6. fejezet

Magánbiztonsági vállalatok szerepe az állami műveletekben

Koller Marco

Bevezetés

Az elmúlt évtizedekben a biztonsággal kapcsolatos általános felfogás módosult. A világban, így Európában is negatív irányban változott a biztonsági helyzet, ami kihat a kibertér biztonságára is. Az utóbbi évtizedekben a technológiát jellemző robbanásszerű fejlődés, kiemeltképpen a kiberteret érintően, a fejlődés mellett egyértelműen indukálta a biztonsági kockázatok növekedését is.[1]

Megállapítható, hogy a fentiekben is említett fejlődés mentén létrejövő digitális társadalmak digitális hadsereget hoztak és hoznak létre. A kibertér, kiberfegyverek és kiberműveletek értelmezése multidiszciplináris megközelítést igényel, figyelemmel arra, hogy ezen témakörök több tudományterületet is átfednek, továbbá a kiberműveletek egyre szélesebb körű alkalmazása szükségessé teszi a különböző állami szervek, illetve a kutatók és a magánvállalatok közötti kommunikációt és összefogást, hiszen a „kibertérben végrehajtott műveletek, azaz a kiberműveletek, vagyis az informatikai rendszerek támadása és védelme a katonai és politikai stratégiaalkotás részét képezi".[2]

A kibertérben végbemenő különböző támadások elhárítása a mai világban kiemelt prioritással rendelkező problémává vált a világ országai számára. A kiberbiztonság fejlesztése elengedhetetlen a különböző információs rendszerek védelme érdekében, kiemeltképpen a létfontosságú intézmények esetén kell elhárítani a különböző kibertámadásokat.[3]

[1] Kovács László: A kiberbiztonság és a kiberműveletek megjelenése Magyarország új Nemzeti Biztonsági Stratégiájában. *Honvédségi Szemle,* 148. (2020), 5. 3–18.

[2] Dévai Dóra: A kiberfegyver koncepció evolúciója. *Hadmérnök,* 14. (2019), 2. 273.

[3] Nagy Zoltán András: Kiberháborúk kora. In *Magyar Tudomány Napja a Délvidéken – 2018. Tanulmánykötet.* Vajdasági Magyar Tudományos Társaság, 2018. 174–193.

https://doi.org/10.36250/01079_06

Egy-egy állam saját képességeinek fokozása mellett a biztonsági szektorban lévő hiátusok megoldása érdekében kiszervezheti tevékenységét magánbiztonsági vállalatoknak, vagy egyes esetekben olyan szolgáltatásokat vehet igénybe, amelyekkel az adott kormányzati szervezet a saját képességeit fejlesztheti mind humán, mind technikai téren.

A kutatás célja, módszertana

„A nemzetek szigorúan titkosan kezelik a kiberképességeikre vonatkozó adatokat, és a kiberműveleti stratégiáik is csak részben nyilvánosak, ezért csak korlátozott mennyiségű adat áll rendelkezésre."[4] Jelen fejezet célja, hogy bemutassa a magánszektor, magánbiztonsági cégek szerepvállalását az állami műveletekben, azon belül is kiemelten az állami kiberműveletekben. A tanulmány aktualitását magyarázzák a fentiekben már kifejtettek, azaz a kibertér növekvő szerepe a mindennapokban, valamint az állami felelősség növekedése. A növekedő felelősség növekvő felelősségvállalást, így humán, illetve technikai fejlődést is megkíván, amihez szinte nélkülözhetetlen a magánszektor bevonása is. A kutatás során a vonatkozó hazai és nemzetközi szabályozókat tekintettük át, kiemelten a magyar *Nemzeti Biztonsági Stratégiát* és *Kiberbiztonsági Stratégiát,* továbbá a *Tallinni kézikönyvet.* A jogi szabályozók mellett a hazai és a nemzetközi szakirodalmat vizsgáltuk meg, majd elemeztük a(z állami) kiberműveletekről, a magánbiztonsági vállalatokról és az azok kapcsolatáról szóló részeket. A tanulmány során a fogalmi háttér bemutatásán túl esettanulmányon keresztül kívánom ismertetni a magánbiztonsági vállalatok szerepét az állami műveletekben.

Fogalmi háttér

A következő fejezetben a témakör, illetve kontextusának komplex értelmezéséhez szükséges nagyobb és fontosabb definíciókat mutatom be, hogy az olvasó a későbbiekben kifejtetteket megfelelő minőségben tudja absztrahálni.

[4] Dévai (2019): i. m. 278.

A kibertér fogalma

A fogalmat a korábbi fejezetekben már több szempontból is körbejártuk, így emlékeztetőül csak annyit írunk, hogy a szót William Gibson alkotta meg az 1982-ben megjelent *Burning Chrome* című novellájában, illetve az 1984-ben kiadott *Neoromancer* című regényében. A kibertér fogalmát rendkívül sok szervezet próbálta megfogalmazni, így több adekvát definíció is létezik. Az Egyesült Államok Védelmi Minisztériuma által kiadott és 2016 februárjában pontosított katonai terminológiai szótárban meghatározottak szerint a kibertér „az információs környezet egy globális tartománya, amely tartalmazza az informatikai infrastruktúrák, a bennük tárolt adatok egymással összefüggő hálózatát, beleértve az internetet, a távközlési hálózatokat, a számítógép-rendszereket, valamint a beágyazott feldolgozó és vezérlő elemeket”.[5] Továbbá ki kell emelni a Magyarország hálózati és információs rendszerek biztonságára vonatkozó stratégiájáról szóló 1838/2018. (XII. 28.) Korm. határozatot, amely úgy fogalmazza meg a kiberteret, hogy: „globálisan összekapcsolt, decentralizált, folyamatosan változó elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét jelenti”.[6] A fenti megfogalmazásokon túl Haig Zsolt adja a legszélesebb körű megfogalmazását a kibertérnek, amely részletesen taglalja a definíció egyes elemeit, azok jelentőségét.

