NEMZETI KÖZSZOLGÁLATI EGYETEM

Hadtudományi Doktori Iskola

Berzsenyi Dániel

Különleges kiberműveletek

A kiber különleges műveleti képesség és kialakításának vizsgálata

Doktori (PhD) értekezés

Témavezetők:

Szenes Zoltán, CSc

……..

Kovács László, DSc

……..

Budapest, 2022

Tartalomjegyzék

Bevezetés 6
I. A kutatási probléma és a kutatási célok megfogalmazása 8
I.1 A kutatási probléma 8
I.2 A kutatás aktualitása 10
I.3 A kutatási célok 11
I.4 Hipotézisek 12
I.5 Kutatási módszerek 14
I.6 Szakirodalmi áttekintés 16
II. Elméleti keretek 22
II.1 Globális közös terek 22
II.2 Vizsgált időszak 27
II.3 A tudatos felhasználótól az APT-kig: 21. századi kiberbiztonsági kihívások 31
II.4 Védelmi szervezetek kihívásai és a kibertér szerepe a 21. században 38
II.5 A kortárs fegyveres konfliktusok és a kiberhadviselés kapcsolata 44
II.6 A vizsgálat szintje: nemzeti képességfejlesztés 49
II.7 Nemzeti érdek, nemzeti-érdekérvényesítés és a kiberműveleti képességek 53
III. A kiberműveleti képességek 58
Bevezetés 58
III.1 Stratégiai kitekintés 60
III.1.1 Környező országok kiberképességei 61
III.1.2 Kiber képességek a kisállamok stratégiáiban 68
III.1.3 Nagyhatalmi kiberműveleti képességek és ambíciók 73
III.2 A defenzívtől az offenzív kiberműveletekig – a teljes spektrum 77
III.2.1 Passzív kibervédelem 78
III.2.2 Aktív kibervédelem 80
III.2.3 Offenzív kiberképességek 84
III.3 A kiberműveleti képességek fejlődése 88
III.3.1 Az orosz állami szereplők és megbízottjaik kiberképességei 89
III.3.2 Kína kibertéri aktivitásának főszereplői 92
III.3.3 Az Amerikai Egyesült Államok kibertevékenységének végrehajtói 96

Összegzés, következtetések 99
IV. Kiberképességek és Fejlett Perzisztens Fenyegetések (APT) 102
Bevezetés 102
IV.1 APT alapok és értelmezés 103
IV.1.1 Az APT-k paraméterei és sajátosságai 104
IV.1.2 Az első APT-k és kategorizálásuk 107
IV.1.3 Az APT csoportok állami támogatása 111
IV.1.4 Az APT csoportok hatékony működésének körülményei és feltételei 113
IV.1.5 Az APT-k és tagjaik azonosítási nehézségei 114
IV.2 Az APT-k által generált kihívás és fenyegetés jelentősége 116
IV.2.1 Fejlettség 116
IV.2.2 Perzisztencia 120
IV.2.3 Fenyegetés 121
Összegzés, következtetések 126
V. Védelmi szervezetek különleges műveleti képességei 129
Bevezetés 129
V.1 Katonai különleges műveleti erők 129
V.1.1 A különleges erők feladatrendszere 130
V.1.2 A különleges erők jellemzői, a működés körülményei és feltételei 132
V.1.3 Képzés, kiképzés és követelmények a különleges műveleti erőknél 134
V.2 Rendvédelmi speciális egységek 136
V.2.1 A rendvédelmi speciális egységek feladatrendszere 136
V.2.2 A speciális rendvédelmi tevékenységek jellemzői és feltételei 138
V.2.3 Képzés, kiképzés és követelmények a speciális rendvédelmi egységeknél 139
V.3 Nemzetbiztonsági különleges képességek 141
V.3.1 A nemzetbiztonsági szervezetek (különleges) képességei 141
V.3.2 A speciális nemzetbiztonsági képességek feladatrendszere 142
V.3.3 Képzés, kiképzés és követelmények a nemzetbiztonsági szolgálatoknál 144
Összegzés, következtetések 146
VI. A kiber különleges műveleti erők 149
Bevezetés 149
VI.1 Miért van szükség kiber különleges műveleti erőkre? 150

VI.1.1 Kitekintés a különleges műveletek középtávú kihívásaira 151
VI.1.2 Stratégiai szempontok 153
VI.1.3 Műveleti szempontok 156
VI.2 A kiber különleges műveleti erők létrehozása és működési háttere 158
VI.2.1 A működési keretek kialakításának dilemmái 158
VI.2.2 A polgári demokratikus kontroll szerepe és jelentősége 160
VI.2.3 Az azonnali cselekvés képessége a demokratikus kontroll tükrében 163
VI.3 A kiber különleges műveleti erők szerepe és szervezeti integrációja 165
VI.3.1 Katonai integrációs lehetőségek 169
VI.3.2 Nemzetbiztonsági integráció, vagy önálló szervezet 171
VI.3.3 Félkatonai, paramilitáris koncepció 172
VI.3.4 „Kontraktor" modell – CCaaS (Cyber Capability as a Service) 175
VI.4 A kiber különleges műveletek végrehajtóinak toborzása és kiválasztása 177
VI.4.1 Technikai ismeretek 178
VI.4.2 Mentális, logikai és más készségek, képességek 180
VI.4.3 Fizikai alkalmasság 181
VI.4.4 Az interoperabilitás keretrendszere 183
VI.4.5 Humán kihívások 184
VI.5 A kiber különleges műveleti felkészítésről és kiképzésről 185
VI.5.1 Értékelő központok 186
VI.5.2 Az oktatás és kiképzés infrastrukturális kérdései 187
VI.5.3 Felkészítéssel szembeni elvárások 190
VI.6 A kiberképességek és elrettentés teljes spektruma 194
VI.6.1 A nélkülözhetetlen CTI 195
VI.6.2 Az offenzív műveleti komponens 197
VI.6.3 A támogató és K+F komponens jelentősége 200
VI.7 A képesség kialakításának erőforrásai és kockázatai 202
VI.7.1 Beágyazottság és interoperabilitás 202
VI.7.2 Állandó és rugalmas költségvetés 203
VI.7.3 Kockázatok és kihívások 208
Összegzés, következtetések 210
VII. Összegzett következtetések 213

VIII. Új tudományos eredmények 223
IX. Az értekezés kutatási és tudományos eredményeinek felhasználhatósága 224
X. Ajánlások 225
X.1 Ajánlások a tudományos kutatás terén 226
X.2 Szakpolitikai lépésekre vonatkozó ajánlások 228
Irodalomjegyzék 229
Függelék 259

Bevezetés

A konfliktusok egyidősek az emberiség történelmével. A különböző értékek és érdekek mentén kialakuló nézeteltérések rendezésére az emberi társadalmak az eszközök széles skáláját alakították ki, melyek között a számtalan békés módszer mellett megtalálhatók az erőszak alkalmazásának különböző formái is. A konfliktusok történetét vizsgálva kiderül, hogy az érdekelt felek és vezetőik eltérő módon igyekeztek a rendelkezésükre álló eszközrendszert alkalmazni. A napjaink nemzetközi rendszerében igénybe vett eszközökre hatást gyakorol, hogy a kétpólusú világrend felbomlásával a biztonsági kihívások, kockázatok és fenyegetések egyrészt kibővültek, másrészt olyan szereplők igyekeznek érdekeiket érvényesíteni, akik különböző kultúrkörhöz tartoznak, illetve eltérő fejlettségi szinttel, erőforrásokkal és biztonságpercepcióval rendelkeznek. Ezeknek a hatásoknak a következménye az aszimmetrikus képességek térnyerése, a hagyományos és nem hagyományos hadviselési formák kevert (hibrid) alkalmazásának terjedése, valamint az információs hadviselés, a kiberhadviselés [1] és a kibertérben végzett hírszerző tevékenység szerepének felértékelődése. Utóbbiak az emberiség technikai fejlődésének következtében olyan képességeket és műveleteket is lefednek, amelyekkel szemben kifinomultságuk, komplexitásuk, valamint időbeli és térbeli kiterjedtségük okán egyéni és társadalmi szinten egyaránt védtelenekké válunk.

Napjaink nemzetközi rendszere több pólusú (multipoláris) és meghatározó az összekapcsoltság, valamint a kölcsönös függőség (interdependencia) jelensége. Emiatt az érdekek érvényesítése és a konfliktusok kezelése kizárólag hagyományos módszerekkel egyre kevésbé hatékony, különösen a háborús küszöb alatti konfliktusokban, illetve a nemzetközi kapcsolatok nyíltan fel nem vállalt tevékenységeit rejtő „szürke zónában”. A nemzeti érdekérvényesítés eszköztárában a nem hagyományos módszernek tekintett kiberműveleti képességek megítélése és stratégiai beágyazottsága eltérő a nemzetközi rendszer szereplőinek szintjén. A stratégiai és technológiai téren egyaránt érettebb szereplők a kiberműveleti képességek teljes spektrumát igyekeznek lefedni, amihez különleges szemléletmódot alkalmaznak, valamint együttesen alkalmazzák a védekező

[1] A két főnévből álló – jelöletlen birtokos jelzői vagy jelentéssűritő – alárendelő összetételeket a magyar helyesírási szabályok alapján egybeírjuk. Ennek megfelelően a dolgozatban minden főnevet (pl.: hadviselés, művelet, képesség, háború, védelem, fenyegetés stb.) ami elé a kiber főnév kerül egybeírok. Kivételt csak az értekezés második felében vizsgált kiber különleges műveletek képeznek, ahol a minőségjelzős kapcsolatok tagjainak általános különírására vonatkozó helyesírási szabályt alkalmazom.

(defenzív) és támadó (offenzív) komponenseket. A komponensek integrált alkalmazása kimutatható párhuzamot jelez olyan fenyegetések ismert paramétereivel, amikhez a kiberbiztonsági ágazat a legjelentősebb negatív hatásokat köti és amire a tudományos kutató és szakmai elemző közösség nem, vagy csak részleges figyelmet fordított.

A 21. század turbulens világpolitikai körülményei jelentős kihívások elé állítják a nemzetközi kapcsolatok szereplőit, elmossák a hatalmi erőviszonyokat, valamint a határokat a konfliktusok különböző szintjei között és az érdekérvényesítés eszközeinek kreatív alkalmazására ösztönöznek. A kibertér tekintetében a kihívásokra adott válaszok között említhetők például a NATO 2014-es és 2016-os döntései. A szövetségesek előbb a walesi csúcstalálkozó zárónyilatkozatában (NATO, 2014) deklarálták, hogy a kibertérből érkező fenyegetések indokolttá tehetik a Washingtoni Szerződés 5., kollektív védelemről szóló cikkelyének életbe léptetését. Két évvel később a varsói csúcstalálkozó kommünikéje (NATO, 2016) a hadviselés 5. dimenziójaként ismerte el a kiberteret. A kiberműveleti képességek jelentőségének vizsgálatakor tekintettel kell lenni az egyik alapvető sajátosságra, a többszöröző (multiplikáló) hatásra. Ez egyfelől tetten érhető a fizikai világban a különleges műveleti tevékenységek során is, másfelől különösen fontos a kevésbé érett, illetve korlátozott erőforrásokkal rendelkező szereplők számára. Ebből kiindulva egy sajátos modell kialakításával, specifikus kiberbiztonsági kihívások paramétereivel ötvözve vizsgálom a kiberműveleti képességekben rejlő lehetőségeket kisállami szemszögből. Hazánkat gazdasági mutatói, földrajzi adottságai, érdekérvényesítő képessége és védelmi potenciálja alapján a korlátozott erőforrásokkal rendelkező, kisállami kategóriába sorolom. A kiberműveleti képességek széles skáláján belül a kutatás fókuszában azok a speciális motívumok állnak, amelyek túlmutatnak a reguláris tevékenységeken, akár csak a fizikai hadszíntereken a különleges műveleti erők alkalmazása. Módszertani szempontból a kiber különleges műveleti képességek kialakításának vizsgálatát alaposabbá és informatívabbá teszi, három aspektus elemzése és összehasonlítása: a stratégiai dokumentumok és beágyazottság, a különleges műveleti tevékenységek sajátosságai, valamint a legjelentősebb negatív hatásokat kiváltó kiberfenyegetések paraméterei. Az ezek alapján folytatott kutatással új tudományos eredményekre, valamint a nemzetközi jógyakorlatokat tartalmazó értékes háttérismeretekre tehetünk szert. Kutatásom éppen ezért kitér a kiber különleges műveleti képességek kialakításával összefüggő követelmények és mintázatok azonosítására. Értekezésem ezzel a fókusszal, a továbbiakban ismertetett kutatási célkitűzésekkel, hipotézissel és

módszertannal, valamint a következő fejezetben (II. fejezet) bemutatott elméleti keretrendszerrel készült.

I. A kutatási probléma és a kutatási célok megfogalmazása

Értekezésemben védelmi szervezeti [2] és stratégiai nézőpontból, a nemzeti érdekérvényesítés elemeként, a nemzeti képességfejlesztés szintjén vizsgálom a kiber különleges műveleti képességek kialakítását, mint a kibertérből érkező kihívásokra adandó válaszok egyik lehetséges formáját az ezredfordulót követő időszakban.

I.1 A kutatási probléma

A Maryland Egyetem tanulmánya szerint 39 másodpercenként történik egy számítógépes támadás (Cukier, 2007, 39). Miközben a kiberbiztonsági incidensekhez kapcsolódó valamennyi mérőszám drasztikus növekedést mutat, a társadalom egyre szélesebb rétegei számára válnak valóban kézzelfoghatóvá a kibertérben zajló folyamatok negatív hatásai. Az akadozó szolgáltatások, a kifosztott bankszámlák, a személyazonossággal történő visszaélések, a személyes adatok titkosításán alapuló zsarolások és számos további negatív hatás már az egyén szintjén is súlyos problémákat okozhat, míg társadalmi szinten válsággá vagy nemzetbiztonsági kérdéssé fajulhat. A kiberbiztonság és -védelem területén jártas szakemberek az elmúlt időszakban növekvő számban találkoztak olyan eseményekkel, amelyek szándékos tevékenység eredményeként következtek be és társadalmi szinten is súlyos következményeket generáltak. Az ilyen események hátterében gyakran geopolitikai feszültségekkel és törekvésekkel összefüggő érdekérvényesítési motiváció húzódik meg, ami az érintetteken túl kihívás elé állítja a 21. századi nemzetközi közösséget is.

Növekszik azoknak a nemzetközi szereplőknek a száma, amelyek felismerték a kibertérben vagy azon keresztül folytatott tevékenységek jelentőségét és időszerűségét. A kibertérben vagy azon keresztül kiváltott hatások rendkívül szerteágazók lehetnek, miközben a kibertér sajátosságai miatt

[2] Az értekezésben védelmi szervezetek, illetve a védelmi szektor szervezetei alatt Magyarország Alaptörvénye 45. cikk és 46. cikk szerint, továbbá az 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról 151. és 178. pontja alapján a fegyveres erőket, illetve a rendőrséget és a namzetbiztonsági szolgálatokat is magába foglaló rendvédelmi szerveket értem. Ezt a hármas felosztást és értelmezést alkalmazom a nemzetközi kitekintések és összevetések során is.

korlátokba ütközik a megelőzés, a védekezés és a számonkérés is. A hadtudományi terminológiából kölcsönzött műveleti képességek kibertérre specializált szegmensének dinamikus bővülése a technológia fejlődésének és térnyerésének üteme miatt egyetlen hagyományos műveleti képességgel sem vethető össze. Mindez speciális megközelítést igényel, amely a kiber műveleti képességeket el tudja helyezni a teljes műveleti spektrumban és hatékonyan tudja alkalmazni azokat.

Nemzeti szinten az érdekek érvényesítésében és értékek védelmében közreműködő kiberműveleti képességek jellemzően a fegyveres testületeken belül kerülnek kialakításra. A hivatalos kapcsolat ugyanakkor ritkán egyértelmű, jellemzően nehezen kimutatható és szinte sosem bizonyítható, ezért elterjedt az államilag támogatott terminológia alkalmazása. A kibertér hibrid jellege és aszimmetrikus természete lehetővé teszi az alkalmazott erők és képességek multiplikálását, miközben az anonimitás fenntartása magas szinten biztosított. A kibertérben történő incidensek és az ott zajló konfliktusok, az ezek során alkalmazott módszerek és eljárások különböző aspektusokból épp úgy vizsgálhatók, mint a kinetikus hatásokkal járó fizikai térben megvalósuló incidensek és konfliktusok.

A kiberműveleti képességek proliferációja a védelmi és támadói oldalon egyaránt jelentkezik. A jelenség negatív hatásaival naponta találkozhatunk, miközben nincsenek gyors, hatékony és egységes válaszok a kibertérből érkező kihívásokra és fenyegetésekre. Néhány állam tekintélyes előnyre tett szert ezen a téren az elmúlt évek során és mára olyan kiberműveleti képességeket birtokol, ami a saját és szövetséges rendszerek védelmén jelentős mértékben túlmutat. A speciális kiberműveleti képességekkel sebészi pontosságú kibertámadásokat tudnak végrehajtani tetszőleges célpontok ellen, amivel társadalmi, gazdasági, politikai, katonai és nemzetbiztonsági hatások érhetők el.

Ilyen hatások kiváltása a fizikai térben jellemzően a katonai különleges erők, a rendvédelmi speciális egységek, illetve nemzetbiztonsági szolgálatok erre kiképzett állományával végrehajtott műveletekkel érhető el. A fizikai térhez hasonlóan a kibertérben is azonosíthatók olyan akciók és képességek, amelyek bizonyos szempontból megfeleltethetők a különleges műveleti képességeknek. A kibertér különleges műveleti erői hasonló tevékenységet folytatnak, mint a kinetikus térben tevékenykedő társaik, csak eltérő dimenzióban. Ugyan korlátozottan érhető el információ azzal kapcsolatban, hogy a nemzetközi rendszer egyes szereplői milyen szintű

kiberműveleti képességekkel rendelkeznek, a társadalmi berendezkedésre és stabilitásra [3], a gazdasági biztonságra [4] vagy épp az energiabiztonságra [5] leselkedő legjelentősebb kiberfenyegetések között több olyan is található, amelyik államilag támogatott tevékenységre utal.

Mivel az egyik oldalon kiberműveleti képességként jelennek meg azok a tevékenységek, amik a másik oldal számára kiberfenyegetést jelentenek, időszerű a kérdés hadtudományi feldolgozása és a kiberműveletek szerepének vizsgálata a nemzetközi kapcsolatokban, a konfliktusokban, illetve a politikai és nemzeti érdekérvényesítés során. További analízis szükséges a kiberműveleti képességek speciális típusainak azonosításához, valamint az ilyen műveleteket megtervezni és végrehajtani képes egységek kialakításához.

I.2 A kutatás aktualitása

Az elmúlt időszak eseményei – köztük a fent említettek – ráirányították a figyelmet a kibertérben zajló folyamatok negatív hatásaira, valamint az incidensek és konfliktusok kiber dimenziójának jelentőségére. A kibertérből érkező kihívások és fenyegetések bővülése jelentős mértékben összefügg a technológia és a digitalizáció térnyerésével, aminek következtében a fiziológiai szintű egyéni szükségletektől kezdve, magas szintű társadalmi folyamatokig bezárólag minden területtel összekapcsolódik a kibertér. A kiber dimenzió térnyerésére és a digitális eszközök proliferációjára világ szinten is jelentős hatást gyakorolt a 2020-ban kitört SARS-CoV-2 (koronavírus) járvány, amelynek következtében komplett országok és emberek milliói kényszerültek rá arra, hogy alternatív, digitális megoldásokat találjanak az oktatásban, a munkavégzésben vagy épp a szociális élet és a kikapcsolódás terén.

Az urbanizáció, a kistelepülések fejlesztése vagy a kommunikációs rendszerek korszerűsítése olyan társadalmi folyamatok, amelyek régóta jelen vannak, azonban mára már olyan jelenségekkel egészülnek ki, mint például az okos város koncepciója, az ötödik és hatodik generációs távközlési rendszerek, a mesterséges intelligencia terjedése vagy az ipar 4.0 megjelenése. Ezek nyomán a

[3] A társadalmi berendezkedésre és stabilitásra veszélyt jelentő kiberműveletnek tekinthető az amerikai elnökválasztásba történt 2016-os beavatkozás. Bővebben: https://www.cfr.org/cyber-operations/
[4] A gazdasági biztonságra veszélyt jelentő kiberműveletnek tekinthető a Bangladesh Bankon keresztül a nemzetközi bankközi elszámolási rendszert (SWIFT) ért 2016-os támadás. Bővebben: https://www.cfr.org/cyber-operations/
[5] Az energiabiztonságra veszélyt jelentő kiberműveletnek tekinthető az ukrán energiaszolgáltatást ért 2016-os támadás. Bővebben: https://www.cfr.org/cyber-operations/compromise-power-grid-eastern-ukraine

mindennapi élet egyre több szegmensébe férkőznek be különböző, egymással kommunikálni képes szenzorok és érzékelők, illetve irányító és vezérlő megoldások, amelyek működéséhez egyre kevésbé szükséges az emberi jelenlét és felügyelet. Ezek a kibertérben, illetve azon keresztül zajló folyamatok egyéni és társadalmi szinten egyaránt jelentős mértékben növelik a kibertérből érkező kihívásokkal és fenyegetésekkel szembeni kitettséget.

Mivel a kitettség növekszik és a fenyegetések bővülnek felmerül a válaszadási képesség kialakítása, a kárelhárítási tervek elkészítése, a rendszerek karbantartása, a kutatás-fejlesztés irányainak átgondolása és a védekezésre való felkészülés koordinációja is, mint aktuális probléma. Ezek kapcsán a nemzetközi rendszer szereplői különböző megközelítést alkalmaznak, ugyanakkor több állam kiterjedt programok segítségével fókuszáltan foglalkozik az olyan kritikus kérdésekkel, mint a kiberfenyegetésekkel kapcsolatos megelőzés, védelem és válaszadás. Napjainkra több tucat ország rendelkezik valamilyen szintű kiberműveleti képességgel és bár készülnek kimutatások a kiberképességek és a kapcsolódó hatalmi potenciál kapcsán (Voo és mtsai., 2020), a rendelkezésre álló szakirodalom hazai és nemzetközi szinten egyaránt korlátozott.

I.3 A kutatási célok

Kutatási céljaim a következők:

1) **Feltárni** az aktuális kiberbiztonsági és kibervédelmi stratégiai dokumentumok alapján **a nyíltan felvállalt kiberműveleti képességeket és ambíció szintet** Magyarország és a nemzetközileg feldolgozható stratégiai dokumentummal rendelkező szomszéd országok, illetve néhány kiválasztott kisállam és nagyhatalmi szereplő esetében. Ezek alapján **következtetéseket megfogalmazni a kiberműveleti képességek megismerésének korlátjaira vonatkozóan**.

2) **Azonosítani** azokat a kibertérből érkező fenyegetéseket, amelyekhez a legsúlyosabb ismert kiberbiztonsági incidensek köthetők és **a legkifinomultabb eszközöket, módszereket és eljárásokat** alkalmazva érik el a céljukat. Ez alapján **meghatározni azokat a paramétereket, amelyek a** védelmi szervezetek által folytatott **különleges műveleti tevékenységek és a fejlett perzisztens fenyegetések kapcsán egyaránt megfigyelhetők**, különös tekintettel a fedett körülmények között, kiemelkedő színvonalon, szervezetten és tervezetten, felsőbb – biztonsági, katonai, nemzetbiztonsági, politikai – érdekek mentén történő végrehajtásra.

3) **Javaslatot tenni** az észleléshez, felszámoláshoz és megelőzéshez szükséges, támadással arányos – megelőző és ellentámadási kapacitást is magába foglaló – **kiber különleges műveleti képességek elhelyezésére** a nemzeti képességfejlesztés szintjén, a nemzeti érdekérvényesítés eszköztárának elemeként, a nemzeti érdekek hatékonyabb érvényesítésének elősegítése céljából.

4) **Kidolgozni** a kiberműveleti és különleges műveleti képességek hasonlóságot mutató mintázatai és szabályszerűségei alapján **a kiber különleges műveleti képességek kialakításának lehetőségeit és feltételrendszerét** a kiberképességek teljes spektrumán, különös tekintettel az erőforrások alkalmazására.

I.4 Hipotézisek

Az értekezésben a kutatási célkitűzésekkel összhangban az alábbi hipotéziseket és azok komponenseit vizsgálom:

a) A jelenlegi stratégiai környezetben az államok nyíltan nem, vagy csak részben vállalják fel azokat a kiberműveleti képességeket, amelyeknek teljes spektrumához hozzá tartozik az arányos válaszadáshoz szükséges megelőző és ellentámadási kapacitás. (H1)
b) Az ismert fejlett perzisztens fenyegetések (Advanced Persistent Threat – APT)[6] több jellemzője is azonosítható, amelyek hasonlóságot, illetve párhuzamot mutatnak a kinetikus tartományban alkalmazott különleges műveleti erőkkel és képességekkel. (H2)
c) A kiberműveletek teljes spektrumát lefedő képességek megelőző és ellentámadási feladatok ellátására alkalmas elemeinek kialakítására létrehozható egy keretrendszer, amely a kinetikus különleges műveleti képességekhez mérhető speciális megközelítéssel valósítható meg. (H3)

[6] Az APT-k kapcsán leginkább elterjedt magyar elnevezés az állandó, illetve folyamatos szavakat használja a perzisztencia szó helyett. Bár mindkét alternatíva kétséget kizáróan magyarosabban cseng, az idegen szavak szótárát tanulmányozva, a perzisztencia jobb leírást ad tartósan fennálló jelentése révén. Míg az állandó és folyamatos szavak arra utalnak, hogy megszakítás nélküli azonos dinamikájú fenyegetésről van szó, ez nem feltétlenül felel meg a valóságnak az APT-k esetén. Az APT-k tevékenysége jellemzően több szakaszból épül fel, amelyek időtartamban, intenzitásban, valamint az alkalmazott eszközök és eljárások tekintetében is jelentősen eltérhetnek egymástól. A jellemzően több hónapon, vagy akár éveken át tartó APT tevékenységek kapcsán tehát pontosabb megfogalmazás a tartósan fennálló fenyegetés szókapcsolat és szinonimaként a perzisztens kifejezés, ami kevésbé determinisztikus, ezért nagyobb teret enged az APT jelenség valódi természetének érzékeltetésére.

Az első hipotézis (H1) vizsgálata biztonság- és védelempolitikai megközelítést alkalmazva azoknak a stratégiai dokumentumoknak az elemző-értékelő feltárásával és leírásával valósul meg, amelyek az értekezés készítésekor hatályosak Magyarországon és a nemzetközileg feldolgozható stratégiai dokumentummal rendelkező szomszédos államokban (Ausztria, Horvátország, Szlovákia, Szlovénia, Ukrajna), négy – a kiberbiztonsági érettség magas szintje, illetve az igazoltan fejlett kiberbiztonsági képességek megléte miatt – kiválasztott kisállamban (Izrael, Észtország, Svájc, Hollandia) és három nagyhatalmi szereplő (Kína, Amerikai Egyesült Államok, Oroszország) tekintetében. Az értekezés első hipotézishez kapcsolódó része arra a kérdésre is választ ad, hogy stratégiai szinten „Milyen szintet mutat a kibervédelmi képességek nyíltan felvállalt fejlesztésére vonatkozó ambíció a vizsgált országok és szervezetek tekintetében?”.

A második hipotézis (H2) vizsgálata a védelmi szervezetek által kialakított különleges műveleti képességek és tevékenységek, illetve a fejlett perzisztens fenyegetések kapcsán beazonosítható mintázatok és szabályszerűségek összevetésével és szakmai interjúk felhasználásával valósul meg, amelyek alapján feltételezésem szerint jól láthatóvá válnak a fedett körülmények között, kiemelkedő színvonalon, szervezetten és tervezetten, felsőbb – politikai, biztonsági, katonai, nemzetbiztonsági – érdekek mentén megvalósuló végrehajtásból fakadó hasonlóságok. Az értekezés második hipotézishez kapcsolódó részei arra a kérdésre is választ adnak, hogy „A szükséges politikai felhatalmazással a nemzeti érdekek védelmében tevékenykedő APT-k felfoghatók-e a kibertér különleges műveleti erőiként?”.

A harmadik hipotézis (H3) vizsgálata a feldolgozott primer és szekunder szakértői források, valamint a szakértői interjúk nyomán kirajzolódó feltételrendszeren alapul. A feltételrendszer – a nemzeti képességfejlesztés szintjére fókuszálva – lehetőséget biztosít a kiber különleges műveleti képességek kialakításában szerepet játszó erőforrások és azok felhasználási és alkalmazási módjának beazonosítására. Az értekezés harmadik hipotézishez kapcsolódó részei arra a kérdésre is választ adnak, hogy „Milyen tartalmi elemekkel bíró keretrendszer megteremtésével valósítható meg a kiber különleges műveleti képességek sikerrel történő létrehozása és fejlesztése?”.

I.5 Kutatási módszerek

Az értekezésben meghatározott első kutatási cél teljesítése a biztonság- és védelempolitikai folyamatokon belül a kiberbiztonsághoz és kibervédelemhez kapcsolódó stratégiai nézőpontok és célkitűzések elemzésével válik lehetővé. A II. fejezetben meghatározott elméleti keretek és a téma szűkítésével foglalkozó alfejezetek alapján a III. fejezet előbb a stratégiai dokumentumokban megjelenített kiberképességekre vonatkozóan elemzi behatóan és veti össze a vizsgált államok ambíció szintjét. Majd a stratégiai célkitűzések ismeretében meghatározom és értékelem a kiberműveletek teljes spektrumának passzív és aktív védelmi, valamint offenzív területeit és a kapcsolódó képességeket (III.2). Az első hipotézishez (H1) kapcsolódóan a III.3 alfejezet esettanulmányainak tükrében a stratégiai dokumentumok és a szekunder szakértői források elemzésével kirajzolódó kép segítségével összevetem és értékelem az egyes országok és szervezetek nyílt ambíció szintjét a kiberműveletek teljes spektrumán elhelyezkedő képességekhez viszonyítva.

Az értekezésben meghatározott – az első (H1) és második (H2) hipotézishez is kapcsolódó – második kutatási cél elérését a kiberbiztonsági és kibervédelmi stratégiai nézőpontok és célkitűzések átfogó, biztonságpercepció alapú elemzése és értékelése teszi lehetővé. A feldolgozott stratégiai dokumentumokból (III.1) szintetizálható a kitettség mértékére és a biztonság szintjére vonatkozó felfogás, ami a kiberműveleti képességek teljes spektrumának összetevőivel összekapcsolható. A megismert kihívások és fenyegetések kártékonyságának és kifinomultságának azonosítását a kiberműveleti képességek fejlődését bemutató esettanulmányok (III.3) egészítik ki, illetve támasztják alá.

A második hipotézis (H2) állítását, miszerint az ismert fejlett perzisztens fenyegetések (Advanced Persistent Threat – APT) több jellemzője is azonosítható, amelyek hasonlóságot, illetve párhuzamot mutatnak a kinetikus tartományban alkalmazott különleges műveleti erőkkel és képességekkel, a második kutatási célkitűzéssel összhangban vizsgálom. Eszerint részletesen elemzem a fejlett perzisztens fenyegetéseket a IV. fejezetben és a védelmi szervezetek különleges műveleti képességeit a V. fejezetben a működési karakterisztikák meghatározása érdekében. Az APT-k által generált kihívásokról szóló (IV.2), illetve az V. fejezetben a párhuzamok és analógiák azonosítására a működési körülmények paraméterei közül azokat veszem figyelembe, amelyek a tevékenység során a domináns, kevésbé domináns és egyáltalán nem domináns kategóriákba

besorolhatók. A beazonosítható szabályszerűségek elemző jellegű alkalmazása feltételezésem szerint lehetővé teszi a fejlett perzisztens fenyegetések honvédelmi, rendvédelmi vagy nemzetbiztonsági speciális tevékenységként történő értelmezését.

Az értekezésben meghatározott harmadik cél megvalósulását a kiberműveleti képességek elemzése (III.2), az azt követő empirikus esettanulmányok (III.3), illetve a kiber különleges műveleti erőkkel foglalkozó alfejezetek (VI.1, VI.2, VI.3) teszik lehetővé, amelyek a stratégiai és műveleti szempontok egységes keretrendszerben történő feldolgozásával, valamint a szabályzói háttér, a demokratikus kontroll, illetve a hatékonyság kritériumai mentén határozzák meg a kiber különleges műveleti képességek kiépítésének és elhelyezésének lehetőségeit a nemzeti képességfejlesztés szintjén a potenciális szervezeti integrációs alternatívák bemutatásával. Ezáltal a harmadik cél kisebb mértékben a második (H2) és nagyobb mértékben a harmadik (H3) hipotézisre válaszol.

A harmadik hipotézis (H3) állítását, miszerint a kiberműveletek teljes spektrumát lefedő képességek megelőző és ellentámadó feladatok ellátására alkalmas elemeinek kialakítására létrehozható egy keretrendszer, amely a kinetikus különleges műveleti képességekhez mérhető speciális megközelítéssel valósítható meg, a negyedik kutatási célkitűzéssel összhangban vizsgálom. A kiértékeléshez és a keretrendszer kialakításához az APT-kkel (IV.) és a védelmi szervezetek különleges műveleti képességeivel foglalkozó (V.) fejezetekben azonosított analógiák, valamint a kutatás során kibervédelmi, honvédelmi, rendvédelmi és nemzetbiztonsági területen jártas szakemberekkel folytatott irányított interjúk biztosítják az alapot. Az interjúk során kifejezetten cél volt a három szektor sajátos szempontjainak felderítése, a különleges műveleti képességekkel összefüggésben feltárt analógiák helytállóságának igazolása, illetve az eredmények megjelenítése a keretrendszerben. A felkészítéssel, toborzással és struktúrával foglalkozó (VI.4, VI.5, VI.6) alfejezetekben a kiber különleges műveleti képesség kialakításának kinetikus különleges műveleti megközelítéséhez a mentális, fizikai és technikai egyéni készségek és képességek tekintetében kialakított átlagon felüli követelmények szolgálnak kiindulási pontként.

A harmadik (H3) hipotézishez kapcsolódóan az értekezésben meghatározott negyedik célkitűzés elsősorban a VI. fejezet kiber különleges műveleti erők struktúrájával és kihívásaival foglalkozó (VI.6, VI.7) alfejezeteiben, szegmentáltan valósul meg. Egyfelől a kiberműveleti képességek multiplikátor hatásával és a kisállamok kiberműveleti képességfejlesztési lehetőségeivel

foglalkozó szakirodalom szintetizálásával, valamint az irányított szakmai interjúk releváns részeinek összehasonlításával valósul meg az értekezés negyedik célkitűzése.

I.6 Szakirodalmi áttekintés

A kutatás során vizsgált témakör szakirodalmi forrásai lehetővé teszik az átfogó megközelítést az értekezésben felvetett célkitűzések és hipotézisek tekintetében. A téma rendkívül összetett, egyfelől a kibertér mindent átható jellegéből fakadóan, másfelől a kiberbiztonság és biztonsági tanulmányok metszetében való elhelyezkedése okán. Mindez az átfogó szakirodalom gazdagságával és dinamikus bővülésével együtt számos kapcsolódó kutatási lehetőséget kínál, egyúttal megköveteli a téma szigorú behatárolását, ami az értekezés fókusza tekintetében a nyilvánosan hozzáférhető szakirodalom korlátozottságára, illetve hiányosságához vezet.

Az elméleti keretekhez és az alapfogalmakhoz a nemzetközi kapcsolatok meghatározó elméleti irányzatai, ezen belül pedig olyan jelentős publikációk szolgálnak kiindulási pontként, mint Robert Cooper a posztmodern állam és világrend kapcsán megfogalmazott nézetei (Cooper, 2000), Robert Kaplan a hidegháborút követő világrendet leíró fundamentális tézisei (Kaplan, 1994), illetve Hans Morgenthau hatalmi politikáról és politikai realizmusról szóló nagyhatású könyve (Morgenthau, 1978). További támpontként szolgálnak nem csupán az elméleti keretekhez és az alapfogalmak kapcsán, hanem a katonai műveletek és fegyveres konfliktusok tekintetében is a biztonsági tanulmányok és a hadtudomány teoretikusainak munkái, így például Karl von Clausewitz a napóleoni háborúkat követően megfogalmazott időtálló megállapításai (Clausewitz, 1917), Basil Liddel Hart átfogó történelmi analízise a görög-perzsa háborútól a második világháborúig, amelyben külön figyelmet fordít a taktikára, a stratégiára és a hadviselés olyan jelenségeire, mint a gerillahadviselés (Liddel Hart, 2002). Utóbbi kapcsán Carlos Marighella a sikeres forradalom kulcsát a városi gerilla képében látta, ami a dolgozat későbbi részeiben is előkerül, mivel párhuzamok mutatkoznak a kiberhadviseléssel és a kiberműveletek végrehajtóival szemben támasztott követelményekkel (Marighella, 1969). A nemzetközi szakirodalom mellett, hazai szakemberek írásai is széleskörűen használhatók kiindulási pontként az elméleti keretek és az alapfogalmak kapcsán. A felhasznált publikációk között – a teljesség igénye nélkül – megtalálhatók Gazdag Ferenc az érdekről és érdekérvényesítésről szóló nézetei (Gazdag, 2007), továbbá Szenes Zoltán a NATO helyzetéről, feladatairól, új kihívásairól és a szövetség új stratégiai koncepciójáról szóló (Szenes, 2021), valamint a 21. századi biztonsági kihívásokon belül a katonai

biztonságról(Szenes, 2017), illetve a honvédelemről és védelempolitikáról(Szenes, 2020) szóló írásai. Szintén értékes az értekezés szempontjából Csiki Varga Tamás és Tálas Péter Magyarország új nemzeti biztonsági stratégiájáról szóló elemzése (Csiki Varga és Tálas, 2020), valamint Tálas Péter magyar stratégiai kultúráról szóló írása (Tálas, 2014) és Csiki Varga Tamás a stratégiai dokumentumok rendszerét bemutató publikációja (Csiki, 2008). Ezek mellett Kiss Álmos Péter negyedik generációs konfliktusokkal és azok tapasztalataival foglalkozó értekezése (Kiss, 2011), illetve Forgács Balázs hadikultúrákkal (Forgács, 2009), valamint a politika és a háború viszonyrendszerével foglalkozó tanulmánya (Forgács, 2017) szolgál támpontként. Az akadémiai tanulmányok között ugyanakkor nemzetközi munkák is feldolgozásra kerülnek, így Marvin Soroos globális politológiával és problémamegoldással foglalkozó elméleti keretrendszere (Soroos, 1990), illetve a globális közös tereket történelmi perspektívából vizsgáló publikációja (Soroos, 1988). Hasonló megközelítéssel, a történelmi perspektívát a jelen korlátozásaival és tilalmaival ötvözve publikálta értékes gondolatait Nico Schrijver a globális közös terek kezelése kapcsán (Schrijver, 2016), illetve George Perkovich és Ariel E. Levite különböző analógiákat felhasználva teszi közérthetővé a kiberkonfliktusokat (Perkovich és Levite, 2017) közös írásukban, ami az értekezés kapcsolódó részeinek megírását nagyban elősegíti. A pontosabb megértés és a hitelesség megerősítése érdekében az említett publikációkat több esetben olyan primer források egészítik ki, mint például Magyarország Nemzeti Kiberbiztonsági Stratégiája (NKBS, 2013), Magyarország Nemzeti Katonai Stratégiája (NKS, 2021), az Egyesült Nemzetek Tengerjogi Egyezménye (UN, 1966), az Egyesült Nemzetek szerződése az államok tevékenységét szabályozó elvekről a világűr kutatása és felhasználása terén, beleértve a Holdat és más égitesteket (UN, 1982) vagy épp a Kiberbűnözés Elleni Egyezmény (Council of Europe, 2001).

A kiberműveleti képességek elemzéséhez és értelmezéséhez mérvadó dokumentumok a nemzeti stratégiák, amelyek kiválasztásánál a kisállami perspektíva mellett fontos szempontként érvényesült, hogy a dokumentum nemzetközileg feldolgozható legyen, vagyis el lehessen érni akár a nemzeti dokumentumtárban, akár az illetékes nemzetközi szervezetek archívumaiban a hivatalos nyelven kívül angol nyelven is. Így került kiválasztásra többek között a horvát(MoD HR, 2018), az észt (MKM, 2019), az holland (ENISA, 2018), az izraeli (Cyber Israel, 2021), a szlovén (Digital Slovenia, 2016) vagy épp a szlovák (SK CERT, 2021) stratégia. A stratégiai elemzést tartalmazó fejezetben az áttekinthetőséget és a kiberműveletek különböző aspektusainak megértését, illetve a kiberműveletek teljes spektrumának feltérképezését jelentős mértékben segíti a defenzív és

offenzív kategóriák különböző megközelítéseivel foglalkozó akadémiai munkák felhasználása, melyek közül feltétlenül kiemelésre érdemes Dorothy E. Denning munkája, amelyben az aktív kibervédelmet az aktív légvédelem, illetve rakétavédelem koncepciójával veti össze (Denning, 2014). Robert S. Dewar tanulmánya szintén az aktív kibervédelem kifejezés konceptualizálásához járul hozzá és szélesebb, stratégiai perspektívába helyezi (Dewar, 2017), míg Dennis C. Blair a kiberműveletek, valamint a politikai és stratégiai szürke zónák összefonódását (Blair, 2016) hangsúlyozza. Winnona DeSombre és munkatársai az offenzív kiberképességek proliferációjának narratíváját a kiberműveletek életciklusához igazítják és ehhez öt pillért határoznak meg, melyek keretrendszerként használhatók a politikai döntéshozók számára (DeSombre és mtsai., 2021), egyúttal támpontot adnak az értekezés kiberműveleti erőkkel kapcsolatos részeihez. Az offenzív kiberműveleti képességek definiálásában nyújt támpontot a Tom Uren és munkatársai által készített elemzés (Hanson, 2018), amit tovább árnyal Ruperto P. Majuca és Jay P. Kesan a kibertérben folytatott önvédelem optimális alkalmazásáról írt tanulmánya (Majuca és Kesan, 2009).

A fejezet végén található három kiberműveleti esettanulmányhoz változatos jelentések, iparági és internetes dokumentumok biztosítják a szakmai alapot. Kína esetében ilyen például Desmond Ball a kínai kiberhadviselési képességekkel foglalkozó tanulmánya (Ball, 2011), Ming-shih Shen kínai kiberhadviselési stratégiáról és megközelítésről szóló elemzése (Shen, 2019), illetve Jamie M. Ellis a kínai haderő modernizálását támogató kiberkémkedést bemutató értékelése (Ellis, 2015). Kína kibertéri elköteleződésével foglalkozik mélyrehatóan Francis Domingo (Domingo, 2016), míg a kínai haderő számítógépes hálózati műveleti és kiberfelderítő infrastruktúráját vizsgálja Mark A. Stokes egyénileg (Stokes, 2015), illetve két munkatársával (Stokes, Lin, és Hsiao, 2011) is. Ehhez Lyu Jinghua a kínai kiberképességek és szándékok bemutatásával (Jinghua, 2019), míg Li Zhang a kínai kiberháborúval kapcsolatos perspektívák ismertetésével (Zhang, 2012) járul hozzá. Oroszország esetében is hasonlóan széles a dokumentumok köre, ugyanakkor dominálnak az iparági jelentések és beszámolók, illetve oknyomozó riportok, mint például az orosz hírszerző szolgálatok kiberképességeit bemutató elemzés (Galeotti, 2016), vagy a 21. századi stílusban prezentált, nyíltforrású oknyomozás eredménye az FSB elit hackereiről (Tanriverdi, Flade, és Frey, 2022). Konkrét orosz fenyegetést mutat be Stefan Tanase jelentése az orosz APT-k műholdas képességeiről (Tanase, 2015), illetve Brian Bartholomew egyéni elemzése (Bartholomew, 2017), míg szerzőtársával a célzott támadások során alkalmazott hamis, illetve idegen zászlós műveletekbe avat be (Bartholomew és Guerrero-Saade, 2016). Az orosz kiberképességek és erők

múltja, jelene és jövője kapcsán Joe Cheravitch és Bilyana Lilly elemzése (Lilly és Cheravitch, 2020) szolgál kiinduló pontként. Az Amerikai Egyesült Államok kibertevékenységének végrehajtásával foglalkozó egységek képességeinek angol nyelven való dokumentáltsága is számos hiányosságot mutat, azonban a kiberbiztonsági iparág sajátosságai miatt ez egyáltalán nem meglepő. A feltérképezést leginkább szakmai blog bejegyzések, illetve iparági jelentések segítik, mint például a kiberhírszerzési piaccal foglalkozó Elena Gomez előrejelzése (Gomez, 2022), az egyik orosz központú kiberbiztonsági vállalat elemzései (Kaspersky, 2015, 2015a), Pierluigi Paganini amerikai APT-k és nemzetbiztonsági szervezetek összefonódásával foglalkozó írásai (Paganini, 2015, 2017), illetve az amerikai kiberparancsnokságot bemutató hivatalos dokumentumok (Cyber Command, é. n.).

A fejlett perzisztens fenyegetésekkel kapcsolatos kutatásokhoz szükséges dokumentáció feltárása meglehetősen nehézkes a bőséges forrás ellenére. Ennek oka, hogy az információk fragmentáltan érhetők el – a Dmitri Alperovitch (Alperovitch, 2011), az Imperva (Imperva, 2014), vagy a Mandiant (Mandiant, 2013) által publikált – nagyszámú iparági jelentés, akadémiai publikáció, illetve az iparágban elterjed blogbejegyzések és más dokumentumok formájában. A források jelentős része az iparból származik, ami az ipari szereplők viszonylagos monopóliumának köszönhető. Ez elsősorban abból adódik, hogy a kiberbiztonsági incidensekre történő reagálás kapcsán keletkező információk az iparági szereplőknél jönnek létre és sok esetben ott is maradnak, így évekre visszamenő esemény adatbázisok alakulnak ki, ami az akadémiai szektor és a tudományos kutatások számára nem, vagy csak korlátozottan elérhető. Bár elméleti szinten több kutató is foglalkozott a fejlett perzisztens fenyegetések különböző vetületeivel, amelyek akadémiai publikációk formájában hozzáférhetők, mint például Ping Chen és munkatársainak a fejlett perzisztens fenyegetésekről szóló – nem hagyományos ellenintézkedéseket is érintő – átfogó tanulmánya (Chen, Desmet, és Huygens, 2014), Yu-Kyunk Kim és szerzőtársainak az APT-k és az állami szereplők aszimmetrikus kapcsolatát vizsgáló elemzése (Kim és mtsai., 2020), vagy Martin C. Libicki és társai által a nulladik napi sérülékenységekről és a mögöttes piacról szóló publikációja (Ablon, Libicki, és Golay, 2014), az ipari források felhasználásának jelenleg nincs alternatívája. Az iparági források kapcsán azonban minden esetben szem előtt kell tartani, hogy sokszor nem ellenőrizhető forrásokra támaszkodnak, a következtetések hitelesítése gyakran hiányos, illetve sokszor marketing célból készülő kiadványokról van szó, ezért alkalmazásuk esetén fontos a kritikai szemlélet.

A védelmi szervezetek különleges műveleti képességeivel kapcsolatos szakirodalom kettős képet mutat, mivel a honvédelmi, rendvédelmi és nemzetbiztonsági szektorokban zajló folyamatok tudományos feldolgozása jelentős mértékben a nyílt területekre korlátozódik. A különleges műveletekkel kapcsolatos információk ugyanakkor gyakran minősítettek, így a hozzáférés nehezen megoldható, a felhasználásra pedig nincs mód egy nyílt értekezésben. Ennek ellenére a különleges műveletek kapcsán is szép számban állnak rendelkezésre főként hadtudományi és rendészettudományi publikációk az akadémiai szektorból. A külföldi szerzők munkái közül az előbbiek között említendő egy a diplomácia és a különleges műveletek egyedülálló kapcsolatát bemutató értékelés (Kashkett, 2017), továbbá egy lázadóellenes tanulmányokat tartalmazó munka (Paul, Clarke, és Grill, 2010), valamint a különleges műveleti erők stratégiai jelentőségével és hasznával foglalkozó tanulmányok (Horn 2014) (Watts és mtsai. 2021). Magyar szerzők közül kiemelésre méltó Kőszegvári Tibor (Kőszegvári, 2006), Forray László (Forray, 2012) és Gerőcs Imre (Forray és Gerőcs, 2013), illetve Völgyi Zoltán (Völgyi, 2017) elsősorban a különleges erőket, illetve hazai történetüket és alkalmazásukat bemutató publikációi. Rendészettudományi szempontból kiindulási pontot jelent egy a magyar rendőrség különleges szolgálatának történetét feldolgozó publikáció (Beke, 2020), valamint az amerikai szövetségi taktikai egységekről írt kongresszusi jelentés (James, 2015). Nemzetbiztonsági oldalról a hírszerző ügynökségek demokráciában betöltött szerepéről (Vitkauskas, 1999), illetve a mindezt a hírszerző szolgálatok felelősségével és a biztonsági szektor irányításával kiegészítő (Harder, 2017) tanulmányok jelentik a kiindulási alapot.

Az értekezés megírása kapcsán kiemelt jelentőséget tulajdonítok a kiberháborút, a kibertérben megvalósított elrettentést, illetve a kiber különleges műveleti erőket érintő kérdéseket taglaló szakirodalmi forrásoknak. Arról, hogy a kiberháború miért nem fog bekövetkezni Thomas Rid írt széles körben elismert publikációt (Rid, 2012), míg a kiberhatalom kiépítésével és a kibertérben történő kényszerítéssel többen is foglalkoztak (Valeriano, Jensen, és Maness, 2018) (Hodgson, 2018). Jarno Limnéll gondolatai ezen a területen is nyomot hagytak az offenzív kiberképességek elrettentő erejével és szükségességével kapcsolatban (Limnéll, 2013). Katonai szempontból Maren Leed műveleti szintű offenzív kiberképességeket vizsgáló írása (Leed, 2013), illetve Jason Healey a kibertér és a civil-katonai együttműködés kapcsolatát bemutató elemzése (Healey, 2022) nyújt kiindulási pontot, amit a kiber különleges műveleti képességek iránti igényről szóló (Brown, 2018) publikációhoz hasonló források egészítenek ki. A többnyire katonai felsőoktatási és kutató intézeti

programok keretében megjelent publikációk között jelentések, elemzések, szakmai vélemények és értekezések egyaránt megtalálhatók.

Az értekezés központi témájához – a kiber különleges műveleti képességekhez – szorosan kapcsolódó nemzetközileg elemezhető szakirodalom jelenleg hazai és világ szinten is korlátozott, illetve erősen amerikai központú. A nyilvánosan elérhető dokumentumokból két megközelítés rajzolódik ki. Az egyik irány a különleges műveleti erőkből, valamint a változó műveleti környezetből és feladatrendszerből indul ki, amire a különleges erőknek reagálniuk kell. Ezt a megközelítést alkalmazza Patrick Duggan és Elizabeth Oren (Duggan és Oren, 2016), valamint Matthew Nordmoe (Nordmoe, 2015) a kibertér különleges erőkre gyakorolt hatásairól szóló írásaikban. Christopher Paul (Paul és Schwille 2021) és munkatársai (Paul, Porche, és Axelband, 2014) a jövő kiberképességeinek és a különleges erők fejlődésének elemzésekor szintén a különleges erőket veszik modellként. A másik irány a meglévő kiberműveleti képességekből, illetve az azon belül azonosítható, valamint a kihívásokból fakadó speciális feladatokból indul ki. Ennek mentén kiemelhető két értékelés, amelyek igyekeznek igazolni a kiber különleges műveleti erők létjogosultságát (Brown, 2018), illetve a kiber különleges műveleti parancsnokság létrehozását, valamint a „kétsapkás" irányítás megszüntetését (Schoka, 2019).

A hazai és a nemzetközi szakirodalom áttekintése során több olyan témakör is kirajzolódik, amelyeket a kutató közösség a nyilvános forrásokban elhanyagolt, illetve csak érintőlegesen foglalkozott velük. Ilyen témakor a kiberműveletek teljes spektrumának azon szegmense, amely túlmutat az aktív védelem körén és olyan támadó elemeket is tartalmaz, amelyek végrehajtása speciálisan felkészített és felszerelt szakállomány meglétét feltételezi. A nyílt elérésű források lehetővé teszik a védelmi szervezetek különleges műveleti képességeinek összehasonlítását a legfejlettebb és legtöbb kár okozására képes kiberfenyegetésekkel. Módszertani szempontból a közös paraméterek meghatározásával alaposabbá és informatívabbá tehető az összehasonlítás, továbbá a különleges műveleti specifikumok felhasználásával meghatározhatók a kiberműveletek teljes spektrumának speciális felkészítést és felszerelést igénylő komponensei. A fejlett perzisztens fenyegetéseket kiber különleges műveleti képességként vizsgálva értékes háttérismeretek megszerzése mellett új tudományos eredményeket érhetünk el. Ezért kutatásom ezzel a fókusszal zajlott a korábban ismertetett kutatási célkitűzésekkel, hipotézisekkel és módszertannal, illetve a következő fejezetben bemutatott elméleti keretrendszerrel.

II. Elméleti keretek

A doktori értekezés vizsgálati kerete az alábbi komponensekből épül fel: a vizsgálat tárgyát a *kiber különleges műveleti képességek kialakítása* adja, aminek fókusza a *globális közös terek* egyik speciális típusa, a *kibertér* az *ezredforduló után*i időszakban, amikor azt a nemzetközi tapasztalatok tükrében a kibertérből érkező fenyegetésekre adott válaszként vizsgálom *védelmi szervezeti* és *stratégiai nézőpontból* a *nemzeti érdekérvényesítés* elemeként, a *nemzeti képességfejlesztés* szintjén.

II.1 Globális közös terek

A globális közös terek kifejezés eredetileg olyan területekre és természeti erőforrásokra alkalmazható, amelyek felett egyetlen szuverén állam sem rendelkezik joghatósággal (Schrijver, 2016). Egyes nézetek szerint a globális közös terektől elkülöníthetők azok a nemzetközi, illetve szupranacionális közös terek, amelyek felett egynél több állam alakított ki valamilyen rezsimet (Soroos, 1988). Példaként szokás említeni az 1959-es Antarktisz-egyezményt, amelyet az eredeti 12 aláíró országot is beleértve, napjainkig mindössze 54 ország írt alá (ATS, 1959). Miközben az Antarktisz-egyezmény és a hozzá hasonló módon szabályozott nemzetközi közös terek a „nem részes" államokra nézve (pl.: nem aláírók, regionális fókusz) kirekesztők, a nyílt tengerek, a tengerfenék, a világűr és a benne található égitestek jelenleg olyan közös térként vannak számontartva, amelyeket egyetlen szuverén állam sem tart ellenőrzése alatt, de minden állam hozzájuk férhet.

A globális közös terek definíció ugyanakkor magában foglal olyan, nem konvencionális tereket is, mint az atmoszféra és annak időjárási jellemzői, vagy az elektormágneses spektrum. Ezek olyan természeti erőforrások, amelyek tekintetében a szuverén államok határai nem értelmezhetők (Soroos, 1988). Tágabb értelmezésben ide sorolhatók az olyan globális természeti erőforrások is, mint a levegő, a szelek, vagy a napfény, melyek mindegyike létfontosságú eleme a Föld ökoszisztémájának (Schrijver, 2016). Utóbbiak esetében a határokon átnyúló jellegük mellett szintén igaz, hogy nem állnak egyetlen szuverén állam ellenőrzése alatt sem, azonban minden állam, szervezet vagy egyén számára hozzáférhetők. A kibertér és a globális közös terek kapcsán

elméleti síkon gyakran alkalmazzák a területi szuverenitást, melynek lényege, hogy „*az állam saját területén teljes mértékben és egyedül gyakorolja a főhatalmat, cselekvési szabadsággal rendelkezik"* (Regős, 2019). A területi szuverenitás klasszikus elvei a globális közös terekben nem, vagy csak nehezen értelmezhetők. A területi szuverenitással összehasonlítva, egyetlen állam nem képes az ellenőrzése alá vonni és kormányozni a globális közös tereket, pont azok megközelíthetetlen vagy épp mindenütt jelenlévő jellege miatt. Továbbá az esetlegesen egymással szembemenő követelések magukban hordozzák egy nemzetközi konfliktus kialakulásának lehetőségét is, ezért az államok kölcsönös érdeke a terek szabad hozzáférése és felhasználása (Kaushik, 2021).

Abban a tekintetben, hogy a globális közös tereknek a kibertér is része-e, megoszlanak a vélemények. A kérdéskört vizsgáló korai megközelítések rendre az internetet[7] vették alapul, ami meglehetősen szűk értelmezési keretet biztosít, így több kritériumnak sem felel meg, ha globális közös térként akarjuk értelmezni. Az internet alapvetően nem természeti erőforrás, hiszen ember által alkotott komponensek (számítógépek, hálózati kábelek, forgalomirányító eszközök stb.) képezik az úgynevezett fizikai rétegét, amelynek kezdeti fejlesztése ráadásul egyetlen országhoz, azon belül is egy szervezethez köthető. Az internet több szempontból erős nemzeti karakterisztikája mellett az erőforrásai, valamint a hozzáférés is jelentősen korlátozott.

Miközben az internet önmagában több szempontból sem felel meg a globális közös terek ismérveinek, léteznek olyan drasztikus módszerek, amelyek rendkívüli mértékben képesek korlátozni az egyén, egy szervezet, de akár egy vagy több állam számára is az internethez történő hozzáférést. Ilyen módszer például a szolgáltatás megtagadás[8] elérése, amely kiválóan alkalmas a hozzáférés korlátozására, de nem szabad elfelejteni az internet fizikai rétegének mesterséges

[7] Az internet egy globális számítógépes rendszer, amely szabványosított kommunikációs protokollok alkalmazásával kapcsolja össze a világ különböző pontjain található számítógépes hálózatokat, ezért szokás a "hálózatok hálózatának" is hívni. Fejlesztését az Amerikai Egyesült Államok Védelmi Minisztériuma alá tartozó – akkori nevén – Fejlett Kutatási Projektek Ügynökség (Defense Advanced Research Projects Agency – DARPA) kezdte el még az 1960-as években és a közvetlen elődjének tekintett akadémiai hálózatot ARPANET-nek hívták, amely csak az 1970-es évektől kezdett nemzetközivé válni norvég, svéd és brit rendszerek bekapcsolódásával.

[8] A szolgáltatás megtagadás (Denial of Service – DoS) nem feltétlenül rosszindulatú tevékenység következménye. Lényege, hogy egy legitim internetes szolgáltatást olyan mennyiségű elérési, vagy egyéb kéréssel (pl.: bejelentkezési kísérlet a kormányablak online felületén) árasztanak el, hogy a szolgáltatás mögé telepített szoftveres és hardveres infrastruktúra egy ponton képtelenné válik kiszolgálni a megnövekedett igényeket és ezért elutasít (megtagad) minden kapcsolódást, így elérhetetlenné válik. A szolgáltatás megtagadás jelenségét kiválthatja műszaki hiba, illetve főként állami rendszerek esetében gyakran fordul elő, hogy alultervezett infrastruktúrát alakítanak ki, azonban elterjedt kibertámadási módszernek számít, amikor fiktív kérésekkel árasztanak el egy szolgáltatást annak érdekében, hogy az elérhetetlenné váljon.

mivoltát és rombolhatóságát sem. Az internet alapvető infrastruktúrájának törékenységére talán az egyik legszemléletesebb példa a tengerfenéken vezetett, ezért láthatatlan, mégis létfontosságú kommunikációs kábelek sérülékenysége. Évente mintegy 150-200 kábelhiba fordul elő, jellemzően kereskedelmi halászatból és hajózásból, illetve vízfelszín alatti földrengésekből fakadó, tehát nem szándékos fizikai behatások miatt, ugyanakkor egyes nem állami és állami szereplők képesek lehetnek a kábeleken bonyolított adatforgalom lehallgatására, vagy akár a kábelek átvágására is (Morcos és Wall, 2021), ami szélsőséges esetben az internet összeköttetés és hozzáférés megszűnését is eredményezheti.

A kortárs elemzői megközelítések az internet helyett már a kiberteret vizsgálják, mint globális közös tér, ami az olyan klasszikusnak mondható globális közös terekhez is szorosan kapcsolódik, mint a hadviselés színtereiként régebb óta számontartott tengerek és a világűr. Az értelmezési keretek kibertérre történő kiterjesztése kapcsán fontos megjegyezni, hogy nincsen egységesen elfogadott értelmezés, illetve definíció a kibertér vonatkozásában (Ottis és Lorents, 2012). Mivel az alfejezetnek és a dolgozatnak sem célja a különböző kibertérre vonatkozó értelmezések és meghatározások bemutatása, ezért egy-egy kiválasztott nemzeti és nemzetközi leírás segítségével vizsgáljuk tovább a kibertér és a globális közös terek összefüggéseit. A nemzeti értelmezések közül a magyar kiberbiztonsági stratégia az alábbi meghatározást alkalmazza: *„A kibertér globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét jelenti.”*(NKBS, 2013) Nemzetközi kitekintésben a NATO meghatározása szerint a kibertér: A globális domén, amely magába foglal minden összekapcsolt kommunikációs és információs technológiát és egyéb – beleértve a szeparált vagy független, adatot feldolgozó, tároló és továbbító – elektronikus rendszereket, hálózatokat és azok adatait. (NATO, 2020a) A kibertérben végrehajtott műveletekre vonatkozó szövetséges összhaderőnemi doktrína többek között kitér arra, hogy a kibertér jóval több mint az internet és bár alapvető eleme a mesterségesen kialakított és folyamatosan fejlesztett számítógépes környezet, nem csupán arra korlátozódik. A kibertér infrastruktúrája globális szinten jelentős mértékben összekapcsolt, azonban földrajzi határok mégis értelmezhetők a joghatóság és a nemzeti felelősség tekintetében. Ezt erősíti a magyar kiberbiztonsági stratégia meghatározását kiegészítő mondat is, mely szerint *„Magyarország kibertere a globális kibertér elektronikus információs rendszereinek azon része, amelyek Magyarországon találhatóak, valamint a globális kibertér elektronikus rendszerein keresztül*

adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok közül azok, amelyek Magyarországon történnek vagy Magyarországra irányulnak, illetve amelyekben Magyarország érintett."(NKBS, 2013) Tehát nemzeti és nemzetközi szinten egyaránt megjelenik egyfajta szuverenitás értelmezés a kibertérrel összefüggésben.

Folytatva a már hivatkozott NATO doktrína értelmezését, a globális közös terek szempontjából kifejezetten fontos a felhasználásra vonatkozó kitétele, illetve a rétegzett megközelítése a kibertér tekintetében. A doktrína egyfelől megállapítja, hogy a kiberteret bárki használhatja szinte bármilyen céllal, másfelől a kiberteret három rétegre osztja fel, melyek a fizikai, a logikai, illetve a kiber-személyiség (cyber-persona). Ebben a megközelítésben a különböző hardver komponensek (számítógépek, szerverek, forgalomirányító eszközök, kábelek, szenzorok stb.) földrajzi helyhez kötődnek. A logikai réteget alkotó elemek leginkább számítógépes kód, illetve adat formájában manifesztálódnak és az ember számára operációs rendszerek, protokollok, alkalmazások és más szoftver vagy adat komponensek formájában válnak értelmezhetővé. Ezek nem képesek funkcionálni a fizikai réteg nélkül és a két réteg együtt teszi lehetővé a harmadik réteg számára a kommunikációt és működést. A kiber-személyiségnek nevezett réteg nem tartalmaz valódi személyt vagy szervezetet, de azok virtuális identitásaként értelmezhető. A virtuális identitás lehet akár egy e-mail cím, egy felhasználói azonosító, vagy egy közösségi média profil. Amiben a második és harmadik réteg jelentősen eltér a fizikai rétegtől, hogy nincsenek határaik. Az államhatárok jogi értelemben csak a fizikai rétegben található hardver komponensek tekintetében relevánsak, mivel pozíciójuk földrajzi értelemben meghatározható.

A kibertér sajátosságait figyelembe véve nincs könnyű dolga annak, aki a globális közös térként való értelmezés mellett érvel, hiszen a való élet azt mutatja, hogy a kibertérhez való hozzáférés számos módon korlátozható. Sőt, a gyakorlat azt is bebizonyítja, hogy egyes államok képesek ellenőrzésük alá vonni a kibertér bizonyos szegmenseit. Ez azonban hasonlóságokat mutat a tengerekre és édesvizekre vonatkozó szabályokkal, melyek a parti tengerek, vagy a kizárólagos gazdasági övezetek révén bizonyos előjogokat garantálnak egyes államok számára. Tény, hogy a tengerjog napjainkban jóval érettebb szabályrendszernek tekinthető, mint a kibertérre vonatkozó szabályozás, de a vizsgálat szempontjából a tengerek olyan globális közös terek, amelyek bizonyos részei állami, vagy nemzetközi ellenőrzés alatt állnak, akár csak a kibertér. Ezen a ponton pedig érdemes kitérni a szabályok betartathatóságára, illetve kikényszeríthetőségére. Ebben fontos

szerepe van a már említett rétegzett felépítésre vonatkozó NATO megközelítésnek, ami alapján két rétegre teljes mértékben igaz a határokon átnyúló jelleg, mely rendkívül komplikálttá, gyakran lehetetlenné teszi a nemzeti szabályrendszer hatékony érvényre juttatását. Ez minimum megkérdőjelezi az állam főhatalmát a kibertérben, miközben bizonyos kibertéri műveletek képesek akár egy államot is korlátozni, vagy megfosztani cselekvési szabadságától. Ezek után a kibertérhez való mindenki általi hozzáférés kérdése inkább csak elméleti síkon értelmezhető. Biztonság- és védelempolitikai szempontokat alapul véve elenyésző jelentősége van annak, hogy egy elmaradott, vagy fejlődő régió milyen arányokat mutat a világ digitalizációban élenjáró részéhez képest. A magas szintű digitalizáció magas szintű kitettséggel jár együtt, ezért sokkal fontosabb és a valósághoz közelebb áll a NATO által alkalmazott megközelítés, mely szerint a kiberteret bárki szinte bármire használhatja. Ezt erősíti hazánk Nemzeti Katonai Stratégiája (NKS, 2021) is, amely kissé burkoltan, de úgy fogalmaz, hogy *„viszonylag szabadon hozzáférhető”* a kibertér. Az utolsó és egyben vitán felül álló érv a kibertér globális közös térként való értelmezhetőségével szemben, hogy nem fizikai terület, természeti erőforrás vagy természeti jelenség. Kétségtelen, a kiberteret az ember hozta létre. A kibertér mesterséges mivolta és az emberi élet egyre több elemére befolyást gyakorló dimenziói túl mutatnak minden eddigi emberi alkotáson és pont ez az, ami annyira egyedivé teszi, hogy egy ember által alkotott globális közös térként tekinthetünk rá.

Összegezve az alfejezetben leírtak alapján biztosan kijelenthető, hogy a globális terek értelmezési keretein a kibertér mindenképpen túl mutat mesterséges mivolta miatt, azonban ezt az egy kritériumot leszámítva több ponton is hasonlóság látszik az olyan hagyományos globális közös terekkel, mint a világűr, vagy éppen a világtengerek. Ezen túlmenően, a kibertér különböző rétegei masszív kiterjedéssel rendelkeznek az említett globális közös terekben, miközben az olyan természeti erőforrásokban és nem konvencionális terekben is jelen vannak, mint a légtér, vagy az elektromágneses spektrum. Globális közös térként a kibertér földrajzi szempontból nehezen szűkíthető, ugyanakkor fontos aspektus, hogy a kutatás Magyarországon, részben magyar szakemberek közreműködésével, a kisállami perspektívát mindvégig szem előtt tartva készült. Ennek tükrében a kutatás fő iránya Magyarország szövetségi rendszereire tekintettel a kibertér szereplőinek képesség alapú elemzése és az eredmények lehetséges hazai, illetve kisállami implementálásának vizsgálata. Bár katonai értelemben – különösen a NATO tagállamai számára – a kibertér jelentősége hivatalosan csak 2016-ban értékelődött fel, a katonaság a kezdetektől fogva jelentős szerepet tölt be az internet, illetve a kibertér létrejöttében, mivel több komponensének

kifejlesztése is az amerikai haderő égisze alatt történt. A globális közös terek meghatározására irányuló elméletek tekintetében az egyik fontos ismérv azok határokon átnyúló mivolta, amelyet a kibertér az említett terekre való kiterjedésével tulajdonképpen automatikusan megörököl. Tekintettel a fenti megállapításokra az értekezés további részeiben a kiberteret globális közös térnek fogadjuk el azzal a kitétellel, hogy a mesterséges fundamentuma révén más globális közös terekhez képest könnyebben rombolható akár hagyományos és nem hagyományos katonai eszközökkel is.

II.2 Vizsgált időszak

Nincs egyetlen olyan dátum, amikor a kibertér globális közös térré válása megkezdődött, sokkal inkább egy a technikai, társadalmi, gazdasági és politikai dimenziókon átívelő, jelenleg is zajló folyamatként, egy fokozatos fejlődésként érdemes felfogni. Tekintettel arra, hogy a kibertér fizikai infrastruktúrájának a kialakulása felé tett első lépések egybe vágnak az internet, illetve elődjének születésével érdemes kiemelni és áttekinteni néhány technológiai folyamatot, melyek mindezt lehetővé tették[9]. Mindenképpen fontos mérföldkőnek tekinthető az Amerikai Egyesült Államok haderejének hidegháborús hálózati kommunikációs törekvései nyomán az 1960-as években létrejött kutató hálózat, az ARPANET. Illetve nem szabad elfeledkezni a személyi számítógépek forradalmáról sem. Előbbi tekintetében 1980-ra kialakult és nemzetközileg is elfogadottá vált az internet máig fontos szerepet betöltő nyílt architektúrája a TCP/IP[10]. Az évtized végére pedig elindulhatott az első kereskedelmi célú elektronikus levélküldő szolgáltatás, miközben az internet éves fejlődése elérte a száz százalékot. Eközben a személyi számítógépek terén 1977-ben megjelentek az első olyan eszközök, melyek már magánszemélyek és kisvállalkozások számára is megfizethető áron kerültek piacra. A technológiai fejlődés és a személyi számítógépek elterjedése nyomán az 1980-as évek közepén beindultak társadalmi folyamatok is. Létrejöttek az első elektronikus úton szerveződő közösségek, amihez nagyban hozzájárult az 1984-ben bevezetett domén név címzési rendszer, majd az 1988-ban megvalósult első valós idejű beszélgetés az

[9] Lásd bővebben: Brief History of the Internet, https://www.internetsociety.org/internet/history-internet/brief-history-internet/ (Elérés: 2022. február 14.)
[10] A TCP/IP egy angol betűszó, a Transmission Control Protocol/Internet Protocol rövidítése. Magyarul átviteli vezérlő protokoll/internetprotokoll, ami valójában egy több rétegből álló kommunikációs protokoll struktúra a hálózati eszközök összekapcsolására. A TCP/IP az internet architektúrájának gerince.

interneten. Szintén ebben az évben készült el az első transzatlanti optikai kábel, amelyhez hasonlóból napjainkra több mint 1,2 millió kilométernyi hálózza be a világtengereket[11]. Jóval költségesebb és több szempontból kevésbé megbízható szegmense a kibertérnek a műholdak által kínált lehetőségek, melyek közül talán a legismertebb a Globális Helymeghatározó Rendszer, a GPS (Global Positioning System). A GPS-hez kapcsolódó kutatások szintén a hidegháború korszakába nyúlnak vissza, miközben a rendszer teljes műveleti képességét 1995-ben érte el először[12]. Az 1990-es években teret nyert az internet publikus felhasználása és előtérbe került a kereskedelem. Az évtized végére már több mint 10 ezer internet szolgáltató működött világszerte. Az ezredfordulót megelőző évekre a fejlődés dinamikája olyan mérteket öltött, hogy az internetre kötött eszközök mennyisége miatt új IP cím szabványt kellett bevezetni. Az ezredforduló és az azt követő évek számos új jelenséget hoztak a kibertérbe, kezdve az első szolgáltatás megtagadással járó támadással (2000), a jelenleg globális szinten meghatározó közösségi média felületek – a LinkedIn (2002), a Facebook (2004) vagy a Twitter (2006) – megjelenésén át, egészen a mobil internet forradalmáig, amit az Apple vállalat iPhone modelljének 2007-es piacra dobása és az Android operációs rendszer 2008-as megjelenése robbantott be. (Benito, 2020) Ugyanakkor megjelentek az első olyan konfliktusok is, amelyekben kiberműveleteket alkalmaztak. Előbb 2007-ben Észtország, majd 2008-ban Grúzia tapasztalhatta meg az offenzív kiberműveletek következményeit.(Perkovich és Levite 2017, 6)

A kibertér tekintetében nehezen vitatható jelenség a szabályozás esetenként évtizedes elmaradottsága a technológiai fejlődés üteméhez képest, azonban léteznek a kibertér szempontjából meghatározó egyezmények és megállapodások. Mivel a műholdak révén a kibertér kiterjed a világűrre is, időrendben az első említésre méltó nemzetközi egyezmény az 1967-es Világűrszerződés (UN, 1966), amelynek értelmében a világűr mindenki által szabadon használható, de senki által nem kisajátítható tér. Többek között a már többször szóba került tengeralatti kábelek révén a kibertér szintén kiterjed a világtengerekre is, amely szempontból meghatározó az 1982. évi Egyesült Nemzetek Tengerjogi Egyezménye (UNCLOS), ezen belül is főként a nyílt tengerekre és az ott végezhető tevékenységekre vonatkozó rendelkezések (UN,

[11] Lásd bővebben: How Does Cyberspace Work? *World101 from the Council on Foreign Relations*, https://world101.cfr.org/global-era-issues/cyberspace-and-cybersecurity/how-does-cyberspace-work (2022. február 14.)

[12] Lásd bővebben: History of GPS Program, https://www.aiaa.org/docs/default-source/uploadedfiles/about-aiaa/press-room/videos/iaf-60th-anniv-gps-nomination.pdf?sfvrsn=9bc64bfa_0 (Elérés: 2022. február 14.)

1982). Az elsősorban a kibertér fizikai infrastruktúráját érintő nemzetközi egyezmények mellett érdemes szót ejteni a közpolitikai és felhasználási szempontból mérföldkőnek számító szabályzókról. Az Amerikai Egyesült Államoknak a kibertér történetében betöltött szerepe nyomán, az egyik közpolitikai szempontból meghatározó dokumentum a Clinton adminisztráció idején 1996-ban megjelent Telekommunikációs Törvény, ami határozott különbséget téve a telekommunikációs és információs szolgáltatások között, útjára indította az internet korszakot (Ehrlich, 2014). Nem csak nemzeti, hanem regionális szinten is születtek olyan dokumentumok, amelyek fontos szerepet töltöttek be az elmúlt évtizedek során. Ilyen az Európa Tanács égisze alatt 2001-ben éppen Budapesten megszületett, a kiberbűnözés visszaszorítását célul kitűző egyezmény (Council of Europe, 2001), ami „*világszerte olyan referenciaként szolgál, mely a kibertér számos szabályozási hiányossága mellett szinte egyetlenként világos feladatrendszert szab a csatlakozó államok számára azzal kapcsolatban, hogy nemzeti jogukban hogyan kezeljék az egyre jobban elharapódzó kiberbűncselekményeket*" (Krasznay, 2021). Bár kötelező jogi erővel nem bír, mégis fontos megemlíteni a NATO akkreditációval rendelkező Kooperatív Kibervédelmi Kiválósági Központ (Cooperative Cyber Defense Centre of Excellence – CCDCOE) által készített kézikönyvet, a Tallinn Manual-t. A kézikönyv először 2013-ban foglalkozott a nemzetközi jog alkalmazhatóságával a kiberműveletekkel összefüggésben. Miután 2016-ban a NATO Varsóban megrendezett csúcstalálkozóján hivatalosan is műveleti területként ismerte el a kiberteret (CCDCOE, 2016), 2017-ben megjelent a felülvizsgált Tallinn Manual 2.0, 2021 óta pedig már a harmadik kiadáson dolgoznak a központ szakemberei[13].

Bár szabályrendszerre égető szüksége lenne a világnak, a kibertér technikai és technológiai sajátosságai sok esetben lehetetlenné teszik a hatékony szabályozás kialakítását. Ebben a tekintetben az egyik legkomolyabb – egyelőre feloldhatatlannak látszó – probléma a támadó fél beazonosítása, illetve az azonosítás folyamata során beszerzett információk hitelessége. Nehéz bármilyen jogszabályt úgy érvényre juttatni, ha nem lehet meghatározni, hogy kivel szemben alkalmazzuk a szóban forgó előírásokat. A Kevin Mitnick[14] által az 1970-es évektől elkövetett

[13] Lásd bővebben: The Tallinn Manual, https://ccdcoe.org/research/tallinn-manual/ (Elérés: 2022. február 14.).
[14] Az 1963. augusztus 6-án született Kevin David Mitnick a világon az egyik legismertebb hacker, aki elsősorban az emberi hiszékenységet kihasználó (social engineering) módszereivel képes volt hozzáférést szerezni nagyvállalati rendszerekhez, vagy egy kávés bögrével a kezében bejutni egy védett épületbe. Bővebben: https://www.mitnicksecurity.com/about-kevin-mitnick-mitnick-security

emberi hiszékenységet kihasználó támadások, vagy az 1988-as Morris[15] számítógépes kártevő megjelenése óta nagyot fordult a világ kiberbiztonsági szempontból. 2002-ben az internet egyik alapvető infrastruktúráját, a domén név rendszert (Domain Name System – DNS) történelmi jelentőséggel bíró túlterheléses támadás érte[16], 2006-tól pedig az egyik elismert amerikai kutató szervezet, a Stratégiai és Nemzetközi Tanulmányok Központ (Center for Strategic & International Studies – CSIS) önálló listát vezet a szignifikáns kiber incidensekről[17]. Jelenlegi ismereteink szerint az első digitális fegyver, a Stuxnet névre keresztelt kártevő, melyet sikerrel vetettek be az iráni atomprogram ellen 2010-ben[18], miközben a különböző számítógépes kártevők száma a kiberbiztonsági incidenst elszenvedő szervezetek számával együtt azóta is jelentős mértékben növekszik. A társadalom számára szélesebb körben először 2010 után váltak ismertté az olyan kiber incidensek, amelyek mögött a kiberbiztonsági szakemberek állami támogatást sejtettek. Egy évtized alatt pedig már a támadó oldalon is megjelentek az olyan csúcstechnológiának számító megoldások, mint az automatizálás, a gépi tanulás, vagy éppen a mesterséges intelligencia, melyek révén nagyobb lehet a támadások volumene és jobban álcázhatóvá válnak, miközben a támadó kiléte is könnyebben elrejthető. (Fehér és Négyesi, 2021)

[15] Az 1988-ban 23 éves Robert Tappan Morris egyetemista hozta létre azt a számítógépes kártékony kódot, ami 24 óra leforgása alatt mintegy 6000 számítógép megfertőzésével az okkori internet 10 százalékát érte el. A készítője után Morris névre keresztelt kártékony szoftver nem tett tönkre, vagy semmisített meg fájlokat, azonban rendkívüli módon lelassította a megfertőzött rendszereket, az e-mail akár napokat is késhettek. Bővebben: https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218

[16] Az internet telefonkönyveként is emlegetett domén név rendszerrel (DNS) teszi lehetővé, hogy a számítógépek hálózati azonosításához használt IP címek (számok) helyett elegendő legyen csak neveket megjegyeznünk. A rendszer felépítéséből fakadóan 2002-ben összesen 13 ún. gyökér (root) DNS szerver üzemelt, amelyek a rendszer gerincét adták, tulajdonképpen az internet létfontosságú infrastruktúrájának meghatározó elemei voltak. A támadás 9 szervert érintett összesen. Bővebben: https://www.cs.cornell.edu/people/egs/beehive/rootattack.html

[17] A CSIS 1962-es alapítása óta számtalan témában jelentetett meg tudományos igényességgel elkészített elemzéseket és tanulmányokat. A szervezet 2006 óta önálló projekt keretében listát vezet azokról a kiber incidensekről, amelyek kormányzati ügynökségeket, védelmi vagy technológiai cégeket érnek, illetve 1 millió dollárnál nagyobb veszteséget okozó gazdasági bűncselekménynek számítanak. Bővebben: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

[18] 2010-ben a Stuxnet névre keresztelt számítógépes kártevő felbukkanása hidegzuhanyként hatott a biztonság különböző területeivel foglalkozó szakemberekre. Nagy nyilvánosság előtt a kiberbiztonsági szakemberek korábban még soha nem találkozhattak hasonló képességekkel rendelkező kártevővel, ahogy az ipari folyamatirányító rendszerek üzemeltetői sem voltak felkészülve egy ennyire komplex kiber támadásra. Míg a nukleáris biztonságért felelős szakértők számára szintén merőben új megközelítést mutatott, hogy tárgyalások és leszerelés helyett egy kiber-fizikai támadás következett be, a biztonságpolitikai szakértők azért aggódhattak, hogy hosszú távon milyen következményekkel jár egy ilyen esemény és milyen geopolitikai folyamatokat indíthat el. Későbbi szakértői elemzések szerint az incidens legalább másfél évvel vetette vissza az iráni atomprogramot azáltal, hogy a nukleáris létesítményekben használt ipari folyamatirányító rendszerek megtámadásával túlpörgették és tönkretették az urán dúsításához használt centrifugákat. Bővebben: http://hadmernok.hu/2010_4_kovacs_sipos.pdf

A vizsgált időszak tekintetében nem szükséges az ezredfordulót megelőző éveket mélyrehatóan tanulmányozni. A kibertérhez kapcsolódó technikai, gazdasági és társadalmi folyamatok nagyjából az ezredforduló környékére érték el azt a szintet, ami nem csak lehetővé tette, de fokozatosan alapvető követelménnyé transzformálta a nemzetállamok számára az olyan képességek kialakítását, amelyek segítségével az államok közötti interakciók kiterjeszthetővé váltak a kibertérre. Bár ezeknek a képességeknek a létezése csak a 2000-es évek második felében vált széles körben ismertté, a katonai képességfejlesztés terén jártas szakemberek számára nyilvánvaló, hogy egy bevetésre alkalmas képesség mögött több éves fejlesztési és szervezési munka áll. Ezek alapján a tudományos vizsgálódás időszaka az elmúlt két évtizedet öleli fel, amelytől – indokolt esetben – néhány év eltérés előfordulhat. Az értekezés tárgyát képező vizsgálat időszaka 2022. januárig terjed[19], amitől a források feldolgozása eltérést mutathat.

II.3 A tudatos felhasználótól az APT-kig: 21. századi kiberbiztonsági kihívások

Ha figyelembe vesszük az Amerikai Egyesült Államok Haditengerészeti Intézete (U.S. Naval Institute – USNI) által Thomas Moorer tengernagynak[20] tulajdonított megjegyzést (Naval Institute, 2021), amely szerint 1959-es megjelenését követően „a fénymásoló gép az egyik legnagyobb nemzetbiztonsági fenyegetés, amit valaha is kitaláltak”; valószínűsíthető, hogy a kibertér kialakulásával és térnyerésével összefüggő negatív hatások és kihívások miatt elsőként szintén katonai körökben kezdtek el aggódni. Az elmúlt évek jelentősebb kiberbiztonsági incidensei alapján mára már nem csak a kiberbiztonsági kihívásokkal foglalkozó szakemberek, hanem szélesebb társadalmi rétegek számára is nyilvánvaló, hogy a kibertérben zajló folyamatok számos ponton fenyegetést jelenthetnek egy nemzet biztonságára, ezáltal kihívások elé állítva az azt garantálni hivatott rendvédelmi, honvédelmi és nemzetbiztonsági szervezeteket. A kiberbiztonsági

[19] A 2022. február 24-én kitört orosz-ukrán konfliktus kibertérben zajló eseményeit az értekezés nem érinti, mivel az értekezés írásának idején az információk hitelessége nem vagy csak nehezen ellenőrizhető, számottevő az ellentmondásos információk aránya, illetve az elemzésre és értékelésre rendelkezésre álló idő nem teszi lehetővé a tudományos igénnyel történő feldolgozást.

[20] Thomas Hinman Moorer 1912. február 9-én született az Alabama államban található Mt. Willing településen. Haditengerészeti pilotaként tengernagyi rendfokozatig jutott, majd 1970. július 2-án kinevezték a Vezérkari Főnökök Egyesített Bizottságának (Joint Chiefs of Staff – JCS) élére. Az elnöki posztot négy éven keresztül töltötte be. Ez alatt az idő alatt aktívan részt vett a Vietnámba vezényelt amerikai erők drasztikus csökkentésében 1970 és 1972 között, továbbá aktív szerepet játszott a stratégiai fegyverzet korlátozó (Strategic Arms Limitation Talks – SALT) tárgyalások alakulásában. Bővebben: https://www.jcs.mil/About/The-Joint-Staff/Chairman/Admiral-Thomas-Hinman-Moorer/

kihívások tekintetében a legfontosabb kérdés általában az, hogy ki és mit tekint kiberbiztonsági kihívásnak, hiszen ez alapjaiban határozza meg a reakciót. A kiberbiztonsági kihívások bemutatása több kiegészítéssel, de jelentős mértékben a közreműködésemmel 2021-ben megjelent „A globalizált világ kihívásai" című tanulmánykötet kiberbiztonsági fejezetén alapul, mivel az abban foglaltak jelenleg is időszerű megállapításokat tartalmaznak. (Berzsenyi, 2021)

A kiberbiztonsági kihívások többféle módon csoportosíthatók, ezért a kiberbiztonság definíciójához hasonlóan nem található olyan felosztás, amit mindenki egyöntetűen alkalmazna. Ennek hátterében az áll, hogy a kiberbiztonsági kihívások számos eltérő szempontrendszer alapján vizsgálhatók és a különböző iparági szereplők is jobbára saját preferenciáikat igyekeznek érvényre juttatni. A kiberbiztonsági kihívások kapcsán az átlagember a médiában leggyakrabban előforduló kibertámadásokra asszociál, azonban a kibertér biztonsága és védelme túlmutat a támadások egyszerű felsorolásán és megkülönböztetésén. Tágabb értelemben véve a kiberbiztonsági kihívások magukba foglalják a támadások megelőzése, a felhasználók tudatossága vagy a technológiai fejlődés kapcsán felmerülő problémákat is, de egy olyan entitás számára, ahol korábban nem foglalkoztak kiberbiztonsággal, a hatékony kiberbiztonsági szabályozás és szervezeti struktúra kialakítása – különösen szakértelem hiányában – szintén kihívást jelenthet. A rendelkezésre álló kereteken belül nincs lehetőség minden egyes kiberbiztonsági kihívás eltérő szempontok alapján történő megvizsgálására és részletes bemutatására. Ha a kiberbiztonsági kihívásokat pusztán a támadásokra szűkítjük le, még mindig többféle megközelítést alkalmazhatunk. A kiberbiztonsági támadások motivációjukat tekintve szinte kivétel nélkül besorolhatók valamelyik kategóriába az alábbiak közül: politikai/ideológiai, pénzügyi/gazdasági, hírszerzési/kémkedési, hacktivista vagy destruktív indíttatású.

A kibertámadásokat a motiváció szempontjából vizsgálva az élmezőnyben a pénzügyi, illetve gazdasági haszonszerzés okán elkövetett támadások mellett az egyre jelentősebb arányt képviselő hírszerzési, illetve kémkedési céllal indított, leginkább állami szereplők által megvalósított vagy állami szereplő támogatásával megvalósuló támadások állnak. Ugyanakkor a politikai és ideológiai motiváció is egyre nagyobb számban merül fel a támadások kapcsán. Ide sorolható a gyakran külön kezelt terrorizmus is, hiszen – a legtöbb terrorizmus definícióban megjelenő motívumot elfogadva – a terroristák végső célja a saját politikai, ideológiai vagy vallási akaratuk másokra történő rákényszerítése. A motivációk kapcsán fontos kiemelni, hogy a legismertebb hacktivista

mozgalmak (Anonymous, LulzSec) jellemzően szintén valamilyen politikai vagy ideológiai cél köré szerveződnek, így ezek támadásai – akárcsak a terrorizmus – a végső cél tekintetében a politikailag, illetve ideológiailag motivált támadások közé sorolhatók. A hacktivizmusnak mára kevésbé domináns ága, amikor valaki csak azért hajt végre egy kibertámadást, hogy a képességeit bizonyítsa saját maga, a megtámadott vagy egy harmadik fél számára. Miközben a kvázi „kedvtelési célú" támadások eltűnőfélben vannak, feltűntek olyan kibertámadások, amelyeknek egyetlen célja a rombolás és pusztítás, elsősorban a kibertér működését és használatát biztosító eszközök és szolgáltatások működésképtelenné tételével. A kibertámadások trendjei folyamatosan változnak, így könnyen találhatunk olyan csoportosítást, ahol a destruktív és a politikai, illetve ideológiai támadásokat a kiberhadviselés címszó alatt gyűjtik össze. Minden esetben érdemes arra ügyelni, hogy az adott kategorizálást milyen metodika mentén alakították ki, és milyen céllal. Az Amerikai Egyesült Államok Kiberbiztonsági és Infrastruktúra Biztonsági Ügynöksége (Cybersecurity & Infrastructure Security Agency – CISA) a kiberfenyegetések lehetséges forrásai alapján az alábbi kategóriákat alkalmazza[21] nemzeti kormányok, terroristák, ipari kémek és szervezett bűnözői csoportok, hacktivisták és hackerek.

Ez tulajdonképpen egy módosított és részben egyszerűsített értelmezése az amerikai Kongresszus által létrehozott Kormányzati Számvevőszék (Government Accountibility Office – GAO) által kiadott kiber kihívásokat leíró dokumentumnak[22]. A kibertérből érkező kihívások egy másik módon történő csoportosítása, amit sokszor ötvöznek a motivációval, az a támadó és a megtámadott szervezet között fennálló kapcsolatra utal. A kibertámadásokkal összefüggésben sokakban él az a téves prekoncepció, hogy a támadások az adott rendszeren vagy szervezeten kívülről érkeznek, és a szervezet számára ismeretlenek az elkövetők. Azonban a valóság az, hogy a kibertámadások jelentős része köthető valamilyen belsős közreműködéshez, mint például jelenlegi vagy korábbi munkavállaló szándékos vagy nem szándékos tevékenysége. Látható, hogy a belülről érkező fenyegetések rögtön tovább bonthatók két újabb kategóriára. Az információs rendszerek auditálásával és biztonságával foglalkozó szakembereket tömörítő nemzetközi szervezet (Information Systems Audit and Control Association – ISACA) felmérése alapján 2016-ban a 3

[21] Lásd bővebben: Cyber Threat Source Descriptions https://www.cisa.gov/uscert/ics/content/cyber-threat-source-descriptions#gao (Elérés: 2022. február 16.)
[22] Lásd bővebben: Cyber Threats and Data Breaches Illustrate Need for Stronger Controls across Federal Agencies https://www.gao.gov/assets/gao-15-758t.pdf (Elérés: 2022. február 16.)

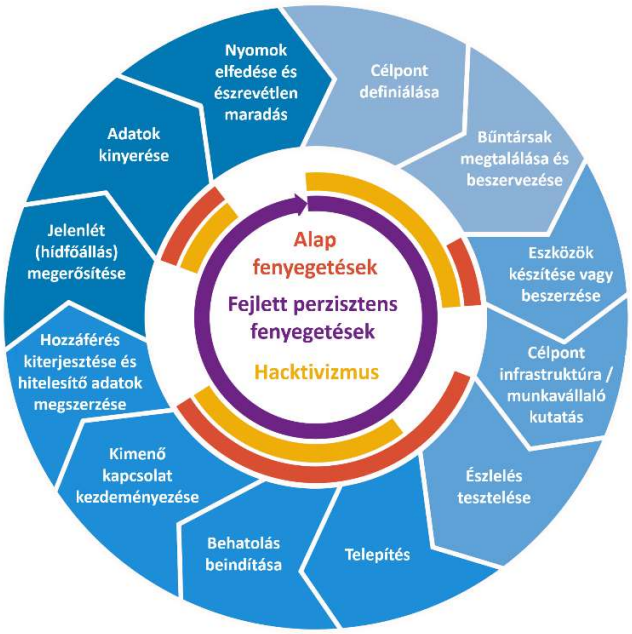
legjelentősebb kiberbiztonsági kihívás között negyven százalékkal a második helyen voltak a belülről érkező fenyegetések. (Dimitriadis, 2016) A belső fenyegetések jelentőségére utal az amerikai Reptéri Kooperatív Kutatási Program (Airport Cooperative Research Program – ACRP) keretében kiadott jelentés is, amelynek kiberbiztonsági kihívásokat kategorizáló listája több alkategóriát is alkalmaz a belső fenyegetések leírására. (Muphy és mtsai., 2015) Tekintettel arra, hogy a kiberbiztonság nemcsak technológiai, hanem jelentős mértékben humán kihívás is, minden esetben kiemelt figyelmet kell fordítani az emberi tényezőre, azon belül is a végfelhasználóra. A kibertérből érkező kihívások tovább elemezhetők a támadások típusának meghatározásával, azonban fontos megjegyezni, hogy napjainkban a különböző technikákat és eljárásokat a támadók legtöbbször kombináltan alkalmazzák, aminek számos oka lehet. Az úgynevezett elosztott szolgáltatásmegtagadással járó (Distributed Denial of Service – DDoS) támadásokat például gyakran alkalmazzák önmagukban egy-egy nagyobb rendszer megbénítására és elérhetetlenné tételére, de nem ritka, hogy csak elterelésként vetik be azért, hogy egy szofisztikáltabb műveletet leplezzenek vele. Napjainkban gyakoriak az adathalász (phishing), illetve a pszichológiai manipulációra (social engineering) épített támadások, amelyek a felhasználók megtévesztésén alapulnak, és elsősorban információ megszerzésére irányulnak (például személyes adatok, online banki bejelentkezéshez szükséges adatok, vállalati belső információ stb.). Egy-egy ilyen támadást jellemzően valamilyen rosszindulatú szoftver (malicious software – malware) bevetése követ, amelyek számtalan funkciót és feladatot képesek ellátni az áldozat számítógépén vagy okos eszközén anélkül, hogy tudomást szerezne róla. Ezen a ponton érdemes visszatérni a támadó motivációjára, hiszen, ha valaki kémkedni akar, attól nagy valószínűséggel nem kell féltenünk a pénzügyi hozzáféréseinket, annál inkább a vállalati kommunikációt (például: azonnali üzenetküldők, elektronikus levelezés stb.) és a céges dokumentumokat. Ez többnyire fordítva is igaz, ha egy anyagi haszonszerzési céllal indított kibertámadás áldozatává válunk, akkor elsősorban a bankszámlánk megcsapolása, illetve az ismeretlen tranzakciók miatt érdemes aggódni, ettől még a személyes fotó- vagy videógyűjteményünk nem feltétlenül kerül veszélybe. Más a helyzet az úgynevezett zsarolóvírusok esetében, amelyek az áldozat eszközére települve titkosítanak minden adatot, amelyekhez csak váltságdíj megfizetése után férhetünk hozzá újra, ha szerencsénk van, és megkapjuk a feloldókulcsot a támadótól. A kibertér bizonyos szegmensei kimondottan veszélyesek az átlagfelhasználó számára, ezért is fontos az általános kiberbiztonsági tudatosság növelése, a kiberhigiénia megteremtése már a legfiatalabb generáció esetében is. Sajnos ezen a téren nem áll

túl jól társadalmunk, nem véletlen, hogy a legtöbb nemzetközi szervezet kiberbiztonságot érintő napirendjén kiemelt helyen szerepelnek a képzés, oktatás és a tudatosság növelésével összefüggő kihívások.

