MÉDIATUDOMÁNYI KÖNYVTÁR

FARKAS ÁDÁM –
KELEMEN ROLAND

NEMZETI BIZTONSÁG ÉS KIBERTÉR

Nemzeti Média- és Hírközlési Hatóság
Médiatanács • Médiatudományi Intézet

Nemzeti biztonság és kibertér

Médiatudományi Könyvtár

50.

Sorozatszerkesztő:

Koltay András – Nyakas Levente: 2012–2019
Nyakas Levente – Szadai Károly: 2020–

Farkas Ádám – Kelemen Roland

Nemzeti biztonság és kibertér

Médiatudományi Intézet

2023

Egyes fejezetek szerzői:
Farkas Ádám (Első rész II. fejezet 1–3., Második rész I., VI. fejezet, Negyedik rész)
Kelemen Roland (Első rész I. fejezet, II. fejezet 4., Második rész II–V. fejezet, Harmadik rész)

Szakmai lektor:
Smuk Péter
Németh Richárd

A kutatást támogatta:

NMHH
Nemzeti Média- és Hírközlési Hatóság
Médiatanács • Médiatudományi Intézet

Tartalom

Ajánlás

Farkas Ádám és Kelemen Roland arra vonatkozó felkérését, hogy „Nemzeti biztonság és kibertér" című kötetükhöz ajánlást írjak, több okból a legnagyobb megtiszteltetésnek tartottam. Mindkét kolléga a Széchenyi István Egyetem Állam- és Jogtudományi Doktori Iskolájának alumnusa, szakmai pályájuk anyaintézményünkben, a Nemzeti Közszolgálati Egyetemen, továbbá a Katonai Nemzetbiztonsági Szolgálat kötelékében párhuzamosan, egymást támogatva halad előre, teljesedik ki. A kiemelkedő tudományos értéket képviselő, oktatási tevékenységet is magas színvonalon szolgáló könyv nemcsak a szerzők szakmai felkészültségét tükrözi vissza, hanem évtizedekre visszatekintő barátságukat, kollegiális együttműködésüket is.

A kötet amellett, hogy az akadémiai írás minden kritériumának kiválóan megfelel, így elsősorban a kiberbiztosnság témájával foglalkozó szakemberek referencia dokumentuma lesz, az egyén számára, személyes kiberbiztonságát illetően, rendkívüli információtartalommal és jelentőséggel bír. A tiszteletre méltó szakmai alázattal megírt könyv mindemellett stílusos, érdekes, a figyelmet nem lankadni hagyó olvasmány is. Az interdiszciplináris megközelítés, illetve a más tudományterületekről, például az orvostudományból merített analógiák ahhoz járulnak hozzá, hogy az olvasó az átfogó és komplex elemzést magáénak érezze.

Végül annak komprehenzív jellege, a kiberbiztonság vertikumának és horizontális spektrumának teljeskörű áttekintése okán tartom egyedülállóan magas színvonalúnak a kötetet, ami a vonatkozó szabályozás nemzetközi szervezet általi, regionális integrációs szintet és nemzetállami szabályozási modelljeit egyaránt lefedi.

Lukács Eszter
Nemzetközi stratégiai elnök-helyettes
Széchenyi István Egyetem

Előszó

A 21. század első felében egyértelmű, hogy az info-kommunikáció robbanásszerű elterjedésének és egyben fejlődésének időszakát éljük. Ez a változás technikai alapokon nyugszik, de ma már vitán felül áll, hogy jószerével az élet minden területét áthatja, érinti, formálja. Az információs rendszerek fejlődése, hordozhatósága és minél kompaktabb megjelenés melletti minél nagyobb teljesítménye újrarajzolja azokat a képzeletbeli vonalakat, amelyekkel életünk képesíthető módon leírható.

A digitalizáció már önmagában jelentékeny módon hat az emberi létezés legfőbb szegmenseire. A gazdaság, a különféle ügyek intézése, a munkavégzés, az oktatás-képzés, a tudományos és műszaki tevékenységek, illetőleg a biztonság fenntartása és megerősítése mind-mind jelentős mértékben változott az elmúlt évtizedekben a digitalizációnak köszönhetően. Az a hatás-mátrix, amit a digitális technológia evolúciója és elterjedése magával hozott, sokkal szélesebb azonban, hiszen életünk minden területén jelen van a „kötött" időszakokon – munkavégzésen, tanulmányok folytatásán, ügyintézésen stb. – túl a szabadidőnk eltöltésén át a személyes kapcsolatainkig.

E hatásrendszert pedig hatványozza az internet mind szélesebb és szélesebb körben való elérhetősége. Az internet jóvoltából széles körben – de nem teljeskörűen – bomlottak le a fizikai távolságok jelentette korlátok, és lényegében azzal, hogy a kommunikáció és az online cselekvések révén a világ másik fele valós időben érhető el, kiteljesedett a globalizáció folyamata is. Az internet révén a világ különféle számítógépes hálózatai, információs rendszerei egy nagy, globális hálóba kapcsolhatók össze, melyben ezáltal az információk terjedésének és kialakulásának, az emberi kapcsolatoknak, továbbá a cselekvésnek is új módozatai és keretei alakulnak ki. Nagyon leegyszerűsítve, a számítógépes rendszerekre és a felhasználókra épített volta miatt a fizikai térből táplálkozó, de részint önálló és alternatív teret képezve így alakult ki a kibertér.

A kibertér hatalmas lehetőségeket rejt magában, hiszen nem csak történelmileg még soha nem látott közvetítő közege lehet a különféle kultúrák jó értelemben vett kölcsönhatásainak, hanem az innovációs és gazdasági tevékenységek hatékonyabbá tételét, illetőleg a világ különféle pontjain lévő összekapcsolható szaktudások kooperációját is rendkívüli mértékben segítheti. Szükségszerű azonban, hogy a pozitívumok mellett a kibertér negatívumokat is rejt magában, melyek sorából az emberi viselkedésre gyakorolt egyéni és csoportszintű kártékony hatásoktól, a célzottan torz vagy hamis információk terjesztésén át egészen az ártó/támadó célú információs cselekményekig, ha úgy tetszik, információs műveletekig széles a skála. A kibertér tehát rendkívüli kihívást jelent az egyének és a nemzetek biztonságára is.

A kibertér jellegének és hatásainak elemzése-értékelése, illetve hatásmechanizmusainak defenzív és offenzív alkalmazása az elmúlt évek, lassan inkább évtizedek kiemelt témája. Az államok, azok szövetségei és nemzetközi kapcsolódási platformjai a különféle kibertérből következő kihívásokra törekedtek újabb és újabb válaszokat adni. A kiberteret érintő nemzeti és európai uniós szabályozási törekvések, a nemzetközi jog kibertérben zajló tevékenységekre való alkalmazhatósága, a kiberbiztonsági hatóságok és különféle állami képességek fejlesztése vagy épp az erre irányuló kutatások ösztönzése mind-mind egyértelműen tükrözi ezt az irányt. Látni kell azonban, hogy az elmúlt évekig a kibertér és a biztonság viszonyát, különö-

sen az állami fellépés tematikáját jelentős mértékben a műszaki-technikai, illetőleg a katonai-rendészeti-nemzetbiztonsági műveleti megközelítés határozta meg. Ez valahol érthető, hiszen maga az az újdonság, amit esszenciájában a kibertér jelent, végső soron technikai bázisú, számítógép-hálózatok véges-végtelen összekapcsolódására, illetve azokon keresztül technikai jellegű – programozott és virtuális – cselekmények sorozatára épül, amire elsőként a technikai válaszok tűnnek adekvátnak. Az elmúlt évek nagy előrelépése azonban, hogy egyre nagyobb jelentőséget tulajdonítunk a kiberteret kiaknázó felhasználóknak, vagyis a humán tényezőnek, amelynek jelentősége a biztonság felől nézve legalább akkora – ha nem nagyobb –, mint a technikai dimenziónak.

A kibertéren keresztül megjelenő sérülékenységek kiaknázásához alapvetően emberi közrehatás kell vagy a rendszert tervező, az alkalmazott szoftvereket fejlesztő, vagy épp az üzemeltető/felhasználó személyek vonatkozásában, nem beszélve arról, hogy a beavatkozó oldalon is szükséges az emberi fellépés, akár aktív cselekvéssel, akár egy káros kód kifejlesztésével. Innen nézve a technikai behatás lehetősége sem választható el az embertől a maga teljességében. Az emberi tényező biztonsági vonatkozása azonban a kibertér kapcsán ennél sokkal szélesebb, hiszen a kibertér a fizikai tértől részint különváló alternatív térként egy globális, valós idejű információs csatornarendszer is egyben. A kibertér ma már egy, a glóbusz jelentős részére kiterjedő információs idegrendszer, amelynek azonban nincs kifejezett központja és perifériális részei sem csak egy ponton kapcsolódnak a hálózat egészéhez. Mint ilyen, lehetőséget teremt arra, hogy az embereket gyorsabban, megbízhatóbban juttassa információkhoz, de arra is, hogy mind egyéni, mind csoportos szinten téves, torz, hamis információkkal lássa el őket, ezáltal pedig végső soron szemléletbeli, érzetbeli, cselekvésbeli befolyásoló hatást fejtsen ki.

Az emberi gondolkodás kibertér útján történő befolyásolása rendkívül jelentős biztonsági kihíváshalmazt fed le. Az egyéni és kisebb csoportos szinten a radikalizáció erősítése épp úgy opció, mint a kibertérben, vagy annak felhasználásával megvalósuló bűnözési módozatok fokozódása. A makro szintű információs hatások azonban rendkívüliek lehetnek, hiszen a bizalom különféle területeire hatnak, így gazdasági hatások kiváltására épp úgy alkalmasak lehetnek, mint a biztonságérzet alakítására, a legitimitás aláaknázására, illetve alternatív helyzetértékelések kialakítására egy-egy kérés kapcsán. E tekintetben fontos látni, hogy a biztonság megóvása, sőt megerősítése érdekében úgy kell új kereteket adni a működésnek, hogy azok közben ne hátráltassák a kibertérből származó előnyök kibontakozását, sőt fokozását a jövőben.

A nemzeti biztonság és a kibertér relációjában ezért úgy véljük, hogy megkülönböztetett az állam szerepe, de még a biztonság fenntartásában – kikényszerítésében – sem tekinthető immár megkerülhetetlen aktornak, mivel a kibertérnek nincs központja, felhasználóinak száma pedig nem átfogható. Az államnak ezért nélkülözhetetlen a társadalmi és gazdasági szereplőkkel együttműködve szavatolnia a biztonságot, és az ehhez szükséges szabályozási, intézményi és képességbeli kereteket, hiszen közös érdek a kibertérben rejlő fenyegetések és veszélyek mérséklése, ebből következően pedig a fejlődési és gyarapodási lehetőségek fokozása.

Ahhoz, hogy ezt a kívánt szerepfelfogást elő tudjuk mozdítani, fontos, hogy a kibertérrel kapcsolatos gondolkodás a szabályozás és igazgatás dimenziójában, illetve a biztonság állami szavatolása és megóvása tekintetében is fejlődni tudjon. Erre figyelemmel jelen kötetben arra törekszünk, hogy a nemzeti biztonság és a kibertér viszonya kapcsán az előzőekben összefoglalt irányultságnak megfelelően értelmezzük (1) a kibertér fogalmát; (2) hatásait az államra,

társadalomra és egyénekre; (3) kapcsolódásait a modern biztonsági kihívásokhoz és fenyegetésekhez; (4) Európai Uniós és NATO-s vonatkozásait; (5) helyét és szerepét a védelem és biztonság – angolszász megfogalmazással: a nemzetbiztonság – jogi és intézményi rendszerében.

A jelen kötet célja egyfajta multidiszciplináris megközelítés alapjainak rögzítése mindazok számára, akik a nemzeti szintű biztonság és a kibertér számos-számtalan kérdéssel és kihívással terhelt, de ki nem kerülhető kapcsolatának emberi, társadalmi, állami, gazdasági, jogi és védelmi vonatkozásai iránt érdeklődnek. E megközelítés talán elősegítheti idővel egy olyan közös gondolkodási módozat kibontakozását, amely nemcsak egymás mellé állítja, vagy eseti jelleggel összekapcsolja a különféle érintett szakterületeket, hanem egy új és valóban kölcsönhatásos, azaz a kezelendő jelenségek és a különféle kezelési módok jobb megértését is szolgáló, interoperábilis értelmezési sémaként tudja szolgálni a fejlődéssel járó valamennyi érdek fenntartható egyensúllyal párosuló érvényesülését.

***

A jelen kötet szakmai tartalmának létrejöttét a lengyel Fulbright bizottság által gondozott *Cybersecurity in universities – study visits to the U.S.* programhoz kapcsolódó pályázati keretrendszer biztosította, és reményeink szerint mint eredmény rövidesen felhasználásra kerül a Széchenyi István Egyetemen kibontakozó kiberbiztonsági tárgyak oktatása, illetve további kutatások megalapozása során. Ugyanakkor ki kell emelni, hogy a kötetben foglaltak a szerzők számos korábbi kutatási eredményére építenek, így Kelemen Roland tekintetében a Széchenyi István Egyetem Deák Ferenc Állam- és Jogtudományi Karán végzett kutató és oktató munka mellett a Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Karának Honvédelmi Jogi és Igazgatási Tanszékén végzett tevékenységhez is kötődik, Farkas Ádám tekintetében pedig az előbbi két intézményen túl a Katonai Nemzetbiztonsági Szolgálat Tudományos Tanácsában, illetőleg a hazai védelmi és biztonsági szféra különféle központi igazgatási szerveinél végzett különböző szakértői tevékenységek eredményeire is építkezik.

A kötet megvalósulása kapcsán megkülönböztetett köszönet illeti a Fulbright Poland bizottságot és Anna Kertyczak-ot, továbbá a Széchenyi István Egyetem vezetését, valamint Lukács Eszter elnökhelyettes asszonyt a Fulbright pályázat és a kiberbiztonsági tematika intézményi támogatása miatt, illetőleg Smuk Pétert, a Széchenyi István Egyetem Deák Ferenc Állam- és Jogtudományi Kar dékánját és Németh Richárdot mint jelen kötet lektorait. A kötet nyomdai kivitelezéséért és megjelentetéséért köszönet illeti a Nemzeti Média- és Hírközlési Hatóságot, és kifejezetten Koltay András elnök urat.

Bízunk abban, hogy jelen munka egy hasznosnak mutatkozó hídfőállás lehet annak érdekében, hogy Magyarországon tovább erősödjön az a szemlélet, amely az állam- és jogtudományi gondolkodást és megközelítést egy tágabb társadalomtudományi, emellett számos humántudományi, illetőleg védelmi és biztonsági területtel összekapcsolva tudja mind kutatási, mind oktatási, mind pedig szabályozási és működési szempontból a kibertér biztonságos alkalmazásával kapcsolatos fejlődés szolgálatába állítani.

Győr, 2023. március 20.
a szerzők

I. rész
Alapvetések – Kibertér és biztonság*

1. A kibertér jellemzőinek biztonsági alapú megközelítése

A kibertér fogalmának abszolút érvényű meghatározása, annak multidiszciplináris jellegéből adódóan lehetetlen, sőt kifejezetten tudománytalan vállalkozás volna, hiszen e fogalomban szerepelnie kellene az információs technológia megközelítésnek, a társadalomtudományok, így kifejezetten az állam- és jogtudományi, szociológiai, filozófiai, gazdaságtudományi diszciplínák kapcsolódásainak, valamint legalább ilyen hangsúlyban a természettudományi (geográfia, matematika, fizika) aspektusoknak, továbbá az elmúlt évtizedekben tapasztalható hadi, védelmi célú felhasználása okán a hadtudományi értelmezéseknek is. Ebből kifolyólag ezen fejezet nem azt tűzi ki célul, hogy egy átfogó kibertér fogalmat alkosson meg, hanem egy multidiszciplináris áttekintését kívánja adni a kibertér fogalmi jegyeinek, amellyel megfelelő mélységben tudja megalapozni a könyvben megjelenő fogalmak használatát, és azok felhasználásán alapuló következtetéseket.

A kibertér elnevezés William Gibson nevéhez köthető, aki 1984-es disztópikus sci-fijében, a Neurománcban tette közzé a kifejezést. A regényében egy olyan társadalmat ábrázol, ahol a kibertérhez való csatlakozás a normális emberi létezés alapfeltétele, ennek hiányában az egyén a társadalom peremére szorul. Magát a kiberteret úgy mutatta be, mint egyfajta kollektív hallucinációt vagy benyomást, a számítógépes adatok grafikai reprezentációját.[1] Maga Gibson sem gondolta azt, hogy az általa teremtett világ ilyen mértékben valósággá válik napjainkra. Természtesen merész állítás volna azt kijelenteni, hogy eme disztópia tökéletes leírása jelenkorunk államának vagy társadalmának, azonban napjainkban tapasztalható folyamatok és jelenségek egyes jegyeiben hasonlóságot mutatnak a könyvében felépített világgal (gondoljunk itt példának okáért a közösség média kiterjedtségére és a felhasználói kultúrára), a háttérrendszerek további fejlődése pedig töretlen. Sőt, ezen innováció folyamatosan gyorsul, ami abban fogható meg leginkább, hogy Moore-törvénye,[2] amely szerint az egy chipben lévő tranzisztorok száma körülbelül 18 havonta megduplázódik, napjainkra a technológiai óriásvállalatok álláspontja szerint megdőlt.[3] Az infokommunikációs területnek ez a robbanásszerű fejlődése tehát sok tekintetben fizikai valósággá változtatta Gibson akkor még fikciónak vélt világát, mivel „a globális számítógépes hálózatokban végbemenő kölcsönhatások révén megszületett a kibertér (cyberspace), a kibernetikus világegyetem."[4] E kibertér rendkívül egyedi és összetett jelenség, hiszen leírható fizikai és földrajzi fogalmakkal, emellett azonban virtu-

* Financed from the mini grant provided by Polish-U.S. Fulbright Commission, from Special Congressional Appropriation

1 Gibson (1984): 5.

2 Moore (1965)

3 Moore's Law Is Dead. Where Is Energy Saving Heading in the Electronic Information Industry? *LightReading,* 2022.10.12. www.lightreading.com/moores-law-is-dead-where-is-energy-saving-heading-in-electronic-information-industry/a/d-id/781014

4 Nagy Károly (1999): 173.

ális jellemzői is komoly relevanciával bírnak megismerése során, továbbá rendkívüli térnyerésének következtében újra kell gondolni olyan alapvető területeket is, mint a szociológia, a geopolitika, valamint a biztonságpolitika, vagy éppenséggel a védelmi jog.

A kibertér összetettsége elvárhatóvá teszi, hogy annak fogalmi jellemzése is a multidiszciplinaritás talaján álljon. Ennek a szemléletnek megfelelve kézenfekvő kiindulási pontot ad a fogalom felbontása a kiber és tér szavakra, így pedig a szemlélődés kezdőpontja a kibertér tér jellegének vizsgálata, amely a földrajztudomány, azon belül is a kibergeográfia vagy virtuális geográfia területére visz el minket. A hagyományos természettudományok elkülönült tér értelmezéseket használnak. Megkülönböztetnek abszolutista és relativista térfelfogást. Az abszolutista értelmezés szerint a tér egy változatlan befogadási közeg, amelyet a benne zajló folyamatok nem módosítanak, míg a relativista pontosan az ellenkezőjét gondolja, ugyanis szerintük a tér a benne megjelenő folyamatok révén nyer értelmet. A földrajzi tér fogalma valahol a kettő között helyezhető el, ugyanis az nem azonos a fizikai térrel, de attól nem is független.[5] A földrajzi tér alatt egy összetett jelenséget értenek, amely számos alrendszert foglal magába, amelyek egymásra kölcsönösen hatnak. Ennek a földrajzi térnek az egyik legfontosabb sajátossága, hogy az ember és természet közötti interakció hozza létre, módosítja, alakítja, így ennek köszönhetően fejlődik: „A földrajzi tér tulajdonképpen fizikailag létező struktúrák és az azokról alkotott képzetek, valamint teljesen virtuális, a fizikai térben kézzel nem fogható, ámbátor mindennapjainkban használt, vagy megélt hálózatok összességeként fogható fel".[6] Ez a lényegében ember által formált tér olyan struktúrákat is magába foglal, amelyet a társadalmi viszonyrendszerek hoztak létre, így például a hatalmi struktúrákat vagy az etnikai és vallási struktúrákat.[7] Megelőlegezve a későbbieket: érdekes kérdés, ha a földrajzi térnek része a virtuális tér is, akkor ezen struktúrák ott is megjelennek-e, illetve, ha igen, milyen módon?

Viszont, hogy erre a kérdésre választ tudjunk adni, tovább kell bontani a földrajzi tér fogalmát, és megvizsgálni, hogy a kibertér milyen viszonyban van a földrajzi tér egészével. A földrajzi tér esetében különböző felosztásokkal találkozhatunk. A vertikális metszeteket a vizsgálódás középpontjába helyező megközelítés szerint elkülöníthetünk társadalmi környezetet, épített környezetet, élő környezetet és élettelen környezetet, és akár ezt bővítve virtuális környezetet. E szemlélődés lényege, hogy úgy különítenek el szférákat, hogy hasonló helyekből állítanak össze halmazokat. Egy másik felfogás szerint az egyén oldaláról osztjuk fel a földrajzi teret, amely az egyén észlelésén, tapasztalatain és tevékenységén nyugszik. E felosztás kettős: virtuális tér és fizikailag létező tér. Előbbi az individuális térből, kognitív térből, kibertérből és fiktív térből áll; utóbbi az individuális térből, antropológiai térből, biológiai térből és fizikai térből tevődik össze. Látható, hogy e felosztás szerint a virtuális tér jóval bővebb, mint, amit mi kibertérnek tekintünk, hiszen ebbe beletartozik az egyén képzelete és az azáltal leírt világ is.[8]

Fentiekből adódóan a virtuális tér (így a kibertér is) immanens részét képezi a földrajzi térnek, annak tág – lásd egyéni központi felosztás – és szűk értelmében is, vagyis mint infokommunikációs közeg is. Érdemes azonban ezen körben kitérni arra, hogy a hagyományos

5 Pirisi–Trócsányi (2019): 39–40.
6 Pirisi–Trócsányi (2015)
7 Pirisi–Trócsányi (2019): 41.
8 Uo., 58-61.

térszemléletet miként érintette a kibertér kialakulása és glóbuszt behálózó jellege. A virtuális geológia atyjának tekinthető Michael Batty szerint a kibertér önmagában megváltoztatja a valós (földrajzi) helyek szerepét, módosítja a hely és tér fogalmát és kapcsolatát, megváltoztatja a távolság definíciókat, leszűkíti a hely- és térfelfogás hagyományos értelmezését.[9] Emellett azonban számos tekintetben kiszélesíti azt, hiszen a kibertér nem egy homogén térből áll, abban ugyanis számtalan gyorsan növekvő kiberterület található, amelyek mindegyike másfajta interakcióra képes, miközben a technológiák gyors konvergenciája miatt új hibrid terek jönnek létre.[10] Ezek a megállapítások át is visznek minket a terület legvitatottabb kérdésére, hogy a kibertérnek köszönhetően a tér, a földrajzi tér és azon belül a távolság egyáltalán értelmezhető fogalmak-e. A főként társadalomtudományi megközelítés szerint az információs társadalomban az információ mindenhová eljut és eljuttatható, vagyis az egyenes csatornák bárhová elérnek, így a tér, az idő és a távolság már irreleváns. Manuel Castells ezt úgy fogalmazta meg, hogy „az időtlen idő mint az idő technológia által történő megsemmisítésére irányuló törekvés (…) A technológia kisszámú, esetleges pillanatra sűríti az időt, ily módon szakítva meg a társadalom folyamatosságát és fosztva meg történetiségétől a történelmet."[11] Ezzel a felfogással szemben – főként a földrajztudomány képviselői – azon az álláspontón vannak, hogy a földrajzi tér továbbra is releváns, amelynek hagyományos tér rétegei is hatással bírnak a kibertérre, nem elhallgatva, hogy „a digitális információs interakciók egy önálló és sajátos teret, egy párhuzamos kibertéri világot generálnak, mely azonban nem teljesen független a világunk fizikai-térbeli sajátosságaitól."[12]

Az igazság valójában a kettő közötti aranyközépúton található, ami Mészáros Rezső kiberteret leíró jellemzésében is tetten érhető: a kibertér

> „sok mesterségesen konstruált térből áll – ezek tervezőik, sőt gyakran használóik alkotásai, és csak akkor veszik fel a »földrajzi« (euklidészi) tér tulajdonságait, ha kifejezetten erre programozták őket. Sőt a terek gyakran tisztán olyan vizuális tárgyak, amelyeknek nincs se súlya, se tömege, sőt még az is bizonytalan, hogy mozdulatlanok-e (a terek egy szempillantás alatt megjelennek vagy eltűnnek). A kibertérnek anyagtalan és dinamikus térbeli és szerkezeti formái (felépítései) vannak, a szó fizikai (szoros) értelmében nem kézzel fogható, mert csak az agyunk segítségével vagyunk képesek megvizsgálni, de a metafora szintjén kapcsolatban áll testi tapasztalatokkal (érzékeléssel) is."[13]

Erre kapcsolódik rá Jakobi Ákos is, aki szerint a kibertér nem más, mint „az új komputerizált világ sajátos, elvont tere."[14] Azonban ezek a fizikai valóság oldaláról történő megközelítések önmagukban nem elégségesek, ahhoz, hogy pontos képet kapjunk a kibertér valós jellegéről és hagyományos térrel való kapcsolatáról, főként, hogy látható módon egyes társadalomtudományi megközelítések a kibertér és a hagyományos tér kapcsolatáról élesen eltérő képet adnak. Így szükséges további vizsgálódás tárgyává tenni a kibertér tér jellegét.