> „Az ember által mesterségesen létrehozott, dinamikusan változó tartomány, amelyben az információ gyűjtését, tárolását, feldolgozását, továbbítását és felhasználását végző, egymással hálózatba kapcsolt és az elektromágneses spektrumot is felhasználó infokommunikációs eszközök és rendszerek működnek, lehetővé téve ezzel az emberek és a különféle eszközök közötti folyamatos és globális kapcsolatot.”[7]

[5] Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms (2010. november 8.); Berki Gábor: Kiberháború, kiberkonfliktusok. In Pintér István (szerk.): *A virtuális tér geopolitikája. Tanulmánykötet.* Budapest, Geopolitikai Tanács Közhasznú Alapítvány, 2016. 248.

[6] A hálózati és információs rendszerek biztonságára vonatkozó Stratégia. Lásd: https://bit.ly/39PHBE4

[7] Haig Zsolt: *Információs műveletek a kibertérben.* Dialóg Campus, 2018. 15.

A kiberbiztonság és a kibertérben jelen lévő fenyegetések

A téma szempontjából elengedhetetlen tisztázni azt, hogy mit jelent a kiberbiztonság, illetve a kibertérben milyen jellegű fenyegetések vannak jelen. Magyarország hálózati és információs rendszerek biztonságára vonatkozó stratégiája szerint a kiberbiztonság:

> „a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez és működtetéséhez."[8]

A kormányhatározat jól szemlélteti, hogy a kiberbiztonság egy folyamat, illetve aktuális állapotot is jelöl, amely multidiszciplináris megközelítést igényel. Ahhoz, hogy egy adott állam vagy bármilyen szervezet szavatolhassa a kiberbiztonságot, tudni kell, hogy milyen típusú fenyegetések jelentkezhetnek a kibertérben. A kibervédelmi kihívások megfelelő kezeléséhez kiemelten fontos a kibertér és az abban előforduló események definiálása, a kibervédelmi fenyegetések tipizálása, a kibertérben tapasztalt incidensek kezeléséből levonható következtetések rendszerezése.[9]

A támadások alapvetően az informatikai rendszereken tárolt és kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, illetve a rendszerelemek rendelkezésre állása és funkcionalitása ellen irányulhatnak. Az adatok bizalmassága pedig azt jelenti, hogy azokat csak a jogosultak ismerhetik meg, használhatják fel, az adatok jogosultsági szintjének megfelelően. A sértetlenség azt jelenti, hogy nem történt benne illetéktelen változtatás. A rendelkezésre állás arra vonatkozik, hogy az adatot az arra jogosultak a szükséges helyen és időben elérhessék, használhassák.[10] A rendelkezésre álló szakirodalom több módon csoportosítja a kibertéri fenyegetéseket, azonban a legegyszerűbben és legérthetőbben Berki Gábor írta le, miszerint ezek: kiberbűnözés, kiberkémkedés, hacktivizmus, kiberterrorizmus, kiberhadviselés.[11]

[8] A hálózati és információs rendszerek biztonságára vonatkozó Stratégia.

[9] Fekete-Karydis Klára – Lázár Bence: A kibervédelem katonai dimenziói. *Honvédségi Szemle,* 148. (2020), 3. 44.

[10] Muha Lajos – Krasznay Csaba: *Az elektronikus információs rendszerek biztonságának menedzselése.* Budapest, Nemzeti Közszolgálati Egyetem, 2014. 13–14.

[11] Berki (2016): i. m. 250.

Kiberműveletek

Haig Zsolt *Információs műveletek a kibertérben* című munkája alapján kiberműveletnek az alábbiakat nevezzük:

> „a kibertérben érvényesülő információs képességek integrált, összehangolt és koordinált alkalmazására irányuló tevékenységek összessége, amelyek a műveletek célkitűzéseinek elérése érdekében, a kibertéri hálózatos infokommunikációs rendszereket felhasználva, a kognitív képességekkel közvetlenül, illetve a technikai képességekkel közvetetten hatásokat gyakorolnak a műveletekben részt vevő célközönség szándékára, helyzetértelmezésére és képességeire."[12]

A fentiek alapján jól látható, hogy a kiberművelet mint fogalom a legkönnyebben úgy írható le mint a kibertéri képességek alkalmazása, az adott célok elérésének érdekében. A Berki Gábor *Kiberháború, kiberkonfliktusok* című tanulmányában lefektetettek szerint a kiberműveleteket az alábbiak szerint lehet rendszerezni:

- *Támadó kiberműveletek.* Céljuk az ellenség hálózatba kötött informatikai rendszereinek feltérképezése, működésük befolyásolása, lerontása, megbénítása.
- *Védelmi kiberműveletek.* A saját informatikai rendszereink megvédése az ellenség támadó tevékenységével szemben (például vírusvédelmi szoftverek, tűzfalak).
- *Katonai információs hálózati műveletek*.[13] Céljuk a fentiekben leírtak támogatása, azok hátterének biztosítása (például felhasználói képzések, üzemeltetés és karbantartás).

