vezetőjének a stratégiához írt bevezetőjével kezdődik, nagyon jól szerkesztett, látványos kiadványelemekkel – például borító, színes belső szerkesztés stb. – ellátott anyag. Az ilyenfajta kiadványok nyilvánvalóan több célt szolgálnak, hiszen azon kívül, hogy a nemzetközi közösség számára elérhetővé válnak, a másik eredmény az adott ország ezen a területen vallott nézeteinek, értékeinek és akár érdekeinek a kinyilatkoztatása is.

A közigazgatás kiberbiztonságának és kibervédelmének szervezeti háttere esetében az egyes szervezetek vagy szervezeti elemek közötti hatékony koordináció elengedhetetlenül fontos. Ugyanakkor jelen írás a kibertérrel kapcsolatos szervezetfejlesztési igények közül mégis elsősorban a Magyar Honvédségre koncentrál. Az MH fejlesztése során általánosságban a kibertér műveleti képességek fejlesztése, illetve a kibertéri műveletek tervezéséhez, szervezéséhez és vezetéséhez szükséges szervezeti keretrendszer kialakítása az első cél. Az ezeket a feladatokat a jövőben megvalósító szervezetnek három nagy csoportra osztható feladategyüttese várható: 1. kibervédelmi és kiberműveleti fejlesztések koordinálása és ezek vezetése; 2. a kiberműveleti tevékenységek vezetése és végrehajtása különböző szinteken (hadműveleti szint, harcászati szint); 3. a kiberműveletek integrálása a szárazföldi csapatok és a légierő műveleteibe. Ezeknek a feladatoknak az ellátása érdekében létrehozandó katonai szervezetnek természetszerűleg rendelkeznie kell kutatás-fejlesztési kapacitással is.[54]

A kibertéri műveletek alapvető információigényét több forrásból kell kielégíteni. Ezek a források lehetnek a nemzetbiztonsági szolgálatok forrásai, a kiberbiztonsági adatbázisok, valamint saját tevékenységben ellátott elemző és értékelő munka eredményeként létrejövő adatbázisok is. Ez utóbbi nem példa nélküli, hiszen az elektronikai hadviselésben a saját műveletek és tevékenységek szemben álló félre és/vagy technikai eszközökre – az elektronikai hadviselés esetében az elektromágneses kisugárzó eszközökre vagy az azok által továbbított adatok és információk minőségére – gyakorolt hatásainak elemzése régóta bevett és nagyon jól működő gyakorlat. Ennek számos oka van, hiszen alapvetés ilyen tevékenységek során is az előzetes szimuláció; a reális szimulációnak azonban megbízható és sok esetben valós idejű információkra kell/kellene épülnie. Ezek azonban nem minden esetben állnak rendelkezésre, vagy például az említett nem baráti elektromágneses kisugárzások esetében nem mindig pontosak. Ezért a gyakorlati tapasztalatok, illetve a különböző tevékenységek során gyűjtött adatokra épülő hatáselemzés jó közelítéssel már megfelelő alapot nyújt egy ugyanilyen vagy hasonló tevékenység megtervezéséhez és kivitelezéséhez a jövőben. Ennek analógiája a kibertér műveleti szervezetek számára is követendő.

Ennek megfelelően az említett katonai kibertér műveleti szervezetnek rendelkeznie kell megfelelő technikai és humán elemző- és értékelőképességgel. Ez természetesen sem volumenében, sem feladataiban nem váltja és nem válthatja ki a nemzetbiztonsági szolgálatok ilyen irányú tevékenységét.[55]

A kiberműveletek szervezeti hátterének kialakítása és fejlesztése a Magyar Honvédségben megkezdődött. Az új Nemzeti Biztonsági Stratégiából levezethető iránymutatások ezt a munkát már nagyban segítik és meg is gyorsíthatják.

---

[54] Nyilvánvalóan ezeknek a szervezeteknek számos más feladata is várható. Az egyik ilyen feladat az oktatás, képzés és kiképzés rendszerének és akár intézményrendszerének a megteremtése. Ez nemcsak a saját állomány felkészítését jelenti, hanem a Magyar Honvédség egészére vonatkozó, elsősorban kibervédelmi képzéseket jelent. Ezekkel a képzésekkel lehetséges emelni a kiberbiztonsági tudatosság és elkötelezettség szintjén. Nyilvánvalóan ezek a képzések és kiképzések az eltérő szinteken eltérő célokkal is párosulnak, hiszen amíg az említett kiberbiztonsági tudatossági képzéseket minden szinten folytatni kell, addig a kiberműveletek stratégiai kérdéseit a katonai felső vezetés szintjén, de a konkrét technikai végrehajtást műveleti és harcászati szinten szükséges oktatni.

[55] Ennek oka az, hogy egy katonai szervezet nem rendelkezik nemzetbiztonsági jogosultsággal. Természetesen van ellenpélda is, hiszen a német Kiber- és Információs Parancsnokság (Das Kommando Cyber- und Informationsraum, CIR) rendelkezik bizonyos nemzetbiztonsági felhatalmazásokkal. Lásd Kommando Cyber- und Informationsraum. https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum/kommando-und-organisation-cir/kommando-cyber-und-informationsraum (Letöltés időpontja: 2020. 05. 15.)