Mélyebb és részletesebb kategorizálást alkalmaz az Európai Hálózat és Információ Biztonsági Ügynökség (European Network and Information Security Agency – ENISA) kihívás-taxonómiai táblázata, ami 8 főcsoportra bontva számos kihívást rögzít (ENISA, 2016). A dokumentum – szó szerinti fordításban – „aljas tevékenységek és visszaélések" főcsoportjában találhatók a „célzott támadások", ahova többek között a fejlett perzisztens fenyegetések (Advanced Persistent Threat – APT) is tartoznak. Az angolszász terminológiából, elsősorban a rövidítéssel ismertté vált jelenség pontos meghatározásával és részletesebb bemutatásával később, a III. fejezetben foglalkozom. A kiberbiztonsági kihívásokkal összefüggésben az APT-k jelentőségét alapvetően az elnevezésben érdemes keresni, de a téma szűkítése kapcsán mindössze arra célszerű fókuszálni, hogy a kiberbiztonsági iparág legtöbb szereplője igen magas kockázatú kategóriába sorolja az APT tevékenységet. (Johnson, 2020) Bár az APT tevékenység sok esetben a korábban leírt kiberbiztonsági kihívások tetszőleges kombinációját jelenti, vagyis a cél hálózatot védők számára ismerősek lehetnek az alkalmazott eljárások és megoldások, az eszközök kreatív és kifinomult alkalmazása, a rosszindulatú szoftverek tudatos és hatékony fejlesztése, valamint a nem ismert hibák és sérülékenységek kihasználása a legjelentősebb fenyegetések közé pozícionálja. A fenyegetés mértékét tovább növeli, hogy az APT tevékenységre jellemző a tervezett, célzott és kitartó végrehajtás, amit olyan szereplők valósítanak meg, akiknek biztos anyagi és szakmai háttér áll rendelkezésére. Egy 2017-es elemzés (Lemay, 2018) megjegyzi, hogy az APT elnevezés mára egy újabb marketing címkévé alakult át a kiberbiztonsági termékek prospektusaiban, ezért a kifejezés degradálódása következtében sok esetben ma már valamilyen alternatív – de továbbra is a legsúlyosabb fenyegetéseket tartalmazó – kategóriában, például a célzott támadások, vagy a stratégiai és kormányzati tevékenység alatt lehet megtalálni a kiberbiztonsági kihívásokkal foglalkozó nemzetbiztonsági beszámolókban (Lella és mtsai., 2021), iparági előrejelzésekben (Mandiant, 2022a) és nemzetközi szakmai jelentésekben (NSA, 2022).

A kibertérből érkező kihívások és fenyegetések közötti eltéréseket egy életciklus ábra segítségével szemléltetem. Az ábra külső ívén fentről az óramutató járásával megegyező irányba haladva támadási lépéseket, illetve tevékenységeket látunk, amikhez a belső vörös, sárga és lila ívek révén

három fenyegetés kategória tartozik. Az ábra alapvetően három csoportba sorolja a kiberfenyegetéseket: alap fenyegetések, hacktivizmus, fejlett perzisztens fenyegetések. Jól látszik, hogy míg az alap fenyegetések és a hacktivizmus csak bizonyos lépéseket tartalmaz, a fejlett perzisztens fenyegetések minden támadási lépést magukba foglalnak. Ezek közül is kiemelendő a szofisztikáltságra utaló infrastruktúra kutatás és észlelés tesztelés, a jelenlét megerősítése, valamint a nyomok elfedése, amikkel a hagyományos támadások során kevésbé törődnek a támadók. Ennek eredménye, hogy a hagyományos támadások gyakran a célpontok rendkívül széles körét érintik, azonban jóval alacsonyabb siker rátával dolgoznak, miközben elterjedtebb a „fogd és vidd" szemléletmód. Nem fektetnek energiát a pontos célkiválasztásra, nem törődnek a támadásból hátramaradó digitális nyomokkal és nem foglalkoznak azzal, hogy a megszerzett hozzáférést hosszú távon fenntartsák.



1. ábra: A fejlett perzisztens fenyegetések támadási életciklusa kiegészítve az alap fenyegetésekkel (commodity threats) és hacktivizmussal (hacktivism). Fontos megjegyezni, hogy az ilyen és ehhez hasonló ábrák szinte minden esetben tartalmaznak bizonyos mértékű általánosítást, így előfordulhat, hogy egy-egy specifikus támadás esetében az ábrán szereplő lépések közül hiányzik egy tevékenység, vagy plusz lépés is azonosítható. Ez azonban a támadások trend szintű vizsgálatát nem befolyásolja. Az ábrát fordította és szerkesztette a szerző. (Forrás: https://www.kaspersky.com/resource-center/threats/advanced-persistent-threat és https://commons.wikimedia.org/wiki/File:Advanced_persistent_threat_lifecycle.svg) (Elérés ideje: 2022. július 26.)

Szintén a hagyományos és fejlett fenyegetések közötti különbségek bemutatását segíti a leuveni egyetem három kutatójának APT-kről szóló tanulmányában (Chen, Desmet és Huygens, 2014) szereplő ábra, amely táblázatos formában hasonlítja össze a támadók, a célpontok, a szándékok és a megközelítés, illetve szemléletmód alapján a hagyományos és a fejlett perzisztens fenyegetéseket.

Hagyományos és APT támadások összehasonlítása		
	Hagyományos támadások	APT támadások
Támadó	Többnyire egyéni	Magasan szervezett, szofisztikált, eltökélt és jól ellátott csoport
Célpont	Nem meghatározott, többnyire egyedi rendszerek	Specifikus szervezetek, kormányzati intézmények, kereskedelmi vállalatok
Szándék	Pénzügyi haszonszerzés, képességek demonstrációja	Verseny előny megszerzése, stratégiai haszonszerzés
Megközelítés	Egyszer futtatott, rövid ideig tartó, „törj be és vidd”	Ismétlődő próbálkozások, lassú és alacsony profilú, adaptáció a védelmi intézkedésekkel szemben, hosszútávú

2. ábra: A hagyományos és APT támadások összehasonlítása. (Forás: http://link.springer.com/10.1007/978-3-662-44885-4_5 - a szerző fordítása) (Elérés ideje: 2022. február 17.)

A fenti ábrák jól szemléltetik és alátámasztják, hogy ma már nem csak egyszerű kibertámadásokról (hackelésekről) beszélünk, amiket pusztán anyagi megfontolásból követnek el, hanem az értekezés szempontjából releváns kiberhadviselésről, stratégiai célkitűzésekről és a kapcsolódó eszközrendszerről van szó.

Összegezve, az alfejezetben leírtak alapján a legtöbb elterjedt és ismert – a kibertérből érkező kihívások és fenyegetések csoportosítását is magába foglaló – modell kiemelt jelentőséget tulajdonít a fejlett perzisztens fenyegetéseknek. Az alkalmazott módszereken és megoldásokon túl a vélt vagy valós állami háttér, illetve támogatás csak tovább súlyosbítja a fenyegetés jelentőségét, miközben az APT tevékenységek hatásai korábban nem tapasztalt gazdasági, energiabiztonsági vagy akár társadalmi folyamatokat indíthatnak el. Mindezek együttesen alkalmassá teszik az APT

tevékenységeket arra, hogy nemzetbiztonsági szempontból kiemelt kockázatú jelenségként kezeljük és átfogó megközelítést alkalmazva összevessük a különleges műveleti képességekkel.

II.4 Védelmi szervezetek kihívásai és a kibertér szerepe a 21. században

A védelmi szervezetek tekintetében a kutatás főként a hazai biztonsági szektor kapcsán elérhető forrásokkal dolgozik olyan leegyszerűsített felosztást alkalmazva, amely a legtöbb állam tekintetében – ha minimális különbségekkel is, de – a fennálló aktuális helyzetet tükrözi. A biztonsági szektorban azok az állami intézmények és szereplők találhatók, amelyek az állam és a lakosság biztonságát garantálni hivatottak. Az értelmezési keretek szűkítése és a szövetségi rendszerbe (Észak-atlanti Szerződés Szervezete – North Atlantic Treaty Organisation – NATO, Európai Unió – EU, Európai Biztonsági és Együttműködési Szervezet – EBESZ) tagozódott államok közötti univerzális megközelítés okán a kiber különleges műveleti képességek kialakításával kapcsolatban a biztonsági szektor végrehajtói szintjén három fundamentális védelmi szervezet kihívásaival foglalkozunk: ezek a haderők, a rendvédelmi szervek, valamint a nemzetbiztonsági szolgálatok. A védelmi szervezetek kihívásai kapcsán máig érvényes megállapításokat közölt Tálas Péter és Gyimesi Gyula integrált biztonsági szférával foglalkozó tanulmánya. Ahogy azt a bevezetőben írják, a „*globalizálódó biztonsági környezetben – szemben a korábbi korszakokkal – a külső és a belső biztonság közötti határvonal egyre inkább elmosódik, a hagyományos területelvű biztonság- és védelempolitika helyett az érdekalapú (érdekérvényesítő, érdekvédő) és értékalapú biztonságpolitika került előtérbe.*” (Tálas és Gyimesi, 2008) A bipoláris világrendet követő multipoláris világrend kialakulásával egyidejűleg kibővült a biztonság fogalma is. Napjaink kihívásai a nemzetek biztonságát érintő alapkérdéseket is megváltoztatják, ami egyfelől a teljes biztonsági szektort átfogó kihívást generál, másfelől a korábbiaktól eltérő megközelítést igényel az államok részéről. Az állami komplex biztonságfelfogást tükröző stratégiai dokumentumokban rendre megjelennek azok a kihívások, amelyek a legtöbb állam biztonsági szektorában beazonosítható honvédelmi, rendvédelmi és nemzetbiztonsági elemek tekintetében relevanciával bírnak. A védelmi szervezetek 21. századi biztonsági kihívásainak elemzéséhez a legfelső szinten ezek a dokumentumok kínálnak lehetőséget, amelyek *„alapját az állam biztonságfelfogása, azaz a biztonságról, annak alkotóelemeiről, területeiről, különösképpen pedig a biztonságot fenyegető tényezőkről alkotott képe jelenti”*. (Csiki, 2008) Hazánk esetében az elsőszámú ilyen dokumentum az aktuális Nemzeti Biztonsági Stratégia (NBS), ami 2020

áprilisában jelent meg „Biztonságos Magyarország egy változékony világban” címmel. A globális biztonsági környezet értékelése tekintetében a stratégia *„romló tendenciát”* (NBS, 2020) állapít meg és összesen *„17 kiemelt, a magyar nemzeti érdekek szempontjából jelentős biztonsági kihívást és kockázatot sorol fel”* (Csiki Varga és Tálas, 2020).[23]

A már említésre került szövetségi rendszerek szintjén is találhatók olyan stratégiai dokumentumok, amik egyfelől iránymutatásként szolgálnak a nemzeti stratégiák kidolgozásához, másfelől a nemzeti szintű dokumentumokhoz hasonlóan a biztonság területén bemutatják azokat a kihívásokat, amikkel szemben feladatai vannak az adott szövetségnek. Mindez jellemzően az adott szövetség saját szervezetei esetében közvetlenül, míg a tagállamok végrehajtói szintjén közvetett módon jelenik meg.

Az Európai Unió tekintetében ez a dokumentum 2020-ban jelent meg és „A biztonsági unióra vonatkozó uniós stratégia” címet viseli (EU, 2020a). A kibertérből érkező fenyegetések már a dokumentum bevezetőjében megjelennek. Bár a stratégia elismeri, hogy az európai jólét forrásai közé tartozik a globalizáció, a szabad mozgás és a digitalizáció; egyúttal a kitettséget is növelik: a terrorizmus, a szervezett bűnözés, a kábítószer-kereskedelem és az emberkereskedelem egyaránt veszélyt jelentenek az európai életmódra. A jóléti források kapcsán negatívumként jelenik meg a kibertámadások és kiberbűncselekmények terjedéséhez való hozzájárulás.

A NATO esetében a legfelsőbb szintet a Washingtoni Szerződés[24], illetve a stratégiai koncepciók (NATO, 2022) jelentik, amelyek leírják a szövetség céljait, alapvető biztonsági feladatait, valamint érdemben foglalkoznak a szövetséget érintő biztonsági kihívásokkal és lehetőségekkel, amelyekkel a változó biztonsági környezetben szembesül. Mivel a legújabb koncepció elfogadása 2022 nyarára várható, az aktuális pedig már több mint 10 éves, az elméleti keretek meghatározásának

[23] Az NBS által kiemelt kihívások és kockázatok: illegális migráció; váratlan fegyveres támadás; összehangolt diplomáciai, információs és titkosszolgálati műveletek; jelentős károkat okozó kibertámadások; terrorcselekmény elkövetése; nemzeti szuverenitást sértő és a határon túli magyar közösségek elleni törekvések; kritikus demográfiai helyzet kialakulása; gazdasági válság és a globális kereskedelem leállása; energiaellátási válsághelyzet kialakulása; instabilitás, illetve “bukott állam” létrejötte a régiónkban; forradalmi technológiák illetéktelen kezekbe kerülése; bűnszerevezetek és szervezett bűnözői csoportok térnyerése; tömegpusztító fegyverekkel, illetve ABV anyagokkal végrehajtott támadások; regionális hatással bíró ipari balesetek és katasztrófák bekövetkezése; tömeges és súlyos megbetegedést okozó járványos betegség terjedése; természeti katasztrófák és extrém időjárási jelenségek bekövetkezése; a globális felmelegedés bioszférára gyakorolt negatív hatásai.

[24] A Washingtoni Szerződés – más néven Észak-atlanti Szerződés – a NATO alapító egyezménye, amelyet 1949. április 4-én írt alá 10 európai ország mellett az Egyesült Államok és Kanada azzal a céllal, hogy közösen tartsák fenn a békét és biztonságot, előmozdítsák a stabilitást és jólétet, valamint megőrizzék a demokrácia, az egyéni szabadság és jog uralmának közös értékeit.

időpontjában egy köztes dokumentum bír relevanciával a NATO által érzékelt biztonsági kihívások kapcsán. A „NATO 2030 – Együtt egy új korszakért" című jelentés (NATO, 2020b) tekinthető az új stratégiai koncepció előfutárának is, egyrészt mert a koncepció előkészítő dokumentuma, másrészt az új koncepció várhatóan tükrözni fogja a jelentés által alkalmazott megközelítést és annak javaslatait. Ahogy elemzésében Szenes Zoltán írja, a NATO *„a biztonsági kihívásokat és a kockázatokat többféleképpen csoportosította"*: geopolitikai, szektorális, tevékenységi fajták. (Szenes, 2021) A biztonsági környezet kapcsán a dokumentum kiemeli a globális verseny erősödését és a fenyegetések egyre nehezebb előrejelezhetőségét, beleértve a terrorizmust, a kibertámadásokat, a diszruptív technológiákat, a klímaváltozást, illetve az orosz és kínai kihívást. (NATO, 2021)

Az átlagember számára a leginkább kézenfekvő és könnyen értelmezhető biztonsági kihívások azok, amelyekkel saját maga is kapcsolatba kerül mindennapi élete során. Ugyanakkor a bankkártyával történő visszaélések, az online világban megvalósuló zaklatások, vagy éppen az emberkereskedők által alkalmazott kegyetlen módszerek, amivel az állampolgár akár a napi sajtótermékek fogyasztásával, akár saját tapasztalás nyomán szembesül, jellemzően a rendvédelmi szektor és a rendvédelmi szereplők számára jelent egy-egy esetnél magasabb szintű, komplexebb kihívást. Napjaink rendészeti kihívásaival kapcsolatban Sallai János arról írt, hogy a világ összekapcsoltságából adódóan felerősödött a szervezett bűnözés, a kibertér pedig folyamatosan új lehetőségeket nyújt a kiberbűnözők számára, akik leginkább adathalász módszerekkel és rosszindulatú szoftverek küldésével igyekeznek a lehető legnagyobb haszonra szert tenni. Kiemeli a kiberbűnözés arctalan és határok nélküli jellegét, valamint a kibertér gyermekeket érintő kockázatait. (Sallai, 2015)

Az Europol[25] 2016-ban éppen Budapesten tartott konferenciát a jövő rendvédelmi képzéseiről, ahol arra a következtetésre jutottak, hogy az alábbi fenyegetésekre és a kapcsolódó bűncselekményekkel szembeni tevékenységre kell felkészíteni a jövő rendvédelmi dolgozóit (Mainwright, 2016): terrorizmus, migráció, kiberbűnözés, szervezett bűnözés, illetve a szervezett bűnözői csoportok online térnyerése. Elsőként a kiberbűnözés és az elkövetők egyre növekvő agresszivitását, illetve

[25] Az Europol az Európai Unió bűnüldöző ügynöksége, melynek székhelye Hágában található. Az ügynökség segítséget nyújt a súlyos nemzetközi bűnözés és terrorizmus elleni küzdelemben az EU 27 tagállama számára, így jelentős szerepet vállal a pénzmosás, a kábítószer-kereskedelem, a szervezett csalás, az euró hamisítása, az embercsempészet és a terrorizmus elleni küzdelemben.

a meglévő sérülékenységek ismétlődő kihasználását emeli ki a dokumentum, amit a digitális higiénia és biztonság hiánya, illetve az ismert eszközök és módszerek újrahasznosítása tesz lehetővé. A feltörekvő technológiák (pl.: kriptovaluták[26]) bűnözők által történő felhasználása, illetve a rosszindulatú szoftverek kifinomultsága és elterjedése szintén kiemelt fenyegetés. Ezeket elsősorban információ lopás, zsarolás (zsarolóvírusok), illetéktelen távoli hozzáférés, illetve bankautomaták manipulálása során alkalmazzák. Végül kiemelt szerepe van az adatszivárgásoknak, az online csalásoknak és a gyermekek kizsákmányolásának, amikhez új dimenziót nyitnak az alternatív pénzügyi szolgáltatások, az élő közvetítést lehetővé tevő funkciók, illetve az internet sötét oldala (darknet)[27].

Sok szempontból a nemzetbiztonsági szolgálatok tevékenysége a rendvédelmi és honvédelmi szektor szereplőinek feladatrendszerével együtt vizsgálható, mivel a stratégiai elképzelésekben megjelenő biztonság- és védelempolitikai kihívások azonosak, csak a válaszok tekintetében eltérő eszközrendszert és módszereket alkalmaznak a három terület szervezetei. Míg a rendvédelmi és honvédelmi szektor eszközrendszerének nagyrésze jól átlátható, a nemzetbiztonsági és hírszerző szolgálatok esetében a kihívásokkal és fenyegetésekkel kapcsolatos tényeken alapuló képalkotást nehezíti a transzparencia rendkívül alacsony foka, a minősített dokumentumok jelentős száma és az operatív tevékenységek fedett jellege. Kifejezetten magyar vonatkozásban ezt támasztja alá Dihen Mihály publikációja (Dihen, 2020) is, amely a hazai hírszerzés, vagyis az Információs Hivatal (IH)[28] kapcsán a szolgálat létrehozása óta egyedülálló intézkedéssorozat központi elemeként említ egy olyan 2018-as, a szervezet működési környezetével és tevékenységével foglalkozó koncepciót, amely kormányzati jóváhagyás mellett nem nyilvános besorolást kapott. A dokumentum hordereje kapcsán a szerző szerint hasonló utoljára az IH elődszervezetében, az 1989-es demokratikus körülményekhez történő átalakulás során történt.

[26] A kriptovaluta egy olyan digitális eszköz, amelyet különböző számítógép hálózatokon keresztül végrehajtott tranzakciók biztonságos lebonyolítására használnak. Digitális, alternatív és virtuális valutaként is nevezik őket, legfőbb jellemzőjük a decentralizáltság. Központi (pl.: nemzeti bankok) felügyelet nélkül működnek országhatárokon átnyúló fizetőeszközként. 2022 márciusában több mint 18 ezer kriptovaluta létezik.

[27] A darknet – más néven darkweb – kifejezés az 1970-es évekből ered, tehát nagyjából egyidős az internettel. Eredetileg az internettől független hálózatokat jelölte a „sötét hálózat" kifejezés, napjainkban azonban egy olyan információ-réteget jelöl, amely nagyon magas szintű titkosítás mellett működő, jellemzően névtelenül üzemeltetett oldalakat rejt, amik csak speciális szoftverekkel érhetők el. A darkneten elérhető anonimitás és a kriptovaluták nyújtotta előnyök miatt a bűnözés melegágyának számít, ahol például drogokkal, fegyverekkel, személyes- és banki adatokkal vagy éppen kiberfegyverekkel kereskednek.

[28] Az Információs Hivatal Magyarország nemzetbiztonsági szolgálatai közül a polgári hírszerzésért felelős szervezet, amely jelenleg a külügyekért felelős minisztérium irányítása alatt áll.

Mivel hasonló dokumentumok a többi nemzetbiztonsági szolgálat vonatkozásában sem érhetők el nyilvánosan, ezért indirekt megközelítéssel az egyik leginkább kiterjedt struktúrával rendelkező és legjobban dokumentált ország az Amerikai Egyesült Államok kapcsán tekintjük át a biztonságpercepció azon nemzetbiztonsági vonatkozású elemeit, amelyek más régiók és országok tekintetében is relevanciával bírhatnak. A stratégiai versengés (Kína, Oroszország) és a hagyományosnak tekinthető geopolitikai ellenfelek (Irán, Észak-Korea) jelentette kihívásokon túl a nemzetbiztonsági szervezetek számára kiemelt helyen szerepel az egészségügyi biztonság, illetve azon belül a pandémia, a biológiai fegyverek, és a rendhagyó egészségügyi incidensek. Szintén kiemelt figyelmet kap a klímaváltozás és a környezet rombolása, valamint az olyan transznacionális tényezők, mint az új technológiák innovatív alkalmazása, a szervezett bűnözéshez kapcsolódó drogkereskedelmi, pénzmosási és kiberbűnözői tevékenységek, továbbá a migráció és a globális terrorizmus. Míg a kibertérrel összefüggésben – az elérhető dokumentumok alapján – az amerikai nemzetbiztonsági szektor számára a határokon átnyúló, esetszámban, kiterjedésben és kifinomultságban egyaránt dinamikusan növekvő zsaroló szoftverekkel elkövetett támadásokat és azok következményeit azonosítják kihívásként(DNI, 2022), a hazai szolgálatok tekintetében úgy tűnik, hogy a kiberbűnözés elleni tevékenység mellett a kiberterrorizmus megelőzése és elhárítása kap kiemelt figyelmet. (Dobák, 2014)

Amikor a honvédelem és a kibervédelem metszetét vizsgálva keressük a választ arra, hogy a haderők számára milyen jelentőséggel és kihívásokkal bír a kibertér, fontos figyelembe venni alapvető hadtudományi és hadtörténeti aspektusokat. A hadviselés tulajdonképpen az emberiség kezdete óta folyamatosan jelen van és fejlődik, emiatt különböző időszakait generációkra szokás osztani[29]. Ahol jelenleg is tartunk az a negyedik generációs hadviselés, amelynek legfontosabb sajátossága, hogy nem feltétlenül államok között zajlik. Míg az egyik hadviselő fél állam, a másik fél nélkülözi az állami ismérveket. Utóbbiakra gyakran hivatkoznak úgy, mint nem állami szereplő (pl. terrorszervezetek, hacktivista csoportok stb.), amely elnevezés nem zárja ki az állami támogatás bármely formájának lehetőségét. A negyedik generációs hadviselésre az aszimmetria jellemző az alkalmazott erők és eljárások tekintetében egyaránt, amitől összehasonlításuk

[29] A hadviselés generációiról bővebben Orosz Zoltán (Szegedy-Maszák Mihály, Vincze Ferenc, és Zákány Tóth Péter, szerk., *Nemzeti művelődés--egységesülő világ*, Kútfő bibliotéka 6 (Budapest: Napkút, 2010)) és Kiss Álmos Péter („Kiss Álmos Péter PhD - kiss_almos_peter_doktori_ertekezes.pdf”, elérés 2022. február 27., https://tudasportal.uni-nke.hu/xmlui/static/pdfjs/web/viewer.html?file=https://tudasportal.uni-nke.hu/xmlui/bitstream/handle/20.500.12944/12252/kiss_almos_peter_doktori_ertekezes.pdf?sequence=6&isAllowed=y) munkáiban olvashatunk.

értelmezhetetlenné válik. Annak ellenére, hogy a kapcsolódó jelenségek nem újak, egyfajta paradigmaváltásról lehet beszélni, amelynek keretében az állam hadviselési monopóliuma megszűnik és a nem állami hadviselő a reguláris erőkkel egyenrangú hadviselővé válik.

A haderők kihívásainak tekintetében a negyedik generációs hadviselés és a 21. századi fegyveres konfliktusok jellemzőire figyelemmel érdemes folytatni a vizsgálódást, amihez a nemzeti katonai stratégiai dokumentumok nyújtanak kézenfekvő tájékozódási pontot. Magyarországon az aktuális Nemzeti Katonai Stratégia (NKS, 2021) 2021-ben jelent meg és alapvetően a hierarchiában felette elhelyezkedő Nemzeti Biztonsági Stratégiában meghatározott kihívásokat tekinti mérvadónak, amelyek kezeléséhez összkormányzati együttműködésre van szükség. A Magyar Honvédség vezető, illetve támogató szerepe felmerül az állami és nem állami fenyegetések kapcsán egyaránt, a váratlan fegyveres támadások esetén hazai és szövetséges területen, a tömegpusztító fegyverekkel szemben, a radikális ideológiák és a terrorizmus terjedése miatti válságkezelési képességek terén, valamint az illegális migráció, a pandémiás helyzetek, továbbá a klímaváltozás következményeivel, illetve a természeti és ipari katasztrófák kezelésével kapcsolatban. A Magyar Honvédség szerepvállalását igénylő fenyegetések és kihívások között az előkelő második helyen említi a stratégia a nem hagyományos hadviselés eszköztárán belül az információs technológiai eszközök jelentette fenyegetéseket. Ezzel kapcsolatban a stratégia kitér az azonosítás (attribúció) nehézségeire és arra, hogy hazánk a „*kiberképességeket fegyvernek, alkalmazásukat pedig akár fegyveres támadásnak*” (NKS, 2021) is tekintheti, amire katonai választ adhat. A stratégia készítői megjegyzik, hogy más műveleti területekhez képest a kibertérben jóval gyorsabban lehet hatást kiváltani, miközben az elkövetők kilétének leplezése jobban megoldható. A stratégia elismeri a kibertér egyre növekvő szerepét a műveleti fölény megszerzésében és megtartásában, az elrettentés és a konfrontáció idején egyaránt. A Magyar Honvédségről szóló pont kitér arra, hogy a kiberműveleti erők által a kibertérben végrehajtott műveletek – beleértve az offenzíveket is – hozzájárulnak a kinetikus műveletek hatékonyságához, míg békeidőben aktív szerepet vállalnak a nemzeti kibervédelmi feladatokban. Ezt a harc- és harctámogató képességek pontban tovább részletezi a dokumentum és előírja *„minden műveleti szinten passzív és aktív kibervédelmi képességek”* (NKS, 2021) kialakítását, amelyek biztosítják a kibertérből érkező és katonai jelentőséggel bíró fenyegetések és veszélyek azonosítását, kezelését, valamint a hatékony válaszlépéseket és ellenintézkedéseket. Mindezzel nem csak Magyarország kiberbiztonságához járul hozzá aktívan a Magyar Honvédség, hanem a szárazföldi erők, a légierő és a különleges

műveleti erők kinetikus képességeit is támogatja. A kibervédelmi képességek terén kívánatos fejlesztések kiterjednek a katonai felderítő és hírszerző képességekre is, amivel kapcsolatban a tevékenységek fokozására létrejönnek a *„kibertér műveletek végrehajtására való készségek és képességek”* (NKS, 2021).

Összegezve, az alfejezetben leírtak alapján az látszik, hogy a haderőket, illetve rendvédelmi és nemzetbiztonsági szerveket egyaránt jelentős kihívások elé állítják a kibertérből érkező fenyegetések. A vonatkozó ágazati stratégiák és egyéb dokumentumok szinte kivétel nélkül kiemelt jelentőséget tulajdonítanak a digitalizálódó világ, illetve a kibertér terjedése következtében folyamatosan növekvő kitettségnek. A kibertérben zajló folyamatok hatással vannak a védelmi szervezetek feladatrendszerére is. Míg a haderőknek jellemzően a katonai rendszerek kibervédelmére történő felkészülés az elsődleges, addig a rendvédelmi szervek számára a kiberbűnözés változatos formáival szembeni felkészülés, a nemzetbiztonsági szerveknek pedig a nemzeti értékeket és érdekeket sértő kibertérből érkező fenyegetésekkel szembeni felkészülés jelent kiemelt feladatot. Ebben a feladatrendszerben elhelyezhető a kiberműveletek teljes spektrumának az a szegmense, amely a kinetikus dimenzióban létrehozott különleges műveleti képességekhez hasonló felkészülést és felszerelést igényel, illetve ami képes biztosítani az arányos válaszadási és ellentámadási kapacitást a nemzeti érdekérvényesítés számára.

II.5 A kortárs fegyveres konfliktusok és a kiberhadviselés kapcsolata

Korábban már szóba kerültek a hadviselés különböző generációi, amelyek tekintetében a világ különböző régióiban zajló konfliktusok aktuális trendjei olyan elemek kombinált megjelenését, vagy felerősödését mutatják, mint az aszimmetria és a hibrid összetevők alkalmazása. *„A nemzetközi katonai biztonsági rendszer változásai tükröződnek a közelmúlt háborúinak, katonai konfliktusainak változó karakterében, amelyet eltérő módon ír le a külföldi és hazai szakirodalom. A hidegháború utáni konfrontációkat, napjaink háborúinak, konfliktusainak széles spektrumát a különböző szerzők különféleképpen jellemzik.”* (Szenes, 2017) A katonai biztonsággal foglalkozó kutatások kiterjednek az aszimmetrikus- és hibrid hadviseléssel kapcsolatos elméletekre, azonban ezeket a teljesség igénye nélkül csak a téma szűkítése okán érintjük. Az aszimmetrikus- és hibrid hadviseléssel kizárólag a kiberhadviselés kontextusba helyezésének szintjén, átfogó megközelítést alkalmazva foglalkozunk azzal a céllal, hogy értelmezzük a kiberműveleti képességek aszimmetrikus- és hibrid hadviselésben betöltött helyét, szerepét.

Frank Hoffman[30] 2009-ben a modern konfliktusok fejlődő karakterisztikájának újragondolása kapcsán úgy fogalmazott, hogy az Egyesült Államok afganisztáni és iraki szerepvállalásai rámutattak a modern hadviselés komplexitásának korlátozott értelmezésére (Hoffman, 2009). Nézetei szerint a gyakran hibrid fenyegetésnek nevezett multinacionális kihívások tulajdonképpen a hibrid megközelítést alkalmazó ellenfelek különböző képességeinek kombinált alkalmazása aszimmetrikus előny megszerzésére, kialakítására, amit rövid és középtávon a legnagyobb műveleti kockázatként értékelt. A hibrid hadviselés során legalább az egyik fél a fenyegetések és képességek egyedi kombinációját alkalmazza a másik fél gyenge pontjainak és sérülékenységeinek kihasználására, ezáltal elkülönülő kihívások és alapjaiban különböző (hagyományos, irreguláris, terrorista) megközelítések helyett a háború és fegyveres konfliktusok összes formáját alkalmazó kihívókra kell számítani. A gyakorlatban ez azt jelenti, hogy a hibrid konfliktusok során a kihívást nem egyetlen állam jól meghatározott megközelítése jelenti, hanem több állam, vagy csoport, amelyek a taktikák és technológiák teljes menüjéből választva innovatív módon vegyítik azokat saját stratégiai kultúrájuk, geopolitikai beágyazottságuk és céljaik érdekében.

A modern háborúkkal összefüggésben Martin van Creveld[31] azon az álláspontón van, hogy ezekben a konfliktusokban a főszerepet az államok helyett szubnacionális szereplők, fegyveres és gerilla csapatok, etnikai, vallási és terrorista csoportok, illetve ezeknek és a bűnbandáknak a határán elhelyezkedő alakulatok játszák (Creveld, 1991). Robert Kaplan[32] megközelítése ezt azzal egészíti ki, hogy a jövő háborúit a működésképtelen, illetve törékeny és bukott államok generálják jellemzően az erőforrások (víz, termőföld) szűkülése, az extrém időjárási és környezeti jelenségek, illetve a gyarmati idők öröksége és a biztonságérzet hiánya mentén (Kaplan, 1994). Ralph Peters szerint a jövő konfliktusaiban egy új harcoló osztály (new warrior class) is azonosítható, amely a lázadók, nemzetközi bűnözők, hadurak, terroristák, valamint a konfliktusok egyéb

[30] Dr. Frank G. Hoffman az amerikai tengerészgyalogság nyugalmazott alezredese, a jövő konfliktusainak egyik elismert kutatója, aki több think-tank számára végez stratégiai és globális folyamat elemzéseket 30 éves szakmai tapasztalattal. PhD fokozatát a King's College háborús tanulmányok szakirányán szerezte és részt vett az amerikai Nemzeti Védelmi Stratégia kidolgozásában a védelmi miniszter különleges tanácsadójaként 2017-ben.

[31] Martin Levi van Creveld izraeli hadtörténész és teoretikus, stratégiai gondolkodó és író. PhD fokozatát a London School of Economics történelem szakán szerezte, pályája során számos polgári és katonai felsőoktatási intézményben tartott előadásokat és tanított.

[32] Robert David Kaplan amerikai külügyi és politikai író. Munkáiban gyakran foglalkozik a kortárs világ civilizációs konfliktusaival, illetve a kulturális és történelmi feszültségek újbóli megjelenésével a hidegháború utáni időszakban.

haszonélvezőinek széles skáláját jelöli és akik „*nem tisztelik a hadviselés történelmileg kialakult szabályait*” (Szenes, 2017). Harcukat a városokban és az információs dzsungelben egyaránt vívják.

Ahogy Szenes Zoltán is leírja, a jövő fegyveres konfliktusainak katonai kihívásaiból *sokszínű hadviselési forgatókönyv konstruálható meg* (Szenes, 2017) és a korszerű háború Clausewitz által megfogalmazott „kaméleonja” megmarad. Ahogyan a múltban is, a háború mindig a stratégiai körülményekhez idomul és a jövőben államok közötti, állami szint alatti, valamint államhatárokon átnyúló hadviselési módokban, illetve ezeket kombinálva jelenik meg. „*Az új háborús érában a hagyományos és a nem hagyományos, a szimmetrikus és az aszimmetrikus műveletek egyszerre, egy időben lehetnek jelen, térben és időben összefonódhatnak egy hibrid háborúvá.*” (Szenes, 2017) Egy hibrid konfliktusban a katonai képességeket civil hatalmi eszközökkel együttesen alkalmazzák és bizonyos esetekben az irreguláris erők kiemelt szerephez jutnak, ami miatt jelentősen felértékelődik a különböző állami támogatók, szponzorok, illetve az irreguláris és aszimmetrikus hadviselés logisztikai biztosítóinak szerepe. A negyedik generációt követő hadviselés hálózatos és összhaderőnemi jellegét tovább erősíti az információs technológia fejlődése és kiterjedt alkalmazása, illetve a többdimenziós hatásalapú eljárások mellett a kontaktus nélküli és koncentrált csapások.

Az információs technológia területi határokat lazító hatásának egyik eredménye, hogy a kibertér globális jellege kialakulhatott és aminek következtében egyre nehezebb a határok fogalmával definiálni a nemzeti biztonságot. A kínai hadsereg két ezredese – Qiao Liang és Wang Xiangsui – által ismertetett „korlátlan hadviselés” korában nincs különbség abban, hogy mi harctér és mi nem. A hadviselés természeti dimenziói (szárazföldi, tengeri, légi, kozmikus) mellett a társadalmi dimenziók (katonai, politikai, gazdasági, kulturális és pszichológiai) is műveleti területekké váltak, amiket a kibertér kapcsol össze. Ezekben a terekben a hadviselés lehet katonai, kvázi katonai vagy nem katonai, miközben az erőszak alkalmazása és az erőszakmentesség is jelen lehet. A hadviselés ilyen mértékű kiterjesztése a professzionális katonai erők összecsapása mellett a reguláris erők és az átlagemberek és szakemberek által alkotott új erők közötti összecsapás lehetőségét is magába foglalja, ami a tradicionális és korlátlan hadviselés közötti lényegi különbséget adja (Qiao és Wang, 1999).

A hibrid és aszimmetrikus hadviseléssel, illetve a hadviselés új generációival és a jövő háborújával számos orosz katonai teoretikus és vezető is aktívan foglalkozik. Ezek közül Timothy Thomas[33] összegző munkája nyomán (Thomas, 2016) több katonai felsővezető megközelítéséből is az olvasható ki, hogy a háborúk természetének változása még inkább elmossa a háború és béke határát, miközben a nem katonai eszközök szerepe megnövekedik a dezinformáció, a megtévesztés, a hadicsel, a hírszerzés és az elhárítás terén. Az ellenfelek kommunikációjának, navigációjának, légvédelmének, nukleáris erőinek és felderítő rendszereinek megzavarása elektronikai és más aszimmetrikus módon a hibrid háborúban általános jelenség. Ezek a háborúk hadüzenet nélküliek és a lakosság ellenálló potenciáljának, a különleges műveleti erőknek, illetve a fedett katonai és információs hadviselésnek jut a főszerep, miközben politikai, gazdasági, információs és egyéb nem katonai eszközök komplex alkalmazása történik. Az űr és információs hadviselés felértékelődik, a direkt és indirekt műveletek átalakulnak. A gyakorlat azt mutatja, hogy egy ország fejlődése megzavarható, szuverenitása rombolható, a vezetők megváltoztathatók, ami annak a jele, hogy az információs hatások bizonyos esetekben felérnek a katonai erő alkalmazásával. Az aszimmetrikus műveletek kivitelezésének legfontosabb feltétele az ellenfél legsérülékenyebb és leggyengébb területeinek precíz meghatározása annak érdekében, hogy a saját erők és erőforrások minimális ráfordítással maximális hatást keltsenek.

A kortárs fegyveres konfliktusokkal összefüggésben említést kell tennünk a többdimenziós (multidomain) hadműveletekről. Ahogy Hegedűs és Hennel írja, „*a jövő hadszínterén többféle művelet folyik majd egyszerre, a hagyományosnak vett (légi, szárazföldi, tengeri) műveletek mellett az űrhadviselés, illetve az információs- és kiberműveletek is megjelennek.*" (Hegedűs és Hennel, 2020) A többdimenziós műveletek (Multi-Domain Operations – MDO) jellemzője, hogy dimenziókon átívelő integrált és egymással együttműködő rendszereket alkalmaznak, miközben párhuzamos, illetve egyidejű műveletek zajlanak a különböző dimenziókban. A dimenzió ebben a megközelítésben olyan közeget jelent, amelyben a katonai erő manőverezhet és hatást válhat ki. Ezek – a nem földrajzi kiber dimenzió kivételével – katonaföldrajzi, hadműveleti és haderőnemi fogalmakon alapuló műveletek szinergikus hatást gyakorolnak egymásra. Bizonyos szempontból a többdimenziós hadviselés az összfegyvernemi, illetve összehaderőnemi hadműveleteknek egy új

[33] Timothy L. Thomas az amerikai szárazföldi erők nyugállományú alezredese, a Szovjetunió és Oroszország szakértője, a Külföldi Katonai Tanulmányok Iroda (Foreign Military Studies Office) szenior elemzője.

szintje, ahol a korábbi koncepciókhoz képest jelentős különbség a jóval kisebb egységek, akár egy különleges műveleti raj többdimenziós alkalmazása. (Hegedűs és Hennel, 2020)

A hibrid, az aszimmetrikus, illetve más hadviselési formák meghatározása nem célja az értekezésnek és a kiberhadviselés definiálása sem cél. Annak érdekében, hogy a kiber különleges műveleti képességek elhelyezhetők legyenek a kiberhadviselés, illetve a kiberműveletek halmazában, munkadefinícióként a NATO kibertér műveletekről szóló összehaderőnemi doktrínájának (AJP-3.20) meghatározását alkalmazom. Azonban a hangsúly sokkal inkább azon van, hogy a legfontosabbnak ítélt jellemzők ismertetésével elhelyezzük a kiberhadviselést a jelenkor és a jövő fegyveres konfliktusaival összefüggésben. A jelen és a jövő fegyveres konfliktusaira jellemző fenyegetések és kihívások komplex természete arra enged következtetni, hogy a kinetikus hadviselés mellett meghatározó szerepe van már most is a kognitív hadviselésnek és a kiberhadviselésnek (Suckhov és Tack, 2019). Ezt támasztják alá a közelmúlt történései a posztszovjet térségben bekövetkezett színes forradalmaktól, a dél-oszétiai háborún, az Arab tavasz eseményein és a szíriai polgárháborún át, a Krím-félsziget és a kelet-ukrajnai területek annektálása is. Ebben az értelemben a legújabb háborúk a kibertérben végzett és kinetikus akciók kombinációja, aminek hátterét az ellenséges nemzet moráljának lerombolására irányuló elhúzódó kognitív felkészülés adja (Suckhov és Tack, 2019).

A katonai képességek elterjedése és fejlesztése a kibertérben nem fogja átalakítani a háború természetét. A kiberháborúk alapkoncepciója, hogy megcélozza az ellenfél kommunikációs infrastruktúráját és politikai, gazdasági alapjait, koránt sem nevezhető forradalminak. Ami az idők során megváltozott, az a kiberkörnyezet – az infrastruktúra, amely ma már támogatja a kommunikációt, a gazdasági együttműködést és a politikai retorika közvetítését. Bár a kiberkörnyezet olyan eszközökből áll, amelyek eltérnek a hagyományos háborúkra jellemző fizikai környezet eszközeitől és más erőforrás-konfigurációt és technikát igényelnek, ennek a környezetnek a stratégiai szabályai abban a tekintetben megegyeznek a kinetikus hadviseléssel, hogy a cél az ellenfél sebezhetőségének azonosítása és a megfelelő egyensúly megtalálása a védekező és támadó képességek között (Suckhov és Tack, 2019).

Összegezve, az alfejezetben leírtak alapján kirajzolódó jövőbeli konfliktusoknak szerves részét képezi már az előkészületek során az információs hadviselés és a kibertéren keresztül, illetve a kibertérben végrehajtott műveletek. Miközben annak valószínűsége alacsony marad, hogy egy

konfliktus kizárólag a kibertérben valósuljon meg, egyre gyakrabban fordulnak elő olyan hibrid megoldások, amely a szemben álló felek különböző érdekei mentén ötvözik a hagyományos katonai képességeket a nem reguláris, hírszerzési és civil képességekkel. Tekintettel arra, hogy korunk társadalmának egyre inkább integráns része a kibertér és az ott zajló folyamatok, a kiberműveleti képességek jelentősen felértékelődnek minden fél számára függetlenül attól, hogy állami vagy nem állami szereplőről van szó. A fentiekre tekintettel a modern konfliktusok megvívására alkalmas haderők és a teljes kapcsolódó védelmi szektor számára nélkülözhetetlenek azok a kiberműveleti képességekkel összefüggő kutatások, amelyek hozzájárulnak a fejlesztési irányok kijelöléséhez, legyen szó akár szervezetről, személyzetről vagy felszerelésről.

II.6 A vizsgálat szintje: nemzeti képességfejlesztés

A stratégiai dokumentumoknak a szövetségesek, partnerek és ellenfelek irányába történő kommunikáción túl szignifikáns szerepe van a kockázatértékelés eredményeként meghatározott védelmi igények, illetve a biztonságot garantálni képes megoldások kialakítása és fejlesztése terén. Ezeknek a jelentőségét az adja, hogy egyetlen nemzetállam sem rendelkezik végtelen erőforrásokkal a biztonság garantálása tekintetében, így kénytelen priorizálni a birtokában levő korlátozott forrásokat az allokáció és felhasználás vonatkozásában. A végrehajtói szinten, azaz a rendvédelem, honvédelem és nemzetbiztonság szintjén ezek a priorizált erőforrások – gyakran a nyilvánosság számára átláthatatlan transzformációs folyamat végén – képességekként jelennek meg. A rendvédelmi, honvédelmi és nemzetbiztonsági képességeket szinte kivétel nélkül a kockázatokkal és fenyegetésekkel arányosan alakítják ki, fejlesztik tovább, működtetik vagy építik le, ezért a képességek teljes élettartama alatt fontos szerepe marad annak, hogy milyen a megítélése egy adott kockázatnak vagy fenyegetésnek. A biztonság- és védelempolitikai kutatások, illetve szakmai dokumentumok által biztonság percepciónak nevezett jelenség tehát a nemzet biztonságát szavatolni hivatott képességek elemi összetevőjeként fogható fel, ami egyúttal kritikus fontosságú indikátorként is funkcionál a képességek bármely irányú alakításában. Az alfejezetben a biztonság percepció és a képességfejlesztés összefüggéseibe, illetve a képességfejlesztés bizonyos mozzanataiba történő rövid betekintéssel szűkítjük tovább a kutatás fókuszát. Nem cél a különböző kibertérre vonatkozó képességfejlesztési metódusok átfogó bemutatása és elemzése, csupán a vizsgálati szint ismertetéséhez szükséges mértékben és mélységben érintjük ezeket.

Példaként említve, hazánk Nemzeti Biztonsági Stratégiája több pontban is foglalkozik a kiberbiztonsági kihívásokkal és kockázatokkal, azonban a 159. pont két aspektusa is fontos a kiberképességek kialakítása kapcsán. *„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. 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. 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."* (NBS, 2020) Egyfelől az elsődleges feladatként meghatározott azonosítási és nyomon követési tevékenység nem más, mint az iparági szinten kiber fenyegetésekkel kapcsolatos hírszerzésként ismert képesség (Cyber Threat Intelligence – CTI) kialakítása, másfelől a kiberműveleti, azon belül is az offenzív képességeket kifejezetten a haderő vonatkozásában írja elő a stratégia, ami a kutatás hangsúlyának szempontjából is fontos. A dokumentum utolsó előtti pontja írja elő az egyes részterületekért felelős állami szervezetek számára, hogy az NBS-ben rögzített iránymutatásokkal összhangban alkossák meg, illetve vizsgálják felül a szakági szabályzókat (katonai, rendészeti, nemzetbiztonsági, kiberbiztonsági, terrorelhárítási stb.). Ezen a ponton érhető tetten a stratégiai szintű biztonsági kihívások transzformációja a végrehajtói szint, illetve védelmi szervezetek számára.

Ha azonban a képességfejlesztés értelmezését átfogóan szemléljük, többféle megközelítéssel találkozhatunk. A képességfejlesztés – a katonai célok elérésének aspektusára fókuszálva nem más, mint – a haderő struktúrájának és készültségének kombinációja, amit az egyes országok jól kivehető hangsúlyeltolódásokkal fogalmaznak meg, ahogy arra a Védelmi Elemzések Intézete (Institute for Defense Analyses – IDA)[34] 2019-es képesség alapú védelmi tervezésről szóló

[34] Az Institute for Defense Analyses egy amerikai nonprofit vállalat, amely három szövetségi finanszírozású kutató és fejlesztő központot felügyel, székhelye Alexandria, Virginia. Mindhárom központ az amerikai kormányzatot segíti

tanulmánya (Taliaferro és mtsai., 2019) is felhívja a figyelmet. Az Egyesült Királyság Védelmi Minisztériuma szerint tartós képesség a kívánt műveleti eredmény vagy hatás létrehozására, amely arányos a fenyegetéshez, a fizikai környezethez és a koalíciós partnerek hozzájárulásához (Yue és Henshaw, 2009). Az Amerikai Egyesült Államok Védelmi Minisztériumának katonai szótára alapján annak képessége, hogy meghatározott feltételek és teljesítményszint mellett elvégezzenek egy feladatot vagy végrehajtsanak egy műveletet (US DOD, é. n.). Kanada Védelmi Minisztériuma meghatározásában egy adott képesség, amely hozzájárul a kívánt hatás eléréséhez egy adott környezetben, meghatározott időn belül, és a hatás meghatározott ideig történő fenntartásához (Rempel, 2010). Az Ausztrália Védelmi Minisztériuma által kiadott Védelmi Képességfejlesztési Kézikönyv (DOD Australia, 2014) megfogalmazásában a műveleti hatás eléréséhez szükséges kapacitás vagy képesség. A műveleti hatás meghatározható vagy leírható a hatás természetével, valamint azzal, hogy hogyan, mikor, hol és mennyi ideig valósul meg.

A katonai képességfejlesztés tekintetében bár nincs univerzálisan elfogadott definíció, a NATO által alkalmazott terminológia stabil kiindulópontként szolgál az értelmezési keretek kialakításához. A hivatalos NATO terminológiai adatbázis[35] két releváns bejegyzést is tartalmaz a képesség kifejezés kapcsán. A katonai erő mérhetőségére és minőségére koncentráló rövidebb definíció szerint a képesség nem más, mint a katonai potenciál kifejezése kvantitatív és kvalitatív értelemben. A NATO másik meghatározása alapján a képesség különböző aspektusok integrált alkalmazásán keresztüli hatás keltés. Ezek az aspektusok kategóriákba sorolhatók: doktrína, szervezet, kiképzés, anyagok, vezetésfejlesztés, személyzet, létesítmények és interoperabilitás. A felsorolt aspektusok láncolata, illetve hálózata képezi a különféle katonai képességek elemi struktúráját. Az előző bekezdésben említett IDA tanulmány szerzői komponensként azonosítják a NATO által aspektusnak nevezett kategóriákat és egyfajta szintézisként saját definíciót is megalkottak, amely szerint a képesség egy feladat elvégzését vagy hatás kiváltását teszi lehetővé meghatározott teljesítményszabványok és környezeti feltételek között. A NATO-ban 2002-es megalapítása óta a Szövetséges Transzformációs Parancsnokság (Allied Command Transformation – ACT) feladata a képességek fejlesztése, így vezető szerepet betöltve ösztönzi, elősegíti és

nemzetbiztonsági kérdésekben, kiemeleten azokon a területeken, ahol tudományos és technikai szakértelemre van szükség.

[35] Lásd bővebben: https://nso.nato.int/natoterm/content/nato/pages/home.html?lg=en (Elérés: 2022. március 11.)

támogatja a Szövetség képességeinek folyamatos fejlesztését a Szövetség katonai jelentőségének és hatékonyságának fenntartása és fokozása érdekében.[36]

Az euro-atlanti szövetségi beágyazottság alapján a NATO és az EU tagállamai számára a két integrációs szervezet képességfejlesztésre vonatkozó dokumentumai iránymutatásként szolgálnak és bizonyos esetekben kötelező érvénnyel bírnak a védelmi képességek fejlesztésére, valamint a kapcsolódó együttműködésekre vonatkozóan. Bár prioritási és más szempontú eltérések érzékelhetők, amiket a kiberbiztonsági stratégiák áttekintésekor egyértelműen láthatunk majd, a szövetségi rendszerek biztonság percepciója a nemzetállamok szintjén is érvényesül. A tagállamok saját jól felfogott érdeke, hogy a korlátozott erőforrásaikat a lehető leghatékonyabban használják fel biztonságuk és védelmük megteremtésekor. Ehhez elengedhetetlen a szövetségi képességfejlesztési irányokhoz történő igazodás legyen szó könnyű- vagy nehézfegyverzetről, légtér- és rakétavédelemről, nehéz légiszállításról, stratégiai kommunikációról, vagy épp kiberbiztonságról és -védelemről. A kibervédelmi képességek tekintetében az aktuális szövetségi narratívák a korábbi egyértelműen defenzív irányhoz képest jelentős elmozdulást mutatnak. Több dokumentum implicit és/vagy explicit módon is foglalkozik az aktív, reaktív, illetve offenzív kiberképességekkel, miközben a védelmi kifejezés alkalmazása továbbra is megmarad. A hosszú-, közepes- és rövidtávú védelmi tervezési folyamatok – jellemzően a nemzetállami specifikumokat figyelembe véve – követik a képességfejlesztésre vonatkozó szövetségi irányelveket. Ezek alapján a nemzeti szintű képességfejlesztési tervekben, a szövetségi folyamatok determinisztikus hatásának eredményeként hasonló hangsúlyeltolódás következik be, vagyis a kiberképességek teljes spektruma megjelenik a nemzeti szintű képességfejlesztés során.

Összegezve az alfejezetben leírtakat, az látható, hogy az államok jellemzően a felső szintű nemzeti biztonsági és katonai stratégiákból kirajzolódó biztonságpercepció alapján igyekeznek allokálni és felhasználni a rendelkezésükre álló erőforrásokat. Bár az euro-atlanti régióban az erőforrások felhasználásában és a képességfejlesztés irányainak meghatározásában szerepe van a szövetségi rendszereknek is, a kibertérből érkező fenyegetések bővülése már önmagában is arra ösztönzi nemzeti szinten a védelmi szektort, hogy nagyobb hangsúlyt fektessen a kibervédelemhez kapcsolódó képességfejlesztésre. A folyamat egyes aspektusai, illetve komponensei tekintetében,

[36] Lásd bővebben: NATO Allied Command Transformation - Brief https://www.europarl.europa.eu/meetdocs/2014_2019/documents/sede/dv/sede031214act_/sede031214act_en.pdf (Elérés: 2022. március 11.)

mint például a doktrínák, az állomány, a kiképzés vagy az infrastruktúra jelentős eltérések lehetnek, ugyanakkor a kibervédelmi, illetve kiberműveleti képességek egyre jelentősebb mértékben válnak integráns részévé a védelmi szektor képességfejlesztési törekvéseinek, ami az értekezés vizsgálati szintjének alapját is adja.

II.7 Nemzeti érdek, nemzeti-érdekérvényesítés és a kiberműveleti képességek

A nemzeti szintű kiberműveleti képességek, illetve azok teljes spektrumának elemzésekor fontos kitérni a nemzeti érdekérvényesítésre és a kiberképességek által betöltött szerepre a nemzeti érdekérvényesítés eszköztárában. Az alfejezet kitér a nemzeti érdekekre és azok érvényesítésének lehetőségeivel összefüggésben a különleges műveleti képességekre, aminek célja a kutatás értelmezési kereteinek pontosítása és további szűkítése. A nemzeti érdek és nemzeti-érdekérvényesítés meghatározása és alapvető fogalmai kapcsán nagymértékben támaszkodom Gazdag Ferenc 2007-es nemzeti érdekérvényesítés témában született tanulmányára, illetve Szörényi András 2009-es a nemzetközi- és biztonsági tanulmányok két alapvető iskolájának, az érdekek érvényesítésére vonatkozó tételeit bemutató elemzésére.

Anélkül, hogy elméleti részletekbe bonyolódnánk, a nemzetközi tanulmányokban a realista megközelítés lényege, hogy a nemzetközi rendszert egy a hatalom megszerzésére, megtartására vagy növelésére irányuló anarchikus természetű rendszerként értelmezi. A realista irányzat másik központi témája az államok túlélésért folytatott küzdelme, valamint a túlélés katonai-biztonsági szempontú prioritása, aminek alapja az államok biztonsági dilemmája és ami abból indul ki, hogy a 20. és 21. században az államok már csak egymás kárára képesek terjeszkedni. Ennek nyomán egyfelől „*Az érdekek – bár általánosan érvényesek és minden esetben a hatalomra irányulnak – nem állandóak és változatlanok, hanem az adott helyzethez igazodva folyamatosan alakulnak, a hatalom jellegének időbeli és térbeli változásával, fejlődésével együtt változhatnak.*" (Szörényi, 2014) Másfelől az érdekek meghatározásakor a nemzetközi aktorok ugyan nem kizárólagosan veszik figyelembe a politikai, gazdasági, jogi és egyéb szempontokat, de minden terület és szereplő a saját szemszögéből definiálja érdekeit és ezeket elsőbbséghez juttatva hozza meg a szükséges döntéseket. A realista iskola alapjait követő Gilpin[37] féle politikai gazdaságtan irányzata ezt azzal – a kutatás szempontjából fontos megközelítéssel – egészíti ki, hogy az egyes államok politikáit és

[37] Robert Gilpin 1930. július 2-án született amerikai tudós, szakterülete a politika és a nemzetközi kapcsolatok. A Princeton Egyetem professzora, a nemzetközi kapcsolatok és a nemzetközi politikai gazdaság teoretikusa.

érdekeit, valamint a közöttük lévő politikai kapcsolatokat a gazdasági és technológiai erők is alakítják. (Gilpin, 2004)

A nemzetközi tanulmányok másik meghatározó irányzata a liberális iskola, amely elutasítja a hatalom és a hatalmi egyensúly fogalmán keresztüli megközelítést és az államközpontú megközelítési keretet az állam alatti szintre cseréli. Andrew Moravcsik [38] olvasatában egy racionálisan cselekvő liberális állam a saját érdekei alapján mérlegel, de azt az együttműködés várható hasznának és költségeinek szempontjaira tekintettel teszi. Az állami érdekeket pedig a belpolitika, illetve annak különböző szereplői alakítják ki. Az így létrejövő nemzeti értékrendet és érdekrendszert azután nemzetközi szinten és szupranacionális intézményi szinten is igyekeznek érvényre juttatni. Utóbbira jó példa az euro-atlanti integráció, ahol az államok azonos, vagy hasonló érdekek mentén alakítanak ki együttműködést, de az integrációt megtestesítő szervezetek nem létezhetnek az államoktól függetlenül.

A nemzetközi tanulmányok nemzeti és nemzetközi érdekérvényesítéssel kapcsolatos tézisei nyomán érdemes magát az érdek fogalmát közelebbről megvizsgálni, ami elsőre egyértelműnek tűnhet, azonban nem létezik egyszerű, általánosan elfogadott és univerzális használatú definíció. „*Legáltalánosabban értelmezve az érdek gondolat – esetleg érzelem – és cselekedet formájában megnyilvánuló indíték olyan magatartásra, állásfoglalásra, cselekedetre, amelynek hátterében különbözőképpen minősíthető szükségletek állnak. Az érdek társadalmi, nemzeti, nemzetközi szinten politikai, gazdasági, ideológiai igények megfogalmazásához és keresztülviteléhez vezet, vagy ilyesmit céloz. Azaz társadalmi és politikai értelemben: hajtóerő. Hierarchikus rendeződésű, függőségi hálózatot képez. Érvényesítésének sajátos mechanizmusai vannak, amelyek révén a kedvező lehetőségek hasznosíthatók, az akadályok leküzdhetők, megkerülhetők, de legalábbis számításba vehetők. Az érdekellentétek érdekütközéshez, érdekkonfilktushoz vezetnek, az érdekek egyeztetésének eredménye a megegyezés, a konszenzus, az egyetértés.*" (Gazdag, 2007) Gazdag tanulmánya folytatásában arról értekezik, hogy a szervezett politikai közösségek olyan mechanizmusokat alakítanak ki, amelyek a belső érdekek felszínre juttatásában és különböző érdekcsoportok akaratérvényesítésében fontos szerepet töltenek be. Ezek a mechanizmusok a társadalmi törekvéseket egyfajta érdekaggregációs folyamat eredményeként döntési alternatívákká

[38] Andrew Maitland Moravcsik 1957-ben született akadémikus, a politikatudomány és a nemzetközi kapcsolatok professzora a Princeton Egyetemen. Kutatásai középpontjában az európai integráció, a nemzetközi szervezetek, az emberi jogok állnak.

transzformálják, „*amelyek közül mindig a döntési helyzetben lévő politikai elitcsoport választja ki, hogy melyek mögé sorakoztatja fel az állam erőforrásait.*" (Gazdag, 2007) Ebből következik, hogy a nemzeti érdek fogalma egy adott időpontban jellemzően azokat a törekvéseket rejti, amelyek az aktuálisan domináns szerepet betöltő elitcsoportokhoz köthetők.

Történelmi, illetve nagyhatalmi kitekintésben „*az erők megoszlásának konfigurációja határozza meg: ki irányítja valójában a nemzetközi rendszert, és hogy ez a rendszer leginkább kinek az érdekeit szolgálja. Következésképpen a kisebb képességekkel rendelkező államok számára a mozgásteret az határolja be, milyen hatékonysággal képesek érdekeiket beilleszteni egy kellő befolyású államcsoport érdekei közé.*" (Gazdag, 2007) A nemzetközi folyamatokat alakító nemzeti, illetve állami külpolitikák tehát minden esetben érdekpolitikának tekinthetők, amelyeket a különböző nemzeti és állami érdekek töltenek meg tartalommal.

A fent leírtak alapján megállapítható, hogy a kormánypolitika olyan nemzeti és nemzetközi feltételek kialakítására törekszik, amelyek képesek elősegíteni a nemzeti, illetve állami értékek védelmét és a nemzeti érdekek érvényesítését. A gyakorlatban az ilyen politika sikerességéhez szükséges, hogy az aktuális állami vezetés reális képpel rendelkezzen a nemzetközi környezetről és az ország nemzetközi rendszerben betöltött helyéről és szerepéről. Ezen felül szükség van arra, hogy reálisan határozzák meg az ország céljait, szövetségesi rendszerét, a potenciális ellenségeket, valamint pontosan számba vegyék az ország biztonságát befolyásoló vélt vagy valós fenyegetéseket és azokat a képességeket, amelyek a fenyegetések elhárításához, a kihívások kezeléséhez szükségesek. (Tálas, 2014) A mindezeket tételesen és deklaratív módon tartalmazó hivatalos dokumentum egy adott ország nemzeti biztonsági stratégiája (Csiki, 2008).

Ugyanakkor a stratégiákban rögzített érdekeknek, illetve a bilaterális és multilaterális úton történő nemzeti érdekérvényesítésnek és képességfejlesztésnek létezik egy másik terepe is: ezek azok a tevékenységek, amelyeket a különleges műveleti képességek gerincét adó honvédelmi, rendvédelmi, illetve nemzetbiztonsági egységek végeznek. A honvédelmi szektorban egyfelől a különleges műveleti erő (Special Operations Force – SOF) által az úgynevezett nem háborús katonai műveletek (Military Operations Other Than War – MOOTW) [39] során játszott

[39] MOOTW: jellemzően azok a békekinyszerítő, terror és felkelés ellenni, humanitárius vagy éppen navigációs szabadságot biztosító műveletek, amelyek fókuszában a háború elrettentése, a konfliktus megoldása, a béke promotálása és a civil hatóságok támogatása áll. Bővebben: (US Joint Staff 1995)

szerepvállalás a mérvadó. Másfelől a SOF képességek szerepe növekszik egy olyan időszakban, amikor a fenyegetések és a fenyegetésekre adott válaszok a konfliktusok kontinuumának egy olyan szegmensében zajlanak, amelyet „kétértelmű hadviselésnek" (ambiguous warfare), „szürke zónának" (grey zone) és „háború nélküli versengésnek" (competition short of war) is neveznek (Broyles és Blankenship, 2017). A „szürke zónát" intenzív politikai, gazdasági, információs és katonai versengés jellemzi, amely hevesebb természetű, mint a normál állandósult diplomácia, de a hagyományos háborúból hiányzik. A diplomácia és a nyílt hadviselés közötti térben játszódó politikai hadviselés az a „szürke zóna", ahol a hagyományos államvezetés nem megfelelő vagy nem hatékony és a nagyszabású hagyományos haderő alkalmazása nem lehetséges, vagy különféle okok miatt nem célszerű. George Kennan[40] jellemzése szerint a szürke zónában „egy nemzet parancsára minden eszközt alkalmaznak, a háború kivételével nemzeti céljainak eléréséhez" (Kennan, 1948). A különleges műveleti erőket arra optimalizálták, hogy kiemelkedő katonai hozzájárulást nyújtsanak a nemzeti politikai hadviselési képességhez, a tevékenységük kis nyoma (small-footprint) és alacsony láthatósága (low-visibility), illetve a politikailag érzékeny műveletekben való eredendő jártasságuk miatt. A különleges műveleti erő stratégiai lehetőségeket kínál a nemzeti döntéshozók számára az ország nemzeti érdekeinek védelmére és előmozdítására anélkül, hogy jelentős harci erőket kötne le költséges, hosszú távú készenléti műveletekre. (Votel és mtsai., 2016) Az irreguláris és aszimmetrikus fenyegetések mellett ez, vagyis a költségvetési nyomás, ami tovább növeli a SOF képességek iránti igényeket (Robinson, 2013), mivel azok relatív olcsók a hagyományos erőkhöz képest.

A rendvédelmi szektorban szintén vannak különleges szolgálati területek, mint például a közismert nevén kommandónak hívott jellemzően terrorelhárítási és egyéb speciális feladatokra kiképzett taktikai egységek, vagy a nemzetközi békefenntartó missziókban szerepet vállaló rendőri alakulatok. Utóbbiak alapvető szerepet játszanak egy válságövezet békéjének és biztonságának helyreállításában, illetve különleges politikai missziókban, ezzel hozzájárulva a küldő állam érdekei szerinti politikai kontextus formálásához, a bizalomépítéshez és a nemzetközi bűnözés csökkentéséhez (UN, 2016). A taktikai egységek szerepe inkább az állam belső stabilitásához, társadalmi rendjéhez és az állampolgárok rendészeti biztonságához fűződő létfontosságú érdekei

[40] George Frost Kennan 1904. február 16-án született amerikai diplomata és történész. Főleg a Szovjetunió és az Egyesült Államok kapcsolatával foglalkozott, nevéhez fűződik a Truman doktrína alapjainak, illetve a "feltartóztatás" politikájának kidolgozása a hidegháború idején.

mentén azonosíthatók az olyan képességekkel összefüggésben, mint a túszmentés, a terrorelhárítás és más magas kockázatú biztonsági műveletek és speciális tevékenységek (pl.: mesterlövész), amik túlmutatnak a hagyományos rendőri képességeken (NTOA, 2018).

Az eredetileg gyakran speciális rendőri alakulatként létrehozott nemzetbiztonsági szervezeteknek már az elnevezése jelzi, hogy az egyik legfontosabb államérdekhez, a nemzet külső és belső biztonságához köthető a tevékenységük. Az állam függetlenségének és törvényes rendjének védelme, nemzetbiztonsági érdekeinek érvényesítése áll a feladatrendszerük középpontjában. Ennek keretében fellépnek a nemzet érdekeinek rovására menő kémkedéssel és szabotázs akciókkal szemben, elősegítik a nemzeti érdekek külföldi érvényesítését, miközben óvnak a külföldi befolyásolási tevékenységektől. (Vitkauskas, 1999) A felderítő, információ gyűjtő, átvilágító, rejtjelező, illetve elemző és értékelő tevékenységeket (Nb. tv., 1995) a hagyományos rendvédelmi és honvédelmi eszközrendszertől eltérő, speciális eszközökkel és módszerekkel szinte minden esetben fedett körülmények között végzik.

Ezekhez hasonló, az állam érdekeinek érvényesítésében lényeges szerepe a kiberműveleteknek is van, ahogyan azt történelmi példák is bizonyítják. A korábban már szóba került Stuxnet pusztítása egyértelműen a nyugati érdekeket szolgálta az iráni atomprogram befolyásolására tett erőfeszítések sorában. A Stuxnet drasztikus eredményeihez képest inkább csak szimbolikus jelentőségű, de az államérdek kifejeződése jól tetten érhető az Észtország elleni 2007-es kibertámadásban[41] is, amely – bár nem bizonyított – egyértelműen az orosz érdekeket szolgálta. És afelől is kevés kétség maradt, hogy a Sony Pictures Entertainment elleni támadás[42] Észak-Koreának állt érdekében. Miközben a példák sora hosszan folytatható lenne, a nemzeti kiberbiztonsági stratégiák is egyre határozottabban említik a környezet értékelését tartalmazó részekben a „nemzeti érdekeket veszélyeztető" kibertéri tevékenységeket, így a kiberműveleti képességek a nemzeti érdekérvényesítés eszköztárának elemeiként is felfoghatók, amit a következő fejezetben feldolgozott stratégiai dokumentumok támasztanak alá.

[41] Egy szovjet emlékmű eltávolítását követően 2007 tavaszán több elemből álló politikailag motivált kibertámadás sorozat érte a digitálisan már akkor is élvonalbeli Észtország kereskedelmi és kormányzati rendszereit, amiért egyetlen csoport sem vállalta a felelősséget. Bővebben: https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf

[42] A 2014 novemberében történt támadásért december elején a Szövetségi Nyomozó Iroda (FBI) nyíltan Észak-Koreát tette felelőssé, így ez lett a történelem első olyan amerikai vállalat elleni destruktív kibertámadása, amivel az Egyesült Államok egy külföldi kormányt vádolt meg. Bővebben: https://www.secureops.com/wp-content/uploads/2021/06/Sony-Breach-Analysis-v4.pdf

Az alfejezetben leírtakat összegezve elmondható, hogy az érdek, illetve érdekérvényesítés elméleti alapjaiból levezethető állami érdekérvényesítésnek számtalan formája létezik ma a világban. Az állami értékek védelmét és érdekek érvényesítését jellemzően a nemzetközi környezet, illetve a nemzetközi rendszerben betöltött szerep determinálja. Ugyanakkor az érdekérvényesítéssel kapcsolatban létezik egy szegmens, amit a katonai terminológia nem háborús műveletnek nevez és aminek részét képezik olyan tevékenységek, amelyek leginkább a különleges műveleti erők profiljához illeszkednek. Ezek a jellemzően nagy politikai kockázattal járó műveletek alkalmasak az irreguláris és aszimmetrikus fenyegetésekkel szembeni fellépésre és tetten érhetők a rendvédelmi, illetve nemzetbiztonsági területeken is. Továbbá az állami érdekek érvényesítésével és értékek védelmével számos olyan eset kapcsolatba hozható, amelyek részben vagy egészben a kibertérben, illetve azon keresztül valósultak meg. Ezek alapján az elméleti keretek további szűkítéseként az értekezés kiber különleges műveleti képességekre vonatkozó részeiben főként azokra a tevékenységekre fókuszálok, amelyek különleges műveleti megközelítést igényelnek, egyúttal a kiváltott hatások miatt a nemzeti érdekérvényesítés elemei közé beilleszthetők.

III. A kiberműveleti képességek

Bevezetés

A kibertérben folytatott tevékenységeket többféle módon is csoportosíthatjuk. De mindenekelőtt azt érdemes tisztán látni, hogy mit értünk kiberművelet alatt. Ehhez a legkézenfekvőbb forrást a különböző szabványügyi és szakmai szervezeti meghatározások szolgáltatják, mivel a vizsgált stratégiai dokumentumok és doktrínák alapján – bár a nemzetközi és szakmai elvárások megkívánnák – azok nem tartalmaznak értelmező rendelkezéseket, vagy ha mégis, azokban nem szerepelnek a kiberműveletek. Az amerikai Nemzeti Szabványügyi és Technológiai Intézet (US National Institute of Standards and Technology – NIST) a kibertér műveletekről azt írja (NIST, 2015), hogy a kibertér képességek alkalmazása azzal az elsődleges szándékkal, hogy a kibertérben vagy azon keresztül érjék el a célokat. Az amerikai védelmi minisztérium kiberműveleti lexikonja alapján a kibertér műveletekre két meghatározást is alkalmaznak (DOD US, 2009). Míg az egyik az előbbi definíciót azzal egészíti ki, hogy az ilyen műveletek számítógép hálózati műveleteket és

tevékenységeket foglalnak magukba a globális információs rendszer működése és védelme érdekében, addig a másik meghatározás szerint a kiberművelet az a tevékenység, ami a kibertérben vagy azon keresztül a védelmi minisztérium katonai, hírszerző, vagy hagyományos műveleteit támogatja. Az amerikai kongresszus számára főként döntéselőkészítő és háttértanulmányokat készítő szervezet (Congressional Research Service – CRS) egyik témába vágó dokumentumában (Theohary, 2021) a kibertér műveleteket szintén a védelmi minisztérium kibertéren keresztül végzett katonai, hírszerző és normál tevékenységhez sorolható műveletei alkotják. A katonai kibertér műveletek kibertéri képességeket alkalmaznak olyan hatások elérésére, amelyek támogatják a fizikai és kibertéri műveleteket. A kibertér műveletek eltérnek az információs műveletektől, mivel utóbbiak csak közegként használják a kiberteret és a céljuk, hogy a katonai műveletek során befolyásolják az ellenfél döntéshozatalát, miközben megvédik a saját folyamatokat. Az Ausztrál Kiberbiztonsági Központ (Australian Cyber Security Centre – ACSC) (ACSC, é. n.) szerint a kiberműveletek offenzív és defenzív tevékenységek arra tervezve, hogy a kibertérben vagy azon keresztül fejtsenek ki hatásokat. Az eredetileg a hidegháborús enyhülési folyamatban a kölcsönös megértést elősegíteni hivatott svájci Kelet Nyugat Intézet (East West Institute – EWI) által kiadott kritikus terminológiai alapokkal foglalkozó dokumentum (Godwin III és mtsai., 2014) a kiberműveletet az alábbiak szerint határozza meg: a kibertérben folytatott szervezett tevékenységek, információ gyűjtése, előkészítése, terjesztése, korlátozása vagy feldolgozása egy cél elérése érdekében. A meghatározások alapján a közös elemekre tekintettel jól látszik, hogy olyan tevékenységről van szó, amely a kibertérben vagy azon keresztül éri el célját. Azonban a kiberműveletek vizsgálhatók a végrehajtók kiléte szempontjából, így lehetnek állami és nem állami hátterűek, elemezhetők az elérni kívánt célkitűzés tekintetében, ami lehet taktikai vagy stratégiai, de kategorizálhatók a motiváció alapján is, ami kiterjedhet információk megszerzésére, manipulálására vagy törlésére. A kutatás szempontjából azonban a kiberműveletek jellege, illetve a küldetés alapja a leginkább meghatározó, ami lehet defenzív, azaz védelmi és offenzív, azaz támadó. Mielőtt rátérnénk a kiberműveletek küldetés alapú elemzésére, áttekintjük a kiber műveleti képességek megjelenését a kiberbiztonsági stratégiai dokumentumokban. Ehhez a NATO korábban már hivatkozott kiberműveleti doktrínájának meghatározását veszem alapul, ami szerint a kibertér műveletek a kibertérben vagy azon keresztül folytatott akciók a baráti szabad cselekvés megőrzésére a kibertérben, illetve a parancsnoki szándéknak megfelelő hatások kiváltására (NATO, 2020a). A doktrína meghatározása kellően átfogó alapot nyújt a stratégiai szintű

vizsgálathoz, ugyanakkor különbséget tesz a defenzív és offenzív kiberműveletek között. Míg előbbi a kibertérben történő szabad cselekvés megőrzésére fekteti a hangsúlyt, utóbbi az erőkivetítésre és a katonai célok elérését szolgáló hatások kiváltására. A vizsgálatra azért van szükség, hogy képet alkothassunk az egyes államok nyíltan felvállalt elképzeléseiről a kiberműveleti képességek kialakításával, fenntartásával és alkalmazásával kapcsolatban.

III.1 Stratégiai kitekintés

Ebben az alfejezetben arra a kérdésre keresem a választ, hogy különböző államok miként tekintenek a más államok által birtokolt, illetve a saját maguk által fejlesztett kiberműveleti képességekre. A vizsgálat fókuszában a kiberműveletek, illetve kiberműveleti képességek explicit és implicit módon való megjelenése, valamint a stratégiák kiberműveletekhez kapcsolódó részeinek tömör szakmai áttekintése áll, ezért a stratégiák további elemeit nem érintem. Amint az már korábban szóba került a stratégiák azok a legfelsőbb szintű dokumentumok, amik nyíltan meghatározzák más államok és a nemzetközi közösség számára egy adott államnak a biztonságról, a gazdaságról és egyéb területekről alkotott elképzeléseit, továbbá a biztonságpolitikai elemzések egyik alapvető forrásaként szolgálnak. A vizsgált stratégiák kiválasztásánál elsődleges szempont volt a regionális és kisállami megközelítés, aminek elengedhetetlen része a nemzetközi és nagyhatalmi kontextus értelmezése. Így a nemzetközileg feldolgozható dokumentumokkal rendelkező szomszédos országok (Ausztria, Szlovénia, Szlovákia, Ukrajna, Horvátország) mellett a kiberbiztonsági érettség magas szintje, illetve az igazoltan fejlett kiberbiztonsági képességek megléte miatt további négy állam (Svájc, Hollandia, Észtország, Izrael) került kiválasztásra. A nagyhatalmi kontextus vizsgálatában a kiberműveleti képességek terén számottevő erőforrásokkal rendelkező Oroszország, Egyesült Államok és Kína stratégiai megközelítését elemzem. A nemzetközi szervezeteken és szövetségi rendszereken keresztül történő érdekérvényesítés gyakran alkalmazott megoldás a kisállamok részéről, ugyanakkor a szövetségi rendszerek szintjén a kiberműveleti képességek stratégiai elemzése olyan komplexitást mutat, amely az értekezés keretein jelentős mértékben túlmutat. Ennek következtében, illetve a nemzeti képességfejlesztési fókusz megtartása miatt a nemzetközi szervezeteket és szövetségi rendszereket a stratégiai

kitekintés nem részletezi és az értekezésben csak a legszükségesebb mértékben kerülnek említésre (pl. definíciók és meghatározások).

III.1.1 Környező országok kiberképességei

Ausztria

A 2013-ban kiadott osztrák kiberbiztonsági stratégiát tartalmazó dokumentum (BMI, 2013) életciklusa végén jár, ezért nem sok értelme lenne a közvetlen összevetésnek olyan dokumentumokkal, amik 2020 után jelentek meg. A köztes időszakban annyi változás történt a kiberbiztonság terén és a kibertérből érkező kihívások is olyan drasztikus mértékben alakultak át, hogy indokolt lenne új stratégiai dokumentum készítése Ausztria számára. A hatályos osztrák stratégia kilenc területre bontja szét azokat a stratégiai célokat, amit a dokumentum nyomán létrehozandó keretrendszerben az ország el kíván érni. Ezek között szerepel a biztonságos, ellenálló és megbízható kibertér garantálása, amit a kompetens szövetségi minisztériumok hatáskörébe utalnak. Szintén az illetékes hatóságok feladata a kiberbiztonság jogi összetevőivel kapcsolatos intézkedések megvalósítása a nem kormányzati szereplőkkel együttműködésben. Ausztria fontosnak tartja a tudatossággal kapcsolatos intézkedéseket, a kiberbiztonság kultúrájának megteremtését és élen kíván járni a digitális társadalom biztonságát szavatoló intézkedések implementációjában, amihez aktív szerepet vállal a nemzetközi együttműködésben és az e-kormányzás biztonságának erősítésében. Az osztrák vállalkozások és a lakosság tekintetében egyaránt az egyéni felelősséget emeli ki a stratégia. Azt, hogy a stratégiai célokat miként kívánja elérni az ország hét akciópontban foglalták össze, amelyek konkrét intézkedéseket is tartalmaznak. A kiberbiztonsági struktúrák és folyamatok tekintetében a politikai-stratégiai szinten Ausztria létrehozott egy Kiberbiztonsági Kormányzó Csoportot (Cyber Security Steering Group – CSSG), míg a műveleti és operatív szinten egy koordináló elem megvalósításával növelik a hatékonyságot. Az osztrák belügyminisztérium alá rendelt Operatív Koordinációs Struktúra (Operational Coordination Structure – OCS) az állam és a magán szektor együttműködésén (Public Private Partnership – PPP) alapszik. A stratégia előírja külön kiber válsághelyzet kezelési (Cyber Crisis Management – CCM) elem létrehozását, melynek képességeit kiberbiztonsági gyakorlatokkal kell tesztelni. A meglévő operatív szintű kiberbiztonsági struktúrák kapcsán a kormányzati eseménykezelő központot (Computer Emergency Response Team – CERT), a kiberbűnözési kompetencia központot (Cyber Crime Competence Center – C4) és az osztrák eseménykezelő

központok szövetségét (CERT Association) emeli ki, illetve szab feladatot a stratégia. A kiber kormányzás terén megfogalmazott intézkedések között az operatív szintű, illetve kifejezetten műveleti kiberképességek szempontjából nem tartalmaz lényeges elemet a stratégia és ugyanez elmondható a kormányzati, a gazdasági és a társadalmi szereplők közötti együttműködés kapcsán is. A negyedik akciópont a létfontosságú infrastruktúrák védelmével foglalkozik és alapvetően a válság kommunikációra, az átfogó biztonsági architektúra megteremtésére, valamint a kiberbiztonsági incidensek bejelentésére fókuszál. Az ötödik akciópont a tudatosság növelése és a kiberbiztonsági képzések kapcsán az ezen a téren már működő – illetve elindítandó –, a digitális kompetenciát erősítő kezdeményezésekre és programokra koncentrál, míg a hatodik pont a kutatás fejlesztés feladatait tekinti át. Az utolsó akciópont a nemzetközi együttműködés területén a legfontosabb partnerségi irányokat jelöli ki, illetve azokat a területeket amire az együttműködésnek koncentrálnia kell. Az osztrák stratégiában explicit módon nem jelennek meg kiberműveleti képességek, sem defenzív, sem offenzív aspektusban. Ugyanakkor implicit módon a stratégia a válságkezelés kapcsán utalást tesz arra, hogy a Szövetségi Védelmi Minisztérium (Federal Ministry of Defense – FMoD) vezető szereppel rendelkezik az ország szuverenitásának védelmében, illetve a kibervédelem meghatározásánál a haderő fizikai képességeinek támogatása is említésre kerül. Ennél direktebb módon azonban az osztrák kiberbiztonsági stratégia nem foglalkozik kiberműveleti képességek kialakításával katonai, rendvédelmi vagy nemzetbiztonsági téren.

Szlovénia

A Szlovénia kiberbiztonsági stratégiáját tartalmazó dokumentum (Digital Slovenia, 2016) 2016-ban jelent meg, így frissnek ez sem nevezhető, ugyanakkor a szlovén megközelítés átfogó jellegét jól mutatja, hogy a dokumentum elkészítésében nem kevesebb mint 16 szervezet vett részt. A kibertérből érkező kockázatok számbavételét itt a stratégia implementálásának területei, nevezetesen a megelőzés, a válaszadás és a tudatosság növelése követi. Ezekhez kapcsolódóan a dokumentum készítői nyolc stratégiai célkitűzést határoztak meg. Az első célkitűzés alapvetően a kormányzati szinttel foglalkozik, illetve a kibertér biztonságát szavatolni hivatott összkormányzati rendszerrel és erőfeszítésekkel, amelyeknek szerves része a szlovén kormányzati eseménykezelő központ (SIGOV-CERT). A második és harmadik pont az egyének, illetve a gazdasági szereplők kiberbiztonsága kapcsán elsősorban a tudatosság növelése és az új technológiák bevezetésének

elősegítése terén fogalmaz meg elvárásokat. A dokumentum negyedik pontja a létfontosságú infrastruktúrák üzemeltetésével foglalkozik és előírja a rendszeres felülvizsgálatot a támogató informatikai rendszerek tekintetében, valamint a kockázatok megfelelő szintű csökkentését. Kifejezetten a társadalom biztonságérzetével és a kiberbűnözés elleni harccal foglalkozik a következő pont, amely a szükséges kiber kapacitások kialakítását, rendszeres képzést, valamint a vonatkozó jogszabályok rendszeres frissítését írja elő. A hatodik – meglehetősen kurtára sikerült – pont a védelmi kiber képességek fejlesztéséről (Development of defence cyber capabilities) szól. Ennek értelmében Szlovénia kibervédelmi képességeket fog fejleszteni, amelyek a szövetséges országokkal együtt és tőlük függetlenül is képesek a rendszerek védelmére, valamint támogatást nyújtani a katonai műveletekhez és a válsághelyzeti tervezéshez. A képességfejlesztésre vonatkozóan szintén felmerül a szövetségi rendszerben történő és a független fejlesztés lehetősége is. A két utolsó stratégiai célkitűzés a jelentős természeti és más katasztrófák bekövetkezése esetén szükséges működés biztosításáról, illetve a kiberbiztonság terén nélkülözhetetlen nemzetközi együttműködésekről szól. Visszatérve a szlovén stratégia hatodik pontjára, a dokumentum explicit módon említi a kiber képességeket és direkt módon szerepel a katonai műveletek támogatása is. Ám annak ellenére, hogy a katonai műveletek támadó jellegűek is lehetnek, a kontextus egyértelműen védelmi arculatot igyekszik teremteni a szlovén kiber képességek kialakítása kapcsán.

Szlovákia

Szlovákiában egészen friss, 2021-től 2025-ig szóló kiberbiztonsági stratégia (SK CERT, 2021) van érvényben. Az előszó alapján a stratégia megalkotóinak célja nem kevesebb, mint az, hogy Szlovákia mindig egy lépéssel a potenciális fenyegetések előtt járjon. Ehhez a dokumentum a szokásos struktúrát követve először a fenyegetéseket veszi sorba, majd stratégiai célkitűzéseket határoz meg az implementálás részleteire és a folyamatok mérhetőségére kiterjedő elemekkel, amit a finanszírozás is kiegészít. Második, vagy ha úgy tetszik új generációs stratégia lévén, a szlovák dokumentum explicit módon tartalmazza a hatalmi és politikai hátterű támadások kapcsán, hogy egyre több állam épít offenzív képességeket a kibertérben annak érdekében, hogy politikai és hatalmi dominanciájukat közvetíteni tudják a nemzetközi közösség többi szereplője felé. A szlovák állam stratégiai célkitűzései között első helyen szerepel a fenyegetésekkel szemben felkészült,

megbízható állam víziója, amihez a kezdeti állapot nem túl rózsás a felvázolt rendszerszintű hiányosságok tükrében. Erre jó példa, hogy miközben a kiberbiztonsági incidensek detektálása és kezelése terén a szektorális helyett nemzeti képességfejlesztésre fókuszálva igyekeznek javítani a helyzeten, a kiberbiztonsági incidensek tekintetében nincs a tulajdonításra (attribúcióra) vonatkozó egységes folyamat, ahogy az azt követő diplomáciai és jogi mechanizmus se létezik. A dokumentum alapján a cél eléréséhez képességfejlesztésre van szükség a nemzeti kibertér biztonsághoz kapcsolódó események észlelése és gyűjtése, illetve az incidens észlelés és a kiértékelés kapcsán is, amihez a modern technológia különböző formái nyújtanak segítséget. Az incidenskezelés területén szintén képességfejlesztésre, illetve automatizálásra van szükség amellett, hogy a szükséges felszereléssel és kapacitásokkal kell rendelkezni a helyszíni incidenskezelési képesség megteremtéséhez. Szintén a felkészült és megbízható állam célkitűzésével összefüggő elvárás az aktív és passzív kiberhírszerzés hatékony működése annak érdekében, hogy a Szlovák Köztársaságra fenyegetést jelentő kibertérben folyó tevékenységekről információt gyűjtsenek, aggregáljanak és értékeljenek. Szabályok és mechanizmusok kialakítása szükséges a sértő tartalmak (támadók irányító szerverei, rosszindulatú kódot terjesztő eszközök stb.) blokkolására és fejleszteni szükséges a biztonsági fenyegetéseket elemző kapacitásokat a technikai és politikai attribúciós folyamat kialakításához. Ezzel egyidőben a felelős intézmények, valamint a jogi és kiberdiplomáciai mechanizmusok meghatározása elengedhetetlen. A szlovák stratégia második célkitűzése a kiberbűnözés észlelése kapcsán szükséges hatékonyság növeléssel foglalkozik és szintén az észlelés, illetve műveleti képességfejlesztés mellett az érintett szervezetek közötti együttműködést és szakképzés erősítését szorgalmazza. A harmadik pont a privát szektor ellenállóképességével és rugalmasságával, míg a négyes pont a közigazgatással, mint a kiberbiztonság alapvető elemével foglalkozik. Ez a kérdéskör a korábbi nemzeti stratégiákban jellemzően az e-kormányzás címszó alatt jelenik meg. Az együttműködés erősítésével foglalkozó ötödik pont alapvetően nemzetközi fókuszú, azonban a megvalósítás tekintetében számos nemzeti szintű intézkedést ír elő az eseménykezelő központok, illetve a főként az Amerikai Egyesült Államokban elterjedt, de Szlovákiában újonnan felállítandó ágazati információ megosztó és elemző központok (Information Sharing and Analysis Center – ISAC) tekintetében. A hatodik pont az oktatás és képzés kérdéskörét dolgozza fel külön kitérve egyrészt a szakemberhiány kapcsán a specialisták képzésére, másrészt az általános kiberbiztonsági tudatosság növelésére társadalmi szinten. Az utolsó pont szintén képességfejlesztéssel foglalkozik, de elsősorban a kutatás és

fejlesztés terén, például a kiberbiztonsági kompetencia és tanúsító központ (Competence and Certification Cyber Security Centre – CC CSC) részvételével. Az aktuális szlovák kiberbiztonsági stratégia explicit módon csak az ellenfél tekintetében tartalmaz offenzív kiberképességeket, azonban implicit módon bele kerültek aktív kibervédelmi, illetve kiberhírszerző képességek, amiknek a kialakítására az ország hangsúlyt fektet a 2025-ig tartó időszakban. Ezen túlmenően a nemzetközi politikai partnerséggel foglakozó részből érdemes kiemelni a NATO-nak tulajdonított elrettentő védelmi képességeket, ami valószínűleg a kibertér műveleti dimenzióként történő elismerése okán került be és a súlyos kibertámadásokra adható kinetikus válaszcsapás lehetőségére utal.

Ukrajna

Bár Ukrajna nem tartozik hazánk szövetségi rendszereihez – az országban zajló háborútól[43] függetlenül is – instabilitást mutat és egy gyenge állam (Messner és mtsai., 2015) képét közvetíti. Már az említett két ismérv is elegendő ahhoz, hogy bekerüljön a kutatás stratégiákat vizsgáló részébe, azonban különös jelentőséget ad az ukrán kiberbiztonsági stratégiai elképzelések vizsgálatának, hogy az elmúlt időszakban több komolyabb kiberbiztonsági incidens elszenvedője volt az ország (CPI, 2022). Sőt, egyes szakmai nézetek szerint Ukrajna egyfajta „tesztpálya" funkcióját tölti be az orosz offenzív kiberképességek kipróbálására (Cerulus, 2019). Az ukrán kiberbiztonsági stratégiát (CCDCOE, 2018) tartalmazó dokumentum 2016 tavaszán jelent meg, így korát tekintve ez sem nevezhető frissnek. Az első, általános rendelkezéseket tartalmazó részben a dokumentum készítői kifejtik a kibertér nyújtotta lehetőségeket és előnyöket, majd rövid úton rátérnek arra, hogy az orosz agresszió, valamint az ország külső és belső biztonsági környezetében történő fundamentális változások nyomán a kiberbiztonságnak a nemzeti biztonság részévé kell válnia. Arra vonatkozóan, hogy ezt miként lehet elérni, a komplex jogi, intézményi és információs intézkedések között a dokumentum megemlíti a proaktív intézkedések prioritását és a kibertér jogellenes és katonai felhasználásának megelőzését. A második, környezetet és fenyegetéseket

[43] 2022. február 24-én Oroszország a nemzetközi béke és biztonság alapjait veszélyeztetve, több nemzetközi egyezményt felrúgva, hadüzenet nélkül megtámadta Ukrajnát. A konfliktus jelentős mértékben kiterjed a kibertérre is, azonban egy aktív konfliktus fejleményeinek ilyen rövid időn belül történő feldolgozása nem összeegyeztethető a tudományos igényességgel és szakmai elvárásokkal. Ezen túlmenően az értekezés tárgyát képező kérdések vizsgálati időszaka 2022. januárig tart. Mindezek tükrében az értekezés nem foglalkozik a jelenleg zajló orosz-ukrán háború kiber dimenziójával.

értékelő rész előkelő helyre sorolja tulajdonképpen az összes nagy ellátó rendszer és szektor jelentős sérülékenységét a külföldi hírszerző szolgálatokkal szemben, amit „hírszerzési-felforgató" tevékenységként aposztrofál. A dokumentum arra is kitér, hogy a rendszerek ilyen mértékű sérülékenységéhez hozzájárul az, hogy közvetlenül vagy közvetetten Oroszországhoz köthető szervezetek, csoportok és egyének vannak jelen – sokszor domináns mértékben – az ukrán információs infrastruktúrában. Az ukrán kiberbiztonság nemzeti rendszerének több letéteményese is van, amelyek közül a védelmi minisztérium és a vezérkar felelős a saját információs infrastruktúrájának védelméért és a kibertérben megjelenő katonai agresszió elhárításáért. A megelőzési, észlelési és válaszadási tevékenységek megoszlanak az érintett nemzetbiztonsági szervezetek között, míg a kiberhírszerzési feladatokat általánosságban az ukrán hírszerző ügynökségek végzik. Az ukrán stratégia cselekvési prioritás tekintetében az első pontba sorolja a számítógépes eseménykezelő csapatok felállítását, illetve a kiberfenyegetések időben történő észlelését, megelőzését és semlegesítését akár önkéntes szervezetek bevonásával. A második pontban kerül említésre a kibertámadások és kibertéri incidensek kapcsán az azonnali reagálás és a helyzetkezelő központok integrált hálózata, míg a negyedik pont előírja a kibertérből érkező agresszióra történő válaszadáshoz szükséges eszközök fejlesztését, amik a katonai konfliktusokat elrettentő, illetve a katonai fenyegetések tekintetében megelőző – proaktív – eszközökként funkcionálhatnak. A négyes pont kiberbiztonság és kibervédelem terén az ukrán haderő számára önálló egység alakítását írja elő stratégiai, műveleti és taktikai szinteken, miközben az ukrán nemzeti kiberbiztonságban szerepet vállaló többi szervezetnek is dedikált alegységeket kell létrehoznia. A külföldi különleges szolgálatok, szervezetek, csoportok és egyének hírszerző és bomlasztó tevékenységével szembeni cselekvőképesség erősítéséhez kapacitás bővítést ír elő a stratégia. Az ukrán kiberbiztonsági stratégia érezhetően turbulensebb környezetben készült, mint az eddig feldolgozott többi dokumentum. Konkrét agresszort nevesít, miközben dedikált szervezeti képességek kialakítását és fejlesztését írja elő műveleti és operatív szinten. Bár explicit módon nem szerepel offenzív ukrán képesség kialakítására irányuló szándék, a proaktív kifejezés implicit módon magába foglalhat olyan képességeket, amely a defenzív és offenzív képességek határán helyezkedik el.

Horvátország

Horvátországban a jelenleg is hatályos kiberbiztonsági stratégia (ENISA, 2015) 2015-ben jelent meg. A dokumentum sajátos struktúrába foglalva tekinti át a kiberbiztonsági feladatokat, melyeket a kiberbiztonság összetevői alapján először három részre oszt: elektronikus kommunikációs és információs infrastruktúra és szolgáltatások, létfontosságú kommunikációs és információs infrastruktúra és kibertéri válságkezelés, kiberbűnözés. A következő fejezet a kiberbiztonság területei közötti kapcsolatokat tekinti át az információvédelemtől a számítógépbiztonsági incidenskezelésen és nemzetközi együttműködésen keresztül, a kiberbiztonsági tudatosság növeléséig. A sajátosság pedig abból adódik, hogy a számozással ellátott fejezeteken átívelően az abc betűi szerint besorolva rögzítik az egyes területekhez kapcsolódó feladatokat. A dokumentum kiterjedten foglalkozik a kibertér jelentőségének felismerésével, az átfogó megközelítéssel és a szakterületre jellemző különböző összefüggésekkel. A készítők tankönyvszerű alapossággal írják le a kiberbiztonság különféle szereplőit és az érintett szektorokat, azonban a kibervédelem terén jelzik, hogy a kiberbiztonsági stratégia nyomán felmerülő intézkedések a védelmi stratégia részét képezik, miközben a nemzetbiztonság kibertérhez kapcsolódó aspektusaival az állami szervezeteknek egy szűk köre, a biztonsági és hírszerző entitások foglalkoznak eltérő megközelítés alapján. A defenzív és offenzív technológiák, metódusok, algoritmusok, eszközök, szoftverek és hardverek az oktatás, kutatás, fejlesztés és tudatosság növelése kapcsán kerülnek előtérbe és stratégiai kutatási szektorok meghatározására van szükség a dokumentum alapján. Ezért bátorítani szükséges azon kutató csoportokat és kutatási projekteket, amelyek a horvát stratégiai érdekek mentén az információ biztonság területére fókuszálnak. A horvát kiberbiztonsági stratégiában nem jelennek meg explicit módon a kiberműveleti képességek, sem defenzív, sem offenzív aspektusban. Ugyanakkor a stratégia a kiberműveleti képességekre, illetve a különböző szakterületeken megjelenő specializáltságra implicit módon utal azáltal, hogy említést tesz a katonai, rendvédelmi és nemzetbiztonsági szektorok eltérő megközelítéséről.