Magánbiztonság

A magánbiztonságot gyakran relatíve új jelenségként tartják számon, holott a valóság az, hogy egyes formái már évszázadok óta léteznek. Nehéz adekvát fogalmat meghatározni a magánbiztonsággal kapcsolatban, figyelemmel arra, hogy a szakirodalomban rendkívül sok definíciót alkottak. A Christián László által meghatározott fogalom a következőképpen hangzik:

[12] Haig Zsolt: *Információs műveletek a kibertérben*. Budapest, Dialóg Campus, 2018. 15.
[13] Berki (2016): i. m. 262–263.

> „A magánbiztonság egy olyan ellenszolgáltatás keretében, piaci alapon működő, engedéllyel rendelkező vállalkozás (vagy természetes személy) által nyújtott szolgáltatás, amely a megbízó személyes biztonságát, tulajdonát védelmezi, elősegíti a jogainak teljesebb körű gyakorlását. A magánbiztonság felfogható egy halmazként, amely egyre nagyobb közös részhalmazt alkot a közrend, közbiztonság által képzett halmazzal, és van egy önálló, tekintélyes részhalmaza is."[14]

Látható, hogy nem lehet éles határvonalat húzni a közrend és közbiztonság, valamint a magánbiztonság fogalomkör közé, hiszen céljuk egy irányba mutat, azaz közös társadalmi és nemzeti érdek. Általában magánbiztonság alatt az alábbiakat értik: személyvédelem, magánnyomozás, közrend fenntartása, biztonsági ellenőrzések hatósági intézkedésre. Azonban a tágabban vett értelmezésben már idetartoznak a biztonsági szakértők, a biztonságtechnológiai szakemberek, a biztonsági képzés oktatói, továbbá a magánkatonai haderő (*private military company,* PMC). A magánbiztonsági tevékenységek köre nagyon sokszínű, mivel azok legfőképpen a megbízók igényeitől, szükségleteitől függnek.[15] Egy 2009-es ASIS-szimpóziumon[16] a szakértők a magánbiztonság tizennyolc alapkövét határozták meg az alábbiak szerint:

1. objektumvédelem,
2. személyvédelem,
3. információs rendszerek biztonsága,
4. nyomozások,
5. veszteségmegelőzés,
6. kockázatelemzés,
7. jogi aspektusok,
8. sürgősségi és veszélyhelyzeti tervezés,
9. tűzvédelem,
10. kríziskezelés,
11. katasztrófamenedzsment,
12. terrorelhárítás,
13. üzleti hírszerzés,
14. végrehajtói védelem,

[14] Christián László: Magánbiztonsági számvetés. In Dobák Imre – Hautzinger Zoltán (szerk.): *Szakmaiság, szerénység, szorgalom. Ünnepi kötet Boda József 65. születésnapja alkalmából.* Budapest, Dialóg Campus, 2018. 147–148.

[15] Rottler Violetta: Gondolatok a magánbiztonság köréből. *Magyar Rendészet,* 19. (2019), 4. 81–95.

[16] ASIS: American Society for Industrial Security, amelyet 1995-ben alapítottak. A közösség a magánbiztonsági szektor egyik legnagyobb szövetsége, már nemzetközi szinten működik.

15. munkahelyi erőszak elleni fellépés,
16. bűnmegelőzés,
17. bűnmegelőzés környezeti tervezéssel,
18. biztonsági építészet és mérnöki munka.[17]

A hagyományos őrzés-védelem mellett egyre hangsúlyosabb szerephez jut a magánbiztonság területén az információbiztonság, az adatvédelem, a logisztikai szolgáltatások, az üzleti hírszerzés stb. A magánbiztonsági iparág egyre fontosabb szerepet kap a nemzetközi biztonság területén.

A magánszektor és a kiberbiztonság kapcsolatának megjelenése a magyar stratégiai dokumentumokban

A 2020-as *Nemzeti Biztonsági Stratégiában* (a továbbiakban: Stratégia) 33 alkalommal szerepel a „kiber" kifejezés különböző kontextusokban. A „magán" kifejezés 2 alkalommal. Egyértelműen meghatározó szerep jut a kiberbiztonságnak a 2020-as *Nemzeti Biztonsági Stratégiában,* hiszen a jelenlegi technológiai fejlődés mellett az annak eredményeképpen létrejövő új típusú kihívások és kockázatok sem hagyhatók figyelmen kívül, az államnak muszáj volt reagálnia[18] a korábbi, 2012-ben megjelent stratégia óta bekövetkezett változásokra. A Stratégia alapvető érdekként definiálja, hogy: „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."[19] Ehhez kapcsolható elem a Stratégiában a kibervédelemhez tartozó, hazai bázisú kutatás-fejlesztés: „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."[20] Jelen pont világít rá, hogy az állam már a stratégiaalkotáskor is figyelembe vette azt, hogy szüksége van a magánszektorban jelen lévő, kiemelt fontosságú kibertudással rendelkező

[17] Nagyné Bereczki Szilvia – Nagy József: *Magánbiztonság és kritikus infrastruktúra védelem.* Budapest, 2014.
[18] Kovács (2020): i. m.
[19] 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról, 106. pont.
[20] 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról, 160. pont.

szakismeretre, szakemberekre, akiknek az integrálása a hazai kibervédelembe rendkívül fontos. Ugyanakkor kiemelendő, hogy a Stratégia kockázati faktorként is deklarálja a különböző magánszervezeteket a kibertérben, itt kifejezetten magánbiztonsági cégeket említ a jogalkotó.