9 Batty (1997): 337–352.
10 Dodge–Kitchin (2001): 1–33.
11 Castells (2007): 433.
12 Jakobi–Lengyel (2014): 42.
13 Mészáros Rezső (2006): 494.
14 Jakobi (2002): 1484.

Ennek megfelelően érdemes a kibertérrel kapcsolatos térfelfogásokra kitérni. A fizikai térhez legközelebb álló felfogás az infrastrukturális térfelfogás, amely a számítógépes hálózatok effektív kapcsolatait, vagyis a hardveres összeköttetést jelenti. Ettől már jóval árnyaltabb képet mutat a koncepcionális térfelfogás, mely a virtuális világ széles értelmezése, vagyis lényegében a körön belüli részelemek egymás közötti kapcsolatait jelenti. Ennek megfelelően a kibertér különböző kommunikációs rendszerek önálló belső tereiből épül fel, amelyek további téregységekre bonthatóak. „A kibertér így az információk és a kommunikáció áramlásának egyfajta koncepcionális tereként jellemezhető, amely a digitális világ hardver eszközei, a számítógépek szoftverei, a telekommunikációs hálózatok és az emberi elme szerves kombinációjából jött létre."[15] Utóbbi szemléletből mindenképpen kiemelendő, hogy a tér elkülönült részének tekinti a hardvert, a szoftvert és az egyént is. Ez pedig lehetővé teszi az egyik legegyszerűbb és leginkább kézenfekvő felosztás vizsgálatát, vagyis külső és belső tér fogalompárosának górcső alá helyezését. Ennek a két fogalomnak – külső kibertér vs. belső kibertér – felvázolása, majd későbbi alábontása lehetővé teszi annak a gordiuszi csomónak az átvágását, amely az eltérő tudományterületek sajátos kiindulópontjából következőleg néhol ellentétes következtetések enged levonni a kibertér és a hagyományos tér kapcsolatáról.

A külső kibertérnek „csak olyan tereket nevezhetünk, amelyekben meghatározhatóan jelen van a lokalizáció, a földi (földrajzi) térhez kapcsolódás momentuma", ebből adódóan a „kibervilág külső terének tehát a rendszerhez köthető infrastrukturális tartozékok földi térszerkezetét nevezzük."[16] A belső kibertér ennél sokkal nehezebben megfogható, ugyanis „a kibertér virtuális összetevői fizikailag nem létező dolgok, amelyek egyik része a valós világ bizonyos dolgainak helyettesítője, reprezentációja, másik része mögött létező valós dolog nem áll."[17] A belső kibertérről akkor beszélhetünk, amikor a kibertér „önmagában mutat térjellemzőket, egyenlőtlenséget és rendezettséget."[18] Ezzel pedig a kibertér egy alternatív földrajzi struktúrát hoz létre.

A kettő elválasztásából egyértelműen következhetne – és az esetek egy részében következik is – az, hogy a lokalizálható külső térben megjelenő erőforrások, szerkezetek, hálózati elemek körében a klasszikus jogi, védelmi, biztonságpolitikai fogalmak alkalmazhatóvá válhatnak, hiszen ezek esetében egyértelműnek hathat akár az állami főhatalom kérdése, akár a tulajdonosi jogok gyakorlása. A belső tér fogalma azonban ezt is relativizálhatja, tudniillik a kibertér mint technológia formálja a teret, mert mint technológia egyedi térbeli viszonyokat hoz létre.[19] Így a belső kibertér önmaga által létrehozott térjellemzőkkel rendelkezik, amelyek semmissé tehetik azt a hagyományos térfogalmat, amelyet a külső kibertérfogalom is megtestesít, vagyis például, hogy egy-egy adathalmaz megjelenése egy lokalizálható szerveren, hálózaton nem egyértelműen jelenti akár a jogi felelősség megalapozhatóságát, akár az állami főhatalom tényleges kiterjeszthetőségét. Ez viszont azon alapszik, hogy a belső kibertér lokalizálható hely nélküli tér,[20] vagyis a külső kibertér lokalizálható szegmensei nem egyértelműen azonosíthatók a belső tér szegmenseivel.

15 Jakobi–Lengyel (2014): 43.
16 Jakobi (2002): 1487.
17 Szkála–Munka (2018): 346–347.
18 Jakobi (2002): 1487.
19 Blount (2016): 4.
20 Jakobi (2002): 1488.

Önmagában a hagyományos térfogalom-gondolkodás csapdába vezetheti akár a jogalkotást, akár biztonsági intézkedések mechanizmusának kialakítását, továbbá sok esetben külön mechanizmusokra és szabályokra van szükség a külső és belső tér esetében, azonban a valódi nehézségét az adja eme feladatnak, hogy mindvégig fenn kell tartani a két területre vonatkozó gondolkodás összhangját. Ehhez viszont az általánosnak ható – és némiképp meghaladott – külső és belső elhatárolásnál részletesebb, a napi folyamatokhoz jobban igazodó alábontás szükséges, hasonlóan a fentebb már bemutatott földrajzi tér szegmenseihez. Az egyik első ilyen modellt, az ún. OSI-modellt (Open Systems Interconnection Model) a Nemzetközi Szabványügyi Szervezet dolgozta ki az 1980-as évek közepére. A modell létrehozásának a célja az volt, hogy megalkossanak egy referenciarendszert, amely biztosítja a hálózati együttműködést, mégpedig gyártósemleges módon. A modell azt írja le, hogy egyes rétegek esetében minek kell megvalósulnia, így elkerülve a hálózati protokollok túlburjánzását. Az OSI-modell hét réteget különít el: a fizikai (physical) réteget, az adatkapcsolati (data link) réteget, a hálózati (network) réteget, a szállítási (transport) réteget, a viszonyréteget (session), a megjelenítési (presentation) réteget és az alkalmazási (application) réteget. A modell túlzott bonyolultsága okán, annak inkább csak egyes részeit használják.[21] Ennek is köszönhető egy másik modellnek a térnyerése, a TCP/IP-modellnek. A TCP/IP-modell kezdetei majd egy évtizeddel megelőzték az OSI-modellt, azonban dominánssá válása az ARPANET[22]-ből kinövő internetnek köszönhető, illetve az OSI-hoz mért átláthatóságának. TCP/IP-modell lényege is abban fogható meg, hogy az egyes rétegek meghatározott feladatokat látnak el, amely rétegek szolgálatelérési pontokon kommunikálnak. TCP/IP-modell az alábbi rétegeket különíti el: kapcsolati réteg (network interface), internet réteg (internet), szállítási réteg (transport) és alkalmazási réteg (application).[23] Eme modelleket alapul véve dolgozta ki Werbach és Kulesza rétegfelfogásaikat, amelyeket nevezhetünk a kibertér rétegelméletének. Ezen alábontás lehetővé teszi a különböző, ugyanakkor egymással összefüggő technológiák funkciók szerinti csoportosítását, és feltárja, hogy az egyes önálló technológiák, rétegek hogyan kapcsolódnak egymásba.[24] Werbach négy, míg Kulesza három réteget különít el. Werbach felosztása szerint fizikai réteg (physical layer), logikai réteg (logical layer), alkalmazás réteg (applications layer) és tartalmi réteg (content layer) adja a kibertér totalitását.[25] Kulesza az alkalmazási réteget nem választotta külön.[26] A fizikai réteg lényegében a hardver oldalt jelöli, vagyis a klasszikus felosztások szerinti külső kiberteret. A logikai réteg zökkenőmentessé teszi az információ áramlását a hálózat egyes pontjai között, ez a réteg rendkívül szoros kapcsolatban van a fizikai réteggel, lényegében az adatok fizikai réteg számára továbbítható állapotba, formátumba alakítását, konverzióját segítik elő a szoftverprotokollok révén. Az alkalmazás vagy más néven szolgáltatás réteg a végfelhasználók számára megjelenő funkciók összességét jelenti.

21 Stokes (2009): 16–17.

22 Az ARPANET (*Advanced Research Projects Agency Network)* az Egyesült Államok Védelmi Minisztériuma által finanszírozott fejlesztésű hálózat a védelmi szféra területén érintett, főként tudományos intézetek közötti számítógép-hálózat. A Védelmi Minisztériumhoz való kapcsolata okán külső szereplők korlátozottan tudtak kapcsolódni a hálózathoz. Az ARPANET 1990-ig működött. Lásd: Gavin Wright: ARPANET. *TechTarget/ Networking*. www.techtarget.com/searchnetworking/definition/ARPANET

23 Stokes (2009): 17.

24 Blount (2016): 37.

25 Werbach (2006): 59.

26 Kulesza (2012): 125.

A tartalmi réteg pedig az adatok, információk összessége.[27] Eme felosztás már könnyebben megfogható szinteket különít el a kibertér mint tér fogalmi vizsgálódásban. Utóbbi felosztás lehetővé teszi például jogi szabályozási területek leválasztását is, hiszen a fizikai és logikai réteg esetében a rendszerbiztonságra vonatkozó szabályok vonatkoznak, míg utóbbi két réteg esetén a tartalommal kapcsolatos elvárások határozhatóak meg, emellett pedig világossá teszi, hogy a külső és belső aspektusok bár azonosítható elkülönült szintjei vannak, azonban nem szétválaszthatóak, hiszen annak integritása csak egészében szavatolható, amennyiben bármelyik réteg sérül, az egész rendszer biztonsága sérül.

Az eddigieket összegezve tehát elmondhatjuk, hogy a kibertér a földrajzi tér egy sajátos szegmense, amely jelentős hatást gyakorol a hagyományos tér, távolság és idő értelmezésünkre és felfogásunkra, azonban azokat egészében nem tudja felülírni, és ebből adódóan, mivel a földrajzi tér totalitásának a része, az abban megjelenő jellegadó tendenciák, folyamatok a kibertérben is megjelennek, arra is hatással vannak. Látszik viszont az is, hogy a valódi jellegadó folyamatok – bár a legtöbb esetben külső téri eredményeik is vannak – a belső térben zajlanak, mindazonáltal osztva mind Jakobi, mind a Pirisi–Trócsányi szerzőpáros véleményét, a hagyományos fizikai tér hatásai alól a kibertér sem mentesülhet.

A Moore-törvényét meghaladó fejlődés, a glóbusz egészére kiépült kibertér sajátos térjellemzői miatt az az elmúlt évtizedekben radikálisan megváltoztatta a társadalmi, kulturális, politikai, intézményi és gazdasági életet.[28] Ennek a radikális átalakulásnak a kezdőpontja és motorja az ún. új gazdaság megjelenése volt az 1970-es években, amely szakított a fordista termelési rendszerrel – megteremtve a posztfordista rendszert –, ami fejlett ipari országoknál azt eredményezte, hogy a gyáripari tömegtermelés elkezdett visszaszorulni. Ennek az új gazdasági szemléletnek a fogalmi alapját jelentik az információ gazdaság, a kreatív gazdaság, a kulturális gazdaság. Az információgazdaság az új gazdaság digitális oldalát jelenti, így a gazdasági játszótér két részre bomlott: hagyományos offline és online gazdaságra. Előbbi azonban az utóbbi nélkül már nem tud versenyképes lenni, ugyanis a kulturális gazdaság átalakulásnak köszönhetően a fogyasztói szokások is jelentősen átalakultak, ami már odáig jutott, hogy a teljes gazdaság jelentős hányadát a szolgáltatásközpontúság jellemzi, amely pedig elválaszthatatlan a kibertértől és a hozzá kapcsolódó eszközöktől.[29] E folyamatok során

> „(…) valóban forradalmi változások kezdődtek el, amikor a gazdasági, pénzügyi, társadalmi és politikai folyamatokat egyaránt a kibertérre alapozzák (…) Kialakul a közösségi (másnéven megosztott) gazdaság (shared economy), amely rátelepül a határokon átnyúló infokommunikációs hálózatokra. A közösségi gazdaság az olyan eddig állandónak bizonyult alrendszereket is érintheti, mint a nemzeti pénzkibocsátás, vagy a nemzetközi pénzügyi közvetítő rendszer."[30]

Tehát a kibertér kiépülésének és az azt megalapozó gazdasági átalakulásnak köszönhetően beteljesedett a globalizáció a pénzügyi, gazdasági és a kulturális viszonyokban.

27 Werbach (2006): 60–64.
28 Dodge–Kitchin (2001): 13.
29 Baji (2014): 119–120.
30 Pintér István (2016): 330.

E közegben, ahol a fogyasztói igények alakítása alapvető gazdasági igényként fogalmazódik meg, nem véletlen, hogy az egyén társadalmi helyzete, szerepe és gondolkodása jelentősen átalakul, ami erőteljesen köthető a kibertérhez is. Ennek kitűnő példája a WEB 2.0 megjelenése, amely meglehetősen bizakodó hangulatot eredményezett: az elvárást, hogy kialakulásával létrejött a korlátok nélküli kommunikáció terepe. Azonban – ahogy arra Gosztonyi Gergely kiválóan rámutat – csakhamar kiderült, hogy valójában a magáncenzúra (vagy óvatosabban magánkuratálás) korszakába léptünk,[31] ahol a szűrőbuborék-rendszer[32] révén a kibertér egyes szereplői „képesek befolyással lenni az éntudatra és a közösségre".[33] E keretből pedig nincs menekvés, ugyanis – ahogy Manuel Castells spanyol szociológus írja – a hálózathoz tartozás a létezés fokmérőjévé vált,[34] ahol a „hálózati társadalom testetlenné teszi a hálózati viszonyokat."[35] Mary Aiken, a neves ír kiberpszichológus, egyenes odáig megy, hogy azt állítja: az egyén számára „a technológia olyan természetessé vált, mint a belélegzett levegő. Olyan szükség a 21. században való túléléshez, mint a testünket felüdítő víz. A környezetünk részévé vált."[36] Mindezt ismerve Castells mégis megfogalmazta a hálózatba ágyazott individualizmus eszméjét, amely szerint a virtuális közösség énközpontú vagy személyre szabott közösség.[37] Sherry Turkle Alone Together című könyvében kifejti, hogy a túlterhelt életvitelnek köszönhetően az emberek olyan kapcsolatokat alakítanak ki, illetve tartanak fenn, amelyek alacsony kockázatúak: Facebook-barátok, avatarok, IRC chatpartnerek, vagyis olyan hálózatokhoz akarunk tartozni, ami kényelmes számunkra – azonos világnézet, tényleges intimitás és a konfliktus hiánya –, és ahol a kontroll látszata fennáll.[38] Tehát egy meglehetősen furcsa kettősséggel találkozunk: az ember számára a hálózathoz tartozás létszükséggé vált, és emellett mégis az énközpontúság jellemzi – ez pedig nyilvánvaló feszültséget okoz, egyénen és társadalmon belül is. Eme feszültség abban jelenik meg szélesebb spektrumú problémaként – ahogy Arturo Escobar erre felhívta a figyelmet, –, hogy nemcsak a kibertér gyakorol hatást a hagyományos térre, hanem az is viszonthatást gyakorol rá. A technológia ugyanis alapvetően társadalmi konstrukció, amely révén a hagyományos tér folyamatai nem szeparálhatók a kibertér folyamataitól; azok szorosan összefonódnak egymással.[39] Megerősíti ezt, ha visszautalunk a kibertér földrajzi térben betöltött szerepére, ugyanis az, egészében társadalmi eredetű, így nem lehet független az offline világtól és annak térbeli totalitásától sem.[40]

Így a hagyományos tér társadalmi feszültségei – legyenek azok politikai, vallási, ideológiai, kriminológiai jellegűek – ebben a globális belső kibertérben szintén megjelennek. Castells is felhívja erre figyelmet, mikor rögzíti, hogy a hálózati társadalmakból – ahogy a korábbi korok társadalmaiból sem – nem hiányoznak a társadalmi konfliktusok.[41] Eme feszültségek ezekben a személyre szabott globális közösségekben azonban – ahol az egyén sérelme, érdeke, világlátása hatványozott számban és mértékben tudja formálni a hálózat többi tagjának

31 Gosztonyi (2022a): 84-86.
32 Koltay (2019): 4-7.
33 Mészáros (2006): 494–495.
34 Pintér Róbert (2007): 25.
35 Castells (2007): 433.
36 Aiken (2020): 103.
37 Bell (2007): 67.
38 Turkle (2011): 295.
39 Escobar (1994): 211–231.
40 Jakobi–Lengyel (2014): 43.
41 Castells (2007): 434.

értékrendjét, éntudatát – fokozott intenzitással jelennek meg. Amerikai szociológusok is felhívták a figyelmet arra, hogy a kibertér alapvetően alkalmas volna arra, hogy a társadalmi töréspontokat csökkentsék a civil szerveződések és az állam szociális szerveinek hatékonyságfokozása által, azonban a kibertér arra is tökéletesen alkalmas, hogy ezek megfelelő működése nélkül a hagyományos konfliktusok tovább éleződjenek.[42] A növekvő társadalmi feszültséget a társadalmi mozgalmak is kifejezésre juttatják, és a saját eszközeit, a globalizálódó technológiát és kultúrát fordítják szembe a hálózati világgal. Ebből kifolyólag a kibertér által nyújtott lehetőségeket kihasználva egyes terrorszervezetek, bűnszervezetek erősítik transznacionális jellegüket, és újfajta, hibrid biztonsági problémaként, kihívásként jelentkeznek.[43] Nem véletlenül használják fel ezek a szervezetek hagyományos tevékenységük fokozására a kiberteret, mivel „szinte végtelen számú búvóhely van itt",[44] tehát a közeg tökéletesen alkalmas arra, hogy a problémás magatartások széles skálájának otthont adjon.[45]

A biztonsági problémát fokozza, hogy a globális kibertérhez kapcsolódnak az egyes gazdasági, pénzügyi szereplők, valamint a nemzetállami és szupranacionális közösségek intézményei. Így a társadalmi feszültségből eredő és az államközi konfliktusok közvetlen célpontjává válhatnak a kibertérhez kapcsolódó előbb felsorolt szereplők is.

> „Az információs társadalom fizikai életterét (hardverét) az állami és a nem állami szervek, valamint a velük közvetlen – ma leginkább elektronikus – kapcsolatban álló állampolgárok hálózata alkotja… az új társadalom »idegrendszere« az informatikai, hírközlési infrastruktúra, az immunrendszere pedig az informatikai biztonság és adatvédelem. A társadalom folyamatainak irányítását és vezetését (szoftverét) pedig azon stratégiák jelenthetik, amelyek képesek a közösség érdekei szerint megvédeni az értékeket, továbbá garantálják az élettér fenntartását és a társadalom különböző szegmenseinek biztonságos működését."[46]

Kifejezetten növeli a sérülékenységét az államokban, hogy a kibertérben elveszítették a kontrollt az információ felett – melyeket sok esetben viszont transznacionális vállalatok birtokolnak –, pedig az információ ellenőrzése már az információ kora előtt is az államhatalom alapja volt.[47] Nem véletlen, hogy a kibertér, bár direktben nem, de közvetett módon a politikai hatalom gyakorlását is érinti:[48] ahol bírják a hatalom birtokosai az információt, ott ezt erősíti, ahol viszont nem rendelkeznek a szükséges információval, ott gyengíti a hatalom gyakorlását. Mindez pedig az állam geopolitikai helyzetét befolyásolja, működését hátráltatja, végső soron pedig a biztonságát is veszélyezteti.[49] Nem véletlen, hogy Észtország 2017-ben, a világon elsőként megállapodott külföldi adatnagykövetség létrehozásáról, amely részeként a legfontosabb észt adatokat tartalmazó biztonsági mentést luxemburgi adatnagykövetségen tárolja, ezzel megnehezítve azt, hogy egyes kibertámadások megbénítsák az országot. Hasonló törekvés

42 Bainbridge (2020): 1.
43 L. bővebben Magyar–Simon (2017): 57–68., Simon–Magyar (2017a): 89–101., Simon (2015): 145–162., Tóth Zoltán (2016): 26–42.
44 Aiken (2020): 295.
45 Jegede–Ovia–Idam (2016): 5.
46 Simon (2016a): 72.
47 Castells (2006): 379.
48 Blount (2016): 5.
49 Cattaruzza (2019)

figyelhető meg a közel-keleti arab államok körében is, igaz, ők inkább a befektetéseik biztonsága érdekében kívánnak kialakítani hasonló rendszereket.[50]

E körülményeket figyelembe véve a kibertér – és ezáltal a hagyományos tér – védelme és biztonsága érdekében szükséges, hogy az egyes államok fegyveres védelmi rendszerei,[51] illetve ezen belül azok katonai karakterű szervei[52] – és az e területtel foglalkozó kutatók – feltérképezzék és a hadtudományokhoz igazított értelmezését adják a kibertérnek, ezzel is elősegítve azt, hogy e szervek definiálni tudják a helyüket, szerepüket a kibertéri folyamatokban.

A kibertér eme szűkített értelmezésének szükségességét megerősíti az is, hogy az

> „információval bárki képes lehet életeket kioltani (…), ugyanis: Az internetes és kommunikációs hálózatokra kapcsolt eszközök akár fegyverhez hasonló felhasználást is eredményezhetnek (…) a pusztítás eszköze, mértéke, illetve társadalmi hatása is inkább a háborúk, vagy az ipari és természeti katasztrófák jogilag csak speciálisan megítélhető következményeihez hasonlíthatók."[53]

Ezt felismerve a NATO 2016-ban a kiberteret is hadszíntérré minősítette.

A definícióalkotás valódi nehézségét e területen az adja – ahogy azt S. Michael Pavelec megfogalmazta –, hogy a hagyományos katonai rendszerekhez képest a kibertér veszélye és előnye, hogy az kiterjed az egész társadalomra, kormányzatra/közigazgatásra, katonaságra, civil szférára és azok mindennapi életére, ennek okán elengedhetetlen, hogy a kibertérre sajátos katonai doktrínákat, stratégiákat dolgozzanak ki, hiszen ezek szükségesek annak megértéséhez, és végső soron a hálózatnak és az ahhoz kapcsolódó személyeknek, szervezeteknek a megvédéséhez.[54] Eme összetettséget hangsúlyozza ki Zachary M. Smith is, amikor a kiberbiztonságról, kibervédelemről ír, ugyanis rögzíti, hogy a kibervédelem nem önállóan állami tevékenység eredménye, hanem a kibertér jellege okán ahhoz elengedhetetlenül szükséges a civil (azaz a magán és gazdasági) szféra is.[55]

Steve Winterfeld és Jason Andress munkájukban úgy fogalmaztak, hogy a kibertérben a csatatér magába foglalja a hálózatokat, a számítógépeket, a hardvereket (ez magában foglalja a beágyazott számítógépes chipeket tartalmazó fegyverrendszereket), a szoftvereket (kereskedelmi és kormányzati fejlesztések), az alkalmazásokat (például parancs- és vezérlőrendszerek), a protokollokat, a mobileszközöket és az embereket, akik működtetik az egyes eszközöket.[56]

Az Egyesült Államok Védelmi Minisztériuma által létrehozott meghatározás szerint a kibertér az

> „informatikai (információs) környezetben értelmezett globális tartomány (domain), amely magába foglalja az IT infrastruktúrák egymással összefüggő elemeinek hálózatát, beleért-

50 Prakash (2018a): 145.

51 A fegyveres védelem rendszeréről és annak kortárs kihívásairól l. Farkas Ádám (2016), Farkas Ádám (2017a) 44–58., Farkas Ádám (2017b): 5–20.