III.1.2 Kiber képességek a kisállamok stratégiáiban

Svájc

Az aktuális svájci kiberbiztonsági stratégia (NCS CH, 2018) 2018 tavaszán jelent meg, így 5 éves ciklusa végéhez közeledik. A dokumentum kiberfenyegetéseket értékelő részében a kibertámadásoknak öt fajtáját különbözteti meg: kiberbűnözés, kiberkémkedés, kiberszabotázs és kiberterrorizmus, dezinformáció és propaganda, kibertámadások konfliktusokban. A kiberkémkedést a dokumentum olyan tevékenységként határozza meg, amely politikai, katonai vagy gazdasági célok érdekében állami, vagy nem állami szereplők általi engedély nélküli hozzáférés információkhoz. A kiberkémkedés kapcsán arra is kitérnek a szerzők, hogy a hatások gyakran nem a támadást követően azonnal jelentkeznek, hanem csak jóval később, amikor a megszerzett információkat felhasználják. Ez azért is lehetséges, mert a támadók olyan módszereket fejlesztettek ki, amikkel sokáig észrevétlenek maradhatnak a megtámadott hálózatokon.

További kockázat az ország számára, hogy erős a külföldi gyártóktól való függés, ezért folyamatosan fennáll a veszélye annak, hogy a gyártók a saját országaik hírszerző szolgálataival együttműködve sérülékenységeket hagynak nyitva, amit kémkedésre használhatnak. A kiberszabotázs tekintetében a szöveg kiemeli a fizikai hatások potenciális lehetősége mellett, hogy növekszik az esélye annak, hogy svájci szervezet ellen nem állami szereplő politikai okból szabotázst követ el. A konfliktusok során megjelenő kibertámadások a katonai erő mellett alkalmazott politikai, gazdasági és bűnözői eszközök tárházát szélesítik. A hibrid konfliktusokban a felelősség álcázása bevett gyakorlat, amihez a számítógépes támadások kiválóak, mivel nehéz egyértelműen beazonosítani a támadó felet. Ezen túlmenően a költségek viszonylag alacsonyak, azonnali hatást lehet kifejteni, tetszőlegesen nagy távolságokból is végre lehet hajtani és lehetővé teszi politikai-katonai hatások kiváltását abban a „szürke zónában”, ami a háborús küszöb alatt marad.

A kiberműveleti képességek a stratégia végrehajtásával összefüggő intézkedések között a kibervédelmi elemnél a 22-24 pontokban jelennek meg. A hírszerző szolgálatokról és a fegyveres erőkről szóló törvények felülvizsgálatával a szövetségi kormány megteremtette a jogi alapot a kibervédelem kiterjesztéséhez az aktív- és ellenintézkedésekre. A hírszerző szolgálatoknak

képesnek kell lenniük a lehető leghamarabb azonosítani az új támadási mintákat a szisztematikus információ gyűjtés és elemzés révén. Szintén képesnek kell lennie minél precízebben meghatározni a támadások elkövetőit (attribúció) a politikai és bűnügyi hatóságok szabad tevékenységének garantálásához. A kibervédelem területén a haderőnek garantálnia kell a műveleti készenlétet bármilyen helyzetben. A korábban említett három intézkedés közül az első az információgyűjtési és tulajdonítási képességek kibővítésére vonatkozik a támadások korai szakaszban történő azonosítása érdekében. A hírszerzés mélyreható elkövetői (aktor) és környezeti elemzéseket végez, ezáltal a támadásokat szisztematikusan feldolgozzák és nyomon követik. A második pont az aktív intézkedések képességét tartalmazza, ami nem más, mint a megfelelő kvalitatív és kvantitatív kompetencia, illetve kapacitás a támadások megzavarására, megelőzésére vagy lelassítására. A harmadik pont a fegyveres erők műveleti készültségének biztosításával foglalkozik, illetve a civil hatóságok támogatásának részleteivel.

Említésre méltó a svájci stratégia végén található kibervédelem meghatározás, amely szerint valamennyi hírszerző és katonai tevékenység ide tartozik, ami megzavarja, elnyomja vagy lelassítja a kibertámadásokat, azonosítja az elkövetőket, illetve biztosítja a fegyveres erők műveleti készültségét bármilyen helyzetben, továbbá a civil hatóságok támogatásához szükséges kisegítő képességek és kapacitások építését szolgálja. A svájci stratégiában explicit módon nem jelennek meg az offenzív kiberműveleti képességek, azonban defenzív aspektusból több konkrétumot is tartalmaz az aktív, illetve ellenintézkedési képességekkel kapcsolatban. A stratégia szisztematikusan felosztja a katonai, rendvédelmi és nemzetbiztonsági szektorokra háruló feladatokat és az azokból levezethető kiberműveleti képességeket.

Hollandia

A holland kiberbiztonsági stratégiát tartalmazó dokumentum (ENISA, 2018) 2018-ban jelent meg és jelenleg is hatályos. A készítők hét ambíciópontban foglalták össze a Hollandiára fenyegetést jelentő kibertérben zajló folyamatokat és ezekhez csoportosítva fogalmazták meg a célkitűzéseket, valamint a kapcsolódó intézkedéseket. Azonban már az ambíciók ismertetése előtt, a digitális doménből érkező fenyegetések kapcsán kitér a dokumentum arra, hogy nem csak a digitális támadó képességeket fejlesztő országok száma növekszik, hanem a végrehajtott támadások komplexitása is. A demokratikus folyamatokat geopolitikai érdekek mentén befolyásolni képes szereplők

támadásai miatt a nemzetek civil és katonai oldalon egyaránt befektetnek a kiberképességekbe. A dokumentum készítői egyértelműen kijelentik, hogy a kiberbiztonság elválaszthatatlanul kapcsolódik a nemzeti biztonsághoz és a Hollandia képességeit taglaló pontban jelzik, hogy a megfelelő képességek kiterjednek az offenzív területre is, azonban erről csak a második ambíció pontban írnak részletesen. A holland stratégia szerzői ebben a pontban gyűjtötték össze a defenzív és offenzív kiberképességekkel kapcsolatos célokat és intézkedéseket. A szerzők megismétlik, hogy növekszik az offenzív katonai kiberképességeket kialakító országok száma, ami jelentős veszély a nemzetközi biztonságra. A növekedés egyik oka, hogy nehéz a kibertérben az attribúció, Hollandiának pedig saját képességekkel és ezközökkel kell rendelkeznie, hogy képes legyen határozottan elhárítani a nemzeti érdekeit ért digitális támadásokat, és – szélsőséges esetben – arányosan megtorolni. Hollandia képes azonnali és megfelelő válaszokat adni egyedül, vagy koalíciós partnerként az állami szereplők általi digitális támadásokra és offenzív képességekkel rendelkezik, amik hozzájárulnak az elrettentéshez. Az intézkedések között a szerzők azzal folytatják, hogy Hollandia széles stratégiai keretrendszert fejleszt a digitális támadásokkal szemben, ami magába foglalja az eszközöket, az attribúciót, az elrettentést, az offenzív képességek alkalmazását és a kiterjedt válaszadás lehetőségét. Annak érdekében, hogy Hollandia képes legyen a potenciális ellenfeleit elrettenteni, tovább fejleszti a haderő offenzív kiberképességeit. A további öt pont a szoftver és hardver biztonsággal, a digitális folyamatok ellenálló képességével és a robusztus infrastruktúra kialakításával, a kiberbűnözés elleni intézkedésekkel, a kiberbiztonsági tudás bővítésével, valamint a kiberbiztonsági szektor közös állami és privát együttműködésen alapuló megközelítésével foglalkozik. A holland stratégiában explicit módon jelennek meg a kiberműveleti képességek defenzív és offenzív aspektusban egyaránt. A stratégia direkt módon tartalmaz olyan képességeket, amelyek akár megelőzésre vagy megtorlásra is felhasználhatók a kibertérben.

Észtország

Az aktuális észt kiberbiztonsági stratégia (MKM, 2019) a 2019 és 2022 közötti időszakra vonatkozóan határozza meg az ország kibertérrel kapcsolatos törekvéseit. A terjedelmes dokumentum célkitűzésekre és a fenntartható digitális társadalommal összefüggő tevékenységi területekre bontva mutatja be a kibertérrel kapcsolatos észt gondolkodás stratégiai szintjét. A

stratégia előzményeit és a dokumentum alapelveit követik a stratégiai célkitűzések, melyek mindegyike a fenntartható digitális társadalmat szolgálja. A tevékenységeket három prioritási csoportba sorolták, ezek a megelőzés, a védelem és a fejlesztés. A szerzők leszögezik, hogy a jövőkép eléréséhez szükség lesz minden szinten:

- elegendő kompetenciára, emberi erőforrásra és finanszírozásra;
- a kiberbiztonság integrálására minden területen és kulcsfontosságú folyamatba;
- a projektek összetettségének adminisztrálására és a bürokrácia minimalizálására jogi és közigazgatási intézkedésekkel egyaránt.

A kiberműveleti képességek tekintetében az észt stratégia nagyon röviden és diszkréten, ugyanakkor lényegretörően fogalmaz. Egyetlen pontban fejti ki, hogy folytatják a kiberműveleti képességek fejlesztését a védelmi erők kiberparancsnokságának korszerűsítésével. Ez magában foglalja a kiber-támadó képességek fejlesztését és a „kiber konskripció" [44] azaz sorozás intézményének előmozdítását annak érdekében, hogy a kötelező sorkatonai szolgálat alatt valaki a gyalogos helyett az IT irányt választhassa. A teljesség igénye nélkül, a dokumentum a legjelentősebb kihívások közé sorolja a szaktudás korlátozottságát a csökkenő és elöregedő észt népesség tükrében, az integrált stratégiai irányítás hiányát, a kiberfenyegetések, -incidensek és kölcsönös függések figyelmen kívül hagyását stratégiai szinten, valamint a tudatosság és a képzés hiányát is. Az észt stratégiában explicit módon megjelenik a kiberműveleti képességek offenzív aspektusa, amit alapvetően a haderő illetékes parancsnokságához utal. A terjedelmes stratégia ezen kívül nem részletezi a kiberműveleti képességeket, nem tartalmaz direkt meghatározásokat a katonai, rendvédelmi és nemzetbiztonsági szektorok kapcsán.

Izrael

Az Izrael kiberbiztonsági stratégiáját tartalmazó dokumentumot (Cyber Israel, 2021) 2021 közepén adta ki a területet felügyelő Nemzeti Kiber Igazgatóság (National Cyber Directorate – NCD). A dokumentum előszava sommás összefoglalót ad a kiberfenyegetésekkel kapcsolatban. A

[44] A konskripció szó szerint összeírást jelent, ami a katonai terminológiában a hadkötelezettek, illetve katonakorúak összeírását, illetve sorozását jelenti. Az észt rendszer külön figyelmet fordít arra, hogy a kiberbiztonság területén jártas katonakorúakat összeírják, besorozzák és számukra alternatív lehetőséget biztosítsanak a sorkötelezettség letöltésére, illetve az önkéntes, illetve túlszolgálat idejére.

kiberkockázatok növekednek, az offenzív eszközök egyre kifinomultabbá válnak és egyre több rosszindulatú szereplő számára elérhetők, a technológiai környezetre egyre inkább jellemző az összekapcsoltság, miközben a technológia egyre mélyebben ágyazódik be a mindennapi életünkbe, a kibermunkaerő pedig nem növekszik az igényekkel arányosan. Szintén az előszóban kerülnek említésre a perzisztens kibertámadások, illetve a velük szerzett éles tapasztalatok és az ország több területen betöltött úttörő szerepe. A nemzeti kibervédelem koncepcióját a stratégia három rétegre osztja fel. Az első a piaci szektor ellenálló képessége, ahol önálló képességekkel rendelkező entitások vannak ugyan, de az állam számára is fontos a kölcsönös együttműködés a nemzet támadási felületének csökkentése érdekében. A második réteg az operatív válaszadás, ami magába foglalja a fenyegetések észlelését, az elemzést, az eltávolítást, a funkcionális helyreállást, és az immunizálást hasonló támadásokkal szemben. A harmadik réteg a nemzeti védelem képessége a támadókkal szemben, ami magába foglalja a diplomáciai, rendvédelmi, információs, gazdasági, katonai és kiber eszközöket egyaránt. Az izraeli érdekeket aláásó ellenfelekkel szemben elfogó, védelmező és elrettentő lépéseket alkalmaznak. Szükség esetén Izrael határain túl is. A fenyegetési tendenciák kapcsán a stratégia azzal számol, hogy a következő években a rosszindulatú szereplők kifinomultsága növekszik, még többen fognak hozzáférni offenzív kiberképességekhez és folytatódnak a nagyértékű célpontok elleni támadási kísérletek. Izrael külön figyelmet fordít a stratégiában a nemzetközi jogra és az erővel való fenyegetés vagy alkalmazás tilalmára vonatkozóan, amihez az Egyesült Nemzetek Szervezetének Alapokmánya ad támpontot és a kibertérben is alkalmazható. Hasonlóan látják az önvédelemhez való jog alkalmazhatóságát is, így a számítógépes eszközökkel végrehajtott támadásokkal szemben számítógépes vagy kinetikus eszközökkel is felléphetnek. Egy a stratégiai megközelítéssel foglalkozó dokumentum (National Cyber Directorate, 2017) a nemzeti kibervédelmet két kampánynak nevezett elemre bontja. A nemzeti védelmi kampányok olyan védelmi erőfeszítéseket tartalmaznak, mint a védelmi műveletek, a nemzeti incidenskezelés, illetve a helyzetértékelés képessége, míg a támadók elleni kampányban találhatók a hírszerzési, megelőzési, illetve a kikényszerítő és elrettentő tevékenységek. Az izraeli stratégiában explicit módon nem jelennek meg az offenzív kiberműveleti képességek, azonban defenzív aspektusból több helyen is említésre kerülnek olyan tevékenységek, amelyek egyértelműen az aktív védelem kategóriájába sorolhatók, illetve az ellenfelek képességeinek semlegesítését szolgálják.

III.1.3 Nagyhatalmi kiberműveleti képességek és ambíciók

Kína

A kínai kiberbiztonsági stratégiának létezik egy nem hivatalos angolnyelvű fordítása (Creemers, 2016), amit a vizsgálat során szekunder forrásokkal egészítek ki. A kínai stratégia a kihívások számbavétele kapcsán kiemeli, hogy a kiberbiztonsági helyzet fokozódik és a kibertámadások veszélyeztetik a politikai biztonságot. A (számítógépes) hálózatok alkalmazása más országok belpolitikai ügyeibe való beavatkozásra, más országok politikai rendszereinek megtámadása, társadalmi nyugtalanságot szítanak, felforgatják más országok rezsimjeit, míg a széles körű kiberfelderítés, kiberkémkedés és hasonló tevékenységek súlyos károkat okoznak a nemzeti politikai biztonságra és a felhasználók információbiztonságára vonatkozóan egyaránt. Mindezek nyomán a stratégiai feladatok között megjelenik a szuverenitás védelme a kibertérben, amihez minden gazdasági, adminisztratív, tudományos, technológiai, jogi, diplomáciai és katonai intézkedés felhasználható. Minden tevékenységgel szemben határozottan fel kell lépni, ami a rezsim felforgatására, vagy az ország szuverenitásának lerombolására irányul a hálózatokon keresztül. A nemzet biztonságának megőrzése érdekében meg kell akadályozni és törvényesen megbüntetni azokat a külföldi hatalmakat, amelyek a (számítógépes) hálózatokat kihasználva hajtanak végre beszivárgást, rombolást, felforgatást és szeparatista tevékenységeket. Szintén a stratégiai feladatok között szerepel az online antiterrorizmus, a kémkedés ellenes és a lopás ellenes képességek erősítése a szigorú fellépés érdekében. Ahhoz, hogy Kína erős kiberhatalommá váljon a kibervédelmi eszközök erőteljes fejlesztésére, a támadások időben történő észlelésére, a behatolásokkal szembeni ellenállásra és egy erőteljes tartalék, illetve támogató erőre van szükség. Egy a kínai kiberképességekkel és -törekvésekkel foglalkozó tanulmány (Jinghua, 2019) kiemeli a katonai stratégiából a vonatkozó részeket, ami szerint a helyzetfelismerés, a kibervédelem, az állam kibertéri törekvéseinek támogatása és a nemzetközi kooperációban való részvétel a legfontosabb célok. Ide sorolják még a kiberválságok megfékezését, a nemzeti hálózati- és információbiztonság erősítését, valamint a nemzet biztonságának és a társadalom stabilitásának fenntartását. A Kína Nemzeti Kiberbiztonsági Központjáról (National Cybersecurity Center – NCC) szóló átfogó elemzés (Cary, 2021) arra mutat rá, hogy három jelentős hátráltató tényezője van a kínai kiberhaderő kiépítésének. Egyrészt a kiberbiztonsági szakemberhiány Kínát is érinti. Képzett

operatív szakemberek nélkül, akik a (számítógépes) hálózatokat védenék, vagy a támadásokat végrehajtanák, a kínai haderő nem képes teljesíteni az elvárásokat. Másrészt a szakemberek nélkül az az aszimmetrikus előny sem valósul meg, amit a kínai stratégák a kibertérrel összefüggésben prognosztizálnak. Harmadrészt Kína jelentős mértékben külföldi technológiára kénytelen építeni képességeit. Zajlik egy honosítási folyamat, aminek keretében a külföldi szoftverek kínaira cserélése megszünteti más kormányok lehetséges befolyását, illetve a védelem javulása jótékonyan hathat az offenzív képességekre is. Kína jelentős mértékben ugyanazokat a szoftvereket használja, mint amiket támad ezért nincs lehetősége az aszimmetria kialakítására, mivel egy sérülékenység kihasználásával maga is sebezhetővé válik egy esetleges ellentámadás során. A kínai kiberhatalmi törekvések térnyerésével foglalkozó elemzés (IISS, 2019) szerint az elmúlt két évtizedben a kínai kiberkémkedési és offenzív műveleti képességek progresszíven bővültek, ami új fenyegetéseket jelent a távol-keleti és más régiókban egyaránt. Kína Állambiztonsági Minisztériuma (Ministry of State Security – MSS) olyan szereplővé vált, amely növekvő szofisztikáltságot és operatív biztonságot demonstrál a globális gazdasági, politikai és stratégiai célokat szolgáló kémkedési kampányok során. Eközben a Kínai Népi Felszabadító Hadsereg (People's Liberation Army – PLA) Stratégiai Támogató Erő (Strategic Support Force – PLASSF) önálló haderőnemként történő megalakulásával a kínai hadsereg kibertéri ereje és információs műveleti képessége is új szintekre lépett. A kínai stratégiában explicit módon nem jelennek meg az offenzív kiberműveleti képességek, azonban defenzív aspektusból több aktív tevékenységet, illetve képességet igénylő feladat is említésre kerül. A stratégiából és a vizsgált dokumentumokból az derül ki, hogy Kína katonai és nemzetbiztonsági téren is építi kiberműveleti képességeit.

Amerikai Egyesült Államok

A hatályos kiberbiztonsági stratégiát (The White House, 2018) még az előző adminisztráció készítette és 2018 őszén jelent meg. A 2021 januárjában beiktatott új amerikai elnöki adminisztráció eddig nem készített új kiberbiztonsági stratégiát, azonban májusban megjelent egy elnöki rendelet, 2022 elején pedig egy nemzetbiztonsági memorandum, amelyek mindegyike a kiberbiztonság helyzetének javításával foglalkozik. A stratégiát tartalmazó dokumentum négy pillér mentén határozza meg az Amerikai Egyesült Államok kiberbiztonságról alkotott elképzeléseit. Az első pillér az amerikai rendszerek védelmére koncentrál a szövetségi hálózatok

és információk, valamint a létfontosságú infrastruktúrák védelmén keresztül, amit kiegészít a kiberbűnözés elleni küzdelem és az incidensek bejelentésének javítására vonatkozó lépések. A második pillér az amerikai eredményesség köré épül és a digitális ökoszisztéma ellenállóképességével, az amerikai digitalizációval összefüggő szellemi termékek védelmével, valamint a kiváló kiberbiztonsági munkaerővel foglalkozik. A harmadik pillér hivatott a béke megőrzésére egyfelől a kibertér normáinak erősítésével, másfelől az attribúció és az elrettentés javításával. Az utolsó pillér az amerikai befolyás növelésével és fejlesztésével foglalkozik elsősorban a nyitott, megbízható és biztonságos internet garantálásával, illetve a különböző kiberkapacitások bővítésével és támogatásával. A harmadik pillér jelzi, hogy az offline világ kihívásai egyre nagyobb mértékben jelennek meg a kibertérben, ezért az országnak a jövőben a kiberteret nem lehet külön kategóriaként kezelni, hanem a nemzeti erő és hatalom integráns részeként tekintenek rá. Ennek nyomán a cél az, hogy a destabilizáló és a nemzeti érdekekkel ellentétes viselkedést a kibertérben azonosítsák, ellensúlyozzák, megzavarják, degradálják és elrettentsék, az ország kibertérben és azon túl betöltött fölényének megőrzése mellett. Az elfogadhatatlan viselkedésnek is nevezett rosszindulatú kibertéri tevékenységek kapcsán a stratégia leszögezi, hogy a felelőtlen viselkedés nem maradhat következmények nélkül és az ország nemzeti erejének minden eszköze rendelkezésre áll a megelőzés, a válaszadás és az elrettentés terén. Ezek magukba foglalják a diplomáciai, információs, katonai (kinetikus és kiber), pénzügyi, hírszerzési, attribúciós és rendvédelmi képességeket. A stratégia készítői azonnali, költséges és átlátható következményeket ígérnek, aminek az egyik alapvető eleme az amerikai hírszerző közösség által működtetett összadatforrású kiberhírszerző tevékenység. Ennek segítségével azonosíthatók az ellenséges külföldi állami és nem állami kiberprogramok, -szándékok, -képességek, -kutatás-fejlesztési erőfeszítések, -taktikák és operatív tevékenységek egyaránt. A stratégia egyfajta kiegészítéseként is felfogható elnöki rendelet a belbiztonsági miniszter hatáskörébe utalja a kiberfenyegetések „levadászására” irányuló, illetve észlelési és válaszadási tevékenységeket, míg az elnöki memorandum szintén kitér az Amerikai Egyesült Államok kiberfenyegetésekkel szembeni védelmi képességeire. Ennek értelmében a Nemzetbiztonsági Ügynökség (National Security Agency – NSA) felhatalmazást kap arra, hogy kötelező érvényű műveleti direktívákon keresztül a hírszerző közösség tagjaival közösen, konkrét lépéseket tegyen az ismert vagy feltételezett kiberbiztonsági fenyegetésekkel és sérülékenységekkel szemben. Az Egyesült Államok stratégiájában explicit módon nem jelennek meg az offenzív kiberműveleti képességek,

azonban az elrettentésre, megzavarásra, illetve ellensúlyozásra vonatkozó megfogalmazás olyan képességekre utal, amelyek túlmutatnak az aktív védelem keretein és képesek a kiberfenyegetések megelőző semlegesítésére is. A stratégia és a kapcsolódó elnöki dokumentumok külön is kitérnek a katonai és nemzetbiztonsági szektor kiberműveleti képességeire.

Oroszország

A kibertérrel kapcsolatos orosz stratégiai elképzelések kapcsán a Lilly – Cheravitch szerző páros által 2020-ban publikált tanulmány átfogó megközelítéssel foglalkozik az orosz kibertéri erők és a stratégia múltjával, jelenével és jövőjével (Lilly és Cheravitch, 2020). Számos forrásra hivatkozva a tanulmány leszögezi, hogy az elmúlt időszakban a hadviselésre vonatkozó orosz felfogás átalakult és az általános konszenzusról – miszerint a hadviselés alapja a fegyveres erőszak – eltolódott egy olyan irányba, ami a hadviselést kiterjeszti a fegyveres erőszak és a nem katonai intézkedések testre szabott ötvözetére. Nagyjából a kétezres évek kezdete óta folyamatos a hadviseléssel kapcsolatos felfogás átalakulása és bővülése a nem katonai elemekkel, amiben jelentős szerepet kap az információs hadviselés. Az erre vonatkozó legutóbbi doktrínák a legnagyobb fenyegetést a létfontosságú infrastruktúra elemek rombolásában, illetve a jogosulatlan hozzáférésekhez és rosszindulatú szoftverek terjesztéséhez kötődő kibertérben elkövetett bűncselekményekben látják. További jelentős fenyegetésként azonosítja Oroszország a külföldi államok növekedő hírszerző tevékenységét a kibertérben, illetve az információs technológia alkalmazásával okozott károkat a területi integritásban, valamint a politikai és társadalmi stabilitásban. Az oroszok reakciójában megjelenik az információs technológia használatából eredő katonai konfliktusok stratégiai elrettentése és megelőzése, valamint az információs fenyegetések előrejelzésének, észlelésének és értékelésének képessége. Bár Oroszországnak nincs kifejezetten kiberbiztonsági doktrínája és az információs közegben betöltött szerep kapcsán a többi stratégiai dokumentum a védelmi aspektust hangsúlyozza, az orosz katonai elméletek tanulmányozása rávilágít a kiberképességekre, azon belül is az offenzív képességek szerepére az oroszok konfliktusokkal kapcsolatos megközelítésében. A tanulmány arra a következtetésre jut, hogy miközben a hivatalos dokumentumok csak a védelemre terjednek ki, az orosz katonai gondolkodók között folyamatos az eszmecsere a kiberfegyverek és az offenzív képességekkel kapcsolatban. Az, hogy hivatalosan az orosz állam nem foglalkozik az offenzív kiberképességek erősítésével,

bizonyos értelemben lehetővé teszi a kormány számára a tagadhatóságot és a nyugati agresszióval szemben védekező hatalom narratívájának fenntartását. A NATO Stratégiai Kommunikációs Kiválósági Központ (Strategic Communications Centre of Excellence – STRATCOM COE)[45] tanulmányához (Hakala és Melnychuk, 2021) hasonlóan a Lilly – Cheravitch szerző páros is arra a következtetésre jut, hogy az orosz offenzív képességek léteznek és alapvetően két nagy hírszerző, illetve nemzetbiztonsági szervezethez, a katonai hírszerzéshez (GRU) és a kémelhárításhoz (FSB) köthetők. A NATO tanulmánya a jelenkori kiberhatalmak között egyedülállónak nevezi az orosz technikai és pszichológiai számítógép hálózati műveletek konceptualizálását. Oroszország minden más államnál nagyobb hangsúlyt fektet a kognitív hatásokra a kiberműveletek során, amelyek az információs konfrontáció közben valósulnak meg a béke és háború közötti „szürke zónában". Az orosz stratégiai gondolkodásban a kiberműveleti képességek tudatosan defenzív aspektusban jelennek csak meg, az offenzív elemek szándékosan hiányoznak az ilyen tevékenységek letagadhatósága okán. A katonai és nemzetbiztonsági szektorban egyaránt megtalálhatók olyan kiberműveleti képességek, amelyek a fenyegetések elrettentését és a megelőzést aktívan támogatják.

III.2 A defenzívtől az offenzív kiberműveletekig – a teljes spektrum

Katonai szempontból a defenzív és az offenzív kiberműveleti képességek adják a napjainkban fejlesztett és alkalmazott kiberképességek teljes műveleti spektrumát. A kutatás további részei a kiberműveleteknek erre a két típusára koncentrálva foglalkoznak a teljes műveleti spektrumot lefedő kiberképességek kialakításával. A kibervédelmi műveleti képességeket további két alcsoportra lehet tagolni. Az aktív és passzív kibervédelem meghatározásához a Dorothy Denning[46] által alkalmazott lég- és rakétavédelmi összehasonlítást (Denning, 2014) veszem alapul. Ennek értelmében az aktív kibervédelem olyan közvetlen védelmi tevékenység, ami rombolja, csökkenti

[45] A NATO akkreditációval rendelkező Stratégiai Kommunikációs Kiválósági Központot 2014-ben alapította 7 ország, melynek központja Riga. A központ feladata, hogy a szövetség és a tagállamok katonai és politikai céljait segítse multinacionális, szektorokon átívelő megközelítéssel, civil és katonai területen, illetve a privát és az akadémiai szektorok bevonásával a modern technológiák, virtuális eszközök, valamint a kapcsolódó kutatások és döntéshozatal tekintetében.

[46] Dorothy Elizabeth Denning 1945-ben született amerikai információbiztonsági kutató, az amerikai Haditengerészeti Posztgraduális Iskola professor emeritusa, többek között a rács alapú hozzáférés-szabályozás (Lattice-Based Access Control – LBAC) és a behatolás észlelő rendszerek (Intrusion Detection Systems – IDS) alapjainak kidolgozása terén végzett munkája tette ismerté. Jelentős eredményeket ért el a kriptográfiai kutatásaival és beválasztották Amerika nemzeti kiberbiztonsági hírességeinek csarnokába.

vagy megsemmisíti a kiberfenyegetések baráti erőkkel szembeni hatékonyságát. A passzív kibervédelem magába foglal minden más intézkedést és tevékenységet, ami nem aktív, de azonos a célja. Míg az aktív védelem konkrét fenyegetésekkel szembeni lépéseket jelent, a passzív védelem fókuszában a kiberrendszerek támadásokkal szembeni ellenállóbbá tétele és rugalmassága van. A George Washington Egyetem Kiber- és Belbiztonsági Központjának egyik átfogó tanulmánya (Blair, 2016) arra a következtetésre jutott, hogy az aktív és passzív védelem közötti megkülönböztetés évtizedekkel korábban, a haderők hagyományos szárazföldi, vízi és légvédelmi tevékenysége kapcsán alakult ki. Nagyjából az 1970-es években kezdődött az aktív védelem kifejezés elterjedni az amerikai haderőben, azonban hosszú időn keresztül ellentmondásos, vitatott terminológiának számított. Az amerikai védelmi minisztérium katonai és kapcsolódó kifejezések szótárába (DOD US, é. n.) végül az aktív védelem úgy került be, mint az ellenség akadályozása a műveleti tér használatában és/vagy a műveletek végrehajtásához szükséges erőforrások elérésében[47] korlátozott támadó és ellentámadó tevékenységek alkalmazásával. A szótár alapján a passzív védelem olyan intézkedéseket foglal magába, amelyek a kezdeményezés szándékának átvétele nélkül csökkentik az ellenséges tevékenység valószínűségét és minimalizálják az abból származó kárt. Az aktív és passzív védelem definíciója jóval a kiber kifejezés megjelenése előtt alakult ki, azonban a tradicionális meghatározások kiberkontextushoz történő igazítása nehézségekbe ütközött. Részben ennek köszönhető, hogy a határvonalak a kiberműveleti képességek csoportosítása tekintetében a mai napig elég lazák, könnyen előfordulhat, hogy bizonyos értelmezési keretrendszerek (pl. két vagy több állam katonai doktrínái) egy-egy konkrét képességet vagy egy adott műveletet és annak elemeit eltérő alcsoportba sorolnak be, ahogy ezt látni is fogjuk. Ez azonban a kutatást nem befolyásolja, mivel a fókuszban a kiberműveletek teljes spektrumát lefedő képességek kialakítása áll.

III.2.1 Passzív kibervédelem

A hadviselés hagyományos keretein belül értelmezve a passzív védelem az ellenséggel szemben csak korlátozott védelmet biztosít katonai beavatkozás nélkül (Blair, 2016). A fizikai dimenzióból vett példával élve, passzív védelemnek minősül egy erődítmény vagy bunker és minden hozzáadott biztonsági és védelmi elem, ami leapasztja az ellenfél erőforrásait azáltal, hogy csak külön

[47] Az angolszász terminológiában Anti-Access Area-Denial kifejezés a hadszíntér-hozzáférést korlátozó képességek rendszere, amire a magyar szakirodalom a stratégiai visszatartást, illetve a stratégiai visszatartó rendszerek kifejezéseket is használja.

erőfeszítéssel képes céljai elérése. A kibertérre átültetve a SANS Intézet[48] által készített jelentés (Lee, 2021) a passzív védelem kapcsán azt mondja, hogy azok az architektúrához hozzáadott rendszerek alkotják, amelyek konzisztens védelmet nyújtanak a fenyegetésekkel szemben, illetve rálátást biztosítanak a fenyegetésekre állandó emberi interakció nélkül. A szerző szerint ezek a rendszerek a tűzfalak, a rosszindulatú szoftverek elleni rendszerek, a behatolás megelőző rendszerek, az antivírus megoldások, a behatolás észlelő rendszerek és más hagyományos biztonsági rendszerek. Ugyanakkor Denning megközelítésében a passzív kibervédelmi megoldások és képességek közé olyan elemek tartoznak, mint például a kriptográfia[49] és a szteganográfia[50], ami a korábbi lég- és rakétavédelmi példánál maradva megfeleltethető az álcázó festés, illetve a lopakodó repülő eszközök alkalmazásának. Szintén a passzív kibervédelemhez tartozik a rendszerek biztonsági szempontokat figyelembe vevő tervezése és ellenőrzése, a konfigurációs beállítások ellenőrzése, a sebezhetőségek felmérése és csökkentése, a kockázatértékelés, a biztonsági mentések és az elveszett adatok visszaállítása, valamint a felhasználók oktatása és képzése. A légtér megfigyelésével párhuzamba állíthatók a különböző naplózó mechanizmusok, amelyek segítségével a kibervédelmi szakemberek a hálózati és végpont aktivitást ellenőrizhetik. Denning szerint a behatolás észlelő rendszerek (Intrusion Detection System – IDS)[51] alapvetően passzív kibervédelmi megoldások, azonban, ha képesek az észlelt fenyegetés semlegesítésére, azzal behatolás megelőző rendszerré (Intrusion Prevention System)[52] transzformálódnak, ami már aktív kibervédelmi képességnek tekinthető. Bármelyik megközelítést

[48] A SANS Institute hivatalos nevén az Escal Institute of Advanced Technologies egy 1989-ben alapított amerikai cég, amely infromációbiztonsági és kiberbiztonsági képzésekre sepcializálódott saját tanúsítvány rendszert kialakítva. A cég teljeskörű képzési kínálatot nyújt az ügyfelei számára a kezdő, illetve belépő szintű tréningektől a legmagasabb szintű, professzionális tréningekig. Bővebben: https://www.sans.org/about/

[49] A kriptográfia szó jelentése titkosírás és napjainkra önálló tudományágnak számít, amely alapvetően a rejtjelezéssel, titkosírással, kódolással foglalkozik. Az ókor óta jelen lévő kriptológia a matematika és az informatika határán elhelyezkedő interdiszciplináris tudomány terület, ami az előállítással és a megfejtéssel egyaránt foglalkozik. Bővebben: https://www.kaspersky.com/resource-center/definitions/what-is-cryptography

[50] A szteganográfia szó jelentése rejtett írás, ami arra utal, hogy csak a kommunikáló felek tudnak az üzenet létezéséről. A kriptológia párjaként is felfogható, ahol az üzenet és a tartalom létezését nem álcázzák, itt azonban az üzenetet elrejtik egy úgynevezett hordozóban és ennek köszönhetően létrejön a stegotext. Korunk számítógépes világában a hétköznapi felhasználók például kép, vagy hangfájlokban tudnak ilyen módon üzenetet elrejteni anélkül, hogy a fájlok elveszítenék funkciójukat. Bővebben: https://www.comptia.org/blog/what-is-steganography

[51] A behatolás észlelő rendszerek és a behatolás megelőző rendszerek között annyira minimálisak a különbségek, hogy a szakirodalom is rendszerint együtt említi a két megoldást. Olyan eszközökről van szó, amelyek képesek figyelni a számítógépes hálózatokat és rendszereket rosszindulatú tevékenység után kutatva. Ez jellemzően különböző szabályrendszerek megsértésének észlelését, vagy előre megadott lenyomatok (szignatúrák) alapján rosszindulatú tevékenység jelenlétének érzékelését jelenti, amit automatikus védelmi intézkedés (válasz) is követhet a rendszer fejlettségének függvényében. Bővebben: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.675.430&rep=rep1&type=pdf

[52] Ld. előző

is fogadjuk el, a passzív kibervédelemmel kapcsolatban elmondható, hogy széles körben elterjedt megoldásokról és rendszerekről van szó. A végfelhasználókat tekintve ma már a legtöbb azonnali üzenetküldő szolgáltatás valamilyen kriptográfiai megoldást alkalmaz a felhasználók közötti kommunikáció titkosítására[53], ahogy a legtöbb mobiltelefonban is alapértelemezett beállítás a készülékben található tároló titkosítása[54], ami szintén kriptográfiai eljárással történik. A vállalati szegmensben ugyanakkor bevált, gyakran kötelezően előírt folyamat a kockázatértékelés és -kezelés, de megfigyelhető a biztonsági mentések elterjedése[55] és a naplófájlok készítésének[56] bővülő tendenciája is a biztonság szintjének növelése érdekében. Az amerikai kongresszus tagjai számára készített hivatalos dokumentum (Theohary, 2021) sajátos felosztást alkalmaz. Ebben a struktúrában a védelmi minisztérium saját információs hálózatán tervezett, épített, konfigurált, üzemeltetett, fenntartott, működtetett és védett kommunikációs rendszerekhez és hálózatokhoz kapcsolódó műveleteket sorolja egy kategóriába DODIN (Védelmi Minisztérium Információs Hálózat) műveletek néven, ami a passzív kibervédelemhez áll legközelebb.

III.2.2 Aktív kibervédelem

Számos biztonsági kontroll alkalmaz aktív védelmet, aminek a részletes bemutatásához a már említett 2013-as Denning tanulmányra (Denning, 2014) is támaszkodom. A hozzáférési jogosultságok ellenőrzésére használt megoldások képesek blokkolni a felhasználókat, hogy

[53] Az azonnali üzenetküldő alkalmazások térnyerését követően nem kellett sokat várni arra, hogy a felhasználók között küldött üzenetekkel kapcsolatban aggályok merüljenek fel elsősorban azok titkosítatlansága miatt. Ez lehetővé tette a szolgáltatók, kormányzati szervek és a támadók számára, hogy komolyabb erőfeszítések nélkül bárkinek a magánjellegű üzeneteit elolvassák, amit aztán fel is használhattak. A szolgáltatók jellemzően a célzott reklámok finomhangolására, a kormányzati szervek bűnüldöző és nemzetbiztonsági érdekekre hivatkozva, a támadók pedig zsarolásra és lopásra használták a gyengén védett privát üzeneteket. Bővebben: https://www.securemessagingapps.com/about/

[54] Korábban szintén nem volt alapértelmezett, sőt egy ideig az opció sem létezett, hogy a mobil eszközökben található tárhelyen tárolt adatokat elrejtsük a kíváncsi szemek elől. Az eljárás lényege, hogy minden a mobil eszközön keletkező adat – függetlenül attól, hogy azon készül, vagy arra küldik – titkosított formában kerül a tárhelyre. Így egy esetleges lopás során a tolvaj az adatokat csak titkosított formában tudja megszerezni. Bővebben: https://source.android.com/security/encryption/full-disk

[55] A biztonsági mentések (backup) készítése a megelőző kiberbiztonsági tevékenységek közé sorolható és lényege, hogy a meglévő adatállományról másolat készül, ami máshol kerül tárolásra annak érdekében, hogy egy incidenst követő adatvesztés után helyreállíthatóak legyenek a biztonsági mentésből az adatok. Bővebben: https://www.kaspersky.com/resource-center/preemptive-safety/backup-files

[56] Naplófájlok (log fájlok) alatt a számítástechnikában azokat a fájlokat jelölik, amelyek egy operációs rendszer, vagy bármilyen más szoftver működése során bekövetkező eseményeket rögzíti valamilyen előre megadott séma szerint. Egy alapvető naplófájl jellemzően tartalmazza az adott esemény időpontját, típusát, időtartamát és kapcsolódó azonosítókat, felhasználókat, de számos szabvány létezik ezen a területen. Kiberbiztonsági szempontból a naplófájlok fontos szerepet töltenek be egy incidens bekövetkezése és kivizsgálása során. Bővebben: https://www.ncsc.gov.uk/collection/10-steps/logging-and-monitoring

számukra nem engedélyezett fájlokhoz, vagy más számítógépes erőforrásokhoz ne férjenek hozzá. A felhasználói hitelesítési mechanizmusok, mint például a jelszavak alkalmazása képesek blokkolni a legitim felhasználó meghamisításával bejelentkezni próbáló ellenfelet. A rosszindulatú szoftverek elleni, a behatolás megelőző és a tűzfal rendszerek pedig képesek a fenyegetési szignatúrák, illetve a viselkedés alapján blokkolni a szoftvereket és hálózati csomagokat. A „honeypot" [57] néven ismert csaliként használt eszközök elszigetelt rendszerekbe terelik a támadásokat, ahol megfigyelhetők és távol tarthatók az éles rendszerektől. Mindezek a rendszerek nagyban hasonlítanak a már korábban említett lég- és rakétavédelmi rendszereknek azon változataira, amelyek képesek megsemmisíteni, vagy elterelni a beérkező támadó eszközöket. Denning szerint az aktív kibervédelem (Active Cyber Defense – ACD) négy fő karakterisztikával bír, a hatókör, az együttműködés szintje, a hatások típusa és az automatizálás mértéke. Ezekkel egy olyan négydimenziós keretrendszer hozható létre, amiben az összes aktív kibervédelmi képesség megkülönböztethető és elemezhető az etikai kérdések szempontjából.

A hatókör tekintetében belső és külső védelemről beszélhetünk, ami előbbi esetben a védett hálózaton belüli tevékenységet, míg utóbbi eseteben a védett hálózaton túli lépéseket is magába foglal. A jogosultság ellenőrzés, vagy a behatolás megelőzés tipikusan belső tevékenységek, míg egy botnet[58] irányítására (Command and Control – C2, C&C)[59] használt IP címek átvétele a védett hálózaton kívüli akció. Az együttműködés szintje kooperatív és non-kooperatív besorolású lehet, ha a kibervédelmi tevékenység által érintett rendszer tulajdonosának tudtával és beleegyezésével, illetve anélkül történik valami. Az előző példánál maradva, ha az IP címeket a tulajdonossal

[57] A honeypot kifejezésre – bár szó szerint mézescsupor a jelentése – a leginkább illő magyar fordítás talán a mézesmadzag. Tulajdonképpen egy megtévesztési eljárásról, illetve csapdáról van szó, ami egy olyan szimulált eszközt vagy hálózati környezetet jelent, ami elhiteti a támadóval, hogy a megcélzott infrastruktúrát támadja. A megoldás a kibervédelem számára azért hasznos, mert lehetőséget biztosít a támadó és a támadás módszereinek megismerésére, így egyszerűbb a megfelelő védelem kialakítása, illetve a további támadások megakadályozása. Bővebben: https://www.kaspersky.com/resource-center/threats/what-is-a-honeypot

[58] A botnet kifejezést alapvetően olyan összekapcsolt (hálózatba szervezett) eszközök halmazára használják, amelyek valamilyen automatikus művelet elvégzésére alkalmas szoftvert futtatnak. Ezek a szoftverek jellemzően nem az eszközök tulajdonosainak és üzemeltetőinek tudtával vagy jóváhagyásával kerülnek az eszközre, hanem rosszindulatú szereplők telepítik azokat. Az eszközökre telepített szoftverek segítségével akár észrevétlenül különböző funkciókat és feladatokat tudnak elvégezni a megfertőzött eszközzel. Bővebben: https://www.trendmicro.com/vinfo/us/security/definition/botnet

[59] Sok más a kiberbiztonságban elterjedt szakmai kifejezéshez hasonlóan a támadás irányításához és kontrollálásához használt infrastruktúra elnevezése is a katonai terminológiából ered. A Command and Control – C2 kifejezést eredetileg szervezeti és technikai folyamatokra alkalmazták, illetve a tekintély és irányítás parancsnok általi gyakorlására a küldetés céljának teljesítése érdekében. A kiberbiztonság a C2 elnevezést inkább egy vagy több eszközre, számítógépre használja. Bővebben: https://sgp.fas.org/crs/natsec/IF11805.pdf és https://www.trendmicro.com/vinfo/us/security/definition/command-and-control-server

blokkoltatjuk kooperatívnak tekinthető a tevékenység míg, ha a botnet segítségével a védett hálózatról egy olyan preparált fájlt tölt le és nyit meg a támadó, ami blokkolja a C2 rendszerhez a hozzáférését, az non-kooperatív megoldásként értelmezhető. A hatások típusa szerint a tevékenység lehet megosztó, gyűjtő, blokkoló és megelőző. A megosztó hatás körébe tartozik a különféle fenyegetésekkel összefüggő információk (pl. IP címek, domén nevek, szignatúrák stb.) terjesztése harmadik fél vagy ügyfél felé. Gyűjtő hatásúnak tekinthetők azok a kibervédelmi tevékenységek, amelyek egy fenyegetés kapcsán további információ megszerzésére irányulnak. Ez jelentheti újabb érzékelők aktiválását és alkalmazását a védett rendszerekben vagy információk bekérését a kibervédelmi közösségtől. A blokkoló jellegű hatások a támadó tevékenységének leállítására, illetve hatásainak minimalizálására irányul. Ide sorolható a konkrét IP címekről érkező forgalom blokkolása a saját hálózaton, illetve egy konkrét program lefutásának a megakadályozása, de a korábban példaként említett C2 hozzáférés blokkolása is belefér ebbe a kategóriába. A megelőző hatás a támadáshoz használt források semlegesítésére és megszüntetésére vonatkozik. Ez lehet egy támadáshoz használt számítógép lefoglalása, vagy a C2 infrastruktúra leállítása is. A megelőző hatást itt olyan értelemben alkalmazzuk, hogy az ellenséges tevékenység folytatását, vagy a támadás kibontakozását előzi meg. Az aktív kibervédelem negyedik karakterisztikája az automatizálás mértéke, ami az emberi részvételre utal. Egy aktív kibervédelmi rendszer akkor automatikus, ha nem igényel emberi beavatkozást, míg manuális, ha a kulcsfontosságú lépéseknél emberi megerősítő intézkedésre van szükség. A legtöbb aktív kibervédelmi rendszer automatikus és manuális komponensekkel egyaránt rendelkezik. Például a behatolás megelőző rendszerek esetében a rosszindulatú kódok és hálózati csomagok észlelése és a kezdeti válasz automatikus, míg a szignatúrák bevitele gyakran manuális, de legalábbis emberi felügyelet mellett történik akár csak a komolyabb fenyegetésekre történő reakció.

Denninghez képest némileg eltérő megközelítést alkalmaz a már említett SANS tanulmányban (Lee, 2021) Robert M. Lee[60]. Az amerikai haderő hagyományos, a kiber kontextust nélkülöző passzív védelem definícióját alapul véve az ellentámadás kifejezés téves használatára hívja fel a figyelmet. Érvelése alapján a szó szerinti fordítás miatt az ellentámadás és a visszatámadás

[60] Robert M. Lee az ipari folyamatirányító rendszerek (Industrial Control Systems – ICS) kiberbiztonságára szakosodott Dragos vállalat alapító ügyvezetője, az iparági CTI és incidens reagálás egyik úttörője. A pályáját az amerikai légierőnél és az NSA-nél kezdte, több iparági elismerés mellett a Forbes 2016-ban beválasztotta a 30 alatti 30-as listájába, jelenleg több nemzetközi szervezet és fórum tanácsadója is.

(hackback)[61] kifejezések közé egyenlőség jelet tettek, azonban ez az értelmezés meglehetősen pontatlan. A hagyományos katonai aktív védelem lényege a manőverezhetőség, a támadás azonosításához szükséges katonai hírszerzési és különböző indikátorok feldolgozására alkalmas képesség, a támadással, vagy a támadó képességgel szembeni válaszadás a védekező zónában, illetve a vitatott területen, és a harcérintkezésből való tanulás képessége. A korábban alkalmazott példánál maradva az integrált légvédelem azon elemei alkotják az aktív védelmi részt, amelyek képesek például az interkontinentális ballisztikus rakéták követésére és megsemmisítésére, mielőtt azok elérnék céljukat. Lee kiberbiztonsági szempontból fontosnak tartja kiemelni, hogy az eredeti ellentámadás szó fókuszában a védett terület, illetve a támadó képesség van és nem az ellenfél. Ebben az értelmezésben az ellentámadás kiberbiztonsági kontextusba helyezve leginkább az incidenskezelő képesség koncepciójában fedezhető fel, mivel az incidenskezelő személyzet a saját hálózaton igyekszik feltartóztatni és elhárítani egy fenyegetést, nem indít támadást az ellenfél hálózatán vagy rendszerein. Pont, mint az integrált légvédelem aktív elemei, amelyek a ballisztikus rakétákat semmisítik meg nem az indító ország lakosságát vagy infrastruktúráját. Ezek alapján Lee szerint az aktív kibervédelem nem más, mint az elemzők által végzett megfigyelési folyamatok a válaszadáshoz, a tanuláshoz és a megszerzett tudás alkalmazásához a fenyegetésekkel szemben a saját hálózaton. Az ilyen aktív védelmet jelentő képességet az incidenskezelők, a fenyegetés és hálózati biztonsági elemzők, a rosszindulatú kódok visszafejtésére képes (malware reverse engineering)[62] szakemberek és a biztonsági személyzet többi tagja jelenti, akik képesek a saját környezetükben vadászni az ellenfélre és választ adni a fenyegetésekre.

A korábban már szintén említett, George Washington egyetemen készített tanulmány szerzői is alkottak egy szerintük a korábbiakhoz képest átfogóbb és pontosabb meghatározást az aktív kibervédelemre (Blair, 2016). E szerint az aktív védelem olyan kifejezés, amely a hagyományos passzív védelem és az offenzív képességek között található, proaktív kiberbiztonsági intézkedéseket foglal magába. Ezek a tevékenységek két nagy kategóriába sorolhatók. Az elsőben

[61] A „hack-back" kifejezés a kiberbiztonságban az önvédelemre, illetve a visszatámadásra utal. Alapvetően aktív védelmi intézkedéseket foglal magába. Jogász teoretikusok és politikai döntéshozók között jelenleg is aktív vita folyik az önvédelem legalizálásáról és kereteinek meghatározásáról, azonban nincs egyetértés abban, hogy egy kibertámadás, vagy az azzal való fenyegetés mikor jogosít fel az önvédelemre, illetve megelőző támadásra.

[62] A reverse engineering angolszász kifejezést arra a folyamatra használják kiberbiztonsági területen, amely egy szoftverprogram működési elvének és felépítésének megismerése érdekében a kód visszafejtésére irányul. A kész kártékony szoftver gépi utasításait magasabb szintre fordítják vissza, amiből a szakemberek számára kiderül, hogy milyen rendszerekkel és mit csinál a program, így kidolgozhatóvá válnak a káros tevékenység kivédéséhez szükséges ellenintézkedések.

a technikai interakciók találhatók a védők és a támadó között. Az aktív védelem második kategóriájában azok a műveletek találhatók, amelyek lehetővé teszik a védők számára a fenyegetéshez kapcsolódó szereplőkről és indikátorokról információk gyűjtését az interneten, továbbá politikai eszközöket (szankciók, vádemelések, kereskedelmi jogorvoslatok), melyek módosíthatják egy rosszindulatú szereplő viselkedését. Az aktív védelem kifejezés nem szinonimája a visszatámadásnak (hacking-back) és használat közben nem felcserélhetők. Aktív védelmi képességekkel manapság meglehetősen sok szereplő rendelkezik a kibertérben. Függetlenül attól, hogy állami vagy nem állami szereplőről van szó, azok a szervezetek, amelyek valamilyen formában a biztonsági műveletek koordinálására létrehozott központot (Security Operations Center – SOC), vagy annak egy fejlettebb változatát, úgynevezett kiberbiztonsági fúziós központot (Cybersecurity Fusion Center – CSFC/CFC) működtetnek, mind rendelkeznek aktív kibervédelmi képességekkel.

Bár aktív kibervédelmi képességeket is említ, a már hivatkozott amerikai kongresszusi jelentés (Theohary, 2021) defenzív kibertéri műveleteknek (Defensive Cyberspace Operations – DCO) nevezi a védelmi minisztérium és más baráti kiberterek védelmét, ami lehet passzív és aktív védelmi művelet és végrehajtásuk történhet a saját hálózatokon vagy azon túl is. A megközelítések közötti eltérésekre mutat rá a zürichi Biztonsági Tanulmányok Központ (Center for Security Studies – CSS)[63] aktív kibervédelem témában készült elemzése (Dewar, 2017) is, ami a kiberhadviselést, illetve a számítógépes hálózati műveleteket (Computer Network Operations – CNO) katonai szerepvállalás vagy konfliktus során alkalmazott offenzív tevékenységnek tekinti, aminek nem része az ACD, ami az incidensek, behatolások és elkövetők azonosítását szolgáló defenzív technika.

III.2.3 Offenzív kiberképességek

Az offenzív kiberképességek értelmezése nem kevésbé problémás, mint a kibervédelmi képességek aktív és passzív területeinek meghatározása. Hasonlóan a másik két szegmenshez, itt sincs egységesen elfogadott terminológia és definíció, teljesen eltérő lehet, hogy egyes államok vagy szervezetek mit tekintenek offenzív képességnek, illetve műveletnek. A másik két szegmens kapcsán is hivatkozott kongresszusi dokumentum az offenzív kibertéri műveletekhez (Offensive

[63] A Zürichi Műszaki Tudományegyetem, Humán, Társadalmi és Politikai Tudományok Karán belül 1986-ban Kurt Spillmann professzor által alapított svájci és nemzetközi biztonságpolitikai kompetencia központ.

Cyberspace Operations – OCO) sorolja az erőkivetítés céljából alkalmazott erőt a kibertéren és azon túl. Ezen műveletek alapja a fizikai doménben végrehajtott műveletekhez hasonló felhatalmazás. Ugyanakkor megjegyzendő, hogy az erő kifejezés alkalmazása egybevág a nemzetközi jog által leírt háborún kívüli jogszerűtlen tevékenységekkel (Lee, 2021).

Az amerikai összhaderőnemi (US Joint Staff ,2013) és brit kiberbiztonsági alapozó (MoD UK, 2016) megközelítés szerint a kibertérben végzett tevékenységek feloszthatók védelemre, hírszerzésre, a műveleti környezet előkészítésére és támadásokra. Utóbbi két további csoportra bontható, a megtagadásra és a manipulálásra. A megtagadás akár csak a kinetikus műveletek esetében az ellenfél erőforrásokhoz történő hozzáférését gátolja. Ennek három különböző módja a degradálás (Degrade), a megzavarás (Disrupt) és a pusztítás (Destroy). A degradálás lényege, hogy az ellenfél hozzáférését, illetve működését redukálják bizonyos mértékben. A megzavarás a degradálás egy speciális formája, amikor az ellenfél hozzáférése és működése időszakosan ellehetetlenül, tehát a redukálás teljes. A pusztítás állandóvá, teljessé és helyrehozhatatlanná teszi az ellenfél hozzáférését és működését. A támadások másik csoportja a manipulálás, ami lényegében az ellenfél rendelkezésére álló információk, információs rendszerek és/vagy hálózatok feletti ellenőrzést és az ezekben – a parancsnok célkitűzései szerint – végrehajtható változtatási képességet jelenti.

Ha a kiberbiztonságot egy skálán képzeljük el, a biztonsági szempontokat figyelembe vevő rendszertervezést, a passzív és aktív kibervédelem követi, majd a hírszerzés, végül az utolsó fázis az offenzív tevékenység, ami közvetlen az ellenféllel szemben, a baráti hálózatokon kívül folytatott tevékenységet jelent (Lee, 2021). A kiberbiztonsági szervezetek és a média gyakran kibertámadásként hivatkozik olyan adatszivárgási incidensekre és kémkedéssel összefüggő eseményekre, amiket pontosabban írna le az ellenséges hírszerző tevékenység kifejezés. Azért is fontos ez, mert az offenzív tevékenységnek minden esetben legálisnak kell lennie annak érdekében, hogy ne lehessen agressziónak tekinteni. Ugyanakkor offenzív tevékenység folytatható a kiberbiztonsági célokon túl is, például a nemzeti politika érdekében, vagy egy konfliktussal kapcsolatban. Ilyenkor azonban minden esetben az ellenféllel szemben a jogos önvédelem keretében folytatott ellentevékenységről és ellentámadásról van szó (Lee, 2021).

Az offenzív kibertevékenység felhasználható átmeneti vagy állandó hatások kiváltására, ezáltal csökkentve az ellenfél hálózatokba vagy képességeibe vetett bizalmát. Az ilyen cselekvés

szándékok vagy fenyegetések közlésével támogathatja az elrettentést. A műveleti és harcászati szinten szükség van a támadó kiberműveletek, illetve az információs műveletek és tevékenységek összehangolására. Az offenzív műveletek fázisai könnyedén besorolhatók hét elkülönülő kategóriába, amik eredetileg a harc megvívásának fázisait leíró katonai terminológiából kerültek átvételre. A Lockheed Martin[64] vállalat által kidolgozott szisztéma angolszász elnevezéséhez (Cyber Kill Chain – CKC) (Lockheed Martin, 2020) nehéz frappáns magyar fordítást találni, ezért a továbbiakban az eredeti idegennyelvű szakkifejezést használjuk. A fázisok nem különálló események, hanem kölcsönhatásba lépnek, átfedik egymást és eltérő időtartamúak lehetnek. Egyformán alkalmazhatók állami vagy bűnözői tevékenységekre. Ezek a támadó szándékától és a támadó által elérhető kiber- és hírszerzési képességektől függenek (Theohary, 2021).

[64] A Lockheed Martin a világ egyik legnagyobb repülőipari, katonai támogató, biztonsági és technológiai vállalata, egyben a legjelentősebb védelmi szolgáltatóipari cég. A mintegy 60 ezer mérnököt és tudóst foglalkoztató cég nevéhez fűződik az olyan híres amerikai katonai repülőgépek kifejlesztése és gyártása, mint az U-2, az SR-71 vagy az F-117, de a cég jelentős erőforrásokat invesztál az egészségügyi rendszerekbe, a megújuló energia rendszerekbe, az intelligens energia elosztó megoldásokba és nukleáris fúziós technológiákba.

3. ábra: A kifinomult kibertámadások keretrendszere, azaz a Cyber Kill Chain fázisai (Szerkesztette és fordította a szerző a Lockheed Martin Cyber Kill Chain ábrája alapján: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html)

Az offenzív kiberműveletek kontextusában a képesség a kibertérben történő hatás kiváltásához szükséges erőforrások, készségek, ismeretek, műveleti koncepciók és eljárások birtoklását jelenti. Általánosságban a képességek alatt azokat az építő elemeket értjük, amelyeket a műveletek során alkalmazva elérhető a kívánt cél. Az offenzív kiberműveletekben offenzív kiberképességeket alkalmaznak a cél kibertérben vagy azon keresztül történő eléréséhez (Hanson, 2018). Az offenzív

kiberképességek azok, amelyek célja az ellenfél befolyásolása (influencing) és műveleteinek, tevékenységének ellehetetlenítése (disabling). Egy védelmi szervezet számára elegendő ismeretnek és képességnek kell rendelkezésre állnia ahhoz, hogy képes legyen offenzív műveleteket végrehajtani a kibertérben a hatékony védekezés és a műveletek támogatása érdekében. Az offenzív kiberképesség erősokszorozó (force multiplier) hatása okán növelheti a fegyveres erők hatékonyságát. Nemzetközi szinten az offenzív műveleti kiberképességek még csecsemő korban járnak. Sok tényező még mindig nem világos ezeknek a képességeknek a természetét, az általuk kínált lehetőségeket és az általuk elérhető hatásokat illetően (ITU, 2012).

Katonai megközelítésben a kiberműveletek képesek egyedülálló taktikai, műveleti és stratégiai hatásokat produkálni, illetve célokat elérni, de csak a katonai parancsnok átfogó tervének integráns részeként. Ez a doktrinális megközelítés azonban az országok viszonylag szűk körének katonai szervezeteitől származik, míg más államokban előfordulhat, hogy az offenzív kiberműveletek kevésbé integrálódnak a katonai tervezésbe, és az állami vezetés politikai és/vagy stratégiai céljainak elérése érdekében történnek. Definíció szerint az offenzív kiberműveletek különböznek a számítógépes kémkedéstől, amelynek célja az információgyűjtés, hatás nélkül. Amikor az információgyűjtés az elsődleges cél, a lopakodó és rejtett működésre van szükség az észlelés elkerülése érdekében, hogy fenntartsák a perzisztens hozzáférést, amely lehetővé teszi a hosszabb távú információgyűjtést (Hanson, 2018). A kiberképességeket vizsgáló és rangsoroló analízisek alapján legalább 30 offenzív kiberműveleti képességgel rendelkező ország van (Voo és mtsai., 2020).

III.3 A kiberműveleti képességek fejlődése

Amikor kiberműveleti képességek kerülnek szóba, viszonylag hamar felmerülnek olyan kérdések, mint például melyik állam és milyen képességeket fejleszt, mióta rendelkezik defenzív vagy offenzív képességekkel és ezekkel a képességekkel milyen műveleteket tud megvalósítani. A fejezet első pontjában (III.1) bemutatott stratégiákból ilyen tekintetben viszonylag kevés hasznos információ nyerhető, mivel az államok jelentős része láthatóan nem hozza nyilvánosságra a kiberműveleti képességeinek szintjét és kiterjedését. Kézenfekvő lenne, hogy a műveleti képességek ismertetésének nem a stratégiai dokumentumokban van a helye, azonban az ágazati

stratégiák és általában az alacsonyabb szintű nyilvánosan elérhető, hivatalos dokumentumok sem tartalmaznak lényegi elemeket a kiberműveleti képességekről. Azok a kormányzatok által készített dokumentumok, amik a kiberműveleti képességekkel érdemben foglalkoznak, jellemzően minősítettek. A legtöbb nyilvánosan elérhető információ egy-egy ország kiberműveleti képességével és annak érettségével összefüggésben a honvédelmi, rendvédelmi és nemzetbiztonsági ágazatok illetékes szervezeteinek és egységeinek létrehozásához kapcsolódik. Ezeknek az ügynökségeknek, hivataloknak, központoknak vagy parancsnokságoknak a megalapítása általában konkrét dátumhoz köthető, az eltelt idő alapján pedig nagy vonalakban következtetni lehet az érettségi szintre. Azonban azt nehéz lenne megmondani, hogy ki és mit kezdett el előbb fejleszteni, kinek az akcióját követte reakció és így tovább. Ahhoz, hogy a kiberműveleti képességek kialakítása, illetve felépítése kapcsán letisztultabb képet alkothassunk, a továbbiakban három esettanulmány segítségével mutatom be Oroszország, Kína és az Egyesült Államok vonatkozásában a kiberműveleti képességek fejlődésének dinamikáját, ami egyben átvezet a következő fejezetben tárgyalt fejlett perzisztens fenyegetésekre.

III.3.1 Az orosz állami szereplők és megbízottjaik kiberképességei

Ahhoz, hogy betekintést nyerjünk az orosz állami szereplők, illetve az orosz állam megbízásából tevékenykedő közreműködők kiberképességeibe, a NATO STRATCOM COE által 2021-ben publikált, Oroszország kibertér stratégiájával foglalkozó tanulmány (Hakala és Melnychuk 2021) illetve különböző iparági jelentések és elemzések megállapításait dolgozom fel. A központ szakértőinek véleménye szerint Oroszország az információs konfrontációk során az állami hírszerző ügynökségekhez köthető állami szereplőket, illetve közreműködőket (proxy) alkalmaz, amelyeknek az irányítása jóval decentralizáltabb képet mutat a szovjet időkhöz képest. Az orosz hírszerző ügynökségek tevékenységét három fő karakterisztika jellemzi: egyrészt elsődleges prioritást élvez a rezsim megóvása megelőző műveletekkel; másrészt elkötelezettek az erőforrásokért és a Kreml kegyeiért zajló „hírszerző versengésben”; harmadrészt nem csupán a döntéshozatal, hanem a közvetlen cselekvés eszközeiként tekintenek magukra. Az egyik legerőteljesebb szervezet a Szövetségi Biztonsági Szolgálat (Federal Security Service – FSB), amely – a KGB utódjaként – eredetileg hazai fókusszal rendelkezik a kémelhárítás terén, de gyakran hajt végre külföldön műveletet és végez hírszerző tevékenységet a kibertérben, miközben erősen érintett a kiberbiztonsági és offenzív információs műveletekben (Galeotti ,2016). Az orosz

információs tér védelmében betöltött szerepe kapcsán számos állami szervezettel működik együtt a lehallgatások és az orosz adatforgalom megfigyelése során, amiben minden internet szolgáltató köteles részt venni.

Ez a leírás sok más ország elhárításával kapcsolatban elmondható lenne, azonban nyugati elemzők régóta az FSB-hez kötik az egyik legkifinomultabb, Turla[65] névre keresztelt APT-t, ami a többi orosz hátterű APT-hez képest is kiemelkedik a célpontok kiválasztása és a műveletek időtartama terén. Jellemzően stratégiai jelentőségű személyeket és szervezeteket támad a katonai, diplomáciai és kormányzati szektorban (ESET, 2019), de akadémiai, telekommunikációs, nem állami és nonprofit, valamint repülőipari szervezetek is célponttá váltak az elmúlt évek során, legalább 42 országban, köztük Magyarországon is (CrowdStrike, 2022a). Több nyilvános forrás is olyan nagy horderejű műveleteket tulajdonít a Turlanak, mint az Amerikai Egyesült Államok Központi Parancsnokságát 2008-ban, a Finn Külügyminisztériumot 2013-ban, a Németország Szövetségi Külügyi Irodáját 2017-ben, illetve a Francia Haderőt 2018-ban érintő kiberbiztonsági incidensek (ESET, 2019). Ugyanakkor a hagyományosan 2007 óta aktívnak tartott változatos támadási vektorokat (Kaspersky, 2014), folyamatosan változó eszköztárat (Bartholomew, 2017), illetve figyelemre méltó kiszivárogtató (Tanase, 2015) és megtévesztő technikákat (Bartholomew és Guerrero-Saade, 2016) alkalmazó Turlát összefüggésbe hozták a világ egyik első, széles körben ismertté vált Moonlight Maze névre keresztelt kibertámadásával is, amit még 1996-ban indítottak az amerikai hadsereg, az űrügynökség és energetikai szervezetek ellen (Rid és mtsai., 2018). Az Oroszországnak tulajdonított elit kiberműveleti képességeket felvonultató Turla FSB-hez fűződő kapcsolatáról német oknyomozó riporterek jelentettek meg bizonyítékokkal alátámasztott elemzést (Tanriverdi, Flade, és Frey 2022), ami alapján kirajzolódnak a személyi kapcsolatok, illetve az infrastrukturális és szakmai háttér biztosításának elemei.

A jelek szerint azonban az FSB mellett az orosz fegyveres erők vezérkarának Felderítő Főcsoportfőnöksége (Main Intelligence Directorate of the General Staff of the Armed Forces of the Russian Federation – GRU) – ami lényegében a katonai hírszerzés – szintén meghatározó szerepet tölt be az offenzív kiberműveletek során. Az elérhető információk alapján a szervezeti struktúrában a 85. Különleges Szolgálati Főközpont (Unit 26165) és a Különleges Technológiák

[65] A Turla APT további ismert azonosítói: Snake, Uroburos, Venomous Bear, Group 88, Waterbug, WRAITH, Pfinet, TAG_0530, KRYPTON, Hippo Team, Pacifier APT, Popeye, SIG23, Iron Hunter, White Bear, Belugasturgeon, MAKERSMARK, Bővebben: https://malpedia.caad.fkie.fraunhofer.de/actor/turla_group

Főközpont (Unit 74455) alkotja a technikai képességeket. Előbbi a jelfelderítés[66] és kriptográfia területén, utóbbi a számítógépes műveletekért felel. Ezt egészíti ki a 72. Különleges Szolgálati Központ (Unit 54777), amely a pszichológiai hadviselési elemet biztosítja az információs műveletekhez (Lilly és Cheravitch, 2020). A GRU által végrehajtott műveletnek tulajdonítják többek között az amerikai elnökválasztás 2016-os megzavarására és befolyásolására irányuló tevékenységeket, több ukrán infrastruktúrát érő kibertámadást (Mueller, 2019) és a NotPetya[67] zsaroló vírust (DOJ US, 2020). A 74455-ös egység főként Sandworm[68] néven vált ismertté és 2009 óta követett tevékenységével az egyik leginkább destruktív aktornak számít. A legalább 2004 (FireEye, 2014) óta aktív 26165-ös egység legelterjedtebb azonosítója a Fancy Bear[69], vagyis az APT28 (EU, 2020b), amelyet amellett, hogy meglehetősen részletes adatok alapján szintén az amerikai választások elleni műveletekhez (DOJ US, 2018) kötnek, többek között összefüggésbe hoznak az EBESZ elleni 2016-os, a NATO elleni 2015-ös és a Kirgizisztán Külügyminisztériuma elleni 2014-es műveletekkel (FireEye, 2017) is.

Az orosz kiberműveleti képességek harmadik jelentős szereplője a Külföldi Hírszerző Szolgálat (Foreign Intelligence Service – SVR), ami főként humán és stratégiai polgári hírszerző feladatai során hagyományos kémkedési tevékenységet végez más államok politikai céljaink kifürkészésére és az orosz geopolitikai érdekek elősegítésére (Weedon, 2018). A nyíltan hozzáférhető források a szervezet által végrehajtott kiberműveleteket Cozy Bear[70], vagyis APT29 azonosítóval illetik, aminek célpontjai között megtalálható legalább 19 ország, köztük Magyarország akadémiai, energetikai, pénzügyi, kormányzati, média és technológiai szektorában érintett szereplők mellett,

[66] Jelfelderítés, vagy más néven rádióelektronikai felderítés (Signal Intelligence – SIGINT), amelyet a hirszerzési elméletekkel foglalkozó szakirodalom jellemzően további két részre oszt, a távközlési- vagy rádiófelderítésre (Communication Intelligence – COMINT), illetve a rádiótechnikai felderítésre (Electronic Intelligence – ELINT). Előbbi az ember és ember közötti kommunikációval foglalkozik, míg utóbbi a gép és gép közötti, leginkább elektromágneses alapú felderítő tevékenységet jelenti.

[67] A NotPetya minden idők egyik leginkább destruktívnak tartott számítógépes kártevője, amely 2017. június 27-én látszólag zsarolóvírusként szabadult el, de gyorsan kiderült róla, hogy nem a váltságdíjakon keresztüli haszonszerzésre fejlesztett szoftverről van szó. A becslések szerint a NotPetya által okozott károk meghaladják a 10 milliárd USD-t.

[68] A Sandworm néven ismert APT további azonosítói: Telebots, Voodoo Bear, Iron Viking, ELECTRUM, BlackEnergy (Group), Quedagh, TEMP.Noble, Bővebben: https://malpedia.caad.fkie.fraunhofer.de/actor/sandworm

[69] A Fancy Bear néven ismert APT további azonosítói: Sofacy, Pawn Storm, STRONTIUM, Tsar Team, Threat Group-4127, TG-4127, Sednit, Group 74, Swallowtail, SNAKEMACKEREL, TAG_0700, IRON TWILIGHT, SIG40, apt_sofacy, Bővebben: https://malpedia.caad.fkie.fraunhofer.de/actor/sofacy

[70] A Cozy Bear néven ismert APT további azonosítói: YTTRIUM, CozyCar, CozyDuke, The Dukes, IRON HEMLOCK, NobleBaron, Dark Halo, StellarParticle, NOBELIUM, UNC2452, Office Monkeys, Group 100, EuroAPT, Cozer, Minidionis, SeaDuke, Hammer Toss, Grizzly Steppe, Bővebben: https://malpedia.caad.fkie.fraunhofer.de/actor/apt_29

a repülőiparban, a kitermelésben, biztosításban, gyógyszeriparban, illetve a mérnöki szolgáltatásokban tevékenykedő szervezetek (CrowdStrike, 2022b). A kiemelkedő szakértelmet igénylő kifinomult eljárásokat alkalmazó és komplex infrastruktúrát működtető (Weedon, 2018) APT29-et szintén összekötik a 2016-os amerikai elnökválasztás elleni műveletekkel (NCCIC, 2016), norvég kormányzati szerveket (Pijnenburg Muller és mtsai., 2018) és a holland választásokat (Ruwhof, 2017) érintő kiber incidensekkel, de a 2020-as rendkívüli jelentőségű SolarWinds[71] néven ismertté vált incidenssel is (CISA, 2021). Az alkalmazott eszközökkel és eljárásmódokkal kapcsolatban megjelenő kutatásokra drasztikus gyorsasággal képes reagálni és módosításokat végrehajtani, hogy kikerülje az észlelést és visszaszerezze a rejtett működést (F-Secure, 2020).

Miközben az orosz hátterűnek tartott APT-k közötti kapcsolatokat feltérképező kutatás (Bassat és Cohen, 2019) azt mutatta ki, hogy a fenti szereplőkre nem jellemző a saját eszközeik egymás között történő megosztása, egyelőre arra is kevés bizonyíték van, hogy az olyan oroszpárti szeparatista, illetve hacker csoportok, mint a CyberBerkut[72] kapcsolatban állnak az orosz kormánnyal (Maurer, 2015). A GRU-val ennek ellenére gyakran összefüggésbe hozott hazafias érzelmű hackereknek titulált csoport jellemzően technikai és propaganda, valamint pszichológiai támadásokban vesz részt szolgáltatás megtagadás elérésével vagy meghamisított dokumentumok terjesztésével azzal a céllal, hogy demoralizáljon, illetve zavart és bizalmatlanságot keltsen (DIA, 2017). A csoport más hazafias hackerekhez hasonlóan nem része a hivatalos állami gépezetnek, ahogy azok a kiberbűnözők sem, akiket előszeretettel alkalmaz (Maurer és Hinck, 2018) az orosz kormányzat a tagadhatóság és költséghatékonyság jegyében (Connell és Vogler, 2017).

III.3.2 Kína kibertéri aktivitásának főszereplői

A rendelkezésre álló információk alapján a Kínai Népköztársaság esetében hangsúly eltolódás látszik a haderő és a nemzetbiztonsági ágazat kiberképességekben betöltött szerepére vonatkozóan az orosz megoldással összevetve. Az elemzés Desmond Ball kínai kiberhadviselési képességekről szóló átfogó tanulmányán (Ball, 2011), illetve hivatalos dokumentumokon és iparági jelentéseken

[71] A SolarWinds egy amerikai üzleti szoftverek fejlesztésére szakosodott texasi központú vállalat. A mintegy 300 ezer ügyféllel rendelkező cég számítógépes hálózati, rendszer és információ technológiai infrastruktúrák kezelését és üzemeltetését segítő szoftvereket gyárt.

[72] A CyberBerkut egy oroszpárti hacktivistákból álló csoport elnevezése, amely jellemzően elosztott túlterheléses támadásokat hajt végre ukrán kormányzati célpontok, illetve ukrán és nyugati cégek weboldalai ellen.

alapul. Kína 1995 óta rendelkezik információs hadviselési tervvel. 1997 áprilisában a Központi Katonai Bizottság (Central Military Commission – CMC) nagyjából száz fős elit egységet hozott létre, hogy amerikai és nyugati országok számítógépes rendszereihez hozzáférést találjanak. 2000-ben megalakult a kínai stratégiai információs hadviselésre szakosodott (az Egyesült Államok által 'Net Force'-nak nevezett) egység, majd 2010 nyarán létrehozták a Népi Felszabadító Hadsereg (People's Liberation Army – PLA) Vezérkarának alárendeltségében az Információs Támogató (Biztosító) Bázist (Information Support (Assurance) Base) (Stokes, Lin, és Hsiao, 2011), ami nagy valószínűséggel egy korabeli számítógépes hálózatvédelmi és műveleti központként funkcionált (Ball, 2011). A kínai haderő átfogó reorganizációjának egyik eredményeként 2015-ben megalakult a Stratégiai Támogató Erő (Strategic Support Force – SSF) névre keresztelt – „információs ernyőként" működő (Kania, 2017) – magasabb (haderőnem) szintű katonai szervezet, amely egyfelől a műholdak fellövéséért és üzemeltetéséért felelős, másfelől a kiber- és elektronikai hadviselés is itt kapott helyet (Pollpeter, Chase, és Heginbotham, 2017). Az elemzők azt valószínűsítik, hogy a kínai kiberhadviselési egységek aktivitása 1999-től detektálható és a kezdetekben főleg tajvani, japán és amerikai weboldalak ellen intéztek alapszintű weboldal rongálási, illetve felülírási (defacement) és elosztott szolgáltatás megtagadásos (DDoS) támadásokat. A támadások kifinomultsága 3 éven belül növekedni kezdett, ekkor már trójai programokat alkalmaztak információk megszerzésére. A számítógépes és hálózati támadó küldetéseket az elektronikai hadviseléssel együtt az Integrált Hálózati és Elektronikai Hadviselés (Integrated Network Electronic Warfare – INEW) tevékenység alatt konszolidálták (IISS, 2019), amiért a Vezérkar 4. Elektronikai Elhárító (Electronic Countermeasures Department – ECD) részlege felel. A számítógépes hálózatvédelem a kiberkémkedési tevékenységgel együtt a 3. Jelfelderítő (Signals Intelligence) részleghez került (Ball, 2011). Utóbbihoz meg nem erősített információk szerint 130 ezer fős állomány tartozik a főparancsnokságon kívül 12 műveleti irodához és három kutatóintézethez beosztva (Stokes, Lin, és Hsiao, 2011). Az elektronikai elhárító tevékenység legalább 4 irodát, egy dandárt és két ezred szintű egységet foglal magába.

Az irodák mögött található, sorszámmal jelölt katonai egységek[73] közül többet is olyan fejlett perzisztens fenyegetésekkel hoznak összefüggésbe, amelyek az elmúlt évek során a kínai

[73] A kínai haderőben a katonai egységeket fedő azonosítóval (Military Unit Cover Designator – MUCD) látják el, így a magyar haderőben is elterjedt – az alárendeltségi viszonyt is gyakran magába foglaló – hosszú alakulat nevek, mint például „MH 2. vitéz Vattay Antal Területvédelmi Ezred 10. Majthényi Károly Területvédelmi Zászlóalj" vagy „MH vitéz Szurmay Sándor Budapest Helyőrség Dandár 32. Nemzeti Honvéd Díszegység" helyett egyszerű, jellemzően öt

kiberműveleti képességek jelentős fejlődésére utalnak. A 61398 számú egységet például az APT1[74] tevékenységével hozzák összefüggésbe (Mandiant, 2013), ami 2006 óta 141 országban mintegy 20 iparágra kiterjedően, előre definiált metodológia mentén jelentős mennyiségű szellemi tulajdonnal kapcsolatos információt szerzett meg tervrajzokhoz, gyártási folyamatleírásokhoz, teszteredményekhez, üzleti tervekhez, árazási dokumentációkhoz, együttműködési megállapodásokhoz és az áldozatok elektronikus levelezéséhez, illetve kapcsolati listájához történő hozzáféréssel. A tevékenység rejtésének és a kifinomultságnak köszönhetően két hónap híján akár öt éven keresztül képes volt észrevétlen maradni a jellemzően az angolt anyanyelvként, illetve munkanyelvként használó áldozatok hálózatán, más esetben pedig több mint 6 terrabájtnyi adatot sikerült megszerezni tíz hónap leforgása alatt. Az ezernél is több szervert magába foglaló támadó infrastruktúrához kapcsolódó IP címek, domén nevek és visszafejtett támadó kódok mindegyike arra utal, hogy kínai aktor áll a háttérben (Mandiant, 2013).

A PLA egy másik alakulatát, a 78020 számú egységet a rendelkezésre álló nyílt információk alapján szintén összefüggésbe hozzák a Naikon[75] névre keresztelt fejlett perzisztens fenyegetéssel. Az egység mandátuma vélhetően kiterjed a regionális számítógépes hálózati műveletekre, rádiójelfelderítésre és politikai elemzésre a Délkelet-Ázsiával határos nemzetek kapcsán, azon belül is azokra, amelyek az energiahordozókban gazdag Dél-kínai-tenger területi vitáiban érintettek (Blue Horn, 2015). A legalább 2010 óta aktív tevékenység kormányzati, katonai, média és energetikai szereplőket céloz jellemzően Mianmar, Vietnám, Szingapúr, Laosz, Malajzia, és a Fülöp-szigetek területén. Az alkalmazott eszközök országspecifikusak és ötletesek, miközben elterelő megoldásokat is alkalmaznak (ThreatConnect, 2014). Hasonlóan specifikált feladatokkal rendelkezik a kínai haderő több alakulata is, a 61786 számú egység számítógép hálózati műveletek adminisztratív és hálózatbiztonsági tevékenységet folytat, a 61785 számú egység rádiókommunikációs és elektronikus jelkibocsátási ellenőrző feladatokat lát el, a 61419 számú egység főként kelet-ázsiai célpontokra specializálódott, a 61565 számú egység orosz célpontokat támad, a 61046 számú egység az európai, közel-keleti és latin-amerikai régióban aktív, a 61221

karakterből álló számsort használnak, mint például „61398”. Ez az alakulat a PLA vezérkar 3. részlegének alárendeltségébe tartozó 2. egység.

[74] Az APT1 további ismert azonosítói: Comment Crew, Comment Group, Comment Panda, PLA Unit 61398, Byzantine Candor, Group 3, TG-8223, Brown Fox, GIF89a, ShadyRAT, Shanghai Group, Bővebben: https://malpedia.caad.fkie.fraunhofer.de/actor/comment_crew

[75] A Naikon további ismert azonosítói: PLA Unit 78020, APT30, Override Panda, Camerashy, APT.Naikon, Lotus Panda, Hellsing, BRONZE GENEVA, https://malpedia.caad.fkie.fraunhofer.de/actor/naikon

számú egység stratégiai hírszerzést, elemzést mellett eszköz üzemeltetést és adatbázis kezelést végez, a 61886 számú egység elsősorban közép-ázsiai és orosz nukleáris, illetve rakéta képességeket figyel meg a kibertéren keresztül, a 61672 számú egység az orosz célpontok mellett kiber bűnüldözéssel foglalkozik, míg a 61486 számú egység feladata a műholdas kommunikációhoz és az űrtelepítésű eszközökhöz kapcsolódó rádiójelfelderítés (Stokes, 2015). Az egységet iparági elemzések összefüggésbe hozzák a PUTTER PANDA néven ismert fejlett perzisztens fenyegetéssel, ami legalább 2007 óta aktív a kormányzati, a védelmi, a kutatási és a technológiai szektorokban főként amerikai és európai országokban (CrowdStrike, 2014).

A kínai kiberműveleti képességek terén eltérő viszonyt és szerepkört vet fel az APT41[76] néven ismert aktor (Mandiant, 2022b). Az elemzői feltételezések szerint az APT41 mögött álló személyek nem állami alkalmazottak, sokkal inkább vállalkozói, illetve beszállítói jellegű kapcsolatban[77] állnak a kínai kormánnyal. A duális, kiberbűnözői és kiberkémkedési tevékenységet vélhetően teljes időbeosztással (full-time) megvalósító személyek célpontjai között megtalálható Hong Kong, Tajvan, Japán, Ausztrália, Mongólia, Mianmar, Vietnám, Makaó és Bahrein, az Egyesült Államok, Dél-Korea, illetve Kuvait is. Iparági bontásban főként a kormányzati, a média és videójáték, a telekommunikációs, az akadémiai és a közlekedési, illetve szállítmányozási szektorból kerülnek ki az áldozatok (NTT, 2021). Bár a tevékenységre kifinomult módszerek és technikai megoldások (Novetta, 2015) jellemzők, az alkalmazott eszközök kódjában bőven találhatók nyílt forrású elemek, illetve több eszköz kódja más fenyegetések és tevékenységek esetén is beazonosításra került, ami alapján az elemzők arra következtetnek, hogy széleskörű a tudásmegosztás, illetve egy nagyobb szervezet része lehet az APT41 (ThaiCERT, 2022). Olyan elemzés is van, amelyik szerint nem lehet a tevékenység kapcsán egyetlen aktort sem egyértelműen azonosítani, sokkal inkább egy megközelítésről van szó, amit több szereplő is magáénak tud (BlackBerry, 2020). További, a nem állami szereplő kategóriába sorolhatók azok az egyetemi hallgatói és hazafias hacker csoportok, amelyek tevékenységének előmozdításában jelentős szerepet játszik a PLA. Ez mintegy 250 hazafias hacker csoportot és 30 ezer kínai állampolgárt jelent a feltételezések szerint, miközben

[76] Az APT41 további ismert azonosítói: Axiom, Winnti Umbrella, Winnti Group, Suckfly, Group 72, Blackfly, LEAD, WICKED SPIDER, WICKED PANDA, BARIUM, BRONZE ATLAS, BRONZE EXPORT, Red Kelpie, Bővebben: https://malpedia.caad.fkie.fraunhofer.de/actor/axiom

[77] Az angolszász terminológiában a "contractor" kifejezés alá sorolják azokat a személyeket és szervezeteket, akik nem állnak közvetlen munkaadói, illetve munkavállalói kapcsolatban, helyette jellemzően zárt határidejű szerződésben rögzített feltételek határozzák meg a felek jogait és kötelezettségeit a közösen folytatott tevékenység során. Jellemzően szolgáltatások nyújtása és igénybevétele, illetve beszállítói tevékenység valósul meg ilyen formában.

Kína az államilag elkötelezett telekommunikációs nagyvállalatai (pl.: Huawei, ZTE) segítségével is igyekszik bővíteni kiberkémkedési rendszerét (Tewari, 2019).

III.3.3 Az Amerikai Egyesült Államok kibertevékenységének végrehajtói

Az államok kiberképességeinek elemzésekor, különös tekintettel a fejlett perzisztens fenyegetések vizsgálatára, erős determinisztikus hatás figyelhető meg. Európában ülve, a nyelvi korlátok okán főként angol és magyar nyelvű forrásokra támaszkodva erős nyugati dominancia érezhető a fenyegetések és a hozzájuk kapcsolt államok tekintetében, amit tovább erősít, hogy a kiberbiztonsági iparág fenyegetések kutatására szakosodott szegmenségben az amerikai és európai szervezetek uralkodó szerepet (Gomez, 2022) töltenek be. Ennek eredményeként, a hagyományos kelet-nyugati megosztottság és szembenállás nyomán az orosz, kínai, iráni vagy épp észak-koreai képességekhez és APT-khez képest a nyugati országok, így az Amerikai Egyesült Államok képességei jóval kevésbé dokumentáltak a nyíltan elérhető forrásokban.

Azonban az elmúlt évtized során több olyan esemény is történt, ami segíti a képalkotást az amerikai kiberképességekkel kapcsolatban. A hírhedt 2013-as Snowden[78] szivárogtatás, illetve a 2016-ban Shadow Brokers[79], majd 2017-ben Vault 7[80] néven nyilvánosságra kerülő dokumentumok betekintést engedtek az amerikai képességekbe. A kiberbiztonsági szakértői közösségben az Egyesült Államok Nemzetbiztonsági Ügynöksége (National Security Agency – NSA) által birtokolt kiberképességnek szokás tekinteni az Equation Group[81] névre keresztelt fejlett perzisztens fenyegetést. Annak ellenére, hogy a közvetlen kapcsolatot explicit módon a vizsgálatok nem írják le, az Equation Group és a rosszindulatú Stuxnet és Flame szoftvereket programozó csapat közötti feltételezett kapcsolat, illetve a célpontok, a motiváció és a kiszivárgott

[78] Edward Joseph Snowden 1983-ban született és számítógépes hírszerzési tanácsadóként dolgozott a Központi Hírszerző Ügynökség (CIA), a Dell és Booz Allen Hamilton vállalatoknak, illetve 2013-ban az amerikai Nemzetbiztonsági Ügynökségnek (NSA), amikor nagy mennyiségű minősített információt hozott nyilvánosságra. Ennek nyomán vált egyértelművé a világ számára, hogy az NSA, az Ötszem Hírszerző Szövetséggel (Five Eyes Alliance), telekommunikációs vállalatokkal és európai kormányokkal együttműködve olyan globális megfigyelési programokat működtet, amelyek súlyos kérdéseket vetnek fel a nemzetbiztonság és a magánszféra sérthetetlenségével kapcsolatban.

[79] A Shadow Brokers nevet használta az a szereplő, aki 2016 augusztusában, a feltételezések szerint egy az NSA-hez köthető kiberműveletekhez használt eszköztárról hozott nyilvánosságra információkat, beleértve magát a forráskódot, illetve nulladik napi sérülékenységeket.

[80] Vault 7 néven vált ismerté 2017 márciusában az a dokumentum csomag, amit a WikiLeaks nevű szervezet tett közzé és részletes információkat tartalmaz a CIA kibertérben folytatott tevékenységéről és kiberképességeiről.

[81] Az Equation Group további ismert azonosítói: Longhorn, PLATINUM TERMINAL, EQGRP, Lamberts, Tilded Team, APT-C-39, Bővebben: https://malpedia.caad.fkie.fraunhofer.de/actor/equation_group

dokumentumok alapján arra lehet következtetni, hogy a népes amerikai hírszerző közösség[82] egy domináns szereplője szignifikáns kiberműveleti képességekkel rendelkezik. Az Equation Group tevékenységével és eszköztárával részletesen foglalkozó elemzések szerint az alkalmazott technikák komplexitása és kifinomultsága terén minden eddig ismertet felülmúl. Részben az elnevezés is onnan ered, hogy magas szintű titkosítási algoritmusokat és elterelő metódusokat alkalmaznak olyan taktikákkal, technikákkal és folyamatokkal kombinálva, amelyek kifejlesztése és működtetése jelentős erőforrásokat követel, ami kormányzati szerepvállalásra utal (Kaspersky, 2015b). A rendelkezésre álló információk alapján az Equation Group célpontjai között kormányzati és diplomáciai intézmények mellett a telekommunikációs, a repülőipari, az energetikai, a nukleáris kutatási, az olaj és gáz, a katonai, a nanotechnológiai, a közlekedési és a pénzügyi szektorok mellett iszlamista aktivistákat és tudósokat, a tömegtájékoztatást és kriptográfiai technológiákat fejlesztő szervezeteket is találunk. Az APT eddigi célpontjai Iránról és Oroszországtól kezdve Afganisztánon, Irakon, Mexikón és Szudánon át egészen Németországig terjednek. Több mint 30 országban, mintegy 500 célpont beazonosítása történt meg (Paganini, 2015). Bár az Equation Groupnak tulajdonított rosszindulatú szoftverek mintái alapján azokat először 2002-ben állították össze, a C2 infrastruktúra elemeit 2001-ben, bizonyos esetekben pedig még 1996-ban regisztrálták, ami arra enged következtetni, hogy olyan szereplőről van szó, amelyik már 1996-ban is aktív volt (Kaspersky 2015a). A Snowden aktákból megismert rosszindulatú szoftverek és az Equation Group által használt szoftverek kódjában az elemzőknek több hasonlóságot és összefüggést is sikerült kimutatni, akárcsak a műveletek során kihasznált nulladik napi sérülékenységek[83] tekintetében. Ez alapján valószínűsitik, hogy az NSA egyik speciális tevékenysége, a Célzott Hozzáférési

[82] Az Amerikai Egyesült Államok Hírszerző Közössége (US Intelligence Community – IC) azt a 17 kormányzati titkosszolgálatot tömöríti, amelyek különböző felelősségi területen és alárendeltségben, de egyformán az USA külpolitikai és nemzetbiztonsági érdekeit szolgálva létfontosságú adatgyűjtő, elemző és értékelő tevékenységet folytatnak. Az IC-t az Egyesült Államok elnöke által kinevezett és közvetlen alárendeltségébe tartozó Nemzeti Hírszerzési igazgató vezeti.

[83] Nulladik napi (zero-day) sérülékenységnek (vulnerability) nevezzük azokat a számítógépes szoftver sérülékenységeket, amelyek ismeretlenek a szoftver készítői és üzemeltetői számára. Egy sérülékenység a felfedezést követően addig marad nulladik napi, amíg a javítást (patch) kiadják hozzá. Az ilyen sérülékenységek köré az utóbbi években kialakult egy piac, ahol kereskednek velük, miközben a sérülékenységek kihasználására készített megoldásokat (exploit) a legális felhő szolgáltatások mintájára már fizetős szolgáltatásként (Exploit-as-a-Service – EaaS) is igénybe lehet venni. Bővebben: https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmwcb-report-detecting-and-responding-to-zero-day-attacks.pdf

Műveletek (Tailored Access Operations – TAO)[84] területe, illetve szervezeti egysége áll az Equation Group akciói mögött.

Az APT-k elnevezése körüli kaotikus viszonyok egyik iskolapéldája is lehetne az amerikai képességek attribúciójában tapasztalható átfedés, különösen a Vault 7 keretén belül 2017-ben nyilvánosságra került dokumentumok nyomán. Bár az Equation Group több ismert azonosítóval is rendelkezik, mint például a Longhorn és az APT-C-39, bizonyos elemzők (Qihoo 360, Secureworks) és nyilvántartások (Malpedia) úgy kapcsolják össze ezeket, hogy utóbbiakat az Amerikai Egyesül Államok Központi Hírszerző Ügynökség (Central Intelligence Agency – CIA) offenzív tevékenységet folytató részlegének tulajdonítják. Elemzők arra a következtetésre jutottak, hogy a Longhorn néven azonosított tevékenységek számos ponton hasonlóságot mutatnak a CIA kiszivárgott dokumentumaiban található eszközökkel, technikákkal és eljárásokkal (Paganini, 2017). A Longhorn számlájára legalább 40 célpontot írnak 16 közel-keleti, európai, ázsiai és afrikai országban (Johnson, 2017), illetve a feltételezések szerint legalább 2009 óta folytat kiber tevékenységet Kínával szemben (Quihoo 360, é. n.). Az elérhető nyílt információk alapján a CIA Műveleti Igazgatóságán (Directorate of Operations – DO) belül, illetve a Nemzeti Titkosszolgálatnak (National Clandestine Service – NCS) is nevezett keretek között kaptak helyet azok a hírszerző feladatok, amelyek teljesítéséhez egy jól ellátott szereplő kifinomult kiberműveleti képességei társulnak (Quihoo 360, é. n.).

Az amerikai kiberműveleti képességek terén a nemzetbiztonsági szektor mellett egyre prominensebb szerepet tölt be a Védelmi Minisztérium (Department of Defense – DoD) és az alá tartozó parancsnokságok közül a kezdeti műveleti képességet 2010-ben elérő Kiber Parancsnokság (Cyber Command – USCYBERCOM), amelynek parancsnoka mindenkor egy négy csillagos tábornok, aki a szabályok értelmében kialakított „kétsapkás" rendszer következtében egyúttal az NSA főigazgatói pozícióját is betölti (Cyber Command, é. n.). A USCYBERCOM alá négy haderőnemi (szárazföldi haderő, légierő, haditengerészet, tengerészgyalogság), kiber specifikus parancsnokság tartozik, amelyek az egyesített erőkkel végrehajtott műveleti megközelítés okán a

[84] A Célzott Hozzáférési Műveletek Irodája az NSA Jelfelderítési (SIGINT) Igazgatóságának egyik egysége, amely a 2013-as Snowden szivárogtatás idején több mint ezer fős hivatásos és civil állománnyal, úgynevezett CNE operátorral (Computer Network Exploitation) rendelkezett. Az egység a marylandi Fort Meadeben található NSA főhadiszálláson egy ultramodern központot (Remote Operations Center – ROC) üzemeltet 24 órában a távoli műveletek irányítására és emellett több kisebb egységgel is jelen van az NSA SIGINT központjaiban. Bővebben: https://foreignpolicy.com/2013/06/10/inside-the-nsas-ultra-secret-china-hacking-group/ és https://www.washingtonpost.com/news/the-switch/wp/2013/08/29/the-nsa-has-its-own-team-of-elite-hackers/

Kiber Missziós Erő (Cyber Mission Force – CMF) útján más parancsnokságoknak is támogatást nyújtanak, mint például a Különleges Műveleti Parancsnokság (Special Operations Command – USSOCOM). A USCYBERCOM alárendeltségében létrehozott CMF három típusa a Nemzeti Missziós Erő (National Mission Force – NMF), a Harci Missziós Erő (Combat Mission Force – CMF) és a Kibervédelmi Csapatok (Cyber Protection Teams – CPT), amelyekből összesen 133 van és 2018-ban érték el a teljes műveleti képességet akkor mintegy 5000 fős állománnyal, ami azóta majdnem eléri a 6200 főt. A Kiber Nemzeti Missziós Erő (Cyber National Mission Force – CNMF), illetve az Összhaderőnemi Főhadiszállás – DoD Információs Hálózatok (Joint Force Headquarters-DoD Information Network – JFHQ-DoDIN) két olyan komponens, amelyek közül az előbbi a kibertéri műveletek során az elrettentésre, megzavarásra és az ellenfelek legyőzésére fókuszál, míg utóbbi küldetése a Védelmi Minisztérium hálózatainak napi szintű felügyelete és aktív védelmének ellátása akár az ellenfél semlegesítésével, amennyiben az átjutott a határvédelmi megoldásokon (Cyber Command, é. n.). A USCYBERCOM 2021 február és március között hajtott végre – főként a Légi Nemzeti Gárda (Air National Guard – ANG) alakulataiból létrehozott különítménnyel – olyan offenzív kiber hatást kiváltó műveletet valódi kiberfenyegetéssel szemben, amit jelentős érdeklődés övezett. A művelet pontos természetéről és célpontjáról nem hoztak nyilvánosságra információkat, de a Védelmi Minisztérium információs rendszereinek biztonsága érintett volt, a művelet jelentőségét pedig az jelzi, hogy a védelmi miniszter személyesen is megtekintette (Tingley, 2022).