> „A technikai fejlődéssel és vívmányainak elterjedésével folytatódik a biztonságot veszélyeztető, nehezen kontrollálható nem állami szereplők – például szervezett bűnözői körök, nemzetközi terrorszervezetek, kiberbűnözői csoportok, szélsőséges vallási közösségek, magán biztonsági cégek, egyes nem kormányzati szervezetek és egyéb transznacionális hálózatok – súlyának növekedése a nemzetközi biztonságpolitikában. Ezek mögött sokszor nehezen azonosítható érdekek és csoportok húzódnak meg, és könnyen szolgálhatnak rejtett állami szándékokat. Mindez átrendezi és áttekinthetetlenebbé teszi egyes térségek biztonsági helyzetét, ami hazánk számára is kihívást jelent."[21]

A fentiek okán egyértelműsíthető, hogy a magyar állam olyan nézőpontot képvisel, amely a kiberképességek állami növelését tűzte ki célul, annak érdekében, hogy a más szereplőkkel szemben csökkentse saját sebezhetőségét. A Stratégia megfogalmazza, hogy a kiberbiztonságot és a vonatkozó képességeket is növelni kell:

> „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."[22]

Azonban jól látható, hogy ennek szavatolása érdekében nem fogalmazza meg a magánszektor szerepkörét, annak ellenére, hogy elvitathatatlan e vállalatok szakértelme. Természetesen megérthető a magyar döntéshozók ódzkodása a biztonság kiszervezésével kapcsolatban, hiszen jól látható következményei lehetnek, amelyek a későbbi fejezetekben lesznek olvashatóak. A Stratégia továbbá kitér a katonai kiberműveletek témakörére is, deklarálja a kiberműveleti erők fejlesztését. Kiemelendő, hogy nem csupán a védekezésre alkalmas képességek fejlesztését,[23] hanem az offenzív képességek erősítését is leírja a stratégia, ami

[21] 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról, 69. pont.
[22] 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról, 159. pont.
[23] Kovács (2020): i. m.

nagy előrelépés ahhoz képest, hogy sokáig még szakmai körökben is csak nagyon óvatosan fogalmazódott meg a támadó kiberképességek fejlesztésének igénye.[24]

Hazánk jelenleg hatályban lévő kiberbiztonsági stratégiájában, bár nem mondható a legfrissebbnek, már deklarálták a kiberbiztonsággal kapcsolatos alapvető értékeket és szemléletmódot. A kiberbiztonsági stratégia, akárcsak a nemzeti biztonsági stratégia, kimondja, hogy a kibertér védelme nemzeti érdek, az ország szuverenitásának része, annak szavatolása állami érdek és feladat. A kiberstratégia egyszer sem hivatkozik sem magánszektorra, sem magánbiztonsági vállalatokra, a „gazdasági szféra" kifejezést alkalmazza. Kijelenti, hogy: „Magyarországon a kibertér szabadságának és biztonságának szavatolása a kormányzat, a tudományos, a gazdasági és a civil szféra közös felelősségvállaláson alapuló, szoros együttműködésével, összehangolt tevékenységével valósul meg."[25]

A civil szféra inkább a nem kormányzati szervekre érthető. További pontokban erősíti meg a kiberstratégia a különböző területek közötti együttműködés fontosságát, sőt, a szabályozás esetében is úgy fogalmaz, hogy: „A többlépcsős jogalkotási tevékenység mellett szükséges a civil, a gazdasági és a tudományos terület szereplőivel együttműködési megállapodásokat kötni, amelyek megfelelő alapot és szabályozást biztosítanak a közös felelősségvállaláson alapuló kiberbiztonság hatékony működtetéséhez."[26]

Habár az újonnan elfogadott magyar *Nemzeti Katonai Stratégia* egyáltalán nem említi kifejezetten a magánszektor szerepét a kiberbiztonságban és a kiberműveletekben, azonban úgy fogalmaz a *Megújuló Magyar Honvédség* című fejezetben, hogy a haza védelmének nemzeti elemeit egyéb biztonsági együttműködések is kiegészítik, illetve megállapítja, hogy növekedni fog a civil-katonai együttműködés hatékonysága.[27]

[24] 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról, 159. pont.
[25] 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról, 6. pont.
[26] 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról, 10/d. pont.
[27] 1393/2021. (VI. 24.) Korm. határozat Magyarország Nemzeti Katonai Stratégiájáról, 5. pont.

Koller Marco

A *Tallinni kézikönyv* szerepe a kiberműveletek értelmezésében

A NATO Kibervédelmi Kiválósági Központot (a továbbiakban: CCDCOE) 2008. május 14-én létesítették Tallinnban, célja a védelmi képességek erősítése volt a kiberbiztonság területén. A Cambridge University Press 2013-ban adta ki a *Tallinn Manual on the International Law Applicable to Cyber Warfare* címet viselő kézikönyvét (a továbbiakban: Kézikönyv). A CCDCOE hívta meg a Kézikönyv szerzőit és közreműködőit, a felsőoktatási intézmények képviselőit, nemzetközi jogászszakértőket, technikai szakértőket. A munka célja, amelynek elérése három évet vett igénybe, az volt, hogy az új típusú hadviselés, a kiberhadviselés terén vizsgálja az alkalmazható jogi és katonai lépéseket. A fő hangsúly a békeidőben végzett ellenséges kibertevékenységekkel szemben alkalmazható jogi lehetőségek vizsgálatán volt. Megállapították, hogy egy kiberművelet csak akkor minősül (katonai) erő alkalmazásának, amennyiben a kiberművelet okozta hatás összemérhető egy hagyományos fegyveres támadással. Ilyen esetben adott államnak joga van az önvédelemhez, azonban jelen esetben is szem előtt kell tartani a szükségesség és az arányosság elvét. Megfogalmazták azt is, hogy az állam jogosult a kibertámadás ellen fellépni, nem csupán akkor, amikor bekövetkezett, hanem akkor is, ha már fenyegető közelségben van az esemény bekövetkezése. Egy művelet akkor minősül a kibertérben elkövetett támadásnak, ha hatására személyek sérülnek vagy halnak meg, illetve vagyontárgyak rongálódnak vagy semmisülnek meg. A támadások célszemélyei lehetnek a fegyveres testületek és szervezetek tagjai.