52 Katonai karakterű szervek fogalmáról lásd bővebben: Farkas Ádám (2012): 3–6.

53 Simon (2016b): 34., 41–42.

54 Pavelec (2015): 120–124.

55 Smith, Z. M. (2017): 62–66.

56 Winterfeld–Andress (2013): 22.

> ve az internetet, a telekommunikációs hálózatokat, számítógépes rendszereket, valamint a beágyazott feldolgozó és vezérlő elemeket."[57]

Szintén ad egy fogalmat a Magyar Honvédség Kibervédelmi szakmai koncepciója is: „a kibertér elektromágneses spektrum használatával meghatározható, dinamikusan változó tartomány, mely az összekapcsolt hálózatok, eszközök és kiegészítő fizikai infrastruktúrák közötti adatok kezelésére szolgál."[58] Mindkét meghatározás hiányossága az, amit e fejezet bevezetőjében is írtam, hogy a kiberteret annak technikai sajátosságai felől definiálja és kihagyja annak a biztonságszavatolás oldaláról jelentős, más tudományterületek is érintő jellemzőit, így például az egyén szerepét a rendszerek integritásában, vagy a térjellemzőiből és azok rétegeiből következő összetett sérülékenység problematikáját.

A katonai karakterű szervek tevékenységéhez igazodó kibertér értelmezés tehát nem nélkülözheti annak civil sajátosságait, azonban ahogy arra Haig Zsolték felhívják a figyelmet, szükséges azt a civil sztereotípiáktól varázstalanítani. Ugyanis többek között

> „a kibertér meghatározásával kapcsolatban – civil értelmezés szerint – általánosan elterjedt nézet, hogy az a számítógép-hálózatokkal és az internettel van összefüggésben. A kibertér katonai értelmezése azonban kiterjeszti ezt a dimenziót, és nemcsak a számítógép-hálózatok működési környezetét érti alatta."[59]

Kassai Károly pedig emellett rögzíti a kibertér katonailag kiemelt sajátosságát, hogy „fizikai jellemzőkkel nehezen meghatározható, a képességek alakulása szerint dinamikusan változó tartalommal bír, beleértve az adatok és hozzáférési lehetőségek sokféleségét",[60] amelyek okán elengedhetetlenül szükséges a nemzetközi trendek és folyamatok ismerete, a sebezhetőségek azonosítása és a felhasználói tudatosság magas szinten tartása, amely magában hordozza a szövetségi és nemzeti szereplők közötti információ áramlást.

A NATO fogalmi attitűdje azonban maradt technológiai központú. Alapvetően a kiberteret egy összetett dinamikus környezetnek tekintik, amely a működési környezet egyik komponense.[61] A 2020-ban közétett kiberműveleti doktrínában található fogalom már a fentieknek – Haig, Kassai – megfelelően tartalmaz új fogalmi elemeket is. Ugyanis a doktrína szerint a kibertér „az összes összekapcsolt kommunikációs, informatikai és egyéb elektronikus rendszerből, hálózatból és azok adataiból álló globális terület, beleértve az elkülönült vagy független rendszereket is, amelyek adatokat dolgoznak fel, tárolnak vagy továbbítanak".[62] Vagyis kiemelt részét képezi a fogalomnak az adatvagyon is. Emellett viszont a fogalmi elhatárolásban továbbra sem jelenik meg a kibertér társadalmi jellege, amely viszont a nemzeti

57 Joint Publication 1–02 Department of Defense Dictionary of Military and Associated Terms, 57. fas.org/irp/doddir/dod/jp1_02.pdf

58 A honvédelmi miniszter 60/2013. (IX. 30.) HM utasítása a Magyar Honvédség Kibervédelmi Szakmai Koncepciójának kiadásáról, 1. melléklet, 2. pont 8.

59 Haig et al. (2014): 23.

60 Kassai (2012): 129.

61 Munk (2018): 115.

62 Allied Joint Publication-3.20 Allied – Joint Doctrine for Cyberspace Operations. NATO standard, January 2020. 4. assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf

biztonság szempontjából legalább annyira releváns, mint a technológiai oldal. Ugyanis például a jogi eljárások és szabályozás kialakítása terén – Escobar és Castells gondolatait továbbfűzve – a technológia és társadalom egymás esszenciális jellegét jelenthetik, hiszen mára a technológiának társadalmi, a társadalomnak pedig a technikai realitása megkérdőjelezhetetlen; a hatás viszonthatás pedig mindkettő esetében strukturális változásokat eredményezhet. Így a jog mint társadalmi jelenség, a társadalmi totalitás egyik részobjektuma is ezen változó környezet része, amelyre ugyanúgy hatással van a technológia. A társadalom oldaláról biztonságos keretek kialakítását teszi lehetővé a megfelelő mélységű és színvonalú jogi szabályozás, a technológia fejlesztések, valamint azok alkalmazása és továbbfejlesztése terén. Nem elhanyagolható szempont, hogy így az ezen nyugvó jogi környezet az állam biztonsági, védelmi, valamint államközi tevékenységének technológiai oldalát nézve is megfelelő, garanciális és nem utolsósorban jogállami foglalatát adhatja. Ehhez viszont szükségképpen fel kell ismerni, hogy a kibertérnek és a kibertér biztonságának nemcsak technológiai fogalmi jegyei vannak, hanem társadalmiak is.

A fenti fogalmak és jellemzők összegzéseként mindenképpen levonható az a következtetés, hogy a kibertér a földrajzi tér egy olyan sajátos, folytonosan változó része, amely a hagyományos térelemekkel kölcsönhatásban van, de azoktól mégis elkülönült, egyedi térjellemzőkkel bíró térréteg. E virtuális téren keresztül milliós nagyságú információs áradat halad át egyetlen perc leforgása alatt. „Egyértelműen prognosztizálható: a kibertér rendszerei egyre nagyobbá, gyorsabbá és komplexebbé vállnak”[63] az elkövetkező években. Ezáltal még inkább mindenki számára könnyen hozzáférhetővé válik ez a folyamatosan bővülő entitás, amely valós hatást gyakorol az egyén, valamint a társadalom önképére, a társadalmi reflexiókra, a globális gazdaságra, és amelyben aktív szereplőként jelennek meg az államok igazgatási és katonai karakterű szervei.

A kibertér tehát ebben a felfogásban nemcsak a földrajzi tér része, hanem a társadalmi totalitás[64] olyan részegysége, amely közvetlenül befolyásolja a társadalmi totalitás többi részegységét, így többek között az egyéneket, a társadalmi hálózatokat és a társadalmi struktúrát, az állami intézményrendszert és feladatellátást, a biztonsági rendszereket és a jogi szabályozást is. E hatás megkerülhetetlen velejárója, hogy a társadalmi totalitás érintett részkomplexumainak választ kell adniuk arra a kihívásra, amelyet a kibertér és a hozzá kapcsolódó technológiák jelentenek.

2. A kortárs biztonsági kihívások és a kibertér kapcsolata

A 20. században a társadalom, a politika, az állam és ezek szervesült részeként a védelem és a biztonság is komoly változások, bizonyos tekintetben korszakváltás korát élte. Ezek jelentős része azonban az úgynevezett hosszú 19. század technológiai, gazdasági és társadalmi változáshullámain, „forradalmain”[65] alapult, amelyek a korábbiakhoz képest jelentős mértékben átalakították a termelés és a közlekedés lehetőségei mellett a kommunikáció, ez által pedig a kapcsolattartás, az információáramlás és nem utolsósorban a tudatformálás vagy befolyásolás közegeit is.

63 Babos (2011): 42.
64 Peschka (1988)
65 L. Hobsbawm (1988), Braudel (2008), Kelemen (2017a) 91–100.

Ezek a változások a közlekedés fejlődésével járó életviteli felgyorsulás, a távolságok fokozatos relativizálódása és vele a világ távoli pontjainak fokozottabb összekapcsolódása mellett elvezetett a politika tömegesedéséhez,[66] ezáltal mind a gondolkodás, mind pedig a hatalomgyakorlás színeváltozásához is. Az információs és politikai értelemben is azonosítható tömegesedés nem csak a demokratikus mozgalmaknak kedvezett, hanem egyidejűleg lehetőséget teremtett arra is, hogy az államok és politikai szereplők versengésüket új szintre emeljék, és a széles értelemben vett társadalom jelentősebb mértékű elérhetőségével új színtérre is tereljék.[67] Mindez a jogállamiság transzatlanti térségben zajló kibontakozásával, megerősödésével együtt azt jelentette, hogy miközben a technikafejlődés az előnyök mellett egyértelműen növelni tudta a civilizációs kockázatok súlyát és a hadviselés jelentőségét is, aközben a társadalmak szabályozott működése megkövetelte a változásokhoz való szabályozási, intézményi alkalmazkodást.

E kérdés kapcsán ma már alapvetésként merül fel az a megközelítés, hogy a 20. század – különösen annak második fele – a biztonság terén a katonai dominanciájú biztonságfelfogástól a komplex – de szektorálisan tagolt – biztonságszemlélet felé mozdult el.[68] Ez a ténymegállapítás azonban sokkal többet sejtet, mint a háborús fenyegetés jelentőségének, lehetőségének változását. Egyik oldalról ugyanis a két világháború, a számtalan helyi konfliktus, illetve a hidegháború egyértelművé tette, hogy a biztonság katonai dimenziója nem vesztett a jelentőségéből, hanem a többi lehetséges veszélyforráshoz mérten került átsúlyozásra. Ezt az értelmezést ugyan a huszadik század végén időlegesen elfeledtük a transzatlanti térségben, de napjaink ukrajnai háborús eseményei és annak előzményei, illetve a világszerte tapasztalható helyi konfliktusok fennmaradása a történelmi pillanatra kiterjedő európai emlékezetkiesésünket a fegyveres szembenállás rideg valóságával írta felül. Másik oldalról azonban a biztonság komplex irányba történő elmozdulása azt tükrözi, hogy a technológiai és társadalmi változások, illetve ezek sokrétű hatásai felértékelték azoknak a veszélyforrásoknak a jelentőségét – károkozó/pusztító erejét –, amelyek korábban a háború jelentette fenyegetéshez képest kevésbé bizonyultak jelentősnek. A biztonság szektorokra vagy dimenziókra osztása tehát egyértelműen tükrözte a technikai és társadalmi fejlődés súlyát, növelve a biztonság fogalom horizontális és vertikális kiterjedését is. A biztonság tartalma tekintetében beállt változás tehát egy olyan korszakforduló volt már a múlt században is, amely a fejlődés lehetséges előnyei és hozadékai mellett annak árnyoldalaira is rámutatott.

A biztonsági környezet ilyetén változása, átalakulása a konkrét védelmi képességek mellett szükségképpen érintette az állam- és jogrendszert is, hiszen a legitim állami erőszakmonopólium a biztonság megóvásának ultima ratio eszköze, de messze nem kizárólagos módozata. Évezredek tanulságai köszöntek hát vissza akkor, amikor a 19–20. század fejlődésének dinamikus hatásai miatt a biztonság terén még inkább felértékelődött a védelmi és biztonsági intézmények viszonyrendszere a többi állami intézménnyel és a társadalommal. Szun Ce, Taj Kung, Huang-si Kung antik Kínából származó politikai és hadtudományi iránymutatásai, Kautilja Artha-sásztrája vagy épp Machiavelli, Zrínyi Miklós, Rumjancev tábornok, illetve Carl von Clausewitz e körben lefektetett gondolatai[69] az állami és társadal-

66 A téma kapcsán l. Ortega y Gasset (2019), le Bon (2018), Szretykó (2005)

67 Példaként l. Aral (2020), Singer–Brooking (2018), Cattaruzza (2020), Farkas Ádám (2021a)

68 Szálkai–Stepper (2015), Buzan–Waever–De Wilde (2006): 53–112., Dannreuther (2016)

69 Szun Ce (2006), Taj Kung (2016), Chanakya Pandit (2015), Machiavelli (2006), Hausner (2017): 61–85., Tömösváry (2017): 87–106., Clausewitz (2014)

mi stabilitás és a védelem viszonya kapcsán[70] tehát a huszadik században új szintre lépett az átfogó nemzetbiztonság koncepciójával, illetőleg a hírszerzési képességek súlyának növekedésével.[71]

A 19–20. századi társadalmi-politikai korszakváltást az állam vonatkozásában Carl Schmitt a totális állam toposzával írta le. Megközelítése szerint:

> „az állam és társadalom kölcsönösen áthatják egymást, s minden eddig államinak számító ügy társadalmivá, és megfordítva, minden eddig »csak« társadalminak számító ügy államivá válik, miként az egy demokratikusan szervezett közösségi szervezetben szükségszerű módon bekövetkezik."[72]

Látni kell azonban azt is, hogy ezen állam totalitása abban rejlik, hogy

> „az eddig »semleges« területek – vallás, kultúra, képzés, gazdaság – megszűnnek »semlegesnek« lenni a nem-állami és nem politikai értelemben (…) A totális államban ennek következtében minden – legalábbis lehetőség szerint – politikai, és az államra való hivatkozás már nem képes arra, hogy a »politikai« speciális megkülönböztető ismertetőjegyét megindokolja."[73]

E tekintetben nem lehet elégszer hangsúlyozni, hogy önmagában a totális állam nem azonosítható a totalitárius diktatúrákkal. Célszerűbb onnan megfogni a kérdést, hogy a totális állam a véleménynyilvánítás szabadsága kibontakozásának[74] és a politika tömegesedésének talaján kibontakozott új állami attitűd, amelyben – minthogy az állam a társadalom intézményesült kerete – a társadalomban releváns témák politikaivá alakulásával, vagy ha úgy tetszik, a politika témakörökre vonatkozó terjeszkedésével elmosódtak azok a korábbi cezúrák, amelyek egyes területeket a politikán kívülivé, és ezáltal az állam vonatkozásában részben-egészben irrelevánssá tettek. A totalitárius diktatúra ennek a fejlődési stádiumnak már az az elfajzása, amely nem egyszerűen kinyitja a politikai és az állami kapuját számos korábban oda nem számító szféra felé, hanem egyenesen dominálni, uralni, szükség esetén elnyomni akarja azokat az emberi hatalomvágyból táplálkozva, az erőszak eszközeit szisztematikusan használva, de legalább a kezdeti szakaszban egy jelentős tömegbázis támogatására, majd csendes beletörődésére építve.

Fontos e tekintetben megjegyezni, hogy a politikai szféra, és vele az állami mozgástér ilyesfajta kiszélesedése vagy totalizálódása szükségképpen igényelte azokat a technikai és társadalmi változásokat, amelyek az információ terjedését felgyorsították, illetve a kultúra és a politika tömegekhez való hatékonyabb eljutását lehetővé tették. A megalapozott értékeléshez feltehetőleg közelebb áll, ha az egész kérdést úgy fogjuk meg, hogy a technikai, gazdasági, társadalmi fejlődés egyik oldalról kényszerítette az államot a változásra, míg a politika szférájában lehetőséget teremtett az új fajta hatalomgyakorlásra mind a demokrácia, mind a

70 Vö. Farkas Ádám (2022a)

71 Vö. Andrew (2021), Murphy–Kondrasov–Bailey (1998), Scott (2018), Huntington (1994), Farkas Ádám (2020a): 5–20.

72 Schmitt (2002) 16.

73 Uo.

74 Vö. Ash (2022), Koltay (2009)

tömegmozgalmak tekintetében. A nyomdaipar fejlődése, a tömeges szabadidős foglalkozások terjedése, a városiasodás erősödése, a közlekedés gyorsulása és szervezettebbé válása, majd a rádiózás és a filmipar megjelenése mind-mind ebbe az irányba hatottak.[75]

Ezek a változások a társadalom, illetve az egyes emberek információ-ellátottsága terén hoztak olyan áttörést, amely aztán a működési keretek egészére hatott vissza mind gazdasági, mind társadalmi, mind politikai értelemben. Schmitt totális állam toposza tehát ennek a hatalmi-politikai dimenzióját ragadta meg a politikai államfogalom révén. Ennek értelmezésében a huszadik század borzalmai és Schmitt személyes szerepe a totalitárius hatalomgyakorlásban az elmúlt évtizedekig elsőbbséget, sőt dominanciát élvezett munkássága mélységi tartalmához és szerteágazó vonatkozásaihoz képest.[76] A tömegesedés és a politika más szférákba való beszivárgása az információterjedés és a társadalmi információfeldolgozás szempontjából kisebb figyelmet nyert idáig, miközben látható, hogy a 21. század elejének tapasztalatai alapján ez az olvasat meglehet, hogy sokkal lényegesebb, mint a korábbiak. Az információfókuszú olvasat ugyanis lehetővé tesz egy olyan értelmezést, miszerint a 20. század a maga totális – és totalitárius – fordulataival inkább a kezdete volt egy történelmi korszakváltásnak, míg jelen korunk globális információs fejlődése a folyamat kiteljesedését hozza magával. Ez a megközelítés egyrészről felerősítheti a kortárs változások jelentőségét, másrészről pedig fokozott figyelmet irányíthat a huszadik századi jelenségek összefüggéseire és távlati hatásaira, a különféle kihívásokra adott reakciókra és megoldásokra, valamint ezek részletezőbb elemzésének és összefüggésbe helyezésének szükségességére.

Így közelítve azonban a totális állam és a mögötte húzódó társadalmi-gazdasági-politikai változások kérdéskörének elemzését a védelem szempontjából célszerű lehet kiegészíteni Schmitt egy másik gondolatával: a partizán elméletével. Ebben a partizánság kapcsán felidézte, hogy annak egyik legismertebb megnyilvánulása a modern történelemben a spanyol ellenállás volt Napóleon hadaival szemben. A téma fontosságát azonban e történelmi tapasztalat mellett az adta, hogy Schmitt a kérdést a 20. század első felének tapasztalatai, az irreguláris, sőt sok tekintetben a nem állami irányítású – de korábbi vagy aktuális államközi konfliktusokhoz kötődő – fegyveres harcosok módszereinek terjedése alapján emelte vizsgálata középpontjába. Ezt később a történelem és a nem állami szereplők konfliktusokban betöltött szerepére vonatkozó kutatások is alátámasztották.[77] Schmitt a jelenség terjedésében jelentős kihívást látott a hagyományos harcmegvívási módozatokhoz képest, részint kapcsolódva azokhoz a környezeti és technikai változásokhoz, amelyek a totális állam szempontjából is értékelést nyertek már. Mind a technikafejlődés, mind pedig az információáramlás változásai felerősítő tényezőként hatottak ugyanis az irreguláris harcmodor hatékonyságára. A támadások hírének könnyebb és gyorsabb terjeszthetősége, vagy épp az újfajta infrastruktúrák elleni támadások szimbolikus jelentősége ugyanis egyértelműen demoralizálni képes az ellenérdekelt fél erőit és társadalmát, miközben erősítheti a saját közössége kitartását. Ennek jelentőségét pedig – hasonlóan a totális állam toposzához – az információs korszak beköszönte ma szintén új megvilágításba helyezi a partizán/gerilla médiától a kiberpartizánig terjedően, miközben ezek természetére nézve több, a huszadik századi keretekre épített megállapítás is

75 Vö. Kósa (1998)

76 L. Cs. Kiss (2004), Cs. Kiss (2022), Techet (2013), Karácsony (2016)

77 A téma kapcsán l. Kajtár (2015), Spitzer (2019a), Simon (2022), Kelemen (2021a)

értelmezhető, igaz, egyes esetekben a harcmegvívástól különválasztva, inkább szemléletmódként, taktikai/stratégiai keretként értelmezve.

Carl Schmitt helyesen állapította meg, hogy

> „A modern partizán sem jogot, sem kegyelmet nem vár el az ellenségtől. Elfordult a megszelídített védelmi intézményekkel körülbástyázott háború konvencionális ellenségességétől és egy másik terület, a valóságos ellenség területe felé vette az irányt, amely a terrorral és ellenterrorral egészen a megsemmisítésig fokozódik."[78]

Ez tehát nem más, mint ellenhatás az aszimmetriára épülő birodalmi hadviseléssel és a polgári lakosságra kiterjesztett stratégiai lépésekkel szemben. A partizánság jelenségével és különösen annak elterjedésével pedig két dologra kell felhívni a figyelmet. Egyrészt arra, hogy a partizán jogon kívüliségéből és a Schmitt által jól érthetően levezetett megsemmisítésig fokozódó, kölcsönhatásos, hatás-ellenhatás spiráljában mozgó, valóságos ellenségességéből a totális ellenállás következett, amely nem ismer határokat és konvenciókat, csak a hatékonyságot és a kívánt eredmény elérését. Ez pedig ma a terrorizmus, a radikalizmus fegyveres szegmensei, vagy épp a nem konvencionális fenyegetések[79] kapcsán is fontos tapasztalat. Nem zárható ki azonban az sem, hogy ez a jelleg az információs térben éleződő feszültségek és különféle mozgalmak, illetve a politika információs térben való kibontakozása kapcsán is hasonló jelentőségre tegyen szert a 21. században. Másrészről arra is figyelemmel kell lenni, hogy a korábbi történelmi példákban az államok nem tudtak kellő hatékonysággal fellépni a partizánok ellen, mivel ez egy átfogó, a megszállt területek társadalma tekintetében rendkívül komplex, a katonai, a rendészeti, a titkosszolgálati, valamint a közigazgatási fellépés összehangolt és jól szervezett megvalósítását igényli, amihez nem készíthető általános receptúra, hiszen az adott helyzethez és az adott társadalmi miliőhöz kell, hogy illeszkedjenek a megoldások.

Ami pedig Schmitt múlt századi értékelését a partizánokról igazán figyelmeztető erővel ruházza fel a 21. században, az nem más, mint az általa felvázolt jellemzők ma terroristákban, kicsi zöld emberekben és különféle radikális csoportokban történő „reinkarnációján" túl a következő gondolat:

> „1914-ben Európa népei és kormányai valóságos ellenség nélkül szédültek bele az első világháborúba. A valóságos ellenségesség csak magából a háborúból keletkezett, amely az európai nemzetközi jog konvencionális államok közötti háborújaként kezdődött és a forradalmi osztályellenesség világméretű polgárháborújával végződött. Ki fogja megakadályozni, hogy ezzel analóg, de végtelenül felfokozott módon váratlanul létre ne jöjjenek az ellenség új fajtái, melyek végbemenetele egy új partizánság nem várt megjelenési formáit hívják majd életre?"[80]

A nemzetközi terrorizmus, a radikalizáció, a különféle mozgalmak, és adott esetben az információs térben zajló széles körű, állami vagy nem állami szereplők által meghatározott beavatkozási/befolyásolási törekvések sora ugyanis a konvencionális kereteket megkérdőjelező,

78 Schmitt (2002) 16.
79 Vö. Simon (2017) 233–242., Farkas Ádám (2018a)
80 Schmitt (2002): 162.

sőt felrúgó partizánjelleg megtartása mellett függetlenítette magát az állami szembenállások korlátozott terepétől, és egy végeláthatatlan témahorizontot nyithat meg a 21. században, amivel komoly kihívás elé állítja a gazdaság, a társadalom és az állam rendszereit is.