Összegzés, következtetések

A III. fejezet első alfejezetében előbb hazánk nemzetközileg feldolgozható stratégiai dokumentummal rendelkező szomszédainak, néhány igazoltan fejlett kiberképességekkel rendelkező kisállamnak, illetve nagyhatalmi szereplőnek a kiberstratégiáját vizsgáltam meg. Arra kerestem a választ, hogy miként jelennek meg a kiberműveleti képességek a nyilvános politikai dokumentumok felső szintjén. Ezután a III.2 alfejezet behatóan vizsgálta a kiberműveleti képességek teljes spektrumát, a passzív és az aktív kibervédelem, valamint az offenzív kiberképességek analizálásával. Ezzel az volt a cél, hogy meghatározhatóak legyenek a kiberműveleti tevékenységek védekező és támadó aspektusai. A III.3 alfejezetben az orosz, a kínai és az amerikai esettanulmányokkal a kiberműveleti képességek empirikus példákkal történő

igazolása volt a cél, illetve a tanulmányokkal rá tudtam mutatni a kiberműveleti képességek megközelítésében azonosítható eltérésekre is.

A biztonságpolitikai elemzések egyik alapvető szegmense a vonatkozó stratégiai dokumentumok áttekintése és értékelése a vizsgált témakör szempontjai alapján. Jelen esetben a nemzeti kiberbiztonsági stratégiák kiberműveleti képességekre vonatkozó cikkelyei nyújtották a kiindulási pontot. A feldolgozás szempontjából nehézséget jelentett az orosz és a kínai stratégia. Ezekből egyfelől a nyelvi korlátok miatt kevésbé pontos információk nyerhetők ki, amin az angol nyelvű fordítások a terminológiai pontatlanságok miatt érdemben nem segítenek. Másfelől az orosz és a kínai vezetés stratégiai elgondolásai kapcsán különösen igaz, hogy átfogó kép csak több dokumentum holisztikus vizsgálatával alkotható meg. Ugyanakkor a pontosabb helyzetkép kialakításához hozzájárul, a fejezet végén található két esettanulmány a kínai és az orosz kiberműveleti képességekről. Ettől függetlenül a kiberbiztonsági stratégiák áttekintésének eredményeként az látható, hogy az államok jellemzően nem adnak precíz információkat a kiberműveleti képességeikkel összefüggésben és a dokumentumok sok esetben nem tartalmaznak egyértelmű meghatározásokat az alkalmazott terminológiához. Így a stratégiai dokumentumok szintjén elmosódnak a határok a kibervédelem és a kiberműveletek különböző szegmensei, valamint alkalmazásuk körülményei között.

Miközben az orosz és a kínai stratégiák elemzésével kapcsolatos hiányosságok leküzdése túlmutatna az értekezés keretein, valószínűleg nem változtatna azon a következtetésen, miszerint pusztán a kiberstratégiák alapján nehéz, esetenként lehetetlen valós képet alkotni egy állam kiberműveleti képességeiről. Ha a vizsgált dokumentum említést tesz kiberműveleti képességekről, jellemzően nem derül ki, hogy pontosan milyen tevékenységek sorolhatók ide, illetve a katonai, rendvédelmi és nemzetbiztonsági szektorok közül melyik és milyen mértékben érintett? Míg legtöbb esetben a védelmi jelleg dominál stratégiai szinten, a nagyhatalmak és a kiber szempontból fejlettebb kisállamok kapcsán előfordul az offenzív képességek nevesítése, vagy az arra való direkt utalás. Van olyan állam, amely képességi szintje lehetővé teszi, hogy szövetségi rendszerben, így a NATO számára felajánljon offenzív kiberképességet (Ritter, 2018). Ezáltal nemzetközi szinten is megjelenhet a kiberműveleti képességek defenzív és offenzív alkalmazása (Maigre, 2022), azonban ezek részletei nem nyilvánosak, a vizsgált stratégiák túlnyomó része pedig óvatos

megközelítést alkalmazva, jellemzően a kiberműveleti képességek védelmi aspektusát hangsúlyozza.

Ugyanakkor a kiberműveleti képességek teljes spektrumának vizsgálata nemcsak ahhoz szükséges, hogy a stratégiák értelmezésével kapcsolatban megfogalmazott célkitűzés teljesülhessen, hanem a kiber különleges műveleti képességek kialakításának is fontos eleme. Tehát a kiberműveleti tevékenységek vizsgálatának célja egyfelől a stratégiák pontosabb értelmezése és precízebb értékelése, másfelől a kiberműveletek azon szegmensének meghatározása, amihez a hagyományos kibervédelemtől eltérő speciális feltételek szükségesek. A vizsgálat rávilágított, hogy léteznek olyan keretrendszerek, amelyek alkalmazásával leírhatók a kiberműveleti képességek egyes komponensei és meghatározhatók azok a technikai, illetve etikai aspektusok, melyek segítségével a defenzív és offenzív képességek szétválasztása abszolválható. Bár a passzív és aktív védelem, valamint az offenzív tevékenységek többnyire néhány paraméter alapján jól szétválaszthatók, sok esetben nincsenek éles határok. Ez különösen igaz a több elemből álló tevékenységek és műveletek esetében. Ezek alapján arra a következtetésre jutottam, hogy a végeredmény ilyenkor egy defenzív és offenzív elemeket egyaránt tartalmazó hibrid művelet lesz, amelyben a hagyományos kibervédelmi képességek mellett speciális képességek is megjelennek. A speciális vagy offenzív elemeket korlátozottan tartalmazó kiberműveletek jellegüket tekintve, a végső cél szempontjából lehetnek defenzívek, erre vonatkozóan nincs nemzetközileg elfogadott gyakorlat, szabvány vagy szabályozás. Tulajdonképpen ez az a bizonyos szürke zóna, amire egyes stratégiák utalnak és amiben egyre több állam igyekszik hatékonyan fellépni.

Ezt támasztják alá azok az esettanulmányok is, amelyek alapvetően Kína, az Egyesült Államok és Oroszország kiberműveleti képességeit mutatják be, azonban sajátos megközelítést alkalmazva egyúttal arra is rávilágítanak, hogy ezek a speciális állami kiberképességek a nemzetközi rendszer többi szereplője számára fejlett perzisztens fenyegetést jelentenek. A tanulmányokból levonható egy másik következtetés is, amely szerint ugyan vannak eltérések a kiberműveleti képességek megközelítésében, a kiberhatalmak jellemzően nagy hangsúlyt fektetnek arra, hogy a katonai és nemzetbiztonsági szektor is hatékony kiberműveleti képességeket alakítson ki. Az esettanulmányok segítségével megállapítottam, hogy multipoláris világunk három hangsúlyos geopolitikai szereplője időben felismerte a kibertér jelentőségét így évtizedes építkezést folytat a kiberműveleti képességek terén. Egyúttal feltártam, hogy bár nyílt körülmények között a

nemzetközi szabályozás kiterjesztését és fejlesztését szorgalmazzák, valójában a kibertér sajátosságait igyekeznek maximálisan kihasználni saját hatalmi törekvéseik és nemzeti érdekeik érvényesítésére.

A III. fejezet nyomán arra a következtetésre jutottam, hogy miközben a kiberbiztonsági stratégiákból sok esetben hiányoznak a kölcsönös megértést szolgáló elemek és korlátozott információkat tartalmaznak a kiberműveleti képességekkel kapcsolatban, a megvizsgált orosz, kínai és amerikai példák azt mutatják, hogy a stratégiák hiányosságai nem befolyásolják műveleti szinten a nemzeti kiberképességek fejlesztését. Véleményem szerint a kiberbiztonsági stratégiák nem alkalmasak a kiberműveleti képességek kapcsán precíz helyzetkép megalkotására, ehhez a legtöbb esetben további dokumentumok feldolgozása szükséges, amelyek azonban gyakran minősítettek, így nem hozzáférhetők az elemzői és kutatói körök számára. Továbbá megállapítottam, hogy a stratégiai dokumentumok szintjén a kiberműveleti képességekkel összefüggésben tapasztalható precizitás-hiányt nem lehet visszavezetni a kiberbiztonsági terület szakmai vagy tudományos elmaradására, mivel többféle megközelítés is alkalmazható a kiberműveletek teljes spektrumának, illetve defenzív és offenzív aspektusainak leírására és rendszerezésére.

IV. Kiberképességek és Fejlett Perzisztens Fenyegetések (APT)

Bevezetés

A reális veszély ellenére nem egyszerű feladat az APT-kkel kapcsolatos kutatásokhoz forrásokat találni. Ahogy azt egy montreáli szerző csapat is írja APT elemzésében (Lemay, 2018), egyrészről nem az információk hiányával, sokkal inkább a szétszórtságával van a probléma. Bár számos iparági jelentés, tudományos publikáció, szakmai blog bejegyzés és más dokumentáció érhető el, az eltérő források, a különböző megközelítés és taxonómia időigényessé teszi a feladatot, hogy globális képet alkossunk az APT-kről. Másrészről a legtöbb forrás alapvetően a védői oldal számára hasznos szempontok szerint foglalkozik az APT-k jelentette fenyegetéssel, ezért lényegesen nehezebb az offenzív aspektusok feltérképezése. A kifejezés legelőször egy 2007-ben az Amerikai Egyesült Államokban beadott szabadalmi beadványban tűnt fel (Schmidt, Rattray, és

Fogle, 2008). Az APT szakirodalommal foglalkozó ausztrál tanulmány szerzői elemzésük során arra jutottak, hogy bár eredetileg az állami támogatottság lehetősége feltételes volt, a médiába egyértelműen állami hátterű fenyegetésként került be az APT kifejezés (Ahmad és mtsai., 2019). Ennek oka, hogy a Northrop Grumman információbiztonsági vezetője egy 2008-ban adott interjú (Walsh, 2008) során a kifejezésről azt mondta, hogy az Amerikai Egyesült Államok Védelmi Minisztériuma kifejezetten nemzetállami fenyegetések vagy államilag támogatott támadások kapcsán használja a megnevezést, ami megfelelő erőforrásokkal ellátott, főként szellemi tulajdon és versenyelőny megszerzésére irányuló támadásokat jelent vállalatok és kormányok ellen. Egy iparági ismertető (Websense, 2011) megerősíti, hogy a Védelmi Minisztériumtól, pontosabban a légierőtől (United States Air Force – USAF) származik a kifejezés 2006-ból. A terminus technicus bevezetésének oka meglehetősen egyszerű. A Védelmi Minisztérium és a hírszerző közösség tagjai az adott fenyegetéseket és a mögöttük álló szereplőket különböző címkékkel és elnevezésekkel látják el, majd ezek segítségével hivatkoznak a konkrét tevékenységre vagy szereplőre. Azonban ezek az elnevezések sok esetben minősítettek, ezért a biztonsági átvilágítással nem rendelkező alkalmazottakkal és partnerekkel folytatott kommunikációhoz bevezetésre került az APT elnevezés.

IV.1 APT alapok és értelmezés

Ha kellő mennyiségű szakirodalmat olvasunk el, egy idő után azzal szembesülhetünk, hogy az APT kifejezéssel gyakran illetnek bizonyos támadói – vagy rendvédelmi terminológiával élve elkövetői – csoportokat (MITRE, é. n.). Ilyen esetben az APT után legtöbbször egy arab szám is áll, ami az adott csoportot hivatott beazonosítani. Más esetekben az APT kifejezéssel nem egy konkrét csoportra, vagy annak tevékenységére, hanem általánosságban az APT-k által alkalmazott eljárásokra és módszerekre utalnak. Ez legtöbbször az offenzív tevékenységek kapcsán már említett, a katonai terminológiából átvett keretrendszert jelenti, ami a harc megvívásának különböző fázisain – Cyber Kill Chain – alapul. Ezen felül az sem ritka, hogy egy konkrét támadásra – amiről kiderül, hogy tartósan fennálló, esetleg tervezett és szervezett jegyeket mutat a karakterisztikája – szintén rásütik az APT kifejezést (Grimes, 2019). Továbbá arra is van példa, hogy az APT-t lényegében csak egy eszközkészletnek (szoftverek és hálózati infrastruktúra)

tekintik, amit különböző szereplők felhasználhatnak céljaik eléréséhez (ESET, 2018). Ha egy pillanat erejéig nem a tudományos meghatározásra koncentrálunk, akkor a hétköznapi ember számára leginkább érthető módon Eric Cole[85] fogalmazta meg az APT jelenséget 2013-as, a témában megjelent könyvében (Cole, 2012). Cole az emberi rákos megbetegedéshez hasonlítja az APT-t és magyarázatában kitér arra, hogy az emberi testben kialakuló daganatos elváltozásokkal a legfőbb probléma, hogy a tradicionális vizsgálati módszerek nem működnek. Az észlelés valamilyen látható szimptóma alapján működik, amivel az a baj, hogy ha megvárjuk a látható jel kialakulását, már túl késő. A „kiber rák" – vagyis az APT – esetén ugyan ez a probléma, a hagyományos észlelési és reaktív intézkedések nem működnek. Az incidens időpontjában nincs látható jele annak, hogy a rendszer kompromittálódott és később mire a támadás jeleit felfedezik, a kár már bekövetkezett.

IV.1.1 Az APT-k paraméterei és sajátosságai

Az APT-k lényegét legegyszerűbben a paramétereik és sajátosságaik megismerésével lehet, amihez néhány kiválasztott meghatározást és leírást mutatok be. Cole szakmai szempontok alapján megfogalmazott definíciója szerint az APT egy olyan ellenfél – tipikusan más állam kormánya – amely a célba vett szervezetet megállás nélkül, a sikeres kompromittálódásig adat kinyerése és hosszú távú hozzáférés céljából támadja. Az APT kapcsán a kulcsszavak, a rejtett, a célzott, az adaptív és az adat fókuszált. Cole szerint az APT egyszerűen hangzik mégis gyakran félre értik a fejlett és a perzisztens kifejezéseket. Miközben a fejlett jelző miatt sokan a legkorszerűbb, szofisztikált támadásokra gondolnak, valójában az ellenfél szofisztikáltságáról van szó. Ez azt jelenti, hogy célzott támadásokat indítanak és arra koncentrálnak, ami működik, de az alkalmazott metódusok gyakran előfordulnak és szokványosak. Cole értelmezésében a perzisztencia arra utal, hogy a támadó nem megy el és egészen addig próbálkozik, amíg el nem éri a célját.

Ennél precízebb az NIST átfogó megközelítése, ami szerint az APT egy kiemelkedő szintű szakértelemmel és szignifikáns erőforrásokkal rendelkező ellenfél, ami lehetővé teszi számára a céljai elérését különböző támadási vektorok (kiber, fizikai, és megtévesztés) alkalmazásával. Ezek a célkitűzések jellemzően magukba foglalják álláspontok (hídfőállások, illetve hozzáférési pontok)

[85] Eric Cole 20 éves tapasztalattal rendelkező, iparági szinten elismert kiberbiztonsági szakember, a Pace Egyetem doktora. Dolgozott a McAfee cég technológiai igazgatójaként (CTO), a Lockheed Martin vezető tudósaként és az amerikai elnöki adminisztráció kiberbiztonsági tanácsadójaként is.

kialakítását és kiterjesztését a célba vett szervezetek információ technológiai infrastruktúrájában annak érdekében, hogy információt szerezzen, aláássa vagy akadályozza egy küldetés, program vagy szervezet kritikus aspektusait; illetve úgy pozícionálja magát, hogy ezeket a célkitűzéseket a jövőben végrehajthassa. A fejlett perzisztens fenyegetés: (i) hosszabb időn keresztül módszeresen követi céljait; (ii) az ellenállás érdekében alkalmazkodik a védők erőfeszítéseihez; és (iii) eltökélt a célkiűzések eléréséhez szükséges interakció szintjének fenntartásában (NIST, 2011).

Az eredeti szabadalmi beadvány (Schmidt, Rattray, és Fogle, 2008) alapján a fejlett perzisztens fenyegetést erőteljesebb szofisztikáltság és szakismeret, gyors együttműködés, és egyre inkább strukturált kapcsolatok jellemzik a komplex hálózatbiztonsági mechanizmusok legyőzése érdekében – ami gyakran belülről történik. A motiváció egyre inkább profitorientált, míg a modus operandi része a perzisztencia és a rejtve maradás. Magába foglal államilag támogatott szereplőket, melyek hatása hosszú távú befolyásolási és kizsákmányolási kampányokhoz járul hozzá a katonai lépéseket kiváltó pusztító hatásokhoz hasonlóan. Ismertető jegyeik közé tartozik a nulladik napi sérülékenységek kihasználása, elosztott terjesztő hálózat alkalmazása, fejlett pszichológiai manipulációs technikák, mint a célzott adathalászat, valamint hosszú távú adatbányászat és -kinyerés. Rugalmasságuk, valamint robusztus eszköz készletük és technikáik megnehezítik a fejlett fenyegetések legyőzését a mai technológia fókuszált hálózatbiztonsággal.

Az ENISA az APT-hez kapcsolódó incidens kezelési kiadványában három különböző meghatározást felhasználva igyekszik értelmezni a fenyegetést. Az oktatási célú dokumentum alapján az APT általában egy csoportra, például egy külföldi kormányra utal, amely rendelkezik a képességgel és a szándékkal is, hogy hatékony és perzisztens módon célba vegyen egy konkrét entitást. A kifejezés gyakran használatos kiber fenyegetésekre, azon belül is az internetes kémkedésre, amely különféle információgyűjtési technikákat alkalmaz érzékeny információkhoz való hozzáféréshez, de ugyanúgy vonatkozik más fenyegetésekre is, mint a hagyományos kémkedés vagy támadás. Az ismert támadási vektorok közé tartoznak a fertőzött adathordozók, az ellátási lánc kompromittálása, és a pszichológiai manipuláció. Egyéneket, például egyetlen hackert általában nem neveznek APT-nek, mivel ritkán rendelkeznek erőforrásokkal ahhoz, hogy fejlettek és perzisztensek legyenek még akkor is, ha egy adott célponthoz szándékoznak hozzáférést szerezni, vagy megtámadni azt (ENISA, 2014).

Richard Bejtlich[86] értelmezése nagyon közel áll egyfelől ahhoz, amit napjainkban APT-nek tekinthetünk, másfelől a kutatás során alkalmazott megközelítéshez is. A szakértő a fejlettséget úgy értelmezi, hogy az ellenfél képes a számítógépes behatolás teljes spektrumában működni. Képes alkalmazni a legalapvetőbb bárki számára elérhető eszközöket és megoldásokat (Imperva, 2014) egy jól ismert sérülékenység kihasználására, vagy képes emelni a téten és a célhoz igazított új sérülékenységet találni, amit egyedileg fejlesztett eszközökkel tud kihasználni. A perzisztencia azt jelenti, hogy az ellenfél hivatalos megbízása a küldetés teljesítése. Nem opportunista behatolókról van szó. Mint egy hírszerző egység, iránymutatásokat kapnak és a „gazdájuk" megelégedéséért dolgoznak. A perzisztencia nem szükségszerűen jelenti, hogy folyamatosan rosszindulatú kódot kell futtatniuk az áldozat számítógépén. Sokkal inkább a cél eléréséhez szükséges interakció-szint fenntartását jelenti. A fenyegetés tekintetében pedig az ellenfél nem egy értelmetlen kódrészlet. Az ellenfél fenyegetést jelent, mert szervezett, finanszírozott és motivált. Bejtlich szerint az APT olyan ellenfél, aki offenzív digitális műveleteket hajt végre, hogy különféle államhoz kötődő célokat támogasson. Az APT-t a célpont számítógépes infrastruktúrájának bizonyos fokú ellenőrzése iránti elkötelezettség jellemzi, kitartóan fellép az irányítás és a hozzáférés megőrzése vagy visszaszerzése érdekében. A kémelhárítás és a katonai elemzők nem minősített tájékoztatói az „agresszív" kifejezést használják annak hangsúlyozására, hogy az APT milyen mértékben törekszik ezekre a célokra különféle kormányzati, katonai és magán célpontokkal szemben (Bejtlich, 2010).

A fenti néhány példa rávilágít, hogy ahány szervezet, annyi féle meghatározás és értelmezés létezik az APT, mint terminus technicus kapcsán. Az értekezésnek nem célja megállapítani, hogy melyik a legjobb, mint ahogyan egy új APT definíció megalkotása sem. Azonban a kutatás szempontjából szükséges már most rögzíteni, hogy a kifejezést milyen értelemben használjuk a továbbiakban tekintettel arra, hogy a kutatás középpontjában olyan képességek kialakítása áll, ami több ponton átfedést mutat az APT-k jellegzetességeivel. Az APT kifejezést Bejtlich megközelítését alapul véve, mint képesség használjuk, illetve kisebb arányban az APT-k képességeivel bíró csoportokra. A képességek alatt az APT-k karakterisztikájának olyan sajátosságait értjük, mint a rejtőzködés és fedett működés, a kivételes szakismeret és kitartás, a célorientáltság és műveleti jelentőség, a

[86] Richard Bejtlich biztonsági stratéga, a FireEye és a Mandiant vállalatok korábbi vezető beosztású szakértője, a Brookings Intézet tagja, a King's College London doktora. Korábban dolgozott az amerikai légierő és a General Electric számítógépes incidens reagáló csapatában.

tervezett és szervezett végrehajtás, vagy éppen a szignifikáns erőforrásokhoz való hozzáférés és adaptivitás.

IV.1.2 Az első APT-k és kategorizálásuk

Korábban már esett szó az APT kifejezés első felbukkanásáról, mint ahogyan arról is, hogy a rövidítéssel gyakran hivatkoznak bizonyos szereplőkre, illetve az általuk végzett tevékenységekre. A terminológia szélesebb nyilvánosság előtt történő első megjelenését követően évek teltek el, mire megjelentek a legelső iparági és akadémiai elemzések, amelyek különféle csoportok tevékenységeként értelmezték az APT-ket és a könnyebb megkülönböztethetőség érdekében sorszámmal látták el azokat.

Még 2009 márciusában egy kanadai székhelyű kiberbiztonsági cég[87] egy iparági elemzésben GhostNet[88] néven hivatkozott egy kiber kémhálózatra, amelyik rosszindulatú szoftvereket alkalmaz műveletei során (Ghafir és Prenosil, 2014). Ugyanakkor több elemzés is arra a következtetésre jutott, hogy az első széles körben is elérhető APT-vel foglalkozó jelentést 2010 januárjában publikálták és az internet kereső-óriása[89] elleni Aurora[90] névre keresztelt művelet részleteit mutatja be (Ghafir és Prenosil, 2014; Lemay, 2018; Websense, 2011). 2011-ben szintén egy kiberbiztonsági cég[91] elemzése állította azt, hogy széleskörű globális kibertámadás sorozatot leplezett le. A művelet neve Shady RAT[92] lett (Alperovitch, 2011). 2012 októberében egy globális lefedettséggel rendelkező fenyegetés-elemző csapat[93] adott ki jelentést egy nagy kiterjedésű kiber

[87] SecDev Group (https://www.secdev.com)
[88] GhostNet néven vált ismerté az a támadó kampány, amelynek nyomait összesen 103 országban több mint 1295 eszközön sikerült kimutatni. A Kínának tulajdonított kampány során tibeti egyénekről és szervezetekről igyekeztek információt szerezni a gh0st RAT névre keresztelt rosszindulatú szoftver segítségével, ami az áldozat számítógépén teljes, valós idejű irányítást biztosított a támadók számára. Bővebben: https://citizenlab.ca/wp-content/uploads/2017/05/ghostnet.pdf
[89] Google (https://abc.xyz)
[90] Operation Aurora néven vált ismerté az a támadás sorozat, ami azt követően indult, hogy a Google bejelentette, a jövőben nem fogja cenzúrázni keresőmotorjának kínai változatában a találatokat. Bár a támadás a Google miatt híresült el, összesen tíz amerikai nagyvállalatot érintett, köztük védelmi ipari beszállítókat is. A forráskód megszerzésére irányuló támadás rendkívül kifinomult és összetett volt, majdnem egy tucat rosszindulatú szoftvert használtak és több szintű titkosítással igyekeztek a támadók elrejteni tevékenységüket. Bővebben: https://www.wired.com/2010/01/operation-aurora/
[91] McAfee (https://www.mcafee.com)
[92] Shady RAT néven ismerhette meg a világ azt a kiberműveletet, ami legalább 2006 óta összesen 14 országban érintett több mint 70 vállalatot, kormányzati szervet és non-profit szervezetet. A támadók weboldalakba ágyazott titkosított HTML kommenteket használtak a megfertőzött számítógépek irányítására és alkalmazkodtak a különböző célpontokhoz, mivel rendkívül széles volt a támadás spektruma. Bővebben: http://www.csri.info/wp-content/uploads/2012/08/wp-operation-shady-rat1.pdf
[93] Kaspersky Lab – Global Research and Analysis Team (https://www.kaspersky.com/about/team/great)

kémhálózatról. A diplomáciai szolgálatokat érintő támadó kampányt Red October [94] névre keresztelték. Tekintettel arra, hogy a legtöbb dokumentum arról számolt be, hogy az adott kampány nyomai a publikálás időpontjához képest már hónapokkal vagy évekkel korábban azonosíthatók az áldozatok infrastruktúrájában, kevésbé releváns, hogy egy-egy kampányt mikor fedeznek fel. Közben viszont elfogadott szabvány és szabályozás hiányában az APT-k karakterisztikáját mutató kampányokat a kiberbiztonsági iparág beszállítói változatos nevekkel kezdték el illetni, ami egyre követhetetlenebbé tette a helyzetet. Bár ez a helyzet egy évtized után is fennáll, 2013 februárjában egy amerikai kiberbiztonsági cég[95] elemzése APT1 néven hivatkozott egy kémkedéssel foglalkozó, Kínának tulajdonított egység tevékenységére. Nem kellett sokat várni az APT2 felbukkanására. 2014-ben egy feltörekvő kiberbiztonsági beszállító[96] számolt be az általa azonosított rosszindulatú tevékenységekről, amit szintén egy Kínai szervezethez kötöttek. Azóta számtalan APT tevékenységet követnek nyomon az állami és nem állami kiberbiztonsági szereplők. Bár a legtöbb APT tevékenység rendelkezik valamilyen számozott besorolással és csoportként szokás rájuk hivatkozni, a különböző kiberbiztonsági beszállítók gyakran saját elnevezést alkalmaznak, ami jelentős mértékben követhetetlenné teszi az amúgy is számos ponton átfedést mutató APT tevékenységeket és csoportokat. Az APT1 csoportot például ismerhetjük Comment Crew, Comment Panda, illetve Shanghai Group néven is, miközben utólag kiderült, hogy a korábban Shady RAT névvel illetett művelet is ehhez az APT-hez köthető. Az elnevezések és azonosítók kapcsán kialakult kaotikus helyzet a később felfedezett és nyilvánosságra hozott APT-knél talán még rosszabbá vált, mivel egyre több kiberbiztonsági szereplő igyekszik felderíteni, figyelni és követni valamilyen módon az APT-k tevékenységét. Ennek köszönhetően például az APT28 csoportot ismerhetjük Fancy Bear, Strontium, Pawn Storm, Sofacy, Sednit és Tsar Team néven is. Az indokolatlanul sok elnevezés egy iparági sajátosságra, egy meglehetősen komplex problémakörre vezethető vissza. Egyrészről rengeteg iparági szereplő van, aki a saját névadási sémáját alkalmazza, sokszor azt sem következetesen. Másfelől egy-egy új névvel illetett APT tevékenységről az elemzések mélyülésével és az információk gyarapodásával később gyakran

[94] Red October néven híresült el az a kelet-európai, posztszovjet és közép-ázsiai országokat érintő támadás sorozat, amely elsősorban diplomáciai és kormányzati testületeket, valamint tudományos kutató szervezeteket vett célba. Az Oroszországnak tulajdonított támadás során népszerű szövegszerkesztő és táblázatkezelő alkalmazások sérülékenységeit használták ki és a munkaállomások mellett különböző operációs rendszereket futtató okostelefonokról, nagyvállalati hálózati eszközökről, illetve külső meghajtókról is képesek voltak a támadók adatokat lopni. Bővebben: https://securelist.com/red-october-diplomatic-cyber-attacks-investigation/36740/

[95] Mandiant (https://www.mandiant.com)

[96] CrowdStrike (https://www.crowdstrike.com)

kiderül, hogy valójában több kiberbiztonsági gyártó és beszállító, vagy állami szerv is azonosította közel ugyanazt a tevékenységet, amik számos átfedést mutatnak egy-egy már beazonosított APT csoport által alkalmazott módszerekkel. Így fordulhat elő, hogy a UPS, a Gothic Panda és a Buckeye nevek mind az APT3 csoportra utalnak. Ezt a folyamatot tovább bonyolítja, hogy a kiberbiztonsági szereplőknek – főként a fenyegetésekkel kapcsolatos információszerzésre szakosodott csapatoknak (Cyber Threat Intelligence – CTI) – gyakran gazdasági érdeke is fűződik ahhoz, hogy az általuk végzett elemzések az újdonság érzetét keltsék, mivel így könnyebben monetizálhatók az általuk kínált szolgáltatások, vagy a csatolt kibervédelmi termékek. De a kaotikus folyamatot nem szükségszerűen táplálja kizárólag nyereségvágy. A CTI csapatok és az APT csoportok között zajló macska-egér harcnak a technikai mélységei szintén komoly szerepet játszanak abban, hogy sokszor évekig tart egy APT feltérképezése, beazonosítása és annak eldöntése, hogy valóban új szereplőről van-e szó. Anélkül, hogy durva technikai perspektívára váltanánk érdemes kiemelni, hogy az APT-k előszeretettel alkalmaznak rejtőzködő és titkosító megoldásokat pont azzal a céllal, hogy minél nehezebb legyen a beazonosításuk és az összefüggések megállapítása. Szintén bevett gyakorlat az APT műveletek során, hogy valódi nyomaik eltüntetésével párhuzamosan hamis nyomokat hagynak hátra, amivel igyekeznek másra terelni a gyanút. És arról sem szabad megfeledkezni, hogy a rosszindulatú szoftverek garmadája felett nem őrködnek a szellemi tulajdon védelmében fellépő szervezetek, így azokat bárki szabadon használhatja vagy módosíthatja. Emiatt nem ritka, hogy heterogén szereplők, eltérő célokkal, különböző célpontok ellen ugyanazt, vagy az azonosíthatóság szempontjából nagyon hasonló eszközt vetnek be egy támadás során. A támadói oldalon az eszközök, technikák és módszerek (Tools/Tactics, Techniques and Procedures – TTPs)[97] folyamatos fejlesztése, módosítása és változó kombinálása, a kiberbiztonsági szakemberek számára komoly fejtörést okoz és nagyban hozzá járul az APT-k és elnevezésük körül kialakult helyzethez.

Bár elsősorban az áttekinthetőség szempontjából kívánatos lenne az iparági gyakorlat megváltoztatása, egyrészt ez a téma még csak érintőlegesen sem kapcsolódik a kutatás által kitűzött célokhoz, másrészt ezzel kapcsolatban jelenleg is élő szakmai vita folyik iparági és akadémiai

[97] Az eszközök, technikák és módszerek, illetve taktikák, technikák és procedúrák kifejezést egy szereplő viselkedésének meghatározására szolgáló attribútumokra használják az NIST definíciója alapján. A taktika a viselkedés magas szintű leírására szolgál, míg a technikák a viselkedés részletesebb leírását tartalmazza a taktika kontextusában. A módszerek a technikák kontextusában még részletesebben írják le a szereplő viselkedését.

körökben egyaránt[98]. Ugyanakkor azzal kapcsolatban érdemes rövid kitekintést tenni, hogy a folyamatosan növekvő számú APT-ket jelenleg milyen módon lehet rendszerezni és erre milyen eljárások és eszközök állnak rendelkezésre. Egy gondolat erejéig vissza kanyarodva az APT első felbukkanásához, eredetileg az ázsiai származású fenyegetések kapcsán kezdték el használni a kifejezést (Bejtlich, 2010), tehát már a keletkezéskor is tartalmazott egyfajta attribúciót[99]. A kifejezés és az APT képességek elterjedésével együtt vált egyre gyakoribbá, hogy adott országokhoz kezdték kötni az egyes APT-ket. Mára több adatbázis is létezik[100], amikben az APT-kről rendelkezésre álló adatokban lehet kutatni és ezek mindegyike tartalmaz földrajzi vagy ország megjelölést. Ezen a ponton a számozás módszeréhez képest az asszociatív hatása miatt hatékonyabb és könnyebben használható lenne az olyan elnevezések következetes használata, mint Oroszország esetében a medve vagy Kína esetében a panda elé tett különböző jelzők.

Kategorizálás terén a legegyszerűbb és elterjedt megoldás a kezdetektől jelen levő földrajzi, illetve geopolitikai alapon történő besorolás. Ennek alapja, hogy az APT-ről megszerzett információk nyomán valamelyik országhoz kötik őket. Ilyen információ lehet a műveletek során alkalmazott számítógépes kártevőkből kinyert elnevezések, időbélyegek, IP és e-mail címek stb. Illetve bizonyos esetekben az is beszédes lehet, hogy a tevékenység céljai melyik ország érdekeivel azonosak.

Egy alternatív csoportosítási megoldást jelent az APT tevékenységek célpontok alapján történő kategorizálása. Az elmúlt évek során napvilágra került, egyre bővülő információ mennyiség alapján megfigyelhető egyfajta specializálódás. Vannak olyan APT-k, amiket kifejezetten kormányzati, diplomáciai, vagy épp katonai célpontok ellen alkalmaznak, míg mások az akadémiai szektorra, illetve a kutatási és fejlesztési tevékenységekre fókuszálnak. Ezen túlmenően további

[98] Az APT-k elnevezése körüli helyzet azért is problémás, mert megnehezíti a követhetőséget, könnyen összezavarja még a témában jártas szakembereket is és különösen nehézzé teszi a pontos, szakszerű kommunikációt a társadalom szélesebb rétegei és a média felé. Míg egyes vélemények a helyzet drámaiságát hangsúlyozzák megoldást sürgetve, más nézetek szerint minden rendben van. Bővebben: https://threatpost.com/the-apt-name-game-how-grim-threat-actors-get-goofy-monikers/141445/ és https://cyb3rops.medium.com/the-newcomers-guide-to-cyber-threat-actor-naming-7428e18ee263 és https://www.cfr.org/blog/when-naming-cyber-threat-actors-does-more-harm-good

[99] Az attribúció szót a kiberbiztonsági terület a szociálpszichológiából vette át, ahol arra a folyamatra alkalmazzák, amely megmagyarázza az egyén viselkedését és döntéseit. Magyarul a tulajdonítás és oktulajdonítás szavakkal megegyező értelemben használatos.

[100] Ilyen például a MITRE amerikai non-profit szervezet ATT&CK adatbázisa: https://attack.mitre.org/groups/, az önkéntes kiberbiztonsági szakemberek által gondozott APT csoport és műveleti adatbázis: https://docs.google.com/spreadsheets/u/1/d/1H9_xaxQHpWaa4O_Son4Gx0YOIzlcBWMsdvePFX68EKU/pubhtml, illetve a Fraunhofer Malpedia: https://malpedia.caad.fkie.fraunhofer.de/actors

alternatív csoportosítási lehetőség is kirajzolódik, mivel a célba vett szektor alapján többnyire arra is következtetni lehet, hogy milyen indíttatás áll az APT tevékenysége mögött. Ez lehet a klasszikus értelemben vett kémkedés, amit az államok évszázadok óta folytatnak egymással szemben. Nincs ez másként a kibertérben sem. Tekinthetjük ezt az államok közötti interakciók során a kezdetek óta jelen levő, klasszikus hírszerzési indíttatású APT tevékenységnek. A kémkedés különböző ágain túlmenően megfigyelhetők olyan APT tevékenységek, amelyek a célpont működésének szabotálására specializálódnak. Ebben az esetben kifejezetten fontos, hogy huzamosabb időn keresztül képes teljesen észrevétlen maradni és a szükséges pillanatban olyan hatást kifejteni, amivel a célpont működése ellehetetlenül. Ezek a hatások jellemzően nem csak a kibertérben jelentkeznek, hanem közvetlen vagy közvetett módon súlyos fizikai hatásokkal is számolni kell.

Az alkalmazott módszerek és eszközök mentén is van lehetőség az APT-k csoportosítására, azonban az APT-k közötti tudástranszfer következtében ez a kategorizálási alternatíva sem nyújt tökéletes, állandó megoldást. Főként az ugyanannak az országnak tulajdonított APT-k esetében figyelhető meg bizonyos módszerek, illetve eszközök megosztott vagy továbbfejlesztett alkalmazása, de arra is van példa, hogy teljesen eltérő háttérrel azonosított APT-k tevékenysége mutat hasonló mintázatot. A leírtakkal összefüggésben az APT-k kategorizálása kapcsán elmondható, hogy több szempontrendszer alapján is megvalósítható a besorolásuk, azonban az APT-kről rendelkezésre álló információk csupán egyfajta „pillanatfelvételként” foghatók fel, így a kategóriák és a hozzájuk rendelt APT-k változhatnak.

IV.1.3 Az APT csoportok állami támogatása

Amikor az APT csoportok állami támogatása felmerül, a legtöbben anyagi támogatásra, illetve finanszírozásra gondolnak, azonban ennél sokkal összetettebb jelenségről van szó. Ahogyan a III.3 fejezet esettanulmányaiban is látható volt, szép számban találhatók olyan APT-k, amiket nem csak konkrét államokhoz kötnek, de az adott állam valamelyik erőszakszervezetével hoznak szoros összefüggésbe. Ezeknek a kapcsolatoknak a további elemzése választ ad az állami támogatás miben létének részleteit illetően.

Az APT1 esetében, ha mélyebbre ásunk a nyilvánosan elérhető információkban, akkor azon felül, hogy a kínai haderő 61398 számú egységével hozzák összefüggésbe, a működés körülményeire vonatkozó részletek is megismerhetővé válnak. Nyílt források alapján az egység központi épülete

Shanghai Pudong negyedében található a Datong út 208 szám alatt, ami egy 2007-ben épült 12 szintes épület, több mint 12 ezer m^2 hasznosítható területtel. A becslések szerint mintegy 2 ezer embernek a munkahelye, azonban a közelben több, az egységhez tartozó támogató funkciót betöltő (orvosi rendelő, logisztikai létesítmény stb.) épületet is azonosítottak, illetve számos más lokáció is a 61398 számú egységhez köthető. Emellett az állami tulajdonú China Telecom a normál ügymenettől eltérően, saját készleteit felhasználva épített az egységgel közösen száloptikai kommunikációs vonalakat a nemzetvédelem jelentőségének elve alapján. (Mandiant, 2013)

Az orosz hátterűnek tulajdonított Turla kapcsán oknyomozó újságírok meggyőző bizonyítékokra bukkantak az FSB-hez fűződő szoros kapcsolat vonatkozásában. A Center-Inform és az Atlas nevű cégekkel összefüggésbe hozható két személy, akik a feltételezések szerint a Turla által alkalmazott eszközök fejlesztői. A rendelkezésre álló információk alapján mindkét cég szoros kapcsolatokat ápolt az orosz kormányzat legfelső szintjével. Ennek egyik kézzelfogható jele, hogy 2004 és 2007 között a cégjegyzék szerint az Atlas egyik irodája a Moszkvától dél-keletre található Rjazanban a Lenin út 46 és 48 szám alá volt bejelentve. A szovjet érában katonai központként fejlesztett és számontartott városban a 46 szám alatt az FSB helyi kirendeltsége található, míg a közös bejárat másik oldalán, a 48 szám a Szövetségi Védelmi Szolgálat (Federal Protection Service – FSO) egyik létesítménye. (Tanriverdi, Flade, és Frey, 2022)

A szakirodalom a valamely állam területén tevékenykedő, de állami háttérrel és támogatással – az elérhető információk alapján – nem rendelkező APT-ket is nyilvántartja. Ezeknek az APT-knek a fő motivációja jellemzően az anyagi haszonszerzés, mint például a kifejezetten orosz és ukrán pénzintézeteket támadó Buhtrap[101]. Az ilyen aktorok az APT-k mellett többnyire magukon hordozzák a kiberbűnözői jellemzőket és működésük kifinomultsága elmarad a stratégiai és geopolitikai érdekek mentén tevékenykedő APT-ktől.

Az állami háttér és támogatás nem feltétlenül anyagi hozzájárulás formájában jelenik meg az APT-k esetében. Nyilván ennek jelentőségét nem szabad alulértékelni, ugyanakkor az APT-k állami támogatásában rendkívül jelentős szerepe van a megfelelő infrastruktúra biztosításának és a

[101] A Buhtrap egy 2014 óta aktív, APT-ként is számontartott aktor. Csak orosz bankoktól 13 sikeres támadással több mint 25 millió dollárt loptak el, de az érintett ukrán bankok számát és az okozott kárt nem hozták nyilvánosságra. Az első olyan kiberbűnözői csoport, amelyik hálózati férget használ a banki hálózatok teljes megfertőzésére, de állami támogatással eddig egyetlen elemzés sem hozta összefüggésbe. Bővebben: https://malpedia.caad.fkie.fraunhofer.de/actor/buhtrap

tevékenység folytatásához szükséges feltételek és környezet kialakításának. Az APT-k tevékenységének jellegéből fakadóan fontos látni azt, hogy a különböző állami erőszakszervezetekbe történő betagozódás révén olyan erőforrásokhoz férnek hozzá, ami piaci körülmények között elérhetetlen vagy túlzottan költséges lenne számukra. A kiemelten védett – nem egyszer fedetten működő – létesítmények, a nagy sávszélességű hozzáférések, a dedikált hálózati eszközparkok és adatközpontok, a szakértelem és a szakember utánpótlás, a csúcs- illetve haditechnikai felszerelések, a diplomáciai védelem vagy a hírszerzési információkhoz való hozzáférés (Chen, Desmet, és Huygens, 2014) mindegyike az állami támogatásnak olyan formája, amit nehéz lenne pénzben kifejezni. Mindez hozzájárul az APT-k magasfokú hatékonyságához és az általuk kivitelezett támadások sikeréhez.

IV.1.4 Az APT csoportok hatékony működésének körülményei és feltételei

Több korábbi fejezetben is szóba került már az APT-k magas fokú hatékonysága, aminek több a működés körülményeihez és feltételeihez fűződő alapfeltétele is azonosítható. A vélt vagy valós állami támogatás az APT-k gyakran emlegetett ismertető jegye, ami fontos szerepet játszik a működési körülmények és feltételek megteremtésében, azonban a nyíltan hozzáférhető elemzések kisebb hangsúlyt fektetnek az utóbbi sajátosságokra.

Az APT-k kapcsán a legtöbb esetben arra a következtetésre jutnak az elemzők, hogy a tevékenységük során akár több nulladik napi sérülékenységet is képesek kihasználni, ami bizonyos esetekben még a definíciók szintjén is megjelenik. (Ahmad és mtsai., 2019) Tekintettel a nulladik napi sérülékenységek felfedezéséhez szükséges szignifikáns időre, csak a legkifinomultabb támadók képesek az alkalmazásukra és az ezáltal szerzett előny kihasználására. (Symantec, 2011) A nulladik napi sérülékenységek kihasználásához tehát vagy magas fokú szakértelemhez párosuló jelentős mennyiségű időre vagy sok pénzre van szükség. Ha egy APT-nek nem áll rendelkezésére megfelelő szakértelem és idő, a vásárlás lehetősége még mindig megmarad, azonban egy-egy sérülékenység ára akár milliós tétel is lehet amerikai dollárban. (Ablon, Libicki, és Golay, 2014)

A szakértelem, mint feltétel és az idő, mint körülmény fontos tényezőknek számítanak az APT tevékenységek esetén, amiket kiegészít a fedett, illetve rejtett működés két aspektusa is. A fedett működés egyfelől értelmezhető a fizikai dimenzióban az APT tevékenységet végző humán erőforrásra, illetve a csoportra, ami főként a nemzetbiztonsági szervezeteknek tulajdonított APT-k

esetében mutatható ki legegyszerűbben. Másfelől a rejtettség a kibertérben is megjelenik az APT-k által alkalmazott titkosítási megoldások és elterelő, illetve lopakodó technikák révén, amikkel képesek észrevétlenek maradni és elrejteni a tevékenységüket a hálózati forgalomban. (Chen, Desmet, és Huygens, 2014) A fizikai- és a kibertérben történő fedett működés egyfelől hozzájárul az adott művelet megrendelőjének elrejtéséhez, másfelől a művelet puszta létezését is elrejti, illetve letagadhatóvá teszi. (Robertsen, 2007)

A rejtett működés egyrészt körülmény, másrészt feltétel is az APT hosszú távú működésének aspektusából és ugyanez elmondható az APT tevékenységek magas fokú tervezettsége és szervezettsége kapcsán. Az APT-k műveletei előkészítést és felkészülést igényelnek, emellett folyamatos erőforrás menedzsmentre és logisztikai, illetve egyéb támogatás biztosítására van szükség. Ha egy művelet elakad a Cyber Kill Chain valamelyik fázisában alternatív megoldások és módszerek alkalmazása válhat szükségessé a végső cél elérése érdekében. Mindez a specifikus célpontok és a hozzájuk igazított támadások miatt szintén koordinációt igényel. A kibertámadások gyorsaságával kapcsolatban a másodperc tört részét szokás emlegetni, azonban a „fogd és fuss" taktikával szemben az APT-k egyik legfontosabb céljának elérése, az észrevétlen perzisztencia kialakítása és megőrzése lassú folyamat, amit kontrollálni kell és szükség esetén beavatkozni. (Symantec, 2011)

IV.1.5 Az APT-k és tagjaik azonosítási nehézségei

Az APT csoportokkal összefüggésben az egyik leggyakrabban felmerülő kérdés különösen állami támogatás esetén, hogy ki áll a tevékenység mögött. Ennek meghatározására koncentrál a korábban többször említett attribúció folyamata. Az attribúció a technikai szinten egyfajta művészet, illetve tudomány, míg a műveleti szinten egyszerű probléma helyett inkább árnyalt folyamatként írható le, ahol semmi sem fekete vagy fehér és nem adhatók válaszok pusztán igennel vagy nemmel. Stratégiai szinten az attribúció a politikai kockázatok meghatározására szolgáló funkcióként fogható fel. Ugyan nincs receptje a korrekt attribúciónak, azonban mindenképpen csapatmunka kell legyen, mivel meghaladja egyetlen ember képességeit és kapacitását. (Rid és Buchanan, 2015)

Megfelelő szakértelem és eszközök birtokában sok információ megtudható egy APT-ről, azonban ehhez jellemzően nem elegendő egyetlen támadás. A támadások során rengeteg indikátor keletkezik, amelyeknek az azonosítása, összegyűjtése és elemzése segíti a válaszadást. A technikai

szinten olyan alapvető kérdések megválaszolása válik lehetővé, hogy mit, honnan és hogyan támadtak, ugyanakkor operatív és stratégiai információkkal kiegészülve a ki és a miért kérdések megválaszolása sem lehetetlen. A hálózati behatolás, illetve a rosszindulatú tevékenység technikai nyomai, illetve bizonyítékai az úgynevezett indikátorok (Indicators Of Compromise – IOC) (Rid és Buchanan, 2015), amelyek összekötik a kompromittálódás folyamatának fázisait. Komplexitásuk alapján az IOC-k három kategóriába sorolhatók: elemi, számított és viselkedés indikátorok. (Villalón-Huerta, Ripoll-Ripoll, és Marco-Gisbert, 2022)

Az attribúció során az IOC-knak jelentős szerepe van, mivel a kibertámadások túlnyomó többségéhez szükséges kétirányú kommunikáció lenyomatait őrzik a támadó és az áldozat számítógéppel összefüggésben. A kifinomult ellenfelek azonban mindent megtesznek azért, hogy elfedjék valódi lokációjukat és személyazonosságukat proxy rendszerek alkalmazásával, amik lehetnek más kompromittált rendszerek vagy anonimizáló szolgáltatások és megoldások. Az elővigyázatosság ellenére a visszakövetés technikai feltételei a támadók felfedésére adottak, az akadályok sokkal inkább jogi jellegűek (Knake, 2010) a kibertér fizikai rétege miatt, ahol a nemzetközi határok és a nem kooperatív országok szerepe megnövekszik.

Az attribúció legfejlettebb szintje, amikor konkrét személyek beazonosítása is lehetővé válik az APT tevékenységek kapcsán (Brandao, 2021), amire egyelőre kevés nyilvános példa van, de ilyenek az Egyesült Államok általi vádemelések kínai (DOJ US, 2014) és orosz (DOJ US. 2020) állampolgárok ellen, akik a dokumentumok szerint amerikai vállalatokat és a kormányzatot érő kibertámadásokban vettek részt. Az attribúció megvalósításával sok szereplő (vállalatok, kormányok, nem kormányzati szervek stb.) foglalkozik, azonban az alkalmazott eljárások és módszerek nem nyilvánosak, így nincs egységes sablon vagy keretrendszer. Egy lehetséges mód a MICTIC (Malware – Infrastructure – Control Server – Telemetry – Intelligence – Cui bono[102]) séma alkalmazása, ami a legkülönfélébb bizonyítékok összegyűjtésével és rendszerezésével képes hozzájárulni az attribúciós folyamat eredményéhez. Bizonyos esetekben ezt nyílt forrású információkkal kombinálva akár az egyén szintjén is lehetővé válik az azonosítás. (Brandao, 2021) Azonban a kibertér sajátosságai következtében a fedett/titkos, illetve megtévesztő műveletek közé sorolható hamis zászló (false-flag) alatt, illetve zászló nélkül (no-flag) végzett tevékenység

[102] Cui bono – latin eredetű kifejezés, ami a rejtett, nem nyilvánvaló motívumokra utal egy esemény kapcsán, illetve a történés háttérben meghúzódó érdekekre, ami alapján más lehet az indíték és a felelős is, mint azt gondolnánk.

megvalósítása jóval egyszerűbb és olcsóbb a fizikai dimenzióhoz képest, miközben a nemzetközi humanitárius jog vonatkozó rendelkezéseinek érvényesítése nehézségekbe ütközhet. Így az attribúció hamis lehet és egy kiberműveletről akár évekig vagy soha nem derül ki, hogy ki hajtotta végre valójában (Maurer, 2017).

IV.2 Az APT-k által generált kihívás és fenyegetés jelentősége

A fejezet legelején érintettük az APT-k meglehetősen széles skálán mozgó, heterogén megközelítését, azonban ez inkább a kifejezés kiberbiztonsági szolgáltatásokra és termékekre gyakorolt hatásának eredménye és nem a fenyegetés degradálása. Az APT tevékenységekkel összefüggő fenyegetések mértékét és jelentőségét a legtöbb felelős szakember igyekszik helyiértéken kezelni és rendszereit felkészíteni a velük szembeni védekezésre. Az állami hátterű APT-k motiváció, érettség és az erőforrások tekintetében a 2020-as évek elejére olyan szintet értek el, hogy a fegyverekkel, diplomáciai intézkedésekkel és gazdasági megszorításokkal vívott konfliktusokban az APT-k által kivitelezett szofisztikált kibertámadások egy újabb vektorként alkalmazhatók a nemzetállamok számára (Johnson, 2020). A IV.1 alfejezetben tárgyalt ellátottság, milliárdos – esetenként multimilliárdos – finanszírozás, a magas fokú fejlettség, illetve a hosszútávú és nagyarányú célzott támadások minden más kibertérből érkező fenyegetéstől jól megkülönböztethetővé teszik az APT-ket, amit az elemi karakterisztikájukhoz társított empirikus minták és precedensek támasztanak alá.

IV.2.1 Fejlettség

Az előző alfejezetben alaposan körbejártuk az APT kifejezés fejlettségre vonatkozó részét elméleti síkon, de érdemes megvizsgálni, hogy pontosan mit is jelent ez a gyakorlatban. Az APT-k kapcsán a fejlettség szinonimájaként használt és gyakran emlegetett szofisztikáltság egyik kézenfekvő példája a már említett Turla csoport. Egy APT a tevékenysége során szerteágazó problémákkal szembesül, amelyek között kiemelt szerepet tölt be, hogy a művelet irányításához használt C2 infrastruktúra elemeit (szerverek, domén nevek, IP-címek) – a Denning féle külső aktív védelmi intézkedésként – folyamatosan lefoglalják és blokkolják, amivel jelentősen degradálják működését és hatékonyságát. A probléma kiküszöbölésére a Turla legalább 2007 óta egy nem túl gyakori

megoldást választva, műholdas kapcsolatokat használ a műveletek irányítására. A műholdas kapcsolatok alkalmazásának legnagyobb előnye, hogy a műholdak által lefedett terület kiterjedt, amin belül a műholdas vevő eszköz bárhol lehet és ez jelentősen megnehezíti a C2 infrastruktúra hardvereinek azonosítását, lokalizálását, illetve lefoglalását. Bár a műholdas kapcsolatok (downstream link) relatív lassúak és instabilak, eltérítésük magas fokú anonimitást tesz lehetővé, miközben nincs szükség érvényes műholdas előfizetésre, így az üzemeltetés is költséghatékony marad. A mélyebb technikai részleteket elkerülve a támadás alapja, hogy a kihasznált műholdas kapcsolat nem titkosított, ami lehetővé teszi a számítógépes hálózati forgalomba történő beékelődést (Man-in-the-Middle – MitM). A támadó legitim felhasználónak adja ki magát és a műholdas kapcsolaton keresztül érkező hálózati csomagok (pl.: TCP/IP SYN) segítségével azonosítja a forrást, majd meghamisított válasz csomagokat (pl.: SYN ACK) küld. Az így felállt kommunikációs kör segítségével az áldozat kártékony szoftverrel fertőzött gépéről egyszerűen eljuttathatók az adatok a C2 infrastruktúra eszközeire. (Tanase, 2015)

Az APT-k esetében egy másik, többek között a szofisztikáltság meghatározására is használt paraméter a nulladik napi (zero-day) sérülékenységek alkalmazása. Ilyen tekintetben az ismert APT tevékenységek között a mai napig rekordernek számít a Stuxnet, ami összesen 6 számítógépes sérülékenység kihasználására volt képes és amiből 5 volt nulladik napi[103]. Ezek felfedezése (vagy megvásárlása) és kihasználása – különös tekintettel arra, hogy az ipari folyamatirányító rendszerek (Industrial Control System – ICS) és programozható logikai vezérlők (Programmable Logic Controller – PLC) szűk szegmenséről volt szó – magas fokú fejlesztői szakértelmet és erőforrásokat igényelt. Becslések szerint 8-10 ember legalább féléves munkája és egy speciális teszt labor kiépítése áll a Stuxnet mögött. (Schneier, 2010) Ugyanakkor a Stuxnet szofisztikáltsága túlmutat a kihasznált nulladik napi sérülékenységek garmadáján. A Stuxnet futtatható fájlok és direkt humán beavatkozás nélkül zárt, más hálózatoktól fizikailag elválasztott (air-gapped) rendszerekbe bejutva volt képes megvalósítani a készítőinek célját, ami arra utal, hogy a kezdetektől fogva az úgynevezett „tüzelj és felejtsd el” (fire-and-forget) szemlélet alapján készült. Ha egyszer „szabadon engedték” képes volt mindent saját magától végrehajtani, nem volt szükséges „haza telefonálnia”

[103] A számítógépes sérülékenységeket egy sérülékenységi és kitettségi adatbázishoz rendelik úgynevezett CVE (Common Vulnerabilities and Exposures – CVE) számokkal, aminek célja az azonosíthatóság és a nyilvános információk megosztásának egyszerűsítése. A Stuxnet által kihasznált 6 sérülékenység közül a CVE-2008-4250 az egyetlen ami a támadáskor ismert volt, a CVE-2010-2568, a CVE-2010-2729, a CVE-2010-2729, a CVE-2010-2743, a CVE-2010-2772 és a CVE-2010-3888 addig ismeretlenek voltak.

és tájékoztatni a készítőit arról, hogy mit csinál, vagy mit talált és utólagos instrukciókra sem volt szüksége. (De Falco, 2012) Ehhez több lopott digitális aláírással is rendelkezett, hogy legitimnek tűnjön (Kovács és Sipos, 2010), miközben hét különböző módon tudott terjedni, képes volt a vírusok detektálásáért és az automatikus frissítésekért felelős programokat semlegesíteni, illetve a különféle titkosító és elterelő megoldás mögé rejtett kódja képes volt a dinamikus mutációra (polymorphic/metamorphic code). (De Falco, 2012) A Stuxnet létezése markánsan demonstrálja a kiberfegyverek és kinetikus képességeik realitását.

A különböző iparágakban eltérő értelmezése és jelentése van az ellátási lánc (supply chain) kifejezésnek. A kibertérben jellemzően a szoftverek és hardverek beszállítói ökoszisztémáját értik az ellátási lánc alatt, illetve a célpont bármely partnere az ellátási lánc részeként értelmezhető, ha a szoftverein és hardverein keresztül támadható a célpont. Dióhéjban az ellátási lánc támadása egy adott eszköz kompromittálására utal, ami lehet egy szoftverszolgáltató infrastruktúrája, illetve szoftvere is. A cél, hogy közvetett módon károsítsanak egy bizonyos célpontot vagy célpontokat, például a kompromittált szoftverszolgáltató ügyfeleit. (ENISA, 2017) A Stuxnet nevével szintén találkozhatunk, mint az ellátási láncok elleni ismert kibertámadások egyike (Herr és mtsai., 2020), azonban az elmúlt néhány évben több globális hatást kiváltó eset is történt, amelyek precízen rávilágítanak az ellátási láncok sebezhetőségeit kihasználni képes APT képességekre.

2017 júniusában úgy tűnt, hogy a 2016-ban már megjelent Petya (Abrams, 2016) zsarolóvírus újra aktív, azonban néhány óra alatt kiderült, hogy a cél nem az anyagi haszonszerzés, hanem a számítógépes hálózatok megbénítása és a rosszindulatú szoftver nem a Petya frissített verziója. A NotPetya egy alig két hónappal korábban a Shadow Brokers által kiszivárogtatott EternalBlue (Dillon és Davis, 2017) nevű, szoftversérülékenységek kihasználására képes kódot tartalmazott, aminek a segítségével jelszavak begyűjtése és a hálózatok közötti emberi beavatkozás nélküli terjedés is megvalósulhatott. A NotPetya készítői ezt egy adminisztrátori hitelesítő adatokra vadászó, nyíltan elérhető Mimikatz (SentinelOne, é. n.) nevű eszközzel kombinálták. (Crosignani, Macchiavelli, és Silva, 2020) A kártékony kód célbajuttatásához kompromittálták az ukrán vállalkozások számára előírt, adózáshoz használt M.E.Doc nevű szoftvert, így manipulálni tudták a szoftverfrissítéseket terjesztő szervereket. A szoftver mit sem sejtő felhasználói a legitimnek hitt szoftverfrissítéssel telepítették a NotPetya destruktív kódját is. (Biasini ,2017) Az elemzések szerint eredetileg az ukrán kritikus infrastruktúra megbénítására fejlesztett NotPetya az ukrajnai

leányvállalatokon keresztül az egész világon elterjedt és nagyságrendileg 10 milliárd dolláros (USD) kárt okozott. (Herr és mtsai., 2020)

Három és fél évvel később fény derült egy hasonló módszerekkel elkövetett támadásra, ami a kompromittált szoftver fejlesztője és szállítója után SolarWinds néven vonult be a történelembe. A texasi székhelyű, a támadás idején 320 ezer kormányzati, pénzügyi telekommunikációs és egyéb ügyféllel rendelkező SolarWinds Orion névre keresztelt hálózat-, rendszer- és alkalmazás teljesítmény felügyeleti platformja (DFS NY, 2021) lett a támadók „fegyverhordozója". A támadóknak a szoftverfejlesztés kulcsfontosságú fázisában, amikor a forráskódot telepíthető szoftverré konvertálják (build), sikerült a Sunburst nevű direkt a támadáshoz fejlesztett rosszindulatú kódot elhelyezni az Orion platformban. A SolarWinds a kártékony kódot tartalmazó frissítésekkel látta el globálisan 18 ezer ügyfelét 2020 márciusától júniusig, amikor a támadók eltávolították a Sunburst kódját az Orion szoftver frissítéseiből.(DFS NY, 2021) Végül 2020 decemberében egy kiberbiztonsági cég[104] vette észre és értesítette a SolarWinds szakembereit a Sunburst létezéséről, ami úgynevezett „hátsó ajtóként" (backdoor)[105] funkcionált és képes volt legitim hálózati forgalom imitálására, egyedülálló domén generáló algoritmust használt a C2 kapcsolatokhoz és ellenőrizni tudta a biztonsági szoftverek jelenlétét. (CFCS, 2021) Az Orion három verzióját is érintő problémát tovább súlyosbította, hogy egy másik, Supernova névre keresztelt távoli elérést lehetővé tevő kódsorra is rábukkantak a fertőzött Orion verziók vizsgálata közben. (DFS NY, 2021) A támadás zsenialitása abban érhető tetten, hogy a háttérben futó hálózatfelügyeleti szoftverek – amilyen az Orion is – képesek egy kijelzőre tenni a teljes hálózatot, szerverekkel, tűzfalakkal, hálózati nyomtatókkal (Temple-Raston, 2021), ezáltal a támadók bármiről információt gyűjthettek, vagy akár mindenhez hozzáférhettek az érintett hálózatokon. A SolarWinds Oriont használó ügyfelei között megtalálható 425 a US Fortune 500[106] cégek közül, a 10 legnagyobb amerikai telekommunikációs cég mindegyike, az amerikai haderő mind az 5 haderőneme, a Pentagon, a Külügyminisztérium, a NASA, az NSA, az Igazságügyi Minisztérium,

[104] FireEye: https://www.mandiant.com/resources/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor

[105] A számítástechnikában az angolszász terminológiából átvett „backdoor", vagyis hátsó ajtó kifejezést használják azokra a rejtett hozzáférésekre és metódusokra, amivel megkerülhető egy számítógép, egy termék, egy beágyazott eszköz, vagy ezek alkotóeleminek hitelesítése vagy titkosítása.

[106] A Fortune magazin által évente, a teljes bevétel alapján a legnagyobb amerikai vállalatokból összeállított 500-as lista.

az Elnöki Iroda, az 5 legnagyobb amerikai könyvelő cég mindegyike és több száz egyetem, illetve főiskola is világszerte. (CFCS ,2021)

IV.2.2 Perzisztencia

Miközben a SolarWinds támadás kiterjedése és hordereje történelmi léptékben is a legjelentősebb kibertámadások közé emeli az esetet, érdemes kitérni a támadók tevékenységének kitartó, illetve visszatérő jellegére. Ebben az esetben az orosz SVR munkatársainak tulajdonított tevékenység feltételezett kezdetét egészen pontosan sikerült visszakövetni. 2019. szeptember 12-én a támadók egy egészen rövid kódrészletet csempésztek az Orion platformba, ami nem csinált mást, mint ellenőrizte a számítógép processzorát és annak függvényében, hogy 32 vagy 64 bites processzort talált egy 1-est vagy 0-át adott vissza. A támadók így ellenőrizték azt, hogy képesek-e módosítani a SolarWinds tanúsítvánnyal védett és aláírt szoftver kódját a publikálást megelőzően anélkül, hogy bárki észlelné azt. Miután kiderült, hogy képesek rá, 5 hónapra eltűntek a támadók. (Temple-Raston, 2021) Amikor 2020 februárjában visszatértek, a korábban szintén ismeretlen és az Orion fejlesztési eszközeinek felügyeletére használt, backdoorként funkcionáló Sunspot nevű kártékony szoftver jelentősen átdolgozott és módosított változatát is magukkal hozták. Ez volt a Sunburst, amit azután 2020 júniusi kivonásáig az Orion frissítéseibe ágyazva terjesztettek és ami a következő 6 hónapban zavartalanul működhetett az áldozatok rendszereiben. (CFCS, 2021) A SolarWinds támadást megvalósító APT tevékenység legalább 459 napig tudott észrevétlen maradni.

A rendelkezésre álló elemzések eltérő eredményeket tartalmaznak az adatsértések észleléséhez szükséges idő kapcsán. Az amerikai informatikai óriás, az IBM 2021-es jelentése alapján átlagosan 212 napig tart, mire észlelnek egy adatok megsértését eredményező eseményt. A felfedezést követően az áldozatnak további 75 napra van szüksége ahhoz, hogy megszüntesse az adatsértést, míg azoknak a szervezeteknek, ahol a munkavállalók több mint 50%-a távolról dolgozik, további 58 nap szükséges egy adatsértés észleléséhez és megszüntetéséhez. (IBM, 2020) Egy évvel korábban az említett adatok még 197, illetve 69 napot vettek igénybe. (Sobers, 2020) Egy másik amerikai szolgáltató, a Verizon szintén 2021-es elemzése arra jutott, hogy hozzávetőlegesen ugyan az incidensek 60%-át néhány napon belül felfedezik, azonban az esetek mintegy 20%-ában akár hónapok telnek el vagy még több idő az észlelésig. (Verizon, 2021)

Az Egysült Királyság Információbiztosi Iroda (Information Commissioner's Office – ICO) 2020 januári közleménye alapján egy támadó majdnem 5400 fizető terminálra telepített kártékony szoftvert, aminek a segítségével 2017 nyara és 2018 tavasza között 9 hónapon keresztül 5,6 millió bankkártya adataihoz és 14 millió ember személyes adataihoz fért hozzá jogosulatlanul. (ICO, 2022)

Korábban az APT1 kapcsán már szóba került, hogy rendkívül hosszú ideig képes fenntartani a hozzáférést az áldozatok hálózataihoz. A leghosszabb idő 1764 nap volt, de ha az APT1 kompromittálni tud egy hálózatot, akkor a megszerzett hozzáférést átlagosan 356 napig képes fenntartani. Ez alatt az időszak alatt az APT1 nem mutat folyamatos aktivitást napi szinten, a módszereik között inkább a visszatérő megfigyelés és adatlopás előfordulása a gyakoribb. (Mandiant, 2013)

Egy másik Kínának tulajdonított fenyegetés, az APT41 perzisztenciája kapcsán az elemzések arra jutottak, hogy rendkívül agilis hozzáállást tanúsítva gyorsan reagálnak az áldozat hálózati környezetében bekövetkező változásokra és az incidens reagálók tevékenységére. Előfordult olyan eset, hogy miután az áldozattá vált szervezet az APT41 elleni módosításokat eszközölt, néhány órán belül új C2 domén nevet jegyeztek be, egy új backdoor variánst állítottak össze és az új eszközt több földrajzi régióban és rendszeren telepítették is. Arra is van példa, hogy az APT41 célzott adathalász üzeneteket küld ki az emberi erőforrás terület alkalmazottainak mindössze három nappal azt követően, hogy a kompromittált rendszereket helyreállították és újra online állapotba kerültek. A rosszindulatú csatolmány megnyitása miatt az APT41 képes volt újra megvetni lábát az áldozat rendszerében és több földrajzi régióban levő szerverre bejutni. (Mandiant, 2022b)

A Stuxnet kapcsán is megfigyelhető a perzisztencia. A rendelkezésre álló adatok alapján a zárt hálózatokon történő terjedést lehetővé tevő sérülékenységet kihasználó rosszindulatú szoftver 2008 novemberében tűnt fel, a C2 szervereit pedig decemberben regisztrálták. A Stuxnet első verzióját 2009 júniusára datálják az elemzések és egy évvel később 2010 júniusában észlelték először, míg a beépített önmegsemmisítés dátuma 2012 júniusa volt. (De Falco, 2012)

IV.2.3 Fenyegetés

Azt, hogy az APT-k képességei miért jelentenek fenyegetést, leginkább a maradék karakterisztika vizsgálatával lehet leírni. Ezek a műveleteik során tapasztalható célzottság és determináltság

kiemelkedően magas foka, a kockázatvállaló mentalitás, ami kreatív és agilis gondolkodásmóddal párosulva veszélyes elegyet alkot. Az APT-k mindezt egy olyan szervezetben ötvözik, amelynek az a feladata, hogy az áldozat szempontjából nézve olyan rosszindulatú tevékenységet folytasson az áldozat információs technológiai infrastruktúráján és/vagy az ellen, ami veszélyezteti a gazdaság, a társadalom és a nemzet biztonságát.

A Stuxnet ilyen szempontból egy specifikus szegmensre fókuszált. Irán, állítása szerint békés céllal, az energiamix diverzifikálása miatt kezdett bele az urándúsításba, azonban több ország is katonai célokat, illetve nukleáris fegyver előállításának szándékát valószínűsítette a tevékenység mögött, ami egy olaj-nagyhatalom esetében nem is alaptalan. A Stuxnet azzal, hogy átlépte a határt a virtuális és a fizikai világ között, az iráni energiabiztonságra és az ország geopolitikai helyzetére is befolyást tudott gyakorolni átmenetileg. (De Falco, 2012) A Stuxnet által kiváltott, Irán érdekeivel ellentétes hatások – függetlenül attól, hogy energiabiztonságról vagy katonai biztonságról van szó – alátámasztják az APT, illetve a nemzeti kiberműveleti képességek fenyegetésként történő értékelésének koncepcióját.

Nem csak energiabiztonsági szempontból jelentenek fenyegetést azok az ugyancsak fizikai következményekkel járó célzott APT tevékenységek, mint amilyeneket az ukrán energiaellátó rendszer vagy az amerikai üzemanyag-szállító hálózat ellen folytattak. 2015 decemberében egy elhúzódó kampány valószínűleg egyetlen aktor szignifikáns és összehangolt erőfeszítései következtében áramszünetet okozott Ukrajnában. A jól szervezett képesség birtokosának közvetett érdeke az volt, hogy kibertámadásokkal ássa alá Ukrajna társadalmi-politikai szövetét. (Styczynski és Beach-Westmoreland, 2015) Az elemzők arra jutottak, hogy a bátor és sikeres kiberművelet hatásai eltérőek lehetnek más államok esetében, azonban a metodológia és a megfigyelt TTP-k a világon bármely infrastruktúra esetén alkalmazhatók. (Lee, Assante, és Conway, 2016) 2021 májusában az amerikai Colonial Pipeline vállalat zsarolóvírusra hivatkozva bejelentette csővezetékes tevékenységének felfüggesztését, ami az egész keleti-part üzemanyag- és egyéb finomított kőolajszármazék-ellátását megzavarta. (Parfomak és Jaikaran, 2021) A több millió dolláros (USD) veszteség mellett az eset pánikot, az üzemanyag-szállítás bénító hiányát és társadalmi zavart okozott. (Reeder és Hall, 2021) A vállalat kiberbiztonsági hiányosságai miatt kevésbé érvényes a magas fokú kifinomultság, sokkal inkább a hatások miatt érdekes az eset, mivel egy sor szövetségi szintű rendkívüli intézkedést (The White House, 2021) váltott ki azonnal vagy

rövidtávon, miközben hosszú távon az amerikai létfontosságú infrastruktúrák nemzetbiztonsági kitettségének ijesztő mértékére és működésük megzavarásának bomlasztó következményeire is rávilágított.

Az APT tevékenységek pontos és egyértelmű célokat szolgálnak. A hagyományos kiberbűnözők számára sikerrel kecsegtető kiterjedt támadásokkal szemben az APT-k precízen és fokuszáltan tevékenykednek olyan versenyelőnyt, vagy stratégiai hasznot hozó digitális tőke megszerzése érdekében, mint a nemzetbiztonsági adatok, szellemi tulajdon és kereskedelmi titkok. (Khaleefa és Abdulah, 2022) Ennek egyik kézenfekvő példája a Turla nevű aktornak tulajdonított Crutch névre keresztelt backdoor-ként és dokumentum lopásra is használt szoftver. A mintegy 5 éven keresztül használt kártékony szoftvert az Európai Unió tagállamaiban a külügyminisztériumi hálózatokon azonosították és kifejezetten arra tervezték, hogy szenzitív dokumentumokat és egyéb fájlokat szivárogtasson ki a támadók által ellenőrzött, de legitim tárhelyszolgáltatói fiókokon keresztül. A Crutch üzemeltetői a felderítői és kémkedési tevékenység mellett a hálózaton történő terjeszkedésre is használták az eszközt. (Faou, 2020)

IV.2.4 APT képességek állami támogatással

A III.3 alfejezet esettanulmányai rávilágítottak arra, hogy vannak olyan országok, ahol nagyságrendileg legalább két évtizede foglalkoznak a kiberműveleti képességek teljes spektrumának kialakításával és fejlesztésével. A mostanra gyakran APT tevékenységekkel összemosódó kiberműveleti képességekkel azonban nem csak Kína, Oroszország és az Egyesül Államok rendelkezik. Egységes mérőszámok, statisztikák, szabványok és szabályzók hiányában nehéz objektív szempontok alapján összevetni az egyes országok képességeit, amit tovább bonyolít, hogy eltérő mennyiségű és részletességű információ áll rendelkezésre egy-egy ország kiberműveleti képességeiről. Az euro-atlanti integrációhoz tartozó és más fejlett államok esetében viszonylag korlátozott információ áll rendelkezésre kiberműveleti képességeik részleteire vonatkozóan. Vannak azonban olyan államok, amelyeket az elemzések következetesen összefüggésbe hoznak APT tevékenységekkel és eseményekkel.

Például a dél-koreai kiberbiztonsági szakemberek meglehetősen sok nyilvánosan is megosztható információval rendelkeznek északi szomszédjuk kiberműveleti képességeivel kapcsolatban, amiről Kim Dzsong-un már 10 évvel ezelőtt is úgy nyilatkozott, hogy „a kiberhadviselés egy mindenre használható kard, amely a nukleáris fegyverekkel és hordozórakétákkal együtt garantálja Észak-

Korea Népi Fegyveres Erőinek könyörtelen ütőképességét". (Ji-Young, Jong In és Kyoung Gon, 2019) Az elemzések szerint Észak-Korea ellenfeleivel szemben különböző módokon alkalmazza kiberműveleti képességeit, így megtalálható az anyagi haszonszerzés céljából terjesztett zsarolóvírus, a számítógépes rendszerek rombolására fejlesztett kiberfegyver és a szenzitív információk gyűjtéséhez használt láthatatlan kémkedési eszközök alkalmazása egyaránt. Észak-Korea kiberműveleti képességeinek alapjait még az előző vezető, Kim Dzsong-il rakta le, aki szerint, ha az internet fegyver, akkor a kibertámadások atombombák és a modern háborúkat az elektronikai hadviselés dönti el, ezért a kiberegységeknek kiemelt szerepet tulajdonított. (Ji-Young, Jong In és Kyoung Gon, 2019) Észak-Korea úgy tekint a számítógépes hálózati támadásokat magába foglaló offenzív kiberképességeire, mint egy költséghatékony és letagadható eszköz, amelyet a megtorlás alacsony kockázatával alkalmazhat. (DIA, 2021) A kiberműveletek tervezése és végrehajtása egyfelől a Központi Felderítő Iroda (Reconnaissance General Bureau – RGB) alárendeltségébe tartozó egységek, másrészt a Vezérkar illetékes irodáinak feladata. A haderő kiterjesztett, küldetés orientált kiberspecifikus egységeibe évente 50-60 külföldön képzett elit katona kerül be, így becslések szerint napjainkban 6800 fő lehet a kiberműveleti specialisták száma a haderőn belül. (Ji-Young, Jong In és Kyoung Gon, 2019) Észak-Koreának tulajdonítják többek között a WannaCry[107] zsarolóvírust, a globális bankközi elszámoló rendszer, a SWIFT elleni 2016-ban történt támadást (CrowdStrike, 2016) és a már említett Sony Pictures Entertainment elleni destruktív műveletet. (DIA, 2021) Olyan kiterjedt tevékenységet folytató APT-ket tulajdonítanak Észak-Koreának, mint például az említett három tevékenység mögött álló Lazarus[108], a dél-koreai entitásokat célzó Kimsuky[109] vagy a főként ipari kémkedésre szakosodott APT37[110]. Az Észak-Koreának tulajdonított eseteknél a nyílt források gyakran gyűjtőfogalomként használják a Lazarus elnevezést, ami részben annak köszönhető, hogy feltételezések szerint a hírszerző apparátus

[107] A WannaCry néven ismertté vált globális kibertámadás 2017 májusában az azonos nevű zsarolóvírushoz köthető, ami Windows operációs rendszert futtató számítógépek adatait titkosította, a feloldásért cserébe pedig váltságdíjat kért.
[108] A Lazarus Group további ismert azonosítói: Dark Seoul, Hidden Cobra, Hastati Group, Anderiel, Unit 121, Bureau 121, NewRomanic Cyber Army Team, Bluenoroff, Guardians of Peace. A csoport karakterisztikája összefüggést mutat további APT tevékenységekkel, mint például: Group 77, Labyrinth Collima, Operation Troy, Operation GhostSecret, Operation AppleJeus, APT38, Stardust Chollima, Whois Hacking Team, Zinc, Appleworm, Nickel Academy, APT-C-26, NICKEL GLADSTONE, COVELLITE. Bővebben: https://malpedia.caad.fkie.fraunhofer.de/actor/lazarus_group
[109] A Kimsuky további ismert azonosítói: Velvet Chollima, Black Banshee, Thallium, Operation Stolen Pencil. Bővebben: https://malpedia.caad.fkie.fraunhofer.de/actor/kimsuky
[110] Az APT37 további ismert azonosítói: Group 123, InkySquid, Operation Daybreak, Operation Erebus, Reaper Group, Reaper, Red Eyes, Ricochet Chollima, ScarCruft, Venus 121. Bővebben: https://malpedia.caad.fkie.fraunhofer.de/actor/apt37

rendelkezik azzal a rugalmassággal, hogy az ország igényeihez szabott – alkalmi – kiberegységeket hozzon létre. Ennek eredményeként az infrastrukúrában, a rosszindulatú programokban, az alkalmazott TTP-kben átfedés és az erőforrások megosztása azonosítható .(Barnhart és mtsai. 2022)

A nemzeti kiberképességekkel foglalkozó elemzések és jelentések szerint számottevő kiberműveleti képességekkel rendelkezik Irán is. Ennek egyik oka, hogy Irán az 1979-es forradalom óta folyamatosan politikai ütközési pályán van más nemzetállamokkal, aminek következtében számos szankció sújtja az országot katonai technológia vásárlására és fejlesztésére vonatkozóan. (KFCRIS, 2020) Az ellentétek nyomán kialakult „puha háború" (soft war) lényege, hogy Irán nem áll fizikai háborúban ellenségeivel, de súlyos információs hadviselést folytat. (Jones és Newlee, 2019) Helyzetéből fakadóan Irán az aszimmetrikus katonai képességek mesterévé vált, aminek logikus és értékes kiterjesztése a kiberműveleti képesség. Irán úgy tekint kiberműveleti programjára, mint a számos eszköz egyike, amivel aszimmetrikus, de arányos megtorlást hajthat végre a politikai ellenségeivel szemben. (KFCRIS, 2020) Irán kiberképességei a 2010-es évek első felében bekövetkezett események (ellenzéki Zöld Mozgalom, Stuxnet, Flame) nyomán kezdtek testet ölteni. Az iráni elnök által vezetett Legfelsőbb Kibertér Tanács (Supreme Council for Cyberspace – SCC) a legmagasabb politikai döntéshozatali szint, ami 27 különféle kormányzati és társadalmi szervezetet foglal magába, köztük a haderőt, az Iráni Forradalmi Gárdát, az állami tévét és rádiót, a bíróságot és a parlamentet, valamint a rendőrség mellett a nemzetbiztonságért és telekommunikációért felelős minisztériumokat. A képességek olyan szervezetek kezében összpontosulnak, mint a Nemzeti Kibertér Központ (National Cyberspace Center – NCC), a Nemzeti Passzív Védelmi Szervezet (National Passive Defense Organization – NPDO), a Kiber Rendőrség, a Forradalmi Gárda Hírszerző Szervezete (IRGC-Intelligence Organization), a haderő Kibervédelmi Parancsnoksága, a Hírszerzési és Biztonsági Minisztérium (Ministry of Intelligence and Security – MOIS) és a haderőbe, illetve kormányzati szervekbe integrált Hírszerzési Védelmi Szervezetek (Intelligence Protection Organizations).(IISS, 2021) A kiberműveletek végrehajtására Irán proxy szervezeteket (Mabna Institute, Iranian Cyber Army) is alkalmaz, amelyek lehetnek hazafias vagy pénzügyileg motivált hackerek, szerződéses privát entitások és kvázi kormányzati szervek. Alkalmazásukat Irán esetében is a hihető letagadhatóság fenntartása és az eszkaláció elkerülése indokolja. Támadási metódusaik széles skálán mozognak, ami a weboldalak megrongálásától, illetve felülírásától (defacement), a DDoS támadásokon és adatlopáson át

egészen a destruktív támadásokig terjed. (Theohary, 2020) Annak ellenére, hogy egy olyan skálán, ahol az Egyesült Államok és Kína a 40 és 50 pont közötti tartományba esik, Irán kiberhatalmi ereje viszont a 10 pontot sem éri el (Voo és mtsai. 2020), számos APT tevékenységet tulajdonítanak Iránnak. A legismertebbek közé tartozik az elsősorban közel-keleti, indiai és amerikai szervezeteket célzó MuddyWater [111], a pénzügyi, kormányzati, energetikai, vegyipari és telekommunikációs ellátási láncokat támadó OilRig [112] és a stratégiai kémkedésre fókuszáló APT35[113]. Irán Kínához és Oroszországhoz hasonlóan formálni szeretné a kibertér jövőjét, ezért a nyugati országok dominanciájának kihívójaként (IISS, 2021) az iráni attribúcióval rendelkező APT-k várhatóan a jövőben is hozzájárulnak a rendszer általi belső elnyomáshoz és külföldre irányuló célzott behatolásokhoz. (CrowdStrike, 2021)

Összegzés, következtetések

A IV. fejezet első alfejezetében a fejlett perzisztens fenyegetéseket, vagyis az APT-ket vizsgáltam meg. Előbb meghatároztam az értekezés szempontjából mérvadó értelmezési keretet, majd az APT-k kialakulása és kategorizálása után külön foglalkoztam az állami támogatás szerepével, a működési körülményekkel és az attribúciós nehézségekkel. Az alfejezetben arra kerestem a választ, hogy milyen értelmezési keretek alakultak ki az APT tevékenységek kapcsán és milyen paraméterek, illetve sajátosságok azonosíthatók, amelyek egyfelől hozzájárulnak a rendkívül hatékony működéshez, másfelől összevethetők a fizikai térben megvalósított különleges műveletek jellemzőivel. Ezután a IV.2 alfejezet külön-külön vizsgálta az APT tevékenységek elnevezéséből fakadó három legfontosabb jellemzőjét, a fejlettséget, a perzisztenciát és a fenyegetést. Ezzel az volt a cél, hogy az APT-k jellemzőinek empirikus alátámasztásával megerősítést nyerjen az APT-k által generált kihívás jelentősége és az állami támogatás beemelésével a képességként történő értelmezés.

Az APT-k működési jellemzőinek részletes vizsgálata elsősorban iparági jelentések és beszámolók, illetve kormányzati szereplők által kiadott dokumentumok segítségével valósítható meg. Jelen

[111] A MuddyWater további ismert azonosítói: TEMP.Zagros, Static Kitten, Seedworm, MERCURY, COBALT ULSTER. Bővebben: https://malpedia.caad.fkie.fraunhofer.de/actor/muddywater
[112] Az OilRig további ismert azonosítói: Twisted Kitten, Cobalt Gypsy, Crambus, Helix Kitten, APT34, IRN2. Bővebben: https://malpedia.caad.fkie.fraunhofer.de/actor/oilrig
[113] Az APT35 további ismert azonosítói: Newscaster, Rocket Kitten, Phosphorus, Charming Kitten, Saffron Rose, Parastoo, iKittens, Group 83, Newsbeef. Bővebben: https://malpedia.caad.fkie.fraunhofer.de/actor/charming_kitten

esetben az APT tevékenységek felderítésével és nyomonkövetésével foglalkozó kiberbiztonsági vállalatok, illetve a fejlett kiberképességekkel rendelkező kormányzatok kiadványai nyújtották a kiindulási pontot. Az elemzés eredményeként arra a következtetésre jutottam, hogy az APT-k precíz és egyértelmű célkitűzésekkel rendelkeznek, magasfokú szervezettséget mutatnak és jelentős erőforrásokhoz férnek hozzá, miközben tevékenységük időben elhúzódó, illetve ismétlődő képet mutat. Megállapítottam, hogy az APT-khez köthető tevékenységek jellemzően nagy horderejű, stratégiai és/vagy politikai érdekek mentén megvalósuló incidensek nyomán kerülnek nyilvánosságra. Továbbá az APT-knek tulajdonított tevékenységekre jellemző a kifinomultság, nehezen észlelhetők és adaptív technikai megoldásokat alkalmazva képesek akár hosszú időn keresztül rejtve maradni.

FEJLETT PERZISZTENS FENYEGETÉSEK	FEDETT JELLEG		JELENTŐSÉG			MŰVELETI TERÜLET		MŰVELETI CIKLUS		CÉLZOTTSÁG	ADAPTIVITÁS	SPECIÁLIS ERŐFORRÁSOK	SPECIÁLIS ELVÁRÁSOK
	FELVÁLLALT	LETAGADHATÓ	NAGY HORDERŐJŰ	STRATÉGIAI	POLITIKAI	BELFÖLD	KÜLFÖLD	RÖVID	FOLYAMATOS				
ÁLLAMI HÁTTERŰ APT-K	○	●	●	●	●	○	●	◑	●	●	●	●	●

4. ábra: A fejlett perzisztens fenyegetések jellemzőinek dominancia alapú vizsgálata. Az egyes paraméterek dominanciáját hármas skálán üres (világos), félig teli (világos/sötét) és teli (sötét) körök jelölik. A teli kör jelentése: a paraméter erősen domináns az APT-k tevékenysége során. A félig teli kör jelentése: a paraméter kevésbé domináns. Az üres kör jelentése: a paraméter nem domináns, vagy egyáltalán nem jellemző az APT-k tevékenysége során. (A szerző saját szerkesztése.)

Az APT tevékenységek által kiváltott hatások elemzéséből levonható konklúzió, hogy többnyire négy fő célkitűzés köré épülnek (Bejtlich, 2010). A célkitűzések egyik csoportjába a politikai, illetve geopolitikai célok tartoznak, például a belső stabilitás fenntartása, vagy egy konfliktussal sújtott régió további destabilizálása. A második a gazdasági hatások kiváltása, ami például a jogosulatlanul megszerzett szellemi tulajdon másolásával, eladásával, illetve tanulmányozásával javíthatja a gazdasági versenyképességet, ugyanakkor kapcsolódó további kutatás esetén új és jobb termékek és szolgáltatások olcsóbb előállítása is lehetővé válhat. A harmadik a technikai hatások elérése, ami forráskódokhoz történő hozzáférést, sérülékenységek kihasználására képes kódok írását, illetve a (védelmi) rendszerek kiismerését foglalja magába és az áldozat gyengítését és kizsákmányolását biztosítja. Az utolsó a katonai hatások generálása, melyek kapcsán elmondható, hogy a kibertérre jellemző erőteljes aszimmetria következtében a gyengébb katonai erő képes lehet felül kerekedni nála erősebb és felszereltebb ellenfelén.

A fejlettség részletes vizsgálata nyomán megállapítottam, hogy az APT-k képesek olyan technológiákat felhasználni és kihasználni a tevékenységük során, amelyek speciális szakértelmet és adott esetben kiemelkedő kreativitást igényelnek. A közvetett támadások, melyek az ellátási láncokat érik egyáltalán nem nevezhetők újszerűnek, azonban a rendszerek komplexitásának növekedése miatt még akkor is rendkívüli precizitásra van szükség, ha a támadás megvalósítása kifejezetten egyszerűnek vagy alapszintűnek hat. A kiberfenyegetések és kiberműveletek egységes szempontok alapján történő vizsgálatával arra a következtetésre jutottam, hogy miközben a nulladik napi sérülékenységek drágák, illetve kifinomult bánásmódot igényelnek, az alkalmazásukkal egyrészt megnő az állami támogatás szerepe, másfelől az APT-t támogató állam saját rendszereire nézve is komoly veszélyt jelenthetnek az ilyen sérülékenységek.

A perzisztencia vizsgálatával kimutattam, hogy akár több száz napon át képes egy APT tevékenység észrevétlen maradni az áldozatok számítógépes rendszerein és hálózatain. Ez jelentős mértékben annak köszönhető, hogy az APT tevékenység nem folyamatos, hanem perzisztens, azaz tartósan fennálló. Vagyis az áldozat rendszereit védő kiberbiztonsági szakemberek és rendszerek nem szembesülnek folyamatos anomáliákkal, ami alapján a támadás észlelhető lenne. Az APT tevékenység jellemzően visszatérő megfigyelést és adatlopást takar magasfokú reaktivitással kombinálva. Így a kibervédelmi intézkedésekre gyors válaszlépések adhatók, a művelet fenntartható marad.

Megállapítottam, hogy az APT tevékenységek több alkalommal is bizonyították, hogy képesek a virtuális és fizikai világ közötti határok átlépésével hatásokat kiváltani, ezért súlyos fenyegetést jelentenek az államok politikai-társadalmi berendezkedésére. Geopolitikai, energiabiztonsági és egyéb célok mentén képesek szenzitív információkat megszerezni, manipulálni vagy akár bomlasztó hatást kiváltani, miközben a letagadhatóság olyan magas szintje érvényesül, amivel egyetlen fizikai művelet sem képes versenyezni. Mindez hozzájárul az eszkaláció elkerüléséhez és alacsonyan tartja a megtorlás kockázatát, ami kifejezetten előnyös eszközzé teszi a kiberműveleti képességeket azokban az esetekben, amikor a nemzeti érdekek érvényesítése egy másik állam kárára történik.

A IV. fejezet alapján igazoltam azt a feltevésem, hogy az APT-k az információs társadalom és a hálózat alapú világ legjelentősebb kihívásai közé sorolhatók, miközben a kiberműveleti képességekkel rendelkező államok jelentős részénél átfedés mutatható ki az APT-k

karakterisztikájával. Továbbá arra a következtetésre jutottam, hogy a kiberműveleti képességeket a nemzetközi kapcsolatok szereplői a konfliktusos és kevésbé konfliktusos időszakokban egyaránt érdekérvényesítési céllal alkalmazzák politikai, gazdasági, technikai és katonai hatások elérése érdekében, maximálisan kihasználva az alacsony láthatóság/észlelhetőség és a letagadhatóság nyújtotta előnyöket.

V. Védelmi szervezetek különleges műveleti képességei

Bevezetés

Az II.4 fejezetben meghatározott védelmi szervezetek, azaz jelen keretek között a haderők, a rendvédelmi szervek és a nemzetbiztonsági szolgálatok jellemzően rendelkeznek olyan speciális képességekkel, illetve szolgálati ágakkal, amelyek a szervezet alapvető rendeltetéséhez valamilyen különleges képességgel járulnak hozzá. Ez az esetek túlnyomó többségében arra utal, hogy az ilyen egységek a szervezet által végzett hagyományos tevékenységekhez képest eltérő – különleges – módszereket, eljárásokat, felszerelést és eszközöket alkalmaznak feladataik végrehajtása során. Mindez tipikusan speciális szaktudást és ismereteket igényel a szervezet tagjaitól, ezért a kiválasztás és a kiképzés, illetve felkészítés is speciális körülmények között zajlik. Nem cél a védelmi szervezetek általános bemutatása és a különbségek feltárása, kizárólag a védelmi szervezetek különleges műveleti képességeinek ismertetése áll a fejezet fókuszában. Az ismertetés nem specifikus szervezetre vagy nemzeti képességre koncentrál, hanem a különleges műveleti képességek átfogó bemutatására a haderők, illetve a rendvédelmi és nemzetbiztonsági ágazat tekintetében.

V.1 Katonai különleges műveleti erők

A különleges műveleti erők (Special Operations Forces – SOF) olyan speciálisan kiválasztott személyzetből álló szervezetek, amelyek nagy kockázatú, nagy értékű különleges műveletek végrehajtására vannak megszervezve, felszerelve és kiképezve. Katonai, politikai, gazdasági vagy információs célok elérése érdekében, speciális és egyedi műveleti módszerek alkalmazásával ellenséges, korlátozott hozzáférésű vagy politikailag érzékeny esetekben és területeken kerülnek

bevetésre a kívánt taktikai, műveleti és/vagy stratégiai hatások elérésére béke, konfliktus vagy háború idején. A SOF költséghatékony és hatásos képességek, illetve lehetőségek széles skáláját kínálja a kormányzatok számára a normál katonai környezeten és képességkészleten kívül. Az a képességük, hogy rövid időn belül, számos területen, helytől függetlenül, nagy valószínűséggel sikerrel produkálják az elvárt eredményeket, nagy feltűnést kelt a politikai és katonai döntéshozók körében. Colin Gray [114] szerint a különleges műveleti erők a nemzeti vagyon részei a nagystratégia[115] szintjén: az államhatalom eszközei, amelyek sebészi pontossággal alkalmazhatók a diplomácia és a (többféle) külföldi segítségnyújtás támogatására a reguláris katonai erők létfontosságú kiegészítőjeként, vagy független fegyverként. (Horn, 2014)

V.1.1 A különleges erők feladatrendszere[116]

Már itt, az alfejezet legelején fontos kiemelni, hogy a nem háborús műveletek során a különleges műveleti erők képességeikkel segítik az ország nemzeti érdekeit szolgáló politika érvényesülését. (Gottlieb, 1987) Teszik mindezt úgy, hogy például az Egyesült Államok esetében a haderő éves költségvetésének mindössze 4 százalékát fordítják a különleges műveleti erőkre, miközben a létszám a teljes haderőre vetítve 5 százalék körül mozog. (Robinson, 2013)

A különleges műveletek olyan katonai műveletek, amelyek egyedi alkalmazási módokat, taktikákat, technikákat, felszerelést és kiképzést igényelnek. Ezeket a műveleteket gyakran ellenséges, korlátozott hozzáférésű vagy politikailag érzékeny környezetben hajtják végre, és a következő elemek közül egy vagy több jellemzi őket: időérzékeny, titkos, rossz láthatóság, helyi erőkkel és/vagy azon keresztül hajtják végre, regionális szakértelmet igényelnek, és/vagy nagyfokú

[114] Colin S. Gray (1943-2020) brit-amerikai geopolitikai gondolkodó, a Reading Egyetem professzora és Stratégiai Tanulmányok Központjának igazgatója. Korábban szolgálta a brit és az amerikai kormányt védelmi tanácsadóként, illetve 5 éven keresztül részt vett az amerikai fegyverzetkorlátozási és -leszerelési törekvéseket koordináló testület munkájában is.