Jelen fejezet szempontjából kiemelendő, hogy a kiberműveletekben részt vevő zsoldosok nem tekinthetők harcoló félnek, ami megalapozhatja azt, hogy egyes államok kiberműveletek végrehajtására zsoldosokat bérelnek fel, hogy az általuk végrehajtani akart művelet ne számítson állam által végbevitt fegyveres agressziónak. A nemzetközi jog a kibertérben is tiltja a terrorizmust és annak eszközeit. A kiberműveletekben a szemben álló feleknek figyelembe kell venni a polgári személyek védelmét, valamint ügyelni kell a támadási módszerek megválasztására, a célok kiválasztására, a támadás előtti figyelmeztetésre, illetve a megtámadott fél védelmi kötelezettségére.[28] A Kézikönyv folytatása 2017 februárjában jelent meg, kiegészítve az előző kézikönyv alkalmazási területét. A folytatás jogi keretet ad minden rosszindulatú kiberművelet kezeléséhez. Deklarálták a NATO

[28] Gyebrovszki Tamás: Stuxnet – mint az első alkalmazott kiberfegyver – a Tallini Kézikönyv szabályrendszere szempontjából. *Hadmérnök,* 11. (2014), 1. 164–174.

együttműködésének növelését az iparral. A Kézikönyv folytatásában áttörést jelentett a 2016. júliusi varsói csúcstalálkozó, amikor a Szövetség a műveletek negyedik színterévé minősítette a kiberteret.[29] 2021-ben a CCDCOE elindította a Tallinn Manual 3.0 projektet, egy ötéves vállalkozást: felülvizsgálják a meglévő fejezeteket, és további fontos új témákat tárnak fel. Figyelembe veszik a nemzetközi és regionális szintű tevékenységeket és nyilatkozatokat.[30]

Magánbiztonsági vállalatok alkalmazása

Az alábbi alfejezetben a magánbiztonsági vállalatok alkalmazásának kérdéskörét két részre osztva mutatjuk be: egyrészt a témakörben megkerülhetetlen országban, az Amerikai Egyesült Államokban alkalmazott jelenlegi trendeket és területeket, hogy tágabb perspektívát kapjon az olvasó. Másrészt a magánbiztonsági vállalatok kiberműveletekben történő alkalmazását.

A magánbiztonság szerepe az Egyesült Államokban

Az Egyesült Államokat tartjuk a magánbiztonsági iparág bölcsőjének, itt alakult ki a szektor a 19. század második felétől. Az USA-ban a 2001. szeptember 11-i terrortámadások idézték elő a magánszektor alkalmazásának előretörését. Egyre szélesebb körű együttműködés vette kezdetét, azóta az államokban olyan új területeken is bevonják a magánbiztonsági szektort, mint többek között a nemzetbiztonsági tevékenység háttértámogatása vagy a katonai műveletek.

Már a statisztikai adatok is jól mutatják, milyen nagy volumenű ez az iparág. 2012 év végén a magánbiztonság 350 milliárd dolláros piac volt az USA-ban. Ebből 282 milliárd dollár – mintegy 80% – a magánszektor részesedése, 69 milliárd dollár – hozzávetőleg 20% – állami megrendelés, amely mutatja, hogy a biztonsági megrendelések nagy része így a piacról érkezett, és nem az állami beruházások uralták a megrendeléseket. Mindenesetre a 69 milliárd dolláros állami beruházást sem lehet félvállról venni.[31] Az IT-biztonsági szolgáltatá-

[29] Fekete-Karydis–Lázár (2020): i. m. 47.

[30] NATO CCDCOE: *The Tallinn Manual.* 2021.

[31] Christián László: A magánbiztonság aktuális nemzetközi trendjei, rövid hazai helyzetértékeléssel. In *Modernkori veszélyek rendészeti aspektusai.* Pécs, Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoport – Magyar Rendészettudományi Társaság, 2015. 57–63.

sok 80 milliárd dollárt tettek ki a 350 milliárdból, és ez érzékelhetően elég nagy szelet. Az igény a magánbiztonság iránt folyamatosan növekszik, az IT-biztonsági üzletág esetén az előre jelzett növekedési ütem 9%[32] volt. A magánbiztonsági szervezetek egyre fontosabb szerepet játszanak az országban, ami mögött a folyamatos biztonsági kiszervezések állnak az USA-ban, például meg lehet említeni a büntetés-végrehajtás privatizációját, illetve a különböző infrastruktúrák védelmét is. Habár az állami szereplők és a magánbiztonsági vállalatok között javult az együttműködés, ennek ellenére a rendvédelem terén a privát szolgáltatókkal kapcsolatban folyamatos a kritika (figyelemmel arra, hogy egyre nagyobb piacot nyernek). A leggyakrabban felhozott, hogy habár hatékonyabban láthatják el az egyes feladatokat, mint az állami szereplők, a kereskedelmi alapon nyugvó vállalkozás mindig profitorientált, így egyes esetekben az ezen vállalatok által alkalmazott metódusoknál megkérdőjeleződhet a humán biztonság, az emberi jogok témaköre is. Ez hatványozottan igaz a büntetés-végrehajtásra.[33]