A helyi háborúk és konfliktusok, a különféle forradalmi hullámok, illetve az orosz–ukrán háború sok tekintetben – de nem teljeskörűen – a 20. századot idéző jelenetei miatt pedig az előzőekben leírtakat érdemes egy további gondolatkörre való kitekintéssel is kiegészíteni. Ez a gondolat a totális háború gondolata,[81] de nem világháborúként, hanem a hadviselés új stádiumaként értelmezve, annak távlatos hozadékait és a technológiai vonatkozásait is figyelembe véve. Egyik oldalról ugyanis úgy fest, hogy a hagyományos hadviselés nem veszett ki a történelemből a második világháború végével, sőt nem korlátozódott kizárólag a transzatlanti térségtől távoli helyi vagy proxy háborúkra. Emiatt már önmagában is célszerű mélyrehatóan, a katonain túl a társadalmi, politikai, gazdasági, és más vonatkozásokkal egybevetve vizsgálni a totális háború tapasztalatait és megoldásait. Másik oldalról a totális háború nem csak a hadszíntéren és a háború megvívásának taktikaitól a stratégiai szintjeiig terjedően hozott történelmi változásokat, hanem a nem katonai tényezők és különösen az információ szerepe tekintetében is. Ez szorosan összekapcsolódik a totális állam tekintetében már felvázolt technikai, társadalmi és politikai változásokkal, melyek ma már információs társadalommá terebélyesedtek. Ez pedig különösen az egyes totális háborús mozdulatokat megelőző leplezett cselekmények történelmi feltárásával egybevetve szintén olyan ismereteket tükrözhet, amelyeknek jelentősége van a 21. század hibrid környezetében.

A totális háború hadviselési oldalról nézve (1) földön, vízen és levegőben (pontosabban a technológiai fejlettség számára elérhető minden térben, így ma már adott esetben a magaslégkörben, a világűrben és a kibertérben is) egyszerre zajlik, (2) minden élő és élettelen erőforrást mozgósít és latba vet az ellenség teljes leküzdése érdekében, (3) a nulla összegű játszma[82] elvén működik, (4) elmossa a hátország és a front közti, a civil és katonai, valamint a stratégiai és a politikai-konspiratív vonatkozások közti határvonalat, valamint (5) rendkívüli eszkalációs képességgel írható le. Hatóképességéhez és átütő erejéhez azonban párosítani kellett a technológiafejlődésre épülő új és hatékonyabb propaganda és hírszerzési megoldásokat, a hadviselésbe lényegében bevont hátország ellátásának és stabilitásának kitettségét, továbbá azt a tömeges tudati előkészítést, amivel a szembenálló felek ellenségeskedése a végletekig fokozhatóvá vált, és a tömeges információáramlás nélkül nehezen lett volna – ilyen történelmileg rövid időtávokon – elképzelhető.

Ha ezeket is figyelembe vesszük a totális háború kapcsán és annak értelmezését így kapcsoljuk össze a totális állam, a partizán, de még inkább az ezek mögött meghúzódó technológiai, gazdasági, társadalmi és politikai változások láncolatával – megkülönböztetett helyen kezelve az információ szerepét –, akkor úgy véljük, nem földtől elrugaszkodott dolog a jelen kihívásai kapcsán is szerepet adni ezeknek a 20. századi kategóriáknak. Ennek elfogadása esetén pedig okkal gondolhatjuk, hogy bár a 20. századot sokan a totalitás évszázadának gondoltak, a 21. század eddigi tapasztalatai alapján mégis célszerű ezt átgondolni, és ha úgy tetszik, megkísérelni a totalitás esszenciájának felvázolását és összevetését a kibertér sajátos-

81 L. Ludendorff (1940): 22–25., Ludendorff (1935)

82 Vagyis a szemben álló felek egyike csak úgy érhet el valamilyen előnyt a háború folyamán, ha annak megfelelő hátrány éri a szemben álló felet. Érdeksérelem nélküli nyereségszerzés vagy pozíciójavítás tehát nem lehetséges.

ságaival, valamint annak a nemzetek biztonságára gyakorolt hatásaival. Ebben a megközelítésben ugyanis a 20. század inkább tűnik a totalitás kibontakozását hozó évszázadnak, amely folyamat azonban még ma sem zárult le, és a kibertér–információs tér komplex hatásaival együtt szemlélve újfajta tapasztalatfeldolgozásra kell, hogy késztessen minket.

2.1. A totalitás biztonsági dimenziója az információs korszakban

Látható tehát, hogy a totalitás jelensége a világháborúk és a diktatúrák nehéz örökségének is sokrétű értelmezést ad, aminek a feldolgozása a hasonló történelmi zsákutcák elkerülésében alapvető fontosságú. A totalitás kérdése azonban túl is nyúlik ezen a nehéz örökségen, és ma a fizikai távolságok történelmi és biztonsági jelentőségét csökkenteni képes globális információs térrel már új értelmet nyer. E kérdéskör – a 20. század értelmezésére is visszahatva – fokozódó jelentőséggel bír napjainkban, amikor egyértelművé vált konkrét államok politikája szintjén is, hogy a totális védelem szemlélete[83] már különválasztható a huszadik század totalitást besározó jellegétől, és bizony szükségszerű megközelítési módja a mai biztonsági környezetnek.

A totalitás biztonsági, és biztonsággarantálási jelentőségéhez meglátásunk szerint az államtudományos értelmezés további jelentős tételeket adhat hozzá a komplex biztonságról, a változó világrendről, illetve a hibrid hadviselésről szóló, ma meghatározónak nevezhető tematikák mellett is. Ennek oka, hogy az államot mint számos környezeti tényező – így az államalkotó társadalom, a nemzetállami és a nemzetközi politika, a nemzeti kultúra sajátosságai, az államhatárokon átívelő kulturális jelenségek, a természeti hatások, a technológiafejlődés, a globális gazdaság,[84] a különféle nem állami szereplők stb. – által övezett és működésre kényszerített entitást az állam-biztonság relációban egyik oldalról az állam hatóképességének vagy hatékonyságának, másik oldalról pedig az államot érő hatásoknak a térbeli és időbeli teljeskörűsége felől közelíthetjük meg. E megközelítések azonban szükségképpen összeolvadnak, ha egy adott államtól elvonatkoztatva az állam és a totalitás viszonyát az általános szintjén vizsgáljuk, hiszen minden más állam ezáltal a környezeti hatások körébe sorolódik. Ez a meglehetősen absztraktnak tűnő megközelítés azonban a nemzeti biztonság, a biztonsági érdekek és a védelem szempontjából kiemelkedő fontosságú, hiszen rávilágít arra, hogy a biztonság a fenyegetések megelőzése és reagálása mellett az érdekek érvényesítésével is szoros összefüggésben áll, ami még tágabb cselekvési horizontot rajzol meg a biztonság fenntartására hivatott szereplőknek.

Hangsúlyozandó e tekintetben azonban, hogy a más államok által generált hatás egy komponense az állam környezetét alkotó rendkívül összetett, sokrétű és dinamikus hatásösszességnek, ami mellett a nem megszemélyesíthető tényezőkre és a nem állami szereplőkre is fokozott hangsúlyt kell fektetni. Utóbbira a védelmi és biztonsági dimenzióban már Carl Schmitt is felhívta a figyelmet a partizán elméletének idézett kérdésével, amely azóta beteljesedett jóslattá és egyben a biztonságunkat jelentős mértékben meghatározó hatássá nőtte ki magát. Fontos azonban arra is kellő figyelmet fordítani, hogy az állam biztonsági aspektusa kapcsán a nem állami szereplők tekintetében is egyre komolyabb súlyra tesznek szert a nem

83 Erre példaként l. Wither (2020) 61–81., Farkas Ádám (2015)

84 A téma kapcsán bővebben l. Pongrácz (2019a), Pongrácz (2018a), Pongrácz (2017a): 168–195., Pongrácz (2015): 222–237.

fegyveres, nem erőszakos behatások, vagyis a partizán mellett vagy azon felül egy differenciáltabb képet kell magunk elé képzelni a biztonságra jelentős hatást gyakorló nem állami, vagy nem közvetlen fenyegetési jelleget mutató jelenségek, szereplők, illetve ezek együtteseként formálódó környezeti tényezők tekintetében. Ebben a képletben pedig az információs térnek kimagasló jelentősége van napjainkban, így az információs tér tekintetében leginkább jelentős kibertér és a nemzeti, illetve nemzetközi biztonság viszonyának értelmezését is célszerű újragondolni.

Ez a megközelítés az előzőekben felvázolt kitételekkel már önmagában is egy adalék a totalitás értelmezéséhez, amely a biztonság 20. század első feléig érvényes – katonai dominanciájú – felfogásával arra mutat rá, hogy bár az előző évszázadban valóban újszerű volt a háború totalitása és az, hogy az állami szembenállás mellett jelentős szerepre tettek szert a partizánok, gerillák, forradalmárok. Azt is látni kell azonban, hogy akkor még az államok rendszerszintű, ártó szándékon nyugvó destabilizálásának döntő terepét az erőszakos, fegyveres, államközi magatartások adták. Ennek fő oka az volt, hogy a technológia még nem állt azon a szinten, hogy a globalizációt fizikai és időbeli értelemben is a glóbusz egészére kiterjedő és valós idejű kölcsönhatások mátrixaként értelmezzük. A gazdasági nyomásgyakorlás, a társadalmak kommunikáció útján történő befolyásolása vagy éppen bármely más fizikai behatás egy állam működésére tehát valamiféle közvetlen jelenlétet vagy kapcsolódást feltételezett, miközben persze az addig elért technológiai forradalmak fokozatosan új és új területekre terjesztették ki, majd nagyobb és nagyobb akciórádiusszal erősítették meg az állami hatóképességet és végső esetben a támadóképességet is. A közlekedés fejlődésével a gazdasági akcióképesség is erősödött, míg a légi közlekedés fejlődése elhozta a légi hadviselést és a repülőgépekről való megfigyelés és propaganda révén a pszichológiai és információs hadviselés új eszközeit. A kémia és az ipar fejlődése, illetve a gépesítés fokozása a szárazföldi hadviselés hatótávolságát mind tüzérségi, mind mozgékonysági értelemben megnövelte. Ezek együttesen pedig a korábbiakhoz mérten forradalmian megváltoztatták a szembenállás kereteit, hiszen a végső – államok közötti – konfliktusok rendezése lényegében elmosta a határt a hátország és a frontvonal között, megadva a totális háború esszenciáját. Ennek tudható be, hogy a 20. századot a katonai versengés és szembenállás determinálta, és annak második felére, az információs technológia fokozódó fejlődésével kezdett felerősödni igazán a hírszerzési háború vagy információs versengés, illetve a diktatúrák számára alapvető eszközként alkalmazott megfigyelő és kontrolláló képesség is a politikai rendészet kapcsán. E körben persze ki kell emelni, hogy az internet létrejöttéig, majd elterjedéséig az infokommunikációs technológiák állami kontrollálása – a fizikai csomópontok felügyelet alatt tartásával – az információkat közvetítő technikai megoldások korlátos számú csomóponthoz kötöttsége miatt még kevesebb kihívással nézett szembe, mint napjainkban. Ez pedig a sajtó- és médiafelügyelet, a titkosszolgálati jellegű megfigyelés, illetőleg a rádióelektronikai felderítés terén is egy olyan időszakot hozott el, ahol az állam szerepe rendkívülinek és megkerülhetetlennek hatott még akkor is, ha az adott állam e funkcióit jogállami keretek között működtette. Magától értetődő persze, hogy a különféle rezsimek ezekben a lehetőségekben páratlan erejű történelmi eszközre leltek, amelyek kiaknázása tovább gyarapította a 20. századi történelem sötét lapjait mind a diktatórikus, mind pedig az az ellen nem ritkán drasztikus fellépéssel védekező szereplők tekintetében. Ez az örökség pedig a totalitás kérdésének beárnyékolásán túl az államok védelmi és biztonsági funkcióin is komoly bélyeget hagyott a 20. század végére.

A 21. századra azonban mind a technológiafejlődés, mind pedig azok a tendenciák – a politika/ideológia tömegesedése, és az ezzel kapcsolatos tudattartalmak közvetítésének kiszélesedése, illetőleg ezek egyéni és társas pszichére gyakorolt hatásai –, amelyekre Schmitt a totális állam létrejöttét alapozta, újabb robbanásszerű változásokon mennek keresztül. Ezzel napjainkban a totalitás, és annak az állam környezetére és működésére vetített jelentése egyértelműen és szükségképpen új értelmet nyer. Ennek sarokpontjaként a következők ragadhatók meg:

Az információs technológiák fejlődése révén a globalizáció a Föld egésze tekintetében valós idejű és térbeli távolságokat lényegében nem ismerő kapcsolódási és hatásbeli lehetőségeket teremtett, amelynek jelentős részben a kibertér[85] adja a meghatározó dimenziót. Ezzel soha nem látott mértékben megközelítettük egy globális információs totalitás állapotát.

Az információs forradalom áthatja a gazdasági, ipari, politikai, politikán kívüli világnézeti, társadalomműködési, államműködési és ezáltal lényegében a teljes biztonsági szférát. Ez nemcsak dinamizmust, hatékonyságnövekedést és gyors reagálóképességet, hanem egyben e rendszerek sérülékenységének növekedését és új támadási/beavatkozási/befolyásolási lehetőségek létrejöttét is jelenti. Innen nézve tehát információs értelemben egy totális biztonsági kihívási mátrix is azonosítható jelenünkben.

A gazdaság infokommunikációs térbe terelésével a világ egyik pontjáról a másikra valós időben lehet pénzügyi tranzakciókat kezdeményezni, ami a visszaélésekre is lehetőséget teremt, úgy a nem állami szereplők (partizánok) külső finanszírozása, mint a bűnözés tekintetében. Ez a kapitalista világgazdaság valódi globalizálódásának totális hatásmechanizmusait mutatja meg.

Az államműködés és az egyének napi életvitelének fokozódó digitalizációja és az információs térben kialakított úgynevezett közösségi hálók révén megnövekedett a nem valós vagy torzított hírekkel való befolyásolás veszélye és hatóképessége is, illetve az állam sérülékenysége is az információs térből érkező támadásokkal szemben. Ez a nézőpont az információs totalitásból fakadó újszerű és nagy hatású sérülékenységek témakörének jelentőségét mutatja meg.

A technológia további fejlődése révén a világ egyik feléről a másik órák alatt elérhető élő erővel is, míg az interkontinentális rakétarendszerek és a műholdas technológiák révén akár percek alatt is lehetséges a távolságok leküzdése, miközben a különféle műholdas, internetes, vagy rejtett légi megfigyelési megoldásokkal a fizikai távolságoktól független megfigyelés, illetőleg műveletvezetés valósítható meg. Ez a fizikai korlátok totális relativizálódását hozza magával, hiszen a nevezett kihívások és fenyegetések korlátozásához már önmagában a fizikai távolság nem elégséges, hanem tevőleges – védelmi – magatartás tanúsítása szükséges a biztonság fenntartásához.

Mindezeket számba véve azt láthatjuk, hogy a totalitás az állam környezete – és vele működése – tekintetében a 21. századdal teljesedik ki igazán, ha azt úgy értelmezzük, mint a környezet hatásainak térben és időben is valós idejű és alacsonyan korlátozott érvényesülési lehetőségét. Kimondható meglátásunk szerint, hogy az információs tér vonatkozásában lényegében a totalitás már kiteljesedett, míg a fizikai távolságokat és korlátokat érintően közelít az újabb és újabb fejlesztések révén a teljességhez. Ez a megállapítás rávilágít arra, hogy

85 Ennek biztonsági kérdéseiről l. Simon–Magyar (2017a): 89–101., Simon–Magyar (2017b): 57–68., Pataki–Kelemen (2014): 103–116., Kelemen (2017b): 117–122., Kelemen–Simon (2020): 150–170., Kelemen–Farkas Ádám (2020): 203–226., Kelemen–Németh (2019): 51–66.

a kortárs infokommunikáció központi terepét adó kibertér egyértelműen kulcsjelentőségű a biztonság tekintetében. A totatlitás ilyetén értelmezése, illetve az e mögött álló komplex folyamatok sok tekintetben kölcsönhatásos és hálózatos megvalósulása új és új kihívások elé állítja az államot, különösen pedig annak védelmi és biztonsági funkcióit. Ezek a kihívások – és a biztonsághoz kapcsolódó társadalmi érdek – hatékony reagálást követel meg az államtól, de a 20. század totalitarizmus-tapasztalatai és történelmi traumái miatt rendkívüli szenzitivitással viszonyul a védelmi fejlesztésekben rejlő esetleges túlhatalom és a visszaélések történelmi kísértéséhez.

2.2. A totalitás kortárs esszenciájának kérdése a kibertér és a nemzeti biztonság viszonylatában

Mindezeket számba véve érdemes lehet kísérletet tenni arra, hogy a totalitás esszenciáját az előzőekben leírtak alapulvételével megpróbáljuk beazonosítani, kibontani. Ez a totalitás és az infokommunikációs fejlődés kapcsolatára építve egyrészt azért tűnik célszerűnek, mert technikailag és társadalmilag is változó környezetben ugyan, de napjaink állama is totális állam, amely számos, elsőre az államtól függetlennek tűnő területre (gazdasági működésre, kutatásfejlesztésre, véleménynyilvánítás és vallásgyakorlás kereteire stb.) nézve gyakorol valamiképp hatást. Másrészt azért, mert ebben a 21. századi totális államban számos – első ránézésre a klasszikus politikai gondolkodásba nem illő – kérdés politikai kulcstémává válhat (számos más mellett a szexualitástól az ökoszisztéma állapotán át, a tudományos fejlődésen keresztül egészen addig, hogy mely technológiai cégek termékei és milyen szempontok szerint tekinthetők biztonságosnak vagy épp veszélyesnek, illetve hogy a közösségi médiát működtető és más információs szolgáltató cégek mennyivel szélesebb adatkört birtokolhatnak az emberről, mint amit az államnak megengednénk). Ezen összefüggések, illetve a biztonságot és annak szavatolását is meghatározó komplex környezet viszonylatában tehát a totatlitás egy olyan értelmezési séma lehet, ami hozzásegíthet minket a valóban komplex és hálózatos, egyúttal pedig szükségszerűen multidiszciplináris megközelítéshez a biztonság és az annak kulcskérdését adó kibertér viszonylatában is. Ezen gondolkodásunkat támasztja alá a skandináv államok visszatérése a totális védelem[86] megközelítéséhez, de ebbe az irányba mutat meglátásunk szerint a hálózattudományok rendkívüli jelentőségének elfogadása is.[87] Ezek mindegyike ugyanis a totalitás újszerűségére és összetettségére irányítja rá a figyelmet a minket körülvevő fizikai és nem fizikai közeg tekintetében.

Az a környezet tehát, amelyben korunk állama funkcionálni kényszerül – ha fenn kíván maradni, illetve társadalmában a fejlődés és gyarapodás feltételeit meg kívánja alapozni –, az

86 Vö. Swedish Defence Commission Secretariat: *Resilience. The total defence concept and the development of civil defence 2021–2025*, inofficial summary www.government.se/4afeb9/globalassets/government/dokument/forsvarsdepartementet/resilience---report-summary---20171220ny.pdf, Norwegian Ministry of Defence – Norwegian Ministry of Justice and Public Security: *Support and Cooperation. A description of the total defence in Norway.* Oslo, Norwegian Ministry of Defence – Norwegian Ministry of Justice and Public Security, 2018. www.regjeringen.no/contentassets/5a9bd774183b4d548e33da101e7f7d43/support-and-cooperation.pdf, Government Offices of Sweden: *Development of modern total defence* www.government.se/articles/2018/06/development-of-modern-total-defence/

87 L. Castells (2005), Barabási (2017), Barabási (2018)

a komplex biztonsággal és a valódi globalitással már bevett módon írható le. Ennek, ahogy arra a biztonság szektorális elmélete rámutatott, számos szegmense és dimenziója van. Ezekkel a biztonság tartalmában egyre inkább túlsúlyba kerülnek a nem fegyveres szférák és az átfogó állami-társadalmi reziliencia igénye. Ez persze nem jelenti azt, hogy a fő ismérvként fegyveres jellegükkel leírható állami szervek jelentősége csökkent volna, egyrészt azért, mert a *differentia specificájuk*at adó fegyveresség nem kizárólagos ismérvük, másrészt pedig azért, mert a nemzetközi terrorizmustól a szervezett bűnözésen át az információs térben végrehajtott műveletekig, de ha úgy tetszik Afrikától Szírián és Ukrajnán át Tajvanig látható, hogy a nem fegyveres szférák szorosan kapcsolódhatnak az erőszakos, majd fegyveres eseményekhez, amelyekkel szemben a védelmi és biztonsági szemlélet szerint egyre inkább összehangolt módon kell fellépni. Ezen összhang tekintetében pedig fontos rögzíteni, hogy az nem csak a gyakorlati feladatellátásra, hanem a stratégiai-szakpolitikai szintre, illetve a tudományos és gyakorlati kooperációra is értelmezendő.[88] E széles látókör nélkül ugyanis a komplexitás megfelelő értelmezése, majd az adekvát válaszok kialakítása kérdőjeleződik meg.

Visszakanyarodva azonban a közeghez, amelyben ma az állam működése megvalósul, látnunk kell, hogy rendkívül összetett, sokrétű, sok tekintetben sajátos törvényszerűségek szerint működő dimenziók metszéspontján elhelyezkedő erőtérről van szó. A totalitás eszszenciájának tehát az első attribútuma az, hogy az egy számos dimenzió és sajátos működési viszonyrendszer metszéseként, közös halmazaként leírható erőtér, amelyben dinamikusan, nagy amplitúdóval és kiszámíthatatlanul váltakozik az egyes részerőterek – vagy biztonsági dimenziók – súlya. Ha úgy tetszik, nincs arra biztos képlet, hogy míg ma a gazdasági hatások a legfontosabb állami reagálást kiváltó tényezők, addig holnapra azok már következménnyé válnak egy biztonsági vagy épp egészségügyi, esetleg természeti esemény miatt. Természetesen ez a reláció megfordítva, vagy nagy számú variációk szerint kombinálódva is elképzelhető. Ez a kiszámíthatatlan kölcsönhatásosság – a 20. század végének, 21. század elejének negatív tapasztalatai alapján – egyértelművé tette, hogy a reagálás képességeinek elhanyagolása, szándékolt leépítése egy éles környezeti változás esetén még a legnagyobb anyagi eszközökkel sem pótolható azonnal. Ezek eredményeként pedig kimondható, hogy a környezethez igazodó képességek nélküli reagálás nagy valószínűséggel hatványozni fogja a dinamikusan változó fenyegetések potenciálisan bekövetkező káros hatásait.

A totalitással azonosítható környezeti kihívások és fenyegetések megfelelő reagálása ebből következően épp oly kölcsönhatásos megoldásokat és szemléletmódot igényel, mint amilyen összekapcsolódás lehetséges a totalitás különböző részerőterei tekintetében. Ezt a megállapításunkat a totalitás szempontjából megkülönböztetett jelentőségű kibertér, illetve az azzal kapcsolatban bővülő, kibontakozó megközelítés is alátámasztja, hiszen a technikai jellegű problémafelvetés és megoldások keresése mellett egyre erőteljesebbé válik a katonai és hírszerzési, a társadalomtudományi, a pszichológiai, illetve a jog- és államtudományi dimenzió hangsúlyozása is. Ezt a sokrétűséget a később még elemzésre kerülő hibrid szcenáriók felértékelődése és sajátosságai is alátámasztják.[89]

Ennek a sok halmaz metszéséből kialakult erőtérnek van azonban egy további totalitáshoz köthető attribútuma, amely elsősorban a technológiai fejlődésen, azon belül pedig nagyrészt – de nem kizárólag – az információs technológia, és különösen a kibertér fejlődésén

88 A téma kapcsán l. Farkas Ádám (2022a)

89 L. Giannopoulos–Smith–Theocharidou (2021)

alapul. Ez pedig nem más, mint a tér és idő rendkívül intenzív relativizálódása. Az információs technológiák fejlődése miatt ugyanis ma már a Föld egyik pontjáról a bolygó ellentétes oldalán lévő másik pontjára valós időben lehet gazdasági, társadalmi, politikai hatást gyakorolni, méghozzá jelentős mértékben. E körben az állami szervezetek, a termelő és szolgáltató szektorok digitalizációja miatt akár támadással egyenértékű működési zavarokat is elő lehet idézni ebből a távolságból, amire korábban csak fizikai kapcsolódás révén, viszonylagos előrejelezhetőség mellett volt lehetőség. A totalitás esszenciájának tehát a második attribútuma az, hogy a tér és idő korlátai az államokra, társadalmakra és egyénekre nehezedő hatások tekintetében elvesztették korábbi korlátozó jelentőségüket, amiből biztonsági aspektusban az is következik, hogy egyre jellemzőbb lesz az államhatárokon átívelő fenyegetési formák súlyának növekedése és az előrejelzés lehetőségeinek korlátozódása. A tér és idő biztonsági jelentőségének relativizálódása tovább erősíti az első attribútum kapcsán vázoltakat, hiszen az előrejelző képesség mérséklődése/korlátozódása a biztonsági szint megtartása érdekében a reagáló képesség fokozását, a multidimenzionális és interoperábilis jelleg miatt tehát a különféle szférák hatékonyabb együttműködését és összehangoltságának fokozását teszi szükségessé.