[115] A nagystratégia fogalmát Basil Henry Liddell Hart brit katonai gondolkodó alkalmazta a nemzet, vagy ország-csoport minden olyan erőforrásának koordinálására és irányítására, ami a háború politikai célkitűzéseinek elérését szolgálja és amit az alapvető politika fogalmaz meg. Bővebben lásd Forgács Balázs A hadikultúra fogalmának historiográfiája II. című publikációjában: http://epa.oszk.hu/02400/02463/00006/pdf/EPA02463_hadtudomanyi_szemle_2009_3_001-008.pdf

[116] A különleges műveleti képesség magába foglalja a különleges műveleti erőket, ami a Magyar Honvédség esetében olyan gyűjtőfogalom, amibe bele tartoznak a különleges erők, a különleges támogató gyalogos erők, a különleges műveletek végrehajtására képes erők, a különleges műveleti repülő erők és együttműködő erők. Bővebben: https://epa.oszk.hu/02400/02463/00012/pdf/EPA02463_hadtudomanyi_szemle_2012_1-2_010-028.pdf Más országok haderői esetében ennél több vagy kevesebb erőt is lefedhet a különleges műveleti képesség és a különleges műveleti erő fogalma, ezért a feladatrendszer átfogó megközelítést alkalmazva kerül bemutatásra és nem tér ki a különleges műveleti erők közötti eltérésekre.

a kockázat. A katonai különleges műveleti erők jellemzően a védelempolitika legfelsőbb szintje, illetve a védelmi miniszter által kijelölt szolgálatok aktív és bizonyos esetekben tartalékos komponensei, amelyek kifejezetten a különleges műveletek lebonyolítására és támogatására vannak megszervezve, kiképezve és felszerelve. (Feickert, 2022)

A katonai különleges műveleti erők stratégiai vetületű feladatai magukba foglalják például a partnerek képességeinek erősítését (belső ellenállás és külső elrettentés) alacsony költségek és állandó jelenlét mellett, alacsony láthatóságú szerepvállalási képességet beleértve az ellenséges tevékenység követését és felkészülést magasabb intenzitású eshetőségekre, az ellenfél hálózatainak megzavarását vitatott környezetben, az ellenséges kormányok fenyegetését nem hagyományos hadviselés útján, illetve olyan képességet, amelyekkel helyettesítők útján léphet fel az erőszakos tevékenységekkel szemben, továbbá az információs műveletek erősítésének képességét is. (Watts és mtsai. 2021)

A különleges műveleti erők feladatai országonként, vagy akár haderőnemenként is mutathatnak kisebb mértékű eltérést, de általánosságban elmondható, hogy három összetevőből állnak: különleges felderítés, közvetlen harci akciók, katonai segítségnyújtás. A különleges felderítő tevékenység olyan feladatokat ölel fel, mint a hadműveleti terület parancsnoki döntéshez szükséges értékelését, kiemelt célpontok folyamatos felderítését, illetve meteorológiai, geográfiai, hidrográfiai és csapás utáni helyzetre vonatkozó adatok gyűjtését és jelentését. A közvetlen harci akciók során a különleges műveleti erők lesállásokat létesítenek, rajtaütéseket és más támadó akciókat hajtanak végre. Robbanó- és egyéb zárakat telepítenek, tűzcsapást hajtanak végre földi, légi és tengeri járművekről, precíziós lőszerek célravezetését végzik és önálló szabotázsakciókat hajtanak végre. A katonai segítségnyújtás a különleges műveleti erőkkel összefüggésben a baráti vagy szövetséges katonai erők számára békében, válságban vagy konfliktusban nyújtott különleges műveleteket jelenti és magába foglalja ellenálló vagy gerilla erők kiképzését, felszerelését, támogatását és szükség esetén vezetését. De ide sorolhatók a humanitárius válságok során nyújtott békeműveleti támogató tevékenységek, az összekötő csoportok támogatása, illetve a kiszabadítási és menekülési hálózatok felkészítése is. (Kőszegvári, 2006)

A különleges műveleti képességek tekintetében élenjáró Egyesült Államok különleges műveleti operátorait az elérhető információk alapján több mint 100 országban alkalmazzák a partnerek képzésére, kapacitásuk fejlesztésére és a velük való hosszú távú kapcsolatok előmozdítására, ami

továbbra is a közvetett megközelítés központi eleme. Az Egyesült Államok különleges műveleti szakértelme páratlan, és nagyon keresett a külföldi haderők, rendőri erők és a belbiztonsági szervezetek körében. Az amerikai elit speciális operátorok olyan képességekkel, taktikával, speciálisan tervezett felszereléssel és hírszerzési tudással (know-how) rendelkeznek, amelyek átalakíthatják egy külföldi kormány meglévő képességeit. (Kashkett, 2017)

Ugyanakkor a SOF az elsődleges terrorizmus elleni feladatok mellett egyre inkább az autoriter nagyhatalmakkal vívott harcban is szerephez jut. Utóbbi főként információk gyűjtésével, szövetségesekkel és partnerekkel való együttműködéssel, stratégiai rajtaütésekkel, válságkezelési szerepvállalással és az ellenfelet sújtó károkozással valósítható meg. (Brands és Nichols, 2020) A különleges műveleti erők kihívásainak és ezáltal feladataik átalakulását támasztja alá Sándor Tamás vezérőrnagy, a Magyar Honvédség Különleges Műveleti Parancsnoksága különleges műveleti személyjének álláspontja, ami a közel azonos képességű és felszereltségű ellenfelekkel való szembenállás tekintetében hívja fel a figyelmet az aktuális változásokra. (Trautmann, 2021b) (Lásd bővebben az VI.1.1 alfejezetben.)

V.1.2 A különleges erők jellemzői, a működés körülményei és feltételei

Ahogy azt Forray László írja, a „*különleges műveletek végrehajtásának sikere az egyének és kis alegységek profizmusán, a gyakran nem hagyományos, speciális képességeinek sokaságán múlik, amelyeket rugalmassággal, rögtönzésekkel és önállósággal alkalmaznak. A kis méret, az egyedülálló képességek és a (korlátozott idejű) önellátás képessége teszi lehetővé, hogy a különleges műveleti erők megfelelő és megvalósítható katonai reagálást biztosítsanak […]. Ezek a műveletek kevésbé járnak a helyzet eszkalációjának kockázatával, amely a nagyobb méretű, jobban látható hagyományos erők alkalmazásában rejlik.*” (Forray, 2012)

Nem csak a magyar SOF tekintetében mondható el, hogy katonáikat *„arra képezik ki, hogy saját vagy barátságos erőktől távol, kisalegységekben működjenek. Ezek az erők úgy vannak felszerelve, hogy kíméletlen környezeti tényezők között is képesek legyenek hosszabb időn keresztül feladatuk kivitelezésére. A különleges erők műveleti elemének egyedi képessége még az adott működési környezet előzetes értékelése, elemzése és az azt befolyásoló körülmények vizsgálata.”* (Forray és Gerőcs, 2013) Ennek eredményeként a magyar különleges műveleti csoportok az afganisztáni szerepvállalásuk során saját maguk hajtottak végre folyamatosan elemzést, értékelést, s így

generáltak feladatokat, azonosítottak célszemélyeket, célobjektumokat. Ezek értékelésével a csoportok dolgozták ki a feladatvégrehajtás terveit, majd ezt megküldték az elöljárónak és az elöljáró a jóváhagyást követően az erőforrások leosztásával segítette, menedzselte a végrehajtását. (Trautmann, 2021b) A magyar különleges műveleti katonák Afganisztánban megtapasztalták a hálózat-központú hadviselés nyújtotta lehetőségeket és később a gyakorlatban sikeresen alkalmazva azokat, napjainkra képesek a műveleti területen egymástól függetlenül, minimális elöljárói irányítással, önállóan, a parancsnok elképzelését követve, a számukra meghatározott műveleteket végrehajtani." (Forray és Gerőcs, 2013)

A kis kötelékek által végrehajtott különleges műveletekre jellemző a célirányosság (stratégiai vagy hadműveleti tevékenység), a támadó jelleg, az erőkoncentráció (egy helyre történő összpontosítás), illetve az erősokszorozó tényező (a hagyományos erőkhöz képest nagyobb pusztítást végez). Ezek mellett a különleges műveletekre jellemző az erők és eszközök gazdaságos alkalmazása, a mozgékonyság, a vezetés egysége, az információ és fizikai védelem, a meglepetés és az egyszerűség. A vonatkozó magyar katonai doktrína alapján „*a különleges műveletek végrehajtására alkalmazott állomány feladatvégzésének célja a stratégiai, hadműveleti szintű tevékenység, amit kiemelt célpontok elleni, kiemelt kockázati szintű tevékenység jellemez. Ebből kifolyólag a feladatot végrehajtó állomány és annak felszerelése a hagyományos feladatellátást végző katonai alegységeknél speciálisabb, ezen kívül sikertelenségük, esetleges elvesztésük nagyobb kockázatot eredményezhet stratégiai szinten. Mindezek miatt az említett jellegű műveletekre jellemző a messzemenőkig részletes tervezés, a körültekintő telepítés, a speciális felszerelés használata. A végrehajtó állomány esetében pedig nélkülözhetetlen a rejtett, vagy fedett jelleg miatt az elszigetelt feladat-végrehajtásra való képesség, ami megfelelő szintű kiképzéssel, felkészüléssel erősíthető. Azért is kiemelt fontosságú a felkészítés, mert a különleges erők katonái a döntéseiket az ellenséges vonalak mögött, és akár interkulturális közegben kell, hogy meghozzák."* (Völgyi, 2017)

A SOF tevékenység jellege kapcsán gyakran merül fel a fedett (covert), illetve titkos (clandestine) jelző, ami egyfelől értelmezhető a műveletet engedélyező és támogató szervezet kilétének elrejtésére, másfelől az egész művelet létezésének elfedésére. Utóbbi esetben a művelet sikere gyakran azon múlik, hogy a tervezés és a megvalósítás titokban maradjon, ugyanakkor a végrehajtást követően a támogató vállalja a felelősséget. Ezzel szemben a hagyományos katonai

műveletek jellemzően nyíltak (overt). (Robertsen, 2007) A támogató kilétét elfedő műveletre jó példa az orosz különleges erők alkalmazása a Krím-félsziget 2014-es megszállása idején, míg a teljes titoktartással tervezett és kivitelezett művelet kapcsán Osama bin Laden likvidálása bír precedens értékkel.

De akkor miért különleges ebből a szempontból a SOF? A válaszok a SOF szervezeti felépítésében és foglalkoztatási módszertanában rejlenek. A speciális műveletek akkor a legsikeresebbek, ha az alkalmazás módja alacsony profilú. Ez a karakterisztika a hagyományos hadműveletektől eltérően, lehetővé teszi az alkalmazó számára műveleti tevékenység folytatását olyan régiókban, ahol a külső segítségnyújtás politikailag népszerűtlen lehet, vagy ahol az alkalmazó ország hadseregének jelenlétét esetleg nem értékelik. Azt, hogy a SOF képes úgy működni, hogy nem kelt túlzott feltűnést tevékenységével, jól jelzi a területek magas száma, ahol SOF alkalmazására sor került, azonban a bevetést nem követte nyilvános felháborodás és média figyelem. Ahogy azt az alfejezetben korábban is érintettük, a szervezet által elérni kívánt hatás átfogó megértése érdekében a taktikai egységek tudják legjobban felmérni (első kézből származó ismereteik alapján), hogy mit kell tenni a siker érdekében. Ebben kockázatot jelent, hogy ha nincs jól kommunikált cél, előfordulhat, hogy a taktikai egységek erőfeszítései nem lesznek szinkronban. Illetve kihívás annak biztosítása, hogy a legkisebb csapatig minden parancsnoki szint megértse, hogyan illeszkedik a feladatuk a stratégiai célokhoz. Ez megköveteli, hogy hagyományos társaikhoz képest a különleges műveleti beavatkozók már pályafutásuk korai pontján kiterjedt ismereteket szerezzenek és megismerjék a biztonsági stratégiákat. Erre azért van szükség mert nagyon valószínű, hogy egy országban a rangidős különleges műveleti operátor egy tiszt vagy főtiszt, akit egy rendkívül tapasztalt altiszt vagy tiszthelyettes közvetlenül támogat. Egy ilyen elrendezés példátlan lenne hagyományos haderő esetén, és ez az oka annak, hogy a különleges műveleteket magasan képzett és kiképzett operátorok hajtják végre a küldetés kudarcával vagy lelepleződésével járó jelentős – elsősorban politikai – kockázatok miatt. (Peterson, 2014)

V.1.3 Képzés, kiképzés és követelmények a különleges műveleti erőknél

Kialakulásuk óta a különleges műveleti erőknek sikerült demonstrálniuk stratégiai hasznosságukat azáltal, hogy képesek a válságos helyzeteket időben és megfelelő választ adva kezelni, többnyire innovatív és adaptív megoldásokkal. Ennek a központi elemei azok az egyének, akik fejlett kognitív készségeiket alkalmazva, agilis módon képesek felmérni a helyzetet. Teszik mindezt

gyakran hiányos információkkal és/vagy kétértelmű, illetve kaotikus körülmények között, olyan kreatív megoldások kidolgozásával, amelyeket nem korlátoznak a doktrínák vagy a konvenciók. (Horn, 2014)

A különleges műveleti állománynak ehhez kiegészítő kiképzés szükséges nyelvi, kultúrák közötti kommunikáció, területi orientáció, biztonsági segítségnyújtáshoz kapcsolódó jogi, önvédelmi és általános jogi, illetve emberi jogi területen (Gottlieb, 1987). Ugyanakkor a különleges műveleti erők állományába történő bekerüléshez többnyire összetett feltételrendszernek kell megfelelni. A különleges erők eltérő követelményeket alkalmazhatnak, de jellemzően a jelentkezőknek felsőfokú végzettséggel kell rendelkezniük, a fizikai és pszichológiai felméréseken kiemelkedő teljesítményt kell nyújtsanak, az ejtőernyős és úszó képességek megléte is fontos, továbbá olyan biztonsági átvilágításon is meg kell felelni, ami alkalmassá teszi a jelentkezőket a szigorúan titkos besorolású információk megismerésére. Bár a SOF kiválasztási folyamat főként a fizikai erőt próbára tevő elemei és a jelentkezők jelentős számú lemorzsolódása miatt vált ismertté szélesebb körben, a kiválasztásnak lényegi elemét képezik a mentális, tanulási és személyiségi tesztek (Russell és mtsai. 1995).

A SOF tevékenységek kockázatos, szokatlan és megerőltető jellege ellenére a jelöltek értékelését és kiválasztását ugyanazok az elvek határozzák meg, mint a többi szofisztikált szervezet jelöltjeinek esetében. A felmérő és kiválasztási rendszer alapja a munkaköri elemzés, amely képes meghatározni a tudást, a készségeket, képességeket és más személyi karakterisztikákat (Knowledge, Skills, Abilities, and Other characteristics – KSAOs) amik előre jelzik a sikeres teljesítményt. Ehhez különböző formátumú eljárásokra, valamint a szakterületi specialisták, a személyzet-kiválasztó és a klinikai szakemberek közötti együttműködésre van szükség, ami egyúttal növeli a rendszer létjogosultságát, megbízhatóságát és jogi védettségét. Anélkül, hogy mélyebb technikai részletekbe mennénk az említett jellemzők vizsgálata és más elemző-értékelő modellekkel történő kombinálásuk kapcsán, röviden az alábbi meghatározások alkalmazhatók. A tudás alapvetően munkaköri teljesítmény szempontjából releváns, emlékezetből előhívható technikai ismeretek, koncepciók, nyelvek és eljárások meglétét méri. A készségek fejlesztéssel vagy kiképzéssel szerzett kapacitásra vonatkoznak, amelyek különböző feladatok eszközökkel, felszereléssel és gépekkel történő végrehajtásához szükségesek. A képességek relatív tartós kapacitást takarnak a készségek vagy ismeretek megszerzésére, illetve olyan feladatok elfogadható

szintű elvégzésére vonatkozóan, amelyeknél az eszközök, felszerelések és gépek nem fontosak. Az egyéb személyi jellemzők fedik le a munkakörhöz kapcsolódó érdeklődési köröket, preferenciákat, a temperamentumot és személyiség jegyeket, amik megmutatják, hogy egy személy milyen jól teljesít a mindennapi rutin során. (NATO, 2012)

V.2 Rendvédelmi speciális egységek

A rendvédelmi speciális alakulatok, vagy ahogy a rendvédelmi szakzsargon gyakran hivatkozik rájuk, a rendvédelmi speciális szolgálati ágak létrejötte főként a mai értelemben vett klasszikus terrorcselekményeknek köszönhető. Ezek az 1960-as években kezdtek el általános jelenséggé válni a világban, ezen belül is Nyugat-Európában. Akkoriban a kor terrorszervezeteinek (Vörös Hadsereg Frakció - Rote Armee Fraktion, Vörös-Brigádok - Brigate Rosse, Közvetlen Akció - Action Directe, Fekete Szeptember - Black September) olyan politikai jelenségek szolgáltak bázisul, mint például a diáklázadások, szélsőbaloldali csoportok, vagy az arab/palesztin nemzeti mozgalmak. A terrortámadások megelőzésére és megszakítására (felszámolására) elsősorban katonai megoldásokat alkalmaztak, azonban nem háborús (műveleti) területen ezek kevésbé bizonyultak hatékonynak. Ehhez hozzájárult az is, hogy az államok többsége főleg Nyugat-Európában szigorúan szabályozta, nem ritkán tiltotta, hogy hadserege békeidőben az országhatárokon belül bevethető legyen. (Beke, 2020)

A rendvédelmi speciális egységek kialakulása az Egyesült Államokban is az 1960-as években kezdődött, amikor Los Angeles városának rendőrségén belül megalakult az első Speciális Fegyverek és Taktikák (Special Weapons and Tactics – SWAT) alkalmazására szakosodott egység. Az azóta eltelt idő alatt szinte minden rendvédelmi szerv létrehozta saját taktikai csapatát, amelyek jellemzően az Igazságügyi Minisztérium vagy a Belbiztonsági Minisztérium alárendeltségébe tartoznak és számuk meghaladja a 271-et. Idő közben feladatrendszerük is átalakuláson ment át, mivel egyre gyakrabban kerülnek bevetésre nagy horderejű bűncselekmények esetén, illetve különösen veszélyes bűnözőkkel szemben. (James, 2015)

V.2.1 A rendvédelmi speciális egységek feladatrendszere

Bár a rendvédelemi szektorban is beazonosítható több olyan speciális egység, amelyek a rendőrökkel szemben támasztott átlagos követelményeken felüli extra elvárásokkal rendelkeznek

az állomány tagjainak tekintetében, illetve feladataikat az átlag rendőr eszközrendszerétől eltérő speciális eszközökkel hajtják végre (pl.: kutyás szolgálat, tűzszerész szolgálat, légirendészet), a téma szűkítése miatt csak a különleges fegyvereket és taktikákat alkalmazó, a köznyelvben kommandóként ismert egységekkel foglalkozunk. Az alkalmazott megközelítés értelmében a speciális rendőri egység minden figyelmét a fizikai erő és kényszer alkalmazására fordítja, míg a többi nem speciális rendvédelmi egység sok mást is csinál ezen kívül. (Rantatalo, 2013)

A gyakran rendőrségi paramilitáris egységnek is nevezett speciális alakulatokra nincs univerzális definíció. Jellemzően kiemelt bűnüldöző csoportokról van szó, amelyek tagjait a közbiztonságot fenyegető olyan kritikus események megoldására toborozzák, választják és képzik ki, illetve szerelik fel és jelölik ki, amelyek egyébként meghaladnák a hagyományos rendészeti gyorsreagáló (first responder) és nyomozó egységek képességeit. Fontos különbség a hagyományos rendvédelmi egységekhez képest az erőfeszítéseik és tevékenységük, amik egyértelműen a taktikai megoldásokra fókuszálnak (James, 2015), illetve feladataik dedikáltan az erőszak koncentrált alkalmazásával járnak. (Rantatalo, 2013)

A speciális rendvédelmi alakulatok feladatai több ponton is párhuzamot mutatnak a katonai különleges műveleti erők közvetlen akcióival. Manapság a speciális rendvédelmi alakulatok feladatai között megtalálható a terrorizmus elleni tevékenység, illetve az ehhez kapcsolódó készenléti és reagáló képesség. Szintén a speciális rendvédelmi egységek foglalkoznak a túszmentő szituációkkal, illetve a fegyveres és öngyilkos hajlamú magukat elbarikádozó elkövetőkkel. Nem idegen a speciális egységek számára, hogy erőszakos, mentálisan beteg személyekkel kell interakcióba lépniük, de gyakran vetik be őket magas kockázatú letartóztatások és elkövetők felkutatása esetén is. (IACP, 2011)

A szűkös forrásbázis alapján az európai megközelítésről svéd példán keresztül kaphatunk képet. A speciális rendőri egységek két fő feladata a terrorizmus elhárító tevékenységek, illetve a területi rendőrség által kért támogatás nyújtása különféle beavatkozások során. Utóbbiak magukba foglalnak nagy kockázatú, veszélyes helyzeteket, tárgyalási technikákat igénylő szituációkat, túszejtést, a nehéz és komplex környezetben zajló beavatkozás kapcsán megfigyelést és feltérképezést, különféle merülési (búvár) feladatokat, illetve bármilyen szituációt, amiben az egység speciális kiképzése és kompetenciája hozzájárulhat az incidens sikeres megoldásához. (Rantatalo, 2013)

Bár a közvélemény számára főként a nagy horderejű incidensek kapcsán lehetnek ismerősek, a speciális rendőri egységek nem csak terroristák elfogásával és veszélyes bűnözők lefegyverzésével foglalkoznak. Komplex feladatrendszerükből és kiképzésükből fakadóan képesek végrehajtani rajtaütéseket, orvlövésszel szembeni akciókat, rendőri megfigyeléseket, kiemelt személyek védelmét ellátni, illetve kiemelési és kimenekítési szituációkat, valamint robbantásos támadásokat is képesek kezelni. (Ferguson, 1991)

V.2.2 A speciális rendvédelmi tevékenységek jellemzői és feltételei

A speciális rendvédelmi alakulatok nem csak feladatrendszerük tekintetében mutatnak párhuzamokat a katonai különleges műveleti erőkkel. Ahogyan sok másik országban, hazánkban is alapvetően a haderők állományából, elsősorban azoknak is a speciális egységeitől, a mélységi és csapatfelderítőktől érkezett az a szaktudás, amivel az 1960-70-es években el tudták kezdeni a rendvédelem speciális egységeinek kialakítását. (Beke, 2020) Ebből a közös pontból fakad az is, hogy a rendvédelmi taktikai bevetési egységek mind létszámban, mind az egység tagjainak szerepe kapcsán ugyan eltérésekkel, de szintén hasonlóságot mutatnak a katonai különleges műveleti erők bevetési csapataival. A különleges műveleti erőkhöz hasonlóan van parancsnok, parancsnok-helyettes, beavatkozók, illetve operátorok helyett rohamcsoportosok, illetve felszámolók, mesterlövészek, műszakisok, illetve speciális elfogó-kutyavezetők (Beke, 2020), valamint felcserek is.

A rendvédelmi speciális egységeknél külön foglalkoznak a lőkiképzéssel, a közelharccal, a taktikai ismeretekkel, a tervezés-szervezés feladataival és a műszaki-technikai területtel (Beke, 2020), amire azért van szükség mert a speciális feladatokat csak speciális felkészítéssel lehet sikeresen megvalósítani, így külön figyelmet fordítanak a bevetések során szükséges képességek és feltételek meglétére. Az amerikai rendvédelmi speciális egységek számára több taktikai és műveleti szabványt is meghatároztak az idők során, melyek magukba foglalják a szervezeti struktúrát, az alkalmazott eszközöket és anyagokat, a fegyverzetet, illetve a ruházatot is. A csapatok jellemzően rendelkeznek egy taktikai parancsnoksággal, ami a parancsnokot és a csapatvezető mellett a támogató (hírszerzés, rádió kezelés, felvétel készítés) személyzetet jelenti. A felszámolók jellemzően kettesével vannak beosztva és halálos, illetve nem halálos fegyverekkel, bizonyos esetekben taktikai kutyákkal látják el feladatukat. A rohamcsoportosok, illetve behatolást végzők

összetétele a feladat típusától és komplexitásától, valamint a műveleti környezettől függően változhat, de a tagok biztonsága elsődleges az összeállításnál. (NTOA, 2018)

A rendvédelmi speciális alakulatok a feladataikhoz illeszkedő speciális felszereléssel vannak ellátva, így esetükben az egyéb védőfelszerelés (kesztyű, szemüveg, térd és könyök védő stb.) mellett alapvető a lövedékálló mellények és sisakok használata. A rövid és nagy hatótávolságú halálos és nem halálos lövedékek, illetve fegyverek alkalmazása mellett a vegyi anyagok bevetése is gyakori. Utóbbira jó példa a füst, illetve könnygáz gránátok és lövedékek használata. A fegyverek jellemzően precíziós optikai rendszerekkel vannak felszerelve, illetve elterjedt az éjjellátók, valamint a különböző infra- és hőképet biztosító eszközök alkalmazása. A helyszínek megközelítésére speciális, gyakran páncél védettséggel ellátott járműveket használnak, míg a behatolást olyan eszközök segítik, mint a faltörő, a feszítő vas, illetve nagyteljesítményű feszítő-vágó és speciális zárnyitó szerszámok és megoldások (ballisztikai, mechanikai, termikus, hidraulikus). A feladatok végrehajtását egyre gyakrabban segítik taktikai robotok, pilóta nélküli repülő járművek, továbbá egyre erősebb a technikai és felderítő felszerelések alkalmazása (miniatűr kamerák, száloptikai megoldások stb.). A légi és vízi környezetben folytatott tevékenységekhez szükséges speciális felszerelések szintén az egységek rendelkezésére állnak. (NTOA, 2018)

A rendvédelmi speciális egységekkel szemben támasztott elvárásokat és követelményeket, valamint a működési feltételeket jellemzően a létrehozó (rendőrség, önkormányzat, kormány ügynökség stb.) határozza meg, ezért nem ritkák az eltérések a különböző egységek között még országon belül sem. Ugyanakkor általánosan elmondható, hogy a feladatok kiemelkedő fizikai kondíció meglétét kívánják, miközben a tagok ismeretei a fegyverek, robbanószerek, vegyi eszközök, taktikai eljárások tekintetében is átlagon felüliek kell legyenek. Erre épül rá a különböző munkakör, illetve beosztás specifikus szakismeret, aminek meglétét és frissítését rendszeresen ellenőrzik, akár csak az egészségügyi, fizikai, pszichológiai és biztonsági alkalmasságot.

V.2.3 Képzés, kiképzés és követelmények a speciális rendvédelmi egységeknél

A magyar rendőrség az internetes felületén azt írja a speciális alakulata kapcsán, hogy *„az osztály állományába kerülőknek összetett és különleges szempontoknak kell megfelelniük. Kizárólag többéves szakmai tapasztalattal, kiváló állóképesség és lőtudás birtokában fogadja be őket a csapat. Az egység tagjaival szembeni elvárás, hogy jogi tájékozottságuk, intézkedéstaktikai*

jártasságuk, reflexeik, valamint fizikai erejük messze haladja meg az átlag rendőrtől kívánatos színvonalat. A kimagasló képességek szinten tartásához folyamatos képzések és lelkes önképzés szükségeltetik." (Fenyvesi, 2019)

Mindez elmondható szinte bármelyik speciális rendvédelmi alakulatról. Nem ritka, hogy minimum 3-5 éves szakmai tapasztalatot várnak el a jelentkezőktől és a rendőri szakma minden területén kiemelkedő teljesítményt kell nyújtaniuk. A kiválasztásnál számos írásbeli, szóbeli és fizikai teszten kell megfelelniük, amihez háttér elemzés és pszichológiai felmérés is társul. (Singh, 2001) Mindenütt fontos, hogy csapatjátékosokat keresnek, a speciális egységekben alapvető a csapatmunka, így a magányos farkasoknak nincs helye az ilyen alakulatoknál. (Ferguson, 1991) A tagoknak egyéni szinten és csapat szinten is rendszeresen vizsgákat kell tenniük és évente akár többször is újra igazolniuk kell a specializációjukhoz szükséges szaktudás és ismeretek meglétét. (Ventura County Sheriff's Office, 2019)

A speciális rendvédelmi alakulatok tagjainak kiképzése jellemzően olyan területekre fókuszál, amivel a mindennapi tevékenységük, illetve a bevetések során találkozhatnak. Így külön figyelmet kapnak az épületekbe történő behatolási és az épületeken belüli kereső technikák, a dinamikus behatolási technikák, továbbá a speciális fegyverek és járművek kezelésének elsajátítása. A speciális alakulat tagjai akár csak a katonai alakulatoknál további szakirányú képzést és felkészítést kapnak, annak függvényében, hogy milyen munkakörben dolgoznak. Ilyen lehet a mesterlövész, a taktikai vezetői, a tűzszerész vagy a túsz- és válsághelyzeti tárgyaló kiképzés. A legtöbb esetben elvárásként jelenik meg az idegennyelv ismeret, a régió kulturális beágyazottságának ismerete, valamint a mentális és emocionális stabilitással társuló döntésképesség. Az előképzettségi feltételeket, illetve az alakulatok tagjaként további képesítéseket jellemzően rendvédelmi akadémiai keretek között lehet megszerezni, de gyakori, hogy az alakulat saját maga gondoskodik bizonyos szaktudás fejlesztéséről. Elterjedt szokás, hogy a speciális rendvédelmi egységek közösen gyakorlatoznak a katonai különleges műveleti erők alakulataival és különféle eljárásokat és technikákat sajátítanak így el, mivel számos területen (mesterlövész, gerilla hadviselés, kis alegység taktikák stb.) átfedések vannak, azonban ez a módszer sokszor jogi és alkotmányossági problémákat vet fel, mivel így éles helyzetben a rendvédelmi szervek katonai taktikát alkalmaznak civilekkel szemben. (Singh, 2001)

A képzés és kiképzés, valamint a megszerzett tudás és képességek megfelelő szintentartása fontos eleme a speciális rendvédelmi alakulatok mindennapjainak. Az alakulatok tagjai a szolgálati idejük 25-50 százalékát töltik gyakorlatozással és edzéssel, amihez további tréninggel töltött idő párosul a különböző speciális beosztásokhoz szükséges szakismeretek miatt. Nincs univerzális, minden speciális alakulat által elfogadott szabvány arra vonatkozóan, hogy a rendvédelmi szektorban mennyi időt kell tölteni a felkészítéssel és gyakorlatozással, azonban a tapasztalatok azt mutatják, hogy a teljes munkaidős speciális rendvédelmi alakulatok tagjai számára nem csak az elvárások átlagon felüliek, hanem a gyakorlással és kiképzéssel eltöltött idő is.(IACP, 2011)

V.3 Nemzetbiztonsági különleges képességek

Azokban az országokban, ahol a hírszerző és elhárító szervezetek elkülönülnek a rendőri és bűnüldöző szervektől, előbbiek jellemzően nem rendelkeznek végrehajtói, illetve intézkedési jogkörrel, csupán információkat gyűjtenek, amiket elemzések és jelentések formájában juttatnak el a kormányhoz. Az olyan országokban, mint például az Egyesült Államok a hírszerző közösségből több szervezet is jogosult nyomozó tevékenységet folytatni, aminek az eredményét egy ügyésznek vagy az Igazságügyi Minisztérium megfelelő tisztviselőjének bemutatják, aki eldönti, hogy indokolt-e vádemelés vagy más intézkedés. (Vitkauskas, 1999) Függetlenül attól, hogy egy országban melyik modellt alkalmazzák, a hírszerzési és elhárítási tevékenységet folytató szervezet alapvető feladataiból fakadóan speciális tevékenységet végez a hagyományos haderőkhöz és rendvédelmi szervekhez képest. Ugyanakkor az országonként eltérő mandátumok és a feladatkörök heterogén eloszlása miatt nehéz átfogó képet alkotni a nemzetbiztonsági szektor különleges képességeiről. Ezért a honvédelemhez és rendvédelemhez képest, ahol az általánostól való szektoron belüli eltérés biztosította a kontextust, a nemzetbiztonság esetében a másik két szektor általános elemeivel történő összevetés adja az elemzési perspektívát.

V.3.1 A nemzetbiztonsági szervezetek (különleges) képességei

A hírszerzéssel és elhárítással foglalkozó nemzetbiztonsági szervezetek rendeltetésüknél fogva az állam biztonsága szempontjából releváns információk gyűjtésére, elemzésére és értékelésére létrehozott speciális állami ügynökségek. Az államok rendszerint egy vagy több kijelölt ügynökséget tartanak fenn, amelyek földrajz, tematika, vagy technika alapján specializálódnak. A működési terület lehet erősen fókuszált, mint például a belföldi, külföldi, illetve katonai hírszerzés

vagy a bűnfelderítés, terrorelhárítás, valamint pénzügyi/gazdasági hírszerzés esetén, de az sem ritka, hogy egyetlen szervezet átfogó felelősséggel rendelkezik több területen. Ezeknek a speciális állami ügynökségeknek az elsődleges feladata, hogy hitelt érdemlő információkkal lássák el a kormányokat az államra és lakosságára leselkedő fenyegetésekkel kapcsolatban. Jellemzően a nemzetbiztonsági szervezetek hívják fel a döntéshozók figyelmét a feltörekvő problémákra, a nemzeti érdekeket érintő fenyegetésekre, kockázatokra és lehetőségekre. A munkájuk segíti a politikai döntéshozókat a nemzeti érdekek meghatározásában, koherens nemzeti biztonsági és katonai stratégiák, illetve megfelelő biztonságpolitika kialakításában, a nemzeti válsághelyzetekre való felkészülésben és reagálásban. Az elhárítás képességeinek középpontjában a megelőzés áll olyan cselekményekkel szemben, mint például az idegen országok hírszerző szolgálatai és politikai csoportjai által elkövetett kémkedés, felforgató tevékenységek vagy szabotázs akciók. A kémelhárítás defenzív oldalán lekérdezések, átvilágítások és megfigyelések találhatók, míg az offenzív oldal magába foglalja a más szervezetekbe történő behatolást és beépülést, továbbá megtévesztést, megzavarást és manipulálást célzó műveleteket. (Harder, 2017)

A fedett, illetve titkos akciók lényegében olyan speciális politikai akciók és aktív intézkedések, amelyek idegen országok politikai, katonai vagy gazdasági befolyásolásának céljával megvalósuló nemzetbiztonsági műveletek. A fedett akció lehet külföldön folytatott propaganda és politikai tevékenység, külföldi kormányoknak nyújtott segítség vagy akár idegen ország területén folytatott tiltott tevékenység megzavarása. A fedett tevékenység olyan alternatívát kínál az államok számára a diplomáciai és más politikai intézkedések kudarca esetén, amire a közvetlen katonai fellépés nem alkalmas. (Harder, 2017)

V.3.2 A speciális nemzetbiztonsági képességek feladatrendszere

A kormányok a nemzetbiztonsági szervezeteknek mandátumuknak megfelelő speciális jogi felhatalmazást és képességeket biztosítanak. Ezek a felhatalmazások és képességek egy adott államban általában a nemzeti kontextustól és az adott szervezet funkcióitól függenek, de jellemzően kiterjednek az emberi jogok, a magánszféra és különböző polgári jogok korlátozására bizonyos esetekben. A hírszerző tevékenység az információk gyűjtése közben felderítéssel, illetve a kommunikáció megfigyelésével sértheti a magánélethez való jogot, míg azokban az országokban, ahol intézkedési jogkörrel rendelkezik egy nemzetbiztonsági szervezet, a szabad mozgást is

korlátozhatják letartóztatással és őrizetbe vétellel. A nemzetbiztonsági fenyegetések elleni fedett műveletek bizonyos esetben törvénysértéssel járhatnak. (Harder, 2017)

A nemzetbiztonsági szervezetek hírszerző tevékenységére fókuszálva – a teljesség igénye nélkül is – több különböző hírszerzési kategóriát lehet azonosítani, amelyek a források, illetve az információ megszerzésének módja szerint elkülönülnek. Két fő kategóriának tekinthető a nyilvánosan és nem nyilvánosan hozzáférhető információk és forrásaik. Mivel a média is előszeretettel alkalmazza, ezért az egyik legelterjedtebb kategóriának számít a nyílt forrású hírszerzés (Open Source Intelligence – OSINT), ami a nyíltan elérhető információk hírszerzési célú gyűjtését és felhasználását jelenti. Főként a hidegháború idején alkalmazott, továbbra is létező, klasszikus kategóriának számít az emberi erőforrásokat felhasználó és kiaknázó hírszerzési módszer, amely emberek által emberektől gyűjtött információkra utal ügynökök, belsősök és más informátorok közreműködésével (Human Intelligence – HUMINT). Korábban már szóba került a jelfelderítés vagy más néven rádióelektronikai felderítés (Signal Intelligence – SIGINT), ami további két alkategóriára bontható. A távközlési-, illetve rádiófelderítés (Communications Intelligence – COMINT) alapvetően az ember és ember közötti kommunikációra fókuszál és telefonbeszélgetések lehallgatását, valamint elektronikus levelek, illetve rádióforgalmazás elfogását és rögzítését takarja. A rádiótechnikai felderítés (Electronic Intelligence – ELINT) ezzel szemben a gép és gép közötti kommunikációt célozza többnyire az elektromágneses alapon működő adatátvitelre fókuszálva, amire jó példa a rádiólokációs eszközök által sugárzott jelek elfogása vagy manipulálása.(C4ADS, 2019) Az OSINT tevékenységhez hasonlóan szintén egyre ismertebb és elterjedtebb a technológiai transzfernek köszönhetően a képfelvételeken alapuló hírszerzés (Imagery Intelligence – IMINT), ami a műholdak és egyéb repülő eszközök által, különböző technikákkal készített felvételekből nyerhető információk gyűjtését és feldolgozását jelenti. Az IMINT hőskorának egyik triviális példája az Egyesült Államok által készített SR-71, illetve U-2 kémrepülőgépek, közismert nevükön a „Blackbird” és a „Dragon Lady”. Szintén technikai kategóriának minősül az érzékelésen és szignatúrákon alapuló (Measurement and Signature Intelligence – MASINT) hírszerzés, aminek lényege, hogy nukleáris, optikai, rádiófrekvenciás, akusztikus, szeizmikus vagy más szenzorokból nyernek ki technikai és tudományos adatokat, amiből következtetni lehet az ellenérdekelt fél tevékenységére, vagy az általa üzemeltetett objektumokra és működtetett eszközökre. Az említetteken kívül számos további hagyományos hírszerzési kategória létezik és vannak újabbak is, mint például a közösségi média

felületeken alapuló (Social Media Intelligence – SOMINT) hírszerzés, azonban a kutatás fókusza miatt ezek bemutatásától eltekintünk. (Harder, 2017)

A hírszerző és elhárító tevékenység specializáltsága, illetve különleges mivolta leginkább egyéni szinten, a műveleti területen dolgozók tekintetében érhető tetten, ahol gyakorlatban kell alkalmazni a konspirált kapcsolattartás és a titkos információszerzés technikáit és módszereit. Továbbá – a teljesség igénye nélkül – olyan fedett műveleti tevékenységekben való részvételt is magába foglal, mint a tömegpusztító fegyverek és alkotóelemeik vagy a kettős felhasználású technológiák jogellenes forgalmának felderítése, különböző objektumok és személyek védelme, rejtjelező eljárások, algoritmusok és a rejtjelezésre használt eszközök kriptográfiai bevizsgálása és minősítése, a szervezett bűnözéssel és terrorszervezetekkel kapcsolatos hírszerzés, különféle nemzetbiztonsági célú beszerzésekkel összefüggő minősítések elvégzése, a jogrend megváltoztatására vagy megzavarására irányuló jogellenes törekvések leleplezése és elhárítása, speciális távközlési összeköttetés és a fedett működéshez szükséges speciális technikai eszközök biztosítása. (Nb. tv., 1995)

V.3.3 Képzés, kiképzés és követelmények a nemzetbiztonsági szolgálatoknál

A titkosszolgálatok toborzási és kiképzési követelményeinek egyik meghatározó specifikuma, hogy a kapcsolódó információk jelentős hányada minősített, ezért a kutatás kerete és nyílt jellege korlátozza a bemutatást. Általános megközelítést alkalmazva elmondható, hogy az operatív munkakörökben, illetve műveleti területen tevékenykedő szakemberek és a háttérben elemző-értékelő munkát végzők is emelt szintű elvárásoknak kell megfeleljenek. Mivel egy nemzetbiztonsági szervezet működése meglehetősen sok területre kiterjedhet, ezért jellemzően a toborzáshoz egy általános, de a biztonsági- és védelmi szektor hagyományos szolgálati ágaihoz képest szigorúbb követelményrendszernek kell megfelelni és sikeres teljesítés esetén az egyéni fizikai, pszichológiai és egyéb paraméterek függvényében dől el, hogy ki milyen területre alkalmas. Ezzel kapcsolatban a magyar Információs Hivatal honlapja például csak annyit közöl, hogy mivel a szaktudás klasszikus iskolai keretek között nem megszerezhető, ezért saját oktatási kapacitás segítségével 10 hónapos alapkiképzés keretében az elméleti alapok mellett intenzív és célirányos gyakorlati felkészítés valósul meg. Sok esetben a nemzetbiztonsági szolgálatok paramilitáris tevékenységeihez olyan a rendvédelmi és honvédelmi szektorból ismert kommandós képességekre van szükség, amelyek segítségével például ellenálló csoportok kiképzése és vezetése valósítható

meg, vagy védett objektumokba történő behatolást lehet megoldani. Ugyanakkor klasszikus képességnek számít a kapcsolattartók és informátorok beszervezése, kezelése, illetve a velük folytatott titkos kommunikáció is. (Burkett, 2013) Azt, hogy egy nemzetbiztonsági szolgálat mennyire szerteágazó tevékenységi körrel és ezáltal kiképzési kapacitással rendelkezik, leginkább annak az adott országnak az elvárásai és lehetőségei határozzák meg, amelyik létrehozta. Ezért is nehéz összehasonlítani például az Egyesült Államokban működő legnagyobb ügynökségeket és az ezeket kiszolgáló sokrétű képzési struktúrát (Jurkanin, 2013), egy kelet-közép-európai kisállam hírszerző, illetve elhárító szolgálatának képességeivel, valamint képzési, kiképzési rendszerével.

Ennek ellenére a nemzetbiztonsági terület követelményeivel kapcsolatban, a hazai felsőfokú nemzetbiztonsági képzés segítségével általános kép alkotható az érintett szakértelemmel és elvárásokkal összefüggésben. A polgári nemzetbiztonsági szakértő átfogó és magas szintű ismeretekkel rendelkezik a nemzetbiztonsági tevékenység jogszabályi normáiról, összefüggéseiről, az érintett szervezetek sajátosságairól, tisztában van a nyílt és nem nyílt források, adatbázisok jelentőségével, megfelelő pszichológiai és kommunikációs, továbbá a preventív gondolkodást megalapozó ismeretekkel rendelkezik. Képességeit tekintve együtt tud működni a nemzetbiztonsági és terrorelhárító műveletek végrehajtásában társ- és partnerszolgálatokkal, gyorsan és körültekintően tudja az előre nem modellezhető helyzeteket is értékelni, a kapcsolódó döntéseket előkészíteni és szükség esetén döntést is hozni, a tipikus és sajátos nemzetbiztonsági eszközök és módszerek alkalmazását meg tudja tervezni, szervezni, képes a feladatok végrehajtására és irányítására, továbbá képes a rendelkezésre álló humánforrásokat, titkosszolgálati eszközöket- módszereket, terrorelhárító eljárásokat szakszerűen alkalmazni. Attitűd tekintetében a nyitott, fogékony, önfejlesztő természet mellett fontos a bajtársiasság és lojalitás, továbbá a szervezeti hierarchiának megfelelő engedelmesség és parancsadási készség. Annak függvényében, hogy a nemzetbiztonsági szektorban milyen területen helyezkedik el valaki, szükség lehet többek között speciális krimináltechnikai eszközök alkalmazásában való jártasságra, az elektronikus információs rendszerek sajátosságainak és a kiberbiztonság főbb kihívásainak ismeretére, vagy a terrorelhárító műveletek tervezésében, előkészítésében, végrehajtásában történő közreműködésre, valamint az erők és eszközök alkalmazásában, illetve a műveletek irányításában való részvételre. (NKE, é. n.)

Összegzés, következtetések

Az V. fejezet három alfejezetben azt vizsgálta, hogy a biztonsági és védelmi szektor egymástól elkülönülő honvédelmi, rendvédelmi és nemzetbiztonsági területei milyen különleges és speciális képességekkel rendelkeznek, illetve milyen feladatok ellátására alkalmazhatók ezek a képességek. Ezen felül a fejezetben arra kerestem a választ, hogy milyen körülmények mellett működtethetők a speciális képességek hatékonyan, továbbá milyen követelményrendszer párosul hozzájuk a képzéssel és kiképzéssel összefüggésben. A V.1 alfejezetben a katonai különleges műveleti képességek feladatrendszere, körülményei és követelményei vizsgálatának célja az volt, hogy a katonai dimenzió sajátosságait feltárjam és azonosítsam a fejlett tartósan fennálló fenyegetésekkel összevethető működési feltételeket. A V.2 alfejezetben a rendvédelmi speciális egységek feladatainak, működési körülményeinek és személyi követelményeinek vizsgálata az előző alfejezettel azonos célokat szolgált azzal a különbséggel, hogy a rendvédelmi specifikumok voltak a meghatározók. A V.3 alfejezetben a nemzetbiztonsági különleges képességeket a védelmi szektor többi ágával összevetve vizsgáltam, ami lehetővé tette a nemzetbiztonsági szektorban is azoknak a paramétereknek az azonosítását, amik a fejlett perzisztens fenyegetésekkel történő összehasonlítás alapjául szolgálnak.

A vizsgálat nyomán megállapítottam, hogy az egyes területek különleges és speciális képességei ágazatok szerint, a tevékenységi területnek megfelelően jól elkülöníthetők, ugyanakkor vannak átfedések, amik esetenként szoros kapcsolatra, illetve tudástranszferre utalnak. A haderőkben létrehozott és a vizsgálat részét képező különleges műveleti képességeket alapvetően idegen államok területén, konfliktussal sújtott övezetekben, vitatott hovatartozású térségekben alkalmazzák. Belföldön csak rendkívüli esetekben, megfelelő felhatalmazás és jogi szabályozás alapján kerülnek bevetésre. Jellemzően terrorelhárítási, hírszerzési, kimenekítési és kiképzési feladatokat látnak el meglehetősen mostoha körülmények között. Ezért a haderők különleges műveleti beavatkozóit arra képzik ki, hogy akár több napig képesek legyenek utánpótlás, ellátás és bármilyen külső segítség nélkül, kis csoportban tevékenykedve végrehajtani feladataikat. A végrehajtás sikerének növelése, illetve lelepleződés esetén a letagadhatóság miatt a küldetések és akciók szinte kizárólag fedett körülmények között zajlanak, továbbá kiemelkedő hadműveleti, stratégiai és politikai jelentőséggel bírnak.

A rendvédelmi szervek esetében a létrehozott és vizsgált különleges képességeket szinte kizárólag belföldön, illetve olyan területeken alkalmazzák, ahol az állam joghatósággal rendelkezik. Legfőképp terrorelhárítási, illetve bűnfelderítési- és felszámolási feladatok során kerülnek bevetésre, így merényletek, túszmentések, különösen veszélyes bűnözők elfogása közben azonosíthatók a rendvédelmi különleges képességek. A rendvédelem különleges alakulatainak tagjait arra készítik fel, hogy kis csoportban tevékenykedve képesek legyenek terroristák és felfegyverzett bűnözők bármilyen körülmények között történő ártalmatlanítására és elfogására, az áldozatok testi épségének megőrzésére és a túszok kimenekítésére, kijelölt objektumok és személyek védelmére, illetve rendőri megfigyelésre. Az alakulatok tagjai gyakran inkognitóban végzik tevékenységüket és sok esetben az alkalmazott eszközök és módszerek is minősítettek annak érdekében, hogy az ellenérdekelt felek számára ne legyenek kiszámíthatóak a tevékenység egyes elemei. A különleges rendvédelmi tevékenység fedett jellege ellenére azonosíthatók olyan összetevők, így például a mesterlövész, a tűzszerész vagy a taktikai kutya alkalmazása, amelyek egyfelől megtalálhatók a katonai különleges műveleti képességek eszköztárában is, másfelől a műveleti területen alkalmazott módszerek és eljárások közötti átfedések miatt nem ritkák a közös gyakorlatok.

A nemzetbiztonsági szolgálatok tevékenysége önmagában speciálisnak tekinthető az alapvető honvédelmi és rendvédelmi tevékenységek körülményeihez képest, mivel az orientáció lehet külföldi és belföldi egyaránt, illetve egyéb módon specializált, továbbá itt a leginkább kiterjedt a tevékenység fedett jellege. A nemzetbiztonsági szolgálatok tagjainak a másik két ágazathoz hasonlóan különleges elvárásoknak kell megfelelniük és elvárt az átlagon felüli teljesítmény. Idegen környezetben általában a helyi elhárítással szemben kell hatékony hírszerző vagy befolyásoló tevékenységet folytatni, míg belföldön más országok azonos tevékenységének leleplezése és akadályozása a cél. Továbbá mindkét területen megjelenik a terrorizmus elleni harc, illetve a szervezett bűnözéssel szembeni fellépés. Feladataik ellátásához a nemzetbiztonsági szolgálatok tagjai az átlagon felüli ismereteik és képességeik mellett máshol nem elsajátítható ismeretekre és képességekre is szert tesznek, jellemzően a szolgálatok saját oktatási bázisán. Ezek egyebek mellett tartalmaznak humán és technikai hírszerzési fortélyokat, terrorelhárítási módszereket, illetve titkosszolgálati eszközök és eljárások alkalmazásában való jártasságot. A nemzetbiztonsági szolgálatok sikeres működésének egyik alapvető mértéke, hogy tevékenységüket mennyire képesek leplezni, így sok esetben egy nagy horderejű bűncselekmény vagy egy

terrorhálózat leleplezése esetén is rejtve marad a nemzetbiztonsági szál és a közreműködő szolgálatok szerepe, ami a politikailag jelentős nemzetbiztonsági ügyek esetén is elmondható, mivel a letagadhatóság ebben az esetben is fontos szempont.

A vizsgált honvédelmi, rendvédelmi és nemzetbiztonsági különleges képességekkel összefüggésben a tevékenységekre leginkább jellemző paraméterek összefüggéseit és a párhuzamokat táblázatban mutatom be. A tevékenység fedett jellege, jelentősége (politikai, stratégiai, nagy horderejű), a végrehajtás helye (belföld, külföld) és a végrehajtókkal (beavatkozók, operátorok, felszámolók, ügynökök, közreműködők) szembeni elvárások (fizikai, pszichikai, biztonsági, képzettség), valamint a tevékenység intervalluma (rövid idejű, folyamatos) képezi azokat a kategóriákat, illetve paramétereket, amiknek a segítségével kimutattam az APT tevékenységek és a különleges műveleti képességek közötti analógiákat.

KÜLÖNLEGES MŰVELETI KÉPESSÉGEK	FEDETT JELLEG		JELENTŐSÉG			MŰVELETI TERÜLET		MŰVELETI CIKLUS		CÉLZOTTSÁG	ADAPTIVITÁS	SPECIÁLIS ERŐFORRÁSOK	SPECIÁLIS ELVÁRÁSOK
	FELVÁLLALT	LETAGADHATÓ	NAGY HORDERŐJŰ	STRATÉGIAI	POLITIKAI	BELFÖLD	KÜLFÖLD	RÖVID	FOLYAMATOS				
KATONAI	●	●	◑	●	●	○	●	●	◑	●	●	●	●
RENDVÉDELMI	●	○	●	○	◑	●	○	●	◑	●	●	●	●
NEMZETBIZTONSÁGI	◑	●	●	●	●	●	●	◑	●	●	●	●	●
FEJLETT PERZISZTENS FENYEGETÉSEK	FEDETT JELLEG		JELENTŐSÉG			MŰVELETI TERÜLET		MŰVELETI CIKLUS		CÉLZOTTSÁG	ADAPTIVITÁS	SPECIÁLIS ERŐFORRÁSOK	SPECIÁLIS ELVÁRÁSOK
	FELVÁLLALT	LETAGADHATÓ	NAGY HORDERŐJŰ	STRATÉGIAI	POLITIKAI	BELFÖLD	KÜLFÖLD	RÖVID	FOLYAMATOS				
ÁLLAMI HÁTTERŰ APT-K	○	●	●	●	●	○	●	◑	●	●	●	●	●

5. ábra: A katonai (honvédelmi), rendvédelmi és nemzetbiztonsági különleges műveleti képességek és a fejlett perzisztens fenyegetések jellemzőinek dominancia alapú vizsgálata. Az egyes paraméterek dominanciáját hármas skálán üres (világos), félig teli (világos/sötét) és teli (sötét) körök jelölik. A teli kör jelentése: a paraméter erősen domináns az adott képesség, illetve az APT-k tevékenysége kapcsán. A félig teli kör jelentése: a paraméter kevésbé domináns. Az üres kör jelentése: a paraméter nem domináns, vagy egyáltalán nem jellemző az adott képesség, illetve az APT-k tevékenysége kapcsán. (A szerző saját szerkesztése.)

VI. A kiber különleges műveleti erők

Bevezetés

Az értekezés előző fejezeteiben áttekintettem a kiberműveletek teljes – offenzív műveleteket is magába foglaló – spektrumát és olyan honvédelmi, rendvédelmi, valamint nemzetbiztonsági különleges képességeket tanulmányoztam, amelyek rendeltetése, továbbá létrehozásuk és működtetésük körülményei és feltételei eltérnek a hagyományostól. A kiberbiztonsági kihívások közül szintén egy olyan, a hagyományostól eltérő fenyegetéssel foglalkoztam mélyrehatóan, ami számos ponton párhuzamot mutat a kinetikus különleges képességekkel. Az azonosságok mentén kialakuló analógia nyomán azok a kibertérben tevékenykedő alakulatok, amelyek jellemzően destruktív és/vagy hírszerző tevékenységet folytatnak stratégiai jelentőségű aktív kibervédelmi, illetve offenzív kiberműveletek során, felfoghatók kiber különleges műveleti egységként, illetve erőként. Ezek az erők a kibertérben, vagy a kibertéren keresztül, a kinetikus megfelelőikhez hasonló rendeltetéssel és specifikumokkal képesek hatást kiváltani. A kiber különleges műveleti erők és képességek kapcsán a NATO különleges műveleti, illetve kiberműveleti doktrínái alapján az alábbi munkadefiníciókat használom:

A kiber különleges műveletek olyan tevékenységek, amelyeket egyedileg dolgoznak ki, szerveznek meg és hajtanak végre fedett, illetve rejtett módon a kibertérben vagy azon keresztül annak érdekében, hogy stratégiai jelentőségű célt valósítsanak meg a nemzeti érdekérvényesítés és politikai célkitűzések érdekében.

A kiber különleges műveleti erők speciálisan kiválasztott, szervezett, kiképzett és felszerelt egység, amely képes a hagyományos erőknél és a passzív kibervédelemben nem használt módszerek és eljárások alkalmazásával fokozott politikai és stratégiai kockázatot jelentő kibervédelmi, kiberhírszerzési és destruktív kiberműveletek végrehajtására önállóan vagy más egységekkel együttműködve.

A kiberkonfliktusok során a kiber különleges műveleti erők kifejezéssel leírható szereplők által végzett tevékenység aspektusai jól körülhatárolhatók, így alkalmasak arra, hogy kisállami perspektívából a nemzeti érdekérvényesítés és képességfejlesztés szintjén vizsgáljuk őket.

VI.1 Miért van szükség kiber különleges műveleti erőkre?

Napjainkban a kiberbiztonsági trendek meghatározására használt indikátorok meglehetősen heterogén képet mutatnak. Nincsenek univerzális, minden szereplő által alkalmazott iparági szabványok arra vonatkozóan, hogy mit tekintenek incidensnek, támadásnak vagy egyéb eseménynek, mit és mennyi ideig számítanak bele a károkba és költségekbe, de sokszor még arra is nehéz választ adni, hogy egy-egy esemény hány felhasználót érintett, mivel sok esetben csupán az adatbázis bejegyzések számát használják a kiterjedés meghatározására. Ebből a szempontból 2021 egyik legnagyobb számot produkáló eseménye a Cognyte kiberbiztonsági vállalat 5 milliárd bejegyzést tartalmazó adatbázisának incidense volt (Bischoff, 2021), aminek keretén belül felhasználói hitelesítés nélkül bárki számára hozzáférhető volt az a gyűjtemény, ami korábbi incidensek során kiszivárgott felhasználói adatokat tartalmazott.

A kiberbűnözés szintén olyan fogalom, ami számos területre bontható, ezért nehéz pontos képet alkotni olyan esetben, amikor egy kiberbiztonsági beszállító a kiberbűnözés 600%-os növekedését állapítja meg a SARS-CoV-2 pandémia következtében (Firch, 2020). A kiberbűnözés egyik formája, illetve a kibertámadások egyik fajtája a DDoS, aminek a száma 2020-ban elérte a percentként 18-at, vagyis napi 26 ezret[117] (NetScout, 2021). Beszédesek azok a kimutatások is, amelyek szerint az államilag támogatott kibertámadások 80%-a kormányzati szervezeteket, agytrösztöket és más nem kormányzati szervezeteket céloztak (Microsoft, 2021), miközben csak 2021 első negyedévében 42%-os növekedést tapasztaltak az ellátási láncokat érő támadások számában (Blue Voyant, 2021). Más megközelítés, de szintén beszédes előrejelzés, hogy 2025-re a becslések szerint az IoT (Internet of Things)[118] eszközök önmagukban több mint 73 zettabájt[119] adatot generálnak majd (Hojlo, 2021).

[117] A DDoS támadások kapcsán fontos megjegyezni, hogy a kiberbiztonsági szakemberek számára a darabszám önmagában kevésbé értelmezhető, az inkább a témában kevésbé jártas olvasó számára szemléletes. Az iparági szakemberek elsősorban a támadások volumenét, illetve időtartamát tekintik mérvadónak. Ilyen téren 2021-ben november 6-án Csehországot érte az egyik legnagyobb támadás, amely 612Gbps sávszélességű volt és kevesebb mint 17 percig tartott. Ugyanakkor figyeltek már meg terrabit volumenű támadást is.

[118] Internet of Things – IoT egy angolszász kifejezés, amely azokra az eszközökre, illetve az általuk alkotott hálózatra vonatkozik, amelyek képesek más eszközökkel kétirányú kommunikációt folytatni annak érdekében, hogy a működés közben keletkezett adatokat és információkat eljuttassák és megosszák más berendezésekkel, adatbázisokkal vagy szolgáltatásokkal, illetve fogadni tudjanak a működésükkel összefüggésben adatokat és információkat. Magyarul a nem túl szerencsés „dolgok internete" kifejezést szokás használni.

[119] A zettabájt egy mennyiségi egység, amivel a digitális tárhely méretét szokás megadni. A rendszer alapegységei a bit, illetve a bájt. Nyolc bit tesz ki 1 bájtot, ahonnan 1024 a váltószám felfelé a skálán. A kilobájt, megabájt, gigabájt és terabájt a hétköznapi felhasználó számára leginkább ismert egységek. A jelenleg kevésbé elterjedt exabájt, zettabájt,

Ez az elképesztő méretű adatvagyon és a többi kiberbiztonsági trend önmagában is elegendő indok kellene legyen ahhoz, hogy hatékony védelmi alternatívákról gondoskodjunk. Ezt tovább erősíti azoknak az állami és nem állami kiberképességeknek a proliferációja, amelyek alkalmasak arra, hogy megzavarják egy állam belső rendjét vagy épp megsértsék szuverenitását egy olyan dimenzióban, ahol egyelőre nem léteznek kikényszeríthető nemzetközi normák és jogi szabályok. Mivel a tapasztalatok és az előrejelzések is azt mutatják, hogy egy széleskörben elfogadott, kibervédelmi szempontból biztonságot nyújtó jogi keretrendszer kialakítása több évet, évtizedet is igénybe vehet, mindenképpen érdemes a kibervédelmi képességek összes alternatíváját számításba venni. Ezek közül az egyik legfejlettebb és legkifinomultabb a kiber különleges műveleti képesség.

A kiber különleges műveleti képesség koncepciójának kialakításához az elvégzett szakirodalmi kutatás mellett irányított interjúkat is felhasználtam, amelyeket elsősorban olyan hazai szakemberekkel készítettem, akik jelenlegi vagy korábbi beosztásukból fakadóan megalapozottan tudnak állást foglalni a koncepció részleteivel kapcsolatban. Az interjúkon elhangzott kérdések megtalálhatók az értekezés Függelékében.

VI.1.1 Kitekintés a különleges műveletek középtávú kihívásaira

A hazai és nemzetközi tudományos, illetve szakmai elemzések is azt mutatják, hogy a hagyományos, kinetikus különleges műveleti képességek a változás időszakát élik, ami elsősorban a fenyegetések hangsúlyeltolódásából következik, de a technikai fejlődés és a nemzetközi kapcsolatok átrendeződése is kifejti hatását.

Az V.1.1 alfejezet végén szóba került a különleges műveleti képességek feladatrendszerének átalakulása. A feladatrendszer kapcsán a hivatkozott interjúból kiderül, hogy azt elsősorban az elmúlt két évtized afganisztáni szerepvállalása határozta meg, ami a magyar különleges műveleti katonák esetében is 11 évet jelent. A lázadóellenes műveletek, a katonai segítségnyújtás szerepköre, illetve ennek keretén belül különböző feladatok afganisztáni körülmények között történő végrehajtása az, ami sok különleges műveleti erő számára a feladatrendszer megszokott alapját képezi. Bár ezek elég széles spektrumot fednek le az egyszerű biztonsági járőrtől egészen a nagy kockázatú elfogásig, az afganisztáni fókusz és ezzel együtt az, hogy a megfelelő felderítési-

yottabájt és brontobyte a hétköznapi felhasználó számára szinte felfoghatatlan mennyiségű adatot jelent. Csak az érzékeltetés miatt: 1 zettabájt az 1024 exabájt – becslések szerint a Google által birtokolt összes adat 15 exabájt.

hírszerzési-megfigyelési képességek vagy éppen a közeli légitámogatás szinte minden feladat esetén rendelkezésre áll, természetessé vált a különleges műveleti katonák számára. Ugyanakkor koránt sem biztos, hogy ez másutt, más ellenfelekkel szemben is így lesz, miközben a feladatszabás is átalakuló félben van. A megváltozott stratégiai környezetben szükséges a hasznos és jó afganisztáni tapasztalatok megtartása, miközben a már nem használhatók helyett az új körülményekre kell fókuszálni. (Trautmann, 2021b)

Miközben a különleges műveleti egységek fő képessége továbbra is az irreguláris és nem hagyományos hadviselés az ellenség mélységében történő műveletek végrehajtása során, jelentősen felgyorsult az információáramlás, a tervezés és a döntéshozatal is. A stratégiai környezetre szignifikáns hatást gyakorol a technológiai robbanás, amelynek „*köszönhetően ma már gyakorlatilag bárkinek elérhető a „polcról levehető", a közel legmagasabb szintű technika is*" (Trautmann, 2021a). A feladatrendszer átalakulása nyomán egyrészt megmarad a nem hagyományos hadviselési irány akár nagyon nagy mélységekben, másrészt a precíziós műveletek végrehajtásával kapcsolatos elvárások dominanciája is tetten érhető. Mindez újragondolást igényel a struktúrák, illetve a feladatokba bevont erők és eszközök tekintetében egyaránt. (Trautmann, 2021a)

Egy a különleges műveleti képességek globális versengésben betöltött szerepével foglalkozó tanulmány szerint a konfliktusok teljes spektrumában, a különleges erők feladatai a de-eszkalációs (de-escalating), semlegesítő (neutralizing) és eszkalációs (escalating) szerepvállalások mentén definiálhatók, amelyek végrehajtása már ma is a jövő nyílt konfliktusainak elkerülését szolgálják. Ezek szerint míg az elmúlt évtizedek során a SOF képességek fókuszában a hagyományos hadszíntéri, illetve korlátozott, valamint hibrid konfliktusok során az irreguláris, nem hagyományos hadviselés folytatása állt, jelentős hangsúlyeltolódás azonosítható a fegyveres konfliktusok szintjét el nem érő, a hatalmi versengésre jellemző kétértelmű, szürke zónás, irreguláris körülmények felé. (Broyles és Blankenship, 2017)

Az egyik leginkább kiterjedt különleges műveleti képességekkel rendelkező Egyesült Államok esetében egy közel 10 évvel ezelőtti elemzés arra jutott, hogy a fő irányt a partnerek megfelelő képességeinek kialakításában való közreműködés jelenti majd, amivel a partnerek képessé válnak a saját határaikon belül a hatékony fellépésre, így csökkenhet az amerikai különleges műveleti beavatkozók létszáma, az amerikai jelenlét a világ konfliktusaiban és így a kapcsolódó költség is.

Az alkalmazási modell kevesebb direkt, illetve unilaterális akcióval számol, miközben a feladatok a különleges műveleti képességek teljes spektrumában jártas és megfelelően felkészített vezetők által irányított egyesített szervezetek által kerülnek végrehajtásra. (Robinson, 2013)

Egy a főként orosz fókuszú stratégiai versengésben betöltött amerikai különleges műveleti szerepvállalással foglalkozó tanulmány arra jutott, hogy hosszú évek után a lázadó- és terrorizmus ellenes erőfeszítéseket az egyenrangú és közel egyenrangú (peer and near-peer) versenytársak jelentette fenyegetések váltották az élen. A hatékony szerepvállaláshoz szükséges koncepciók, doktrínák és eszközök azonban nem fejlődtek a kellő mértékben. Ez érinti a stratégiai versengés során az ellenfelek által küldött társadalmi üzenetek hatásainak enyhítését, a lakosság kulcsfontosságú rétegének megnyerését, a döntéshozók támogatását, a partnerek ellenállóképességének javítását, az ellenfelek elrettentését, valamint hálózatainak megzavarását és leleplezését. Bár a különleges műveleti erők számos képességgel rendelkeznek ezeken a területeken, sok esetben csak korlátozott tevékenység folytatására alkalmasak és azt is jelentős kockázattal. (Watts és mtsai., 2021)

Az alfejezet elején is idézett álláspont – miszerint a különleges műveleti erők feladatrendszere átalakulóban van – egybevág azzal a következtetéssel, amire a Közpolitikai Kutatások Amerikai Intézete (American Enterprise Institute for Public Policy Research) által kiadott, a különleges műveleti erők 21. századi nagyhatalmi versengésben betöltött szerepét vizsgáló tanulmány is jutott. Ma ezek az erők rotáció alapú terrorizmus elleni harcra vannak optimalizálva, miközben a támogató képességek garmadáját horizontálisan integrálják, továbbá az állományt az örök háború szempontjai alapján választják-, képzik ki és értékelik. A jövő különleges műveleti erőinek egyedi kiválasztási és kiképzési utakat kell kidolgoznia, meg kell szüntetnie a felesleges kapacitásokat és a küldetések átfedéseit, valamint meg kell erősítenie és erőforrásokat kell biztosítania a legváltozatosabb küldetésekhez. (Brands és Nichols, 2020) Ellenkező esetben egy kevésbé képzett vagy felkészített állomány olyan harcászati hibát követhet el, „*aminek stratégiai szintű bukás*” lehet a vége (Trautmann, 2021a).

VI.1.2 Stratégiai szempontok

A fent idézett gondolat megalapozottságát az adja, hogy a különleges műveleti erők tevékenysége szignifikáns hatást képes gyakorolni stratégiai szinten, amit a korábbi fejezetek több aspektusból

is érintettek. Ezúttal a különleges műveleti, illetve kiber képességek létjogosultságát a Liddel Hart féle nagystratégiai megközelítéssel a kisállami érdekérvényesítés perspektívájából támasztom alá.

Az államok közötti kiberkonfliktusokat jelentős mértékben geopolitikai és politikai megfontolások táplálják és ezért nem választhatók el más konfliktusoktól vagy politikai célkitűzésektől. Miközben a kiber stratégiák egyáltalán nem újak vagy forradalmiak, a gyakorlat azt mutatja, hogy a kibertérben végzett tevékenységek a korlátozott kényszerintézkedések tartományába esnek, amelyek célja az információk egyensúlyának megváltoztatása, valamint a hosszú távú versengéssel összefüggő interakciók során az eszkalációs kockázatok kezelése. A kis államok különösen érzékenyek a kiberkonfliktusok hatásaira, miközben a nagyobb államok politikai befolyásolási törekvéseik során előnyben részesítik a kibereszközök alkalmazását. Ennek legfőbb oka, hogy bár egyre több stratégiában szerepel a kibertámadás fegyveres támadásként történő értékelésének és a kibertéren kívüli válaszadásnak a lehetősége, a gyakorlatban eddig egyetlen kibertámadás sem lépte át a fegyveres támadási küszöböt, így a nemzeti és nemzetközi válaszadás nem csak nehéz, de példátlan is. Napjainkban az államok megtalálják a kiberkonfliktusok kezelésének módját, de érdemben nem kerülnek közelebb ahhoz, hogy elfogadható mechanizmust találjanak az államok viselkedésének szabályozására a kibertérben. (Tan, 2019)

Clausewitz[120] egyik leghíresebb tézise szerint a „*háború a politikának folytatása csupán, csakhogy más eszközökkel. Látjuk tehát, hogy a háború nem csupán valamely politikai ténykedés, hanem valóban politikai eszköz, a politikai érintkezés folytatása: a politikai érintkezés végrehajtása, sajátlagos eszközökkel*" (Clausewitz, 1917). Ez a megállapítás helytálló a kiberkonfliktusok esetén is. Bár a kiberkonfliktusok egyelőre nélkülözik a háborúk erőszakos természetét, a tapasztalatok azt mutatják, hogy kiberkonfliktusok gyakran alakulnak ki politikai célok elérése mentén, illetve politikai érintkezés eszközeként. Modern megközelítésben a politikailag motivált kibertámadások csupán három, a hadviseléssel egyidős tevékenység kifinomult verziói: a szabotázs, a kémkedés és a felforgatás (Rid, 2012). Egy racionális, kompetitív, nemzetközi szituációban nem elképzelhetetlen, hogy bármelyik állam megpróbáljon bármilyen eszközt – a kibereszközöket is beleértve – alkalmazni azért, hogy ellenfeleivel szemben abszolút előnyre tegyen szert az elrettentést és kényszerítést vegyítve (Tan, 2019). A kiberkonfliktusok kényszerítő hatásai

[120] Carl Philipp Gottfried von Clausewitz (1780-1831) porosz tábornok és katonai teoretikus, munkáiban a háború morális és politikai aspektusaival foglalkozott főként, melyek közül legjelentősebb „A Háborúról" című művében a mai napig érvényes hadtudományi alapvetéseket fogalmazott meg.

korlátozottnak tekinthetők, mivel a kibereszközök és kiberképességek használata kiegészíti, nem pedig helyettesíti az államhatalom tradicionális eszközeit és képességeit, ezáltal kiegészítő külpolitikai eszközként szolgál (Valeriano, Jensen és Maness, 2018).

Miközben a kiberképességek az államhatalom, illetve az állam akaratának kényszerítő eszközeként történő alkalmazását empirikus példák támasztják alá, azt, hogy mikor alkalmazhatók és egy állam miként tudja csökkenteni a hatásokat, jelentősen befolyásolja a kontextus és a konkrét képesség. Az államok számára a kiberképességek kényszerítő alkalmazásának attraktivitását növeli a kibertámadásokhoz használt eszközök kereskedelmének és a kapcsolódó szürke-, illetve fekete piacok bővülése mellett – a technológia robbanásszerű fejlődése miatt – a támadási felület szignifikáns növekedése. Bár a kiberképességek kényszerítő alkalmazása a kontextus tekintetében több esetben is jelentős kétértelműséget mutathat, az olyan fenyegetések, mint az orosz vagy észak-koreai kiberképességek, a magasabb stratégiai célok elérésében fontos szerepet töltenek be. (Hodgson, 2018)

Amennyiben – az államokhoz hasonlóan – egy haderő fent kívánja tartani hiteles szereplőként való megítélését, a kiberképességek a katonai stratégia szintjén is létfontosságú tényezővé válnak. A kibertér a hadviselés ötödik dimenziójaként a világpolitika fontos arénájává vált – kiváltképp, mióta a béke és háború közötti határok elmosódása a köztes állapot „szürke zónáit" létrehozta. A kibertér realitásainak következtében a konfliktusok kezdete és vége bizonytalanná válik, a szereplők gyakran nincsenek is tudatában annak, hogy konfliktusban vannak valakivel. A digitális világ egy olyan tér, ahol a stratégiai előny a hadviselés többi dimenziójához hasonló jelentőséggel bír és épp úgy elveszíthető vagy megszerezhető, mint a hagyományos terekben. Mióta a kibertámadásokat az erő sokszorozására kezdték használni a hagyományos műveletek során, a hagyományos- és kiberműveletek közötti határok egyre inkább elmosódnak. Katonai szempontból a stratégiai környezet komplexitását növeli, hogy a kibertámadások képesek olyan pusztító és példátlan hatásokat kiváltani, amiket a hagyományos fegyveres támadások nem. (Limnéll, 2013)

A digitalizált világ és a kibertér alapvető jellemzői, mint például a globális elérés, az összekapcsoltság, az egyszerűen megvalósítható anonimitás vagy a hatások azonnalisága kisállami szempontból is ugyanolyan relevanciával bírnak, mint a nemzetközi rendszer bármely más szereplője számára, ezért a kiberképességek teljes spektrumának kialakítása a nagyhatalmakhoz

viszonyított relatív korlátozott erőforrások ellenére is indokolt, főként a megelőzés és elrettentés terén gyakorolt, számos előnnyel járó aszimmetrikus hatások miatt.

VI.1.3 Műveleti szempontok

Az előző alfejezet már érintette a hagyományos- és kiberműveletek közötti határok fokozatos eltűnését, ami egyenes következménye egyfelől a kinetikus és nem kinetikus környezetek közötti differenciák elmosódásának, másfelől a két környezet sok szempontból történő eggyé válásának. Azáltal, hogy digitálisan minden összekapcsolódik és a kibertér egyre kiterjedtebbé és komplexebbé válik, katonai értelemben a modern hadviselési szempontoknak hatékonyan kell érvényre jutniuk a kiber-, a kinetikus- és a kombinált műveletekben egyaránt.

Mindezt plasztikus részletekkel támasztja alá a korábban már idézett Sándor Tamás vezérőrnagy, a Magyar Honvédség Parancsnoksága különleges műveleti személője, aki a 2022-es év egyik legnagyobb különleges műveleti gyakorlatára való felkészülés kapcsán beszélt arról, hogy „*kiemelt szerepet kapnak majd a kiber- és információs műveletek*”, illetve a meglévő kiber- és információs műveleti képességeknek köszönhetően „*jelenleg is van kibervédelmi képesség a parancsnokság és az osztagok szintjén*” (Trautmann, 2022). A tábornok véleménye alapján nem valószínű, hogy önálló, robosztus kiberképesség települ magába a különleges műveleti végrehajtó alegységbe, viszont a különleges műveleti beavatkozóknak tudniuk kell róla, ha valami történik a virtuális térben, tisztában kell lenniük a kinyerhető és átadható információkkal, illetve azzal, hogy hova és milyen csatornán kell ezeket eljuttatni. Annak is ki kell derülnie, hogy milyen gyors az információáramlás a különleges műveleti alegységek és a kiberműveleti képességekért felelős központ között, továbbá melyek azok a képességek, amivel a központ azonnal és hatékonyan képes támogatni a különleges alegységeket műveleteik végrehajtása során.

Ugyanakkor a műveleti szint tekintetében az Egyesült Államok által fejlesztett kiberképességek már évekkel ezelőtt rávilágítottak azokra az eltérő nézőpontokra, amik a kiberképességek hadműveleti és hírszerző alkalmazása kapcsán detektálhatók. Elsősorban az offenzív kiberképességek kifejlesztésére jellemző, hogy olyan programok keretén belül történik, amelyek minősítettek, méghozzá nagyon magas szinten. Ha azonban a képességeket alsóbb szinten alkalmazzák, egy műveleti parancsnok a műveleti tervezés során nem fogja figyelembe venni a kibereszközök alkalmazhatóságát a képességeik teljes ismerete nélkül, mivel azok besorolása

magasabb szintre korlátozódik. A magas szintű besorolást elsősorban az indokolja, hogy egy kibertámadás során használt eszköz – visszafejtés után – komoly sebezhetőséget is jelenthet az alkalmazó fél oldalán, a minősítés módosítása ezért akár elfogadhatatlan mértékű kockázatot is jelenthet. Éppen ezért létfontosságú, hogy az azonnali operatív, illetve a rövid és hosszabb távú hatásokat, eredményeket és kompromisszumokat nagyon pontosan, minden területre kiterjedő méltányossággal kalkulálják. Ehhez az összhaderőnemi műveleti terület (Joint Operational Area – JOA) értelmezésének és kezelésének fejlesztése is elengedhetetlen, mivel a hagyományos földrajzi határok kevésbé értelmezhetők a kibertérben .(Leed, 2013)

A rendvédelem operatív szintjén a digitalizáció térnyerése meglévő és új bűnözési formák fejlődését eredményezi, amelyek több állam joghatóságát is érinthetik egyetlen gomb megnyomásával. Ugyanakkor az elérhető elemzések alapján a bűnüldözői tevékenység nem képes lépést tartani a rosszindulatú kiberbiztonsági incidensekkel. A legtöbb ország nem is tud adatot szolgáltatni a kiberbűnüldözés eredményeiről, miközben becslések szerint az Egyesült Államokban bekövetkező események alig 1 százaléka végződik letartóztatással. Műveleti szinten elengedhetetlen az elektronikus bizonyítékok elemzéséhez és a büntető eljárások során történő alkalmazásukhoz szükséges technikai szakértelem, a nemzetközi és regionális kiberbűncselekményekkel kapcsolatos kooperáció a bűnüldöző szervek napi szintű tevékenysége során, a kiberbűnözés és a kiberbűnözői *modus operandi* tekintetében a technológiai innováció követése, továbbá a kiberbűncselekményekkel kapcsolatos információ és adatgyűjtés kiterjesztése, illetve kölcsönös megosztása a büntetőeljárásban és a hírszerzésben érintett szervezetekkel. Globális szinten mindezek annak ellenére is messze elmaradnak a kívánatostól, hogy a legtöbb kormány elismeri a határozottabb fellépés szükségét a kiberbűnözés elleni küzdelemben. Azonban mindennek elenyésző jelentősége van, ha a technikai, műveleti és jogi hiányosságok, valamint a belőlük fakadó kihívások felszámolásához szükséges erőfeszítéseknél sürgetőbb problémák megoldására koncentrálnak a rendvédelmi és politikai döntéshozók, mint például a globális terrorista tevékenységekre való válaszadás. (Peters és Jordan, 2020) Változás vélhetően csak a kiberbűnözéssel kapcsolatos gondolkodásmód átalakulásával érhető el, illetve a hiányosságokat kiváltó okokra is több figyelmet kell fordítani (Peters és Garcia, 2020). Ennek eredménye lehet a kiber különleges műveleti képességek rendvédelmi szempontból szignifikáns elemeinek kialakítása és fejlesztése.

VI.2 A kiber különleges műveleti erők létrehozása és működési háttere

Elméleti síkon nézve, kiber különleges műveleti erőket, illetve azzal egyenértékű képességeket szinte bárki létrehozhat. Állami és nem állami szereplők egyaránt rendelkeznek speciális képességekkel a kibertérben, amelyeket saját elképzeléseik és céljaik megvalósítása érdekében alkalmaznak. Állami szinten ezek a képességek jellemzően a haderőkön és a nemzetbiztonsági szolgálatokon belül kerülnek kialakításra. Nem állami szereplők esetén azonban meglehetősen heterogén állapotok uralkodnak a háttér és tevékenység függvényében. A profitorientált, technológiai szempontból élenjáró nagyvállalatok gyakran tartanak fenn házon belül olyan képességeket, amelyek többek között a megelőzés és elrettentés terén hasonlóságot mutatnak a kiber különleges műveleti képességekkel. Ilyen például a Microsoft MSTIC (Microsoft, é. n.), a Citibank CSFC (Citibank, é. n.) vagy az IBM X-Force IRIS (IBM, 2021) proaktív koncepciója. Bár szupranacionális szinten a felvállalt megközelítés továbbra is a reaktív képességek kialakítása, speciális összetételük és funkcionalitásuk miatt az Európai Unió kiber gyorsreagáló csapatai (Cyber Rapid Response Teams – CRRT) is azonosságot mutatnak a kiber különleges képességek bizonyos szegmenseivel. Meghatározó trend, hogy kisebb cégek és induló vállalkozások egy-egy *niche* területre specializálódnak és így nyújtanak bárki által igénybe vehető azonnali incidens reagáló, kiberhírszerzési, az internet sötét oldalát ellenőrző vagy épp sérülékenységeket felderítő szolgáltatásokat. Míg az említett entitások tevékenységüket a legális szempontok betartásával végzik, szép számmal találhatunk az etikusság és/vagy illegalitás határain egyensúlyozó szereplőket is, mint például a nulladik napi sérülékenységekkel és az azok kihasználására alkalmas eszközökkel kereskedő Zerodium (Zerodium, é. n.). A kiber különleges műveleti képességek egy része ugyanakkor egyértelműen a kibertér szürke zónájához, illetve a kibertér „feketepiacához" köthető, amelyek szintén bárki számára elérhetők, mint a szolgáltatás alapú DDoS támadások (Imperva, é. n.), illetve zsaroló (Ransomware as a Service – RaaS) (Baker, 2022) és rosszindulatú (Malware as a Service – MaaS) (Tudor, 2022) szoftverek fejlesztése és üzemeltetése.

VI.2.1 A működési keretek kialakításának dilemmái

Jelenleg az esetek túlnyomó többségében rendkívül nehézkes egyértelműen meghatározni a kiberműveleti képességek tekintetében az alkalmazási szabályok kereteit. Többek között olyan kérdések maradnak megválaszolatlanok, mint például: mennyire tekinthető szürke zónás

tevékenységnek egy adott képesség puszta birtoklása vagy aktív alkalmazása; jogos és arányos-e az önvédelem, amikor egy kiber incidens során az egyik fél erre hivatkozik; mi számít megelőző tevékenységnek és mikor, milyen feltételek mellett alkalmazható stb. A kiber különleges műveleti képességekre vonatkozó normák és szabályok mélyreható elemzése önmagában több doktori értekezéshez elegendő témát kínál, így a kutatás fókuszának megtartására való tekintettel nem foglalkozom részletesen a nemzetközi és szövetségi szabályrendszerek dilemmáival, csak néhány átfogó problémát ismertetek röviden.

Ahogy azt Jarno Limnéll[121] írja, a kibertér minden játékost támadóvá tesz, ami arra vezethető vissza, hogy a kiberműveleteket olyan „puha" tevékenységként értelmezik, ami a hagyományos katonai műveletekkel összevetve az elfogadhatósági küszöböt jóval alacsonyabbra teszi. A kibertér a támadóknak kedvez, ezért az offenzív tevékenység domináns a védekezéshez képest. Mindez olyan új és összetett kérdéseket vet fel a nemzeti biztonság szintjén, amelyekre egyetlen állam sem képes egymaga hatékonyan válaszolni. A nemzetközi szabályozás, a digitális hadszíntérre vonatkozó megállapodások és szerződések megoldást nyújthatnának, azonban a kiberfegyverek ellenőrzése nem csak nehézkes, de gyökeresen eltér a kinetikus fegyverek ellenőrző mechanizmusaitól, így nem léteznek bejáratott eljárások és protokollok. A bizonytalanságot tovább növeli az egyértelmű szabályok és normák hiánya, mindez pedig növeli a meglepetés és eszkaláció lehetőségét a nemzetközi kapcsolatokban. (Limnéll, 2013)

Bár léteznek nemzetközi erőfeszítések, mindezek ellenére a kibertér tulajdonképpen a vadnyugat 21. századi, digitális metaforája. Az észak-amerikai kontinens középső részén az 1800-as években uralkodó állapotok számos ponton párhuzamot mutatnak a kibertér jelenlegi körülményeivel, csak Jesse James, Billy a kölyök, a Dalton fivérek vagy épp Butch Cassidy helyett[122] a törvényen kívüli tevékenységeket ma a Fancy Bear, Carbanak, Lazarus vagy Lapsus$ nevek fémjelzik. Ahogy a vadnyugaton bárki banditának állhatott és választhatta a törvényen kívüli életformát, ez a kibertérben ma bármely szereplő számára elérhető opció. A vadnyugat terjeszkedése, a szabályozás hiányosságai és a törvények betartatásának nehézségei mind olyan analógiák, amelyek a kibertérben szinte egy az egyben megfeleltethetők az akkori állapotoknak. Míg vadnyugati elődeik

[121] Jarno Limnéll 1973-ban született, a finn haderő nyugállományú őrnagya, az Aalto Egyetem professzora, kortárs katonai teoretikus és kiberbiztonsági publicista. A hadtudományok doktora, a McAfee kiberbiztonsági cég korábbi vezetője, jelenleg a Tosibox ügyvezető igazgatója.

[122] Valamennyien a vadnyugat törvényen kívüli arcaiként váltak ismertté bankok, vonatok, postakocsik, illetve nem egyszer kormányzati szállítmányok megtámadása és kirablása révén.

jellemzően a bankokat, illetve az értéket szállító postakocsikat és vonatokat fosztották ki, a kibertér banditái a kornak megfelelő pénzügyi infrastruktúrákat támadják szintén anyagi haszonszerzés okán. Ugyanakkor a kibertér vadnyugati jellegét a nemzetközi kapcsolatok szempontjából súlyosbítják a hírszerzési és destruktív motivációval indított támadások.

Napjainkban a kiberműveleti képességek fejlesztését alapvetően egyetlen nemzetközi jogszabály vagy norma sem gátolja, az alkalmazásuk pedig leginkább az adott ország politikai berendezkedésén múlik. Erre utal a Clinton és Bush adminisztráció terrorelhárítási igazgatójának, Richard Clarke-nak a nyilatkozata is, aki a Stuxnet kapcsán utalt arra, hogy egy ilyen támadás egy felelős kormány bürokratikus intézményrendszerén és különféle jóváhagyási folyamatokon kell átmenjen (Gross, 2011). Kiberfegyverek alkalmazása, illetve kibertámadások esetén elsősorban az állami szereplők, illetve állami támogatás vonatkozásában vélhetően léteznek olyan nemzeti szintű eljárási korlátozások, amelyek a fejlesztésre, a célpontok kiválasztására és a bevetésre vonatkoznak és megfelelnek a demokratikus elszámoltathatóság által támasztott feltételeknek (Herr és mtsai., 2020).

Mivel az állami és nem állami szereplők egyre inkább érdekeltek a támadó és védekező kiberképességek fejlesztésében, a játékszabályok kialakítása csak bonyolultabb lesz. A tekintélyelvű rezsimek jelentős szabadságot élveznek a szabályok meghatározásában és adaptálásában. Demokratikus berendezkedésű ellenfeleiknek ezzel szemben korlátozottabbak a lehetőségeik, mivel a kormányokat köti a jogállamiság és a nyilvánosság szigorúbb felügyelete mellett működnek. Bár a nemzetközi kezdeményezések, ha lassú ütemben is, de haladnak a hasonló gondolkodású országok között, sajnos keveset lehet tenni, ha bizonyos szereplők úgy döntenek, hogy nem a szabályok szerint játszanak. Ebből kifolyólag más országok számítógépes hálózatainak megelőző kibertámadása vagy egy kibertámadás gyors megtorlása reális válasznak tűnhet, amely képes elriasztani a jövőbeni incidenseket. Az ilyen akciók azonban hosszú távon aláásható a kibertér még ki sem fejlődött nemzetközi jogi szabályozását és tovább nehezíthetik a kibertér normái kapcsán folytatott vitákat .(Pawlak és Petkova, 2015)

VI.2.2 A polgári demokratikus kontroll szerepe és jelentősége

Az olyan demokratikus berendezkedésű országokban, ahol domináns a honvédelmi, rendvédelmi és nemzetbiztonsági szektorok polgári felügyelete, a kiber különleges műveleti képességek

kialakítása és üzemeltetése tekintetében számos kérdés merülhet fel. Bár az egyes országok szintjén lehetnek eltérések, általánosságban elmondható, hogy legfelső szinten a három szektort választott politikusok, illetve az általuk kinevezett döntéshozók és/vagy testületek felügyelik.

A kiber különleges műveleti képességek kialakításának és működtetésének demokratikus kontrollja kapcsán a kutatás során megkérdezett interjúalanyok egybehangzó véleménye volt, hogy szükség van a biztonsági kontrollok kialakítására, a speciális jogosítványokra és a legmagasabb szintű politikai beágyazottsággal párhuzamosan a politikai felügyelet maradéktalan megvalósítására. A gyakorlati kivitelezés tekintetében a válaszokból több egyszerűen átemelhető nemzetközi példa is kirajzolódott. A nemzeti érdekérvényesítés célkitűzéseihez a központosított felügyelet optimális, ami megvalósítható egy direkt a területhez rendelt tárcanélküli miniszter vagy önálló minisztérium, illetve a törvényhozás által létrehozott bizottságok szintjén. Fontos azonban a hatáskörök pontos rögzítése, amely a műveleti hatékonyság fenntartása érdekében elsősorban a nemzeti érdekérvényesítési célkitűzések és a törvényességi kritériumok teljesülésének ellenőrzését jelenti egy szűk, beavatott kör számára. Míg a hatáskör indokolt esetben kiterjedhetne a kiber különleges műveleti képességet irányító felsővezetők szankcionálhatóságára, az elszámoltathatóság ciklikus jellege dominálna, ami rendkívüli esetben azonnali beszámolási kötelezettséggel egészülne ki. Felmerült a demokratikus kontroll szűk, szakmailag felkészült támogatásának lehetősége, amely a műveleti jóváhagyást meghagyná a képesség irányításának szintjén, azonban olyan mandátummal rendelkezne, ami elősegítené a három szektor érintett tevékenységeivel történő összehangolást és az interoperabilitást. Több esetben szintén felmerült, hogy a kiber különleges műveleti képességeknek más területeken meglévő különleges képességekhez hasonlóan speciális jogosítványokkal, illetve jogkörrel kell rendelkezniük, amire egyfelől a stratégiai és politikai jelentőségű hatások miatt van szükség, másfelől a törvényesség és az erős kontrollok nehéz értelmezhetősége, illetve alkalmazhatósága miatt, például a külföldre irányuló hírszerzés területén.

Mivel a kiber különleges műveleti képességek esetén is fennáll a polgári-katonai kapcsolatok egyik klasszikus etikai dilemmája, amit legjobban a „ki őrzi az őrzőket?” kérdés foglal össze, az interjúk során megfogalmazódott a demokratikus kontrollnak egy olyan eleme, amit nem irányít az államigazgatás, vagy a kormány. Bár ezt elméletben a legtöbb esetben a hatalmi ágak szétválasztása, illetve a törvényhozáshoz vagy bíróságokhoz delegált felügyelet garantálja, a fékek

és egyensúlyok rendszerében esetlegesen bekövetkező anomáliákkal szemben is védelmet nyújthatna egy speciális szisztéma. Ez még ha távoli összehasonlítás is, de az amerikai bírósági eljárások során alkalmazott esküdtszék mintájára működhet. A testület tagjai nem ismernék egymást és a döntéshozatali procedúra is anonim módon zajlana, ugyanakkor a legtöbb országban a szükséges technikai ismeretek és jogi kompetenciák nem állnak rendelkezésre egy ilyen jellegű független szervezet létrehozásához így a megvalósíthatósága erősen kérdéses.

Más megközelítésben olyan politikai, stratégiai irányítási szintre van szükség, ami meghatározza a célokat és a kereteket, ez azonban túlmutathat egy miniszter hatáskörén, így jó gyakorlat lehet a nemzetbiztonsági tanácsadó, a nemzetbiztonsági kabinet, vagy a kormányfő egyszemélyben. A fékek és egyensúlyok szükségszerűen visszaszorulnak a kiber különleges műveleti képesség tevékenysége kapcsán, mivel bizonyos szempontból még egy nemzetbiztonsági szolgálatnál is védettebbnek kell lennie: a létezése is titkos kell legyen.

Annak ellenére, hogy az Egyesült Államok kiber polgári-katonai kapcsolatai jóval régebbi múltra tekintenek vissza, mint sok más országé, több területen is a kapcsolatok javításának szüksége merült fel az elmúlt időszak tapasztalatainak tükrében. A polgári ellenőrzés hagyományos modelljei már nem illeszkednek egy olyan területhez, ahol az ellenféllel való kapcsolat folyamatos és állandó, a frontvonalban pedig a magánszektor áll, amely aktívan védi a kulcsfontosságú digitális területeket a nukleáris fegyverrel felszerelt ellenfelek erőivel szemben. A polgári ellenőrzésnek kritériumokat és ütemtervet kell meghatároznia a siker és a kudarc tekintetében a kibertérben folytatott műveletekkel összefüggésben annak érdekében, hogy a kibertérben elkerülhetők legyenek az olyan nyílt végű konfliktusok, mint az iraki vagy afganisztáni beavatkozás. Az elnöknek egyfajta politikai fojtószelepként képesnek kell lenni a kiberműveletek visszaszorítására vagy indokolt esetben a fokozásra. Amennyiben elmarad egy művelet „lejárati dátumának" meghatározása, az amerikai előretolt védelem koncepciója[123] alapján a művelet

[123] Az előretolt védelem (Defend Forward) koncepciója az Egyesült Államok 2018-as kiber stratégiájában jelent meg. Ennek értelmében a Védelmi Minisztérium a rosszindulatú kiber tevékenységeket – beleértve a fegyveres konfliktus szintje alattiakat is – azok forrásánál zavarja vagy állítja meg. Ez a rosszindulatú tevékenységet követő válaszadással szemben olyan proaktív megközelítést jelent, ami lehetővé teszi az amerikai kibertéren kívüli manőverezést annak érdekében, hogy megfigyelhessék és megérthessék a változó ellenséges szervezeteket és jóváhagyás esetén olyan műveleteket hajtsanak végre, amelyek megzavarják, visszatartják, degradálják az ellenséges képességeket és infrastruktúrát mielőtt azok elérhetnék céljukat. Bővebben: https://cyberdefensereview.army.mil/Portals/6/Documents/2020_fall_cdr/CDR%20V5N3%2002_Murphy_Borghard.pdf?ver=SGIrAHDc1d3ZOrQihG_XFg%3d%3d

állandósulhat még akkor is, ha drága és csekély sikereket ér el. Ezért az előretolt kibervédelmi műveletek lejárata egy-két év kellene legyen, hogy a Kongresszus és a Nemzetbiztonsági Tanács rendszeresen felülvizsgálhassa a siker és a kudarc kritériumait, illetve szükség esetén visszafogja vagy fokozza a tevékenységet. A politikai ellenőrzésnek figyelembe kell vennie, hogy a hagyományoshoz képest a kiberkonfliktusok eltérőek és soha véget nem érők lehetnek, amihez a korábbiaktól eltérő polgári-katonai alkukra van szükség .(Healey, 2022)

A kiber különleges műveleti képességek feletti demokratikus polgári kontroll kialakításánál nem sok, ám annál fontosabb alapelvet szükséges figyelembe venni. Egyrészt kiemelt figyelmet kell fordítani a meglévő kulturális, politikai és jogi keretrendszerre és az ehhez igazított adaptálásra. Másrészt a kiberműveletek sajátos paraméterei alapján – mint például a folytonosság, a magas eszkalációs kockázat vagy a baráti, semleges, illetve ellenséges rendszerekben végzett tevékenység – a hagyományos műveletekhez képest sűrűbb ellenőrzési ciklusokra és felülvizsgálatokra, valamint az ehhez kapcsolódó pontosan meghatározott kritériumokra van szükség. Harmadrészt nagy jelentőséggel bír az egyensúly megtalálása a demokratikus jogállami keretek és a transzparencia biztosítása, valamint a műveleti sikerességet garantáló fedett, illetve letagadható működés között. Bár az autoriter rezsimekkel szemben a demokratikus jogállamok számára az említett alapelvek betartása hátránnyal és több erőforrás bevonásával jár, a teljes kiberműveleti képesség csak akkor működtethető hatékonyan és biztonságosan, ha a hosszú távú fenntartást szavatoló stabil alapok már a kezdetek idején kialakításra kerülnek.

VI.2.3 Az azonnali cselekvés képessége a demokratikus kontroll tükrében

A demokratikus felügyelet és ellenőrzés szignifikáns hatással lehet a kiber különleges műveleti képességek egyik legfontosabb paraméterére, a rendkívül gyors reagáló képességre. Gyakran emlegetett mondás, hogy lerombolni könnyebb és gyorsabb, mint felépíteni valamit. Ez igaz a kibertérben is.