További kérdéseket vet fel a katonai magánvállalatok témaköre, amely az elmúlt évtizedben rendkívül felkapott lett mind a külföldi, mind a magyar médiában, főként a PMC alkalmazása miatt Irak és Afganisztán kapcsán.[34] A téma rendkívül kényes, ugyanis a katonai magánvállalatok megítélése a közvéleményt, a szakértőket és a témával foglalkozó tudósokat is egyaránt megosztja, hiszen akármennyire is hatékony egy ilyen jellegű cég alkalmazása a hadműveletek során (még ha csak az objektumok őrzése-védése területén is), egy sor emberi jogi és nemzetközi jogi kérdést vet fel, ha egy állam nem a lobogója alá tartozó erőt alkalmaz, hanem egy kvázi független, kívülálló személyi kört, hiszen a PMC-k által esetlegesen elkövetett etikai vagy szakmai hibák esetén az adott alkalmazó állam saját felelőssége megkérdőjeleződhet, a kormányzat viszont megpróbálhatja elbagatellizálni azt.

[32] Christián László – Rottler Violetta: A magánbiztonság és az önkormányzati rendészet fogalomrendszere. In Christián László – Major László – Szabó Csaba (szerk.): *Biztonsági vezető kézikönyv*. Budapest, Dialóg Campus, 2019. 13–36.

[33] Pap András László: *A megfigyelés társadalmának proliferációjától az etnikai profilalkotáson át az állami felelősség kiszervezéséig.* Budapest, L'Harmattan, 2012.

[34] Varga Krisztián: Katonai biztonsági magánvállalatok amerikai alkalmazása Irakban. *Nemzet és Biztonság,* 2. (2009), 3. 57–69.

A magánszektor állami alkalmazása a kiberbiztonság területén

A különböző magánbiztonsági vállalatok részvétele már-már elkerülhetetlen a kibertérben végrehajtott műveletek esetén, már ha csak a kibertér fogalmának jellemzőire gondolunk is. A kiberműveletek során alkalmazott eszközök és módszerek esetén nincs teljesen éles határ a katonai és a polgári célú alkalmazás között. A kiberbiztonság mindennapjaink szerves részévé válásával, illetve növekedése miatt egy adott államnak nincsenek meg azok a képességei, hogy teljes mértékben meg tudja védeni saját állampolgárait, ezért a magánvállalatok bevonása elengedhetetlen; ugyanakkor, ahogy a PMC-k esetén is felmerülnek a nemzetközi jogi kérdéskörök és felelősségek, úgy ez szintén elmondható a kiberműveletekben alkalmazott magáncégek esetén. Továbbá a „zsoldos" vállalatok esetén felmerülhet annak lehetősége, hogy mint technikai szolgáltató esetleg ellenséges ország is alkalmazhatta őket.

A támadó jellegű kiberműveletekben a magánszektor alapvetően két funkciót tölthet be. Az egyik a hírszerzési műveletek, a másik pedig a tervező-támogató műveletek terepe. A Stanford Egyetem által készített tanulmány is kimondja,[35] hogy a magánvállalatok ezirányú alkalmazása kockázatokkal és előnyökkel egyaránt jár. Az előnyök főként a gyorsan fejlődő technológia és a hatékony képesség alkalmazásának kategóriájába tartoznak. A hátrányok közé a belső szabályozások és a nemzetközi kapcsolatok esetleges megsértése. Az előnyök közé sorolja a tanulmány a képességek növelésének lehetőségét, hiszen az ilyen cégek munkatársait nem kell kiképezni, alkalmazásuk rugalmas, olykor olcsóbb, mint a hivatásosoké, főként rövid távon.[36]

A kiberműveletek esetében rendre felmerül a kérdés, hogy egy állam vagy állami szervezet milyen mértékben támaszkodhat, illetve mennyire indokolt egyáltalán támaszkodnia magánbiztonsági cégekre. Figyelembe kell azonban venni a technológia rohamos fejlődését és azt a tendenciát, hogy konfliktushelyzetben a nem katonai eszközök (diplomáciai, gazdasági vagy jogi intézkedések) sikertelensége esetén egy támadó kiberművelet lehet az első katonai csapásmérés eszköze. A rendelkezésre álló jogi dokumentumok, hazai és nemzetközi szakirodalom alapján arra a következtetésre jutottam, hogy a támadó jellegű kiberműveletek esetén a magánbiztonsági vállalatok közvetlen alkalmazása

[35] Irving Lachow: The Private Sector Role in Offensive Cyber Operations: Benefits, Issues and Challenges. *SSRN Electronic Journal,* (2016).

[36] EGov: *A támadó kiberműveletek stratégiája* (2019. március 31.).

aggályos lehet, azonban az állam saját szakértőinek képzéséhez, illetve a megfelelő technikai háttér megszerzéséhez és fejlesztéséhez elengedhetetlen az ezen a területen dolgozó magánbiztonsági vállalatok alkalmazása.