Ez a kibertér kérdésére vetítve például megragadható úgy, hogy a technikai jellegű védekezés és reagálás képességei mellett kiemelkedő fontosságú a technikain túl a hatósági és képzési-felkészítési jellegű megelőzés erősítése, a potenciális támadásokból következő további (például társadalmi, politikai, gazdasági stb.) hatások azonnali enyhítésének biztosítása, vagy épp a megfelelő eseménykezelési, tapasztalatfeldolgozási és döntéselőkészítési mechanizmusok biztosítása az ismétlődő kártételek elhárítása, illetve a reagálás hatékony, gyors, de megalapozott biztosítása érdekében. A kibertérre vetítve kapcsolódó követelmény a technikai fókuszpontok mellett a pszichológiai, szociológiai, politikai és szabályozási sajátosságok megfelelő azonosítása, számításba vétele és korszerű reagáláshoz kapcsolása. A tér és idő relativizálódása kapcsán tehát látni kell, hogy a valós idejű és fizikai korlátoktól kevéssé/alig kötött fellépésre való közvetlen reagálás mellett a biztonság komplexitásából következő valamennyi dimenzióban számolni kell a relativizálódás hatásaival, de lehetőleg úgy, hogy az elhamarkodott és hibás döntések, lépések lehetősége minimalizálva legyen.

Erre, és az államnak a biztonság garantálásában betöltött sajátos és kivételes szerepére figyelemmel még legalább egy tekintetben fontos a totalitás és az állam relációján elgondolkodni. Ez pedig a hatékony, vagy ha úgy tetszik, a jó állami működés és a totalitás kapcsolata. Abból adódóan ugyanis, hogy a totalitás a tér és idő korábban megszokott korlátjaitól részint elszakadva képes rendkívül intenzív behatásoknak, nyomásgyakorlásoknak teret engedni, az a képlet is megváltozott, hogy az állam hatékony működésének elsődleges záloga a működéshez és a védekezéshez való konkrét képességek, ha úgy tetszik, az erő és annak megmozdításához szükséges rutinok megléte. Ma ugyanis, amikor már a nyugati típusú szabályozott államiság globálisan elterjedőben van – igaz, sok helyen ez csak formális követelményként érvényesül Európán kívül –, az állam képességein túl fontos a képességek alkalmazásának hogyanja, szabályozottsága és szabályszerű működése is. Ennek keretei ugyanis a jogbiztonságból fakadó nyílt szabályozás és az információs tér révén globálisan megismerhetők, és adott helyzetekben úgy és oly módon is vizsgálhatók és értékelhetők, hogy az az állam hatékony fellépését ne erősítse, hanem éppen, hogy gyengítse, ha az adott állam a cselekvés ideje előtt elhanyagolta a saját szabályozását, működési rendjének korszerűsítését vagy jogi

vállalásainak körülbástyázását. Ezt a jelenséget nevezi a szakirodalom *lawfare*-nek[90] az angol jog és hadviselés szavak ötvözésével, de ebbe az attribútumba tudhatók be mindazok a megoldások is, amelyek a jog alkalmazhatóságát, és ezáltal a legitim állami fellépést igyekeznek aláásni például a hibrid konfliktusok tekintetében.[91] Ennek megvalósulási példái az egyes távol-keleti területi viták eltérő nemzetközi jogi értelmezéseinek világhálón való propagálása, az ukrán válság majd háború és különösen a Krím félsziget annektálásának nemzetközi jogi értelmezései, vagy éppen a különféle válságok esetén a rendfenntartó és katonai erők felhatalmazásainak világsajtóban való elemzése körében is megtapasztalhatók. Komoly felületet adhat azonban ennek a jelenségnek és a jogon túl különösen a politikai és társadalmi kapcsolódásainak a konkrét krízisek utáni – indulati jellegű, drasztikus – állami reakciók kérdésköre. A PATRIOT Act, illetőleg a terrorizmus jelentette kihívással összefüggő, illetve azon túl is nyúló titkosszolgálati tevékenységek a transzatlanti térségben erőteljes példáját adták ennek. Nem szabad ugyanis elfelejteni, hogy e vonatkozásban a totalitás kapcsán nem „jogászkodás" zajlik, hanem a jog társadalmi és politikai kötöttségének és determinációinak alkalmazása adott helyzetek és állami cselekvések delegitimizációjára. Az államot korlátozni hivatott, és az állam által fejleszthető szabályozás naprakészsége tehát bekerült a totalitás értelmezési tartományába a tényleges képességek mellé. A totalitás esszenciájának harmadik attribútuma tehát, hogy az állam cselekvőképességét és stabilitását nemcsak a cselekvéshez szükséges technikai és élőerős képességei, hanem azok szabályozási és működési mechanizmusainak összessége, különösen a hálózatosság kritériumainak való megfelelés, vagyis az állam rendszerszintű korszerűsége is meghatározza. Ennek avíttsága a tényleges képességek kiaknázásának hatékonyságát csökkenti, míg legitimációs-politikai-tudati oldalról komoly sérülékenységet, támadási felületet jelenthet mind az államközi szembenállások, mind a nem állami szereplők viszonylatában. Ezt az elmúlt évek helyi háborúihoz kapcsolódó lélektani műveletek, illetve diplomáciai és kommunikációs kampányok épp úgy alátámasztják, mint a terrormarketing tapasztalatai, illetve a különféle hackercsoportok fenyegetései és üzenetei. Nem véletlen, hogy a kapcsolódó külföldi szakirodalomban a jogi reziliencia[92] gondolata is jelen van már, amit szükségszerű a jog társadalmi-politikai konstruktum jellegéből adódóan a szabályozás konkrétumain messze túlmutató keretek között értelmezni. E téren a kibertér, az információs technológia fejlődése, a mesterséges intelligencia mind-mind olyan hívószó, amely komoly lehetőségeket és kihívásokat is jelent az állam- és jogrendszer következő évtizedekben jelentkező fejlesztései során.

A konkrét képességek megfelelő alkalmazhatósága, illetve az idejétmúlt, nem korszerűsített szabályozás tényleges védekezésre és reagálásra gyakorolt hatásait úgy véljük, korszakosan példázta a terrorizmus elleni fellépés szabályozásának dinamikus fejlesztési kényszere mind a 9/11, mind pedig a 2015–2016-os terrorhullám vagy a Covid19 világjárvány után. Ugyanilyen negatív tapasztalatként tekinthetünk azonban az Európa-szerte látható haderőfejlesztések szabályozási kérdéseire, illetve a technológiafejlődés szorításában lévő hírszerzési és elhárítási funkciók korszerűsítése és a kapcsolódó szabályozás problémái tekintetében. Ezek

90 Hazai megközelítése kapcsán l. Hódos (2020): 39–64., Farkas–Resperger (2020): 132–149., Farkas Ádám (2020a): 11–23.

91 A téma kapcsán l. Treverton et al. (2018), Cullen (2018), Resperger (2018a), Simicskó (2017): 3–16., Somodi–Kiss (2019): 22–28., Porkoláb (2015): 36–48.

92 L. Sari (2019a)

a példák mind-mind évtizedekre háttérbe szorult vagy elhanyagolt funkciók és szabályozási-működési szisztémák konkrét fenyegetések, illetőleg támadások által kikényszerített korrekcióját tükrözik.[93] Fontos azonban kiemelni, hogy az ilyen módon kikényszerített változtatások jellemzően az adott kiváltó okra fókuszálnak és jellemzően erősen túlzó megoldásokat eredményeznek. Ezt a magyar különleges jogrendi rendszer 1989 és 2022 közötti változásai épp úgy tükrözik, mint a 9/11 utáni jogalkotás, az amerikai hírszerzési botrányok és szabályozási leképezésük az elmúlt évtizedekben, illetve a francia különleges jogrend kihirdetése, majd terrorellenes arcélű jogalkotásba fordulása. A rendszerszintű naprakészséghez komplex megközelítés és ciklikusan ismétlődő felülvizsgálat kell, amihez viszont a sajátos felkészültségű szakállomány és a think tank jellegű háttértámogatás megkerülhetetlen, ahogy ezt a reziliencia körüli törekvések, illetve a hibrid fenyegetések elleni fellépés példái mutatják az elmúlt években. Az ilyetén módon komplex megközelítéshez pedig nélkülözhetetlen például a kibertér és a nemzeti biztonság összefüggéseinek széles körű elemzése is.

Mindezeket számításba véve egyértelműen látszik, hogy a totalitás tartalma az állam környezetére vetítve rendkívüli mértékben kitágult és elmélyült. Az állam és a jog pedig nem önmagában és önmagáért való, hanem az államalkotó nemzet, illetve társadalom biztonságát, rendezett működését és fejlődését hivatott garantálni, amiből következően az állami működés és a jogi szabályozás a totális biztonság viszonylatában már egy komoly képességi és hatékonysági összetevőként értékelendő. Ahogy Schmitt írta: „egy normális állam teljesítménye mindenekelőtt abban áll, hogy az államon és területén belül létrehozza a teljes megelégedettséget, fenntartja a »nyugalmat, biztonságot és rendet« és ezáltal normális helyzetet teremt".[94] A környezet változása tehát kényszerhelyzetbe hozta az államot, hogy reagáljon a változásokra a saját rendszerei tekintetében is, alkalmazkodjon a környezethez a hatékony és eredményes fennmaradás, a rend, a biztonság és a nyugalom garantálása érdekében. Ez az állam történelmi evolúciójának törvényszerűsége, amelyen egyébként a gazdaságilag jól teljesítő államok működése alapvető és nélkülözhetetlen „közszolgáltatásként" nyugszik és amelyből következően a jólét egyik összetevőjeként is értelmezni kell az állam biztonsági funkcióinak hatékony működését.

Ehhez célszerű hozzátenni azt is, hogy az állam védelmi és biztonsági funkciói nem csak a kényszerintézkedéssel, fegyveres fellépéssel párosuló cselekmények lehetősége miatt sajátos jelentőségű, hanem az ezek szervezéséhez, fejlesztéséhez, illetve az állam- és társadalom védelmi-biztonsági felkészítéséhez szükséges sajátos szemléletmód és ismeretanyag miatt is. Ezek a speciális tudásbázisok ugyan részlegesen piaci alapon is szervezhetők, de össztársadalmi és államrendszeri léptékben csak állami szerepvállalással valósíthatók meg, amely azonban ma már nélkülözhetetlenül igényli az állami-társadalmi együttműködést. Az infokommunikációs fejlődés jelentette kihívás és a kibertér e tekintetben is komoly indukciós tényezőként értelmezhető – a korábbi hadiipari együttműködések mellett –, hiszen egyértelmű példák mutatnak afelé, hogy jelentős transzatlanti szereplők sora tesz olyan nyilatkozatokat és deklarációkat, amelyben a hatékony biztonságszavatolás tekintetében nélkülözhetetlenné nyilvá-

93 A téma kapcsán l. Sulyok (2019): 35–60., Farkas Ádám (2017b): 5–20., Kelemen (2019a): 9–35., Spitzer (2019b): 1–13., Bartkó (2019): 37–57., Bartkó–Sántha (2018): 83–100., Bartkó (2017a): 315–327., Bartkó (2017b): 5–18.

94 Schmitt (2002): 31.

nítja az iparral és a „civil" szférával való együttműködést.[95] E körben a kibertérrel összefüggő fejlődés dinamikája, valamint a már most is nehezen átlátható kihívások sora korszakos hatásokat mutat.

Álláspontunk szerint a totalitás kiteljesedésével párhuzamosan látni kell azt is, hogy az infokommunikáció fejlődése kulcsszerepet játszott abban, hogy a biztonságfelfogás a 20. században előbb elhagyta a katonai dominanciát és a komplexitás felé mozdult el, majd napjainkban olyan szintre lépett, ahol a biztonság rendszerszintű garantálásában korábban kizárólagos vagy legalábbis döntő túlsúlyt képviselő államnak megkerülhetetlen a kooperatív hozzállás kialakítása a nem állami szférával. Ezt a jelenséget ugyan nem csak az infokommunikációs jelenségek és a kibertér táplálják, de ki kell mondanunk, hogy ezek szerepe kulcsfontosságú. Azt pedig a jövő kutatásai, fejlesztései és szabályozási-szervezeti reformjai kapcsán kell rögzítenünk, hogy ez a szemléletváltás komoly működési, megközelítésbeli kérdéseket is napirendre fog tűzni, elsőként azon kognitív képességek kialakítását, amelyek hatékony és szakszerű transzformációt tudnak szavatolni a civil és az állami – védelmi-biztonsági – szférák között, illetve ezeken belül az egyes szakterületek, majd az elmélet és gyakorlat, végül védelmi dimenzióban a harcászati és hadműveleti, valamint a stratégiai szintek között. Ebben a kihívásban a kiberbiztonság területe szintén kulcsszereppel, példaadó jelleggel bírhat a jövőben, hiszen egyszerre zajlik a konkrét képességek és megoldások fejlesztése, a szakpolitikai és szabályozási környezet alakítása, valamint a megfelelő tudatosítási és multidiszciplináris tudástranszfer megoldások kialakítása e téren.

A totalitás esszenciájának fent azonosított fő vonásaira tekintve tehát – a további kutatások szükségessége mellett is – meghatározhatjuk azokat a fő irányokat, amelyek a megváltozott és a változásban lévő környezethez való alkalmazkodás érdekében az állam fő kötelezettségei. Ezeket röviden a következőkben foglalhatjuk össze:

(1) Az államnak a fennmaradás, a társadalmi rend, stabilitás és fejlődés, valamint az egyéni jogok érvényesülése (összefoglalóan a biztonság) érdekében éppúgy komplex módon kell felkészülnie a környezetből érkező hatásokra, amiképp maga a totalitással leírható környezeti erőtér is összetett, sokrétű és váltakozó dinamikájú. Ez egyik oldalról azt jelenti, hogy a klasszikusan védelmi és biztonsági szegmensekben is egyre nagyobb figyelmet kell szentelni a nem fegyveres és nem erőszakos tényezőknek és szféráknak. Ehhez a nézőponthoz fontos hozzávenni azon képességek kialakításának megkerülhetetlenségét, amelyek tudományos-szakmai-gyakorlati dimenziókat együtt kezelve tudnak interfészként működni a védelmi-biztonsági szféra ágazatai és szervezetei, illetve az azokon kívüli állami és nem állami – együtt: „civil" – szereplők között. Másik oldalról azonban azt is szükségessé teszi, hogy az állam fegyveres védelmi és biztonságszavatoló funkcióin kívüli ágazatoknak és viszonyrendszereknek is nyitottságot kell mutatni a biztonság- és védelemtudatosságuk fokozására, és az ehhez szükséges protokollok meghonosítására és begyakorlására. E két aspektus szintézise akkor érhető el, ha az állam a képességei korszerűsítése és fejlesztése mellett szabályozásának rendszerszintű megújítására, illetve a képességek alkalmazásának összehangolt irányítására és a személyi állomány megfelelő felkészítésére is figyelmet fordít. Egy komplex és váltakozó dinamikájú kihívási közegben ugyanis az összehangolt és sokrétű látásmód nélkül irányított, koordinált és fejlesztett képességek „önálló" vagy „domináns" tényezőként hatékonyan már

95 Vö. Petruska–Vikman (2021), Budavári (2023): 34-48., Farkas Ádám (2021b)

nem tudnak érvényesülni, vagyis a legköltségesebb fejlesztések hatásfoka is komolyan csökkenhet a működési diszharmóniák miatt.

(2) Figyelemmel arra, hogy a totalitás esszenciája a tér és az idő klasszikus korlátozó jellegeit – elsődlegesen az információs technológiák széles körű alkalmazása és további terjedése miatt – feloldotta, az államnak úgy kell a digitalizáció előnyeit kiaknázni és a maga területén a magáncélú digitalizációs tevékenységeket szabályozni, hogy azok tekintetében egyrészről a biztonság garantálása fajsúlyosan jelenjen meg, másrészről pedig a legfontosabb – úgynevezett létfontosságú – rendszerek és szolgáltatások tekintetében biztosított legyen az információs térből érkező támadások vagy az ott keletkezett üzemzavarok esetére is a legszükségesebb szintű működés. Evolúciós példával élve tehát az államnak a civilizálódás minden előnye mellett is fenn kell tartania az önvédelem legalapvetőbb és a fejlődés hajnala óta meglévő ösztöneit és rutinjait is. Ez szükségképpen annak a követelményét is magában rejti, hogy az állam és az annak védelmét és biztonságát szavatolni hivatott intézmények és szakemberek képesek legyenek a tér és idő korlátait relativizáló/feloldó komplexitásban és gyorsaságban működni és gondolkodni, de egyben fel legyenek vértezve egy olyan látásmóddal is, amely akkor válik szükségessé, ha az információs tér destabilizálódik, és vele a tér és idő korlátozó volta újra felerősödik. Ez ugyanis a digitalizáció miatt megváltozott életvitelre tekintettel prognosztizálhatóan rendkívüli társadalmi hatásokat válthat ki az egyéb krízisek, fenyegetések, támadások lehetősége mellett.

(3) Figyelemmel arra, hogy a totalitásban az állam képességein túl annak egész rendszere, szabályozása és vállalt kötelezettségeinek teljesítése is tényezőként jelenik meg, amelyet a világ bármely pontjáról ellenőrizni, kritizálni, támadni lehet egészen az államalkotó társadalomra irányuló befolyásolási törekvésekig, kulcsfontosságú, hogy az állam fejlesztése, korszerűsítése ne csak a képességekre és aktuális kihívások kezelésére fókuszáljon, hanem a korszerű szabályozási, működési megoldásokra és a biztonsági érdekek érvényesítésének szisztematikus körülbástyázására is. Az állam fejlesztése során tehát rendszerszerűen az állam egésze felől kell közelíteni, mert az egy-egy területre fókuszáló vagy egy-egy eseményre ad hoc módon reagáló fejlesztési beavatkozások biztos, hogy rendszerszintű inkonzisztenciához, biztonsági szempontból pedig sérülékenységhez, új támadási felülethez vezetnek.

A totalitás értelmezésére és 21. századi esszenciájának azonosítására tett kísérlet is egyértelműen rámutat arra, hogy az állam, és ennek megfelelően az államtudomány és jogtudomány sem kerülheti el a körülményekhez való alkalmazkodás kényszerét. Korunk térben és időben kevéssé korlátozott, korábban nem látott hatóterű és hatóerejű totalitása és az ezt tápláló elsődlegesen technológiai, másodlagosan gazdasági, társadalmi, ökológiai, pszichológiai folyamatok mind-mind azt teszik szükségessé, hogy az államról és annak fejlesztéséről komplex módon, a külső környezet változásaival összhangban álló módon gondolkodjunk. Ezt a sokrétűséget csak a multidiszciplináris megközelítés megfelelő alkalmazása, a stratégiai fejlesztési think tankek meghonosítása, illetve az elméleti és gyakorlati, illetőleg a specialista és generalista szemléletmód megfelelő egyensúlya mellett lehet elképzelni, amely irány már önmagában is komoly reformkihívásként értelmezhető a mai működési modellekhez mérten. A kibertér sokrétűsége és számos területhez való kapcsolódása azonban ebben is értékes példákat mutathat, illetve indukciós tényezőként hathat, remélve, hogy idővel a kibertér multidiszciplináris megközelítésének kibontakozása a totális biztonság egészére is ki tud majd terjedni a korszerű, hatékony, de szükséges és arányos működés elérését segítve.

2.3. A hibriditás mint a totalitásból táplálkozó nem konvencionális kihívás

A hibrid konfliktusok képében bizonyos szempontból egy régi ismerős tekint vissza ránk, egy valóban újszerű formában.[96] Ha csak a fogalommal szinte összemosott orosz állam 20. századi történelmét nézzük, akkor azt látjuk, hogy a Szovjetunióban óriási hagyományai voltak a sokrétű, nem tisztán katonai lépésekre építkező stratégiai érdekérvényesítésnek és eszközrendszernek. A maszkirovka katonai alkalmazása, majd ennek a szemléletmódnak a kiszélesítése több mint százéves múltra tekint vissza. Ehhez persze hozzá kell tenni, hogy önmagában véve a nem katonai tényezők hadászati-stratégiai célokat megalapozó vagy előkészítő, illetve konkrét katonai művelteket kísérő alkalmazása messze nem újdonság a világtörténelemben, mivel Sun Ce, Taj Kung vagy Vej Liao-Ce óta ismertek. Az állami, társadalmi sajátosságok katonai műveletekkel összefüggő kiaknázása, a kémek alkalmazása, az ellenséges területek lakosságához való viszonyulás, az ellátási láncokra való hatásgyakorlás mind-mind olyan témakörök, amelyek már az antikvitás óta jelen vannak a hadviselésre, stratégiai gondolkodásra vonatkozó irodalomban. Ez a komplex, a katonai és a nem katonai elemeket vegyítő – és ilyenként hibrid – megközelítés aztán egyre markánsabban átszivárgott a katonai gondolkodástól különváló politikai filozófiai és államtudományi gondolkodásba is Niccolò Machiavellitől Napóleonon át Carl Schmittig, hogy aztán visszahasson a hadviselés elméletére, és abban szélesebb horizontot tárjon fel, mint maga a háború megvívásának katonai dimenziója, ahogy ez Carl von Clausewitz abszolút háború felfogásában, majd Erich Ludendorf totális háborújában megjelent.

Így szemlélve tehát, ha a hibrid fenyegetéseket a katonai és a nem katonai tényezők és célok kombinált alkalmazásaként fogjuk fel, nem mondhatjuk, hogy a jelenség magja újszerű lenne. Feltehető a kérdés, hogy mi eredményezte mégis a régi ismerős forradalmi átalakulását, amely révén mára a hadviselés új generációjáról, sőt a biztonsági környezet gyökeres változásáról beszélünk. A válasz világos: újszerűsége a „korábban is alkalmazott nem katonai tényezők tárházának robbanásszerű gyarapodásának és ezáltal kialakulni látszó stratégiai dominanciájából, illetve ezek hatóerejének a társadalom- és technológiafejlődés miatti megerősödéséből következik."[97] A mögöttes technológia- és társadalomfejlődés origóját pedig a digitalizáció és annak – különösen, de nem kizárólag társadalmi – térnyerése jelenti. Ez ugyanis alapjaiban szabta újra az állam működését és a társadalmi, gazdasági folyamatokat az egyéni szintű interakciók széles körétől a napi szokásokon át a csoportos és társadalmi szintű viszonyulásokig. Ezzel pedig a stratégiai – és ezek között hadászati – célokra is használható nem katonai tényezők szerepe páratlan mértékben megnőtt. Míg tehát a történelem korábbi szakaszaiban ezek a tényezők korlátozott szereppel bírtak, hiszen kiaknázásukhoz fizikai jelenlétre volt szükség, addig ma a digitalizáció által részben feloldott fizikai kötöttségek miatt sokkal nagyobb szerepe van a nem katonai tényezőknek, mint korábban valaha.

A hibriditás védelmi és biztonsági vonatkozásai kapcsán jellemzően három fogalom keveredik gondolkodásunkban: a hibrid hadviselés, a hibrid konfliktus, valamint a hibrid fenyegetés. Ezek szoros összefüggésben állnak egymással, de nem tehető közéjük egyenlőségjel. Keveredésük azonban tévútra viheti mindazokat, akik a katonai-stratégiai értelmezésnél tágabb kontextusban kívánják megérteni ezeket a jelenségeket, márpedig a jelenleg zajló orosz–

96 L. Murray–Mansoor (2012), Fridman–Kabernik–Pearce (2019)
97 Farkas Ádám–Resperger (2020): 132.

ukrán háború ellenére korunk biztonsági környezetét ez a kérdéskör a hagyományos katonai konfliktusok terepénél jóval nagyobb mértékben szövi át.