A kibertérben a védő és támadó oldal számára egyaránt a sikert meghatározó tényező a sebesség és az idő. A CrowdStrike kiberbiztonsági vállalat publikusan elérhető globális jelentése alapján a kifinomult támadóknak átlagosan mindössze másfél órára volt szükségük 2021-ben ahhoz, hogy az első kompromittált számítógépről képesek legyenek a számítógépes hálózatokon laterálisan terjeszkedni. (CrowdStrike, 2022a) A cég három évvel korábbi, a támadók sebességével kiemelten

foglalkozó globális jelentése az eltérő állami hátterű szereplőkre lebontva adja meg a támadási intervallumot. Ez alapján a leggyorsabb állami hátterű szereplők Oroszországhoz köthetők és kevesebb mint 19 percre volt szükségük 2018-ban egy támadáshoz. Ugyanez az észak-koreai támadásoknál 2 óra 20 perc, a kínai támadóknál 4 óra, az iráni szereplőknél pedig 5 óra 9 perc volt. Figyelemre méltó, hogy az orosz hátterűnek tulajdonított támadások nyolcszor gyorsabbak voltak a sorban utánuk következő észak-koreai eredetű támadásoknál, miközben az összes támadás átlaga alig haladja meg a négy és fél órát. (CrowdStrike, 2019) A IV. fejezet perzisztenciával foglalkozó alfejezetében már szóba került, hogy a védői oldalon ezzel szemben akár több mint 200 nap is eltelhet, mire egy támadást észlelnek. Ahhoz, hogy a kiber különleges műveletek hatékonyak maradhassanak a védelmi tevékenységek során kulcsfontosságú teljesítmény indikátorok alkalmazása (észlelés átlagos ideje, válaszadás átlagos ideje, hibák közötti átlagos idő stb.) segíthet a reaktív megközelítést proaktívvá tenni (Yoo, 2021). Az offenzív tevékenységek során hasonló indikátorok (hozzáférés megszerzésének átlagos ideje, sérülékenység kihasználásának átlagos ideje, jogosultság-eszkaláció átlagos ideje stb.) alkalmazása kulcsfontosságú a műveletek dinamikájának fenntartása, az észlelés megnehezítése, valamint a kiértékelés tekintetében.

A katonai és félkatonai szervezetek hagyományos parancsnoki lánca túl lassú ahhoz, hogy képes legyen hatékonyan működtetni a kiber különleges műveleti képességet. Ahhoz, hogy az engedélyezési és jóváhagyási folyamatok ne rontsák a műveleti sebességet, két ponton érdemes speciális megoldásokat alkalmazni. Az egyik ilyen a demokratikus kontroll politikai szintre történő korlátozása, amit az interjúalanyok többször is említettek. Az egybehangzó vélemények alapján a demokratikus kontroll nem érheti el a műveletek végrehajtásának alsóbb szintjeit, ott kizárólag a szakmai szempontok érvényesülése dominálhat, ellenkező esetben súlyosan sérülhet a műveleti siker feltételrendszere.

Egy félkatonai szervezetben ugyanakkor könnyedén megvalósíthatók olyan a reguláris haderők eljárásaira emlékeztető megoldások, amelyek a stratégiai és politikai célkitűzések érvényesülését folyamatosan szem előtt tartva, minimális hatékonyságvesztés mellett képesek növelni a műveleti biztonságot. A kiber különleges műveleteket végrehajtó egységek vezetői nem feltétlenül rendelkeznek átfogó információkkal a párhuzamosan zajló egyéb kiber és kinetikus műveletekről, illetve a jogosultsági szintek kapcsán elképzelhető, hogy a művelet szempontjából érdemi információkhoz nem férnek hozzá azok minősítése miatt. Ilyen esetben a hosszas engedélyeztetési

és egyeztetési folyamatokat hatékonyan tudja kiküszöbölni az egység tagjaként tevékenykedő, kvázi „(had)műveleti tiszt”. Egy ilyen pozíció mandátuma kettős. Egyfelől a kiber különleges műveleti egység szerves része, az egység tagjaként részt vesz minden tevékenységben a kiképzéstől és felkészítéstől a műveletek végrehajtásán át a kiértékelésig. Másfelől az egység egyedüli tagjaként magas szintű minősítéssel rendelkező információkhoz fér hozzá, közvetlenül a felsővezetői szinthez van bekötve, speciális jogosultságokkal rendelkezik a társszervek irányában, illetve más kiber különleges műveleti egység azonos beosztású tagjaival különálló műveleti koordinációs tevékenységet folytat. Az egység taktikai és technikai vezetése nem feladata, tevékenysége egyfelől az egység műveleti sikerét, másfelől a stratégiai célkitűzések teljesülését hivatott garantálni.

Hazai viszonylatban eleve problémát jelent, hogy „túl sok gazdája van a kiber területnek”. Nincsenek átgondolva és szétválasztva megfelelően a különböző szegmensek. Ennek ellenére a kiberműveletek teljes spektrumának offenzív képességeket lefedő komponense tekintetében nem szerencsés, ha az a reguláris szervezetek integráns részét képezi. Egy ilyen képesség számára a legfontosabb a letagadhatóság, máshogy nem elképzelhetők a szürke vagy fekete zónás műveletek. Ugyanakkor egy ilyen szeparált szervezetnek mégis a központi kormányzat irányítása alatt kell állnia valamilyen formában, ami magas szintű minősítés mellett megvalósítható akár egy reguláris szervezet dedikált vezetőjén, vagy adott esetben kormányzati, illetve kormányfői nemzetbiztonsági tanácsadó révén.

VI.3 A kiber különleges műveleti erők szerepe és szervezeti integrációja

A kiber különleges műveleti képességek kialakítása lehetőséget biztosít a nemzeti érdekeket és a nemzeti biztonságot érintő fenyegetéseket kezelni képes politikai opciók kiterjesztésére. A kibertér modern konfliktusokban betöltött szerepének növekedése új lehetőségeket teremt a különleges műveletek területén is a stratégiai célkitűzések elérésére. A kiberképességek – ahogy más területeken is – a különleges műveletek során egyre inkább a tevékenységet elősegítő és lehetővé tevő elemmé válnak. A kiber különleges műveleti képességek azonban szervezeti integrációs kérdéseket vetnek fel.

„Korábban még különbség volt a külső és belső biztonság között, amely megjelent szervezeti, intézményi különállóságban is. A szakirodalomban a „defence policy” mindig a haderővel, a

katonai védelemmel kapcsolatos kérdéseket foglalja magában, míg a „home defense", a „home security" a belső biztonság teljes spektrumával (terrorizmus elleni védelem, katasztrófavédelem, kibervédelem, bűnözés elleni harc stb.) kapcsolatos elvi és gyakorlati kormányzati tevékenységet jelentette." (Szenes, 2020) A honvédelmi és rendvédelmi tevékenységek szétválasztása Finszter Gézánál is megjelenik. *„Létezik két hivatás, a katonáé és a rendőré, amelynek egyaránt a veszélyelhárítás a társadalmi rendeltetése. Mindkét szakma gyakorlójának speciális tudása, hogy képes felismerni a szakmai kompetenciájába tartozó fenyegetéseket"* .(Finszter, 2010) A 21. század honvédelmet és rendvédelmet érintő folyamatai azonban több szempontból is kihívások elé állítják azt a történelmileg kialakult modellt, amely alapján a katona a külső fenyegetésekkel szemben, míg a rendőr a belső kihívásokkal szemben lép fel. *„A sokféle veszély és fenyegetés halmozódik, összeadódik, hibriddé válik, a külső és belső fenyegetettség közötti határ elmosódik, vagy éppen megszűnik."* (Szenes, 2020)

Amikor a világ nemzetei terrorizmussal, lázadókkal vagy határaikon túli túszválságokkal szembesülnek, a legjobban képzett és speciálisan felszerelt egységeikhez – a legelitebb harcosaikhoz – fordulnak. Ami közös bennük, hogy ezeknek az egységeknek a tagjai szigorú kiválasztáson és speciális képzésen esnek át, hogy azután készen álljanak az azonnali bevetésre. (Marsh, 2017) A műveletek kibővülése a kibertérrel, illetve a fizikai és kiber műveletek közötti határok elmosódása azt eredményezi, hogy a világ nemzeteinek a kibertérben vagy annak felhasználásával megvalósuló különböző indíttatású műveletekkel is számolniuk kell már. A nemzeti kiberbiztonság megteremtéséhez a kiberműveletekben is magasan képzett és speciálisan felszerelt egységekre van szükség. Tagjaik speciális kiválasztáson és képzésen esnek át és bármikor bevethetők a legmagasabb kockázatú szituációkban is, a műveletek teljes spektrumán.

6. ábra: A kiberműveletek passzív és aktív védelmet, valamint offenzív műveleteket is magába foglaló teljes spektruma. (Az ábrát szerkesztette a szerző Panayotis A. Yannakogeorgos Strategies for Resolving the Cyber Attribution Challange és a George Washington Egyetem Into The Gray Zone című publikációi alapján.)

Azzal kapcsolatban, hogy egy ilyen képességet milyen formában és szervezeti integrációs keretek között érdemes létrehozni, a nemzetközi példák három alternatívát kínálnak. Egyfelől gyakori, hogy a haderőkön belül önállóan, vagy a katonai hírszerző és elhárító területhez kapcsolva jönnek létre speciális kiberműveleti képességek. Másfelől elterjedt megvalósítási mód a polgári hírszerző és elhárító szervezeteken belül történő kialakítás, illetve önálló szervezet létrehozása a polgári nemzetbiztonsági szektorban. A harmadik mód nyilvánosan a legkevésbé dokumentált és azokat a képességeket fedi le, amelyek állami érdekek mentén megvalósuló tevékenységet folytatnak, azonban nincs bizonyított kapcsolat egyetlen katonai vagy nemzetbiztonsági szervezettel sem, ezért számos kérdés merül fel az irányításukkal és ellenőrzésükkel összefüggésben.

A kiber különleges műveleti erők létjogosultsága kapcsán az interjúalanyok egyöntetű véleménye, hogy abszolút szükség van ilyen képességekre és alapvető része kellene legyen az állami érdekérvényesítés eszközrendszerének. Egy ilyen képesség ugyanolyan jelentőséggel bír, mint a szárazföldi erők vagy a légierő bármely képessége, miközben jelentősége folyamatosan növekszik, ezért egyre inkább nélkülözhetetlen. A szervezeti integráció kapcsán a válaszokból az derül ki, hogy nehéz kizárólagosságot meghatározni, vagyis egyetlen honvédelmi, rendvédelmi vagy nemzetbiztonsági szervezethez telepíteni a képességet. Ez egyfelől a három szektor eltérő céljaiból és feladataiból fakad, másfelől a különböző területek igyekeznek kialakítani a saját igényre szabott kapacitásaikat, ami szétszórtan eltérő minőségű és mennyiségű kapacitásokat eredményez. Több esetben felmerült a kiberműveletekhez szükséges gondolkodásmód miatt a katonai és nemzetbiztonsági integráció lehetősége, illetve az összes szektor felett álló egyfajta „ernyőszervezet” kialakítása.

A képesség összetevőinek passzív és aktív védelmi, illetve offenzív felosztása mellett az interjúk során felmerült a három tagú defenzív, offenzív és destruktív besorolás, valamint egy tanulmány nyomán egy öt elemből álló megközelítés is. Utóbbi tartalmaz passzív és aktív védelmi képességeket a hozzáférés megtagadásának keretén belül, elterelést is magába foglaló passzív offenzív képességeket, illetve két aktív offenzív elemet: a kiberhadviselést és a kiberhírszerzést. (Jaquire és von Solms, 2017) A felosztásoknak megfelelően eltérő lehet a képességek kialakítása és szervezeti integrációja, azonban többen is egyetértettek abban, hogy szigorú feltételek mellett szükség lehet privát, illetve szerződéses képességek és kapacitások igénybevételére. Ennek megvalósítása legtöbb esetben az adott állam lehetőségeitől és erőforrásaitól függ. Amennyiben

ezek korlátozottak, előfordulhat, hogy a kiberképesség bizonyos elemeinek házon belül történő kialakítása nem lehetséges vagy költséghatékonyabb a piacról beszerezni. A nemzetbiztonsági háttérrel rendelkező válaszadók felhívták a figyelmet arra, hogy ha nincs kiberhírszerző és -elhárító képesség, az kiszolgáltatottságot eredményez nemcsak az ellenfelek, hanem a baráti és azonos szövetségi rendszerhez tartozó országok érdekérvényesítő törekvéseivel szemben is.

VI.3.1 Katonai integrációs lehetőségek

A kiber különleges műveleti képességek katonai szervezeti integrációjára több nemzetközi példa is van. Az Egyesült Államok Kiber Parancsnoksága, illetve a kínai haderő és az orosz katonai hírszerzés kiberképességei egyaránt ide sorolhatók. Ahogy az a III.3 alfejezet esettanulmányaiból is kirajzolódott a gyakorlati megvalósítás országonként eltérő lehet, nincs egységes megközelítése a kiberműveleti képességek haderőkön belül történő kialakításának.

Az interjúkból az derül ki, hogy a katonai kiberműveletek jól elválaszthatók más szektorok kiberképességeitől. A haderőkben elsősorban olyan offenzív tevékenységek valósulnak meg, mint a hírszerző és destruktív műveletek. Ennek okát a haderők alaprendeltetésén túl többnyire a gondolkodásmódban és a felkészítésben, illetve kiképzésben érdemes keresni. A katonai gondolkodásmódban hagyományos műveletek esetén is domináns szerepe van a támogató hírszerző tevékenységnek, miközben a végső cél eléréséhez az ellenség erőinek pusztítása és infrastruktúrájának rombolása általánosan bevett megközelítés. Optimális esetben a katonai kiber különleges műveletek ennek megfelelő jogosítványokkal kell rendelkezzenek és a működési feltételek kialakítását is ehhez kell igazítani. A túlzott szabályozás elkerülése fontos a műveleti sebesség és eredményesség szempontjából, ezért a jogos-jogtalan képességhasználat kérdését a képességek alkalmazásának szakszerű és pontos naplózása segítheti a leghatékonyabb módon.

A kiber különleges műveleti erők (SOF) a kibertartományban speciális műveleti tevékenységek végzésére szakosodott erők. Létrehozásuk biztosíthatja azokat a képességeket, amelyek szükségesek ahhoz, hogy egy ország különleges műveleteit teljes mértékben kiterjesszék a kibertartományra. Azonban a politikai és stratégiai lehetőségek jelentőségteljes bővítéséhez a kiber SOF szervezeti felépítése kapcsán speciális kritériumoknak kell teljesülniük. A kiber SOF képes kell legyen a sebészeti csapásmérő és a speciális hadviselési küldetések végrehajtására a speciális műveletek alaptevékenysége során. A kinetikus SOF képességek támogatásán túl a kiber SOF

olyan saját küldetéseket is végre kell tudjon hajtani, amelyek során az erőfeszítések elsődleges dimenziója a kibertér. A kinetikus SOF képességek bővítése és a magas szintű adaptáció nem megvalósítható, ha a kibertartomány csak mellékes vagy utógondolatként jelenik meg a küldetések során. (Brown, 2018)

Az amerikai haderő kiber parancsnokságának felépítését alapul véve a kiber missziós erők 133 csapatából 27 nyújt támogatást a harctéri parancsnokságoknak, 68 csapat a haderő számítógépes rendszereit védi. Ez az elosztás kérdéseket vet fel, hogy egy hagyományos katonai struktúrában működő kiberképesség mennyire tud hatékony és átfogó támogatást nyújtani a különleges műveletekben. Amennyiben a kiber különleges műveleti képesség nem a kinetikus különleges műveleti képességekért felelős parancsnoksághoz tartozik, a szervezeti elhatárolás koordinációs problémákhoz vezethet a kiber és kinetikus SOF tevékenységek között. A szilárd szervezeti határok létrehozása a kiber és kinetikus különleges műveleti képességek között zavaros C2 hierarchiához és a kiképzési integráció, valamint az interoperabilitás hiányosságához vezethet. (Brown, 2018)

A kiber SOF katonai integrációs lehetősége kézenfekvő megoldás lehet minden ország számára, ahol a haderő rendelkezik kinetikus különleges műveleti képességekkel függetlenül attól, hogy már létezik-e a kibertartományban folytatott katonai tevékenységekért felelős egység. Azonban országonként eltérő lehet és erősen függ a haderők kultúrájától, hogy a kiber különleges műveleti képességek milyen szervezeti beágyazottsággal kerülnek kialakításra. A nemzeti érdekek érvényesítésében és védelmében betöltött szerep, illetve a kibertér növekvő dominanciája a jövő konfliktusaiban együttesen indokolja, hogy a kiber SOF a kinetikus különleges műveleti erők alárendeltségében vagy velük nagyon szoros kapcsolatban működhessen, esetleg közös parancsnokság alatt fejlődjenek. Egy ilyen szervezeti integráció elsősorban a hírszerző és destruktív kiberképességek terén hozhat jelentős eredményeket, azonban a hagyományos kibervédelem fejlődéséhez csak csekély mértékben képes hozzájárulni, azokat más módon szükséges biztosítani. Erre utal az a gondolatmenet is, ami az egyik interjú során hangzott el: az uniformizáltság miatt a különleges képességeket egyetlen reguláris szervezet sem tudja „se kiköpni, se lenyelni”, aminek a gyökere abban keresendő, hogy a reguláris képességek a törvényes célokat törvényes eszközökkel érik el, míg a különleges és egyéb (pl. nemzetbiztonsági) szolgálatok sokszor nem reguláris (törvénytelen) eszközöket alkalmaznak a céljaik eléréséhez.

VI.3.2 Nemzetbiztonsági integráció, vagy önálló szervezet

A kiber különleges műveleti képességek nemzetbiztonsági integrációjára – a katonaihoz hasonlóan – több nemzetközi példa is van. Az Egyesült Államok Nemzetbiztonsági Ügynöksége és az elhárításért felelős orosz Szövetségi Biztonsági Szolgálat kiberképességei egyaránt ide sorolhatók. Ahogy a III.3 alfejezet esettanulmányaiban látszódott, a gyakorlati megvalósítás itt is országonként eltérő lehet, nincs egységes megközelítése a kiberműveleti képességek nemzetbiztonsági szektoron belül történő kialakításának.

Az interjúk kapcsolódó kérdéseire adott válaszok alapján sok szempont teszi indokolttá a nemzetbiztonsági szektor kiberképességeinek specializált fejlesztését. Ezt főként az indokolja, hogy egy ország érdekeinek érvényesítését és védelmét békeidőben is fontos, hogy magas szinten legyen képes ellátni az erre kijelölt apparátus. Mivel egyre inkább igaz, hogy a konfliktusok része vagy egésze a kibertérben zajlik, a befolyásolási törekvésekkel szemben jelentős mértékű kitettség alakul ki ebben a dimenzióban. Tekintettel arra, hogy a legtöbb országban a külföldi befolyásolástól való mentesség garantálása a nemzetbiztonsági szervezetek feladatkörébe tartozik, kézenfekvő a hatékony és erőteljes nemzetbiztonsági kiberműveleti képességek kialakításának igénye. A kiber különleges képességek kialakításának szektorális megközelítése nem nélkülözheti a nemzetbiztonsági érdekeket, azonban a katonai képességekhez viszonyítva jelentősen eltérő jogosítványokra van szükség. A polgári hírszerző és elhárító tevékenységek a lefedett területek számából és heterogén jellegéből fakadóan komplexebb megközelítést igényelnek, és ennek a kiber dimenzióban is érvényesülnie kell. Ugyanakkor a nemzetbiztonsági szektorra jellemző a leginkább, hogy hiányosságok vannak az információk megosztása és a technológiai transzfer terén az alrendszerek között.

Ennek kiküszöbölésére nyújthat alternatívát egy új, önálló szervezet létrehozása vagy egy ernyőszervezet kialakítása a meglévő képességek bázisán. Az interjúalanyok mindkét opció tekintetében erős szkepticizmussal nyilatkoztak. Bár a képességek minősége és mennyisége tekintetében az önálló szervezet létrehozása járna a legtöbb eredménnyel, a negatívumok között mindenképpen említésre méltó, hogy ez veszi igénybe a legtöbb időt és valószínűleg a legtöbb forrást is. Ez a legmagasabb szintű politikai és stratégiai elköteleződést igényli olyan hosszú távon, ami a legtöbb országban akár több kormányzati cikluson is túlmutat. Emiatt politikai aspektusból nézve kicsi a valószínűsége, hogy a különböző politikai és ideológiai irányzatokat képviselő elit

egységes támogatása nélkül megvalósítható lenne egy kiber különleges műveleti képességeket tömörítő nemzetbiztonsági szervezet. Operatív szinten a hagyományos nemzetbiztonsági szervekkel történő hatékony együttműködést a megfelelő szabályozással le lehetne fedni, illetve a műveletekben való szerepvállalást könnyedén fel lehetne osztani a támogató és vezető szerepkörök mentén, amihez optimális jogosultságok és kötelezettségek társulnának.

Az együttműködésnek erre a szintjére kevés példa van a nemzetbiztonsági szektorban, ezért is választja sok esetben a politikai elit, hogy ernyőszervezetet hoz létre az egymással rivalizáló nemzetbiztonsági szolgálatok által megszerzett információk, illetve az általuk folytatott műveletek koordinálására. A kiber különleges műveleteket koordináló ernyőszervezet esetében érdemes megvizsgálni nemzetközi vagy akár hazai példákat más területeken (pl.: terrorelhárítás). Többnyire az látható, hogy nem új képességek kialakítására valók, hanem a meglévő képességek hatékonyságának növelését szolgálják, egyfajta integrációs szervezetként próbálnak működni, több-kevesebb sikerrel. A kiber SOF ernyőszervezetként történő létrehozása relatív olcsó és gyors megvalósíthatóságot kínál, cserébe a szervezettel szemben támasztott elvárások nem mutathatnak túl az operatív és stratégiai szintek közötti koordináción. Így nem is lehetne valódi kiber SOF. Az ernyőszervezet létrehozásának abban az esetben van értelme, ha a honvédelmi, rendvédelmi és nemzetbiztonsági ágazat is kialakította már a saját igényeihez és feladataihoz szabott kiber különleges képességeket.

A kiber SOF nemzetbiztonsági fókuszú kialakítása a kiber és fizikai konfliktusok közötti határok elmosódása, valamint a „szűrke zónás” tevékenységek terén szerzett tudás és tapasztalat miatt lehet indokolt, azonban a rendvédelmi és honvédelmi szektor igényeinek becsatornázása jelentős nehézségekbe ütközhet.

VI.3.3 Félkatonai, paramilitáris koncepció

A legkevesebb nyilvános információ a kiber különleges műveleti képességek félkatonai megvalósításával kapcsolatban áll rendelkezésre. Bár több jel is arra utal, hogy léteznek olyan, például az Egyesült Államok hírszerző közösségéhez vagy az orosz, illetve kínai fegyveres erőkhöz köthető szervezetek, amelyek különböző kiberműveletekben jutnak szerephez, nyíltan egyetlen ország sem vállalja fel, hogy ilyen koncepció mentén hajtana végre kiberműveleteket. A III.3 alfejezet esettanulmányaiból a félkatonai megvalósításhoz valószínűleg az amerikai célzott

hozzáférésekkel foglalkozó szervezetek strukturális és működési mintái állnak a legközelebb. Fontos megjegyezni, hogy a nemzetbiztonsági, illetve rendvédelmi területen hivatásos állománnyal működő kiberműveleti képességek is alapvetően félkatonai megvalósításnak tekinthetők, mivel a működésük számos ponton átfedést, illetve hasonlóságot mutat a katonai szervezetekkel, azonban a haderőknek nem részei.

A hagyományos félkatonai koncepció kapcsán a válaszadók több esetben is hátrányként hozták fel a transzparencia hiányosságait és ehhez kapcsolódóan a társadalmi beágyazhatóságot, ami olyan területekre is jelentős hatást gyakorolhat, mint a toborzás. A koncepciónak univerzális jelleget biztosít, hogy bármelyik szektorban megvalósítható, azonban a jogi háttér kialakítása már jóval több fejtörést okozhat. Különösen igaz lehet ez abban az esetben, ha civil képességek vagy szakértelem bevonása is megtörténik. Azzal kapcsolatban jelentős egyetértés mutatkozott, hogy a kiber különleges műveleti képességeket hivatásos állományra kell alapozni, azonban az „államigazgatási mentalitás" ezt többé-kevésbé teljesen ellehetetleníti. A kiber SOF olyan speciális szakértelmet igényel sok esetben, amit egy kizárólag hivatásosokból álló szervezet nem képes kialakítani.

Ezen a ponton merül fel egy olyan hibrid megoldás, amelyben a félkatonai szót a hagyományos alkalmazásától eltérő megközelítésben használjuk. A kiberbiztonsági területhez kapcsolódó szakértelem növekvő hiányáról még lesz szó, a koncepció alapjaihoz elegendő megérteni azt a jelenséget, ami a hiányt generálja. Ez pedig nem más, mint a kibertér bővülésének dinamikája. Akkora sebességgel és olyan mértékben terjed a mindennapos társadalmi tevékenységek során a kibertérhez kapcsolódó eszközök és folyamatok alkalmazása, hogy sokszor észre sem vesszük azt, hogy egy újabb ponton kapcsolódunk a kibertérhez. Ennek a dinamikának azonban vannak negatív jelenségei, az ezekből fakadó kihívásokat, kockázatokat és fenyegetéseket pedig a kiberbiztonsági szakemberek igyekeznek elfogadható szintre csökkenteni. És itt válik a kiberbiztonsági szakértelem mennyiségi kérdéssé, mivel az elérhető szakemberek száma egyrészt korlátozott, másrészt a kiberbiztonsági szakértők számának változása nincs arányban a kibertér bővülésével és az ebből eredő kitettség növekedésével. Bár az automatizáció bizonyos területeken képes radikálisan csökkenteni a humán szakértelem szükségét, a terület bővülésének lendülete következtében még a legjobb ajánlatokat biztosító versenyszféra számára is nehéz és hosszú idő betölteni a nyitott kiberbiztonsági pozíciókat. Egy ilyen, a kiberbiztonsági szakértelemért folytatott

kiélezett versenyben a közszféra nem csak, hogy „labdába sem tud rúgni”, de bizonyos országokban már a „pályára való kiállás” sem megy.

A kiberműveletek teljes spektrumában bevethető különleges műveleti képességek kialakítása egy olyan szervezetben, ahol a félkatonai jelző nem csak az állomány hivatásos mivoltára és hovatartozására, hanem a működési körülmények egyéb aspektusaira is utal, megfelelő alternatíva lehet a nem hagyományos és hibrid kihívásokkal szemben. Az egyik ilyen aspektus a civil szakértelem hatékony bevonása és hosszútávú megtartása, aminek egyik módja lehet, ha a hivatásos állományra vonatkozó feltételrendszer és jogi szabályozás módosításra kerül. Az interjúalanyok a hivatásos állományt elsősorban az átvilágíthatóság, illetve a számonkérhetőség és szankcionálhatóság, valamint egyéb biztonsági feltételeknek való megfeleléssel indokolták. Ugyanakkor ehhez nem feltétlenül van szükség arra, hogy az állomány tagjai a fegyveres testületekre vonatkozó, különböző jogállási szabályozás hatálya alá essenek, vagy a tagjait katonai bíróság elé lehessen állítani. A fegyveres szervezetekre jellemző „beöltöztetési kényszert”[124] könnyedén vissza lehet szorítani a kiber különleges műveleti tevékenységet ellátókra vonatkozó büntetési tételek és más speciális jogszabályok kialakításával, illetve jelentős mértékű átalakításával. Szintén a professzionális szakértelem bevonását és a „beöltöztetési kényszer” redukálását szolgáló módszer a kiválasztási feltételrendszer reformja, a juttatások struktúrájának átalakítása és a feladatellátáshoz kapcsolódó személyi követelmények felülvizsgálata.

Egy ilyen gondolkodásmód (mindset) mentén kialakított kiber különleges műveleti képességben bár megmaradhatnak a hivatásos elnevezések, beosztások és rendfokozatok, az állomány összetétele teljes mértékben heterogén lehet, ami a fegyveres szervek hierarchikus struktúrájához képest jóval laposabb, horizontális szerkezetű, lazább szervezetet eredményez. Ugyan maradnak speciális elvárások és követelmények, ezek sok esetben minimális mértékben térnek csak el a versenyszférában alkalmazott feltételrendszerektől.

A félkatonai jelző kibővített használatának másik aspektusa a kiber SOF fizikai és kiber körülményeire vonatkozik. Mivel a kiber dimenzió térnyerése átírja a nemzetközi kapcsolatok során a kooperáció és a konfliktusok játékszabályait, illetve sok esetben a szereplők nem tartják be

[124] A beöltöztetési kényszer szókapcsolat arra a jelenségre értendő, hogy a honvédelmi és rendvédelmi szektorokban az állomány eredetileg civil tagjait gyakran annak ellenére átveszik hivatásos, illetve szerződéses szolgálatba és egyenruhába öltöztetik, hogy az általuk végzett tevékenység ezt nem indokolja.

azokat, a hatékony működésének létfontosságú feltétele, hogy a szervezet adaptív legyen. Ehhez szükséges olyan körülményeket és környezetet kialakítani, amiben a kiber SOF a lehető legnagyobb szabadsággal, a korlátozó tényezők minimálisra szorításával tud működni. Ez a fizikai dimenzióban a teljesség igénye nélkül kiterjed a szükséges jogosítványok meglétére, védett objektumok használatára, kettős felhasználású és katonai technológiákhoz való natív hozzáférésre, konspiratív és fedett eljárások, módszerek, technikák alkalmazására, illetve mindenre kiterjedő, műveletekre szabható eszközparkra, amelyek feltétlenül magukban foglalják a kibertér fizikai rétegét. A kiber dimenzióban az ideális működési körülményekhez és környezethez tartoznak többek között a speciális jogosultságok és hozzáférések, számottevő kriptográfiai és szteganográfiai képességek, szignifikáns (szuper)számítógépes kapacitások, valamint a feltörekvő technológiák rapid elérése.

A kiber SOF kiterjesztett félkatonai koncepciója képes feloldani a biztonsági- és védelmi szektor képességfejlesztést gátló dilemmáit, egyúttal választ ad a legjelentősebb képességfejlesztési kihívásokra is, azonban olyan szemléletmódot, hosszútávú elköteleződést és tervezést igényel, ami sok országban nem, vagy csak nagyon nehezen megvalósítható.

VI.3.4 „Kontraktor" modell – CCaaS (Cyber Capability as a Service)

A kiber különleges műveleti képességek „kontraktor", azaz szerződéses alapú megközelítésének alapját a katonai magánvállalatok (Private Military Company/Contractor – PMC)[125] adják. Ezen a téren a nagyhatalmak közül az Egyesült Államok és Oroszország is tart fenn képességeket a fizikai dimenzióban. Előbbi esetében ismerős lehet az Academi (ex Blackwater), utóbbinál pedig a Wagner Csoport neve csenghet ismerősen. Bár erősen vitatott, van olyan megközelítés, ami alapján ebbe a kategóriába (PMC) sorolják az amerikai Northrop Grumman és Raytheon, a francia GEOS, a lengyel Európai Biztonsági Akadémia (European Security Academy), a német Asgaard és a brit Aegis nevű cégeket is. A Fegyveres Erők Demokratikus Ellenőrzésének Genfi Központja (Geneva Centre for the Democratic Control of Armed Forces – DCAF)[126] meghatározása szerint a PMC-k olyan üzleti tevékenységet takarnak, amelyek háborúhoz és konfliktushoz kapcsolódó speciális

[125] A katonai magánvállalatok fegyveres harci és biztonsági szolgáltatásokat nyújtanak pénzért. A szolgáltatások jellemzően a kormányzatok biztonsági, katonai és rendőri erőinek tevékenységéhez és szakértelméhez hasonlít, azonban kisebb méretben.

[126] A Fegyveres Erők Demokratikus Ellenőrzésének Genfi Központja egy alapítványi formában működő kormányközi think tank, amely főként kutatási és projekt támogatási tevékenységet nyújt állami és nemzetközi szereplők számára a biztonsági szektor irányításához és reformjához.

szolgáltatásokat nyújtanak, beleértve a harci műveleteket, stratégiai tervezést, hírszerzést és információgyűjtést, műveleti és logisztikai támogatást, valamint a beszerzést és fenntartást. Lényeges ismertetőjegyük, hogy vállalati struktúrában működő regisztrált üzleti vállalkozások és szolgáltatásaikat politikai indíttatás helyett haszonszerzés céljából kínálják. (Law, Caparini, és Kartas, é. n.)

Tekintettel arra, hogy a katonai és biztonsági magánvállalatoknak könyvtárnyi irodalma van, nem kerül részletes kifejtésre a modell működőképessége kiber különleges műveleti aspektusból. Továbbá a katonai és biztonsági magáncégek fegyveres konfliktusokban való részvételéhez köthető államokra vonatkozó nemzetközi jogi kötelezettségek, illetve a műveletekkel kapcsolatos bevált gyakorlatokról szóló Montreauxi Dokumentumon (ICRC, 2009) kívül a PMC-k nemzetközi jogi szabályozása a kiberkonfliktusokhoz hasonló hiányosságokkal küzd. Ezért a kiber különleges képesség katonai magánvállalati alapú megvalósításának nemzetközi jogi háttere önmagában több doktori disszertáció témája lehetne.

Mindazonáltal a kiberképességek teljes spektrumának szolgáltatásként (Cyber Capability as a Service – CcaaS) történő igénybevétele, illetve megteremtése teljesen reális megoldás lehet egy olyan országban, ahol adottak ehhez a körülmények. A modell egyik legnagyobb előnye, hogy az állam és a szolgáltató közötti kapcsolat könnyedén letagadható, így a műveletek során adódó probléma esetén, a felelősség áthárítása egyszerűbb. Szintén előnyként értelmezhető az azonnali bevethetőség, az erő alkalmazás negatív megítélésének csökkenése és az, hogy a nemzetközi jogi hiányosságokból fakadóan a szankcionálhatóság nehézségekbe ütközik. Negatívumként hozható fel, hogy kevés az olyan PMC, amelyik a kiberműveleti képességek teljes spektrumában képes lenne szolgáltatást nyújtani, ezért akár egy műveleten belül is több PMC közreműködésére lenne szükség. Még így is előfordulhat, hogy bizonyos feladatokat egy PMC csak harmadik félhez történő kiszervezéssel tud megoldani. Ez mindenképpen rontja a műveleti integritást, illetve hatásköri konfliktusokhoz vezethet, miközben számos kérdés merül fel a kiber képességeket nyújtó PMC-k jogosítványaival és engedélyeivel, valamint a felhatalmazásukkal összefüggésben.

Az állam és képesség között létrejövő kapcsolat okán a kontraktor modellhez áll legközelebb az egyik interjú alany által felhozott megközelítés, amivel napjainkban nem nagyon foglalkozik sem a politikai sem a szakmai közösség, mivel szinte kizárólagos a nemzeti megközelítés. Tekintettel a szakemberek és a szaktudás körüli nehézségekre a Francia Idegenlégió (Légion étrangère) egy

olyan minta lehet, amit minimum alaposabban körbe kellene járni hadtudományi, rendészettudományi és más aspektusokból, hogy milyen elemeit lehetne átemelni és hasznosítani egy esetleges „kiberműveleti idegenlégió” létrehozásakor. A vizsgálatnak ki kellene terjednie a szövetségi rendszerekre, a potenciális partnerországokra, illetve olyan régiókra ahol biztosan nincs érdekütközés, hogy hiteles képet lehessen alkotni a teljes spektrumú kibervédelem multinacionális keretek között történő megvalósításáról

VI.4 A kiber különleges műveletek végrehajtóinak toborzása és kiválasztása

Mivel a kiberbiztonság harmadik pillére – a technológia és a folyamatok mellett – az ember, különösen fontos szerepe van a kiber SOF humán erőforrás ellátásának. Többféle megközelítéssel is találkozhatunk, kezdve a kiberbiztonsági szakmai utánpótlás biztosítására létrehozott, több mint 20 éves amerikai programmal, ami 300-nál is több Nemzeti Kiberbiztonsági Akadémiai Kiválósági Központ (National Centers of Academic Excellence in Cybersecurity – NCAE-C) (NCAE, é. n.) hálózatát jelenti. Másutt inkább a nemzeti kibervédelemért is felelős szervezet tapasztalat, nyelvtudás és szakképzettség nélkül keres operatív beosztásba (Sz.n., 2022) munkatársakat. És akad példa arra is, hogy a kiberbiztonsági humán kapacitások bővítését különböző események szervezésével, kiberképzési adatbázissal és a kiberbiztonsági készségek keretrendszerének kialakításával (Nurse és mtsai., 2021) igyekeznek elősegíteni.

A kiber különleges műveleti képességek tervezésekor mindenképpen figyelembe kell venni azokat a trendeket és előrejelzéseket, amelyek alapján napjainkban közel 3 millió kiberbiztonsági szakember hiányzik globális szinten. (ISC2, 2021) Bár a becslések alapján ez nagyságrendileg 400 ezres csökkenést jelent egy év alatt, ha a kiberbiztonsági területen megjelenő 700 ezer új pozíció számával vetjük össze, az látszik, hogy több mint 4 millió kiberbiztonsági szakemberre van szükség globális szinten. Ez is annak a fejlődési, illetve bővülési dinamikának a része, amire az VI.3.3 fejezetben már utaltunk. Miközben a 2010-es évek derekán készült előrejelzések (McAfee, 2016) már a jelenlegi felére becsült szakember hiányt is jelentős problémának ítélték (Kaspersky, 2016), a jelenséget további váratlan tényezők is jelentősen befolyásolják. A 2020 tavaszán kitört világjárvány következtében a távoktatási és távmunka megoldásokra történő hirtelen és tömeges átállás megnövelte a kiberbiztonsági igényeket is, ami újabb lendületet adott a kiberbiztonsági szakemberek iránti kereslet növekedésének. A jelenség egyik kézzelfogható momentuma volt,

amikor az egyik meghatározó videó konferencia alkalmazás felhasználói bázisa alig 5 hónap alatt húszszoros növekedést könyvelt el, majd 90 napra felfüggesztette minden funkció fejlesztését és a teljes fejlesztői kapacitást az adatvédelmi és biztonsági problémák megoldására csoportosították át. (Warren, 2020) Ugyanakkor nem csak a kiberbiztonsági munkaerő szempontjából értékelhető hátrányos következményként, hogy a világjárvány által generált bizonytalanságból fakadóan a szervezetek közel negyede csökkentette a munkavállalói képzések költségvetési kereteit. (Cybrary, 2020)

A kiber különleges műveleti képességek tervezőinek helyzete nem könnyű. Bár vannak olyan – elsősorban hazai – szakemberek, akik szerint nincs, illetve nem jelentős a szakemberhiány, a jelenség mértékétől függetlenül várhatóan még egy ideig biztosan velünk marad, miközben egy ilyen speciális területen további szempontokat is figyelembe kell venni a toborzás során, amik csökkenthetik az alkalmas jelöltek számát. Az interjúk során egyetértés mutatkozott több készség, képesség és ismeret tekintetében, amelyek nélkülözhetetlenek egy kiber különleges műveleti alakulatnál. A léptékek megismeréséhez viszonyítási alapot nyújt a Stuxnet kifejlesztése és alkalmazása kapcsán kialakított empirikus feltevés. E szerint megközelítőleg 45 ember minimum fél éves összehangolt tevékenységére volt szükség a Stuxnet elkészítéséhez, köztük ipari folyamatirányítási tanácsadókra (2), SCADA és PLC tervező mérnökökre (2), a Siemens eszközeinek programozására szakosodott fejlesztőkre (3), nukleáris fűtőanyag termelési szakértőkre (2), operációs rendszer fejlesztőkre (5-10), sérülékenység elemzőkre (2), a sérülékenységet kihasználni képes eszközt elkészítő programozókra (3), minőségbiztosítási operátorokra (3), labor tesztelőkre (3), infrastruktúra üzemeltetőkre (5), továbbá helyszíni hírszerzőkre (1-10) és a telepítést elvégző specialistákra (1-2). (De Falco, 2012) Egy ilyen majdnem 50 fős csapatban szükséges készségeket, képességeket és ismereteket az interjúk nyomán a következő alfejezetekben tárgyaljuk.

VI.4.1 Technikai ismeretek

Több fontos megállapítás között az egyik minden interjúban megjelenő elem a technikai ismeretek alapvető szüksége volt. Bizonyos esetekben ez volt a legfontosabb szempont: a mély, bizonyos értelemben ösztönös technikai képességek. A kiber különleges műveletek fő profiljára való tekintettel ez a kibervédelmi, illetve incidenskezelési technikai ismeretek mellett például a behatolásvizsgálat (penetration testing – pentest) technikai hátterének kiterjedt és alapos ismeretét

jelenti. Az információs technológiákon belül egyfajta multidiszciplináris megközelítésre van szükség, tehát egy kiber különleges műveleti „beavatkozónak” vagy „operátornak” a technikai ismeretek minden szegmensében használható tudással kell rendelkeznie és legalább két területen kiemelkedő teljesítményt kell nyújtania. Ezen a ponton fontos kiemelni, illetve elválasztani a kiberműveleti „operátoroknak” azt a csoportját, amelyik egy harmadik fél által fejlesztett eszköz üzemeltetését felhasználóként, a felhasználói kézikönyv elolvasásával és az ügyfélszolgálat alkalmankénti bevonásával látja el (Sz.n., 2014), illetve azt a csoportot, amelyik képes a számára kijelölt rendszerben önállóan sérülékenységek felfedezésére és kihasználására az ehhez célzottan és egyedileg fejlesztett szoftver(ek) segítségével (lásd Stuxnet).

Anélkül, hogy a szükséges ismeretek tekintetében mélyebb technikai részletekbe bonyolódnánk, az egyik legfontosabb tényező a technikai oldalon az ismeretek naprakészen tartása. Ez egy elengedhetetlen folyamat, amit egyfelől a szervezetnek is erősen ösztönöznie kell, másfelől a kiber különleges műveleti szakemberek személyiségének alapértelmezett része kell legyen az önfejlesztés igénye. Optimális esetben a két irányból érkező motivációnak a szervezet megfelelő teret biztosít térben és időben egyaránt, vagyis a munkaidő egy jelentős részét – akár több, mint 40 százalékát – az ismeretek naprakészen tartása teszi ki, amihez biztosított a megfelelő technológiai környezet.

Az amerikai szárazföldi haderő kibertéri műveletei koncepciójának 2028-ig szóló képességi terve több olyan feladatot is meghatároz a kibertéri helyzetismeret (Situational Awareness) részeként, amelyek elvégzése technikai ismereteket igényel. A kibertámogató (Cyber Support – CyberSpt) tevékenység egyebek mellett magában foglalja a sérülékenységek felmérését (Vulnerability Assessment – VA), a fenyegetés alapú biztonsági elemzést (Threat-Based Security Assessment), a sérülékenységi és biztonsági kármentesítést (Vulnerability/Security Remediation), a rosszindulatú szoftverek visszafejtését (Reverse Engineering Malware), a helyszíni kiber szempontú kihasználhatóság feltérképezését (Cyber Aspects of Site Expoitation), az elhárítást (Counter Intelligence), valamint a kiber nyomrögzítést- és elemzést (Cyber Forensics). Az említett feladatok sorvezetőként szolgálhatnak a szükséges technikai ismeretekhez az adott művelet vagy misszió célkitűzéseinek és felépítésének függvényében. (US Army, 2010)

VI.4.2 Mentális, logikai és más készségek, képességek

Az interjúk során adott válaszok alapvetően két megközelítést rajzolnak ki a szükséges készségek és képességek terén, ami részben a technikai ismeretekre is hatással lehet, de főként a „lágy" vagy „puha" képességekre vonatkozik. Az egyik megközelítés szerint mindenképpen idealista beállítottságra van szükség és hazaszeretetre ahhoz, hogy valaki az összes előforduló feladatot hajlandó legyen elvégezni. Ebben a tekintetben a szervezeti háttér és kultúra is kulcsfontosságú, mivel a honvédelmi, rendvédelmi és nemzetbiztonsági szektorok eltérő jellemű embereket igényelnek. A több interjúalany által is alkalmazott másik megközelítés, ami nem zárja ki, sőt kombinálható az előzővel, két részre osztja az elvárt képességeket a feladatok alapján. Ebben a felosztásban az egyik csoportba az állománynak azok a tagjai tartoznak, akik egyértelmű támogató feladatokat végeznek, jellemzően a háttérországban, védett körülmények között, ami minimálisra csökkenti a lehetőségét annak, hogy közvetlen fizikai konfrontációba kerüljenek az ellenféllel. A másik csoportba tartoznak az állománynak azok a tagjai, akiket műveleti területen alkalmaznak például azonnali válaszadás során. Számukra fontos több olyan képesség és felkészültség megléte, amelyek a fizikai alkalmasság körébe sorolhatók.

Mindegyik felosztásban és csoportosításban előfordulnak azonban a következő tulajdonságok. Az alkalmazkodó (adapt) és befogadó képesség (adopt) jelentőségét az extrém helyzetek kialakulásának esélye, illetve a folyamatosan változó taktikák, technikák és procedúrák adják. A jó helyzetfelismerő és gyors döntési képességre azért van szükség, hogy a kiber különleges műveletek végrehajtói rendkívüli helyzetekben is képesek legyenek nyugodtak maradni és a lehetséges megoldási alternatívákat mérlegelve, a műveleti célkitűzés szempontjait figyelembe véve, optimális elhatározásra jutni a lehető legrövidebb időn belül. Fontos a lojalitás, a kitartás és a céltudatosság ahhoz, hogy a műveletek kudarca elkerülhető legyen. Az említett tulajdonságokkal nem rendelkező vagy ezen a téren gyengének ítélt jelentkező valószínűleg könnyebben zavarodna össze, vagy adná fel például egy konspirált művelet végrehajtása során jelentkező probléma esetén, ami negatív hatással lehet akár az egész képességre. A proaktivitás, illetve kezdeményezőkészség szerepe például olyan műveleti szituációkban válhat meghatározóvá, amikor a végrehajtás folyamata bármilyen okból elakad.

A fizikai térben tevékenykedő különleges műveleti katonák mellett egy másik, szemléletes párhuzam a magas fokú mentális és pszichikai felkészültség szükségességére, a drónpilóták esete.

A kibertér határokat nem ismerő, mindent átfogó jellegéből fakadóan könnyedén adódhat olyan szituáció, hogy akár több ezer kilométeres távolságból, egy védett helyiségből olyan folyamatok elindításában és lebonyolításában kell aktív szerepet játszania egy kiber különleges műveleti beavatkozónak, ami súlyos fizikai károkat okoz vagy akár emberi életek elvesztéséhez vezet. Ehhez hasonló kritikus helyzetekben kell helytállniuk azoknak a drónpilótáknak is, akik adott esetben eltérő kontinensről irányítják azokat a katonai megfigyelő és csapásmérő eszközöket, amikkel a kijelölt célpontok megsemmisíthetők.

Több interjúalany is kiemelte, hogy kizárólag csapatjátékost tud elképzelni a kiber különleges műveleti tevékenységek során, amihez fontos az együttműködési és kompromisszum képesség. Műveleti szempontból a képesség akkor lehet sikeres, ha a végrehajtó állomány olyan precíz, mindenre odafigyelő tagokból áll, akik képesek a műveletek minden aspektusát, annak teljes életciklusa alatt kontrollálni. Mivel rengeteg a részlet a műveletek során, a komplexitást tudni kell kezelni és itt kerül képbe a mindenre kiterjedő figyelem, az apróságokat is beleértve. Létezik példa arra, hogy ezeknek a képességeknek a szintje elérheti a kognitív zavar (pl. autizmus, savant-szindróma) határesetét, aminek hátterében komplex neurobiológiai betegség húzódhat, így valószínűleg egy ilyen személy az egyéb képességei és készségei miatt nem lehetne hivatalosan tagja a szervezetnek. Ehhez hasonlóan főként a rosszindulatú szoftverek visszafejtésén, illetve a célrendszerek sérülékenységeinek felfedezésén és az ezeket kihasználni képes eszközök fejlesztésén dolgozókkal összefüggésben lehet meghatározó jelentősége a megértéshez, illetve megoldáshoz való ragaszkodásnak. Hivatalos elnevezés valószínűleg nem létezik a tulajdonságra és a kettő nincs is teljes átfedésben, de vannak olyan személyiségek, amelyek nem képesek elereszteni egy problémát anélkül, hogy megértenék. Illetve ezzel szoros analógiát mutatnak azok a személyiségek, amelyek csak akkor tudnak elengedni egy problémát, ha megtalálják a működőképes megoldást az adott problémára. Az ilyen személyiségjegyekkel rendelkező jelöltek, ha a többi elvárásnak megfelelnek vagy könnyen felkészíthetők, rendkívül hasznos tagjai lehetnek a csapatnak.

VI.4.3 Fizikai alkalmasság

A fizikai alkalmasság kapcsán a legtöbben valószínűleg anélkül is a fizikai térben tevékenykedő különleges műveleti beavatkozók (Delta Forca, Navy Seals, SAS, Grom stb.) testfelépítésére, állóképességére és erejére gondolnának, ha egyébként nem a különleges műveleti analógiák adnák

az értekezés egyik pillérét, de a kiber SOF kapcsán a fizikai alkalmasság nem (csak) erről szól. A kiber különleges műveleti beavatkozók fizikai alkalmasságára jelen esetben egy olyan értelmezési keretet használunk, amiben azok a tulajdonságok kapnak helyet, amik a nem logikai dimenzióban játszanak fontos szerepet. Egy egyszerű példával szemléltetve, a kiberműveletek során az egyik legalapvetőbb elvárás, hogy a művelet és a végrehajtók is észrevétlenek tudjanak maradni a célpont számítógépes hálózataiban. Ezt a logikai észrevétlenséget, fizikai értelemben vett észrevétlenség is ki kell egészítse, ha műveleti területen, mondjuk egy politikailag kényes zónában vagy konfliktus övezetben vetik be a kiber különleges műveleti erőket.

Ebben a megközelítésben tehát nem „kommandós" fizikai tulajdonságokkal rendelkező jelöltekre van szükség. A korábban említett támogató szerepkörben és műveleti területen tevékenykedő beavatkozók közül leginkább az utóbbiak esetében fontos az alapvető fizikai alkalmasság, míg előbbiek esetében azt lehet követelményként meghatározni, hogy a szükséges kiképzés és felkészítés után akár a helyszíni műveleti alkalmazás is lehetővé váljon. Ehhez olyan jelöltekre van szükség, akik erre fogékonyak és a személyiségük teret biztosít jelentősebb módosításokra.

A kiber különleges műveleti beavatkozó képes magát megvédeni. Ez nem azt jelenti, hogy a harcművészetek mestere kell legyen, de olyan közelharc technikákat el kell tudjon sajátítani és képes kell legyen alkalmazni, amik a honvédelmi, rendvédelmi és nemzetbiztonsági szektorok alapkiképzései során előfordulnak. Egy műveleti helyszínen lelepleződés esetén előfordulhat, hogy feltartóztatják. Ilyenkor az önvédelmi ismereteknél is hasznosabb lehet a magas intelligencia, empátia, a hely- és nyelvismeret, illetve bármely tulajdonság, amivel a beavatkozó képes „kimagyarázni" magát az adott helyzetből. Ez lényegében a pszichológiai manipulációs (social engineering) képességeket, illetve eljárásokat és módszereket fedi, amikre akkor is szükség lehet, ha valahonnan nem kijutni, hanem pont fordítva, bejutni kell.[127]

Műveleti területen a fizikai állóképesség olyan mértékben feltétlenül fontos követelmény, hogy a rövid időn belüli nagy távolságok megtétele és az, hogy néhány nap leforgása alatt sarkvidéki vagy sivatagi körülmények is előfordulhatnak, ne okozzon problémát a beavatkozó számára. Tehát a nagy távolságok megtétele ezúttal sem a „kommandósokra" jellemző fél mázsánál is nehezebb

[127] A témában való ismeretek bővítésére kiválóan alkalmas Kevin D. Mitnick, a világ egyik legendás hackerének és Steve Wozniak (Woz), az Apple egyik alapítójának „A megtévesztés művészete" címmel megjelent könyve, amely számos valódi esetet dolgoz fel szórakoztató formában.

felszereléssel történő erőltetett menetet jelenti, sokkal inkább a kiberműveletek helyszíni végrehajtásából adódó – nagy távolságokkal összefüggő – fizikai körülményekkel szembeni felkészültséget. A hagyományos különleges műveleti erők tagjaival szemben gyakori elvárás, hogy képesek legyenek különböző kategóriájú járművek vezetésére, hogy a kijuttatásra, illetve kiemelésre használt járművek használhatatlanná válása esetén ne okozzon problémát, ha valaki életében először vezet bal/jobb kormányos vagy 3,5 tonnánál nehezebb járművet. A kiberműveletek egyik jellemző közege a városi környezet, ahol a különféle jogosítványokkal szemben előnyt jelenthet a közösségi közlekedési- és a mikromobilitási eszközök alapos ismerete és használata névtelen, illetve nem követhető módon.

Műveleti területen alkalmazott beavatkozónak jól kell tudnia mozogni és tevékenykedni ellenséges területen is, amihez elengedhetetlen az idegen környezetben való gyors asszimilációs képesség. Ehhez fontos, hogy ne legyen feltűnő jelenség, csendes, de hatékony munkaerőre van szükség, a „kirakat”[128] emberek helyett. Ismernie kell a műveleti környezetet és azt is tudnia kell, hogy az adott közegben milyen eszközökre lesz szüksége. Mivel a logikai eszközök alkalmazása esetenként hálózatmentes körülmények között történhet, az ezek tárolásához és a művelet végrehajtásához szükséges egyéb fizikai eszközöket magával kell vinnie, illetve gondoskodni kell a feltűnésmentes, de biztonságos szállításról. A fizikai követelmények valószínűleg a legkönnyebben fejleszthető képességek, ugyanakkor ezek között is található olyan, ami tehetséget, rátermettséget igényel.

VI.4.4 Az interoperabilitás keretrendszere

Az interjúkból egyfelől az derült ki, hogy a megvalósítás függvényében a különböző szektorok és szakterületek közötti együttműködés szintje várhatóan alacsony marad a szervezeti kultúrák közötti eltérések, a versengés és egyéb faktorok okán. Másfelől felmerültek olyan képességek és ismeretek, amelyek az interoperabilitás magas fokának eléréséhez szükségesek.

Ide sorolhatók az általános biztonságpolitikai, geopolitikai és gazdasági ismeretek, amikre azért van szükség, hogy a kiber különleges műveletek végrehajtói értsék a tevékenységük mögött meghúzódó célkitűzéseket és stratégiai előrelátással rendelkezzenek. Mindez segítheti egy

[128] “Kirakat tevékenység” alatt azok a szerepvállalások értendők, amikor egy szervezet messze a hatáskörén kívül levő feladatban vesz részt a politika vagy a média figyelmének felkeltése, a létjogosultság igazolása, illetve más nem szakmai okokból. Ilyenre példa, ha egy eredetileg természeti és ipari katasztrófák elhárítására létrehozott szervezet terrorelhárítási tevékenységet végez, vagy fordítva.

potenciális támadás felismerését, azonosítását és kivédését, miközben az offenzív műveleti tervezés során hozzájárulhat a célpontok azonosításához, kiválasztásához, illetve az alkalmazott eszközök és módszerek kijelöléséhez. A műveleti tervezésen és előkészületeken felül a végrehajtás során lehet jelentősége a nem hagyományos hadviselési ismereteknek, amibe bele tartoznak a gerilla hadviselés írott és íratlan szabályai is. Ha az előző két alfejezetben tárgyalt személyi kvalitásokat összevetjük például Marighella[129] városi gerillákról megfogalmazott alapvetéseivel, ismét analógiákra bukkanunk. „A városi gerilla kézikönyvé"-ben az áll, hogy a gerillának rendelkeznie kell kezdeményezőkészséggel, mozgékonysággal és rugalmassággal, valamint fontos a sokoldalúság, hogy minden helyzetre felkészült legyen. A városi gerillának tudnia kell, hogyan vegyülhet el a városi környezetben úgy, hogy ne tűnjön idegennek, jó megfigyelőnek és jól informáltnak kell lennie, továbbá a lehető legtöbb tudással kell rendelkezzen a műveleti területről és az ellenség képességeiről. A technikai felkészültségre vonatkozó részek is számos párhuzamot tartalmaznak, míg a csapásmérés kapcsán azt írja: akkor sikeres, ha egy kis csoport akciója révén szerveződik, ha gondosan, titokban és a legtitkosabb módszerekkel készül. (Marighella, 1969)

Jól hasznosítható tudást jelent, ha valakinek vannak kriminalisztikai ismeretei. Ez elsősorban olyan műveletekben válik hasznosság, ahol a feladatnak része a támadó kilétének meghatározása, vagy a támadás nyomainak szakszerű elfedése. Ha valaki tisztában van azzal, hogy a célpont milyen nyomrögzítő és nyomelemző módszereket alkalmaz, illetve azok mire képesek, akkor az azonosítás elkerülése már a támadó művelet tervezése során figyelmet kaphat és beépülhet minden támadási fázisba. A kriminalisztika kapcsán felmerülnek az analitikai képességek és a rendszerszemlélet, ami segíti a művelet végrehajtása közben eldönteni, hogy mi számít és mi nem, illetve egy adott információ más szervek által történő felhasználhatóságát.

VI.4.5 Humán kihívások

Az VI.4 fejezet bevezető gondolataiban említett kiberbiztonsági szakemberhiányon kívül más humán kihívásokat is azonosítottam az interjúk segítségével.

[129] Carlos Marighella (1911-1969) brazil politikus, író, gerillaharcos. A marxista-leninista szemléletű Marighella 1934-ben lépett be a Brazil Kommunista Pártba, majd terrorizmusnak titulált akciókban vett részt, többször letartóztatták. Írói munkássága eredményeként 1969-ben jelent meg a városi gerilla hadviselésről szóló kézikönyve, amiben sok a mai napig érvényes gondolatot fogalmazott meg.

Az egyik ilyen, több válaszadó által is említett kihívás az oktatás. Ez egyfelől abból adódik, hogy jelenleg nincsen olyan képzés vagy szervezet, amely egy ilyen speciális felkészítést meg tudna valósítani. Hiányoznak a képzési keretek. Szétforgácsoltan kisebb elemek adott esetben megtalálhatók piaci szolgáltatóknál, illetve a rendvédelmi, honvédelmi és nemzetbiztonsági szerveknél, de általánosságban elmondható, hogy nincs megfelelő iskola. Az oktatás problémáját egy jóval átfogóbb megközelítéssel szemlélve az derül ki, hogy komoly szinkronizációs hiány mutatkozik, ami középiskolai és felsőoktatási szinten is elavult tananyagot és diszfunkcionális képzést eredményez az informatikai oktatás terén és ez begyűrűzik a kiberbiztonságba is. Egy átfogó reform keretében lehetne áttérni erősen típusos modern programozási nyelvek tanítására, ami a technológia közeli oktatást elmozdíthatná a biztonságosabb szoftverek készítésének irányába.

Jól látszik, hogy a kiber különleges műveleti specialisták kiválogatásához meglehetősen sok szempontot érvényesítő, magas követelmények társulnak, ezért nehéz a megfelelés. Ideális jelölt tulajdonképpen nincs, vagy olyan elenyésző a létszámuk, hogy abból nem lehetséges bevethető képességet kialakítani. Ismét utalva a támogató kiberműveleti állományra, esetükben valamivel könnyebb lehet a helyzet a követelményrendszer kialakítása kapcsán, ennek ellenére érdemes lehet inkább a jó alapszemélyiséggel rendelkező jelentkezőkre építeni és az utólagos kiképzésre bízni a szükséges képességek és ismeretek megszerzését. A műveleti területen alkalmazható specialistáknál az elvárások miatt szinte biztos, hogy nincs más lehetőség, mint erős alaptudással és a feladatok sikeres végrehajtásához illeszkedő személyiséggel rendelkező jelöltekre építeni. Mindkét esetben szükséges a hosszútávú gondolkodás, mert egy ilyen speciális kiberműveleti képesség bevetésre alkalmas felépítése évekig tartó folyamat, amit azután fenn is kell tartani.

VI.5 A kiber különleges műveleti felkészítésről és kiképzésről

Bármelyik honvédelmi, rendvédelmi vagy nemzetbiztonsági képességről legyen szó, humán erőforrás nélkül egyik sem működtethető eredményesen. A harckocsihoz és vadászrepülőgépekhez kezelő személyzetre van szükség, a robbanószerek hatástalanítását emberek végzik, de a tűzszerész robotokat is ember irányítja, továbbá a jelfelderítő tevékenység során gyűjtött információk elemzéséhez és értékeléséhez is szükség van az emberre. Igaz, hogy minden téren egyre nagyobb szerep jut az automatizációnak, ami hangsúlyeltolódást okoz a humán szerepvállalásban, de

minden csúcstechnológia függ az embertől. Nincs ez másként a kibertérben és kiberbiztonság terén sem, amit a szektort sújtó szakemberhiány is alátámaszt.

Az elkészített interjúkból már az előző alfejezetben kirajzolódott, hogy a kiber különleges műveleti képességek egyik legjelentősebb kihívása a megfelelő humán erőforrás megteremtése. A kihívás három alapvető indikátora az iparági szakemberhiány, a speciális követelmények és magas elvárások, valamint a terület általános oktatási és képzési hiányosságai. Ezek együttes hatása, hogy a legtöbb ország esetében valószínűleg olyan radikálisan lecsökkenne az ideális jelöltek száma, hogy jobban megéri a megfelelő személyiséget keresni és célzott kiképzést folytatni. Ehhez azonban átfogó megközelítésre és komplex képzési struktúra kialakítására van szükség.

VI.5.1 Értékelő központok

Ma már a legtöbb munkaadó alkalmaz a leendő munkavállalók személyiségének és alkalmasságának meghatározását lehetővé tevő értékelő központokat (assessment center). A központok legnagyobb szerepe az egyén viselkedési mintáinak feltérképezése különböző módszerek és eljárások segítségével, amik között interjúk, szimulációk, egyéni és csoportos gyakorlatok, felmérések és pszichológiai tesztek is megtalálhatók. A cél, hogy szabványosított módon lehessen egy személy képességeit és teljesítményét megállapítani bármilyen feladat során. Azoknál a szervezeteknél, ahol elterjedt az érétkelő központok alkalmazása, jellemzően az új jelentkezőket és friss munkavállalókat, valamint a vezetői beosztásba készülő munkatársakat mérik fel. A központokban készített multidimenzionális felmérések elősegítik az egyének személyiségének átfogó megismerését, így egyszerűbben eldönthető, hogy ki milyen területre alkalmas. (Ballantyne és Povah, 2004)

Az ilyen értékelő központoknak egy speciális változataként foghatók fel azok a katonai különleges műveleti és vezetői felkészítő, illetve felmérő programok, amik messze földön híresek keménységükről és a kihulló jelentkezők magas számáról. Ilyet működtet például a brit haderő Sandhurst Királyi Katonai Akadémia a tisztképzéssel összefüggésben, az Egyesült Államok haditengerészete a különleges műveleti állomány (SEAL) felmérése és kiválasztása kapcsán, illetve a Magyar Honvédség „Pitbull” néven ismertté vált megmérettetése is azt a célt szolgálja, hogy a legmegfelelőbb jelölteket megtalálják és kiszűrjék az alkalmatlanokat. Ezek a programok jellemzően az extrém fizikai megterhelésről lehetnek ismerősek az átlagember számára, azonban

minden esetben hangsúlyos a pszichológiai felmérés. Vizsgálják az egyéni és csapatmunka során nyújtott mentális teljesítményt, a szakmai ismeretek alkalmazásával kapcsolatos készségeket, a szélsőséges helyzetekben (pl.: alvásmegvonás) nyújtott hatékonyságot, a monotonitás-tűrést és sok más indikátort. A haderők megközelítésében ez egyfajta kompromisszum (trade-off), így próbálják garantálni, hogy a kiválasztottak rászolgálnak a beléjük fektetett erőforrásokra. (T.L. főhadnagy, 2020). Volt olyan interjúalany, aki szerint a kiber különleges műveleti specialistáknál és beavatkozóknál is ugyanolyan kiemelt jelentőséget kell tulajdonítani a pszichikai alkalmasságnak, mint a kinetikus különleges műveleti szolgálatok esetében, ami így akár a hetven százalékot is elérheti a többi tényezőhöz képest.

A kiber különleges műveleti képességek kialakításának egyik pillére az értékelő központ, ami alkalmas arra, hogy a jelentkezők személyiségét és teljesítményét minden, a kiberműveletek szempontjából fontos dimenzióban felmérje. Ehhez speciális szabvány- és értékelőrendszerre van szükség, aminek bizonyos elemei a már létező honvédelmi, rendvédelmi és nemzetbiztonsági értékelő programokból – akár módosítva – átvehetők. Ugyanakkor elsősorban a kiber különleges műveleti képességekhez kapcsolódó technikai és fizikai elvárásokat jelentős részben újonnan kell kialakítani és harmonizálni a képesség létrehozásakor megfogalmazott célkitűzésekkel és az előzetesen elvégzett átfogó munkakör elemzéssel.

Az erőnléttel és kondícióval összefüggő tulajdonságokat nem érdemes magasan priorizálni, ugyanakkor a technikai ismeretek és a mentális rátermettség a két legfontosabb indikátor az alkalmasság értékelésekor. Nehéz arányokat kialakítani, de minden szempontot és követelményt el kell tudni helyezni a struktúrában. Ehhez fontos annak megértése, hogy hiába létezik egy ideális koncepció vagy stratégia, ha az nem megvalósítható. Ezért arra kell törekedni, hogy ne az ideális, hanem megvalósítható stratégiát készítsük el. Nagy a valószínűsége, hogy főleg a kezdetekben szignifikáns eltérések lesznek az alkalmasnak talált jelöltek személyisége és ismeretei tekintetében, emiatt speciális programokra van szükség, ami tehetséggondozás jelleggel egyénre szabott útvonalak mentén képes elérni a megfelelő szintet.

VI.5.2 Az oktatás és kiképzés infrastrukturális kérdései

Mivel a kiber különleges műveleti képességet adó állomány jelentős időt tölt el képzéssel és felkészítéssel, átlagon felüli kapacitásokra van szükség a képzési infrastruktúra tekintetében. A

mennyiségi kapacitásokkal szemben azonban jóval fontosabb a feltörekvő technológiák rutin szerű használata a képzésben, a gyakorlat alapú tanulás (learning by doing) kiterjedt alkalmazása, a honvédelmi és rendvédelmi jellegű gyakorlatok rendszeres tartása, amihez könnyen variálható valósághű szimulációs környezetre van szükség a virtuális és fizikai térben egyaránt, továbbá az ismeretek ellenőrzéséhez a speciális labor körülmények kialakítása is fontos elem.

Szakmai szinten, ha a kiberbiztonsági képzés infrastruktúrája kerül szóba, akkor jellemzően néhány elterjedt megoldásra korlátozódik a párbeszéd. Az egyik ilyen irány a tanuláskezelő rendszerek (Learning Management System – LMS), amik régóta jelen vannak az online, illetve virtuális oktatási piacon és meglehetősen széles spektrumot fednek le az oktatott témakörök és a tudás átadásának módja terén egyaránt. A hagyományosnak mondható rendszerek elterjedtnek számítanak a felsőoktatási és nagyvállalati szegmensben is. Jellemzően hagyományos tananyagok, tehát tankönyvek, jegyzetek és prezentációk érhetők el rajtuk keresztül, amelyek feldolgozását optimális esetben képes követni a rendszer, illetve a megszerzett tudás ellenőrzése is megvalósítható ezekben. Modernebb változataik képesek multimédiás tartalmak kezelésére, illetve interaktív megoldások mellett, játékelemeket (gamification), cselekvés általi tanulást vagy akár virtualizációt és kiterjesztett valóságot is alkalmaznak. Ezeket szinte minden terület használja, a kiberbiztonsággal összefüggésben főleg az alapismeretek, illetve a felhasználói tudatosság növelésére alkalmazzák.

A másik irány a kifejezetten kiberbiztonsági területen mély szakmai ismeretekkel rendelkezők képzését és gyakorlatszerzését szolgáló kiberlőterek (cyber range). Az elnevezés nem véletlen. Míg a fizikai világban a lőterek azok a területek, ahol a legkülönbözőbb fegyvereket biztonságos körülmények között lehet tesztelni és alkalmazásukat gyakorolni, a virtuális lőterek ugyanezt a célt szolgálják a kibertérben. Leegyszerűsítve a kiberlőtér sem több, mint hardver és szoftver, mivel optimális esetben van egy fizikai infrastruktúra, amin jellemzően a virtualizáció jelentette előnyök révén bármilyen szoftverkörnyezet viszonylag egyszerűen szimulálható szerverekkel, hálózatokkal és kliensekkel. Ilyen megoldások fejlesztésével ma már számtalan magánvállalat és állami szerv is foglalkozik, előbbiek jellemzően eladásra, illetve szolgáltatásként kínálják, míg utóbbiak a saját képességek fejlesztésére és tesztelésére használják. Ugyanakkor léteznek nemzetközi támogatást élvező projektek is, amik közül nem egy nyíltan, bárki számára hozzáférhető.

Ilyen nyílt forráskódú megoldás a majd 10 éve fejlesztett cseh KYPO[130], amely úttörő és sokoldalú megoldásnak számít ezen a területen. Ha egy állam saját kiberlőtér vagy -tesztkörnyezet kialakításában gondolkodik, nem feltétlenül kell a semmiből elkezdeni az építkezést. Elég körbe nézni és a jó gyakorlatokat adoptálni ahhoz, hogy flexibilis, skálázható, izolált, interoperábilis, költséghatékony, könnyen hozzáférhető és beépített felügyelettel rendelkező megoldást találjunk a kibertérrel összefüggő kutatás-fejlesztés, a digitális nyomrögzítés és nyomelemzés, valamint a kibertérhez kapcsolódó oktatás és képzés terén. (Vykopal és mtsai., 2017)

Bár a KYPO mellett több megoldás is létezik, amelyek hatékonyan alkalmazhatók lehetnek a kiber különleges műveleti erők tagjainak képzésére, ez a témakör önmagában is nagyszámú kutatási lehetőséget hordoz. A kiber különleges műveleti erők állományának felkészítéséhez kapcsolódó infrastruktúrának 4 pillére van. Az első pillérbe tartoznak azok a módszerek, eljárások és megoldások, amelyek főként az állomány általános és szakmai ismereteinek fejlesztését segítik elő a fizikai és/vagy a virtuális térben. Ezek jellemzően kiscsoportos vagy akár egyéni keretek között megvalósuló felkészítések, amik az elmélet elsajátítását a kognitív tudományok legújabb eredményei alapján valósítják meg és ezzel elősegítik a nagy mennyiségű és szerteágazó tudás megszerzését. A második pillérbe tartoznak azok a módszerek, eljárások és megoldások, amelyek leginkább az állomány technikai ismereteinek fejlesztését szolgálják, jellemzően a virtuális térben. Ezek az egyéni szinttől akár a teljes állomány közös felkészítésére is alkalmasak és amellett, hogy csúcstechnológiás megoldásokat is magukban foglalnak, a cselekvés alapú tanulásra fektetik a hangsúlyt. A harmadik pillérbe tartoznak azok a módszerek, eljárások és megoldások, amelyek alapvetően az állomány fizikai készségeit és képességeit fejlesztik. A nagyrészt fizikai térben megvalósuló felkészítések a honvédelmi, rendvédelmi és nemzetbiztonsági alapkiképzések speciális kombinációján alapulnak, de a fókuszban a fizikai- és kibertér határainak elmosódásából fakadó előnyök és hátrányok ismerete, illetve ezek kihasználása áll. A negyedik pillérbe tartoznak azok a módszerek, eljárások és megoldások, amelyek egyfelől az állomány gyakorlati tapasztalatainak beépülését és hasznosulását, valamint a másik három pillér elemeinek folyamatos fejlesztését segítik elő. Továbbá a negyedik pillér minőségbiztosítási szerepet is betölt, illetve a

[130] A KYPO eredetileg a kibernetikai próbatér vagy terület elnevezésből fakad és egy 2009-ben a Masaryk Egyetem számítógépes incidens reagáló csapatának kialakítását célzó projektből indult. A több fázisú KYPO kutatási projekt 2014-ben egy eredetileg helikopter szimulátor befogadására kialakított épületben helyezték el, ahol mára egy nyílt forrású kiberlőtér működik.

teljes oktatási és képzési infrastruktúra fejlesztési és bővítési irányainak meghatározásában is részt vesz.

7. ábra: A kiber különleges műveleti erők felkészítésének négy pillére: az általános és speciális szakmai ismeretek, az offenzív és defenzív technikai ismeretek, a fizikai készségek és operatív képességek, valamint a gyakorlati tapasztalatok feldolgozása és beépítése. (A szerző saját szerkesztése.)

VI.5.3 Felkészítéssel szembeni elvárások

A kiber különleges műveleti felkészítéssel szembeni elvárások nagyon magasak. Mivel az ideális jelölt nem létezik, vagy csak nagyon kis számban, ezért a képesség kialakítása olyan jelöltekkel valósítható meg, akik akár több területen is arra szorulnak, hogy meglévő képességeiket és készségeiket kiegészítsék. Bár az ehhez megfelelő személyiség megléte elkönyvelhető a siker feleként, a teljes siker elérése csak a legmagasabb normákat és szabványokat teljesíteni képes felkészítési rendszerrel valósítható meg.

A különleges műveletek jellegéből fakadóan a végrehajtó állomány szakértelme és a végzett tevékenység egyes elemei megfeleltethetők a kiberbiztonsági és kibervédelmi szektor „lila csapatainak” (Purple Team). Ezek a csapatok nem feltétlenül különálló szervezeti egységek, sokkal inkább koncepció formájában jelennek meg a fejlett és érett kiberbiztonsággal és -védelemmel rendelkező entitásoknál. A koncepció a különféle információbiztonsági képességek kollaborációján alapul és egy olyan folyamatként lehet rá tekinteni, amely során több csapat és szakember dolgozik együtt a védelmi komponensek (ember, folyamatok és technológia)

tesztelésén, felmérésén és javításán az ellenfelek taktikáinak, technikáinak, procedúráinak (TTPs) és viselkedésének emulálásával. A koncepció alkalmazása operatív szinten a kiberhírszerzés (CTI), az ellenfelet emuláló vörös csapatok (Red Team) és a védelmet ellátó kék csapatok (Blue Team) kollaborációját jelenti. (Buggenhout és Bauters 2022)

A kiber különleges műveleti erők tagjainak felkészítése során központi szerepe van a fejlett és magas színvonalú emulációs eljárásoknak, amelyek esetén a hangsúly a külső (támadó) fél viselkedésének minél pontosabb megközelítésén van. Kiberbiztonsági területen az emuláció lényege, hogy a saját számítógépes környezetben utánozhatók legyenek a különböző ellenfelek által alkalmazott taktikák, technikák és procedúrák. A fejlett ellenfél emuláció (Advanced Adversary Emulation – ADV2E) kimondottan az APT jellegű és a cyber kill chain fázisait alkalmazó ellenfelek viselkedésére fókuszáló eljárás. Az ADV2E alkalmazásának alapvető feltétele a robosztus CTI képesség, ami nem csak kutatja, de továbbítja, illetve megosztja az APT-khez köthető, folyamatosan változó TTP-ket és viselkedési mintákat. Az eljárással főként defenzív, kisebb mértékben offenzív tevékenység egyaránt fejleszthető.

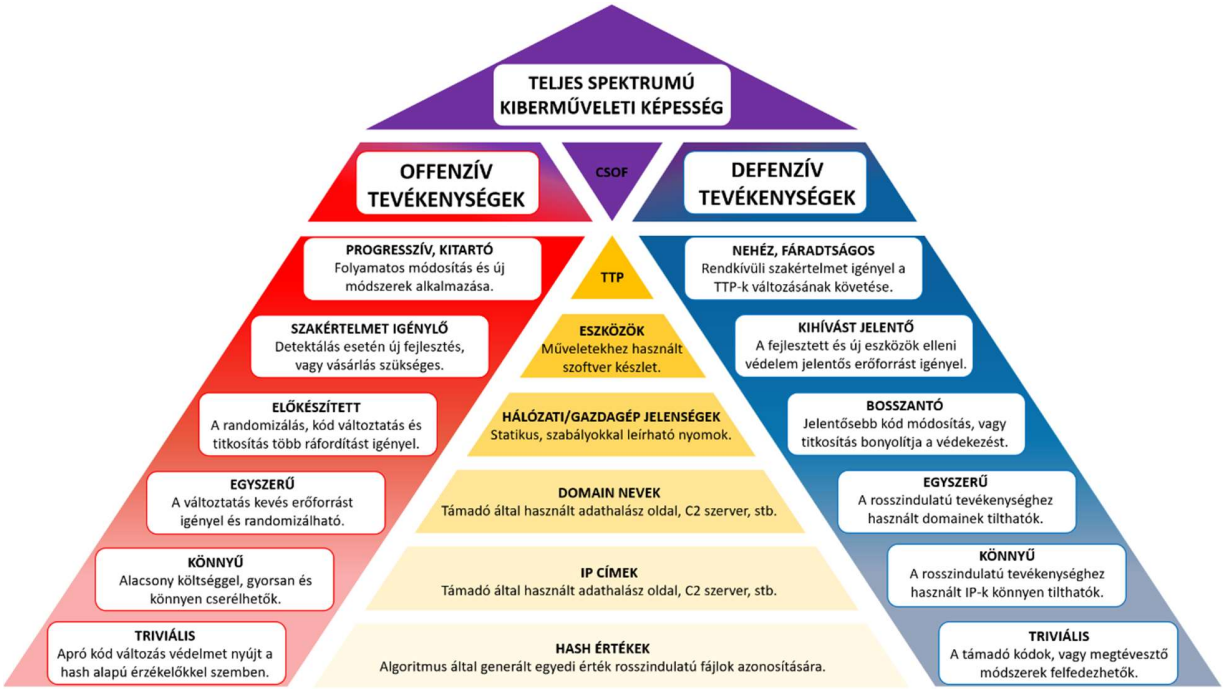
A kiber különleges műveleti állomány felkészítésének másik központi eleme a korszerű és realisztikus szimulációs eljárások, amelyek esetén a hangsúly a külső (megtámadott) fél infrastruktúrájának minél pontosabb imitációján van. Kiberbiztonsági területen a szimuláció lényege a sajáttól eltérő számítógépes környezet olyan módon történő másolása és utánzása, hogy az eredetit minél jobban megközelítse. A fejlett ellenfél szimuláció (Advanced Adversary Simulation – ADV2S) kimondottan az APT jellegű és a cyber kill chain fázisait alkalmazó ellenfelek infrastruktúrájára fókuszáló eljárás. Az ADV2S alkalmazásának szintén alapvető feltétele a robusztus CTI képesség, ami a TTP-ken túlmenően modellezhetővé teszi az ellenfél által alkalmazott infrastruktúra hardver és szoftver komponenseit. Az eljárással elsősorban az offenzív tevékenység, illetve a hírszerző és destruktív képességek fejleszthetők.

A hírszerzés többnyire tanulási képességet, illetve a tudás és készség megszerzésének folyamatát jelenti, amibe bele tartozik a tudás szakszerű használata, a megértés mozzanatai vagy a mentális fölény. Utalhat információk megszerzésére és egy adott szervezetre is, ami információ megszerzésével foglalkozik. A CTI különböző technikák alkalmazása azzal a szándékkal, hogy a védelmi felelősség körében egy kiberbiztonsági hatást kiváltó esemény nemkívánatos kimenetelét megelőzzük. Ilyen lehet a kognitív technikák alkalmazása a bizonytalanság csökkentésére, az

erőforrások hatékonyabb felhasználását segítő előrejelzés és a károk hatékonyabb enyhítése és csökkentése érdekében a káros szereplők tevékenységébe való betekintés, illetve ismeretszerzés. (FIRST, é. n.) Az ADV2E és ADV2S eljárások tekintetében jól látszik, hogy már a felkészítés során is nélkülözhetetlenek azok az ismeretek és a taktikai, illetve technikai mélységű betekintés, ami leginkább kiforrott és beágyazott CTI tevékenységgel biztosítható.

A CTI tevékenység, illetve általában véve a kiberbiztonsági incidensekkel összefüggő adatok és információk megszerzése szerteágazó és összetett folyamat. A különböző adatokat és információkat a IV.1.6 fejezetben ismertetett szisztéma alapján indikátoroknak nevezik és kategóriákba sorolhatók a komplexitásuk, valamint a megszerzés nehézsége alapján. Az elemi, számított és viselkedési indikátorok mennyisége, a megszerzés nehézsége és a kapcsolódó költségek fordított arányban vannak. Az elemi indikátorokat jellemzően alacsony költséggel, nagy mennyiségben állítja elő a támadó oldal. A védekező oldal pedig többnyire képes szignifikáns mennyiségű elemi indikátor költséghatékony feldolgozására. Azonban egy képzeletbeli skálára helyezve az indikátorok különböző kategóriáit, a viselkedési indikátorok száma csökken az elemi indikátorokhoz képest, miközben egyre jelentősebbek az azonosítási és feldolgozási költségek és a komplexitással együtt nő a speciális szakértelem igénye is.

Az indikátorokkal összefüggő jelenségeket a kiberbiztonsági kutatók a Maslow-szükséglethierarchia piramis ábrázolását alapul véve a defenzív oldal szemszögéből, a „fájdalom piramisaként” (Pyramid of Pain) jelenítik meg. (Bianco, 2014) Az eredeti ábrázolás offenzív aspektusokkal történő kiegészítésével létrehozható egy olyan modell, ami lehetővé teszi a kiberműveleti képességek teljes spektrumának indikátor alapú ábrázolását.



8. ábra: A teljes spektrumú kiberműveleti képességek és a kiber különleges műveleti erők modelljének sematikus ábrázolása az offenzív és defenzív tevékenységek indikátor központú skálázódása alapján. (A szerző saját szerkesztése.)

A modell alkalmas a kiberműveleti képességek erőforrás szükségletének indikátor kategóriákhoz kapcsolt ábrázolására és a kiber különleges műveleti képesség elhelyezésére a teljes kiberműveleti spektrumon. Mindez a kiber különleges műveleti felkészítés és a képesség tervezése tekintetében olyan kiindulási pontként szolgálhat, ami egyszerűsíti az egymásra épülő részképességek strukturálását és a kapcsolódó erőforrások hozzárendelését.

Előfordulhat – főként a képesség kialakításának korai fázisaiban – olyan eset, hogy nem áll rendelkezésre megfelelő szaktudás és csak harmadik fél képes biztosítani a megfelelő szintű felkészítést. Amennyiben a képesség kialakítása nem fedett módon történik, illetve vannak nyílt komponensei, akkor harmadik fél bevonása a felkészítésbe egyszerűbb. Az átvilágításon és egyéb biztonsági követelményeknek megfelelő harmadik fél csak a szükséges mértékig, kellő körültekintéssel vontható be a felkészítésbe. Komplikáltabb a külső felkészítés, illetve felkészítő bevonása abban az esetben, ha a képesség fedett módon valósul meg. Azonban legitim fedőszervezetek hálózatának és a szükséges körülmények kialakításával a feltételek kialakíthatók. Ebben az esetben törekedni kell arra, hogy a kezdeti felkészítéshez szükséges szakismeret (know-

how) minél előbb rendelkezésre álljon házon belül és a kiber különleges műveleti felkészítés igényeinek megfelelően skálázható legyen.

A felkészítéssel kapcsolatban már szóba került az egyéni és csapat szintű gyakorlati tapasztalatok hasznosíthatósága. Ezen a téren a kiber különleges műveleti képességek kialakításakor mintaként szolgálhat a kinetikus különleges műveleti erőknél alkalmazott megoldás, ugyanakkor a legfontosabb kérdés, hogy a kiberes szakismeretek és a különleges műveleti szakismeretek között hol húzzuk meg a határt. A kinetikus erőknél a kiképzők szinte kizárólag olyan korábbi operátori és beavatkozó szerepkörben tevékenykedő csapattagok, akik valamilyen okból már nem alkalmasak a műveleti területen történő bevetésre. Az általuk birtokolt tudás és tapasztalat azonban rendkívül hasznos a különleges műveleti erők számára, ezért az ismeretek átadásának jelentős szerepe van. A taktikák, technikák és procedúrák dinamikus változása miatt főleg hosszabb időtávon a gyakorlati ismeretek hasznosítása kapcsán felmerülhet az elavultság. Azonban a támadó oldalon erős a tudástranszfer jelensége és kedvelt módszer az újrahasznosítás, ezért a kiber különleges műveleti felkészítésnek is integráns része kell legyen a gyakorlati úton szerzett tudás és tapasztalat megosztása, amit a rövid- és középtávú fenyegetettségi környezethez szükséges igazítani.

VI.6 A kiberképességek és elrettentés teljes spektruma

A pusztán katonai megközelítés értelmezéséhez jó kiindulási alapot nyújt Gregory Rattray és Jason Healey „Az offenzív kiberképességek és alkalmazásuk megértése és kategorizálása” (NRC, 2010) című tanulmánya, ami a katonai doktrínákat alapul véve hat különböző tradicionális kategóriába sorolja a kiberműveleteket. Az első a kiberelhárítás (Counter Cyber), ami integrálja az offenzív és defenzív műveleteket a kiberfölény kívánt szintjének elérése és fenntartása érdekében. A kibertevékenységek megakadályozása (Cyber Interdiction) olyan akciókat takar, amelyek a baráti erők elleni hatékony felhasználása, illetve céljaik elérése előtt képesek az ellenség katonai kiberképességeinek eltérítésére, megzavarására, késleltetésére vagy megsemmisítésére. A harmadik kategória a kiber közeltámogatás (Close Cyber Support), ami a baráti erők közvetlen közelében található célpontok információs rendszerei elleni akció, illetve azok a kiberműveletek, amelyek szoros integrációt igényelnek a baráti erők csapásaival és mozgásával. Az erők kiberfelderítése (Cyber Reconnaissance in Force) a haderő (és nem a hírszerzés) által végrehajtott

offenzív kiberművelet, aminek a célja az ellenség erejének felderítése és/vagy tesztelése vagy egyéb információk megszerzése. Az ellenség kibervédelmének visszaszorítása (Suppression of Enemy Cyber Defenses) olyan tevékenység, amely pusztító és/vagy zavaró eszközökkel semlegesíti, megsemmisíti vagy ideiglenesen gyengíti az ellenséges kibervédelmet. A hatodik kategória a stratégiai kiber küldetés (Strategic Cyber Mission), amely egy vagy több kiválasztott ellenséges kibercélpont ellen irányul azzal a szándékkal, hogy fokozatosan megsemmisítse és szétzilálja az ellenség háborús kapacitását és akaratát.

Bár az említett kategóriák alapvetően háborús körülmények között használhatók, a kifejezetten katonai felhasználású kiberképességek kialakításának igazodnia kell a harc megvívásának elemeihez és a köré épített katonai struktúrákhoz. A kiberműveleti képességek teljes spektruma azonban további nem háborús műveleteket, illetve békeidőben végzett tevékenységeket is magában foglal. Ezeknek a végrehajtása adott esetben a haderőn kívüli szervezetek feladatkörébe tartozik, így előtérbe kerülnek a rendvédelmi és nemzetbiztonsági kiberképességek.

A kutatáshoz készített interjúkból az derült ki, hogy a válaszadók egy része szerint, bár kívánatos lenne egy integrált szervezetben létrehozni a kiber különleges műveleti képességeket, ennek megvalósulására nem sok esélyt látnak hazai viszonylatban, a többi kiber kapacitás pedig biztosan az adott szektorban van a legjobb helyen. Általános megközelítésben kiber különleges műveleti képességeket a válaszok alapján három szegmensre lehet osztani. A fejezet ezeknek a szegmenseknek a mentén fejti ki a kiber különleges képességek és elrettentés meghatározó elemeit a kiberműveletek teljes spektrumán belül.

VI.6.1 A nélkülözhetetlen CTI

A CTI tevékenység a válaszadók egybehangzó véleménye alapján egy olyan komponens, amire nem csak a különleges műveletekben, hanem a kiberműveletek teljes spektrumában szükség van. Alapjaiban határozza meg a tevékenység minőségét, hogy milyen információkkal rendelkezünk az ellenfelekről, illetve saját kitettségünkről. A kiber különleges műveletek területén ez kiterjed az ellenfél támadáshoz használt taktikáinak, technikáinak és eljárásainak (TTPk) alapos tanulmányozására és a fenyegetési környezet, valamint a kockázati szint folyamatos értékelésére. Ezt az indikátorok felkutatásán és elemzésén túl szerteágazó forrásokból történő információgyűjtés előzi meg, ami kiterjed az üzleti szférára és a darkweb-re is. A begyűjtött információk tükrében

érdemes a fizikai térre is kiterjeszteni az értékelést, mivel a kiberműveletek gyakran fizikai tevékenységgel járnak együtt. Egy konkrét példával szemléltetve, ha egy ipari folyamatirányító rendszer új verzióját készül piacra dobni a gyártója és a darkweb-en felélénkül az ilyen rendszerekkel összefüggő diskurzus, akkor érdemes ellenőrizni a saját kibervédelmi kitettséget. Ha vannak hiányosságok és sérülékenységek, azokkal foglalkozni kell és megszüntetni. Amennyiben egy esetleges támadással kapcsolatban konkrét információk is rendelkezésre állnak (ki, mit, mikorra tervez) és a kitettség nem szüntethető meg időben, akkor van létjogosultsága a megelőző, illetve ellentámadásnak. Bár elméleti síkon egyszerűnek tűnik, a gyakorlatban a CTI tevékenység nem tud minden esetben, minden kérdésre választ adni.

Hírszerzési és elhárítási megközelítésben a CTI elsődleges feladata a kiberműveletek felderítése és az észlelés elősegítése, mert csak arra tud reagálni a képesség többi komponense, amiről tudomásuk van. A CTI tevékenység a V.3.2 fejezetben említett hírszerzési erőforrások és módszerek mindegyikéhez hozzá kell férjen, illetve az elemző-értékelő képességre – különösen önálló szervezetként – kimondottan szükség van. Az elemző-értékelő tevékenység nyomán nyílik lehetőség arra, hogy szoros együttműködés alakuljon ki az érintett szervezetekkel és időben elkezdődjön a védekezés, elhárítás vagy épp támadás, de a politikai és stratégiai döntéshozatal különböző szintjeinek tájékoztatásához is szükséges.

A CTI szerepe megjelenik a kiber különleges műveletek támogatásában, a képességek kiépítésében, illetve a tervezés során egyaránt. Jelen esetben a tervezésnek több szintjén érdemes a CTI tevékenységet vizsgálni. Egyfelől már a kiber különleges műveleti képességek kezdeti tervezése során rendelkezésre kell állnia azoknak az információknak, amik a komponensek létjogosultságát alátámasztják. Ismét egy konkrét példa, hogy ha egy ország egyáltalán nem rendelkezik nukleáris létesítményekkel, akkor a tervezett kiberműveleti képességeknek nem feltétlenül kell a szektor rendszereinek kibervédelmére kiterjednie. Ha azonban az ország olyan képességet kíván létrehozni, amivel a nukleáris létesítmények működésébe be tud avatkozni erőkivetítés, befolyásolás vagy más szándékkal, akkor a környezeti értékelés és a képességgel kapcsolatos pontos irányok meghatározása a CTI tevékenység támogatásával valósul meg. Másfelől a kiber különleges műveletek tervezése – bármely kinetikus művelethez hasonlóan – folyamatos információs támogatást igényel. Ennek szerepe van a műveletet végrehajtó dedikált kapacitások és képességek meghatározásában, illetve a művelet teljes életciklusában.

A CTI technikai, taktikai, operatív és stratégiai szintekre terjed ki.[131] Ebben a megközelítésben a technikai a „bit" szinten folytatott tevékenységet jelenti és adott esetben átfedésben van olyan területekkel, mint a kártékony szoftverek visszafejtése, a hálózati események napló fájljaiban található összefüggések elemzése, illetve kiterjed az ellenfél infrastruktúrájának feltérképezésére vagy korábban használt megoldások technikai eltéréseinek meghatározására. A CTI taktikai szintjén folytatott tevékenységnek is része a kártékony szoftverek elemzése, azonban a kód visszafejtésére jellemzően itt nem kerül sor. A – gyakran automatizált – elemzés izolált környezetben futtatja a kártékony kódot és azt vizsgálja, hogy milyen feladatokat és hogyan hajt végre. Az elemzésekből, illetve más forrásokból megszerzett főleg elemi és számított indikátorokat különböző kibervédelmi szereplőkkel és megoldásokkal osztja meg a taktikai CTI. Az operatív szint fókuszában az ellenfél kapacitásai, infrastruktúrája és a viselkedési indikátorok (TTPk) állnak. Ezek megismerésével és megértésével az operatív szint képes priorizálni vagy magasabb szintű célzottságot elérni a kiberműveletek során. A CTI stratégiai szintje alapvetően a vezetők és döntéshozók tájékoztatását szolgálja azáltal, hogy kontextusba helyezi a kibertérben zajló eseményeket a trendek elemzésével és értékelésével vagy az ellenfelek motivációinak vizsgálatával.

VI.6.2 Az offenzív műveleti komponens

A III.1 alfejezetben áttekintett kiberbiztonsági stratégiákból az látszik, hogy a kiberműveletek teljes spektrumának egy jól meghatározható szegmensében folyamatos és nyílt képességfejlesztés folyik nemzeti és nemzetközi szinten egyaránt. Ezek azok a kiberműveleti képességek, amelyek nagyobb részben a passzív, kisebb részben az aktív kibervédelmi képességeket ölelik fel. A kiber különleges műveletek a kutatás megközelítése alapján azonban az aktív kibervédelmi, illetve offenzív kiberképességeket és a hozzájuk kapcsolódó kapacitásokat fedik le függetlenül attól, hogy a végső cél védelmi, hírszerzési, befolyásolási vagy destruktív.

Az offenzív műveleti komponens által végzett tevékenységek felosztásának egyik módja a direkt és indirekt csoportokba történő besorolás. Az indirekt tevékenységek a III.2.2 és a III.2.3 alfejezetekben tárgyalt aktív kibervédelmi és offenzív képességek átfedésében találhatók. A hatékony működéshez feltétlenül szükség van a támadás és adott esetben a támadó azonosítására.

[131] A leírás Kurt Baker "What is Cyber Threat Itelligence?" című írásának felhasználásval készült. Az írás és a CTI-ról bővebb információ érhető el: https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/

Ha ez megtörtént, akkor az indirekt tevékenységek közül az aktív kibervédelemhez sorolható az a korábban bemutatott példa, amikor a támadó infrastruktúrához köthető indikátorokat a saját rendszereken kívül is fekete listára (black list)[132] tetetjük, vagy gondoskodunk a domén nevek és IP címek eltávolításáról, illetve használaton kívül helyezéséről. Ilyen esetben a támadó féllel nem valósul meg „direkt találkozás", nem közvetlenül a támadó rendszerben történik beavatkozás, hanem harmadik félnél, jellemzően internet, tárhely vagy felhő[133] szolgáltatónál. A tevékenység motivációját és jellegét tekintve defenzív és aktív, a kivitelezéshez pedig hatékony támogató képességek szükségesek.

Az indirekt tevékenységek ennél fejlettebb változata, ami a védelem oldaláról továbbra sem jár direkt hozzáféréssel a támadó infrastruktúrához, azonban képes olyan eszköz alkalmazására, amivel a támadást gyengítheti vagy megszüntetheti. Szintén korábban már említett példa, amikor a védelem oldaláról képesek a támadást olyan szinten elemezni, hogy abban hibákat, illetve kihasználható elemeket találnak, amiken keresztül ellentevékenységet tudnak megvalósítani. Ilyenkor a defenzív tevékenység keretében például egy preparált fájlt helyeznek el az idő közben izolált, de a támadó számára továbbra is elérhető, megtámadott rendszerben. Ez lényegében a támadás, illetve a támadó megtévesztése. Amint a preparált fájl a támadó infrastruktúrát eléri, a korábban felfedezett kihasználható hibákon keresztül a támadás megzavarható vagy leállítható. Fájlok helyett hasonló indirekt tevékenység lehet olyan speciális rendszer vagy hálózati beállítások alkalmazása is, amik a támadás megzavarásához vagy leállásához vezetnek. A motivációt és a jelleget nehéz meghatározni, mert egy offenzív elemet is tartalmazó defenzív célú tevékenységről van szó. Az ilyen aktív kibervédelmi tevékenységekhez fejlett és érett kiberműveleti képességekre van szükség.