Esettanulmány a magánbiztonsággal kapcsolatos vállalatok szerepéről – Stuxnet

Az egyik legkülönösebb kibertámadás, a Stuxnet a kiberháborúk új dimenzióját nyitotta meg. A 2009–2010. évben egy ismeretlen *malware* (Stuxnet) megbénította az iráni natanzi atomerőmű dúsítóját, amit Irán 2010. szeptember 25-én ismert el, azaz, hogy az atomerőmű nukleáris centrifugáiban mechanikai hibák vannak, amelyeket egy kártékony szoftver és annak mutálódott verziói okoztak. Feltételezések szerint Barack Obamához és elődjéhez, George W. Bush elnökhöz köthető a Stuxnet, megbízásukra amerikai és izraeli titkosszolgálati szakemberek hozták létre, és célja az iráni atomprogram akadályozása, illetve megbénítása volt.[37]

A támadó kiberművelet végrehajtása előtt a szakembereknek mérlegelniük kellett az atomprogram akadályozásának mikéntjét, és mivel azt fegyveresek őrizték, egy hagyományos katonai akció nagyobb kihívást jelentett volna. Az izraeli hadvezetésnek kockázatok sorával kellett számolnia az iráni atomerőművek megtámadásának tervezése során, például az 1800 km-es távolság áthidalásával, katonai veszteségekkel, a nemzetközi közvélemény negatív viszonyulásával. Gondoljunk arra, hogy az Európai Unió is óvatos az iráni atomkísérletek megítélésében! Előfordulhatott volna továbbá azonnali, nyílt bosszú Iránról vagy iránbarát terroristacsoportoktól a világ bármely pontján, bármikor izraeli, egyesült államokbeli polgárok (turisták, sportolók) ellen. A Stuxnet csak az adott környezetben, azt felismerve funkcionált, más környezetben passzív maradt. A Stuxnetet úgy kellett megírni, hogy más rendszerekben, funkciókban ne tehessen kárt, hiszen ha felfedezik, akkor az a fő célt veszélyeztette volna. Célzottan a centrifugák működésének megzavarására alkották meg. A vírus hatása (feladata) a centrifugarotorok forgási sebességének lelassítása, majd felgyorsítása volt.[38]

[37] Nagy (2018): i. m. 186.
[38] Gyebrovszki (2014): i. m. 169–170.

A kártékony szoftvert 2010 júniusában a Fehéroroszországban alapított VirusBlokAda cég fedezte fel. A cég tevékenységi köre a víruskereső szoftverek gyártása, illetve az ehhez kapcsolódó szoftverelemző és értékelő munka. Így jól látható, hogy a védelmi tevékenység területén sem elhanyagolható az egyes magánbiztonsági vállalatok szerepe. Amennyiben nem alkalmazták volna a céget, nem tudható, hogy a kártékony szoftver milyen jellegű károkat okozott volna, a fentiekben leírtak szerint akár súlyosabb következményei is lehettek volna.[39] A vírus elemzésében, illetve korábbi verziójának megállapításában hathatós szerepe volt a szintén a magánszektorhoz tartozó Symantec nevű cégnek.

Összegzés

Összefoglalásul elmondható, hogy a technológiai fejlődés következményeként a kiberbiztonság és a kibertér kiemelt prioritássá vált. Már-már közhely, hogy a nemzetközi összefogás elengedhetetlen a kiberbűnözés és a terrorizmus visszaszorítása érdekében, azonban érdekes perspektívákat tár fel a magánszektor, azon belül is a magánbiztonsági vállalatok bevonása a különböző kiberműveletek végrehajtásába, illetve az állami szervezetek alkalmazottainak szakirányú képzésébe.

Az elkövetkezendő években egyre nagyobb szerepet fognak játszani a kibertérben végbemenő műveletek, amelyeknek nem csupán katonai[40] célpontjai lehetnek, hanem polgári, kiemeltképpen kritikus infrastruktúrabeliek. A Stuxnet esetében is láttuk, hogy a kártékony szoftver felismerésében, illetve elemzésében egyértelmű szerepe volt a különböző cégeknek. Azok az országok, amelyek nem fejlesztik kiberképességeiket, rendkívüli hátrányba kerülhetnek, így az állam feladata, hogy a lehető legszélesebb körű együttműködés keretei között védje a kiberbiztonságot, amelybe beletartozik a kutatások szorgalmazása, egyetemi képzések indítása, illetve a megfelelő *know-how*-val rendelkező szakemberek alkalmazása. Mindezek megteremtéséhez elengedhetetlen a magánszektor közreműködése, illetve bevonása az állam kibertérben végzett tevékenységébe. A kiberhadviselés területén is előszeretettel alkalmaznak nem állami, hanem kvázi magánszektorbeli hackereket, hiszen a *Tallinni kézikönyv* kimondta: a zsol-

[39] Kovács László – Sipos Marianna: A Stuxnet és ami mögötte van: tények és a cyberháború hajnala. *Hadmérnök,* 5. (2010), 4. 163–172.

[40] Berki (2016): i. m.

dosok más megítélés alá esnek, mint egy állam hivatásos katonái, így a jövőben várható tendencia, hogy az egyes állami szereplők saját identitásuk leplezése érdekében zsoldosokat alkalmaznak a kibertérben, akik végrehajtják a támadó műveleteket az ellenséges ország valamilyen infrastruktúrája ellen, így próbálva csökkenteni az esetleges nemzetközi botrányt vagy a jogszerű lehetséges katonai retorzió esélyét. A fentiek nyomán jó eséllyel kijelenthető, hogy az egyes PMC-k működési területe a jövőben lehetséges irányváltás elé néz, és a hagyományos őrzési-védési, logisztikai feladatok mellett sokkalta hangsúlyosabb szerepet kap az egyes kiberműveletekben történő részvétel. Figyelemmel arra, hogy egy adott állam saját infrastruktúrájának (főként, ha kritikus infrastruktúra) kibertéri védelmét a megfelelő ellenőrzés alatt akarja tudni, valószínűbb, hogy a magáncégeket nem védelmi, hanem támadó jellegű műveletek során fogják inkább alkalmazni, esetleg az állam saját alkalmazottainak kiképzése során kaphatnak nagyobb szerepet a kiberbiztonság területén jártas magánszektorbeli szakértők.