E három kategória tehát a tág értelemben vett biztonsági környezet hibriditásának tagolásaként is felfogható, amelyek egymáshoz viszonyított megértése azért is fontos, mert rá tud világítani arra, hogy egy hibrid szcenárió szerinti beavatkozásra készülő állami vagy nem állami szereplő milyen módokon, mikor és mennyire elhúzódó módon építheti fel a megcélzott állam vagy közösség ellen megvalósítandó tevékenységeinek láncolatát. Fontos e tekintetben arra külön is felhívni a figyelmet, hogy az államok közti rivalizálásban, sőt a nem állami szereplők államhatalommal szembeni fellépéseiben is hagyományosan nagy szereppel bír a társadalom, amely az állam hatalmának legitimációs és egyben élő alapját adja. A digitalizáció, és különösen annak az egyénitől a társadalmi szintig terjedő hatásai ugyanis könnyebben elérhetővé teszik ezt a hagyományosan fontos társadalmi dimenziót, amivel sokrétű lehetőséghalmazt nyitnak meg mindhárom hibrid narratíva előtt. A hibrid hadviselés – hibrid konfliktus – hibrid fenyegetés reláció ugyanis ebben a sorrendben a szűkebbtől a tágabb kategória felé halad, amit ezért érdemes ehelyütt kibontani.

A hibrid hadviselés egyértelműen katonai értelemben vett, főbb elemeiben katonai gondolkodásmód szerint és eszközrendszer segítségével megvalósított fellépést jelent. Ha nemzetközi jogi értelemben nem is, tartalmi értelemben ez egy háborúmegvívási formulaként is felfogható.[98] Bár az amerikai szóhasználat miatt kedvelt a „hadviselés" kifejezés jelzős szerkezettel való megjelenítése számos új típusú kihívás kapcsán – például információs hadviselés, kiber hadviselés, pszichológiai hadviselés –, fontos rögzíteni, hogy a hadviseléshez tartalmilag szükséges legalább egy olyan fél, amely haderőként, a hadviselés szabályaihoz igazodva lép fel a szembenállásban. Ebben az értelmezésben a hibriditás nagyrészt azt jelenti, hogy a katonai szembenállás megvívása nem tisztán és nem kizárólag katonai eszközök és tényezők alkalmazásával valósul meg.

A szembenállás azonban jól azonosítható és földrajzilag is behatárolható, e kereten belül pedig jelentős részben a katonai gondolkodás stratégiai-hadműveleti-harcászati dimenzióiban bevett sémákra épít. Szigorúan értelmezve az orosz–ukrán szembenállást, álláspontunk szerint a hibrid hadviselésről onnantól célszerű beszélni, ahonnan a felek nyíltan katonai eszközökkel és a hadviselésre jellemző szerveződéssel, katonai műveleti keretek között léptek fel egymás ellen. Kiemelendő persze, hogy a hibrid hadviselésben a katonai megközelítés és működés dominanciája mellett érvényesül a nem katonai tényezők kiaknázása, vagyis azok mögött sok esetben – magas eszkalációnál többségében – a katonai műveleti célok támogatása azonosítható.

E körben beszélhetünk a katonai tevékenységet segítő nem katonai kibertéri cselekményekről, diplomáciai és gazdasági lépésekről, illetve rendkívül jellemző módon olyan információs és kommunikációs törekvésekről, amelyek célja a szemben álló fél erőinek, nemzetközi és nemzeti támogatottságának destabilizálása. Ezutóbbi körben pedig a digitális térnek kimagasló szerepe van az emblematikus személyes történetek propagálásától, a veszteségszámok eltérő kommunikációján át a szembenálló felek egymás ellen vívott, de lényegében a globális társadalmi tér digitális szférájának egészére kiterjeszthető dezinformációs műveleteiig. A digitális tér fizikai kötöttségektől függetlenedő hatóképessége pedig azért is fontos, mert a jelenleg zajló háború kapcsán is jól látható, hogy a katonai-stratégiai célokat támogató

98 Renz–Smith (2016), Zarembo–Solodkyy (2021)

lépések egyik fél részéről sem korlátozódnak a műveleti terület lakosságára, hanem kiterjesztésre kerülnek a konfliktusra reagáló valamennyi állam digitális közösségeire is, amennyiben azokban reagálási hajlandóság mutatkozik.

A hibrid konfliktus az értelmezés következő – tágabb – osztályozási szintje lehet a gondolatrendszerünkben. E körben is jellemző a katonai stratégiai célok fajsúlyos megjelenése, illetve azok előmozdítása vagy elérése, de az az időbeli és a funkcionális horizont jelentősen kiszélesedik. Ebben az értelmezésben is egyértelműen azonosítható egy konkrét szembenállási helyzet. Ez a belbiztonsági krízis szintjén túllépő, esetileg vagy földrajzilag lehatároltan a fegyveres konfliktusra jellemző vonásokkal is párosul. Ebben a megjelenési formában azonban a katonai dimenzió helyett vagy mellett a különféle nem katonai tényezők szimultán alkalmazásának van kimagasló jelentősége. E körben például olyan nem nemzetközi fegyveres konfliktusos jelleg is azonosítható, amelyben csak fenntartásokkal bizonyítható egy szembenálló fél katonai jelenléte, mivel inkább szakadár, illetve polgárháborús jelleget ölt a konfliktus, mint háborúsat.

A hibrid konfliktus vonatkozásában a külső beavatkozás tekintetében a megcélzott államon belül szított fegyveres szembenállással közel egyenértékű súlyt kaphatnak a nem katonai tényezők. E tekintetben a gazdasági és a diplomáciai nyomásgyakorlástól a nemzetközi jogi fellépésen át a titkosszolgálati eszközökkel megvalósuló destabilizációs, dezinformációs és befolyásolási műveletekig terjedő paletta rendkívül széles.[99] Ebben a perspektívában a kibertér alkalmazása már a katonai dimenzión messze túlmutató jelentőséggel bír, elsősorban a döntéshozatal, illetve a társadalmi támogatottság aláásása kapcsán. A hibrid konfliktus tehát felfogható egy köztes állapotként is,[100] amikor jelen lehet már egyfajta katonai jellegű szembenállás vagy annak a perspektivikus lehetősége – akár szövetségi szinten is –, de a nyílt, háborús vonásokkal bíró konfliktus helyett még a nem katonai szférákban zajló beavatkozások súlya tekinthető meghatározónak.

Úgy is mondhatjuk, hogy a hibrid konfliktusban már egyértelmű a direkt és közvetlen szembenállás, de annak megvívásában még nem a katonai erő dominál, hanem a nem katonai tényezők széleskörű és stratégiailag szervezett alkalmazása a szembenálló fél stabilitásának aláaknázása, illetve potenciális – katonai narratívára is kiterjedő – cselekvési lehetőségeinek korlátozása érdekében. A hibrid konfliktus tehát felfogható a hibrid hadviselés előkészítéseként is, de nem jelenti azt, hogy a konfliktusból szükségképpen háborús, illetőleg nyílt katonai szembenállás következne. A hibrid konfliktusnak tehát a hibrid hadviselésbe való átlépés lehetséges, de eshetőleges következménye, ami egyfelől a katonai dimenzión túlmutató beavatkozásokat alapoz meg, másfelől azonban a szembeálló fél korlátozásán belül az esetleges katonai műveletek előkészítését szolgáló beavatkozásokkal is operál.

Mindezekhez mérten a hibrid fenyegetés a legtágabb kategóriaként ragadható meg.[101] Itt a nyílt katonai fellépés távlatos lehetőségként, illetve a többi cselekménnyel szembeni reakciók mérséklésére szolgáló, elrettentésként jelenik „csak" meg. A katonai erő a fellépés hátterében, a geopolitikai versengésbe ágyazottan van jelen. A fenyegetési palettán lényegében a nem katonai tényezők alkalmazása dominál, de a katonai stratégiai gondolkodásból merített szisztematikusság és a nagyhatalmi pozícióerősítés érdekében, vagyis olyan céloktól vezérel-

99 van der Putten et al. (2018)
100 Balaban–Mielniczek (2018)
101 Cucumano–Corbe (2018)

ve, amelyek a történelem korábbi szakaszaiban hagyományosan katonai erővel voltak biztosíthatók, ma azonban ezek direkt alkalmazása nélkül is előmozdíthatók. Ennek fontossága abban rejlik, hogy a nyílt katonai fellépés egyértelműen korlátozó-romboló reakciót vált ki az agresszor nemzetközi kapcsolataira és gazdasági pozícióira nézve, míg az ezt elkerülő hibrid narratíva kiválthat szankciókat, de teljes körű politikai-gazdasági ellentevékenységet nem tud megalapozni.

A hibrid fenyegetésben kulcspozíciót töltenek be a titkosszolgálati eszközök és módszerek, a társadalmi tényezők, a különféle – a beavatkozóhoz közvetlenül nem köthető – nem állami szereplők, illetve a politikai és gazdasági térben megvalósuló cselekmények. Ez persze azt is feltételezi, hogy a hibrid fenyegetések eszközként való alkalmazása több éves vagy akár évtizedes felépítési és alkalmazási ciklusba ágyazottan valósítható meg. A digitális tér jelentősége ebben a szférában az információs és a pszichológiai műveletekbe ágyazottan a legnagyobb,[102] hiszen kiváló terepet biztosít a humán tényezőre épülő destabilizációs és befolyásolási műveleteknek az egyénitől a társadalmi szintig. Lényegét tekintve úgy is fogalmazhatnánk, hogy a hibrid fenyegetéseknek döntően, de nem kizárólag a digitális térre épített cselekményei adják a bevezetőben említett régi ismerős valóban új megjelenési formájának esszenciáját. Ez a legtágabb kategória végső soron valamely hatalmi szereplő szisztematikus, térben rendkívül tág, akár globális keretben is megvalósuló, rövid-, közép- és hosszútávú stratégiai célok elérésére egyaránt alkalmas, nem katonai eszközökre építő, de a katonai erő bevonásának lehetőségével, illetve a katonai és a titkosszolgálati erők nem hagyományos feladatkörben történő alkalmazásával párosuló fellépések összességeként fogható fel.[103]

Ha ezt elvonatkoztatjuk a konkrét szereplők cselekvési sémáitól, akkor lényegében a biztonsági környezet hibriditásával is azonosítható az az újszerűség, hogy az infokommunikációs robbanás miatt az állami és a nem állami szereplők tervezési, szervezési és beavatkozási lehetőségei páratlan mértékű növekedésen estek át. Az persze, hogy a különféle hatalmi szereplők háborús fellépés keretein kívül, nem katonai eszközök felhasználásával avatkoztak be egyes államok és társadalmak működésébe akár későbbi katonai fellépésük előkészítése, akár a háborús szándéktól független érdekek érvényesítése érdekében, nem új a történelemben. Az sem újszerű, hogy a hatalmi szembenállás korábbi eszközrendszere és jellege jelentősen átalakult a technológiai fejlődés nyomán, hiszen a 20. századi totális háború – igaz a hadviselésen belül, de – hasonlóan korszakos változást hozott magával.

A 21. század biztonsági környezetében az az igazi újdonság, hogy a valóban globális kapitalista gazdasági rendszer és annak szürke és fekete tartománya, illetve a glóbusz egészét behálózó és az emberek korábban nem látott tömegeit elérő, valós idejű infokommunikáció révén olyan változások sora megy végbe a mindennapi életet érintően, amelyek miatt az állami és nem állami szereplők érdekérvényesítő lépéseibe alapvető érdek a beavatkozásokat a katonai konfrontáció szintje alatt tartani. Olyan célok és olyan mérvű beavatkozások valósulnak meg jelenleg is, amelyek korábban nagyrészt katonai erővel voltak elérhetők, de a szembenálló fél pozícióinak gyengítése, illetve a nemzetközi béke és biztonság rendszerének kikerülése érdekében alapvető cél, hogy ne nyílt katonai szembenállás útján történjen a hatalmi fellépés. Úgy is fogalmazhatnánk – korábbi kutatásainkra és a skandináv térség államainak kiújuló totális védelmi felfogására figyelemmel –, hogy a hibrid fenyegetések szisztematikus alkalma-

102 L. Leigher (2021), Bagge (2019)

103 Giannopoulos–Smith–Theocharidou (2021)

zása vált a fő fellépési iránnyá, ha úgy tetszik, totális biztonsági kihívási környezetet teremtve ezzel.[104] Ez persze – ahogy az orosz–ukrán háború is mutatja – nem zárja ki a nyílt katonai szembenállás lehetőségét, de azt is formálja működésében.

Ennek a hibrid fenyegetési mátrixnak és az ebben rejlő – feltehetően – történelmi léptékű újdonságnak a fő hozadéka a nem katonai, vagy a hagyományosan nem védelmi és biztonsági tényezők szerepének felértékelődése és védelmi-biztonsági rendszerbe kapcsolásának megkerülhetetlenségén túl az, hogy lényegében folyamatossá teszi az államok védelmi és biztonsági, illetve társadalmi és információközvetítő rendszereire is nehezedő nyomást. Ez a módszer ugyanis a társadalmi közegbe ágyazva tudja leginkább kifejteni hatását, méghozzá akkor, ha az egy szerves és hosszú idejű beágyazódás eredményeként jön létre. Ebből is következik, hogy a hibrid fenyegetések keretében használt eszközök és módszerek sok esetben magasan konspiráltak a valódi célokkal való összefüggés tekintetében, illetőleg az információs csatornák, gócpontok vagy véleményformáló entitások hitelességének kialakítása és megóvása érdekében.

Ez a fajta „köztünk élő" ellentevékenység pedig csak a különféle biztonsági események átfogó megközelítés mentén történő folyamatos elemzésével, illetve az érintett állami szervek és társadalmi szerveződések kooperációjával, valamint a biztonságtudatosság erősítésével azonosíthatók és mérsékelhetők. Ez a védelmi és a biztonsági rendszerek jelentős reformját és az állami-társadalmi ellenállóképesség fokozását teszi elsődleges feladattá a biztonság hatékony garantálása érdekében a hibriditás korában. Fontos azonban kiemelni, hogy a hibrid fenyegetések elleni fellépés vonatkozásában kiemelt figyelmet kell szentelni a tradicionális európai értékek megóvására és lehető legteljesebb fenntartására, hiszen az eltúlzott reakciók állami-társadalmi torzulást idézhetnek elő, ami nem kívánt módon épp az ellenérdekelt tevékenységek céljainak elérését segítheti elő. A megfelelő megoldás megtalálásában tehát az aktuális helyzetekre adott válaszok mellett kiemelt szerepe van az elemzésnek, az értékelésnek és mindezek mellett a tudományos vizsgálódásnak is, illetve a problémakör tudományterületeken átívelő megvitatásának. Egy rendszerszerű és jól strukturált, széles eszköztárra építő fenyegetéssel szemben ugyanis a gyors, pillanatnyi és adott jelenségekre korlátozódó válaszok csak szépségtapaszt, nem pedig megoldást jelentenek.

Természetesen a hibrid fenyegetések körében jól kiaknázható eszközrendszer és a komplex biztonság szinte minden szektorára kiterjedő fellépési lehetőség, ami a hibriditás újdonságát adja, a hibrid fenyegetések mellett a hibrid konfliktusok és a hibrid hadviselés terén is jelentős hatást fejt ki. Az a technológiai robbanás ugyanis, ami a társadalmi-gazdasági-politikai-biztonsági környezetet gyökeresen átalakította, jelentős fejlesztéseket indukált a védelmi és a biztonsági eszköz- és módszerrendszer tekintetében is. Ebből adódóan azonban az infokommunikációs forradalom előnyeinek kiaknázása a konfliktusok és a hadviselés tekintetében új, potenciális sérülékenységeket is magával hozott. Nem véletlen, hogy ezekben a vonatko-

104 A téma kapcsán l. Farkas Ádám (2018a), NATO SHAPE: Exercise Trident Juncture 18: Total Defence Concept, shape.nato.int/news–archive/2018/exercise–trident–juncture–18–total–defence–concept, Bérzina (2019): 71–89., Wither (2020): 61–81., Swedish Defence Commission Secretariat: *Resilience. The Total Defence Concept and the Development of Civil Defence 2021–2025.* government.se/4afeb9/globalassets/government/dokument/forsvarsdepartementet/resilience-report-summary---20171220ny.pdf, *Support and Cooperation. A Description of the Total Defence in Norway.* Oslo, Norwegian Ministry of Defence – Norwegian Ministry of Justice and Public Security, 2018. regjeringen.no/contentassets/5a9bd774183b4d548e33da101e7f7d43/support-and-cooperation.pdf

zásokban a „warfare" kifejezés divatos használatán túl lényegében valóban új fegyvernemek jelentek meg a technológiai újításokkal.

A kiber hadviselés, illetve a kibertér műveleti területté nyilvánítása ennek a fejlődési folyamatnak a legkézenfekvőbb példája, hiszen a digitalizáció a hagyományos kommunikációs csatornákon messze túllépve a harceszközök és a harci járművek működését és irányítását is áthatja, amelyek korrumpálása vagy bénítása ezáltal a szemben álló fél kiemelt céljaként jelenik meg. Hasonlóan fontos a kiber domain lehetőségeinek kiaknázása a hibrid konfliktusok átmeneti vagy ingoványos terepén is, hiszen az egyszerre mozdíthatja elő a nem katonai eszközökkel elérendő stratégiai célok teljesülését, illetve készítheti elő a katonai beavatkozást. Érdemes tehát ennek a vonatkozásnak a további elemeit mélyebben is kielemezni, és mind a hibrid fenyegetések, mind a hibrid konfliktusok, mind pedig a hibrid hadviselés újdonságai kapcsán belátni azt, hogy minden egyes új jelenség végül visszatükröződik a digitális térben, méghozzá azzal a céllal, hogy információs úton befolyásolja a feleket.

Erre kézenfekvő példa az elmúlt időszakból az az internetes információs hullám, ami mind az örmény–azeri, mind pedig az orosz–ukrán harccselekmények tekintetében szabályos kampányként zajlott le a dróntechnológia hagyományos páncélos hadviseléssel szembeni sikerei kapcsán. Ez ugyanis az adott konfliktusok tekintetében demoralizációs hatást célzó információs művelet, a konkrét konfliktusok keretein kívül pedig a technológiai fejlődés hadviselésre gyakorolt hatásaival kapcsolatos információs csomag, ami már a világ minden táján relevanciával bírhat a konkrét fegyveres cselekményekhez való érzelmi és tudati kapcsolódás nélkül is. Érdemes azonban ezt a fajta, információs térben való megjelenést konkrét példákon keresztül is továbbgondolni.

2.4. A dezinformáció a hibriditás kiemelt kibertéri eszköze

Ezen alfejezet célja, hogy felvillantsa, hogy a hibriditás eszközparkjának egy szelete, nevesítve az információs műveletek részét képező dezinformáció milyen módon használja ki a kibertér, azon belül is a közösségi média és annak alapját jelentő, a nyugati jogállami gondolkodás alapjaként funkcionáló véleményszabadság adta lehetőségeket, és ez végső soron mennyire érinti a nemzeti biztonságot.

A közösségi média felhasználása kézenfekvő abban az értelemben, hogy megfelelő közeget jelent a politikai célok katonai jellegű megvalósításához. Makhmut Gareev, az Orosz Hadtudományi Akadémia volt vezetője szerint ugyanis a hibriditás nagy előnye, hogy az információs hadviselési eszközök korai alkalmazása révén a politikai célok katonai erő alkalmazása nélkül is elérhetővé válnak, mégpedig úgy, hogy az információs és egyéb felforgató akciókkal ellenőrzött káoszt teremtenek.[105] Ennek során legszélsőségesebb esetben különféle zavargásokat idéznek elő, hogy belülről döntsék meg a nemkívánatos hatalmi struktúrát, és megzavarják az állam belső stabilitását. Kisebb volumenű szcenáriók pedig elégségesek ahhoz, hogy átmeneti, az állam működését zavaró, a politikai gépezet figyelmét elvonó eseménysort valósítsanak meg. Gerasimov ezt a hírhedt cikkében annyiban pontosította, hogy ez elsősorban gazdasági és katonai potenciál aláásását jelenti, információs és pszichológiai befolyásolással, akár a belső ellenzék aktív támogatásával. Ezzel a cél az állam önszerveződő képességének

105 L. Kelemen (2021b): 177–186., Pongrácz (2019b): 19–28., Nagy Szabolcs (2017): 183–198.

lerombolása.[106] Ennek során a hibriditás cél- és eszközparkja eljutott odáig, hogy a támadással érintett ország döntéshozatali mechanizmusainak, döntéshozatalának a befolyásolása a kívánt eredmény, vagyis ebből adódóan nem szükségszerűen cél az ellenőrzött káosz megteremtése, hanem sokkal inkább stratégiai kényszerítés valósul meg. Ezen esetkörökben nem feltétlenül akarják, vagy reálisan felmérve tudják a folyamatokat magasabb eszkalációs fokra juttatni a támadó felek. A stratégiai cél, amit el kívánnak érni, ebben az esetben gazdasági, politikai döntéshozatal eltérítése, a választási eredmények befolyásolása, amelyekhez kitűnő terepnek tekinthető a kibertér. [107]

Ezekből következik, hogy a dezinformáció lényegében irányulhat gazdasági ágazat, szereplő vagy termék ellen, amely nemzeti biztonsági jelentőséggel bír, valamint a politikai szereplők akaratának, meggyőződésének alakítására, aminek leghatékonyabb módja a társadalmi feszültségek eszkalálása, továbbá választási eredmények befolyásolására.

A közösség média pedig megfelelő közeget jelent az ilyen típusú információs műveletek számára, mivel egyik oldalról teljesen behálózza az emberek hétköznapjait, átalakította a kapcsolatteremtést, a kommunikációt, az egyének információhoz jutását, másik oldalról a felhasználói adatok integritása jelentős problémát jelent, emellett az információhoz jutás befolyásolhatósága, az információ valós tartalma, és a fiatalkorú felhasználókat ért abúzus hatások is kérdéseket vetnek fel.[108]

Ezek már önmagukban társadalmi feszültséget generálnak, de ebben a közegben – ahogy a kibertér egészében – a hagyományos tér töréspontjai is megjelennek, és ezek sok esetben nemzetbiztonsági kockázatokat rejthetnek magukban. Az államok nyilvánvalóan felismerték ezt és kihasználják érdekeik érvényesítésére,[109] másik oldalról pedig próbálnak ellene védekezési mechanizmusokat[110] kialakítani.

A kibertéri dezinformálás első megnyilvánulásai azok voltak, amikor a terrorista csoportok kiberképességeket használtak támadási lehetőségeik bővítése, hatékonyságuk növelése érdekében. A Hamasz a 2010-es évek elején dezinformációs, és a tömeghangulatot befolyásoló eszközöket alkalmazott izraeli és nem izraeli e-mail-címekre és telefonokra küldött álhíreket tartalmazó e-mailekkel és szöveges üzenetekkel, valamint propagandatartalmakkal. Az Iszlám Állam fokozta ezt a tevékenységet; kifinomult és meglehetősen agresszív marketingkampányt folytatott, és magas szintre fejlesztette a kibertérben megjelenő pszichológiai hadviselést. Pakisztáni terroristák 2008-ban pedig arra is rávilágítottak, hogy valós idejű infor-

106 Pyhnöniemi (2021): 4–5.

107 Rosenstedt (2021): 5.

108 A probléma akut, hiszen óriási lelki terhet jelent a gyermekek számára, hogy az online térben, annak eszközei és sajátos jellemzőinek köszönhetően jelentősen felerősödött a korábbi hagyományos térben ismert abúzus hatása. Nem véletlen, hogy Magyarország is saját digitális gyermekvédelmi stratégiával rendelkezik. L. bővebben: Aiken (2020), Sorbán (2020): 81–104., Kiss–Pari–Prazsák (2019), Mezei (2021): 19–30., Magyarország Digitális Gyermekvédelmi Stratégiája, digitalisjoletprogram.hu/files/b9/55/b955b52770e659680b4e537e84df906b.pdf, Kovács-Szépvölgyi (2022a): 227–236.