Az offenzív kiberműveletek direkt tevékenységei közé azok sorolhatók, amelyek közvetlenül érintik a célba vett rendszert. Amennyiben egy aktív támadással szemben folytatott ellentevékenység keretében valósul meg a direkt tevékenység, például a támadó infrastruktúra C2

[132] A számítástechnikában a fekete listákat, más néven blokk listákat egyszerű hozzáférés ellenőrzési mechanizmusként alkalmazzák. A listák tartalmazhatnak e-mail címeket, felhasználókat, jelszavakat, IP címeket, fájl hasheket stb. A mechanizmus lényege, hogy minden elem számára engedélyezett a hozzáférés, kivéve a listán explicit szereplő elemek.

[133] A felhő alapú számítástechnika a számítási szolgáltatások (kiszolgálók, tárolás, adatbázisok, hálózatkezelés, szoftverek, elemzés, intelligencia) elérhetővé tétele az interneten keresztül a gyorsabb innováció, a rugalmas erőforrások és a méretgazdaságosság érdekében. A felhasználó csak a felhasznált felhőszolgáltatásokért fizet, így csökkenthetők az üzemeltetési költségek.

szervereihez történő illetéktelen hozzáféréssel és a cél a támadás leállítása, a motiváció tekintetében továbbra is defenzív akcióról van szó, azonban a jelleg teljes mértékben offenzív lesz. Direkt tevékenységnek tekinthető az offenzív motivációval megvalósuló behatolás egy számítógépes rendszerbe. Abban az esetben, ha „A" ország állami támogatásával adathalász üzenetek érkeznek „B" ország kormányzati levelező rendszerébe, amiknek a megnyitásával „A" ország illetéktelen hozzáférést szerez „B" ország kormányzati rendszereihez, direkt tevékenységből fakadó behatolás történik. „A" ország egyértelműen offenzív műveletet folytat vélhetően hírszerzési, befolyásolási vagy destruktív indíttatásból.

Az offenzív műveletekkel kapcsolatban az átlagember főként magával a behatolás tényével, a megszerzett adat mennyiségével vagy az okozott kár nagyságával szembesül. Kevesebb szó esik azonban a IV.2.2 alfejezetben feldolgozott perzisztenciáról, ami a cyber kill chain egyik fázisa és a kifinomult kiberműveletek meghatározó eleme. Főként államilag támogatott műveletek során a rendszerbe történő bejutás, vagyis a kezdeti kompromittálás után a támadók rendszerint terjeszkedni kezdenek nem csak az eredetileg támadott rendszerben, hanem igyekeznek más rendszerekbe és alkalmazásokba is eljutni, hogy azokat is kompromittálhassák. A laterális mozgás (lateral movement) jelentősége abból adódik, hogy a támadó számára értékes rendszerek közvetlen támadása sokszor nehézkes vagy nem lehetséges. Ilyen esetben egy másik, könnyebben támadható rendszeren keresztül próbálnak a támadók a megcélzott rendszerhez eljutni. A laterális mozgás részeként feltérképezik a rendszereket és hálózatokat, valamint gyakran privilegizált jogosultságok megszerzésével, legitim eszközök segítségével tartják fenn hozzáférésüket a kompromittált rendszerekhez. A perzisztencia fenntartására irányuló tevékenység egyértelműen offenzív.

A direkt és indirekt műveletekben eltérő potenciál rejlik. Különösen igaz ez, ha a kiberműveleti képességeket a nemzeti érdekek védelme és érvényesítése szempontjából vizsgáljuk. Az indirekt műveleteknek főként az elrettentés terén van fontos szerepük. Egy olyan helyzetben, amikor a védekező fél robosztus CTI képességekkel rendelkezik és a különböző támadásokat még a károkozás előtt meg tudja zavarni vagy akár már az előkészítés fázisában akadályozni tudja, azzal megnöveli a támadások erőforrás-igényét. Ezzel egy szolidabb háttérrel rendelkező támadót el lehet tántorítani, aki kénytelen lesz más célpontokat keresni. Illetve abban az esetben is hasznosak lehetnek az indirekt műveletek, ha a támadók proxy-ként vagy fedezékként használják a megtámadott rendszert. Ilyenkor jellemzően az anonimitás fenntartása, illetve a gyanú másra

terelése a cél, amihez az erőforrások optimalizálása okán a legkisebb ellenállás irányába haladnak. Ezek a támadások elrettenthetők az indirekt műveleti képességekkel, mert a támadók igyekeznek könnyebben kihasználható célpontot találni.

A direkt műveleteknél megmarad az elrettentés potenciálja, amit kiegészít a hírszerzési, befolyásolási és destruktív lehetőségek kiaknázása. A szükséges stratégiai elemzés elvégzése és a kontextusba helyezés után ezeknél az offenzív műveleteknél azonosíthatók leginkább azok a motivációk és ösztönzők, amelyek egy adott állam vagy államok csoportjának érdekei mentén alakulnak ki. Az offenzív műveletek körébe tartozó direkt tevékenységek kivétel nélkül az ellenfél információs rendszereinek súlyos megsértésével járnak, azonban a hírszerzési és befolyásolási képességek kibővülése miatt az államok egyre gyakrabban alkalmazzák ezeket inkognitóban. Mindazonáltal egy sikeres offenzív művelet attribúciója a diplomácia nyilvános szintjén történő elítélésen és egyéb negatív hatásokon túl, alkalmas a színfalak mögötti erődemonstrációra és erőkivetítésre.

VI.6.3 A támogató és K+F komponens jelentősége

Az interjúk során elhangzottak alapján a válaszokból kiderül, hogy sok országban nagy szükség lenne modern, innovatív megközelítésre a döntéshozói szinten ahhoz, hogy egy kiber különleges műveleti képességet fel lehessen építeni. Ilyen tekintetben Magyarország a becslések szerint nem áll előkelő helyen, inkább a sereghajtók mezőnyét erősíti. De nem csak hazánkban probléma, hogy a politikai-stratégiai szint nem tud mit kezdeni a kiberműveletek teljes spektrumával, ami miatt a sokszor rendkívül korlátozott erőforrások allokációja is dilemmák sorához vezet.

Az egyik ilyen terület a kiberműveleteket támogató funkciókhoz, illetve általában a kiberműveletek támogató szerepéhez kapcsolódik. Az előbbi tekintetében a problémát az jelenti, hogy egy hatékony kiber különleges műveleti képességnek a kinetikus különleges műveleti erőkhöz hasonlóan támogatásra van szüksége. Ehhez olyan erőforrások biztosítására és szervezeti egységek létrehozására van szükség, amelyek látszólag nem kapcsolódnak szorosan a kiber különleges műveletekhez, azonban a sikeres alkalmazáshoz nélkülözhetetlenek. Ide tartoznak a mellékesnek tűnő ügyviteli, üzemeltetési és karbantartási, illetve egy sor adminisztratívnak nevezhető terület, amelyek nélkül nem tud jól működni egy képesség. Példaként merült fel az egyik interjú során, hogy az eszközöket valakinek be kell szereznie, amiket azután üzemeltetni kell, de már a beszerzés is számos kérdést vet fel egy fedetten működő szervezet esetében. Hazai viszonylatban jellemzően

átvilágításon és speciális minősítésen átesett szolgáltatókon, illetve beszállítókon keresztül van lehetőség eszközöket vásárolni, ami lassú, cserébe drága. Egy ilyen képességnél műveleti biztonsági szempontból felmerülhet az eszközök egy részének teljes cseréje és helyettük újak beszerzése hiba vagy amortizáció nélkül is. Ez a szemlélet távol áll a hagyományos ellátó rendszerektől, így valószínűleg képtelenek lennének kezelni. További komplikációt jelent az eszközök hagyományos igényektől eltérő, speciális jellege. A kiber különleges műveleti képességek támogatása nagy valószínűséggel nem oldható meg hatékonyan a hagyományos állami ellátórendszerek bevonásával. Speciális támogató funkciók kialakítására van szükség, amelyeknél elsődleges a műveleti szempontok és igények érvényesülése, mindent ezeknek kell alárendelni és ennek megfelelően kialakítani.

Ehhez bizonyos szempontból szorosan kapcsolódik a kiberműveletek támogató tevékenységként való megközelítésének problematikája. Mindaddig, amíg a kiberműveletek szerepe a honvédelmi, rendvédelmi és nemzetbiztonsági szektorok egyéb műveleteinek támogatására korlátozódik, nem valószínű, hogy ki tud épülni az a speciális feltételrendszer, ami a kiberműveletek teljes spektrumában való hatékony működéshez kell. Kevés kivétellel, nemzetközi szinten is általános jelenség, hogy egy adott szektorban folyik a kiberműveleti képességek építése, nem igazán van átjárás és együttműködés, miközben a szektorokon belül is egyfajta kiegészítő szerepkörben tartják a kiberműveleti képességeket. Jellemzően a műveletek hírszerzési és felderítési támogatásában, a kibertérben történő biztosító feladatokban és az adott szektor kibervédelmi tevékenységeiben jutnak szerephez. Amennyiben felmerül a kiberműveletek teljes spektrumában működő képesség igénye, megfontolásra érdemes annak teljesen önálló, a honvédelmi, rendvédelmi és nemzetbiztonsági szektorok metszetében történő speciális szervezetként történő létrehozása. Egy ilyen modellben könnyebb ötvözni az egyes szektorok előnyeit és egyéb szempontok érvényesítéséhez is jó alternatíva lehet.

A kiberműveleteket támogató szerepkörhöz és feladatrendszerhez köthető az úgynevezett feltörekvő technológiák kiberműveleti alkalmazása, illetve az ehhez kapcsolódó kutatási és fejlesztési tevékenységek. Többen is kiemelték az interjúk során, hogy önálló kiber különleges műveleti erő nehezen képzelhető el saját fejlesztésű hardverek és szoftverek nélkül. Természetesen nem kell és nem is lehet kizárni a harmadik féltől beszerezhető megoldások alkalmazását, de az egészséges egyensúly megteremtése és fenntartása a képességek kialakításának kezdetétől jelen

kell legyen. Ha nincsenek saját kutatások és fejlesztések, akkor túl nagy lesz a ráutaltság és kitettség a beszállítókkal szemben, ami nem elfogadható mértékű kockázatot jelent különösen az olyan szenzitív ágazatokban, mint a honvédelem, rendvédelem és nemzetbiztonság. A legtöbb ország számára prioritást kellene jelentsen a saját régiójához és kockázati értékeléséhez illeszkedő kutatásokban és fejlesztésekben való részvétel a mesterséges intelligencia, a kvantum számítástechnika és más ma még sokak számára tudományos fikciónak tűnő területen, amelyek rövid időn belül befolyással lehetnek a kibertérben zajló folyamatokra.

VI.7 A képesség kialakításának erőforrásai és kockázatai

Több alfejezetben is érintőlegesen felmerültek erőforrás- és egyéb ellátási igények a kiber különleges műveleti képességek kialakításával kapcsolatban, azonban az interjúk során volt olyan konkrét kérdés, ami erre a területre fókuszált. A válaszokból az eltérő megközelítések ebben az esetben is érezhetők voltak. Ezért kerülnek az elhangzottak a saját gondolatokkal együtt különálló alfejezetbe.

Bár a hagyományos képességek kialakítása kapcsán az erőforrásokkal összefüggésben gyakran emlegetett „pénz, fegyver, paripa” hármas a kiber különleges műveleti képességek esetében is igaz, a valóság árnyaltabb képet fest. Vannak olyan területek, ahol további aspektusokat is figyelembe kell venni.

VI.7.1 Beágyazottság és interoperabilitás

Az egyik ilyen aspektus, hogy a kiber különleges műveleti képességek milyen szervezeti formában jönnek létre. Ha a honvédelmi, rendvédelmi és nemzetbiztonsági szektor meglévő szervezeteihez rendelve, szeparáltan működő rész képességek alakulnak ki, az sok szempontból leegyszerűsíti a beágyazottság kérdését. A szervezeti kultúra és hagyományok megmaradnak, ahogyan a formális és informális kapcsolatok kialakulása és fejlesztése is jóval egyszerűbb. Ebben az esetben jelentősen csökkenthető az esetleges szervezeti ellenállás, a kiber különleges műveleti képességek rövid időn belül integráns részévé válhatnak annak a szervezetnek amelyiknek az alárendeltségébe tartoznak. Ez segíti az adott szektor adta mozgástér maximális kihasználását, azonban egy olyan dimenzióban, ahol a fizikai és logikai határok egyaránt elmosódnak, nagyon hamar problémákat generálhat a szektorális megközelítés és a hagyományos szervezetekkel történő szoros integráció.

Pillanatok alatt hatásköri és jogosultsági problémák merülhetnek fel, ami a hazai helyzetet példaként hozva oda vezethet, hogy egyes műveleteket mindenki a sajátjának érez és ennek megfelelően cselekszik, míg más műveleteket senki nem akar felvállalni. Ezen valamennyit segíthet egy kiberműveleti ernyőszervezet kialakítása, de ez inkább csak komplikáltabbá teszi a helyzetet, mert a beágyazottsággal összefüggő probléma jellemzően folyamatában, illetve több éves működés során csökkenthető.

Az önálló szervezetként történő létrehozás rontja a beágyazottságot, azonban ez a hátrány rövid időn belül átfordítható, ha kellő hangsúlyt helyeznek az interoperabilitás megvalósítására. Sok országban idegenkednek attól, hogy olyan szervezetek közösen hajtsanak végre műveleteket vagy akár csak gyakorlatokat, amelyeknek teljesen eltérő felhatalmazása van az ország védelmének szempontjából. Jó példa erre a rendvédelmi különleges egységek közös gyakorlatai a katonai különleges műveleti erőkkel. Ugyanakkor a biztonsági környezet változása a világ több régiójában is egyre inkább megkívánja, hogy a rendvédelmi vagy honvédelmi szektor szervezetei ne csak egymás között, hanem szektoron kívüli szervekkel is képesek legyenek az intenzív együttműködésre a műveletek szintjén is. A 21. század nem hagyományos, illetve hibrid kihívásai azáltal, hogy elmossák a határokat a konfliktusok térbeli és időbeli határai között, egyúttal a kihívásokat kezelni hivatott szervezetek közötti írott és íratlan szabályokra is hatással vannak, ami jellemzően hatásköri átfedések vagy hiányosságok formájában érzékelhető. Az interoperabilitás szerepe egyre jelentősebb nem csak a hagyományosnak tekinthető szervezetek között, hanem az olyan ma még speciálisnak számító kihívások kezelésére létrehozott szervezetekkel is, mint a kibertér vagy a világűr rosszindulatú felhasználása. Az interoperabilitás kulcsfontosságú terület a kiber különleges műveleti képességek önálló szervezetként történő létrehozása esetén, ezért az ehhez szükséges feltételek megteremtéséről a politikai és stratégiai döntéshozóknak feltétlenül gondoskodniuk kell.

VI.7.2 Állandó és rugalmas költségvetés

A feltételekre és erőforrásokra vonatkozó kérdések tekintetében nem volt olyan válasz, amelyik ne említette volna a pénzt, vagyis a megfelelő anyagi forrásokat, illetve a ráfordítás és megtérülés arányát. Általánosságban elmondható, hogy a szervezet méretétől és létszámától függetlenül, első ránézésre elég magasnak tűnik az az összeg, amit egy kiber különleges műveleti képességbe nem csak kezdetben, hanem a teljes életciklus alatt invesztálni kell. Külön szokatlan lehet a költségeken

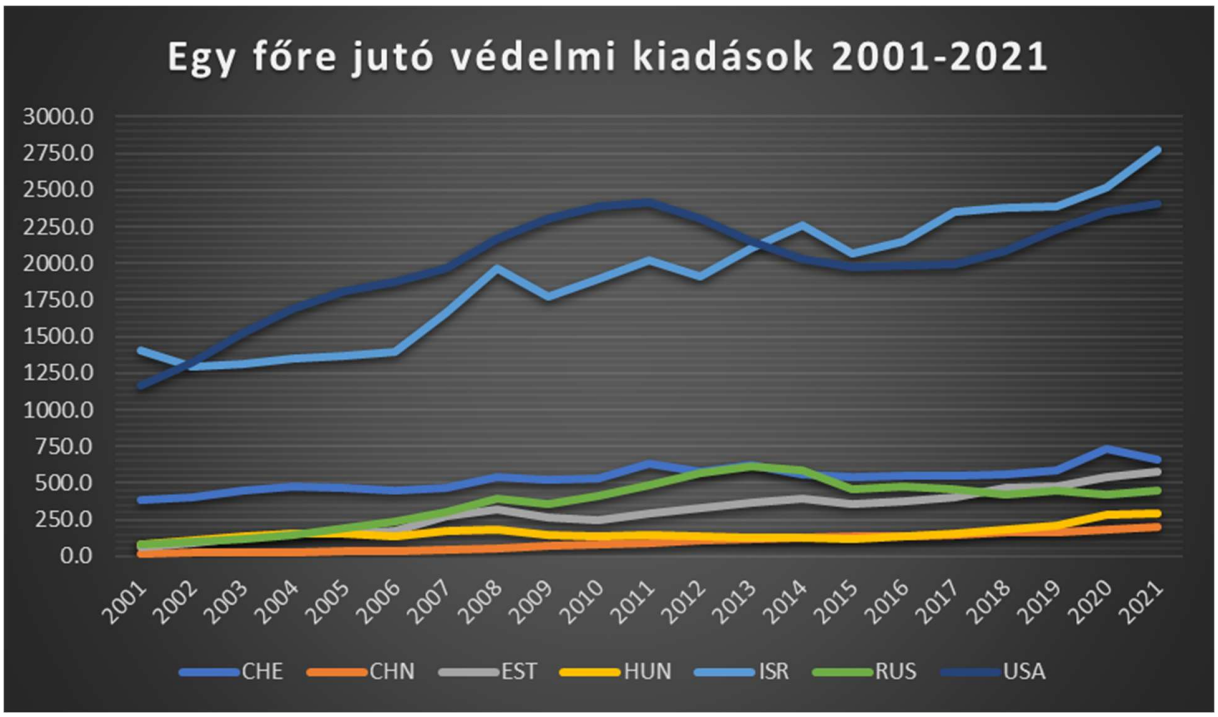
belül a fizetések, illetve kompenzáció aránya. Ennek megértéséhez fontos annak felismerése, hogy a kibertér tudás alapú közeg, ezért az, ami az iparosodott világban az olaj vagy az arany, a kibertérben az információ és a tudás, aminek ára van. Ezért az nehezen elképzelhető, hogy átlagon aluli vagy átlagos kompenzációval foglalkoztatni valakit ezen a területen működőképes alternatíva lehet. Elitista szemléletmód érvényesül, bár eltérő képességek és készségek terén, de a szakma legjobb, nagyjából 5-10 százalékáról van szó, akik számára akár ellenszenves is lehet, hogy valaki egyáltalán megpróbál kevés pénzért foglalkoztatni bárkit egy ilyen speciális területen. Ha figyelembe vesszük, hogy nincs megfelelő oktatás, speciálisak a követelmények és általános a szakemberhiány a szektorban, akkor a versenyszféránál magasabb kompenzáció teljesen reális elgondolás. A helyzetet leegyszerűsítve az államnak nincsenek olyan értelemben részvényesei, mint a versenyszféra nagyvállalatainak, akik számonkérnék vagy módosíthatnák a vállalati vezetés döntéseit. Persze politikai értelemben a demokratikus országokban a választások megfeleltethetők a versenyszféra részvényesi számonkérésének, mégis jóval nagyobb mozgástere van egy államnak ezen a téren, mint egy magánvállalatnak. A képlet egyszerű: ha speciális körülmények között átlagon felüli képességekkel rendelkező humánerőforrásra van szükség, akkor minden másnak is átlagon felülinek kell lennie. Az ellenkező esetben csak a rövid távú gondolkodás és humán tőke, valamint a tudás jelentőségének fel nem ismerése igazolható. Az egyik interjúalany megfogalmazása szerint: a kiadásokon lehet faragni, de vannak költségek, amikből nem. Ilyen a fizetés.

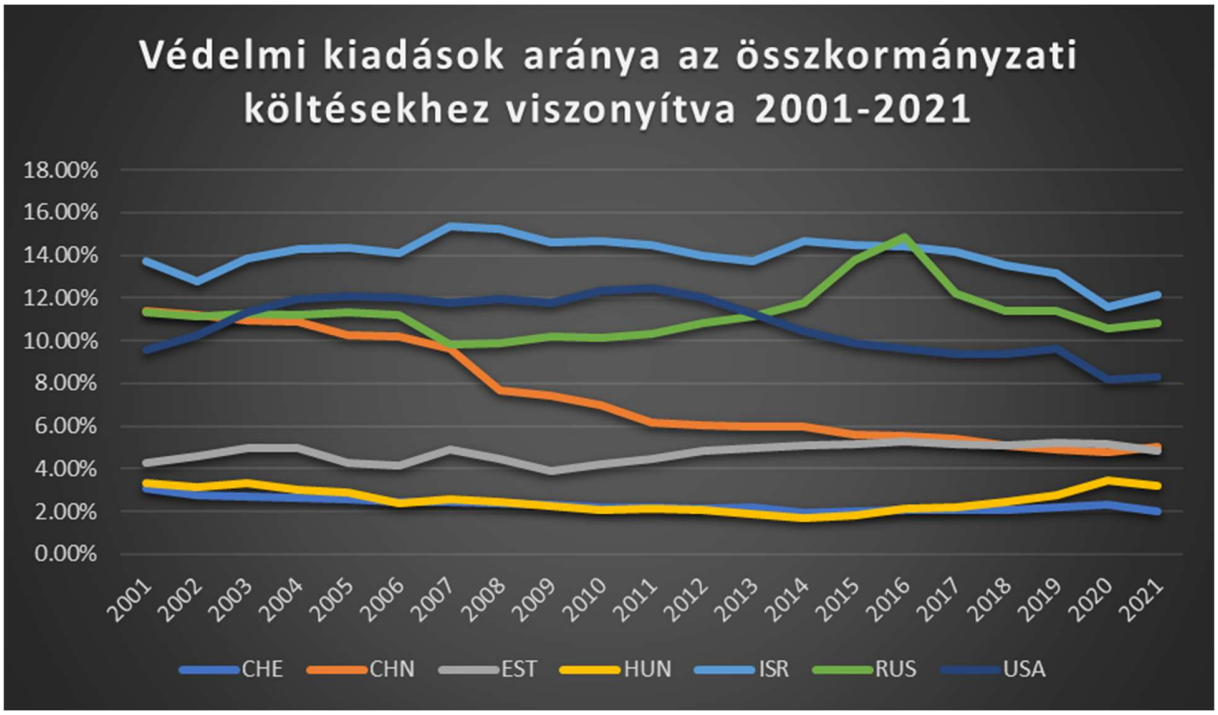
Az, hogy az átlagon felüli fizetések anyagi fedezetét a képességet létrehozó állam milyen módon teremti meg, csupán pénzügytechnikai kérdés, ami teljesen egyedi megoldások megvalósulását eredményezi. Hasonló a helyzet a másik jelentős tétel, az infrastruktúra tekintetében is. Adott esetben az infrastruktúra létszámhoz viszonyított magas költségei kapcsán két tényező felismerése meghatározó. Egyfelől a kisebb befolyással rendelkező országnál jóval nagyobb hangsúlya van a kiber különleges képességeknek, mert a hagyományos katonai képességekkel sokkal kevésbé tud elrettentő lenni egy nagyobb országgal szemben. Ha például egy állam beszerez húsz harckocsit, akkor a nulla harckocsihoz képest nem tudja érdemben növelni az elrettentő képességét egy olyan hatalommal szemben, amelyiknek kétszász vagy kétezer harckocsija van. Viszont a kiberképességek amplifikáló hatása és a kibertér aszimmetriája miatt egy jóval kisebb csapat nagyságrendekkel nagyobb védelmi és támadó képességeket tud felmutatni, mint egy nehéz fegyverzettel működő hagyományos katonai képesség. A válaszok alapján nem releváns, hogy

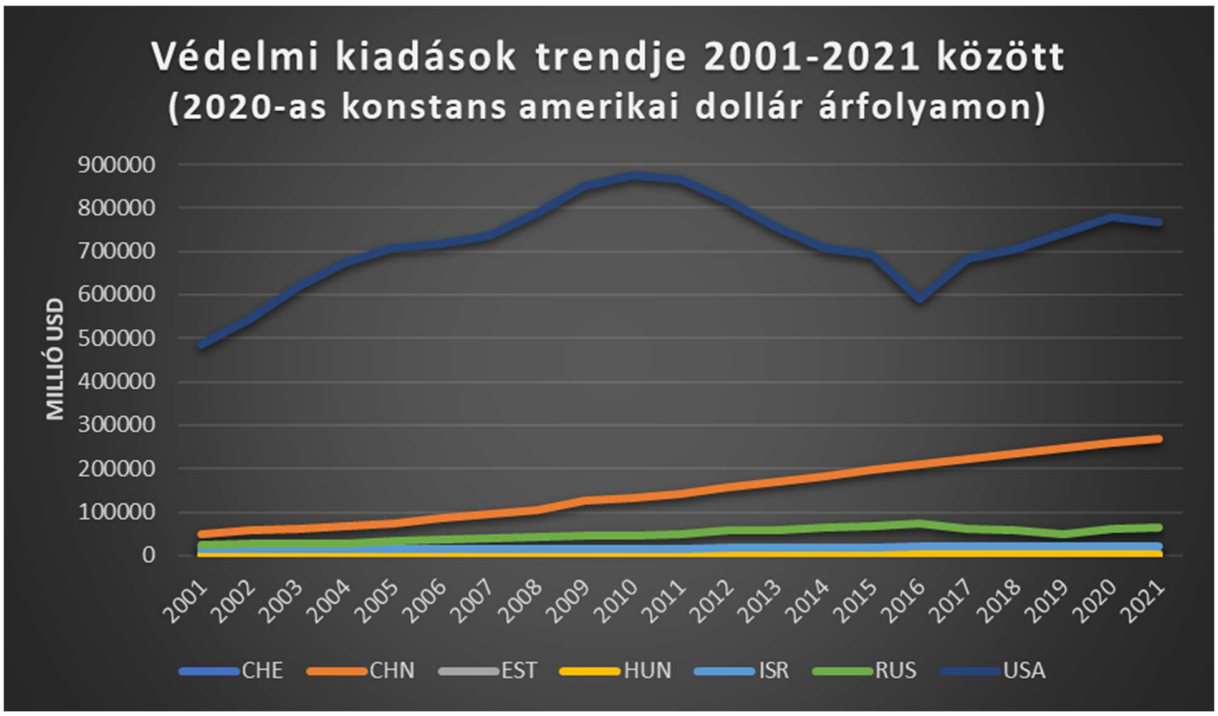
tizenöt, száz vagy hatszáz fős a létszám, mert az aránypárok számítanak és az ebből következő megtérülési ráta. Ez a másik tényező, aminek a felismerése elengedhetetlen. A védelmi beszerzések szinte minden állam számára komoly kiadásokat generálnak. A hadihajók, a harckocsik, a ballisztikus rakéták, a vadászrepülőgépek, a lövedékálló mellények vagy a kézi fegyverek önmagukban is drágák és szinte minden esetben felmerülnek drága járulékos költségek a kiképzéssel, üzemeltetéssel vagy a logisztikai ellátással kapcsolatban. Ha ebből az aspektusból vizsgáljuk a kiber különleges műveleti képesség költségeit, akkor az látszik, hogy – a harckocsizó példánál maradva – az egyforma létszámú kiberműveleti, illetve harckocsizó egységet összevetve, a kiberképesség jóval nagyobb hatásfok mellett, sokkal olcsóbb lesz.

Alapvetően a költségek és a létszám tekintetében jóval kisebb egységben érdemes gondolkodni, mint amit kinetikus viszonylatban elképzelnénk, még akkor is, ha a kis létszám ellenére például az infrastruktúra teljes cseréje jóval gyorsabb tempójú lenne. Ez pedig lehetőséget ad arra, hogy hosszú távra tervezve megfelelő anyagi forrásokat lehessen biztosítani a kiber különleges műveleti képességek kialakítására és fenntartására. A képesség méretét érdemes a létrehozó állam fenyegetettségi szintjéhez, geopolitikai és gazdasági helyzetéhez, illetve politikai berendezkedéshez igazítani. Ismét kinetikus példával élve, ha tíz perc alatt át lehet repülni az ország légterén, akkor nem érdemes száz vadászgépet hadrendben tartani. Ehhez hasonlóan egy ötmillió lakosú kis területű kelet-európai és egy több száz millió lakosú kontinensnyi méretű országnak Ázsiában, eltérő arányban érdemes a kiberműveleti képességeiket fejleszteniük. Ha az értekezésben vizsgált kiberbiztonsági szempontból fejlett államok védelmi költségvetéseit hasonlítjuk össze, a gyakran hivatkozott GDP arányos bontás önmagában nem túl beszédes. Sokkal érdekesebb következtetések vonhatók le az egy főre jutó, illetve az összkormányzati költésekkel történő aránypárok felállítása, valamint a védelmi kiadások hosszú távú trendjei esetén. Utóbbiak alapján egyrészt kiderül, hogy mennyire félrevezető lehet a GDP arányos védelmi költségvetés az adott ország védelmi képességeinek egyedüli indikátoraként, másfelől a magasabb védelmi költségvetés és a fejlett kiberképességek között összefüggés rajzolódik ki. A közvetlen összefüggés bizonyítása további elemzést és mélyebb kutatást igényel, azonban mindenképpen jelzés értékű, hogy a nem GDP arányos összehasonlítás alapján magasabb védelmi költségvetéssel rendelkező államok jellemzően fejlettebb kiberképességeket birtokolnak.

	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
CHE	1.0	1.0	0.9	0.9	0.9	0.9	0.7	0.7	0.7	0.7	0.7	0.7	0.7	0.6	0.6	0.7	0.7	0.6	0.7	0.8	0.7
CHN	2.0	2.0	2.0	1.9	1.9	1.9	1.7	1.7	1.9	1.7	1.7	1.7	1.7	1.7	1.8	1.8	1.7	1.7	1.7	1.8	1.7
EST	1.5	1.7	1.7	1.7	1.5	1.4	1.7	1.8	1.8	1.7	1.7	1.9	1.9	1.9	2.0	2.1	2.0	2.0	2.0	2.4	2.2
HUN	1.6	1.6	1.6	1.5	1.4	1.2	1.3	1.2	1.1	1.0	1.0	1.0	0.9	0.9	0.9	1.0	1.0	1.1	1.3	1.9	1.6
ISR	6.5	6.6	6.5	6.4	6.3	6.0	6.4	6.4	6.1	5.9	5.8	5.6	5.6	5.7	5.5	5.5	5.5	5.3	5.1	5.4	5.2
RUS	3.5	3.8	3.7	3.3	3.3	3.2	3.1	3.1	3.9	3.6	3.4	3.7	3.9	4.1	4.9	5.4	4.2	3.7	3.8	4.3	4.1
USA	3.1	3.4	3.8	4.0	4.1	4.0	4.1	4.5	4.9	4.9	4.8	4.5	4.0	3.7	3.5	3.4	3.3	3.3	3.4	3.7	3.5







9. ábra: A védelmi kiadások különböző aspektusokból vizsgálva Svájc (CHE), Kína (CHN), Észtország (EST), Magyarország (HUN), Izrael (ISR), Oroszország (RUS) és az Egyesült Államok (USA) rendelkezésre álló adatai alapján 2001 és 2021 között. Az ábra tetején a táblázat a GDP arányos védelmi kiadásokat tartalmazza százalékos formában, az első diagram az amerikai dollárban (USD) kifejezett egy főre jutó védelmi kiadásokat mutatja. Az ábra második diagramja az összkormányzati költéshez viszonyítva mutatja a védelmi kiadások arányát, míg a harmadik diagram a védelmi kiadások trendjét mutatja 2020-as konstans amerikai dollár árfolyamon. (A szerző saját szerkesztése. Forrás: SIPRI)

VI.7.3 Kockázatok és kihívások

A kockázatok tekintetében majdnem minden válaszadó az elsők között említette a megtartó képességet és az állomány tagjainak hosszú távú elköteleződését. Látunk arra példát, hogy kibervédelmi területen tevékenykedő állami szervezet a toborzás során a feladatok unikális jellegével kampányol és erősen épít a jelentkezők hazaszeretetére, miközben helyzetéből adódóan nincs lehetősége piaci vagy azt meghaladó kompenzációt biztosítani. Az ilyen megközelítés alkalmazásának következménye, hogy a szervezet nem képes hosszútávon megtartani a szakembereket, ezért az állomány konstans változásban van. Ez mindenképpen kerülendő egy olyan képességnél, ahol kiemelten fontos a csapatszellem, illetve sok esetben erős az egymásra utaltság. Az állomány tagjainak távozása a megszerzett tudás miatt önmagában kockázatot jelent, de a tudás pótlása is kihívást jelenthet. Ilyen szempontból fontos, hogy az állomány tagjai ne legyenek nélkülözhetetlenek, mivel az veszélyeztetheti az egész szervezet műveleti képességeit.

A kiber különleges műveleti képesség létrehozása és a létrehozás elmulasztása egyaránt kockázatokat rejt. A létrehozás kapcsán felmerülő kockázatok közé sorolható a társadalmi megítélés és a transzparencia. Belföldi és külföldi viszonylatban is hátráltató tényező lehet a túl nagy publicitás, ha viszont a fedett körülmények miatt minimális információ érhető el a képességről, akkor nem fogják érteni, ami konfliktusokhoz vezethet. Ilyen tekintetben hatékony megoldás lehet, ha a teljes kiberműveleti spektrum defenzív szegmensét felvállalja a létrehozó és csak az offenzív képességek működnek teljesen fedett körülmények között. Technológiailag így is felmerülhetnek problémák, de ezeknek a kezelése könnyebb. Az offenzív szegmens kapcsán kihívás az esetleges nem megfelelő használat, ami szélsőséges esetben katonai reakciót is kiválthat. Fontos, hogy a kiber különleges műveleti képesség független maradjon a politikától olyan értelemben, hogy a politika ne tudjon a számára kedvező embereket beültetni a szervezetbe.

Az offenzív képességekkel az egyik legnagyobb probléma a haszonélvezők definiálása, illetve az, hogy pontosan mire használják a képességeket, mivel egy offenzív művelet minden esetben sérti valakinek az érdekeit. Ha egy állam offenzív képességekkel rendelkezik, akkor feltételezhető, hogy képes olyan információk birtokába jutni, amiket például nyílt diplomáciai úton nem lehetne megszerezni. Ha túl sok információ gyűlik össze, akkor arra sokan lesznek kíváncsiak és

megnövekedik a célponttá válás lehetősége. Ehhez kapcsolódóan további probléma, hogy a döntéshozói szint gyakran nincs tisztában azzal, hogy mit is szeretne elérni egy ilyen képesség létrehozásával. Ezért nagyon fontos, hogy a politikai döntéshozó tiszta és világos elképzelésekkel rendelkezzen azzal kapcsolatban, hogy a képesség teljes műveleti szinten nem azonnal fog rendelkezésre állni, hanem egy hosszútávú befektetésként, adott esetben kormányzati ciklusokon átívelő időtávlatban lesznek elérhetők azok a részképességek, amik kapcsán azután majd a döntéshozónak elhatározásra kell jutnia, hogy csak fenyegetni, elrettenteni akar a képességekkel, vagy be is veti azokat.

Az időtényezővel kapcsolatban felmerült, hogy ha huzamosabb időn keresztül nincs felmutatható eredmény vagy a képességfejlesztés megreked, az olyan következményekkel járhat, aminek a végén a politika beleszól a szakmai folyamatokba és ez súlyos kockázat egy ilyen speciális területen. Szintén az idővel összefüggő kockázat, hogy ha nem sikerül időben bevetésre alkalmas képességet kialakítani, a pótlás szinte lehetetlenné válik, mivel a helyzet ugyanaz, mint a kinetikus különleges műveleti szolgálatok és erők esetében: nem lehet válsághelyzetben létrehozni. Tapasztalati úton működő szakterület, aminek a megszervezésére nem elég 1 év. Minél nagyobb a tapasztalási lehetőség, minél több idő van a felkészülésre annál biztosabb, hogy sikeres lesz a képességfejlesztés. Több interjúalany véleménye szerint hazánk le van maradva a térség országaihoz képest, de még a nemzetközi terrorizmushoz viszonyítva is, mert utóbbi képes kifizetni a legszofisztikáltabb kiberbűnözőket, ami egy demokratikus berendezkedésű ország számára számos tekintetben probléma lehet.

A képesség kialakításának kihívásaival kapcsolatban negatív és pozitív előjellel is megjelent egy hazai példa. A 2010-es évek elején a semmiből jött létre egy alapvetően rendvédelmi szervezet, aminek nem volt elődje, viszont bármekkora anyagi forrást megkapott, amiről a szervezet saját maga úgy ítélte meg, hogy a képességek kialakításához szükségesek. A szokatlanul nagy anyagi forrás egyfajta rekvirálási jogosítvánnyal társult, ami lehetővé tette a kívánt eszközök és infrastruktúra azonnali megszerzését. A szervezet nagyságrendileg az első öt évét azzal töltötte, hogy majdnem a nulláról igyekezett felépíteni egy képességet, miközben folyamatosan a létjogosultságát próbálta igazolni és több komoly szakmai hibát is összehozott ez alatt az időszak alatt. Mindezek ellenére napjainkra a szervezet szinte teljesen önálló, mivel mindene megvan a magasszintű szakmai munkához. Ugyanakkor a szervezet megalakulása egy mai napig tartó

identitászavart hozott létre a rendvédelmi és nemzetbiztonsági tevékenységek szétválasztása terén. A példához negatív előjel társul, ha a megvalósításból, a kivitelezés részleteiből vagy a szakmai közösségekben generált feszültségből fakadó kockázatokat vizsgáljuk. Ugyanakkor pozitív az előjel, ha olyan példát keresünk, amivel a politikai elhatározást követően az anyagi források bőkezű biztosítását, a szükséges mandátum szavatolását és a gyors megvalósítást kívánjuk szemléltetni. Ezen a ponton érdemes megemlíteni a politikai, illetve stratégiai akaraton, valamint a szükséges erőforrások túl az alapvető feltételek között azt a szakmai stábot, amely képes az egész képesség kialakítására és üzemeltetésére háborúban és békében egyaránt. Ha nincs ilyen stáb, vagy hiányzik a motiváció, esetleg a szaktudás, akkor a képesség gerince hiányzik, ami nélkül bele sem érdemes kezdeni a képességfejlesztésbe.

Összegzés, következtetések

Az VI. fejezetben előbb áttekintettem a kiber különleges műveleti képességek létjogosultságát és vizsgáltam a létrehozás stratégiai, illetve műveleti szempontjait, majd a létrehozás különböző területeit elemeztem. Az VI.2 alfejezet olyan kritikus területeket vizsgált, mint a jogi háttér, a polgári demokratikus kontroll, valamint a cselekvési sebesség. A feltárt tényezők alapján a VI.3 alfejezet a kiber különleges műveleti képességek integrációs alternatíváit tanulmányozta a katonai, a nemzetbiztonsági, az önálló félkatonai, illetve szerződéses modellek segítségével. A fejezet további részeiben jelentős szerephez jutottak a honvédelmi, rendvédelmi, nemzetbiztonsági és kiberbiztonsági szakemberekkel folytatott irányított interjúk, illetve azok a szubjektív igények és elvárások, amik az adott szektorral összefüggésben felmerülhetnek egy speciális kiberműveleti alakulattal szemben. Az interjúk alapján, a különleges műveleti szakirodalom segítségével a technikai, mentális és fizikai követelmények unikális kombinációját mutattam ki, amit kiegészít az interoperabilitás keretrendszere, valamint a kapcsolódó humán kihívások. Az utolsó három alfejezet az interjúk feldolgozásával három olyan kérdéskörrel foglalkozott, ami a kiber különleges műveleti képességek létrehozása és fenntartása kapcsán kiemelt jelentőséggel bír. Ezek a felkészítés és kiképzés, a képesség gerincét adó komponensek, valamint a szükséges erőforrások.

A biztonság- és védelempolitikai elemzésnek csakúgy, mint a védelmi tervezésnek és képességfejlesztésnek szerves része az erőkkel összefüggő átfogó értékelés, ami jellemzően előre meghatározott szempontrendszer alapján történik. A kiber különleges műveleti erők

létjogosultságának vizsgálatát a kinetikus különleges műveleti erők kihívásaival kezdtem, ami kettős képet mutat abban a tekintetben, hogy míg hazai viszonylatban egyelőre nem elképzelhető a robosztus kiberműveleti képesség különleges erők keretén belül történő kialakulása, az Egyesül Államokban aktív vita folyik arról, hogy a speciális kiber missziókban szerepet vállaló egységek a kiberműveleti vagy a különleges műveleti parancsnokság alárendeltségében jöjjenek létre. A kutatás során nem azonosítottam olyan szempontot vagy megoldást, ami alapján egyértelműen állást lehetne foglalni a különböző megközelítések valamelyike mentén. A stratégiai és műveleti szintek vizsgálatával arra a következtetésre jutottam, hogy a nemzetközi rendszer állapota és a kibertér adta lehetőségek az államok egy részénél olyan viselkedési minták létrejöttét generálja, amit a nemzetközi jog szabályrendszere nem képes követni és kontrollálni, ezért az érdekek sérülése esetén jelentősen korlátozódik a válaszadásra alkalmazható hagyományos eszközrendszer.

A kutatás során azonosított indikátorok alapján megállapítottam, hogy a kiberműveletek teljes spektrumában alkalmazható képességek kialakítása értelmezhető a nemzetközi kapcsolatok kiberdimenziójában kialakult anarchikus állapotokra történő válaszadásként, amit manapság leginkább a nagyhatalmak között zajló „kiberháború" kifejezéssel szokás leírni. Bár hadtudományi szempontból a háborús narratíva alkalmazása helytelen, a kutatás által feltárt állami, illetve állami támogatású szervezetek kiberműveleti képességei egyértelműen elérik azt a szintet, amivel bizonyos esetekben a kinetikus támadásokkal összemérhető hatásokat képesek kiváltani gyorsabban, költséghatékonyabb módon és a kibertér kínálta aszimmetria kiaknázásának maximalizálásával.

Ennek lehetőségét egyfelől a nemzetközi jogi rendszer hiányosságai teremtik meg, másfelől a kibertér sajátos jellege, aminek révén rendkívül nehéz teljes bizonyossággal meghatározni, hogy ki az agresszor. Ez alapján azt a következtetést vontam le, hogy várhatóan a nemzetközi jog még évtizedekig képtelen lesz a technika fejlődését beérni, ezért reális alternatíva lehet minden állam számára, hogy érdekeinek védelme és érvényesítése okán a hagyományos képességek mellett robosztus kiberműveleti képességeket fejlesszen, amely a kiberműveletek teljes spektrumában alkalmazható.

Arra vonatkozóan, hogy a kiberműveleti képességek kialakítása során milyen integrációs sémák alkalmazása kínál magasfokú hatékonyságot, egyszerű beágyazhatóságot vagy épp letagadhatóságot, több lehetőséget is megvizsgáltam. Megállapítottam, hogy a katonai,

nemzetbiztonsági, önálló félkatonai, illetve szerződéses modellek mindegyike szép számban rendelkezik előnyökkel és hátrányokkal, amelyeket minden szereplőnek mérlegelnie kell a képességek kialakítása előtt, hogy kiválaszthassa a számára leginkább kedvező megoldást. Az interjúk és a szakirodalmi vizsgálatok alapján a katonai és nemzetbiztonsági integrációval öröklődő robosztus szervezeti háttérrel és az ebből fakadó bonyolult hierarchiával és lassúsággal szemben mindenképpen előnyösebb az önálló félkatonai vagy a szerződéses modell alkalmazása, azonban mindegyik esetben további elemzésre és értékelésre van szükség, hogy pontosabb képet lehessen alkotni az előnyökről és hátrányokról.

A kutatás egyik legfontosabb konklúziója, hogy a kiberműveleti képességekkel összefüggésben a humánerőforrás jelentőségét abszolút prioritásként kell kezelni. A rendelkezésre álló szakirodalom és jelentős mértékben az interjúk alapján meghatároztam a kiber különleges képességek létrehozásához szükséges követelményrendszer alapjait. Ugyanakkor arra a következtetésre jutottam, hogy a technikai, mentális és fizikai alkalmasság terén is további kutatás szükséges annak érdekében, hogy a követelményrendszer pontosítható legyen. Az egyedi elvárásokon túl további két szempontot is meghatároztam. Egyfelől az interoperabilitás, ami különösen olyan esetekben válik jelentőssé, amikor a kiberműveleti képesség önálló félkatonai vagy szerződéses modellként valósul meg. Másfelől a kiberbiztonsági iparágban kialakult szakemberhiány egy olyan megkerülhetetlen tényező, ami várhatóan még évekig velünk marad, így mindenképpen számításba kell venni a kiber különleges műveleti képesség tervezésekor és kialakításakor.

A felkészítés és kiképzés, valamint a képesség fenntarthatósága, illetve komponensei kapcsán jelentős mértékben az interjúkérdésekre kapott válaszokra hagyatkoztam, továbbá beépítésre kerültek a kutatás során feltárt információk. Az interjúalanyok szakmai tapasztalata átfogó kép megalkotását tette lehetővé, így nagy pontossággal körülhatároltam azokat a területeket, amelyek a kiberműveletek gerincét adják, valamint azokat az erőforrásokat és egyéb feltételeket, amelyek a hatékony működéshez nélkülözhetetlenek.

Az VI. fejezetben igazoltam a kiber különleges műveleti képességek létjogosultságát és átfogó megközelítést alkalmazva meghatároztam az alapvető struktúra kialakításának, a különféle szervezeti integrációs lehetőségeknek, valamint a követelményrendszer humán és strukturális elemeinek tekintetében azokat az aspektusokat, amelyeket minden olyan szereplőnek számításba kell vennie, aki kiber különleges műveleti képességeket akar létrehozni.

VII. Összegzett következtetések

Korunk társadalmának digitalizálódó szegmensei egyre kiterjedtebbek, azonban a mögöttes folyamatoknak nem csak pozitív hozadéka van. Az, hogy a mindennapi életünk egyre inkább elválaszthatatlan a digitalizáció központi közegétől a kibertértől, egyúttal folyamatosan növeli a kitettségünket a kibertérből érkező fenyegetésekkel szemben. Leegyszerűsítve, a széles körben elterjedt digitalizáció előtt elegendő volt a pénztárcánkat a zsebtolvajoktól félteni, mára azonban bárkivel előfordulhat, hogy fizikai kontaktus nélkül, az online térben, a digitális világ adta eszközöket fel- és kihasználva fosztják ki. Míg az egyén szintjén ezek a negatív hozadékok elsősorban rendvédelmi feladatokat generálnak, az államok szintjén gyakran honvédelmi és nemzetbiztonsági szintre eszkalálódik egy-egy komplex kibertámadás. Az értekezés fókuszában azok a kibertéri tevékenységek állnak, amelyek a támadó fél szempontjából képességként értelmezhetők, míg a védekező fél számára fenyegetést jelentenek. A kiberműveleteknek nevezett tevékenységek teljes spektruma a passzív védelemitől az offenzív képességekig terjed. Ebben a spektrumban találhatók azok a szofisztikált képességek is, amelyekre a kiberbiztonsági iparág fejlett perzisztens fenyegetésként (APT) hivatkozik. Az APT-ket a hazai tudományos kutatások eddig nem vizsgálták sem a nemzetállami képességfejlesztés, illetve érdekérvényesítés aspektusából, sem pedig a különleges műveleti képességekkel összevetve. Ezért értekezésem fókuszába az APT-k és a különleges műveleti képességek közötti analógiák kerültek, amelyek segítségével kialakítható a kiber különleges műveleti képesség. A fejezetben a kutatás során elvégzett feladatokat és azok eredményeit ismertetem, nagy mértékben támaszkodva az egyes fejezetek végén található összegzésekre és részkövetkeztetésekre.

A biztonságpolitikai elemzések elsődleges kiindulópontja jellemzően a stratégiai dokumentumok áttekintése és értékelése a vizsgált témakör szempontjai alapján. Jelen esetben a nemzeti kiberbiztonsági stratégiák kiberműveleti képességekre vonatkozó részei nyújtották a kiindulási pontot. A kiberbiztonsági stratégiák áttekintésének eredményeként arra a következtetésre jutottam, hogy az államok jellemzően nem adnak precíz információkat a kiberműveleti képességeikkel összefüggésben és a dokumentumok sok esetben nem tartalmaznak egyértelmű meghatározásokat az alkalmazott terminológiához. Ebből kifolyólag a stratégiai dokumentumok szintjén elmosódnak a határok a kibervédelem és a kiberműveletek különböző szegmensei, valamint alkalmazásuk

körülményei között. Azt a következtetést vontam le, hogy a legtöbb ország esetében pusztán a kiberstratégiák alapján nehéz megállapítani, hogy ha a dokumentum említést tesz kiberműveleti képességekről, akkor pontosan milyen tevékenységek sorolhatók ide, illetve a katonai, rendvédelmi és nemzetbiztonsági szektorok közül melyik és milyen mértékben érintett. Míg a nemzetközi szervezetek esetében egyértelműen a védelmi jelleg dominál stratégiai szinten, a nagyhatalmak és a kiber szempontból fejlettebb kisállamok kapcsán előfordul az offenzív képességek nevesítése, vagy az arra való direkt utalás. A vizsgált stratégiák túlnyomó része ugyanakkor óvatos megközelítést alkalmazva, jellemzően a kiberműveleti képességek védelmi aspektusát hangsúlyozza.

Azonban a kiberműveleti képességek teljes spektrumának vizsgálata nemcsak ahhoz szükséges, hogy a stratégiák értelmezésével kapcsolatban megfogalmazott célkitűzés teljesülhessen, hanem a kiber különleges műveleti képességek kialakításának is fontos eleme. Tehát a kiberműveleti tevékenységek vizsgálatával a célom egyfelől a stratégiák pontosabb értelmezése és precízebb értékelése volt, másfelől a kiberműveletek azon szegmensének meghatározása, amihez a hagyományos kibervédelemtől eltérő speciális feltételek szükségesek. A vizsgálat rávilágított, hogy léteznek olyan keretrendszerek, amelyek alkalmazásával leírhatók a kiberműveleti képességek egyes komponensei és meghatározhatók azok a technikai, illetve etikai aspektusok, melyek segítségével a defenzív és offenzív képességek szétválasztása megoldható. A kiberműveletek különböző aspektusaink elemzésével arra a következtetésre jutottam, hogy a passzív és aktív védelem, valamint az offenzív tevékenységek többnyire néhány paraméter alapján jól szétválaszthatók, ugyanakkor sok esetben nincsenek éles határok. Ez különösen igaz a több elemből álló tevékenységek és műveletek esetében. Ilyen esetben a végeredmény egy defenzív és offenzív elemeket egyaránt tartalmazó hibrid művelet lesz, amelyben a hagyományos kibervédelmi képességek mellett speciális képességek is megjelennek. Megállapítottam, hogy a speciális vagy offenzív elemeket korlátozottan tartalmazó kiberműveletek jellegüket tekintve, a végső cél szempontjából lehetnek defenzívek, erre vonatkozóan nincs nemzetközileg elfogadott gyakorlat, szabvány vagy szabályozás. Tulajdonképpen ez az a bizonyos szürke zóna, amire egyes stratégiák utalnak és amiben egyre több állam igyekszik hatékonyan fellépni.

Ezt támasztják alá azok az esettanulmányok is, amelyek alapvetően Kína, az Egyesült Államok és Oroszország kiberműveleti képességeit mutatják be, azonban sajátos megközelítést alkalmazva

egyúttal arra is rávilágítanak, hogy ezek a speciális állami kiberképességek a nemzetközi rendszer többi szereplője számára fejlett perzisztens fenyegetést jelentenek. A kutatás során elkészített esettanulmányokból továbbá az is kiderült, hogy ugyan vannak eltérések a kiberműveleti képességek megközelítésében, a kiberhatalmak jellemzően nagy hangsúlyt fektetnek arra, hogy a katonai és nemzetbiztonsági szektor is hatékony kiberműveleti képességeket alakítson ki. Az esettanulmányokból jól látható, hogy a multipoláris világ három hangsúlyos geopolitikai szereplője időben felismerte a kibertér jelentőségét és évtizedes építkezést folytat a kiberműveleti képességek terén és bár nyíltan a nemzetközi szabályozás kiterjesztését és fejlesztését szorgalmazzák, valójában a kibertér sajátosságait igyekeznek maximálisan kihasználni saját hatalmi törekvéseik és nemzeti érdekeik érvényesítésére.

Miután megállapítottam, hogy a kiberbiztonsági stratégiákból kinyerhető információk a kiberműveleti képességek kapcsán meglehetősen korlátozottak, az értekezés egyik pillérét jelentő fejlett perzisztens fenyegetések részletes elemzésével folytattam kutatásomat. Az APT-k működési jellemzőinek részletes vizsgálata elsősorban iparági jelentések és beszámolók, illetve kormányzati szereplők által kiadott dokumentumok segítségével vált megvalósíthatóvá. Konkrétabban az APT tevékenységek felderítésével és nyomonkövetésével foglalkozó kiberbiztonsági vállalatok, illetve a fejlett kiberképességekkel rendelkező kormányzatok kiadványai nyújtották a kiindulási pontot. Az elemzés eredményeként megállapítottam, hogy az APT-k precíz és egyértelmű célkitűzésekkel rendelkeznek, magasfokú szervezettséget mutatnak és jelentős erőforrásokhoz férnek hozzá, miközben tevékenységük időben elhúzódó, illetve ismétlődő képet mutat. Az APT-khez köthető tevékenységek jellemzően nagy horderejű, stratégiai és/vagy politikai érdekek mentén megvalósuló incidensek nyomán kerülnek nyilvánosságra. Továbbá a tevékenységekre jellemző a kifinomultság, nehezen észlelhetők és adaptív technikai megoldásokat alkalmazva képesek akár hosszú időn keresztül rejtve maradni.

Az APT tevékenységek célkitűzéseivel kapcsolatban arra a következtetésre jutottam, hogy több csoportba sorolhatók. Az egyik csoportba a politikai, illetve geopolitikai célok tartoznak, például a belső stabilitás fenntartása, vagy egy konfliktussal sújtott régió további destabilizálása. A második a gazdasági hatások kiváltása, ami például a jogosulatlanul megszerzett szellemi tulajdon másolásával, eladásával, illetve tanulmányozásával javíthatja a gazdasági versenyképességet, ugyanakkor kapcsolódó további kutatás esetén új és jobb termékek és szolgáltatások olcsóbb

előállítása is lehetővé válhat. A harmadik a technikai hatások elérése, ami forráskódokhoz történő hozzáférést, sérülékenységek kihasználására képes kódok írását, illetve a (védelmi) rendszerek kiismerését foglalja magába és az áldozat gyengítését és kizsákmányolását biztosítja. Az utolsó csoport a katonai hatások generálása, melyek kapcsán arra a következtetésre jutottam, hogy a kibertérre jellemző erőteljes aszimmetria következtében a gyengébb katonai erő képes lehet felül kerekedni nála erősebb és felszereltebb ellenfelén.

Az APT-k elemzése során külön is megvizsgáltam a legfontosabb jellemzőket. A fejlettség vizsgálatából kiderült, hogy az APT-k képesek olyan technológiákat felhasználni és kihasználni a tevékenységük során, amelyek speciális szakértelmet és adott esetben kiemelkedő kreativitást igényelnek. A közvetett támadások, melyek az ellátási láncokat érik egyáltalán nem nevezhetők újszerűnek, azonban a rendszerek komplexitásának növekedése miatt még akkor is rendkívüli precizitásra van szükség, ha a támadás megvalósítása kifejezetten egyszerűnek vagy alapszintűnek hat. A nulladik napi sérülékenységek drágák, illetve kifinomult bánásmódot igényelnek. Ezáltal egyrészt megnő az állami támogatás szerepe, másfelől az APT-t támogató állam saját rendszereire nézve is komoly veszélyt jelenthetnek az ilyen sérülékenységek.

A második jellemző a perzisztencia vizsgálata volt, amelyből kiderült, hogy akár több száz napon át képes egy APT tevékenység észrevétlen maradni az áldozatok számítógépes rendszerein és hálózatain. Ez jelentős mértékben annak köszönhető, hogy az APT tevékenység nem folyamatos, hanem perzisztens. Vagyis az áldozat rendszereit védő kiberbiztonsági szakemberek és kibervédelmi rendszerek nem szembesülnek folyamatos anomáliákkal, ami alapján a támadás észlelhető lenne. Az APT tevékenység jellemzően visszatérő megfigyelést és adatlopást takar magasfokú reagálóképességgel (reaktívitás) kombinálva. Így a kibervédelmi intézkedésekre gyors válaszlépések adhatók, a művelet fenntartható marad.

Megállapítottam, hogy az APT tevékenységek több alkalommal bizonyították, hogy képesek a virtuális és fizikai világ közötti határok átlépésével hatásokat kiváltani, ezért súlyos fenyegetést jelentenek az államok politikai-társadalmi berendezkedésére. Geopolitikai, energiabiztonsági és egyéb célok mentén képesek szenzitív információkat megszerezni, manipulálni vagy akár bomlasztó hatást kiváltani, miközben a letagadhatóság olyan magas szintje érvényesül, amivel egyetlen fizikai művelet sem képes versenyezni. Mindez hozzájárul az eszkaláció elkerüléséhez és alacsonyan tartja a megtorlás kockázatát, ami kifejezetten előnyös eszközzé teszi a kiberműveleti

képességeket azokban az esetekben, amikor a nemzeti érdekek érvényesítése egy másik állam kárára történik.

Miután több paramétert meghatároztam az APT tevékenységekkel összefüggésben, amelyek külön-külön is jelentős mértékben növelni képesek a hatékonyságot, ezeket összevetettem a védelmi szektor különleges műveleti képességeinek paramétereivel. A vizsgálat nyomán megállapítottam, hogy az egyes területek különleges és speciális képességei ágazatok szerint, a tevékenységi területnek megfelelően jól elkülöníthetők, ugyanakkor vannak átfedések, amik esetenként szoros kapcsolatra, illetve tudástranszferre utalnak. A haderőkben létrehozott és a vizsgálat részét képező különleges műveleti képességeket alapvetően idegen államok területén, konfliktussal sújtott övezetekben, vitatott hovatartozású térségekben alkalmazzák. Belföldön csak rendkívüli esetekben, megfelelő felhatalmazás és jogi szabályozás alapján kerülnek bevetésre. Jellemzően terrorelhárítási, hírszerzési, kimenekítési és kiképzési feladatokat látnak el meglehetősen mostoha körülmények között. Ezért a haderők különleges műveleti beavatkozóit arra képzik ki, hogy akár több napig képesek legyenek utánpótlás, ellátás és bármilyen külső segítség nélkül, kis csoportban tevékenykedve végrehajtani feladataikat. A végrehajtás sikerének növelése, illetve lelepleződés esetén a letagadhatóság miatt a küldetések és akciók szinte kizárólag fedett körülmények között zajlanak, továbbá kiemelkedő hadműveleti, stratégiai és politikai jelentőséggel bírnak.

A rendvédelmi szervek esetében a létrehozott és vizsgált különleges képességeket szinte kizárólag belföldön, illetve olyan területeken alkalmazzák, ahol az állam joghatósággal rendelkezik. Legfőképp terrorelhárítási, illetve bűnfelderítési- és felszámolási feladatok során kerülnek bevetésre, így merényletek, túszmentések, különösen veszélyes bűnözők elfogása közben azonosíthatók a rendvédelmi különleges képességek. A rendvédelem különleges alakulatainak tagjait arra készítik fel, hogy kis csoportban tevékenykedve képesek legyenek terroristák és felfegyverzett bűnözők bármilyen körülmények között történő ártalmatlanítására és elfogására, az áldozatok testi épségének megőrzésére és a túszok kimenekítésére, kijelölt objektumok és személyek védelmére, illetve rendőri megfigyelésre. Az alakulatok tagjai gyakran inkognitóban végzik tevékenységüket és sok esetben az alkalmazott eszközök és módszerek is minősítettek annak érdekében, hogy az ellenérdekelt felek számára ne legyenek kiszámíthatóak a tevékenység egyes elemei. A különleges rendvédelmi tevékenység fedett jellege ellenére azonosíthatók olyan

összetevők, így például a mesterlövész, a tűzszerész vagy a taktikai kutya alkalmazása, amelyek egyfelől megtalálhatók a katonai különleges műveleti képességek eszköztárában is, másfelől a műveleti területen alkalmazott módszerek és eljárások közötti átfedések miatt nem ritkák a közös gyakorlatok.

A nemzetbiztonsági szolgálatok tevékenysége önmagában speciálisnak tekinthető az alapvető honvédelmi és rendvédelmi tevékenységek körülményeihez képest, mivel az orientáció lehet külföldi és belföldi egyaránt, illetve egyéb módon specializált, továbbá itt a leginkább kiterjedt a tevékenység fedett jellege. A nemzetbiztonsági szolgálatok tagjainak a másik két ágazathoz hasonlóan különleges elvárásoknak kell megfelelniük és elvárt az átlagon felüli teljesítmény. Idegen környezetben általában a helyi elhárítással szemben kell hatékony hírszerző vagy befolyásoló tevékenységet folytatni, míg belföldön más országok azonos tevékenységének leleplezése és akadályozása a cél. Továbbá mindkét területen megjelenik a terrorizmus elleni harc, illetve a szervezett bűnözéssel szembeni fellépés. Feladataik ellátásához a nemzetbiztonsági szolgálatok tagjai az átlagon felüli ismereteik és képességeik mellett máshol nem elsajátítható ismeretekre és képességekre is szert tesznek, jellemzően a szolgálatok saját oktatási bázisán. Ezek egyebek mellett tartalmaznak humán és technikai hírszerzési fortélyokat, terrorelhárítási módszereket, illetve titkosszolgálati eszközök és eljárások alkalmazásában való jártasságot. A nemzetbiztonsági szolgálatok sikeres működésének egyik alapvető mértéke, hogy tevékenységüket mennyire képesek leplezni, így sok esetben egy nagy horderejű bűncselekmény vagy egy terrorhálózat leleplezése esetén is rejtve marad a nemzetbiztonsági szál és a közreműködő szolgálatok szerepe, ami a politikailag jelentős nemzetbiztonsági ügyek esetén is elmondható, mivel a letagadhatóság ebben az esetben is fontos szempont.

A vizsgált honvédelmi, rendvédelmi és nemzetbiztonsági különleges képességekkel összefüggésben a tevékenységekre leginkább jellemző paraméterek összefüggéseit és a párhuzamokat táblázatban mutattam be. Egyúttal a táblázatba bekerültek az APT tevékenységek azonos paraméterei, amik a dominancia alapú megközelítéssel összehasonlíthatóvá váltak a különleges műveleti paraméterekkel. A táblázatba a vizsgálat tárgyát képező paraméterek kerültek be: a tevékenység fedett jellege, jelentősége (politikai, stratégiai, nagy horderejű), a végrehajtás helye (belföld, külföld) és a végrehajtókkal (beavatkozók, operátorok, felszámolók, ügynökök,

közreműködők) szembeni elvárások (fizikai, pszichikai, biztonsági, képzettség), valamint a tevékenység intervalluma (rövid idejű, folyamatos).

A biztonság- és védelempolitikai elemzéseknek és kutatásoknak – a védelmi tervezéshez és képességfejlesztéshez hasonlóan – szerves része az erőkkel összefüggő átfogó értékelés, ami jellemzően előre meghatározott szempontrendszer alapján történik. A kiber különleges műveleti erők létjogosultságának vizsgálatát a kinetikus különleges műveleti erők kihívásaival kezdtem, ami kettős képet mutat abban a tekintetben, hogy míg hazai viszonylatban egyelőre nem elképzelhető a robosztus kiberműveleti képesség különleges erők keretén belül történő kialakulása, az Egyesült Államokban aktív vita folyik arról, hogy a speciális kibermissziókban szerepet vállaló egységek a kiberműveleti vagy a különleges műveleti parancsnokság alárendeltségében jöjjenek létre. Nem azonosítottam olyan szempontot vagy megoldást, ami alapján egyértelműen állást lehetne foglalni a különböző megközelítések, illetve elképzelések valamelyike mentén. A stratégiai és műveleti szintek vizsgálatával rávilágítottam, hogy a nemzetközi rendszer állapota és a kibertér adta lehetőségek az államok egy részénél olyan viselkedési minták létrejöttét generálja, amit a nemzetközi jog szabályrendszere nem képes követni és kontrollálni, ezért az érdekek sérülése esetén jelentősen korlátozódik a válaszadáshoz alkalmazható hagyományos eszközrendszer.

Megállapítottam, hogy a kiberműveletek teljes spektrumában alkalmazható képesség kialakítása értelmezhető a nemzetközi kapcsolatok kiberdimenziójában kialakult anarchikus állapotokra történő válaszadásként, amit manapság leginkább a nagyhatalmak között zajló „kiberháború" kifejezéssel szokás leírni. Bár hadtudományi szempontból a háborús narratíva alkalmazása helytelen, a kutatás által feltárt állami, illetve állami támogatású szervezetek kiberműveleti képességei egyértelműen elérik azt a szintet, amivel bizonyos esetekben a kinetikus támadásokkal összemérhető hatásokat képesek kiváltani gyorsabban, költséghatékonyabb módon és a kibertér kínálta aszimmetria kiaknázásának maximalizálásával.

Következtetéseim alapján ennek lehetőségét egyfelől a nemzetközi jogi rendszer hiányosságai teremtik meg, másfelől a kibertér sajátos jellege, aminek révén rendkívül nehéz teljes bizonyossággal meghatározni, hogy ki az agresszor. Várhatóan a nemzetközi jog még évtizedekig képtelen lesz a technika fejlődését beérni, ezért reális alternatíva lehet minden állam számára, hogy érdekeinek védelme és érvényesítése érdekében a hagyományos képességek mellett kiberműveleti képességeket fejlesszen.

Arra vonatkozóan, hogy a kiberműveleti képességek kialakítása során milyen integrációs sémák alkalmazása kínál magasfokú hatékonyságot, egyszerű beágyazhatóságot vagy épp letagadhatóságot, több alternatívát is megvizsgáltam. A vizsgálat nyomán megállapítottam, hogy a katonai, nemzetbiztonsági, önálló félkatonai, illetve szerződéses modellek mindegyike szép számban rendelkezik előnyökkel és hátrányokkal, amelyeket minden szereplőnek mérlegelnie kell a képességek kialakítása előtt, hogy kiválaszthassa a számára leginkább kedvező megoldást. Az interjúk és a szakirodalmi vizsgálatok alapján a katonai és nemzetbiztonsági integrációval öröklődő robosztus szervezeti háttérrel és az ebből fakadó bonyolult hierarchiával és lassúsággal szemben mindenképpen előnyösebb az önálló félkatonai vagy a szerződéses modell alkalmazása, azonban mindegyik esetben további elemzésre és értékelésre van szükség, hogy pontosabb képet lehessen alkotni az előnyökről és hátrányokról abban az adott közegben, ahol a képesség kialakításra kerül.

A kiberműveleti képességekkel összefüggésben a humánerőforrás jelentőségét abszolút prioritásként kezelve, a rendelkezésre álló szakirodalom és jelentős mértékben az interjúk alapján meghatároztam a kiber különleges képességek létrehozásához szükséges követelményrendszer alapjait. Arra a következtetésre jutottam, hogy a technikai, mentális és fizikai alkalmasság terén is további kutatás szükséges annak érdekében, hogy a követelményrendszer pontosítható legyen. Az egyedi elvárásokon túl további két szempontot is meghatároztam. Ezek egyfelől az interoperabilitás jelentősége különösen olyan esetekben, amikor a kiberműveleti képesség önálló félkatonai vagy szerződéses modellként valósul meg. Másfelől a kiberbiztonsági iparágban kialakult szakember hiány egy olyan tényező, ami várhatóan még évekig velünk marad, így mindenképpen számításba kell venni a kiber különleges műveleti képesség kialakításának tervezésekor.

Kutatásom utolsó feladata az volt, hogy a kiber különleges műveleti képességgel összefüggésben megvizsgáljam a felkészítés és kiképzés, valamint a képesség fenntarthatósága, illetve komponensei kapcsán azokat a tényezőket, amelyek segítségével egy képességfejlesztési keretrendszer alapjai meghatározhatók. A kutatás ezen részében jelentős mértékben az interjúkérdésekre kapott válaszokra hagyatkoztam, továbbá beépítésre kerültek a kutatás során feltárt kapcsolódó információk is. Az interjúalanyok szakmai tapasztalata átfogó kép megalkotását tette lehetővé számomra, így sikerrel tudtam körülhatárolni azokat a területeket, amelyek a kiberműveletek gerincét adják. Továbbá meghatároztam azokat az erőforrásokat és egyéb feltételeket, amelyek a hatékony működéshez nélkülözhetetlenek.

Az első hipotézis (H1) állítását, miszerint a jelenlegi stratégiai környezetben az államok nyíltan nem, vagy csak részben vállalják fel azokat a kiberműveleti képességeket, amelyeknek teljes spektrumához hozzá tartozik az arányos válaszadáshoz szükséges megelőző és ellentámadási kapacitás, a stratégiai források alátámasztották, ami a kutatás egyik kiindulópontját adta. Ehhez kapcsolódóan – az első és második célkitűzésemmel összefüggésben – megállapítottam, hogy a nyílt stratégiákban megjelenő percepciók és képességek alapján nehéz, sokszor csak korlátozottan lehetséges összevetni és értékelni az egyes országok ambíció szintjét a kiberműveletek teljes spektrumán elhelyezkedő képességekhez viszonyítva. Az első hipotézis kapcsán megfogalmazott kérdésre[134] a válasz az, hogy jelentős eltérések azonosíthatók a vizsgált országok nyíltan felvállalt ambíciószintjei tekintetében a kibervédelmi képességekkel összefüggésben, amit jelentős mértékben befolyásol az adott ország kiberbiztonsági percepciója, a kibervédelmi szektor érettsége, valamint a gazdasági potenciál.

A második hipotézis (H2) állítását, miszerint az ismert fejlett perzisztens fenyegetések (Advanced Persistent Threat – APT) több jellemzője is azonosítható, amelyek hasonlóságot, illetve párhuzamot mutatnak a kinetikus tartományban alkalmazott különleges műveleti erőkkel és képességekkel, a komparatív módszertan igazolta, ami a kutatás egyik pillérét adja. Ehhez kapcsolódóan – a második és harmadik célkitűzésemmel összefüggésben – megállapítottam, hogy ugyanaz a tevékenység különböző aspektusból vizsgálva kiberműveleti képesség és kiberfenyegetés egyaránt lehet, ezért a fejlett perzisztens fenyegetések felfoghatók kiberműveleti képességként. A stratégiai dokumentumokból megismert kihívások és fenyegetések kártékonyságát és kifinomultságát a kiberműveleti képességek fejlődését bemutató esettanulmányok alátámasztják, mivel az látható, hogy fejlett képességek kerültek kialakításra, ami az ellenfél szemszögéből kihívásként, illetve fenyegetésként értékelhető. Továbbá a különleges műveleti képességek és a fejlett perzisztens fenyegetések jellemzőinek dominancia alapú összevetése alátámasztotta a párhuzamokkal kapcsolatban megfogalmazott feltételezéseimet. A második hipotézis kapcsán megfogalmazott kérdésre[135] a válasz az, hogy igen, az APT-k felfoghatók a kibertér különleges műveleti erőiként annak ellenére is, hogy sokszor a politikai

[134] Milyen szintet mutat a kibervédelmi képességek nyíltan felvállalt fejlesztésére vonatkozó ambíció a vizsgált országok és szervezetek tekintetében?
[135] A szükséges politikai felhatalmazással a nemzeti érdekek védelmében tevékenykedő APT-k felfoghatók-e a kibertér különleges műveleti erőiként?

felhatalmazás további egyértelműsítést igényelne és a nemzeti érdekek védelmében folytatott tevékenységet kétségek övezhetik.

A harmadik és negyedik célkitűzésemhez kapcsolódó harmadik hipotézis (H3) állítását, miszerint a kiberműveletek teljes spektrumát lefedő képességek megelőző és ellentámadási feladatok ellátására alkalmas elemeinek kialakítására létrehozható egy keretrendszer, amely a kinetikus különleges műveleti képességekhez mérhető speciális megközelítéssel valósítható meg, a kutatást kiegészítő irányított interjúk igazolták, ami a kutatás másik pillérét adja. A kiberműveletek teljes spektrumában tevékenykedni képes kiber különleges műveleti erők kialakításának elősegítésére megalkottam egy indikátor alapú modellt, illetve az egyén szintjén azonosított analógiák alapján a vizsgálatot kiterjesztettem a felkészítés, a fenntarthatóság és az erőforrás igények összehasonlítására, amivel beazonosíthatókká váltak a kiber különleges műveleti képességek kialakításában alapvető fontosságú strukturális elemek. A harmadik hipotézis kapcsán megfogalmazott kérdésre [136] a válasz az, hogy a keretrendszer alapját az adott ország kiberfenyegetettségi mátrixa és a hosszútávú politikai elhatározás mellett a szükséges pénzügyi források biztosítása jelenti, amit tartalmi elemként az alkalmazott integrációs modell meghatározása és a humán erőforrás kérdéskörének kiemelt kezelése követ. A kiberműveletek teljes spektrumában tevékenykedni képes kiber különleges műveleti képesség nem lehet sikeres robosztus kiberhírszerzés (CTI), offenzív műveleti komponens, illetve támogató és K+F komponens nélkül.

[136] Milyen tartalmi elemekkel bíró keretrendszer megteremtésével valósítható meg a kiber különleges műveleti képességek sikerrel történő létrehozása és fejlesztése?

VIII. Új tudományos eredmények

A kiber különleges műveleti képességeket vizsgáló értekezésem az alábbi új tudományos eredményeket tartalmazza:

1. Feltártam a kiberbiztonsági stratégiák célzott, kvalitatív elemzésével a dokumentumok kiberműveleti képességekre vonatkozó részeit, **összegeztem** a kiberműveleti képességek offenzív és defenzív jellegére utaló információkat és a tapasztaltak alapján **következtetéseket fogalmaztam meg**, a valós kiberműveleti képességek és ambíció szint megismerésének korlátjaira vonatkozóan.

2. Azonosítottam a kiberbiztonsági kihívások közül a fejlett perzisztens fenyegetéseket és **igazoltam**, hogy a legsúlyosabb ismert kiberbiztonsági incidensek köthetők hozzájuk, továbbá a legkifinomultabb eszközöket, módszereket, illetve eljárásokat alkalmazva érik el a céljukat. Ez alapján **meghatároztam** a honvédelmi, rendvédelmi és nemzetbiztonsági szektorok különleges műveleti körülményei, valamint a fejlett perzisztens fenyegetések működési paraméterei közötti analógiákat, ami alapján **kidolgoztam** a kiber különleges műveleti tevékenységek egyedi feltételrendszerét.

3. Igazoltam a kiber különleges műveleti képességek létjogosultságát és a nemzeti érdekek hatékonyabb érvényesítésének elősegítésére, **javaslatot tettem** a kiber különleges műveleti képességek elhelyezésére a nemzeti képességfejlesztés szintjén, a nemzeti érdekérvényesítés eszköztárának elemeként.

4. Komparatív módon értékeltem a honvédelmi, rendvédelmi és nemzetbiztonsági ágazat különleges képességeinek, valamint a kiber különleges műveleti képességek sajátosságait, **rámutattam** azokra a paraméterekre, amelyek alapot biztosíthatnak a szervezeti integráció, a struktúra és a feltételrendszer kialakításához és **megalkottam** a teljes spektrumú kiberműveletek indikátor alapú modelljét.

IX. Az értekezés kutatási és tudományos eredményeinek felhasználhatósága

Az elvégzett kutatás alapján elkészített értekezés eredményei az alábbi területeken használatók fel:

- Szakpolitikai területen: Az értekezés stratégiai szintű képet alkot a kiberműveleti képességfejlesztéssel összefüggő elképzelésekről és az együttműködési lehetőségek formáiról. Feltárja a kiberműveleti képességek beágyazottságát a vizsgált országok védelmi szektorainak szintjén, valamint a kiberfenyegetésekhez kapcsolódó nemzeti percepciókat. Ehhez kapcsolódóan a kiberműveleti képességek nincsenek leírva nyílt, megismerhető forrásokban, ezért indirekt módon lehet következtetéseket levonni. Ezek nem konkrét képességekre vonatkoznak, hanem a felhasználás jellegére utalnak. Ez a jelleg meghatározó a kiberműveletek fenyegetésként, illetve képességként történő megítélésekor is. Ebből kiindulva a fejlett perzisztens fenyegetések egyúttal a kiberműveleti képességek speciális elemeként értelmezhetők és párhuzamba állíthatók a kinetikus különleges műveleti képességekkel. Ezen ismeretek elősegítik a kiber különleges műveleti képességek kialakítását, a szükséges feltételrendszer megteremtését és a kapcsolódó tervezési folyamat felgyorsítását. A kiber különleges műveleti képességeket eredményesen kialakító és alkalmazó országok eljárásainak és módszereinek ismerete növeli a szakpolitikai tervezés és döntéshozatal hatékonyságát és segíti a szükséges koordinációs tevékenységet, míg a hiányosságok azonosítása hozzájárul a hátráltató tényezők kiküszöböléséhez.
- Alkalmazott kutatásokban: Az értekezés Magyarországon eddig nem, vagy csak minimálisan kutatott területtel – a kiber különleges műveleti képességekkel – foglalkozik, így jelentős mértékben feltáró jellegű, kisebb részben pedig az elérhető nemzetközi szakirodalomra építve szintetizáló, elemző és értékelő jellegű. Kvalitatív és komparatív kutatásmódszertana – elsősorban a stratégiai vizsgálat, valamint a fejlett perzisztens fenyegetések és a különleges műveleti képességek terén – a hadtudományban újszerű, a szerző és az irányított interjúk szakértői köre által végzett kutatások és gyakorlati tapasztalatok szintetizálásának eredményét összegzi. A hasonló

fókuszú és tematikájú alkalmazott kutatásokhoz mintaként szolgálhat és módszertani alapot biztosít.

- Oktatásban és kiképzésben: A kutatás során feltárt és szintetizált nemzetközi szakirodalmi források beemelése a hadtudományi, a biztonság- és védelempolitikai, valamint a kiberbiztonsági és különleges műveleti felkészítési területre olyan új ismereteket biztosít a jövő szakembereinek a védelmi szférában és azon túl, amelyekre a – kiberbiztonsági szakemberhiány okán – már rövid távon jelentős igény mutatkozhat. Az értekezés ismeretanyagának és forrásainak jelentős része csak idegen nyelven érhető el, így a magyar szakirodalomban nem szerepeltek, ezért a kapcsolódó képzési tematikák frissítéséhez felhasználhatók.

X. Ajánlások

A kutatás eredményei a megválaszolt tudományos felvetések mellett újabb kérdéseket is felvetnek a kiberműveletekkel összefüggésben. Ezeknek egy része azokhoz a kibertérben vagy kibertéren keresztül folytatott tevékenységekhez és kiváltott hatásokhoz kapcsolódik, amelyek az egyik fél szempontjából kiberműveleti képességként definiálható, míg a másik fél számára kiberfenyegetést jelent. Azt, hogy egy stratégiai, politikai vagy katonai céllal a kibertérben megvalósuló tevékenységet a nemzetközi rendszer szereplői fenyegetésként vagy képességként értékelnek, jelentős mértékben a percepción múlik, ami függ az adott szereplő nemzetközi rendszerben elfoglalt hatalmi pozíciójától, a szövetségi rendszerektől, a kitettség mértékétől és a kibervédelem felkészültségétől is. Ez egy olyan mindenre kiterjedő globális térben, mint a kibertér várhatóan még évtizedekig korlátozni, illetve blokkolni fogja a közös érdekek és célok kialakulását a kibervédelem terén. Ugyanakkor a kibertérből érkező fenyegetésekkel szembeni fellépés és a kiberműveleti képességek fejlesztésének harmonizációja kardinális kérdés abban a tekintetben, hogy létre tud-e jönni olyan politikai és kibervédelmi együttműködés, amely képes gyakorlati eredményeket elérni a fenyegetések visszaszorításában.

Álláspontom szerint az értekezésben vizsgált témák és kérdések egy olyan folyamat korai fázisával foglalkoznak, amely meghatározó lesz a 21. század első felének biztonság- és védelempolitikai

együttműködéseiben, illetve a konfliktusok kialakulásában és kezelésében. A kibertér a hadviselés többi dimenziójához képest olyan eltérő paraméterekkel rendelkezik, amelyek átírják a hadtudomány olykor évszázados téziseit, ami a kibertérrel és a kiberműveletekkel kapcsolatos kutatások és viták szükségességére mutat rá. Ezen túlmenően az értekezés tartalmaz olyan, a magyar hadtudományi kutatás gyakorlatában újszerű megközelítést, illetve elemző és értékelő módszert, amelyek továbbfejlesztése segítheti a felmerülő kérdések megválaszolását.

A kiber különleges műveleti képességek kialakítására vonatkozó keretrendszer fejlesztésének további lépése lehet az olyan kérdéskörök mélyreható nemzeti és nemzetközi szintű vizsgálata, mint például a meglévő jogrendszer alkalmazhatósága, illetve a kialakítandó jogi környezet aspektusai, a követelmények és a felkészítés lebontása elemi, illetve egyéni szintre, a működési körülmények biztosításának lehetőségei, vagy a kiberműveletek megközelítésének stratégiai szint alatti feltárása.

Ezek nyomán két területen, a témával foglalkozó alkalmazott tudományos kutatás, valamint a kiber különleges műveleti képességek kialakításában rejlő lehetőségek megismerését elősegítő szakpolitikai háttértanulmányok és döntéselőkészítő, illetve -támogató dokumentumok tekintetében további ajánlásokat fogalmazok meg.

X.1 Ajánlások a tudományos kutatás terén

A kiber különleges műveleti képességekkel foglalkozó, illetve azt vizsgálni képes interdiszciplináris, műszaki és hadtudományi kutatások újabb szegmensekkel gazdagíthatók, illetve mélyíthetők. A témakör alaposabb feltárását segíthetik a geopolitika, a nemzetközi kapcsolatok, a biztonsági tanulmányok, az informatika és további tudományterületek, amelyek leíró eszközeikkel és komparatív szemléletükkel járulhatnak hozzá a folyamathoz.

Az értekezéshez kapcsolódó tudományos kutatást a kezdetektől fogva kísérte egy erőteljes terminológiai dilemma, amely szinte mindegyik a témakörhöz kapcsolódó meghatározás esetén fennáll. Nincsenek egységesen elfogadott és alkalmazott, egyetemes definíciók a kiberbiztonság, a kibervédelem, a kiberképességek vagy épp a kiberműveletek kifejezésekre. Az értekezés csupán munkadefiníciókat használt, mivel a különböző szereplők jellemzően aktuális helyzetüknek, fejlettségüknek, érdekeiknek és szándékaiknak megfelelően igyekeznek szűkebb vagy épp tágabb

értelmezési keretet biztosítani egy-egy kifejezésnek. Ezért nagy jelentőséggel bírna egy kiterjedt és mélyreható terminológiai vizsgálat, amely képes lenne lefedni és egységes struktúrába foglalni a témakör összes meghatározását.

A kiberműveletek határokon átnyúló jellege olyan tényező, ami hangsúlyossá teszi a nemzetközi kooperációs és integrációs szinten folytatható tudományos kutatásokat. Ugyanakkor a kibertér fizikai rétegének kötöttségeiből fakadóan nem hagyhatók figyelmen kívül a nemzeti szintű megközelítések és törekvések, ahogy az alkalmazott eszközök és módszerek sem. A kiber különleges műveletek hatásainak vizsgálata tekintetében egyaránt fontos szerepe lehet a regionális és multinacionális szemléletnek. Ebben a tekintetben külön kutatási irányt képezhet a kiber különleges műveleti képesség kialakítása a Franci Idegenlégió mintájára. A kizárólag nemzeti megközelítéstől jelentős mértékben eltérő, de a nemzeti érdekérvényesítés és képességfejlesztést megtartó koncepció számos olyan kérdést vet fel, amelyekre a tudomány szolgálhat megfelelő válaszokkal.

Szűkebb értelemben az értekezéshez kapcsolódó alkalmazott hadtudományi kutatások komparatív szemlélettel vizsgálhatják a kiber különleges műveletek előnyeit és hátrányait más kinetikus képességekkel összevetve. Szintén összehasonlító kutatások végezhetők különböző országok kiberműveleti képességei kapcsán, ami elősegítheti a fejlesztési perspektívák bővítését és a szinergiák hatékony kihasználását. A stratégiai szint alatt megismerhető dokumentumok (cselekvési tervek, doktrínák, koncepciók stb.), képességfejlesztési folyamatok és programok összevetésével javaslatok fogalmazhatók meg a kiber különleges műveleti képességek struktúrájának pontosításával, a működési feltételek és a felkészítés erősítésével kapcsolatban, ugyanakkor a jelen értekezés által nem érintett területek és hiányosságok is feltárhatók.

Az értekezésben felállított szempontrendszer önmagában is hozzájárulhat a szervezeti kultúrák hasonlóságainak és különbözőségeinek alaposabb feltárásához az integráció aspektusából. Ugyanakkor továbbfejlesztéssel a szempontrendszer alkalmassá válhat a politikai támogatottság és a demokratikus kontroll mérésére, valamint az interoperabilitás különböző szintjeinek pontos definiálására. Mindez gyorsabbá, hatékonyabbá és eredményesebbé teheti a képességfejlesztést.

A kiberműveletek és a kiberfenyegetések egységes szempontok alapján történő vizsgálata rámutatott arra, hogy az, ami az egyik fél számára fenyegetés a másik fél számára képesség is lehet. Ezt a logikát követve a kiberműveletek tekintetében elméleti szinten meghatározható egy olyan

fordulópont, amely a teljes művelet életgörbéjét defenzív és offenzív oldalon egyaránt jelentősen befolyásolja. A *kiberműveleti inflekszió pont* lehet például egy nulladik napi sérülékenység felfedezése a defenzív oldalon vagy annak kiaknázása az offenzív oldalon, de további események és jelenségek is kiválthatnak fordulópontot. A tudományos kutatás terén a *kiberműveleti inflekszió pont* konceptualizálása hasznos eredményeket hozhat a defenzív és offenzív műveletek pontosabb elválasztása, illetve a közöttük fennálló összefüggések meghatározása kapcsán.

X.2 Szakpolitikai lépésekre vonatkozó ajánlások

Tudományos kutatásként a dolgozat céljai között nem szerepel a szakpolitikai döntéshozók és általában véve a védelmi közösség érintettjei számára konkrét politikai ajánlások megfogalmazása. Ugyanakkor az említett tudományos kutatómunkára vonatkozó ajánlások olyan eredményekhez vezethetnek, amelyek gyakorlati hasznosulásához a szakpolitikai transzformáció elengedhetetlen.

Az olyan államokban, amelyek a kiberműveleti képességek kialakítását nem kezdték el, vagy a képességfejlesztés korai fázisában járnak, a kiterjedt tudományos kutatások nyomán olyan dokumentum állítható össze, amely egyfajta kézikönyvként (zöld könyv) segítheti a jógyakorlatok megismerését és követését.

A tudományos kutatások regionális, multinacionális, illetve nemzetközi perspektívával rendelkező elemei – akár bilaterális vagy multilaterális keretek között – olyan kiberműveleti szakértői támogatás nyújtását teszik lehetővé, amely képes növelni a nemzetközi beágyazottságot, alkalmas arra, hogy akár saját vagy más tapasztalatokat szakpolitikai javaslat formájában becsatornázzanak a döntéshozói testületek felé.

Ugyancsak a kiberműveleti képességek kialakításával összefüggő tudományos munka gyakorlati hasznosulásának egyik formája lehet a különféle szakpolitikai fórumok, illetve koordinációs és ellenőrző bizottságok munkájának támogatása, valamint a szakértői közösségek tevékenységének tematizálása és a társadalmi párbeszéd dinamizálása.

Irodalomjegyzék

Ablon, Lillian, Libicki, Martin C. és Golay, Andrea A. 2014. „Zero-Day Vulnerabilities in the Black and Gray Markets". In: Markets for Cybercrime Tools and Stolen Data, Hackers' Bazaar, RAND Corporation. Forrás: https://www.jstor.org/stable/10.7249/j.ctt6wq7z6.11 (Elérés: 2022. március 31.).

Abrams, Lawrence. 2016. „Petya Ransomware Skips the Files and Encrypts Your Hard Drive Instead". *BleepingComputer*. Forrás: https://www.bleepingcomputer.com/news/security/petya-ransomware-skips-the-files-and-encrypts-your-hard-drive-instead/ (Elérés: 2022. április 11.).

ACSC. é.n. „Glossary". Australian Cyber Security Centre. Forrás: https://www.cyber.gov.au/acsc/view-all-content/glossary (Elérés: 2022. február 25.).

Ahmad, Atif, Webb, Jeb, Desouza, Kevin C. és Boorman, James. 2019. „Strategically-Motivated Advanced Persistent Threat: Definition, Process, Tactics and a Disinformation Model of Counterattack". *Computers & Security 86, 2019*. Forrás: https://linkinghub.elsevier.com/retrieve/pii/S0167404818310988 (Elérés: 2022. február 14.).

AIAA. é.n. „History of GPS Program". Forrás: https://www.aiaa.org/docs/default-source/uploadedfiles/about-aiaa/press-room/videos/iaf-60th-anniv-gps-nomination.pdf?sfvrsn=9bc64bfa_0 (Elérés: 2022. február 14.).

Alperovitch, Dmitri. 2011. „Revealed: Operation Shady RAT". *White Paper.* McAfee. Forrás: http://www.csri.info/wp-content/uploads/2012/08/wp-operation-shady-rat1.pdf. (Elérés: 2022. február 19.)

ATS. 1959. „The Antarctic Treaty | Antarctic Treaty". Forrás: https://www.ats.aq/e/antarctictreaty.html (Elérés: 2021. december 17.).

Baker, Kurt. 2022. „Ransomware as a Service (RaaS) Explained". CrowdStrike Forrás: https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/ (Elérés: 2022. április 27.).

Ball, Desmond. 2011. „China's Cyber Warfare Capabilities". *Security Challenges 2011 7/2*. Forrás: https://www.jstor.org/stable/26461991 (Elérés: 2022. március 24.).

Ballantyne, Iain és Povah, Nigel. 2004. „Assessment and Development Centres". Gower Publishing, Ltd. Forrás: https://books.google.ch/books?id=wWyrlcyQLyUC (Elérés: 2022. május 2.).

Barnhart, Michael, Cantos, Michelle, Johnson, Jeffery, Fox, Elias, Freas, Gary és Scott, Dan. 2022. „Not So Lazarus: Mapping DPRK Cyber Threat Groups to Government

Organizations”. Mandiant. Forrás: https://www.mandiant.com/resources/mapping-dprk-groups-to-government (Elérés. 2022. április 5.).

Bartholomew, Brian. 2017. „KopiLuwak: A New JavaScript Payload from Turla”. Forrás: https://securelist.com/kopiluwak-a-new-javascript-payload-from-turla/77429/ (Elérés: 2022. március 22.).

Bartholomew, Brian, és Guerrero-Saade, Juan Andres. 2016. „Wave Your False Flags! Deception Tactics Muddying Attribution in Targeted Attacks”. Forrás: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2017/10/20114955/Bartholomew-GuerreroSaade-VB2016.pdf (Elérés: 2022. március 22.).

Bassat, Omri Ben, és Cohen, Itay. 2019. „Mapping the Connections Inside Russia’s APT Ecosystem”. Intezer. Forrás: https://www.intezer.com/blog/malware-analysis/russian-apt-ecosystem/ (Elérés: 2022. március 22.).

Bejtlich, Richard. 2010. „What APT Is”. *Information Security Magazine*. Forrás: https://www.academia.edu/6842130/What_APT_Is (Elérés: 2022. február 18.).

Beke, József. 2020. „A magyar rendőrség különleges szolgálati ágának létrehozása, fejlődésének és működésének története 1973-1990”. In: Baráth, Noémi Emőke és Mezei József (szerk): Rendészet-Tudomány-Aktualitások. Doktoranduszok Országos Szövetsége. Forrás: https://www.dosz.hu/__doc/to_dok/120/1611930781.pdf (Elérés: 2022. március 30.).

Benito, Fer. 2020. „The History of the Internet: Pioneers, Milestones, and References”. *The Startup*. Forrás: https://medium.com/swlh/the-history-of-the-internet-pioneers-milestones-and-references-9a7816b535d8 (Elérés: 2022. február 14.).

Berzsenyi, Dániel. 2021. „Kiberbiztonság”. In: Tálas Péter Henrik Et al. (szerk.): A globalizált világ kihívásai. Nemzeti Közszolgálati Egyetem, Ludovika Egyetemi Kiadó, Budapest, 2021.

Bianco, David J. 2014. „The Pyramid of Pain”. Forrás: http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html (Elérés: 2022. május 3.).

Biasini, Nick. 2017. „The MeDoc Connection”. Forrás: http://blog.talosintelligence.com/2017/07/the-medoc-connection.html (Elérés: 2022. április 3.).

Bischoff, Paul. 2021. „5 Billion Records from Previous Data Breaches Leaked by Cybersecurity Company”. *Comparitech*. Forrás: https://www.comparitech.com/blog/information-security/breach-database-leak/ (Elérés: 2022. április 17.).

BlackBerry. 2020. „Decade of the RATs - Thank You”. Forrás: https://www.blackberry.com/us/en/forms/thank-you/decade-of-the-rats (Elérés: 2022. március 24.).

Blair, Dennis C. 2016. „Into The Grey Zone”. Project Report. Center for Cyber & Homeland Security. Forrás: https://wayback.archive-it.org/5184/20190103002934/https://cchs.gwu.edu/sites/g/files/zaxdzs2371/f/downloads/CCHS-ActiveDefenseReportFINAL.pdf (Elérés: 2022. február 26.).

Blue Horn. 2015. „CAMERASHY Closing The Aperture on China’s Unit 78020”. Threat Connect, Blue Horn. Forrás: https://cdn2.hubspot.net/hubfs/454298/Project_CAMERASHY_ThreatConnect_Copyright_2015.pdf?t=1443030820943&submissionGuid=81f1c199-859f-41e9-955b-2eec13777720 (Elérés: 2022. március 24.).

Blue Voyant. 2021. „Managing Cyber Risk Across the Vendor Ecosystem”. BlueVoyant. Forrás: https://www.bluevoyant.com/resources/managing-cyber-risk-across-the-extended-vendor-ecosystem/ (Elérés: 2022. április 18.).

BMI. 2013. „National Cyber Security Strategy - Austria”. Forrás: https://www.bmi.gv.at/504/files/130415_strategie_cybersicherheit_en_web.pdf. (Elérés: 2022. február 20.)

Brandao, Pedro Ramos. 2021. „Advanced Persistent Threats (APT)-Attribution-MICTIC Framework Extension”. *Journal of Computer Science 2021/5*. Forrás: https://thescipub.com/abstract/10.3844/jcssp.2021.470.479 (Elérés: 2022. április 1.).

Brands, Hal és Nichols, Tim. 2020. „Special Operations Forces and Great-Power Competition in the 21st Century”. American Enterprise Institute. Forrás: https://www.jstor.org/stable/resrep25369 (Elérés: 2022. március 30.).

Brown, Benjamin. 2018. „Expanding the Menu: The Case for CYBERSOC”. Forrás: https://smallwarsjournal.com/jrnl/art/expanding-menu-case-cybersoc (Elérés: 2021. július 24.).

Broyles, David A, és Blankenship, Brody. 2017. „The Role of Special Operations Forces in Global Competition”. CNA Strategic Studies. Arlington. Forrás: https://www.cna.org/archive/CNA_Files/pdf/drm-2017-u-015225-1rev.pdf (Elérés: 2022. március 30.).