Irodalomjegyzék

Berki Gábor: Kiberháború, kiberkonfliktusok. In Pintér István (szerk.): *A virtuális tér geopolitikája. Tanulmánykötet.* Budapest, Geopolitikai Tanács Közhasznú Alapítvány, 2016. 247–284.

Christián László: A magánbiztonság aktuális nemzetközi trendjei, rövid hazai helyzetértékeléssel. In *Modernkori veszélyek rendészeti aspektusai.* Pécs, Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoport – Magyar Rendészettudományi Társaság, 2015. 57–63. Online: https://core.ac.uk/download/pdf/356664168.pdf

Christián László: Magánbiztonsági számvetés. In Dobák Imre – Hautzinger Zoltán (szerk.): *Szakmaiság, szerénység, szorgalom. Ünnepi kötet Boda József 65. születésnapja alkalmából.* Budapest, Dialóg Campus, 2018.

Christián László – Rottler Violetta: A magánbiztonság és az önkormányzati rendészet fogalomrendszere. In Christián László – Major László – Szabó Csaba (szerk.): *Biztonsági vezető kézikönyv.* Dialóg Campus, 2019. 13–36.

Dévai Dóra: A kiberfegyver koncepció evolúciója., *Hadmérnök,* 14. (2019), 2. 272–280. Online: https://doi.org/10.32567/hm.2019.2.22

EGov: *A támadó kiberműveletek stratégiája* (2019. március 31.). Online: https://hirlevel.egov.hu/2019/03/31/a-tamado-kibermuveletek-strategiaja/

Fekete-Karydis Klára – Lázár Bence: A kibervédelem katonai dimenziói. *Honvédségi Szemle,* 148. (2020), 3. 44–54. Online: https: //doi.org/10.35926/HSZ.2020.3.4

Gyebrovszki Tamás: Stuxnet – mint az első alkalmazott kiberfegyver – a Tallini Kézikönyv szabályrendszere szempontjából. *Hadmérnök,* 11. (2014), 1. 164–174. Online: http://hadmernok.hu/141_16_gyebrovszkyt.pdf

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

Haig Zsolt: *Információ, társadalom, biztonság.* Budapest, Nemzeti Közszolgálati Egyetem, 2015.

Irving Lachow: The Private Sector Role in Offensive Cyber Operations: Benefits, Issues and Challenges. *SSRN Electronic Journal,* (2016). Online: https://dx.doi.org/10.2139/ssrn.2836201

Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms (2010. november 8.). Online: https://irp.fas.org/doddir/dod/jp1_02.pdf

Kovács László: *A kibertér védelme*. Budapest, Dialóg Campus, 2018.

Kovács László: A kiberbiztonság és a kiberműveletek megjelenése Magyarország új Nemzeti Biztonsági Stratégiájában. *Honvédségi Szemle,* 148. (2020), 5. 3–18. Online: http://dx.doi.org/10.35926/HSZ.2020.5.1

Kovács László – Sipos Marianna: A Stuxnet és ami mögötte van: Tények és a cyberháború hajnala. *Hadmérnök,* 5. (2010), 4. 163–172. Online: http://hadmernok.hu/2010_4_kovacs_sipos.pdf

Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiájáról szóló 1838/2018. (XII. 28.) Korm. határozat alapján a hálózati és információs rendszerek biztonságára vonatkozó Stratégia. Online: https://bit.ly/3u0ohee

Muha Lajos – Krasznay Csaba: *Az elektronikus információs rendszerek biztonságának menedzselése.* Budapest, Nemzeti Közszolgálati Egyetem, 2014.

Nagy Zoltán András: Kiberháborúk kora. In *Magyar Tudomány Napja a Délvidéken – 2018. Tanulmánykötet.* Vajdasági Magyar Tudományos Társaság, 2018. 174–193.

Nagyné Bereczki Szilvia – Nagy József: *Magánbiztonság és kritikus infrastruktúra védelem*. Budapest, 2014. Online: https://securimaster.com/maganbiztonsag-es-kritikus-infrastruktura-vedelem/

NATO CCDCOE: *The Tallinn Manual.* 2021. Online: https://ccdcoe.org/tallinn-manual.html

Pap András László: *A megfigyelés társadalmának proliferációjától az etnikai profilalkotáson át az állami felelősség kiszervezéséig.* Budapest, L'Harmattan, 2012.

Rottler Violetta: Gondolatok a magánbiztonság köréből. *Magyar Rendészet,* 19. (2019), 4. 81–95. Online: http://doi.org/10.32577/mr.2019.4.6

Varga Krisztián: Katonai biztonsági magánvállalatok amerikai alkalmazása Irakban. *Nemzet és Biztonság,* 2. (2009), 3. 57–69. Online: www.nemzetesbiztonsag.hu/cikkek/varga_krisztian-katonai_biztonsagi_maganvallalatok_amerikai_alkalmazasa_irakban.pdf

Jogi szabályozók

JP 1-02 Department of Defense Dictionary of Military and Associated Terms
1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról
1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról
1393/2021. (VI. 24.) Korm. határozat Magyarország Nemzeti Katonai Stratégiájáról