ÖSSZEGZÉS, KÖVETKEZTETÉSEK

Jelen írás célja az volt, hogy a 2020 áprilisában megjelent hazai Nemzeti Biztonsági Stratégia kibertér vonatkozású megállapításait bemutassa, illetve kitérjen ezeknek a jövőbeni szabályozást és szervezetkialakítást meghatározó tényezőire. Mindezeket a dolgozat alapvetően csak a katonai terület szempontjából mutatta be úgy, hogy ahhoz felvezetést a korábbi, 2012-es Nemzeti Biztonsági Stratégia kiberteret érintő megállapításai szolgáltak.

Az új Nemzeti Biztonsági Stratégia nagy változást és igazi újdonságokat is jelent a kibertérrel kapcsolatosan. Az elmúlt évek során egyre inkább felértékelődött azoknak az infokommunikációs rendszereknek a szerepe, amelyek a társadalom egésze működésének az alapját is jelentik. Ebből következően ezeknek a rendszereknek a védelme és a biztonsága ma már nemzetbiztonsági érdek, és így stratégiai cél is egyben. Mindezeket rögzíti a stratégia, és ennek a biztonságnak a megteremtéséhez stratégiai célokat is megfogalmaz. A dokumentum mindezt egységes szemlélettel, világos célok megfogalmazásával teszi meg.

Az egyik legmarkánsabb elem a stratégiában a kibertámadásokra a fizikai térben adható lehetséges válaszok megjelenése. Ez mindamellett, hogy komoly előrelépés és a terület felértékelődését is indikátorként jelzi, komoly elrettentő hatást is jelent. Ez a stratégia az első olyan hivatalos kormányzati dokumentum, amely mindezt kimondja és rögzíti.

A stratégiában igen markánsan megjelenik a Magyar Honvédség kibertéri szerepe és annak feladatai is. A stratégia meghatározza, hogy a Magyar Honvédséget úgy kell fejleszteni, hogy annak kibervédelmi és kiberműveleti erői a kinetikus erők műveleteinek támogatására is legyenek alkalmasak. Mindemellett ennek a fejlesztésnek az offenzív kiberképességek fejlesztését is magában kell foglalnia.

A stratégia fő céljainak támogatására, illetve azok végrehajtásához számos ágazati stratégia átalakítása, aktualizálása vagy éppen megteremtése szükséges. Ilyen ágazati stratégia a Nemzeti Katonai Stratégia, illetve a Nemzeti Kiberbiztonsági Stratégia. Ezekben meg kell jeleníteni a katonai kiberműveleti képességek helyét és szerepét is.

A NBS-nek szervezeti változásokat is kell indukálnia. Katonai téren az egyik ilyen szervezeti változás a katonai kibertér műveleti erők szervezetének megteremtése. A katonai kibertér műveleti képességek szervezeti fejlesztésének együtt kell járnia a kibervédelmi oktatás, képzés és kiképzés intézményesítésével és annak a teljes katonai képzési és kiképzési rendszerbe történő integrálásával.

Mindezeket összefoglalva: az új Nemzeti Biztonsági Stratégia világos iránymutatást és egyértelmű célokat fogalmaz meg a kibertér katonai védelme és műveletei, valamint az ahhoz szükséges szervezetrendszer fejlesztése érdekében. A stratégiában foglalt, a kibertérre vonatkozó olyan kitételek, mint az említett offenzív képességek megteremtésének szükségessége a Magyar Honvédségen belül, valódi biztonság- és védelempolitikai elmozdulást jelentenek a korábbi Nemzeti Biztonsági Stratégiához képest.

FELHASZNÁLT IRODALOM

1035/2012. (II. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról. Magyar Közlöny, 2012/19., 1378–1397. https://2010-2014.kormany.hu/download/f/49/70000/1035_2012_korm_hatarozat.pdf

1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról. http://njt.hu/cgi_bin/njt_doc.cgi?docid=159530.238845

1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról. Magyar Közlöny, 2020/81., 2101–2119. https://magyarkozlony.hu/dokumentumok/6c9e9f4be48fd1bc620655a7f249f81681f8ba67/letoltes

1656/2012. (XII. 20.) Korm. határozat Magyarország Nemzeti Katonai Stratégiájáról. https://net.jogtar.hu/getpdf?docid=A12H1656.KOR&targetdate=&printTitle=1656/2012.+%28XII.+20.%29+Korm.+hat%C3%A1rozat&getdoc=1

2011. évi CXIII. törvény a honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről. https://net.jogtar.hu/jogszabaly?docid=a1100113.tv

AJP 3.20 – Allied Joint Doctrine for Cyberspace Operations. Edition A Version 1. 2.4. NATO Standardization Office, 2020.

Haig Zsolt: *Információs műveletek a kibertérben*. Dialóg Campus, Budapest, 2018.

Kommando Cyber- und Informationsraum. https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum/kommando-und-organisation-cir/kommando-cyber-und-informationsraum

Kovács László: *Kiberbiztonság és -stratégia*. Dialóg Campus, Budapest, 2018.

Munk Sándor: *A kibertér fogalmának egyes, az egységes értelmezést biztosító kérdései*. Hadtudomány, 2018/1., 113–131. http://real.mtak.hu/77921/1/HT20181_115_133_u.pdf
DOI: 10.17047/HADTUD.2018.28.1.113

Nemzeti Kibervédelmi Intézet – Nemzetközi kapcsolatok. https://nki.gov.hu/intezet/tartalom/nemzetkozi-kapcsolatok/

The DoD Cyber Strategy. The Department of Defense, Washington, 17. 04. 2015. https://archive.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf

Warsaw Summit Communiqué – Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8–9 July 2016. NATO E-Library, 09. 07. 2016. www.nato.int/cps/en/natohq/official_texts_133169.htm