Buggenhout, Erik Van, és Bauters, Jonas. 2022. „Purple Concepts - Bridging the Gap”. Forrás: https://sansorg.egnyte.com/dl/7ryuBeREwD (Elérés: 2022. május 3.).

Burkett, Randy. 2013. „An Alternative Framework for Agent Recruitment: From MICE to RASCLS”. Forrás: https://d1wqtxts1xzle7.cloudfront.net/57860600/cia-with-cover-page-v2.pdf?Expires=1649973109&Signature=WqNK5GSJ6i4WgUdC0uqG11tzV1pSy~xLP7fCm2nQRLNAxBvrWlyoxSpjlTO1egdHxYw6F87-FxE0BPgnnH3bgCAeGUxD28XV-wRxT2g-W01A1iTHqfxfPRZLIEWxg2rkG9hNvyV9dbeKTfpYxTtJnZslqRGKD2tHweKRUj6f~RGhbrGHQtqyrH5iyZ8zds0c9iVZjLOZpEWegGAyE8o3WBimU5o2phmTbdFZJMwChAimARD9mATQ1J4MVMBV8YiolqQXtDv8dJ2BWV5N~m9Zj3Cx-

IpeEyI2ObshBc1jkUIJ3QoLgd2YvIkQSUAyfY6lyCilSDWuDoidn0XLHXBKAA__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA (Elérés: 2022. április 14.).

C4ADS. 2019. „Above Us Only Stars - Exposing GPS Spoofing in Russia and Syria". C4ADS. Forrás: https://safety4sea.com/wp-content/uploads/2019/04/C4ADS-Above-us-only-start_Exposing-GPS-spoofing-in-Russia-and-Syria-2019_04.pdf (Elérés: 2022. május 4.).

Cary, Dakota. 2021. *China's National Cybersecurity Center*. CSET. Forrás: https://cset.georgetown.edu/wp-content/uploads/CSET-Chinas-National-Cybersecurity-Center-1.pdf (Elérés: 2022. február 23.).

CCDCOE. 2016. „NATO Recognises Cyberspace as a »Domain of Operations« at Warsaw Summit". Forrás: https://ccdcoe.org/incyder-articles/nato-recognises-cyberspace-as-a-domain-of-operations-at-warsaw-summit/ (Elérés: 2022. február 14.).

CCDCOE. 2018. „National Cyber Security Strategy of Ukraine". Forrás: https://ccdcoe.org/uploads/2018/10/NationalCyberSecurityStrategy_Ukraine.pdf (Elérés: 2022. február 20.).

Cerulus, Laurens. 2019. „How Ukraine Became a Test Bed for Cyberweaponry". *POLITICO*. Forrás: https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks/ (Elérés: 2022. május 26.).

CFCS. 2021. „SolarWinds: State-sponsored global software supply chain attack". Centre for Cyber Security. Forrás: https://www.cfcs.dk/globalassets/cfcs/dokumenter/rapporter/en/CFCS-solarwinds-report-EN.pdf (Elérés: 2022. április 3.).

CFR. „How Does Cyberspace Work?" *World101 from the Council on Foreign Relations*. Forrás: https://world101.cfr.org/global-era-issues/cyberspace-and-cybersecurity/how-does-cyberspace-work (Elérés: 2022. február 14.).

Chen, Ping, Desmet, Lieven és Huygens, Christophe. 2014. „A Study on Advanced Persistent Threats". In: Salinesi, Camille Et al. (szerk): Advanced Information Systems Engineering. Lecture Notes in Computer Science. Springer Berlin. Forrás: http://link.springer.com/10.1007/978-3-662-44885-4_5 (Elérés: 2022. február 17.).

CISA. 2021. „Russian SVR Targets U.S. and Allied Networks". NSA, CISA, FBI Advisory. Forrás: https://media.defense.gov/2021/Apr/15/2002621240/-1/-1/0/CSA_SVR_TARGETS_US_ALLIES_UOO13234021.PDF/CSA_SVR_TARGETS_US_ALLIES_UOO13234021.PDF (Elérés: 2022. március 22.).

Citibank. é.n. „Cybersecurity & Fraud Prevention in Today's Digital Marketplace". Forrás: https://businessaccessuat.citibank.citigroup.com/basqat/citiiwt/images/anatomyOfCyberAttack.pdf (Elérés: 2022. április 27.).

Clausewitz, Karl. 1917. *A Háborúról*. 2nd kiad. Budapest: Athenaeum Irodalmi és Nyomdai Részv.-társ. Forrás: https://mek.oszk.hu/13200/13240/pdf/13240_1.pdf (Elérés: 2022. április 19.).

Cole, Eric. 2012. „Advanced Persistent Threat: Understanding the Danger and How to Protect Your Organization". Waltham. Newnes.

Connell, Michael, és Vogler, Sarah. 2017. „Russia's Approach to Cyber Warfare". CNA. Forrás: https://www.cna.org/CNA_files/PDF/DOP-2016-U-014231-1Rev.pdf (Elérés: 2021. július 15.).

Cooper, Robert. 2000. „The Post-Modern State and the World Order". Forrás: https://www.demos.co.uk/files/postmodernstate.pdf (Elérés: 2022. március 25.).

Council of Europe. 2001. „Convention on Cybercrime". Forrás: https://rm.coe.int/1680081561 (Elérés: 2022. február 14.).

CPI. 2022. „Ukraine: A Timeline Of Cyberattacks". CyberPeace Institute. Forrás: https://cyberpeaceinstitute.org/ukraine-timeline-of-cyberattacks/ (Elérés: 2022. május 26.).

Creemers, Rogier. 2016. „National Cyberspace Security Strategy". China Copyright and Media Blog. Forrás: https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy/ (Elérés: 2022. február 23.).

Creveld, Martin van. 1991. „The Transformation of War". *Small Wars & Insurgencies. 2022/13*. The Free Press. Forrás: https://www.tandfonline.com/doi/abs/10.1080/09592310208559177?journalCode=fswi20 (Elérés: 2022. március 25.).

Crosignani, Matteo, Macchiavelli, Marco és Silva, André F. 2020. „Pirates without Borders: The Propagation of Cyberattacks through Firms' Supply Chains". *SSRN Electronic Journal*. Forrás: https://www.ssrn.com/abstract=3664772 (Elérés: 2022. április 3.).

CrowdStrike. 2014. „Putter Panda - CrowdStrike Intelligence Report". CrowdStrike. Forrás: https://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf (Elérés: 2022. február 19.)

CrowdStrike. 2016. „CSIT-16054 Targeted Malware Designed to Attack Swift Systems Discovered". TIPPER. CrowdStrike. (Elérés: 2016. december 29.)

CrowdStrike. 2019. „Global Threat Report 2019 - Adversary Tradecraft and the Importance of Speed". CrowdStrike. Forrás: https://s3.documentcloud.org/documents/5743766/Global-Threat-Report-2019.pdf (Elérés: 2022. április 28.).

CrowdStrike. 2021. „2021 Global Threat Report". CrowdStrike. Forrás: https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2021GTR.pdf (Elérés: 2022. március 24.).

CrowdStrike. 2022a. „2022 Global Threat Report: Insights from the Threat Landscape | CrowdStrike”. Forrás: https://www.crowdstrike.com/global-threat-report/ (Elérés: 2022. április 28.).

CrowdStrike. 2022b. „Adversary: Cozy Bear - Threat Actor”. Crowdstrike Adversary Universe. Forrás: https://adversary.crowdstrike.com/en-US/adversary/cozy-bear/?L=166/ (Elérés: 2022. március 22.).

CrowdStrike. 2022c. „Adversary: Venomous Bear - Threat Actor”. Crowdstrike Adversary Universe. Forrás: https://adversary.crowdstrike.com/en-US/adversary/venomous-bear/?L=166/ (Elérés: 2022. március 21.).

Cukier, Michel. 2007. „Hackers Attack Every 39 Seconds”. Forrás: https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds (Elérés: 2022. április 3.).

Cyber Command. é.n. „Command History”. Forrás: https://www.cybercom.mil/About/History/ (Elérés: 2022. március 23.).

Cyber Israel. 2021. „National Cyber Security Strategy - Israel”. Forrás: https://www.gov.il/BlobFolder/news/international_strategy/en/Israel%20International%20Cyber%20Strategy.pdf (Elérés: 2022. február 20.).

Cybrary. 2020. „Cybersecurity Skills Gap Research Report”. Cybrary. Forrás: https://www.cybrary.it/business/resources/research-papers/cybersecurity-skills-gap-research-report/ (Elérés: 2022. május 1.).

Csiki Tamás. 2008. „A stratégiai dokumentumok rendszere”. *Nemzet és biztonság - Biztonságpolitikai Szemle 2008. szeptember*. Forrás: https://nemzetesbiztonsag.hu/cikkek/csiki_tamas-a_strategiai_dokumentumok_rendszere.pdf (Elérés: 2022. február 20.)

Csiki Varga Tamás, és Tálas Péter. 2020. „Magyarország új nemzeti biztonsági stratégiájáról”. *Nemzet és Biztonság 2020/3*. Forrás: https://folyoirat.ludovika.hu/index.php/neb/article/view/4906 (Elérés: 2022. február 20.).

De Falco, Marco. 2012. „Stuxnet Facts Report - A Technical and Strategic Analysis”. CCDCOE. Forrás: https://ccdcoe.org/uploads/2018/10/Falco2012_StuxnetFactsReport.pdf (Elérés: 2022. április 2.).

Denning, Dorothy E. 2014. „Framework and Principles for Active Cyber Defense”. *Computers & Security 2014/40*. Naval Postgraduate School. Forrás: https://linkinghub.elsevier.com/retrieve/pii/S0167404813001661 (Elérés: 2022. február 25.).

DeSombre, Winnona, Campobasso, Michele, Allodi, Luca, Shires, James, Work, JD, Morgus, Robert, O'neill, Patrick Howell és Herr, Trey. 2021. „A Primer on the Proliferation of Offensive Cyber Capabilities”. *Issue Brief 2021/03*. Scowcroft Center for Strategy And

Security. Atlantic Council. Forrás: https://www.atlanticcouncil.org/wp-content/uploads/2021/03/A-Primer-on-the-Proliferation-of-Offensive-Cyber-Capabilities.pdf (Elérés: 2022. március 23.).

Dewar, Robert S. 2017. „Active Cyber Defense". CSS Cyber Defence Trend Analysis 1. Center for Security Studies, ETH Zürich. Forrás: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2017-03.pdf (Elérés: 2022. február 27.).

DFS NY. 2021. „Report on the SolarWinds Cyber Espionage Attack and Institutions' Response". New York State Department of Financial Services. Forrás: https://www.dfs.ny.gov/system/files/documents/2021/04/solarwinds_report_2021.pdf (Elérés: 2022. április 3.).

DIA. 2017. „Russia Military Power". DIA. Forrás: https://www.dia.mil/Portals/110/Images/News/Military_Powers_Publications/Russia_Military_Power_Report_2017.pdf (Elérés: 2022. március 22.).

DIA. 2021. „North Korea Military Power: A Growing Regional and Global Threat". Forrás: https://purl.fdlp.gov/GPO/gpo172971 (Elérés: 2022. április 5.).

Digital Slovenia. 2016. „National Cyber Security Strategy - Slovenia". Forrás: https://www.gov.si/assets/ministrstva/MJU/DID/Cyber_Security_Strategy_Slovenia.pdf (Elérés: 2022. február 20.).

Dihen, Mihály. 2020. „A magyar polgári hírszerzés előtt álló kihívások a 21. század elején". *Nemzetbiztonsági Szemle 2020/1*. Forrás: https://folyoirat.ludovika.hu/index.php/nbsz/article/view/1389 (Elérés: 2022. március 18.).

Dillon, Sean, és Davis, Dylan. 2017. „Eternal Blue - Exploit Analysis and Port to Microsoft Windows 10". RiskSense. Forrás: http://risksense.com/download/datasets/4353/EternalBlue_RiskSense%20Exploit%20Analysis%20and%20Port%20to%20Microsoft%20Windows%2010_v1_2.pdf (Elérés: 2022. április 11.)

Dimitriadis, Christos. 2016. „Cyber Security Snapshot 2016". ISACA. Forrás: https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2016/cybersecurity-snapshot-cyberthreats-regulations-workforce-issues-in-2016 (Elérés: 2022. február 16.).

DNI. 2022. „Annual Threat Assessment of the U.S. Intelligence Community 2022". Forrás: https://www.dni.gov/files/ODNI/documents/assessments/ATA-2022-Unclassified-Report.pdf (Elérés: 2022. március 18.).

Dobák, Imre, és Kovács, Zoltán. 2014. „Új technológiák hatása a hírszerzésre". In: Dobák Imre (szerk.): A nemzetbiztonság általános elmélete. NKE. Nemzetbiztonsági Intézet. Budapest. Forrás: https://tudasportal.uni-nke.hu/xmlui/static/pdfjs/web/viewer.html?file=https://tudasportal.uni-

nke.hu/xmlui/bitstream/handle/20.500.12944/8567/Teljes%20sz%c3%b6veg%21?sequence=2&isAllowed=y (Elérés: 2022. március 18.).

DOD Australia. 2014. „Defence Capability Development Handbook (DCDH) 2014”. Forrás: https://defence.gov.au/publications/docs/Defence%20Capability%20Development%20Handbook%20(DCDH)%202014%20-%20internet%20copy.pdf (Elérés: 2022. március 11.).

DOD US. 2009. „The Cyber Warfare Lexicon”. Forrsá: https://info.publicintelligence.net/USSTRATCOM-CyberWarfareLexicon.pdf (Elérés: 2022. február 25.).

DOD US. é. n. „DOD Dictionary of Military and Associated Terms”. Forrás: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf (Elérés: 2022. február 26.).

DOJ US. 2014. „U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage”. Forrás: https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor (Elérés: 2022. április 1.).

DOJ US. 2018. „Indictment - Columbia”. Forrás: https://www.justice.gov/file/1080281/download (Elérés: 2022. március 22.)

DOJ US. 2020. „Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace”. Forrás: https://www.justice.gov/opa/press-release/file/1328521/download (Elérés: 2022. március 22.).

Domingo, Francis. 2016. „Review Essay: China’s Engagement in Cyberspace”. *Journal of Asian Security and International Affairs. 2016/08.* Forrás: https://www.researchgate.net/profile/Francis-Domingo/publication/305709946_Review_Essay_China's_Engagement_in_Cyberspace/links/5a17722ba6fdcc50ade613eb/Review-Essay-Chinas-Engagement-in-Cyberspace.pdf?origin=publication_detail (Elérés: 2022. március 24.)

Duggan, Patrick és Oren, Elizabeth. 2016. „U.S. Special Operations Forces in Cyberspace”. Forrás: https://www.soc.mil/SWCS/SWmag/archive/SW2902/SOF%20in%20Cyberspace.pdf (Elérés: 2022. április 27.).

Ehrlich, Ev. 2014. „A Brief history of Internet Regulation”. Forrás: https://www.progressivepolicy.org/wp-content/uploads/2014/03/2014.03-Ehrlich_A-Brief-History-of-Internet-Regulation.pdf (Elérés: 2022. február 14.).

Ellis, Jamie M. 2015. „Chinese Cyber Espionage: A Complementary Method to Aid PLA Modernization”. Naval Postgraduate School. Forrás: https://www.hsdl.org/?view&did=790444 (Elérés: 2022. március 24.).

ENISA. 2014. „Advanced persistent threat incident handling - Toolset, Document for teachers”. Forrás: https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/advanced_persistent_threat_incident_handling_toolset (Elérés: 2022. február 18.).

ENISA. 2015. „National Cyber Security Strategy - Croatia”. Forrás: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CRNCSSEN.pdf (Elérés: 2022. február 22.).

ENISA. 2016. „ENISA Threat Taxonomy”. Forrás: https://data.europa.eu/data/datasets/enisa-threat-taxonomy-1?locale=en (Elérés: 2022. február 16.).

ENISA. 2017. „Supply Chain Attacks”. *ENISA*. Forrás: https://www.enisa.europa.eu/publications/info-notes/supply-chain-attacks (Elérés: 2022. április 3.).

ENISA. 2018. „National Cyber Security Strategy - Netherlands”. Forrás: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map (Elérés: 2022. február 20.).

ESET. 2018. „LOJAX - First UEFI Rootkit found in the Wild, Courtesy of the Sednit Group”. ESET. Forrás: https://www.welivesecurity.com/wp-content/uploads/2018/09/ESET-LoJax.pdf (Elérés: 2022. február 18.).

ESET. 2019. „Turla Lightneuron - One Email Away from Remote Code Execution”. ESET. Forrás: https://www.welivesecurity.com/wp-content/uploads/2019/05/ESET-LightNeuron.pdf (Elérés: 2022. március 21.).

EU. 2020a. „A biztonsági unióra vonatkozó uniós stratégia”. Forrás: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52020DC0605&from=EN (Elérés: 2022. február 20.).

EU. 2020b. „A TANÁCS (EU) 2020/1536 VÉGREHAJTÁSI RENDELETE (2020. október 22.) az Uniót vagy annak tagállamait fenyegető kibertámadások elleni korlátozó intézkedésekről szóló (EU) 2019/796 rendelet végrehajtásáról”. Forrás: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32020R1536&from=EN (Elérés: 2022. március 22.)

Faou, Matthieu. 2020. „Turla Crutch: Keeping the “Back Door” Open”. *WeLiveSecurity*. Forrás: https://www.welivesecurity.com/2020/12/02/turla-crutch-keeping-back-door-open/ (Elérés: 2022. március 21.).

Fehér András Tibor, és Négyesi Imre. 2021. „Mesterségesintelligencia-alapú kibertértámadási modellek”. *Műszaki Katonai Közlöny 2021/3*. Forrás: https://folyoirat.ludovika.hu/index.php/mkk/article/view/5495 (Elérés: 2022. február 16.).

Feickert, Andrew. 2022. „U.S. Special Operations Forces (SOF): Background and Issues for Congress”. CRS. Forrás: https://sgp.fas.org/crs/natsec/RS21048.pdf (Elérés: 2022. március 29.).

Fenyvesi Beáta. 2019. „Speciális alakulat”. Forrás: https://www.police.hu/hu/hirek-es-informaciok/legfrissebb-hireink/zsaru-magazin/specialis-alakulat (Elérés: 2022. március 30.).

Ferguson, Tom. 1991. „Modern Law Enforcement Weapons & Tactics”. Forrás: https://vdoc.pub/download/modern-law-enforcement-weapons-and-tactics-nelngdavh7k0 (Elérés: 2022. április 12.).

Finszter Géza. 2010. „A rendészeti stratégia alkotmányos alapjai”. Forrás: http://pecshor.hu/periodika/hatarkovek/finszter.pdf (Elérés: 2022. február 20.).

Firch, Jason. 2020. „10 Cyber Security Trends You Can’t Ignore In 2021”. *PurpleSec*. Forrás: https://purplesec.us/cyber-security-trends-2021/ (Elérés: 2022. április 17.).

FireEye. 2014. „APT28: A Window Into Russia’s Cyber Espionage Operations?”. FireEye. Forrás: https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf (Elérés: 2022. március 22.).

FireEye. 2017. „APT28: At the Center of the Storm - Russia Strategically Evolves Its Cyber Operations”. FireEye. Forrás: https://www.mandiant.com/sites/default/files/2021-09/APT28-Center-of-Storm-2017.pdf (Elérés: 2022. március 22.).

FIRST. é.n. „Introduction to CTI as a General topic / Cyber Threat Intelligence SIG Curriculum”. Forum of Incident Response and Security Teams. Forrás: https://www.first.org/global/sigs/cti/curriculum/cti-introduction (Elérés: 2022. május 3.).

Forgács Balázs. 2009. „A hadikultúra fogalmának historigráfiája II.” *Hadtudományi Szemle 2009/3*. Forrás: http://epa.oszk.hu/02400/02463/00006/pdf/EPA02463_hadtudomanyi_szemle_2009_3_001-008.pdf (Elérés: 2022. április 10.).

Forgács Balázs. 2017. „A háború és a politika viszonyrendszere”. In: Gőcze István (szerk.): Az igazságos háború elvétől az igazságos békéig. Dialóg Campus. Forrás: http://real.mtak.hu/85130/1/123_Forgacs_A_haboru_es_a_politika_viszonyrendszereAz_igazsagos_haboru_elvetol_az_igazsagos_bekeig.pdf (Elérés: 2022. április 19.).

Forray, László. 2012. „A Magyar Honvédség különleges műveleti képessége, a katonai erők alkalmazásának keretei között”. *Hadtudományi Szemle 2012/1-2*. Forrás: https://epa.oszk.hu/02400/02463/00012/pdf/EPA02463_hadtudomanyi_szemle_2012_1-2_010-028.pdf (Elérés: 2022. március 29.).

Forray László, és Gerőcs Imre. 2013. „A magyar különleges műveleti erők alkalmazásának módszerei a kiritikus infrastruktúra biztosítása érdekében”. *Repüléstudományi Közlemények 2013/2*. Forrás:

http://www.repulestudomany.hu/kulonszamok/2013_cikkek/2013-2-18-Forray_Laszlo-Gerocs_Imre.pdf (Elérés: 2022. március 29.).

F-Secure. 2020. „The Dukes - 7 Years of Russian Cyberespionage". F-Secure. Forrás: https://blog-assets.f-secure.com/wp-content/uploads/2020/03/18122307/F-Secure_Dukes_Whitepaper.pdf (Elérés: 2022. március 22.).

Galeotti, Mark. 2016. „Putin's Hydra: Inside Russia's Intelligence Services". Policy Brief. European Council on Foreign Relations. Forrás: https://ecfr.eu/wp-content/uploads/ECFR_169_-_PUTINS_HYDRA_INSIDE_THE_RUSSIAN_INTELLIGENCE_SERVICES_1513.pdf (Elérés: 2022. március 21.).

Gazdag, Ferenc. 2007. „Magyarország érdekei és ezek érvényesítésének lehetőségei a nemzetközi szervezetekben (NATO, EU)". Forrás: http://www.grotius.hu/doc/pub/UIVMVC/83%20gazdag%20ferenc%20%20vita%20a%20magyar%20kpol.pdf (Elérés: 2022. március 17.).

Ghafir, Ibrahim, és Prenosil, Vaclav. 2014. „Advanced Persistent Threat Attack Detection: An Overview". *International Journal Of Advances In Computer Networks And Its Security, December 2014*. Forrás: https://www.researchgate.net/profile/Ibrahim_Ghafir/publication/305956804_Advanced_Persistent_Threat_Attack_Detection_An_Overview/links/57a7568008ae455e854698aa.pdf (Elérés: 2022. április 1.)

Gilpin, Robert. 2004. *Nemzetközi politikai gazdaságtan*. Bucipe.

Godwin III, James B., Kulpin, Andrey, Rauscher, Karl Frederick és Yaschenko, Valery. 2014. „Critical Terminology Foundations 2: Russia-US Bilateral on Cybersecurity". Forrás: https://www.files.ethz.ch/isn/178418/terminology2.pdf. (Elérés: 2022. február 25.)

Gomez, Elena. 2022. „Cyber Threat Intelligence Market Outlook By 2022 -2029 | Cisco, Check Point, IBM, Siemens". *The Sabre*. Forrás: https://www.marianuniversitysabre.com/2022/03/21/cyber-threat-intelligence-market-outlook-by-2022-2029-cisco-check-point-ibm-siemens/ (Elérés: 2022. március 23.).

Gottlieb, Aryea. 1987. „The Role of SOF Across the Range of Military Operations". Forrás: https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Chronicles/sofpaper.pdf (Elérés: 2022. március 29.).

Grimes, Roger A. 2019. „What Is an Advanced Persistent Threat (APT)? 5 Signs You've Been Hit". *CSO Online*. Forrás: https://www.csoonline.com/article/2615666/5-signs-youve-been-hit-with-an-apt.html (Elérés: 2022. február 17.).

Gross, Michael Joseph. 2011. „A Declaration of Cyber-War". Vanity Fair. Forrás: https://www.vanityfair.com/news/2011/03/stuxnet-201104 (Elérés: 2022. április 28.).

Hakala, Janne, és Melnychuk, Jazlyn. 2021. „Russia's Strategy in Cyberspace". Forrás: https://stratcomcoe.org/cuploads/pfiles/Nato-Cyber-Report_15-06-2021.pdf (Elérés: 2022. február 20.).

Hanson, Tom Uren, Hogeveen, Bart Fergus. 2018. „Defining Offensive Cyber Capabilities". Forrás: http://www.aspi.org.au/report/defining-offensive-cyber-capabilities (Elérés: 2022. március 27.).

Harder, Ronja. 2017. „Intelligence Services and responsibilities in good security sector governance". DCAF. Forrás: https://www.dcaf.ch/sites/default/files/publications/documents/DCAF_BG_12_Intelligence%20Services.pdf (Elérés: 2022. április 14.).

Healey, Jason. 2022. „Soldiers, Statesmen and Cyber Crises: Cyberspace and Civil-Military Relations". *Lawfare*. Forrás: https://www.lawfareblog.com/soldiers-statesmen-and-cyber-crises-cyberspace-and-civil-military-relations (Elérés: 2022. április 28.).

Hegedűs Ernő, és Hennel Sándor. 2020. „Többdimenziós (multidomain) hadműveletek". *Hadtudomány 2020/2*. Forrás: http://mhtt.eu/hadtudomany/2020/2020_2szam/003-027_Hegedus_Hennel.pdf (Elérés: 2022. június 9.).

Herr, Trey, Lee, June, Loomis, Will és Scott, Stewart. 2020. „Deep Impact: States and Software Supply Chain Attacks". Atlantic Council. Forrás: https://www.atlanticcouncil.org/commentary/feature/deep-impact-states-and-software-supply-chain-attacks/ (Elérés: 2022. április 2.).

Hodgson, Quentin E. 2018. „Understanding and Countering Cyber Coercion". In: *2018 10th International Conference on Cyber Conflict (CyCon)*, Tallinn. Forrás: https://ieeexplore.ieee.org/document/8405011/ (Elérés: 2021. július 27.).

Hoffman, Frank G. 2009. „Hybrid Threats: Reconceptualizing the Evolving Character of Modern Conflict". Forrás: https://www.comw.org/qdr/fulltext/0904hoffman.pdf (Elérés: 2022. március 25.).

Hojlo, Jeffrey. 2021. „Future of Industry Ecosystems: Shared Insights & Data." IDC Blog. Forrás: https://blogs.idc.com/2021/01/06/future-of-industry-ecosystems-shared-data-and-insights/ (Elérés: 2022. április 18.).

Horn, Bernd. 2014. „The Strategic Utility of Special Operations Forces". *Canadian Military Journal 2014, 04/14*. Forrás: http://www.journal.forces.gc.ca/vol14/no4/PDF/CMJ144Ep66.pdf. (Elérés: 2022. március 30.)

IACP. 2011. „Special Weapons and Tactics (SWAT)". International Association of Chiefs of Police. Interantional Law Enforcement Policy Center. Forrás: https://www.theiacp.org/sites/default/files/all/s/SWATPaper.pdf (Elérés: 2022. március 31.).

IBM. 2020. „Cost of a Data Breach Report 2021”. IBM. Forrás: https://www.ibm.com/security/data-breach (Elérés: 2022. április 3.).

IBM. 2021. „Incident Response Services and Threat Intelligence”. Forrás: https://www.ibm.com/security/services/ibm-x-force-incident-response-and-intelligence (Elérés: 2022. április 27.).

ICO. 2022. „National Retailer Fined Half a Million Pounds for Failing to Secure Information of at Least 14 Million People”. Forrás: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/01/nationwide-retailer-fined-half-a-million-pounds-for-failing-to-secure-information/ (Elérés: 2022. április 3.).

ICRC. 2009. „The Montreux Document”. Forrás: https://www.icrc.org/en/doc/assets/files/other/icrc_002_0996.pdf (Elérés: 2022. április 30.).

IISS. 2019. „Chapter Five: China’s Cyber Power in a New Era”. In: Asia Pacific Regional Security Assessment 2019. IISS. Forrás: https://www.iiss.org/publications/strategic-dossiers/asiapacific-regional-security-assessment-2019/rsa19-07-chapter-5 (Elérés: 2022. február 23.).

IISS. 2021. „Cyber Capabilities and National Power: A Net Assessment”. IISS. Forrás: https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power (Elérés: 2021. augusztus 11.).

Imperva. 2014. „The Non-Advanced Persistent Threat”. Forrás: https://www.imperva.com/docs/HII_The_Non-Advanced_Persistent_Threat.pdf (Elérés: 2022. április 1.).

Imperva. é.n. „DDoS for Hire - Booter, Stresser and DDoSer”. Forrás: https://www.imperva.com/learn/ddos/booters-stressers-ddosers/ (Elérés: 2022. április 27.).

ISC2. 2021. „A Resilient Cybersecurity Profession Charts the Path Forward - Cybersecurity Workforce Study 2021”. Forrás: https://www.isc2.org/-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx (Elérés: 2022. május 1.).

ITU. 2012. „National Cyber Strategy - Netherland”. Forrás: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Netherlands_2012_NDL-Cyber_StrategyEng.pdf (Elérés: 2022. március 27.).

James, Nathan. 2015. „Federal Tactical Teams”. CRS. Washington DC. Forrás: https://sgp.fas.org/crs/homesec/R44179.pdf (Elérés: 2022. március 31.).

Jaquire, Victor, és von Solms, Sebastian. 2017. „Developing a Cyber Counterintelligence Maturity Model for Developing Countries”. In *2017 IST-Africa Week Conference (IST-Africa)*, Windhoek. Forrás: http://ieeexplore.ieee.org/document/8102288/ (Elérés: 2021. július 27.).

Jinghua, Lyu. 2019. „What Are China's Cyber Capabilities and Intentions?" *IPI Global Observatory*. Forrás: https://theglobalobservatory.org/2019/03/what-are-chinas-cyber-capabilities-intentions/ (Elérés: 2022. február 23.).

Ji-Young, Kong, Lim Jong In, és Kim Kyoung Gon. 2019. „The All-Purpose Sword: North Korea's Cyber Operations and Strategies". *11th International Conference on Cyber Conflict (CyCon)*, Tallinn, Estonia. Forrás: https://ieeexplore.ieee.org/document/8756954/ (Elérés: 2022. február 27.).

Johnson, Al. 2017. „Endpoint Protection - Symantec Enterprise". Forrás: https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=7ca2e331-2209-46a8-9e60-4cb83f9602de&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments (Elérés: 2022. március 23.).

Johnson, Johna Till. 2020. „Why Nation-State Cyberattacks Must Be Top of Mind for CISOs". *SearchSecurity*. Forrás: https://www.techtarget.com/searchsecurity/opinion/Why-nation-state-cyberattacks-must-be-top-of-mind-for-CISOs (Elérés: 2022. március 25.).

Jones, Seth G, és Newlee, Danika. 2019. „The United States' Soft War with Iran". Forrás: https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/190611_JonesNewlee_U.S.SoftWarwithIran_v5%20(002).pdf (Elérés: 2022. április 5.).

Jurkanin, Thomas J. ed. 2013. „Intelligence Training". *Law Enforcement Executive Forum 06/2013*. Forrás: https://www.iletsbeiforumjournal.com/images/Issues/FreeIssues/LEEF_13.2_Police_Training2.pdf#page=8 (Elérés: 2022. április 15.).

Kania, Elsa. 2017. „PLA Strategic Support Force: The 'Information Umbrella' for China's Military". Forrás: https://thediplomat.com/2017/04/pla-strategic-support-force-the-information-umbrella-for-chinas-military/ (Elérés: 2022. március 24.).

Kaplan, Robert D. 1994. „The Coming Anarchy". *The Atlantic*. Forrás: https://www.theatlantic.com/magazine/archive/1994/02/the-coming-anarchy/304670/ (Elérés: 2022. március 25.).

Kashkett, Steven. 2017. „Special Operations and Diplomacy: A Unique Nexus". Forrás: https://afsa.org/special-operations-and-diplomacy-unique-nexus (Elérés: 2022. március 30.).

Kaspersky. 2014. „The Epic Turla Operation". Forrás: https://securelist.com/the-epic-turla-operation/65545/ (Elérés: 2022. március 22.).

Kaspersky. 2015a. „Equation: The Death Star of Malware Galaxy". Kaspersky. Forrás: https://securelist.com/equation-the-death-star-of-malware-galaxy/68750/ (Elérés: 2022. március 22.).

Kaspersky. 2015b. „Equation Group: Questions and Answers”. Kaspersky. Forrás: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08064459/Equation_group_questions_and_answers.pdf (Elérés: 2022. március 22.).

Kaspersky. 2016. „The Cybersecurity Skills Gap: A Ticking Time Bomb”. Kaspersky. Forrás: https://media.kaspersky.com/uk/Kaspersky-Cyberskills-Report_UK.pdf (Elérés: 2022. május 1.).

Kaushik, Devansh. 2021. „Cyberspace as A Global Commons”. *South Asia Journal*. Forrás: http://southasiajournal.net/cyberspace-as-a-global-commons/ (Elérés: 2021. december 17.).

Kennan, George. 1948. „269. Policy Planning Staff Memorandum”. Forrás: http://academic.brooklyn.cuny.edu/history/johnson/65ciafounding3.htm (Elérés: 2022. március 29.).

KFCRIS. 2020. „Iran’s Cyberattacks Capabilities”. Forrás: https://www.kfcris.com/pdf/50781c86a6f571af0edb0189aa7594d75e2d6570cfa06.pdf (Elérés: 2022. április 5.).

Khaleefa, Eman, és Abdulah, Dhahair. 2022. „Concept and Difficulties of Advanced Persistent Threats APT): Survey”. *International Journal of Nonlinear Analysis and Applications 2022 January*. Forrás: https://doi.org/10.22075/ijnaa.2022.6230 (Elérés: 2022. március 31.).

Kim, Yu-Kyung, Lee, Jemin Justin, Go, Myong-Hyun és Lee, Kyungho. 2020. „Analysis of the Asymmetrical Relationships between State Actors and APT Threat Groups”. In: 2020 International Conference on Information and Communication Technolog Convergence (ICTC). Forrás: https://ieeexplore.ieee.org/document/9289506 (Elérés: 2021. július 27.).

Kiss, Álmos Péter. 2011. „A negyedik generációs konfliktusok jellemzői és tapasztalatai”. Forrás: https://tudasportal.uni-nke.hu/xmlui/static/pdfjs/web/viewer.html?file=https://tudasportal.uni-nke.hu/xmlui/bitstream/handle/20.500.12944/12252/kiss_almos_peter_doktori_ertekezes.pdf?sequence=6&isAllowed=y (Elérés: 2022. február 27.).

Knake, Robert K. 2010. „Untangling Attribution: Moving to Accountability in Cyberspace”. Forrás: https://www.cfr.org/sites/default/files/pdf/2010/07/Knake%20-Testimony%20071510.pdf (Elérés: 2022. április 1.).

Kovács, László, és Marianna Sipos. 2010. „A stuxnet és ami mögötte van: Tények és a cyberháború hajnala”. *Hadmérnök 2010 december*. Forrás: http://hadmernok.hu/2010_4_kovacs_sipos.pdf (Elérés: 2022. április 2.).

Kőszegvári, Tibor. 2006. „A különleges katonai mûveletekrõl”. Forrás: https://www.mhtt.eu/hadtudomany/2006/1_2/2006_1_2_3.html (Elérés: 2022. március 27.).

Krasznay Csaba. 2021. „Húsz év a globális kiberbűnözés elleni küzdelemben : A Budapesti Egyezmény értékelése”. *Külügyi Szemle* 20(Különszám). Forrás: https://kki.hu/wp-content/uploads/2021/08/12_2021_szemle_kulonszam_krasznay.pdf (Elérés: 2022. február 14.).

Law, David, Caparini, Marina, és Kartas, Moncef. é.n. „Private Military Companies”. Forrás: https://www.files.ethz.ch/isn/17438/backgrounder_09_private-military-companies.pdf (Elérés: 2022. április 30.).

Lee, Robert M. 2021. „The Sliding Scale of Cyber Security”. *Egnyte*. Forrás: https://sansorg.egnyte.com/dl/GJEumszLQX (Elérés: 2022. február 26.).

Lee, Robert M., Assante, Michael J. és Conway, Tim. 2016. „Analysis of the Cyber Attack on the Ukrainian Power Grid”. E-ISAC. Forrás: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2016/05/20081514/E-ISAC_SANS_Ukraine_DUC_5.pdf (Elérés: 2022. április 4.).

Leed, Maren. 2013. „Offensive Cyber Capabilities at the Operational Level: The Way Ahead”. CSIS. Forrás: https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/130916_Leed_OffensiveCyberCapabilities_Web.pdf (Elérés: 2022. március 23.).

Lella, Ifigeneia, Theocharidou, Marianthi, Tsekmezoglou, Eleni és Malatras, Apostolos. 2021. „ENISA Threat Landscape 2021”. ENISA. Forrás: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021 (Elérés: 2022. február 17.).

Lemay, Antoine. 2018. „Survey of publicly available reports on advanced persistent threat actors”. Forrás: https://www.sciencedirect.com/science/article/pii/S0167404817301608 (Elérés: 2022. február 17.).

Liddel Hart, B.H. 2002. *Stratégia*. Európa Kiadó.

Lilly, Bilyana, és Cheravitch, Joe. 2020. „The Past, Present, and Future of Russia’s Cyber Strategy and Forces”. In: *2020 12th International Conference on Cyber Conflict (CyCon)*, Estonia. Forrás: https://ieeexplore.ieee.org/document/9131723/ (Elérés: 2021. július 27.).

Limnéll, Jarno. 2013. „Offensive Cyber Capabilities Are Needed Because of Deterrence”. Forrás: https://cyberwar.nl/d/20130200_Offensive-Cyber-Capabilities-are-Needed-Because-of-Deterrence_Jarno-Limnell.pdf (Elérés: 2022. február 20.).

Lockheed Martin. 2020. „Cyber Kill Chain®”. *Lockheed Martin*. Forrás: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html (Elérés: 2022. február 17.).

Maigre, Merle. 2022. „NATO’s Role in Global Cyber Security”. GMFUS. Forrás: https://www.gmfus.org/news/natos-role-global-cyber-security (Elérés: 2022. június 11.).

Mainwright. 2016. „Trends and Challenges for law enforcement training and education”. Forrás: https://www.cepol.europa.eu/sites/default/files/07-rob-wainwright.pdf (Elérés: 2022. február 20.).

Majuca, Ruperto P., és Kesan, Jay P. 2009. „Hacking Back: Optimal Use of Self-Defense in Cyberspace” *Illinois Public Law and Legal Theory Papers Series - Research Papers Series. 2009/03*. Forrás: https://papers.ssrn.com/abstract=1363932 (Elérés: 2022. február 26.).

Mandiant. 2013. „APT1 Exposing One of China's Cyber Espionage Units”. Mandiant. Forrás: https://www.mandiant.com/sites/default/files/2021-09/mandiant-apt1-report.pdf (Elérés: 2022. március 24.).

Mandiant. 2022a. „14 Cyber Security Predictions for 2022 and Beyond”. Mandiant. Forrás: https://www.mandiant.com/sites/default/files/2021-11/rpt-m-Prediction22-000410-02.pdf (Elérés: 2022. február 17.).

Mandiant. 2022b. „APT41, A Dual Espionage and Cyber Crime Operation”. Mandiant. Forrás: https://www.mandiant.com/sites/default/files/2022-02/rt-apt41-dual-operation.pdf (Elérés: 2022. március 24.).

Marighella, Carlos. 1969. „Mini-manual of the Urban Guerrilla”. Forrás: https://www.latinamericanstudies.org/marighella.htm (Elérés: 2021. július 24.).

Marsh, Christopher. 2017. „Introduction: The World’s Elite Warriors”. Forrás: https://www.academia.edu/33356434/Introduction_The_Worlds_Elite_Warriors (Elérés: 2022. március 22.).

Maurer, Tim. 2015. „Cyber Proxies and the Crisis in Ukraine”. CCDCOE. Forrás: https://ccdcoe.org/uploads/2018/10/Ch09_CyberWarinPerspective_Maurer.pdf (Elérés: 2022. március 22.).

Maurer, Tim. 2017. „When States Pretend to Be Terrorists or Hacktivists in Cyberspace”. Carnegie Endowment for International Peace. Forrás: https://carnegieendowment.org/2017/04/18/when-states-pretend-to-be-terrorists-or-hacktivists-in-cyberspace-pub-68703 (Elérés: 2022. április 1.).

Maurer, Tim, és Hinck, Garrett. 2018. „Russia’s Cyber Strategy”. ISPI. Forrás: https://www.ispionline.it/en/pubblicazione/russias-cyber-strategy-21835 (Elérés: 2022. március 22.).

McAfee. 2016. „Hacking the Skills Shortage Report”. Forrás: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hacking-skills-shortage.pdf (Elérés: 2022. május 1.).

Messner, J.J., Haken, Nate, Taft, Patricia, Blyth, Hannah, Lawrence, Kendall, Graham, Sebastian Pavlou és Umana, Felipe. 2015. „Fragile States Index 2015”. FFP. Forrás:

https://fundforpeace.org/wp-content/uploads/2018/08/fragilestatesindex-2015.pdf (Elérés: 2022. június 10.).

Microsoft. 2021. „Microsoft Digital Defense Report” 2021. október. Forrás: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi (Elérés: 2022. április 18.).

Microsoft. é.n. „Microsoft Security Intelligence”. *Microsoft Security Blog*. Forrás: https://www.microsoft.com/security/blog/microsoft-security-intelligence/ (Elérés: 2022. április 27.).

MITRE. „Groups | MITRE ATT&CK®”. Forrás: https://attack.mitre.org/groups/ (Elérés: 2022. február 17.).

MKM. 2019. „National Cyber Security Strategy - Estonia”. Majandus- Ja Kommunikatsiooniministeerium Forrás: https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf (Elérés: 2022. február 20.).

MoD HR. 2018. „National Security Strategy of Croatia”. Forrás: https://www.morh.hr/wp-content/uploads/2018/04/strategy_18012018.pdf (Elérés: 2022. február 22.).

MoD UK. 2016. „Cyber Primer (2nd Edition)”. Forrás: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/549291/20160720-Cyber_Primer_ed_2_secured.pdf. (Elérés: 2022. március 23.)

Morcos, Pierre, és Wall, Colin. 2021. „Invisible and Vital: Undersea Cables and Transatlantic Security”. Forrás: https://www.csis.org/analysis/invisible-and-vital-undersea-cables-and-transatlantic-security (Elérés: 2021. december 28.).

Morgenthau, Hans J. 1978. „Politics Among Nations: The Struggle for Power and Peace”. Forrás: https://www.mtholyoke.edu/acad/intrel/morg6.htm. (Elérés: 2022. április 5.)

Mueller, Robert S. 2019. „Report on the Investigation into Russian Interference in the 2016 Presidential Election”. Forrás: https://www.justice.gov/archives/sco/file/1373816/download (Elérés: 2022. március 22.)

Muphy, Randall J., Sukkarieh, Michael, Haasss, Jon és Hriljac, Paul. 2015. „Appendix A - Categorized List of Cybersecurity Threats, Guidebook on Best Practices for Airport Cybersecurity”. Forrás: https://www.nap.edu/read/22116/chapter/12#88 (Elérés: 2022. február 16.).

National Cyber Directorate. 2017. „National Cyber Security Strategy in a Brief - Israel”. Forrás: https://cyber.haifa.ac.il/images/pdf/cyber_english_A5_final.pdf (Elérés: 2022. február 20.).

NATO. 2012. „Psychological and Physiological Selection of Military Special Operations Forces Personnel (Final Report of Task Group HFM-171)”. Forrás:

https://www.sto.nato.int/publications/STO%20Technical%20Reports/RTO-TR-HFM-171/$$TR-HFM-171-ALL.pdf (Elérés: 2021. július 15.).

NATO. 2014. „Wales Summit Declaration Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Wales”. *NATO*. Forrás: https://www.nato.int/cps/en/natohq/official_texts_112964.htm (Elérés: 2022. június 7.).

NATO. 2016. „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*. Forrás: https://www.nato.int/cps/en/natohq/official_texts_133169.htm (Elérés: 2022. június 7.).

NATO. 2020a. „AJP-3.20, Allied Joint Doctrine for Cyberspace Operations (Edition A)”. Forrás: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf (Elérés: 2021. december 28.).

NATO. 2020b. „NATO 2030: United for a New Era”. Forrás: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf (Elérés: 2022. február 28.).

NATO. 2021. „Brussels Summit Communiqué Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Brussels 14 June 2021”. NATO. Forrás: https://www.nato.int/cps/en/natohq/news_185000.htm (Elérés: 2022. február 20.).

NATO. 2022. „Strategic Concepts”. NATO. Forrás: https://www.nato.int/cps/en/natohq/topics_56626.htm (Elérés: 2022. február 28.).

Naval Institute. 2021. „#OTD in 1906, Xerox Was Founded as the Haloid Photographic Company”. *@NavalInstitute*. Forrás: https://twitter.com/NavalInstitute/status/1383978229619322890/photo/1 (Elérés: 2022. február 16.).

Nb. tv. 1995. „1995. Évi CXXV. Törvény a Nemzetbiztonsági Szolgálatokról”. Forrás: https://net.jogtar.hu/jogszabaly?docid=99500125.tv (Elérés: 2022. március 31.).

NBS. 2020. „A Kormány 1163/2020. (IV. 21.) Korm. határozata Magyarország Nemzeti Biztonsági Stratégiájáról”. Forrás: http://www.kozlonyok.hu/nkonline/index.php?menuindex=200&pageindex=kozltart&ev=2020&szam=81 (Elérés: 2022. február 20.).

NCAE. é.n. „What is a CAE in Cybersecurity?”. CAE Community. Forrás: https://www.caecommunity.org/about-us/what-cae-cybersecurity (Elérés: 2022. április 30.).

NCCIC. 2016. „Grizzly Steppe - Russian Malicious Cyber Activity”. NCCI., FBI JAR. Forrás: https://www.cisa.gov/uscert/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf (Elérés: 2022. március 22.).

NCS CH. 2018. „National Strategy for the Protection of Switzerland against Cyber Risks (NCS) 2018-2022”. Forrás: https://www.ncsc.admin.ch/ncsc/en/home/strategie/strategie-ncss-2018-2022.html (Elérés: 2022. február 20.).

NetScout. 2021. „NETSCOUT Threat Intelligence Report”. Latest Cyber Threat Intelligence Report. Forrás: https://www.netscout.com/threatreport/global-ddos-attack-trends/ (Elérés: 2022. április 17.).

NIST. 2011. „Managing Information Security Risk :: Organization, Mission, and Information System View”. Gaithersburg, National Institute of Standards and Technology. Forrás: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf (Elérés: 2022. február 17.).

NIST. 2015. „Cyberspace operations (CO)”. Glossary. Forrás: https://csrc.nist.gov/glossary/term/cyberspace_operations (Elérés: 2022. február 25.).

NKBS. 2013. „1139/2013. (III. 21.) Korm. határozat - Magyarország Nemzeti Kiberbiztonsági Stratégiájáról”. Forrás: https://njt.hu/jogszabaly/2013-1139-30-22.1 (Elérés: 2021. december 28.).

NKE. é.n. „Polgári Nemzetbiztonsági Alapképzési Szak”. Forrás: https://rtk.uni-nke.hu/document/rtk-uni-nke-hu/Polgari_nemzetbiztonsagi_alapkepzesi_szak_kkk.pdf (Elérés: 2022. április 14.).

NKS. 2021. „1393/2021 (VI. 24) Korm. határozat Magyarország Nemzeti Katonai Stratégiájáról”. Forrás: https://honvedelem.hu/hirek/nemzeti-katonai-strategia.html (Elérés: 2022. február 27.).

Nordmoe, Matthew. 2015. „The Ghost in the Machine: Defining Special Operations Forces in Cyberspace”. Forrás: https://www.academia.edu/12465632/The_Ghost_in_the_Machine_Defining_Special_Operations_Forces_in_Cyberspace (Elérés: 2022. március 22.).

Novetta. 2015. „WINNTI Analysis”. Novetta. Forrás: https://www.novetta.com/wp-content/uploads/2015/04/novetta_winntianalysis.pdf (Elérés: 2022. március 24.).

NRC. 2010. „Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy”. The National Academies Press. Forrás: https://nap.nationalacademies.org/download/12997 (Elérés: 2022. március 30.).

NSA. 2022. „2021 NSA Cybersecurity Year in Review”. Forrás: https://media.defense.gov/2022/Feb/03/2002932462/-1/-1/0/2021_NSA_CYBERSECURITY_YEAR_IN_REVIEW.PDF (Elérés: 2022. február 17.).

NTOA. 2018. „Tactical Response and Opeartions Standard for Law Enforcement Agencies”. Forrás: https://ntoa.org/pdf/swatstandards.pdf (Elérés: 2022. március 30.).

NTT. 2021. „The Operations of Winnti Group”. NTT Limited. Forrás: https://hello.global.ntt/-/media/ntt/global/insights/white-papers/the-operations-of-winnti-group.pdf (Elérés: 2022. március 24.).

Nurse, Jason R.C., Adamos, Konstantinos, Grammatopoulos, Athanasios és Di Franco, Fabio. 2021. „Addressing Skills Shortage and Gap Through Higher Education”. ENISA. Forrás: https://www.enisa.europa.eu/publications/addressing-skills-shortage-and-gap-through-higher-education (Elérés: 2022. április 30.).

Ottis, Rain, és Lorents, Peeter. 2012. „Cyberspace: Definition and Implications”. Forrás: https://dumitrudumbrava.files.wordpress.com/2012/01/cyberspace-definition-and-implications.pdf (Elérés: 2021. december 28.).

Paganini, Pierluigi. 2015. „Equation Group APT and TAO NSA: Two Hacking Arsenals Too Similar - Infosec Resources”. Forrás: https://resources.infosecinstitute.com/topic/equation-group-apt-tao-nsa-two-hacking-arsenals-similar/ (Elérés: 2022. március 23.).

Paganini, Pierluigi. 2017. „Symantec Confirms That Longhorn Group Is Tied to CIA Operators Detailed in Vault 7”. *Security Affairs*. Forrás: https://securityaffairs.co/wordpress/57916/apt/longhorn-group-cia.html (Elérés: 2022. március 23.).

Parfomak, Paul W, és Jaikaran, Chris. 2021. „Colonial Pipeline: The DarkSide Strikes”. Forrás: https://crsreports.congress.gov/product/pdf/IN/IN11667 (Elérés: 2022. április 4.)

Paul, Christopher, Clarke, Colin P. és Grill, Beth. 2010. „Victory Has a Thousand Fathers: Detailed Counterinsurgency Case Studies”. RAND. National Defense Research Institute. Santa Monica. Forrás: https://www.rand.org/content/dam/rand/pubs/monographs/2010/RAND_MG964.pdf. (Elérés: 2021. július 24.)

Paul, Christopher E, és Schwille, Michael. 2021. „The Evolution of Special Operations as a Model for Information Forces”. *JFQ 2021/01-03*. Forrás: https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-100/jfq-100_8-13_Paul-Schwille.pdf?ver=gPNcyKyhmCP12nbuHMWw7g%3d%3d (Elérés: 2022. március 29.).

Paul, Christopher, Porche, Isaac R. III és Axelband, Elliot. 2014. „The Other Quiet Professionals: Lessons for Future Cyber Forces from the Evolution of Special Forces”. RAND Corporation. Santa Monica. Forrás: https://www.rand.org/pubs/research_reports/RR780.html (Elérés: 2021. július 17.).

Pawlak, Patryk, és Petkova, Gergana. 2015. „State-Sponsored Hackers: Hybrid Armies? ” Publications Office, European Union Institute for Security Studies. Forrás: https://data.europa.eu/doi/10.2815/341983 (Elérés: 2022. március 22.).

Perkovich, George, és Levite, Ariel E. 2017. "Understanding Cyber Conflict: Fourteen Analogies". Georgetown University Press. Forrás: https://carnegieendowment.org/files/GUP_Perkovich_Levite_UnderstandingCyberConflict_Introduction.pdf (Elérés: 2022. május 4.).

Peters, Allison, és Garcia, Michael. 2020. „A Roadmap to Strengthen US Cyber Enforcement". Forrás: https://thirdway.imgix.net/pdfs/override/A-Roadmap-to-Strengthen-US-Cyber-Enforcement.pdf (Elérés: 2022. április 27.).

Peters, Allison, és Jordan, Amy. 2020. „Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime". Forrás: https://thirdway.imgix.net/pdfs/override/Countering-the-Cyber-Enforcement-Gap-Strengthening-Global-Capacity-on-Cybercrime.pdf (Elérés: 2022. április 27.).

Peterson, Cory M. 2014. „The Use of Special Operations Forces in Support of American Strategic Security Strategies". Fort Belvoir, VA. Defense Technical Information Center. Forrás: http://www.dtic.mil/docs/citations/ADA601724 (Elérés: 2022. március 30.).

Pijnenburg Muller, Lilly, Gjesvik, Lars és Friis, Karsten. 2018. „Cyber-weapons in International Politics - Possible sabotage against the Norwegian petroleum sector". Norwegian Institute of International Affairs. Forrás: https://nupi.brage.unit.no/nupi-xmlui/bitstream/handle/11250/2486814/NUPI_Report_2018-3.pdf?sequence=1&isAllowed=y (Elérés: 2022. március 22.).

Pollpeter, Kevin L., Chase, Michael S.és Heginbotham, Eric. 2017. „The Creation of the PLA Strategic Support Force and Its Implications for Chinese Military Space Operations". RAND Corporation. Forrás: https://www.rand.org/pubs/research_reports/RR2058.html (Elérés: 2022. március 24.).

Qiao, Liang és Wang, Xiangsui. 1999. „Unrestricted Warfare". PLA Literature and Arts Publishing House. Forrás: https://www.c4i.org/unrestricted.pdf (Elérés: 2022. március 25.).

Quihoo 360. „The CIA Hacking Group APT-C-39". Quihoo 360. Forrás: https://blogs.360.cn/post/APT-C-39_CIA_EN.html (Elérés: 2022. március 23.)

Rantatalo, Oscar. 2013. „Sensemaking and Organising in the Policing of High Risk Situations: Focusing the Swedish Police National Counter-Terrorist Unit". Forrás: https://www.diva-portal.org/smash/get/diva2:642473/FULLTEXT02.pdf (Elérés: 2022. március 31.).

Reeder, Joe R, és Hall, Tommy. 2021. „Cybersecurity's Pearl Harbor Moment: Lessons Learned from the Colonial Pipeline Ransomware Attack". Forrás: https://cyberdefensereview.army.mil/Portals/6/Documents/2021_summer_cdr/02_ReederHall_CDR_V6N3_2021.pdf?ver=6qlw1l02DXt1A_1n5KrL4g%3D%3D (Elérés: 2022. április 4.).

Regős Franciska. 2019. „Területi szuverenitás és a nemzetközi környezetvédelmi jog". *KRE-DIT: A KRE-DOK Online Tudományos Folyóirata 2019/1.* Forrás: http://www.kre-

dit.hu/tanulmanyok/regos-franciska-teruleti-szuverenitas-es-a-nemzetkozi-kornyezetvedelmi-jog/?print=pdf (Elérés: 2021. december 17.)

Rempel, Mark. 2010. „An Overview of the Canadian Forces' Second Generation Capability-Based Planning Analytical Process". Centre for Operational Research and Analysis. Forrás: https://cradpdf.drdc-rddc.gc.ca/PDFS/unc103/p534121_A1b.pdf (Elérés: 2022. március 11.).

Rid, Thomas. 2012. „Cyber War Will Not Take Place". *Journal of Strategic Studies 2012/02*. Forrás: http://www.tandfonline.com/doi/abs/10.1080/01402390.2011.608939 (Elérés: 2022. április 19.).

Rid, Thomas, és Buchanan, Ben. 2015. „Attributing Cyber Attacks". *Journal of Strategic Studies 2015/01-02.* Forrás: http://www.tandfonline.com/doi/abs/10.1080/01402390.2014.977382 (Elérés: 2021. július 17.).

Rid, Thomas, Moore, Daniel, Raiu, Costin és Guerrero-Saade, Juan Andres. 2018. „Penquin's Moonlit Maze - The Dawn of Nation-State Digital Espionage". Kaspersky. Forrás: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180251/Penquins_Moonlit_Maze_PDF_eng.pdf (Elérés: 2022. március 22.).

Ritter, Mario. 2018. „US to Offer Cyber Warfare Technology to NATO". *VOA*. Forrás: https://learningenglish.voanews.com/a/us-to-offer-cyber-warfare-technology-to-nato/4601212.html (Elérés: 2022. június 11.).

Robertsen, Tom. 2007. „Making New Ambitions Work: The Transformation of Norwegian Special Operations Forces". Oslo: Norwegian Institute for Defence Studies. Forrás: https://fhs.brage.unit.no/fhs-xmlui/bitstream/handle/11250/99375/DSS0107.pdf?sequence=1&isAllowed=y (Elérés: 2022. március 30.).

Robinson, Linda. 2013. „Teh Future of U.S. Special Operations Forces". Council on Foreign Relations. Forrás: https://cdn.cfr.org/sites/default/files/pdf/2013/03/Special_Operations_CSR66.pdf (Elérés: 2022. március 30.).

Russell, Teresa L, Rohrback, Michelle R., Nee, Marguerite T., Crafts, Jennifer L., Peterson, Norman G. és Mael, Fred A. 1995. „Development of a Roadmap for Special Forces Selection and Classification Research". Forrás: https://apps.dtic.mil/sti/pdfs/ADA317151.pdf (Elérés: 2022. április 12.).

Ruwhof, Sijmen. 2017. „How to hack the upcoming Dutch elections – and how hackers could have hacked all Dutch elections since 2009". Forrás: https://sijmen.ruwhof.net/weblog/1166-how-to-hack-the-upcoming-dutch-elections (Elérés: 2022. március 22.).

Sallai János. 2015. „A rendészet kihívásai napjainkban”. *Hadtudomány 2015/1-2.* Forrás: http://real.mtak.hu/23559/1/konf_sallai.pdf (Elérés: 2022. február 20.).

Schmidt, Robert, Rattray, Gregory J. és Fogle, Christipher J. 2008. „U.S. Patent Application - APT”. Forrás: https://patentimages.storage.googleapis.com/5c/c5/ed/70957093e1fbf8/US20080167920A1.pdf (Elérés: 2022. február 17.).

Schneier, Bruce. 2010. „Stuxnet - Schneier on Security”. Forrás: https://www.schneier.com/blog/archives/2010/10/stuxnet.html (Elérés: 2022. április 2.).

Schoka, Andrew. 2019. „Cyber Command, the NSA, and Operating in Cyberspace: Time to End the Dual Hat”. *War on the Rocks*. Forrás: https://warontherocks.com/2019/04/cyber-command-the-nsa-and-operating-in-cyberspace-time-to-end-the-dual-hat/ (Elérés: 2022. március 23.).

Schrijver, Nico. 2016. „Managing the Global Commons: Common Good or Common Sink?” *Third World Quarterly 2016/7*. Forrás: https://www.tandfonline.com/doi/full/10.1080/01436597.2016.1154441 (Elérés: 2021. december 17.).

SentinelOne. é. n. „What Is Mimikatz?” *SentinelOne*. Forrás: https://www.sentinelone.com/cybersecurity-101/mimikatz/ (Elérés: 2022. április 11.).

Shen, Ming-shih. 2019. „China’s Cyber Warfare Strategy and Approaches toward Taiwan”. *Taiwan Strategists 02*. Forrás: https://www.pf.org.tw/files/6510/A73CE07D-0D72-4AF8-9075-98A1CB188DA1 (Elérés: 2022. március 24.)

Singh, Karan R. 2001. „Treading the Thin Blue Line: Military Special-Operations Trained Police SWAT Teams and the Constitution”. Forrás: https://scholarship.law.wm.edu/cgi/viewcontent.cgi?article=1357&context=wmborj (Elérés: 2022. március 31.).

SK CERT. 2021. „National Cyber Security Strategy of Slovakia”. Forrás: https://www.nbu.gov.sk/wp-content/uploads/cyber-security/National_cybersecurity_strategy_2021.pdf (Elérés: 2022. február 20.).

Sobers, Rob. 2020. „Data Breach Response Times: Trends and Tips”. Forrás: https://www.varonis.com/blog/data-breach-response-times (Elérés: 2022. április 3.).

Soroos, Marvin S. 1988. „The International Commons: A Historical Perspective”. *Environmental Review 1988/1*. Forrás: https://www.jstor.org/stable/3984374 (Elérés: 2021. december 17.).

Soroos, Marvin S. 1990. „A Theoretical Framework for Global Policy Studies”. *International Political Science Review 1990/3*. Forrás: https://doi.org/10.1177/019251219001100302 (Elérés: 2021. december 17.).

Stokes, Mark A. 2015. „The Chinese People's Liberation Army Computer Network Operations Infrastructure". In: Lidsay, Jon R. Et al. (szerk): China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain, New York, NY, USA: Oxford University Press.

Stokes, Mark A, Lin, Jenny és Hsiao, L C Russell. 2011. „The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure". Project 2049 Institute. Forrás: http://goodtimesweb.org/surveillance/pla_third_department_sigint_cyber_stokes_lin_hsiao.pdf (Elérés: 2022. március 24.)

Styczynski, Jake, és Beach-Westmoreland, Nate. 2015. „Industrial Cybersecurity Threat Briefing". BAH. Forrás: https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf (Elérés: 2022. április 4.)

Suckhov, Maxim, és Tack, Sim. 2019. „The Future of War". Forrás: https://valdaiclub.com/files/26032/ (Elérés: 2022. március 19.).

Symantec. 2011. „Advanced Persistent Threats: A Symantec Perspective". Symantec. Forrás: http://index-of.es/Varios/b-advanced_persistent_threats_WP_21215957.en-us.pdf (Elérés: 2022. március 31.).

Szenes Zoltán. 2017. „Katonai biztonság napjainkban. Új fenyegetések, új háborúk, új elméletek". In: Finszter Géza Et al. (szerk.): Biztonsági kihívások a 21. században. Forrás: https://www.uni-nke.hu/document/uni-nke-hu/3.%20Szenes%20k%C3%B6nyv,%20k%C3%B6nyvr%C3%A9szlet.pdf (Elérés: 2022. március 25.)

Szenes Zoltán. 2020. „HONVÉDELEM – VÉDELEMPOLITIKA". *Kormányzati Tanulmányok*. Forrás: https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/15946/Honvedelem%20-%20vedelempolitika.pdf;jsessionid=F0FEED033601C2D6B6347FE03AFE4FED?sequence=3 (Elérés: 2022. február 19).

Szenes Zoltán. 2021. „Merre tovább, NATO?" *Honvédségi Szemle* 149(6): 3–19. Forrás: https://kiadvany.magyarhonvedseg.hu/index.php/honvszemle/article/view/631 (Elérés: 2022. február 20.).

Sz.n. 2014. „A magyar titkosszolgálatnak még a kémprogram telepítése sem sikerült". Forrás: https://index.hu/tech/2014/08/12/a_magyar_titkosszolgalatnak_nem_sikerult_a_kemprogram_telepitese/ (Elérés: 2022. május 1.).

Sz.n. 2022. „MŰVELETI FELDERÍTŐ állás, munka: NEMZETBIZTONSÁGI SZAKSZOLGÁLAT". *Profession.hu*. Forrás: https://www.profession.hu/allas/muveleti-felderito-nemzetbiztonsagi-szakszolgalat-1658540 (Elérés: 2021. augusztus 2.).

Szörényi, András. 2014. „Kiindulópontok a nemzetközi kapcsolatok elméletében a nem állami szereplők természetének és szerepének értelmezéséhez”. Forrás: http://www.grotius.hu/doc/pub/DLNNSK/2009_160_szorenyi_andras_%20elmeleti_iskolak.pdf (Elérés: 2022. március 17.).

Tálas Péter. 2014. „A nemzeti katonai stratégia és a magyar stratégiai kultúra”. *Nemzet és Biztonság - Biztonságpolitikai Szemle 2014/2*. Forrás: http://www.nemzetesbiztonsag.hu/cikkek/nb_2014_2_03_talas_peter.pdf (Elérés: 2022. március 18).

Tálas, Péter, és Gyimesi, Gyula. 2008. „Az integrált biztonsági szféra magyarországi megteremtésének lehetőségei és feltételei”. Forrás: https://docplayer.hu/1737364-Az-integralt-biztonsagi-szfera-magyarorszagi-megteremtesenek-lehetosege-es-feltetelei.html (Elérés: 2022. február 20.).

Taliaferro, Aaron C., Gonzalez, Lina M., Tillman, Mark, Ghosh, Pritha, Clarke, Paul, Hinkle, Wade. 2019. „What Is a Capability, and What Are the Components of Capability?” Institute for Defense Analyses. Forrás: https://www.jstor.org/stable/resrep22853.5 (Elérés: 2022. március 11.).

Tan, Eugene E.G. 2019. „A Small State Perspective on the Evolving Nature of Cyber Conflict - Lessons from Singapore”. 8/3 2019. Forrás: https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_8-3/prism_8-3.pdf (Elérés: 2022. április 11.).

Tanase, Stefan. 2015. „Satellite Turla: APT Command and Control in the Sky”. Forrás: https://securelist.com/satellite-turla-apt-command-and-control-in-the-sky/72081/ (Elérés: 2022. március 22.).

Tanriverdi, Hakan, Flade, Florian és Frey, Lea. 2022. „The Elite Hackers of the FSB”. BR. Forrás: https://interaktiv.br.de/elite-hacker-fsb/en/ (Elérés: 2022. március 22.).

Temple-Raston, Dina. 2021. „A Worst Nightmare Cyberattack: The Untold Story Of The SolarWinds Hack”. *NPR*. Forrás: https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack (Elérés: 2021. július 24.).

Tewari, Saurabh. 2019. „China’s Cyber Warfare Capabilities”. Forrás: https://usiofindia.org/publication/usi-journal/chinas-cyber-warfare-capabilities/ (Elérés: 2022. március 24.).

ThaiCERT. 2022. „Threat Group Cards: A Threat Actor Encyclopedia”. Electronic Transactions Development Agency. Forrás: https://www.etda.or.th/th/Our-Service/thaicert/report.aspx (Elérés: 2022. március 24.).

The White House. 2018. „National Cyber Strategy of the United States of America”. The White House. Forrás: https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf (Elérés: 2022. február 20.).

The White House. 2021. „FACT SHEET: The Biden-Harris Administration Has Launched an All-of-Government Effort to Address Colonial Pipeline Incident”. The White House. Forrás: https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/11/fact-sheet-the-biden-harris-administration-has-launched-an-all-of-government-effort-to-address-colonial-pipeline-incident/ (Elérés: 2022. április 4.).

Theohary, Catherine A. 2020. „Iranian Offensive Cyber Attack Capabilities”. CRS. Forrás: https://sgp.fas.org/crs/mideast/IF11406.pdf (Elérés: 2022. február 20.).

Theohary, Catherine A. 2021. „Defense primer: Cyberspace Operations”. CRS. Forrás: https://sgp.fas.org/crs/natsec/IF10537.pdf (Elérés: 2022. február 20.).

Thomas, Timothy. 2016. „Thinking Like a Russian Officer”. *APAN Community*. Forrás: https://community.apan.org/wg/tradoc-g2/fmso/m/fmso-monographs/194971 (Elérés: 2022. március 25.).

ThreatConnect. 2014. „Piercing the Cow’s Tongue: China Targeting South China Seas Nations”. Risk-Threat-Response. ThreatConnect. Forrás: https://threatconnect.com/blog/piercing-the-cows-tongue-china-targeting-south-china-seas-nations/ (Elérés: 2022. március 24.).

Tingley, Brett. 2022. „Cyber Command Task Force Conducted Its First Offensive Operation As The Secretary Of Defense Watched”. *The Drive*. Forrás: https://www.thedrive.com/the-war-zone/43776/cyber-command-task-force-conducted-its-first-offensive-operation-as-defense-secretary-watched (Elérés: 2022. március 23.).

T.L. főhadnagy. 2020. „Gondolatok egy »Pitbull« margójára…”. Forrás: https://honvedelem.hu/hirek/gondolatok-egy-pitbull-margojara.html (Elérés: 2021. július 13.).

Trautmann Balázs. 2021a. „Közös útkeresés”. Forrás: https://honvedelem.hu/hirek/kozos-utkereses.html (Elérés: 2021. július 22.).

Trautmann Balázs. 2021b. „Váltani kell – minden területen”. Forrás: https://honvedelem.hu/hirek/valtani-kell-minden-teruleten.html (Elérés: 2021. július 13.).

Trautmann Balázs. 2022. „Black Swan 2022: több, nagyobb, nehezebb”. Forrás: https://honvedelem.hu/hirek/black-swan-2022-tobb-nagyobb-nehezebb.html (Elérés: 2022. április 26.).

Tudor, Dora. 2022. „Malware as a Service. What Is It and How It Can Threaten Your Business?” *Heimdal Security Blog*. Forrás: https://heimdalsecurity.com/blog/what-is-malware-as-a-service-maas/ (Elérés: 2022. április 27.).

UN. 1966. „Szerződés az államok tevékenységét szabályozó elvekről a világűr kutatása és felhasználása terén, beleértve a Holdat és más égitesteket”. Forrás: https://www.unoosa.org/pdf/gares/ARES_21_2222E.pdf (Elérés: 2022. február 14.).

UN. 1982. „United Nations Convention on the Law of the Sea”. Forrás: https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf (Elérés: 2022. február 14.).

UN. 2016. „Police Opeartions in United Nations Peacekkeping Operations an Special Political Missions”. Forrás: https://police.un.org/sites/default/files/sgf-guidelines_police_operations-2015.pdf (Elérés: 2022. március 30.).

US Army. 2010. „Cyberspace Operations Concept Capability Plan 2016-2028”. Forrás: https://irp.fas.org/doddir/army/pam525-7-8.pdf (Elérés: 2022. május 1.).

US Joint Staff. 1995. „Joint Doctrine for Military Operations Other Than War”. Forrás: https://www.bits.de/NRANEU/others/jp-doctrine/jp3_07.pdf (Elérés: 2022. március 30.).

US Joint Staff. 2013. „Cyberspace Operations - Joint Publication 3-12”. Forrás: https://fas.org/irp/doddir/dod/jp3_12r.pdf (Elérés: 2021. július 15.).

Valeriano, Brandon, Jensen, Benjamin és Maness, Ryan C. 2018. „Cyber Strategy: The Evolving Character of Power and Coercion”. Forrás: https://oxford.universitypressscholarship.com/view/10.1093/oso/9780190618094.001.0001/oso-9780190618094. (Elérés: 2022. április 19.)

Ventura County Sheriff's Office. 2019. „Tactical Response Team - Standard Operating Procedures”. Forrás: https://s29762.pcdn.co/wp-content/uploads/2019/12/Tactical-Response-Team-SOP-Redacted.pdf (Elérés: 2022. április 12.).

Verizon. 2021. „DBIR - 2021 Data Breach Investigation Report”. Verizon. Forrás: https://www.verizon.com/business/resources/reports/2021/2021-data-breach-investigations-report.pdf (Elérés: 2022. április 3.).

Villalón-Huerta, Antonio, Ripoll-Ripoll, Ismael és Marco-Gisbert, Hector. 2022. „Key Requirements for the Detection and Sharing of Behavioral Indicators of Compromise”. *Electronics 2022/1*. Forrás: https://www.mdpi.com/2079-9292/11/3/416 (Elérés: 2022. április 1.).

Vitkauskas, Dovydas. 1999. „The Role of a Security Intelligence Service In a Democracy”. NATO. Forrás: https://www.nato.int/acad/fellow/97-99/vitkauskas.pdf (Elérés: 2022. március 31.).

Voo, Julia, Hemani, Irfan, Jones, Simon, DeSombre, Winnona, Cassidy, Daniel és Schwarzenbach, Anina. 2020. „National Cyber Power Index 2020”. Forrás: https://www.belfercenter.org/sites/default/files/2020-09/NCPI_2020.pdf. (Elérés: 2021. július 17.).

Votel, Joseph L, Cleveland, Charles T, Connett, Charles T és Irwin, Will. 2016. „Unconventional Warfare in the Gray Zone”. *Joint Force Quarterly 2016/1.* Forrás: https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-80/jfq-80_101-109_Votel-et-al.pdf Elérés: 2022. március 30.).

Völgyi, Zoltán. 2017. „A különleges műveleti erők funkcionális elődei a magyar hadtörténelemben”. *Hadtudomány 2017*. Forrás: http://real.mtak.hu/70284/1/volgyi2.pdf (Elérés: 2021. július 24.).

Vykopal, Jan, Oslejsek, Radek, Celeda, Pavel, Vizvary, Martin és Tovarnak, Daniel. 2017. „KYPO Cyber Range: Design and Use Cases”: In *Proceedings of the 12th International Conference on Software Technologies*, Madrid, Spain: SCITEPRESS - Science and Technology Publications. Forrás: http://www.scitepress.org/DigitalLibrary/Link.aspx?doi=10.5220/0006428203100321 (Elérés: 2022. május 2.).

Walsh, Katherine. 2008. „Northrop Grumman’s Timothy McKnight on Security and Identity Management”. *CSO Online*. Forrás: https://www.csoonline.com/article/2122398/northrop-grumman-s-timothy-mcknight-on-security-and-identity-management.html (Elérés: 2022. február 18.).

Warren, Tom. 2020. „Zoom Announces 90-Day Feature Freeze to Fix Privacy and Security Issues”. *The Verge*. Forrás: https://www.theverge.com/2020/4/2/21204018/zoom-security-privacy-feature-freeze-200-million-daily-users (Elérés: 2022. május 1.).

Watts, Stephen, Zeigler, Sean M., Jackson, Kimberly, McCulloch, Caitlin, Cheravitch, Joe és Kepe, Marta. 2021. „Countering Russia: The Role of Special Operations Forces in Strategic Competition”. RAND Corporation. Forrás: https://www.rand.org/pubs/research_reports/RRA412-1.html (Elérés: 2022. március 29.).

Websense. 2011. „Debunking APT myths: What it really means and what you can do about it”. Websense. Forrás: http://docs.media.bitpipe.com/io_10x/io_100921/item_427199/Websense_sSecurity_IO%23100921_E-Guide_072811.pdf (Elérés: 2022. február 18.).

Weedon, Jen. 2018. „Beyond ‘Cyber War’: Russia’s Use of Strategic Cyber Espionage and Information Operations in Ukraine”. Forrás: https://ccdcoe.org/uploads/2018/10/Ch08_CyberWarinPerspective_Weedon.pdf (Elérés: 2022. március 22.)

Yoo, Gene. 2021. „Council Post: The Importance Of Time And Speed In Cybersecurity”. *Forbes*. Forrás: https://www.forbes.com/sites/forbestechcouncil/2021/01/22/the-importance-of-time-and-speed-in-cybersecurity/ (Elérés: 2022. április 28.).

Yue, Yi, és Henshaw, Michael. 2009. „An Holistic View of UK Military Capability Development”. *Defense & Security Analysis*. Forrás: https://www.tandfonline.com/doi/abs/10.1080/14751790902749900 (Elérés: 2022. március 11.).

Zerodium. é.n. „ZERODIUM - How to Sell Your Zero-Day (0day) Exploit to ZERODIUM”. Forrás: https://zerodium.com/program.html (Elérés: 2022. április 27.).

Zhang, Li. 2012. „A Chinese Perspective on Cyber War”. *International Review of the Red Cross. 2012/06*. Forrás: https://www.cambridge.org/core/product/identifier/S1816383112000823/type/journal_article (Elérés: 2022. március 24.).

Függelék

AZ ÉRTEKEZÉSBEN SZEREPLŐ ÁBRÁK ÉS TÁBLÁZATOK JEGYZÉKE

1. ábra: A fejlett perzisztens fenyegetések támadási életciklusa 36
2. ábra: A hagyományos és az APT támadások összehasonlítása 37
3. ábra: A kifinomult kibertámadások keretrendszere 87
4. ábra: A fejlett perzisztens fenyegetések jellemzőinek dominancia alapú vizsgálata 127
5. ábra: A katonai (honvédelmi), rendvédelmi és nemzetbiztonsági különleges műveleti képességek és a fejlett perzisztens fenyegetések jellemzőinek dominancia alapú vizsgálata 148
6. ábra: A kiberműveletek passzív és aktív védelmet, valamint offenzív műveleteket is magába foglaló teljes spektruma 167
7. ábra: A kiber különleges műveleti erők felkészítésének négy pillére 189
8. ábra: A teljes spektrumú kiberműveleti képességek és a kiber különleges műveleti erők modelljének sematikus ábrázolása az offenzív és defenzív tevékenységek indikátor központú skálázódása alapján 192
9. ábra: A védelmi kiadások különböző aspektusokból vizsgálva 205-206

IRÁNYÍTOTT INTERJÚK KÉRDÉSEI

1. Mit gondol a kiber különleges műveleti erők létjogosultságáról?
2. A szervezeti integrációs modelleket (haderő, rendvédelem, nemzetbiztonság, önálló szerv, privát) mérlegelve, melyiknek a megvalósítása járna a legtöbb előnnyel/hátránnyal?
3. A demokratikus kontroll fenntartása tekintetében mi a véleménye a képességgel összefüggő jogszabályi változtatásokról és/vagy kapcsolódó igazságügyi, illetve kormányzati struktúra kialakításáról?
4. Véleménye szerint kiből lehet jó kiber különleges műveleti operátor?
5. Milyen arányban célszerű elosztani a technikai, fizikai, mentális és egyéb képességeket a toborzás és kiválasztás, illetve a kiképzés és gyakorlatozás tekintetében?

6. Mit gondol, milyen feltételek biztosítása szükséges a kiber különleges műveleti tevékenységhez, mik az ideális körülmények egy ilyen képesség számára a kialakításra és működtetésre vonatkozóan?
7. Milyen és mekkora erőforrások szükségesek a kiber különleges műveleti képesség kialakításához és működtetéséhez?
8. Véleménye szerint milyen elemekből épülne fel és milyen elsődleges feladatok végrehajtására lenne képes egy kiber különleges műveleti erő/alakulat?
9. Milyen kockázatokat, kihívásokat és veszélyeket rejt a kiber különleges műveleti képesség kialakítása?
10. Van-e bármilyen téma, amit a fenti kérdések nem érintettek, de fontos lehet a kiber különleges műveleti képességek kapcsán?

INTERJÚALANYOK

A téma érzékenységére való tekintettel az interjúalanyok – kérésüknek megfelelően – nem kerülnek nevesítésre. Az értekezés szempontjából lényeges szakterület, illetve szakmai háttérre utaló információk az interjúalanyok hozzájárulásával kerülnek megosztásra.

1. Nemzetbiztonsági szervezet korábbi (kiber) területi vezetője
2. Kiberbiztonsági vállalkozás vezetője, nemzetközi kiberbiztonsági szervezet képviselője
3. Belügyi ágazat operatív középvezetője
4. Privát kiberbiztonsági szakértő
5. Nemzetbiztonsági szervezet korábbi operatív tisztje
6. Nemzetbiztonsági szervezet korábbi középvezetője
7. Nemzetbiztonsági szervezet felsővezetője
8. Honvédelmi terület különleges műveleti felsővezetője

RÖVIDÍTÉSEK JEGYZÉKE

RÖVIDÍTÉS	KIFEJEZÉS ANGOLUL (MAGYARUL)
ACD	Active Cyber Defense (Aktív Kibervédelem)
ACRP	Airport Cooperative Research Program (Reptéri Kooperatív Kutatási Program)
ACSC	Australian Cyber Security Centre (Ausztrál Kiberbiztonsági Központ)
ACT	Allied Command Transformation (Szövetséges Transzformációs Parancsnokság)
ADV2E	Advanced Adversary Emulation (fejlett ellenfél emuláció)
ADV2S	Advanced Adversary Simulation (fejlett ellenfél szimuláció)
AJP-3.20	Allied Joint Publication-3.20 (Szövetséges Összhaderőnemi Publikáció-3.20)
ANG	Air National Guard (Légi Nemzeti Gárda)
APT	Advanced Persistent Threat (Fejlett Tartósan Fennálló Fenyegetés)
ARPANET	Advanced Research Projects Agency Network (Fejlett Kutatási Projektek Ügynökség Hálózata)
BSI*	Federal Cyber Security Authority (Információbiztonsági Szövetségi Hivatal)
CCaaS	Cyber Capability as a Service (Kiberképesség mint szolgáltatás)
CC CSC	Competence and Certification Cyber Security Centre (Kiberbiztonsági Kompetencia és Tanúsító Központ)
CCDCOE	Cooperative Cyber Defense Centre of Excellence (Kooperatív Kibervédelmi Kiválósági Központ)
CCDP	Comprehensive Cyber Defense Policy (Átfogó Kibervédelmi Politika)
CCM	Cyber Crisis Management (Kiber-válságkezelés)
CDP	Capability Development Plan (Képességfejlesztési Terv)
CDP	Cyber Defense Pledge (Kibervédelmi Fogadalom)
CERT	Computer Emergency Response Team (Számítógépes Vészhelyzeti Reagáló Csapat)
CFC	Cybersecurity Fusion Center (Kiberbiztonsági Fúziós Központ)

CIA	Central Intelligence Agency (Központi Hírszerző Ügynökség)
CISA	Cybersecurity & Infrastructure Security Agency (Kiberbiztonsági & Infrastruktúra-biztonsági Ügynökség)
CKC	Cyber Kill Chain (Kifinomult Kibertámadások Keretrendszere)
CMF	Cyber Mission Force (Kiber Missziós Erő)
CMF	Combat Mission Force (Harci Missziós Erő)
CMC	Central Military Commission (Központi Katonai Bizottság)
CNMF	Cyber National Mission Force (Kiber Nemzeti Missziós Erő)
CNO	Computer Network Operations (Számítógépes Hálózati Műveletek)
COMINT	Communications Intelligence (Távközlési-, rádiófelderítés)
CPT	Cyber Protection Team (Kibervédelmi Csapatok)
CRRT	Cyber Rapid Response Teams (Kiber Gyorsreagálású Csapatok)
CRS	Congressional Research Service (Kongresszusi Kutató Szolgálat)
CSDP	Common Security and Defense Policy (Közös Biztonsági- és Védelempolitika)
CSFC	Cybersecurity Fusion Center (Kiberbiztonsági Fúziós Központ)
CSIS	Centre for Strategic & International Studies (Stratégiai & Nemzetközi Tanulmányok Központ)
CSS	Center for Security Studies (Biztonsági Tanulmányok Központ)
CSSG	Cyber Security Steering Group (Kiberbiztonsági Kormányzó Csoport)
CTI	Cyber Threat Intelligence (Kiberfenyegetési hírszerzés)
CYBERCOM	Cyber Command (Kiberparancsnokság)
CyberSpt	Cyber Support (kibertámogatás)
CYOC	Cyberspace Operations Center (Kibertér Műveleti Központ)
C2 (C&C)	Command and Control (Parancs és Irányítás)
C4	Cyber Crime Competence Center (Kiberbűnözési Kompetencia Központ)
DCAF	Geneva Centre for the Democratic Control of Armed Forces (Fegyveres Erők Demokratikus Ellenőrzésének Genfi Központja)

DCO	Defensive Cyberspace Operations (Defenzív Kibertér Műveletek)
DDOS	Distributed Denial of Service (Elosztott szolgáltatásmegtagadás)
DNS	Domain Name System (Domén Név Rendszer)
DO	Directorate of Operations (Műveleti Igazgatóság)
DOD	Department of Defense (Védelmi Minisztérium)
DODIN	Departmnet of Defense Information Network (Védelmi Minisztérium Információs Hálózat)
EBESZ	Európai Biztonsági és Együttműködési Szervezet
ECD	Electronic Countermeasures Department (Elektronikai Elhárító Részleg)
ECS	European Cyber Shield (Európai kiberpajzs)
EDA	European Defense Agency (Európai Védelmi Ügynökség)
ELINT	Electronic Intelligence (Rádiótechnikai felderítés)
ENISA	European Network and Information Security Agency (Európai Hálózat és Információ Biztonsági Ügynökség)
ENSZ	Egyesült Nemzetek Szervezete
EU	European Union (Európai Unió)
EUMC	European Union Military Committee (Európai Unió Katonai Bizottság)
EUMS	European Union Military Staff (Európai Unió Katonai Törzs)
EWI	East West Institute (Kelet Nyugat Intézet)
FMoD	Federal Ministry of Defense (Szövetségi Védelmi Minisztérium)
FSB*	Federal Security Service (Szövetségi Biztonsági Szolgálat (Polgári Elhárítás))
FSO*	Federal Protection Service (Szövetségi Védelmi Szolgálat)
GAO	Government Accountability Office (Kormányzati Számvevőszék)
GDP	Gross Domestic Product (Bruttó hazai össztermék)
GPS	Global Positioning System (Globális Helymeghatározó Rendszer)
GROM*	Polish Special Forces Unit (Lengyel különleges műveleti egység)
GRU*	Main Intelligence Directorate of the General Staff of the Armed Forces of the Russian

	Federation (Az orosz fegyveres erők vezérkarának Felderítő Főcsoportfőnöksége)
HUMINT	Human Intelligence (Humánerőforrás alapú hírszerzés)
IBM	International Business Machines (amerikai multinacionális technológiai vállalat)
ICO	Information Commissioner's Office (Információbiztosi Iroda
ICS	Industrial Control System (Ipari Folyamatirányító Rendszer)
IDA	Institute for Defense Analyses (Védelmi Elemzések Intézete)
IDS	Intrusion Detection System (Behatolás Észlelő Rendszer)
IGF	Internet Governance Forum (Internet Kormányzási Fórum)
IH	Információs Hivatal
IMINT	Imagery Intelligence (Képfelvételeken alapuló hírszerzés)
INEW	Integrated Network Electronic Warfare (Integrált Hálózati és Elektronikai Hadviselés)
IoC	Indicators of Compromise (Kompromittálódási Indikátorok)
IoT	Internet of Things (Dolgok Internete)
IPS	Intrusion Prevention System (Behatolás Megelőző Rendszer)
IRGC	Islamic Revolutionary Guard Corps (Iszlám (iráni) Forradalmi Gárda)
ISAC	Information Sharing and Analysis Center (Információ Megosztó és Elemző Központ)
ISACA	Information Systems Audit and Control Association (Információs Rendszerek Audit és Kontroll Egyesülete)
JCU	Joint Cyber Unit (Közös Kiber Egység)
JFHQ-DoDIN	Joint Force Headquarters-DOD Information Network (Összhaderőnemi Főhadiszállás-DOD Információs Hálózatok)
JOA	Joint Operational Area (összhaderőnemi műveleti terület)
KSAOs	Knowledge, Skills, Abilities and Other characteristics (Tudás, Készségek, Képességek és más karakterisztikák)
LMS	Learning Management System (tanuláskezelő rendszer)
MaaS	Malware as a Service (Rosszindulatú szoftver mint szolgáltatás)

MASINT	Measurement and Signature Intelligence (Érzékelésen és szignatúrákon alapuló hírszerzés)
MDO	Multi-Domain Operations (Többdimenziós műveletek)
MICTIC	Malware – Infrastructure – Control Server – Telemetry – Intelligence – Cui bono (Rosszindulatú szoftver – Infrastruktúra – Kontroll Szerver – Telemetria – Hírszerzés – Rejtett motívum)
MitM	Man-in-the-Middle (Közbeékelődés)
MOIS	Ministry of Intelligence and Security (Hírszerzési és Biztonsági Minisztérium)
MOOTW	Military Operations Other Than War (Nem háborús katonai műveletek)
MSS	Ministry of State Security (Állambiztonsági Minisztérium)
NASA	National Aeronautics and Space Administration (Nemzeti Repülési és Űrhajózási Hivatal)
NATO	North Atlantic Treaty Organization (Észak-Atlanti Szerződés Szervezete)
NBS	Nemzeti Biztonsági Stratégia
NCAE-C	National Centers of Academic Excellence in Cybersecurity (Nemzeti Kiberbiztonsági Akadémiai Kiválósági Központ)
NCC	National Cybersecurity Center (Nemzeti Kiberbiztonsági Központ)
NCC	National Cyberspace Center (Nemzeti Kibertér Központ)
NCD	National Cyber Directorate (Nemzeti Kiber Igazgatóság)
NCS	National Clandestine Service (Nemzeti Titkosszolgálat)
NDPP	NATO Defece Planning Process (NATO Védelmi Tervezési Folyamat)
NIST	National Institute of Standards and Technology (Nemzeti Szabványügyi és Technológiai Intézet)
NKS	Nemzeti Katonai Stratégia
NMF	National Mission Force (Nemzeti Missziós Erő)
NPDO	National Passive Defense Organization (Nemzeti Passzív Védelmi Szervezet)
NSA	National Security Agency (Nemzetbiztonsági Ügynökség)

OCO	Offensive Cyberspace Operations (Offenzív Kibertér Műveletek)
OCS	Operational Coordination Structure (Operatív Koordinációs Struktúra)
OIST	Okinawa Institute of Sience and Technology (Okinawa Tudományos és Technológiai Intézet)
OSINT	Open Source Intelligence (Nyílt forrású hírszerzés)
Pentest	Penetration testing (behatolásvizsgálat)
PLA	People's Liberation Army (Népi Felszabadító Hadsereg)
PLASSF	People's Liberation Army Strategic Support Force (Népi Felszabadító Hadsereg Stratégiai Támogató Erő)
PLC	Programmable Logic Controller (Programozható Logikai Vezérlők)
PMC	Private Military Company/Contractor (Katonai Magánvállalat)
PPP	Public Private Partnership (Köz- és magánegyüttműködés)
RaaS	Ransomware as a Service (Zsaroló szoftver mint szolgáltatás)
RAND	Research and Development (Amerikai agytröszt)
RGB	Reconnaissance General Bureau (Központi Felderítő Iroda)
SANS	Escal Institute of Advanced Technologies
SARS-CoV-2	Severe acute respiratory syndrome coronavirus 2 (Súlyos akut légzőszervi szindróma koronavírus 2)
SAS	Special Air Service (Különleges Légiszolgálat)
SCADA	Supervisory Control and Data Acquisition (Folyamatirányító és adatgyűjtő)
SCC	Supreme Council for Cyberspace (Legfelsőbb Kibertér Tanács)
SEAL	Sea Air Land (Tenger levegő szárazföld (az amerikai haditengerészet különleges alakulata))
SIGINT	Signals Intelligence (Jelfelderítés)
SIGOV CERT	Slovenia Government Computer Emergency Response Team (Szlovén Kormányzati Számítógépes Eseménykezelő Központ)
SOC	Security Operations Center (Biztonsági Műveleti Központ)

SOCOM	Special Operations Command (Különleges Műveleti Parancsnokság)
SOF	Special Operations Force (Különleges Műveleti Erő)
SOMINT	Social Media Intelligence (Közösségi média hírszerzés)
SSF	Strategic Support Force (Stratégiai Támogató Erő)
STRATCOM COE	Strategic Communications Centre of Excellence (Stratégiai Kommunikációs Kiválósági Központ)
SVR*	Foreign Intelligence Service (Külföldi Hírszerző Szolgálat)
SWAT	Special Weapons and Tactics (Speciális Fegyverek és Taktikák)
SWIFT	Society for Worldwide Interbank Financial Telecommunications (Globális Bankközi Pénzügyi Telekommunikációs Társaság)
SYN	Synchronize (Szinkronizáló)
SYN ACK	Synchronize-Acknowledgement (Szinkornizáló-Nyugtázás)
TAO	Tailored Access Operations (Célzott Hozzáférési Műveletek)
TCP/IP	Transmission Control Protocol / Internet Protocol (Átviteli Vezérlő Protokoll / Internet Protokoll)
TTP	Tools/Tactics, Techniques and Procedures (Eszközök/taktikák, Technikák és Módszerek)
UN	United Nations (Egyesült Nemzetek)
UNCLOS	United Nations Convention ont he Law of the Sea (Egyesült Nemzetek Tengerjogi Egyezménye)
USAF	United States Air Force (Egyesült Állami Légierő)
USD	United States Dollar (Egyesült Államok pénzneme – dollár)
USNI	United States Naval Institute (Egyesült Államok Haditengerészeti Intézet)
VA	Vulnerability Assessment (Sérülékenység értékelés/felmérés)

*: A rövidítést az eredeti nyelven történő feloldás alapján használom.

A SZERZŐ TÉMAKÖRBEN MEGJELENT PUBLIKÁCIÓI

BERZSENYI Dániel: Kiberbiztonság. In: TÁLAS Péter Henrik – CSIKI Tamás – ETL Alex – BERZSENYI Dániel (szerk.): *A globalizált világ kihívásai*. Nemzeti Közszolgálati Egyetem, Ludovika Egyetemi Kiadó, Budapest, 2021, 341-358. o.

BERZSENYI Dániel – EDEGBEME-BELÁZ Annamária: Hungary's evolving cyber security strategy. In: MANJIKIAN Mary – ROMANIUK Scott N. (szerk.): *Routledge Companion to Global Cyber-Security Strategy*. Routledge, London, 2021, 99-110. o.

BERZSENYI Dániel: A kibertér aktuális nemzetközi biztonságpolitikai kihívásai. In: BERZSENYI Dániel – BODÓ Attila Pál – KAPITÁNY Sándor – SÁGI Gábor János – SEBŐK Viktória (szerk.): *Incidensmenedzsment. Éves továbbképzés az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy számára 2017*. Dialóg Campus Kiadó, Budapest, 2017, 6-22. o.

BERZSENYI Dániel – EDEGBEME-BELÁZ Annamária: Kiberbiztonsági Stratégia 2.0: A kiberbiztonság stratégiai irányításának kérdései. *SVKK Elemzések, 2017/3*. [online], Elérhető: https://svkk.uni-nke.hu/document/svkk-uni-nke-hu-1506332684763/svkk-elemzesek-2017-4-harom-evvel-az-ukrajnai-hatalomatvetel-utan-talas-p.original.pdf [2022. 07. 16.]

BERZSENYI Dániel: Globális kihívás, regionális válaszok: kiberbiztonság Kelet-Közép-Európában. *Nemzet és Biztonság – Biztonságpolitikai Szemle*. 10. évf., 2017/3. szám, 69-79. o.

BERZSENYI Dániel: A kiberbiztonság humán oldala. *Nemzet és Biztonság – Biztonságpolitikai Szemle*. 10. évf., 2017/2. szám, 54-67. o.

BERZSENYI Dániel – VÁNYI Rajmond: Egy katonapolitikai döntés lehetséges kiberbiztonsági következményei: az Iszlám Állam elleni magyar katonai szerepvállalás margójára. *Nemzet és Biztonság – Biztonságpolitikai Szemle*. 8. évf., 2015/3. szám, 134-143. o.

BERZSENYI Dániel: New dimension in V4 defense cooperation. A comparative analysis of the cybersecurity strategies of CECSP countries. Visegrad Plus – Forum for Visegrad+ Studies. 2015. 01. 18. [online] Elérhető: https://web.archive.org/web/20160611071807/http://visegradplus.org/analyse/new-dimension-v4-defense-cooperation-comparative-analysis-cybersecurity-strategies-cecsp-countries/ [2022. 07. 22.]

BERZSENYI Dániel: Kiberbiztonsági analógiák és eltérések. A Közép-európai Kiberbiztonsági Platform részes országai által kiadott kiberbiztonsági stratégiák összehasonlító elemzése. *Nemzet és Biztonság – Biztonságpolitikai Szemle*. 7. évf., 2014/6. szám, 110-136. o.

BERZSENYI Dániel – SZABÓ I. László: A védelmi szektor néhány elemének transzfomációja. In: TÁLAS Péter Henrik – CSIKI Tamás (szerk.): *Magyar biztonságpolitika 1989-2014 - Tanulmányok*. Nemzeti Közszolgálati Egyetem, Nemzetközi Intézet, Budapest, 2014, 37-58. o.

BERZSENYI Dániel – SZENTGÁLI Gergely: STUXNET: a virtuális háború hajnala. *Biztonságpolitika: Biztonságpolitikai Szakportál*, Budapest, 2010. [online] Elérhető: http://www.biztonsagpolitika.hu/?id=16&aid=932&title=STUXNET:_a_virtu%C3%A1lis_h%C3%A1bor%C3%BA_hajnala [2022. 07. 16.]