109 Bányász (2017a): 108–121.

110 Például Kína a társadalmi pontrendszerrel, illetve az Aranypajzs, vagyis a kínai nagy tűzfal révén kívánja megvalósítani, de ebbe a körbe sorolható Szingapúr okosváros projektjeibe burkolt megfigyelési rendszere, az iráni „halal" internet projekt, az orosz internet kialakítása is. Ezeket l. Gosztonyi (2021a): 87–99., Mosco (2019)

mációgyűjtésre és koordinálásra is alkalmas a közösségi média figyelése és az okostelefonon történő kommunikáció.[111]

A fenti történésekkel párhuzamosan az állami szereplők felismerték az ilyen akciókban rejlő potenciált.

> „ahol az információs tér a hír- és véleménycsere piaca gyanánt minden felhasználó előtt nyitva áll, az állam pedig alig cenzúrázza azt, bárki terjeszthet szándékosan és stratégiai céllal kifinomult üzeneteket, és folytathat felforgató tevékenységet, hogy az ellenfelet lélektanilag befolyásolja és egy bizonyos magatartásra késztesse."[112]

Tehát a jogállamok, amelyek biztosítják a közösségimédia-platformokon is a lehető legteljesebb körben a véleménynyilvánítás szabadságát, önmaguk egyik legalapvetőbb krédója által válhatnak támadhatóvá, hiszen eltérően a korábbi koroktól, a tömegek félretájékoztatásához már nincs szükség repülőgépre, hogy az ellenség vonalai mögé röpiratokat, megtévesztő tartalmú újsághíreket juttathassanak, ugyanis az átpolitizált közösségi felületeken a támadó által kiválasztott, célhoz illeszkedő csoport tagjaihoz eljuttatott információk, hírmorzsák és a *fake news* kiváltják a kívánt hatást.

Ezt segíti az azonnali visszacsatolás lehetősége, vagyis aki ismeri a támadás narratíváját, az látja, mégpedig valós időben, hogy az aktivált információk elérték-e a kívánt hatást. Így lehetősége nyílik arra, hogy nyomban módosítsa a stratégiát, illetve a következő, már jól előkészített tartalmat is elérhetővé tegye. A kiválasztott csoport vagy csoportok tagjai pedig az online platformok sajátosságai okán individualizált hírcsokrokhoz jutnak, vagyis javarészt az érdeklődési körükhöz kötődő információk jelennek meg a felületeiken, így az adott felhasználók jószerével folyamatosan az előre jól lehatárolt támadási célokat szolgáló híranyaghoz jutnak hozzá. Ezen hírek egyre szélsőségesebb állításokat fogalmaznak meg.

> „[A] lényeg, hogy ellehetetlenítsék a tényeket, a nyilvános diskurzusba vetett bizalmat, a politikai helyzet szabad és észszerű értékelését, valamint a konszenzusteremtést. Ezek helyére lépnek az alternatív tények, az érzelmi befolyásolás és a provokáció, hogy kételyt, bizalmatlanságot szítsanak, és megosszák a társadalmat."[113]

A következőkben egy-egy ilyen szcenáró és a hozzá fűződő közösségi média gyakorlat bemutatásával illusztrálom ezeknek a kampányoknak a hatékonyságát és a benne rejlő potenciált.

Az egyik ilyen mintaeseménynek tekinthető a franciaországi sárgamellényes tüntetésekkel kapcsolatos orosz fellépés. Már a mozgalom megszületésében és növekedésében is jelentős szerepe volt annak a Facebook-csoportnak, amit a magas üzemanyagárak és a rendkívül megemelkedett megélhetési költségek indikáltak. Problémát okozott az is, hogy a hagyományos média kezdetben alig vette észre a szerveződést, mivel az egyes tagok a Facebook-csoporton belüli hírekre, üzenetekre, videókra támaszkodtak, az újságírók viszont inkább a Twitterre, ezért meglepte őket a helyzet súlyossága.[114] A többek között a politikai dezinformáció ellen

111 Bachmann–Gunneriusson (2015): 82–83.
112 Hofstetter (2020): 93.
113 Uo., 85.
114 Makela (2019): 10–13.

is küzdő civil szervezet, az Avaaz[115] az eseményekkel kapcsolatban 2018 novembere és 2019 márciusa közötti időszakban a Facebookon megjelent száz legnézettebb álhírt vizsgálta meg, ezek a politikai rendszerellenességgel (28%), a rendőrségi brutalitással (27%), a mozgalom nem valós, koholt támogatottságával (19%), az állami cenzúrával (14%), az ellenőrizhetetlen bevándorlással, a rasszizmussal és az idegengyűlölettel (10%), valamint egyéb, nem kategorizált kérdésekkel (2%) foglalkoztak.[116]

Oroszország aktívan közreműködött a hamis hírek terjesztésében, így német, spanyol, holland, lengyel, svéd és olasz nyelven adta közre ezeket a hírcsomagokat. Az RT orosz állami hírcsatorna néhány riportere részt vett a tüntetéseken, és úgy ábrázolta a helyzetet, mintha Párizs háborús övezet volna. A dezinformációs kampányból nem maradhatott ki a hagyományos média munkatársainak lejáratása sem, őket korruptnak, megbízhatatlannak, a kormánnyal mindenben összejátszónak mutatták be.[117] Megdöbbentő módon a vizsgált száz valótlan hírt több mint négymillióan osztották meg, és ezeket több mint százötmillió ember tekintette meg. A teljes képhez hozzátartozik, hogy az öt legnagyobb francia hírszolgáltató (köztük a *Monde*, a *Figaro*, vagy a France24) Youtube csatornája összesen kicsit több mint 24 millió embert ért el a vizsgált eseményhez kapcsolódó tartalmaikkal, míg a dezinformációs kampány központi orgánuma, az RT France, több mint 30 milliós forgalmat generált ebben az időszakban. [118]

Ezen adatok önmagukban alátámasztanák egy-egy ilyen hibrid dezinformációs kampány hatásosságát, azonban, ha még hozzáveszük az egyes tartalmak terjedési sebességét és az azokra adott szolgáltatói reakciót, akkor még élesebben kirajzolódik a probléma nagysága. Az egyik megosztott tartalom vérző fejű civileket ábrázol, akik a poszt állítása szerint a rendőri brutalitás áldozataivá váltak. Ezt a posztot 2018. november 20-án tették közzé, rövid idő alatt 136 ezren osztották meg, és több mint 3,5 millióan nézték meg. Valójában kiderült, hogy a képek több országban és teljesen más időpontokban készültek (például Spanyolországban 2012-ben és 2017-ben), az összeállítás célja pedig a fellépő rendőri brutalitás ábrázolása és a tüntetők, továbbá a francia és a szolidaritást érző más államok társadalmainak radikalizálása volt.

A Facebook azonban nem távolította el a bejegyzést, érdemben pedig csak 2019 márciusában jelezte egyes mainstream orgánumok cikkeivel – ami a megtévesztettek számára nyilván nem hiteles orgánumok – a tartalmak valótlanságát és az állítások célját. Az ilyen dezinformációs kampányok határokat átívelő jellegét igazolja, hogy e szcenárió részeként már Hollandiában is elterjedt a nézet, hogy a rendőrök – hasonlóan a francia kollégáikhoz – mindenkivel szemben erőszakot alkalmaznak, akik szolidaritást vállaltak a sárgamellényes tüntetőkkel. Ezt fokozó *fake news* volt az a hír, amelyik egy, amúgy jogellenes magatartás megvalósító – a videón gyermekét babakocsiban toló – nővel szembeni rendőri fellépést ábrázolt. A videó szerint a rendőrök minden különösebb indok nélkül alkalmaztak kényszerítő eszközöket a nővel szemben, csak azért, mert a tüntetés jelképét jelentő sárga mellényben volt. Az eredeti videónak a tüntetőkhöz semmi köze nem volt, sőt a babakocsiban is, mint később kiderült, egy műbaba volt. Azonban a platform lassú szűrési és címkézési gyakorlata okán a videót

115 secure.avaaz.org/page/en

116 Yellow Vests Flooded by Fake News: Over 100M Views of Disinformation on Facebook. *Avaaz Report* 15/03/2019 (továbbiakban: Yellow Vests) avaazimages.avaaz.org/Report%20Yellow%20Vests%20FINAL.pdf, politico.eu/wp-content/uploads/2019/03/AVAAZ_YellowVests_100miofake.pdf, 5–6.

117 Makela (2019): 10–13.

118 Yellow Vests: 21.

gyorsan lefordították francia, angol és olasz nyelvre, és csak az angol verziót 31 ezer ember osztotta meg, és 1,3 millió nézte meg.[119]

Az elmúlt évek gyakorlata tehát azt mutatja, hogy a közösségimédia-platformok nem tudtak hatékonyan fellépni az olyan valótlan tartalmakkal szemben, amelyek társadalmi kockázata jelentős mértékű volt. A Google, az Amazon, a Facebook és az Apple ellenőrzik a közösségi felületeket, így a politikai információkat is, a napi hírek kapuőrei, ami által ők irányítják a közbeszédet, ők döntenek a tartalmakról, vagyis arról, hogy mi kerülhet nyilvánosságra. „A szűrőbuborék-elmélet szerint az internetes kapuőrök a társadalmi kohézió gyengülését idézik elő azzal, hogy felhasználóiknak tetsző, az ő egyetértésükkel találkozó tartalmakat teszik leginkább láthatóvá."[120] Tehát a már amúgy is sajátos gondolkodás, elméletek, érdeklődés mentén polarizálódott közösségeket tovább erősíti a közösségimédia-platform által összeállított hírfolyam, amellyel lényegében ezek a platformok már külső állam dezinformációs tevékenysége nélkül is manipulálják az embereket. Jelentős probléma tehát, hogy a közzétett tartalmakat, véleményeket a szolgáltató saját érdeke, világnézete mentén szelektálja, így a magáncenzúrán[121] túl ezzel képes a „társadalmi közvitát torzítani, tematizálni, akár politikai, akár gazdasági vagy más érdekből."[122]

Egy másik érdekes esetkör a választásokkal kapcsolatos befolyásolási tevékenység. Ennek egyik leghíresebb és legnagyobb visszahangot kiváltott eseménye volt a 2016-os amerikai elnökválasztás. Ekkor az orosz beavatkozás lényeges eleme az volt, hogy a választások előtt a közösségimédia-platformokon keresztül megfelelő hírcsomagokhoz juttassák a kiválasztott társadalmi csoportokat, ezzel megpróbálva befolyásolni a választások lehetséges kimenetelét.[123]

Ez viszont számos üzentet hordozott a választások biztonságával kapcsolatban. Egy 2018-as amerikai szakértői jelentés rámutat arra, hogy az európai államokkal kapcsolatos választási dezinformációkból levonható számos lehetséges intézkedési kör a választások biztonsága érdekében. Így többek között a választási rendszereket a kritikus infrastruktúra részének kell nyilvánítani, javítani kell az ellenálló képességet és ennek során rendszeres sebezhetőségi vizsgálatokat kell végezni, ennek része a jogi sérülékenység feltérképezése és a lehetséges jogi szabályozás kialakítása, a választópolgárok felkészítése a lehetséges dezinformációs kampányokra, a közösségi média szolgálatók bevonása a lehetséges hatások enyhítése érdekében. Utóbbi azért is kiemelten fontos, mert a kiemelkedő célpontok között azonosították, az elektronikus választási infrastruktúra mellett. [124]

Ennek ellenére 2019-ben – ahogy International Institute for Democracy and Electoral Assistance jelentése rámutatott – kevés olyan állam volt, amely ilyen irányú jogi szabályozással rendelkezett volna, mivel a vita még mindig ott tartott a dezinformáció kivédésével kapcsolatban, hogy az szabályozás vagy önszabályozás szintjén valósuljon meg. Ezt igazolja például a 2018-as lett választások során tapasztalt esemény is, amikor orosz hackerek a legnépszerűbb lett közösségi hálózatot, a Draugiem-et törték fel, és célzott oroszbarát, a lakosság megfélemlítésére irányuló közleményt tettek közzé. Mivel azonban ez a közösségi oldal magántulajdonban volt, így az állami szervek részéről, a jogi keretek okán, nem volt szükséges

119 Uo., 7–20.
120 Koltay (2019): 4.
121 L. ennek problémáját bővebben: Koltay (2017): 129–140., Koltay (2018): 267–292.
122 Klein (2018): 235.
123 Rosenstedt (2021): 5.
124 Brattberg–Maurer (2018): 27–34.

válaszreakciót adni. A dezinformációs munkacsoport azonban lépéseket tett annak érdekében, hogy ez ne befolyásolja választásokat.[125]

A Helsinkiben működő Hibrid Kiválósági Központ a választások zavartalansága érdekében 2020-ban ajánlásokat fogalmazott meg. Ebben három periódusra osztották fel a választások előtti időszakot: egy éven túli, egy éven belüli és hat hónapon belüli időszakokra. Az egy éven túli periódusban a dezinformációval kapcsolatban azt fogalmazták meg szükségesnek, hogy az egyes államok mérjék fel a normál működést, vagyis a hétköznapokon milyen volumenűek az ilyen típusú műveletek, ezzel meg tudják határozni az alapszintet, amely segít abban, hogy mikor kell a platformszolgálatóhoz fordulni. De ilyen elvárásként fogalmazták meg a nyílt forráskodú alapú hírszerző képesség kialakítását, amely csökkenti a kormányzati függőséget a szolgáltatóktól. Dezinformáció szempontjából az utolsó hat hónap a releváns még, mivel itt fel kell térképezni a választópolgárokat megosztó témákat, és figyelni az ezekre irányuló célzott akciókat. Ezekkel kapcsolatban pedig a politikai döntéshozókat, újságírókat és jelölteket tájékoztatni kell, valamint felhívni a figyelmüket az eszkaláció lehetőségére.[126] Ezen ajánlásnak is központi eleme, hogy az egyes állami szervek megfelelően együtt tudjanak működni a platformszolgáltatókkal.

A tapasztalatok azonban sajnálatos módon azt mutatják, hogy ezen a területen nem történt előrelépés. Az Avaaz csapatának jelentése pontosan erre mutat rá. A 2019-es évben 158 millió megtekintést értek el az Avaaz által megfigyelt, a közelgő amerikai elnökválasztást érintő politikai tartalmú valótlan közlemények. Ez a szám önmagában is horribilis, de ha hozzátesszük, hogy a 2018-as félidős választásokra 153 millió választó regisztrált, akkor egyenesen arra a következtetésre kell jutni, hogy minden egyes választót legalább egy valótlan hír elért. A szám nagyságát érzékelteti még, hogy 2019-ben a két nagy párt Facebook-oldalát mindösszesen közel 60 millióan tekintették meg.[127] Egy másik Avaaz-jelentés, amely a 2020-as amerikai elnökválasztás után készült, rávilágít arra, hogy valós változás nem történt az évek során. Ennek első fejezete azt az egyértelműnek ható alcímet kapta, hogy „Miként hagyta cserben a Facebook az amerikai választókat". A választások után Sheryl Sandberg, a Meta ügyvezető igazgatója, azt mondta, hogy a Facebook óriási erőfeszítéseket tett a dezinformáció ellen, mégpedig sikerrel. Eredményként azonosíthatták, hogy – véleményük szerint – nem volt orosz beavatkozás ebben az időszakban a platform határozott fellépése miatt. Az Avaaz azonban kimutatta, hogy a vizsgált száz legnézettebb *fake* poszt így is 162 milliós nézettséget ért el, emellett hangsúlyozta, hogy ez a száz poszt nem az összes közül a száz, hanem a Facebook tényellenőrei által azonosított *fake news* közül a száz legnézettebb. A jelentés rátért arra is, hogy amíg a platformok kizárólag önértékelést végeznek, továbbá a kutatók és a hatóságok számára csak azok az információk lesznek elérhetők, amiket kiadnak, addig a dezinformáció valós mértékéről még becsléseket is nehéz adni.[128]

Európa esetében ez még fokozottabb veszélyt jelent, amelyet a Covid19 által okozott pandémia időszakának gyakorlata is jól visszaigazolt, ugyanis a közösségimédia-platformo-

125 van der Staak–Wolf (2019): 20.

126 Rosenstedt (2021): 7–9.

127 US 2020: Another Facebook Disinformation Election? US Flooded with Over 158M Views of Political Fake News ahead of the 2020 Elections. *Avaaz Report* 5/11/2019 4–6. secure.avaaz.org/campaign/en/disinfo_report_us_2020.

128 Facebook from Election to Insurrection: How Facebook Failed Voters and Nearly Set Democracy Aflame, *Avaaz Report* 18/3/2021. secure.avaaz.org/campaign/en/facebook_election_insurrection

kon egy világméretű, ún. infodémiát generáltak.[129] A fogalmat a WHO vezette be, és a következőképpen határozta meg:

> „[az] infodémia egy problémával kapcsolatos túlzott információáradat, amely megnehezíti a megoldás azonosítását. Magában foglalja az egészségügyi szükséghelyzet során terjedő félretájékoztatást, a dezinformációt és a pletykákat. Az infodémia hátráltathatja a hatékony népegészségügyi válaszintézkedéseket, továbbá zavart és bizonytalanságot kelthet az emberek körében."

Az infodémia kezelése azonban teljesen eltérő volt az Egyesült Államokban és az Európai Unióban.[130]

A Facebook félretájékoztatás elleni kampányának az a megközelítése, hogy Amerika az első, az következik, hogy a hatékonysága ott a legjelentősebb, ami – mint fentebb láttuk – ott is erősen szubjektív és relatív. Ehhez képest a tényellenőrök a főbb európai, nem angol nyelvű *fake* tartalmak 56%-ára nem reagálnak, ami angol nyelvű *fake* tartalmak esetében csak 26%-os eredménytelenséget mutat. Ez az olasz nyelv esetében 69%, míg a spanyolnál csupán 33%, ami mellett el tudjuk képzelni, hogy a kisebb, közép- és kelet-európai nyelvek, mint a magyar, a szlovák, a cseh vagy a horvát stb. esetében milyen hatékonysággal dolgozik a rendszer. Emellett a „*fake*" címke elhelyezése is jóval lassabban történik meg. Az amúgy sem gyors, az angol nyelvű tartalmak esetében tapasztalható 24 nap alatti „*fake*" címke kihelyezés, a nem angol nyelvű nagyobb európai nyelvek esetében csak 30 nap alatt történik meg. Ez az arány 2021-re kissé javult (55%-ra az első kategória, a címkézés pedig 28 napra), azonban a platform továbbra sem ismeri fel a klónozott tartalmat vagy a hamis állításokból készített egyes variánsokat, amelynek egyes változatait korábban már hamisként jelöltek meg.

A megfigyelt *fake news* esetében 51 eltérő változat 800 ezer interakciót ért el, és ezek 63%-áról hiányzott a Facebook figyelmeztető felirata. Az elkészített jelentés a fentiek mellett hangsúlyozta, hogy a Facebook a vizsgált egy évben nem tartotta be az ígéretét, hogy a lehető legteljesebb mértékben azonosítja a pandémiához köthető hamis híreket, és fellép e tartalmak ellen, így az önszabályozás nem járható út. Megerősítette a 2020-as amerikai elnökválasztások kapcsán már feltártakat: a platformszolgáltatók nem működnek együtt sem az államokkal, sem a kutatókkal, nem teszik átláthatóvá a szűrési rendszereiket, nem adnak megfelelő képet a dezinformációellenes gyakorlatukról.[131] Ennek pedig egyértelmű következménye, hogy a közösségimédia-platformokon az információs műveleteket végző államok és nem állami szereplők továbbra is sikeresen tevékenykedhetnek céljaik elérése érdekében, tovább szaporítva az e terület másik arcát jelentő biztonsági kockázatok garmadáját.

A hibriditás mint korunk biztonsági környezetének szövevényes és szerteágazó jellemzője egyértelműen rávilágít arra, hogy a hatalmi-katonai alapgondolkodású geopolitikai viszony-

129 L. WHO: *Coronavirus disease 2019 (COVID-19). Situation Report.* 45. who.int/docs/default-source/coronaviruse/situation-reports/20200305-sitrep-45-covid-19.pdf

130 Egy másik vizsgálat hasonló képet mutatott Dél-Amerika és kifejezetten Brazília esetében, azonban nincs képünk Afrikáról és Ázsiáról. L. Is Fake News Making Us Sick? How Misinformation may be Reducing Vaccination Rates in Brazil. *Avaaz Report*. avaazimages.avaaz.org/Avaaz%20-%20Is%20Fake%20News%20Making%20Us%20Sick%3F.pdf

131 Left Behind: How Facebook is Neglecting Europe's Infodemic. *Avaaz Report* 20/4/2021. secure.avaaz.org/campaign/en/facebook_neglect_europe_infodemic

rendszerekben is rendkívüli mértékben felértékelődik a nem katonai tényezők szerepe, ezeken belül pedig a digitális tér és különösen a közösségimédia-platformok, valamint más, tömeges információközvetítést lehetővé tevő csatornák jelentősége. Ez a hatás- és arányváltozás mind a hibrid hadviselés dominánsan katonai, mind a hibrid konfliktusok részint katonai, mind pedig a hibrid fenyegetések döntően nem katonai érvényesülési tartományában jelen van, és komoly hatást gyakorol. Ebből adódóan a jelenséghez az államok és társadalmak rendszereinek alkalmazkodnia kell, ha saját érdekeiket és stabilitásukat megfelelő szinten kívánják tartani. Ennek az alkalmazkodásnak pedig a hosszú történelmi fejlődésből következő értékek megóvásával együtt, de a kártékony cselekmények hatékony mérséklését szolgáló módon kell megvalósulnia, amihez a hibriditás elemzése és megértése mellett az új platformok és lehetőségek elemzése is kulcskérdés.

II. rész

Társadalom és állam kibertérben – A Cyberfare state koncepciója

1. A kibertér egyénre gyakorolt hatása

A kibertér és a digitális technológia egyéni életvitelünkre, kibontakozásunkra egyértelműen jelentős hatással van. Elég csak végig gondolnunk, hogy melyek életünk azon területei, amelyekben nincs jelen, vagy amelyekre nincs jelentős hatással ez a közeg. Bizony, ma már nem azt kell mérlegelni, hogy mekkora halmazra van hatással a digitalizáció, hanem azt, hogy mekkorára nincs, mivel európai viszonylatban okkal feltételezhető, hogy lényegesen kisebb és jobban beazonosítható az a kör, amelyet nem érint a digitális tér. Az információink jelentős részének a megszerzése, kommunikációnk zöme, ügyeink intézése, akár a magánszféra ügyletei, akár a hivatali ügyek tekintetében, a tanulási folyamatok és gyermekeink oktatási eredményeinek figyelemmel kísérése, a munkavégzés, a kikapcsolódás mind-mind olyan területek, amelyekre a digitális tér jelentős hatással van, illetve amelyeket az emberek egyre szélesebb körénél meghatároz a digitalizáció.

A digitális eszközök életvitelünkre gyakorolt rendkívüli hatása ma már nehezen megkérdőjelezhető. Elégséges csak az okos telefon–okos karkötő/óra–okos otthon témaköröktől elindulva gondolkodni. Ezek mindegyikének megvannak a maguk előnyei mellett a maguk hátrányai és biztonsági kockázatai is. Természetesen a digitalizáció ilyetén fokozódása az élet felgyorsulásával, az információk terjedésének mind fokozódóbb dinamikájával szorosan összefüggenek, és szükségképpen formálják egyéni életvitelünket, életszervezésünket, személyes kapcsolatainkat, átfogóan mondva a viselkedésünket. Ez a jelenség nem jó vagy rossz önmagában, ez az emberiség egy fejlődési stációjának következménye. Az emberiség esett már át hasonló, csak más intenzitású és tömegességű információs robbanásokon, elég, ha csak a könyvnyomtatás hatásaira, vagy a rádió és a televízió elterjedésére gondolunk, nem elfeledve azt sem, hogy minden áldásuk és pozitív hozadékuk mellett mindegyiknek rendkívül sokrétű, és sok tekintetben kártékony kiaknázási lehetősége is megmutatkozott az elmúlt évszázadok során.[132]

Az emberiségnek mind egyéni, mind társadalmi szinten fel kell nőnie ehhez a mostani információs robbanáshoz, aminek folyamatát jól tükrözi, hogy egyszerre célunk és igényünk a digitalizáció fokozása, hiszen hatékonyabbá tehet számos folyamatot és ezzel javíthat az életminőségen, de közben egyre jobban látjuk, hogy vannak ennek a jelenségnek kezelést igénylő árnyoldalai is. A digitális addikció – digitális detoxikáció gondolata, a digitális tér személyiségtorzító hatásai,[133] a koncentráció és a különféle információs eszközök viszonyának problémái, vagy épp a tartalomszolgálatások bizonyos (például gyermekvédelmi) – szem-

132 A téma katonai vonatkozásairól példaként l. Mercier (2005): 649–659., Gagliarducci et al. (2017), Russel (2019), Puddephatt (2006)

133 A téma kapcsán l. Aiken (2020), Kiss–Parti–Prazsák (2019), Connolly et al. (2016), Price (2018)

pontok szerinti korlátozása mind-mind olyan visszatükröződések, amelyek az arany középút, az egyensúlyi helyzet megtalálása felé vezető utat kövezik. Ezeknek azonban biztonsági relevanciája is van, hiszen visszás hatásaik túlzott mértékű megnyilvánulása az egyén fizikai és mentális egészségére, ezáltal pedig a közösségekre is visszahathat, nem beszélve azokról a szélsőséges esetekről, ahol a torzulás valamely ártó magatartásban ölt testet akár a kibertérben, akár a fizikai térben elkövetett cselekményekkel.

E tekintetben a kibertér egyéni vonatkozásai kapcsán kiemelt szerepe lehet a pszichológiai megközelítésnek és annak a szemléletnek is, amely az evolúciós pszichológiában testet ölt. Ennek alapvetése ugyanis, hogy az ember alapvető pszichés működését az evolúció lassú folyamata alakította, ám az elmúlt másfél-két évszázad rendkívül dinamikus életviteli változásaihoz az emberi agy ilyen jellegű „előre huzalozottsága" nehezebben tud alkalmazkodni, mint az evolúciós folyamatokra jellemző, elhúzódó változásokra.[134] Ennek jelentősége kettős, hiszen egyik oldalról sérülékenységet eredményezhet az egyén szintjén a nem megfelelő reagálástól az addikcióig, másik oldalról pedig nyilván befolyásolási lehetőséget teremt azon szereplők számára, akik megfelelő erőforrások birtokában pontosan az evolúciós folyamathoz képest rendkívül gyors változással járó bizonytalanságokat akarják kiaknázni akár anyagi haszonszerzés, akár más céltól vezérelve. A kibertér hatásai, biztonsági hatásai terén eleve látni kell azt is, hogy az evolúciós folyamat során lassan kialakult, az állatvilágig visszanyúló, majd a fejlődő emberi kultúrában szocializációs keretek közé szorított, részint pacifikált, de mégis előre huzalozott, „kódolt" reakciók virtuális térben való működése még egy feltárás, tapasztalás alatt álló terület. Egyértelműen látható, hogy az agresszió különféle formái, az evolúciós folyamatokra jellemző „automatizált" pozícióharc és versengés, de végső soron az alkalmazkodás emberi kódja is sajátosan jelentkezik ebben a közegben, aminek a folyamatait majd épp úgy ki kell ismerni, ahogy a hagyományos emberi viselkedés folyamatainak kiismerésére törekszünk. A kibertér biztonságát ugyanis a felhasználó ember pszichés alapprogramja is rendkívüli mértékben meghatározza. Mára már közhelyszerű gondolat ugyanis, hogy az információs rendszer legnagyobb sérülékenységét az ember jelenti mind tervezői, mind szervezői-üzemeltetői, mind pedig felhasználói szerepkörben.

Ezzel összefüggő az a tényszerűség is, hogy a digitalizáció számos jelenséget felgyorsít, ezáltal pedig a döntési folyamatok gyorsítását, sok esetben egyszerűsítését vagy felszínessé válását is magával hozhatja. E tekintetben gondoljunk csak az egyes internetes oldalak adatkezelési protokolljainak elfogadására, illetve a különféle alkalmazások, értesítések kezelésére a felhasználók körében. A kívánt előny kihasználása – vagyis az adott oldal megtekintése vagy az alkalmazás használata érdekében – sok esetben rutinszerűen adjuk hozzájárulásunkat az adataink kezeléséhez. Ez a fajta felgyorsulás egyik oldalról biztonsági kérdés, másik oldalról pedig egy a kibertérrel járó jelenséghalmaz egy szelete. Biztonsági kérdés, mivel a felhasználók által biztosított adatok elemzésére, kereskedelmére egész iparág épül, ami bizony nem csak a felhasználói élmény javítását szolgálja,[135] hanem fogyasztási spirálok kialakítását épp úgy, mint adott esetben választási eredmények befolyásolását, vagy geopolitikai célokat.[136] Az

134 A téma kapcsán bővebben l. Bereczkei–Plég–Csányi (2001), Bereczkei (2008), Gyuris–Meskó–Tisljár (2014)

135 A téma kapcsán l. Fuchs (2019): 43–51., Ramge–Mayer-Schönberger (2018), Segura–Waisbord (2018): 412–419.

136 L. bővebben: Geopolitics of the Datasphere – GEODE geode.science/en/home/, Cattaruzza (2020), O'Hara–Hall (2018), Farkas Ádám (2021a)

adatoknak egyértelműen geopolitikája van ma már, és ez a jelenség nagyban épül az egyéni felhasználói magatartásmintákra, adatmegosztásokra vagy a döntéshozók egyéni tudatosságára és biztonságpercepciójára. Nem lehet ugyanis elfelejteni, hogy mind az állami fellépés, mind a különféle cégek működése végső soron egyéni gondolatok, attitűdök, cselekvések valamiképp szervezett halmazaiból állnak, amelyben azonban a legjelentősebb lépéseknél meghatározott személyek egyéni viszonyulásai igenis kimagasló jelentőséggel bírnak az innováció egyéni kreativitásra építkező vonatkozásaitól, a környezetváltozás stratégiai lekövetéséhez szükséges generalista működési mechanizmusokon át a politikai döntésekig.[137]

Innen nézve tehát az egyén kibertérrel kapcsolatos viszonyulása és biztonságtudatossága a társadalmi és állami rendszerekre is hatással van, az egyes „felhasználók" viszonylatában csak a hatás összességhez viszonyított mértéke változó, akárcsak a környezetterhelés tekintetében. A biztonsági dimenziót azonban jelentősen áthatja – újabb pszichológiai kötődésekkel – az a másik aspektus, hogy a döntések felgyorsulása és az adataink „önkéntes" rendelkezésre bocsátásának automatizálása nem egy önmagában álló folyamat, hanem része annak a jelenségegyüttesnek, amely a kibertérben gyors egymásutánban, könnyen elérhető tartalomkavalkád miatt a koncentrált figyelem mérséklődése terén tapasztalható. Ezt ma már szembeötlően példázza, hogy a híradások terén milyen mértékben csökken a hírekre fordított figyelem és emiatt a hírek szövegezése során milyen jelentősége van annak, hogy egy adott beszámolót 3–5–10 vagy 20 perc alatt tud a nyájas olvasó feldolgozni, mivel az igények az előbbi irányba mozdulnak, ami szükségképpen ellene hat a mélyebb és megalapozottabb ismeretközlésnek, és sokkal inkább a téma fókuszált bemutatása helyett egy felszínes, de gyors összefoglalás felé mutat. Ez a jelenség persze nem kizárólag az internetezés viszonylatában jeleníthető meg, hiszen Christopher Andrew is hasonló irányú – maliciózus – fenntartásokat fogalmazott meg a titkosszolgálati információk politikai feldolgozása kapcsán, mikor kiemelte, hogy:

> „A kiberhadviselés és a terroristák esetleges tömegpusztítófegyver-használatából származó fenyegetettségérzet drámaian új kihívásokkal szembesíti a huszonegyedik századi hírszerző közösségeket. Hogy ezeknek megfelelhessenek, olyan hatékonyan, amennyire csak lehetséges, szükségük lesz a hosszú távú perspektívára, amelyet gyakran elfelejtettek vagy ignoráltak. (…) »A történelem nem adja könnyem agát a PowePoint-bemutatóknak és az executive summary-knek, amelyekre politikusaink egyre inkább hagyatkoznak… a történelem igazi megértéshez türelemre van szükség, amit nem könnyű kibékíteni a politika sürgetésével. Jó kiindulópont, ha a múltra a bölcsesség forrásaként tekintünk, nem pedig revelációként. »Csak a hosszú távú történelmi perspektíva menthet meg bennünket a saját kulturális analízisünk parochializmusától« - írja a korábbi cambridge-i történészprofesszor, Quentin Skinner. A stratégiai hírszerzési elemzés, ami nem vesz tudomást a hosszú távról, szükségképpen parochiális."[138]

A kibertér, a digitalizáció és az ezekkel szoros összefüggésben álló mindennapi dinamika fokozódása egyértelmű tehát, hogy komplex módon hat az egyénre, az egyén ehhez való

137 A téma kapcsán példaként l. Epstein (2021), Koetler (2021), Maszaaki (2022), Schühly–Becker–Klein (2020), Dewar–Keller–Malhotra (2022)

138 Andrew (2018): 26.

alkalmazkodási mintája és cselekvése pedig a biztonság vonatkozásában nem csak rá vetítve aknázható ki, hanem tömbösítve, társadalmi szintű jelenségek és a big data végtelenjében, ha úgy tetszik az igazságot módosító lehetőségek rengetegében is relevanciával bír. Ez az aspektus azonban még mindig inkább szól az egyéni és társadalmi létezés felgyorsulásának hatásairól és kihívásairól. Ebben a képletben érdemes azonban a kibertér jelentette sajátosságokra külön is ráirányítani a figyelmet. Ezt már a felhasználói tudatosság igénye, illetve a különféle diszciplínák reakciói is egyértelművé tették, hiszen, ha a kibertérnek nem lenne lényegi sajátossága az egyén – és az egyén révén a társadalom – viszonylatában, akkor elégséges lenne a kibertér technikai megközelítése, és nem bontakozott volna ki a kibertér pszichológiai elemzése, a kibertér szociológiája, vagy épp a kibertérben zajló tevékenységek etikája és geopolitikája az elmúlt évtizedekben.[139]

A sajátosság egyik fontos bázispontja talán az, hogy a fizikai valóságtól, és annak pszichológiai és szocializációs folyamataitól a kibertérben végzett cselekvés részint elkülönül. Sajátos egyéni magatartásminták érvényesülnek, illetve sajátos csoportképződési és csoportdinamikai tendenciák alakulnak ki, amelyek mögött sok esetben a kibertér fizikai – és ezáltal személyes – valóságtól való elkülönülése, vagyis az a tudati kapcsolódás áll, hogy mivel ez a magatartás virtuális, ezért a fizikai valóságban esetlegesen felmerülő kockázatok, veszélyek, hátrányok sokkal kisebbek, vagy nem is jelennek meg. Elégséges e körben a személyes életünk, érdeklődésünk közzétételének – és adatkezelésből, illetve adatkereskedelemből következő kommercializálásának – kérdéseire, mint a társadalmi láthatóság és ez által a személyes kibontakozás mértékként való érvényesülésére gondolni. Ehhez pedig célszerű hozzákapcsolni a felhasználónevek és avatarok által kínált – sok esetben hamis – anonimitás-tudat viselkedéstorzító hatásait, illetve a kibertérben zajló zaklató, nyomasztó, kirekesztő, sértő magatartásminták, valamint az egyéni életvitel beállított és adott irányba konstruált megjelenítéséből következő hatások problematikáját. Ezek ugyanis az egyén és egyén közti kapcsolatok szintjén képesek felerősíteni azokat a negatív magatartás mintákat, amelyek a fizikai valóságban – alapvetően – mérsékeltebben jelennek meg, egyúttal pedig megnyitják a virtuális térben megnyilvánuló véleménynyilvánítás szabadságának és az ehhez párosuló korlátoknak a kérdését. Erre a társadalmaknak reagálnia kell, hiszen egy rendkívül széles palettáról beszélünk, amelyben valóban jelen van a néha kevéssé intellektuális megnyilvánulásokkal járó, de mégis véleménynyilvánítási körbe tartozó kommentek sora épp úgy, mint a konkrét személyt emberi méltóságában sértő megnyilvánulások, vagy a kirekesztés, illetve a gyűlöletre uszítás.

Az ilyen értelemben nem tolerálható tartalmak, illetve a digitális térben zajló „bántalmazás" és kirekesztés kezelése ma már ismert probléma, és kezelési módozatai fejlődnek. Ezzel pedig az egyéni szint fontos – és sajnos mindennapos – kártékony érvényesülési formáira kezdünk újabb és újabb állami és társadalmi válaszokat adni.[140] Ezek a válaszok fokozzák az egyéni biztonságot mind személyünk, mind hozzátartozóink, és különösen az egyre fiatalabb felhasználói korcsoportok tagjai számára, de persze még sok tennivaló áll előttünk.

A biztonságot veszélyeztető egyéni cselekmények másik nagy, és viszonylag jól azonosítható csoportját képezi az információs rendszerekben, vagy azok révén elkövetett bűn-

139 Ezek kapcsán példaként l. Wallace (2002), Suler (2015), Assa (2011), Desewffy (2019), Cavanagh (2007), Lupton (2015), Taddeo–Glorioso (2017)

140 Példaként l. Hazelwood–Koon-Magnin (2013): 155–168., Arató et al. (2022): 160–173., D. Horváth (2022): 46–50., Kovács-Szépvölgyi (2022a): 227–236., Kovács-Szépvölgyi (2022b): 109–122.

cselekmények köre, amelyek terén szintén jelentős fejlődés volt tapasztalható az elmúlt évtizedekben.[141] Ezek egyszerre jelentenek fenyegetést az egyéni és a társadalmi biztonságra, hiszen egyik oldalról az adott egyén sérelmére információs rendszer útján elkövetett bűncselekmény magától értetődően a közrendre is hatással van, másik oldalról azonban e körben elkövethetők olyan bűncselekmények is, amelyek egyének csoportját vagy állami szerveket érintenek, és ezzel már a biztonság makró szintjén is jelentős hatással vannak. Nem véletlen, hogy az államok az elmúlt években a relevánsnak ítélt büntetőjogi válaszok fejlesztése mellett a nyomozóhatóságok és az igazságszolgáltatás terén is fokozta a digitalizációval összefüggő képességeket. A kibertér és az egyén viszonyulása, illetve e kapcsolat biztonsági vonatkozásai tekintetében azonban fontos, hogy kellő figyelmet fordítsunk azokra a megvalósulási formákra is, amelyek nem ennyire maguktól értetődően kategorizálhatók, illetve amelyek látenciája, fedettsége jóval nagyobb, mint a „hagyományos" értelemben vett bűnözés digitalizációjának, vagy a tömeges felhasználásból következő szélsőséges, el nem fogadható viselkedésmintáknak.

Az egyén és a kibertér kapcsolata ugyanis egy, talán fel sem fogható kiterjedtségű biztonsági horizontot jelent. Ennek behatárolásához célszerű onnan indítani a gondolkodásunkat, hogy a kibertérrel kapcsolatba kerülő egyének döntő többsége felhasználó, rendkívül eltérő informatikai ismeretekkel és felhasználói attitűdökkel. E körben nyer értelmet a kiberbiztonság kulcsterületeként megjelenő biztonságtudatosság, hiszen a felhasználónak magának nem kell feltétlenül ártó szándékúnak lennie ahhoz, hogy biztonsági kockázatot generáljon, illetve biztonsági fenyegetést alapozzon meg. Elégséges, ha a kellő felkészültség, gondosság hiányában a kibertér részeként működő rendszerelem használata során olyan magatartást tanúsít (például biztonsági protokollokat figyelmen kívül hagy, tilalmazott tartalmakat akar elérni, vagy csak elmulasztja a kellő körültekintést egy ismeretlen/megtévesztő küldemény kapcsán stb.), amellyel egy szándékoltan ártó cselekmény kiteljesedéséhez nyit ajtót saját rendszerére. Az elvárható gondosság/tudatosság hiánya mint egyéni viszonyulás ma számos kibertérből érkező fenyegetés kártétellé válásához elkerülhetetlen a zsaroló vírusoktól és alkalmazásoktól a rendszerekbe való beszivárgáson át egészen az ártó szándékú információk fürkészésig.

A tudatosság kérdésének azonban van egy másik vonatkozása is, jelesül az információk hitelességével kapcsolatos tudatosság dimenziója. A felhasználói tudatosságnak ugyanis nem csak az információs rendszer megfelelő alkalmazására, az infokommunikációs megoldások alkalmazásával járó felelősségre – ha úgy tetszik, akkor „az internet nem felejt"-elv érvényesítésére – kellene kiterjednie, hanem arra is, hogy a kibertérben sokkal könnyebben és gyorsabban elérhető információk megbízhatóságának elemzése kapcsán is tudatosabbak legyünk. Ez azonban egy sajátos önellentmondásos helyzetet teremt, hiszen a hiányzó, megismerni kívánt információk gyors elérésében rejlő előny alapja a gyorsaság mellett az, hogy befogadható legyen az információ közvetítése. Az interneten rövid idő alatt elért információ mint tudás önmagában nem tud megalapozott és mély lenni, nem tudja kiváltani az adott témakörre vonatkozó hosszas tanulási folyamatot, viszont praktikusan tudja egyszerűsíteni a konkrét részkérdésre vonatkozó információs igény kielégítését. Ez egy természetes törekvés, hogy felgyorsult világunkban adott információt a lehető leggyorsabban szerezzünk meg. Kérdéses azonban, hogy ehhez miként lehet hatékonyan hozzákapcsolni az információfor-

141 A téma kapcsán l. Curtis (2011), Mezei (2022a): 529–549., Mezei (2022b), Ambrus (2021),Bartkó–Gál (2022), Acsai (2020): 1484–1500.

rás hitelességéről való gondolkodást. Az elemző-értékelő tevékenység, illetve a tudományos módszertan erre alkalmazza a forráskritikát, illetve az információk és források ütköztetését. Ez azonban nehezen érvényesíthető a felhasználók széles körére, hiszen akkor olyan többlet információkeresési és feldolgozási kötelezettséget rónak rájuk, amelyek teljesítésével a gyors információszerzés igénye már nem tudna kielégülni. Ez a paradoxon pedig a dezinformáció egyik melegágya, különösen azon esetekben, ahol az információk részleges manipulálása mögött jól szervezett és átgondolt törekvés áll.

Az információk torzítása révén a preparált vagy téves információt használó tudat befolyásolható, ennek pedig különféle fokozatai azonosíthatók. A hatások az egyén biztonságérzetétől a bizalmi viszonyulásán át egészen a szorongásaiig és félelmeiig terjedő skálán tudnak mozogni. Ez pedig egyértelműen hátrányosan hat az egyén biztonságára, de akár társadalmi szintre is tud lépni. E tekintetben gondoljunk azokra a torz- vagy téves hírekre, amelyek a „válságvásárlási" hullámokat táplálják, vagy akár a választások befolyásolását célzó törekvésekre.[142] Végletes esetben azonban a torz és célzottan adagolt információk az egyén radikalizációját is elő tudják mozdítani, amely kapcsán az elmúlt években a terrorizmus és a digitalizáció viszonya volt a legkirívóbb megvalósulási forma a „terrormarketingtől" a digitális toborzásig és irányításig.[143] Ez a fokozat pedig már egyértelműen a társadalmi szintű biztonságra kiterjedő hatással bír, amellyel szemben az államoknak és azok szövetségeinek is fel kell lépnie a biztonság fenntartása érdekében.

A társadalmi léptékben vett biztonság direkt érintettségével járó kibertér-egyén relációk körében számos további séma is felvázolható lenne, ahhoz azonban, hogy az egyén és kibertér közti kapcsolat szürke és sötét zónáinak tényleges hatáslehetőségeit jobban át tudjuk látni, a jövőben szükséges volna a lehetséges veszélyek mátrixát azonosító kutatások elvégzése. Be kell ugyanis látni, hogy a biztonságot érintően az egyén és kibertér kapcsolódása terén nem csak a kibertér újdonságából következő magatartások jelenthetnek komoly kihívást, hanem azok a korábbról is ismert magatartások, amelyek a kibertérben újabb és másabb érvényesülési terepet nyernek. A digitális tér által nyújtott – de sok esetben csak vélt – anonimitás, illetve a valóság mellett alternatív dimenzióként megélt virtuális térérzet révén ugyanis jelentős lehetőségek nyílnak az egyének zsarolására épp úgy, mint a karaktergyilkosságok fokozására, illetőleg a megtévesztésen alapuló befolyásolásra, melynek célja viszont a fizikai térben megvalósuló cselekmények kiváltása.

Az, hogy mindezek bűnözési, hírszerzési, radikalizációs vagy más célból történnek meg, fontos kérdés, de a biztonság fenntartása és erősítése szempontjából a hangsúlyt arra kell fektetni, hogy a kibertér újfajta „hozzáférést" biztosít a különféle információs rendszereken túl a nem kellően tudatosan, nem kellően felkészült vagy valamiképp sérülékeny egyénekhez is. Az egyének biztonságtudatosságának és védettségének erősítése tehát a kibertér és a nemzeti biztonság relációjában kulcsfontosságú, ennek előmozdítása azonban komplex cselekvést igényel, mivel egyszerre kell fokozni a reagálóképességet, az ezt meghatározó szabályozási és intézményi keretek korszerűségét, valamint az állam-társadalom-egyén ellenállóképességét úgy,[144] hogy közben ne alakuljon ki túlzott ellenhatás, bizalomvesztés a digitalizáció viszonylatában.

142 A téma kapcsán l. Mcintyre (2018), Kalpokas (2019), Krekó (2018), Krekó (2021)

143 L. Siboni–Cohen–Rotbart (2013): 3–29., Oteren et al. (2016), Smith, T. E. (2017): 54–58., Lieberman (2017): 95–124.

144 A téma kapcsán bővebben l. Farkas–Vilics (2022), Farkas–Spitzer (2021)

2. Hackerek – Az egyén mint a kibertér aktív szereplője

A kibertérnek a passzív személyi körére gyakorolt hatása mellett érdemes áttekinti azt a kört is, akik a kibertér folyamatait aktívan alakítják, vagyis az egyének azon körét, akiket a társadalom nagy általánosságban hacker jelzővel illet. Maga a hacker elnevezés ilyen általános használata nem megfelelő a jellemzésükre, amely jóval összetettebb fogalmi kört ölel fel. Ennek a fogalmi körnek a kibontása azért szükséges, mert ezen aktorok jelentősége a kibertérben megkerülhetetlen, hiszen ők azok a szereplők, akik vagy magányosan, vagy egy csoport tagjaként, illetve állami szervnél a kibertér mint tér belső folyamatainak tényleges formálását végzik.

E cselekményük során különböző motivációkat követve valósítják meg tevékenységüket. Kiemelkedő jelentőségük tetten érhető abban, hogy már az államok biztonsági kihívásokkal foglalkozó dokumentumaiban is megjelennek mint potenciális veszélyforrás. Az Egyesült Államok egy korábbi nemzetbiztonsági jelentése csoportosítja a kibertér kiemelt veszélyforrásait. Ezek a következők: államok, amelyek fejlett kiberprogrammal bírnak (például Oroszország és Kína); államok, kisebb kiberkapacitással, de veszélyeztető szándékkal (például Irán, Észak-Korea); vagyonszerzési szándékkal kiberműveletet megvalósító személyek; ideológiai szándék vezérelte hackerek vagy szélsőségesek.[145]

Az azonosított veszélyforrásokból a kibercselekményekhez köthető személyi kör is levezethető. A kibertérben tevékenykedők köre lehet: 1) az egyén; 2) az egyének illegális csoportjai: a) terrorszervezetek, b) bűnszervezetek; c) szakadár szervezetek; d) radikális szervezetek; 3) gazdasági szereplők; 4) államok[146] és közösségeik.

Mindez azonban csak a jéghegy csúcsa. Azzal, hogy listáját adjuk a szereplőknek, illetve a klasszikusan az állami potenciált mélyebben jellemezük, nem teszi érthetővé azt a szubkultúrát, ahová ezen egyének tartoznak, nem fedik fel, hogy miért valósítanak meg ilyen típusú cselekményeket, pedig ezen szereplők jellemvonásának ismerete segítheti a megfelelő szabályozás megalkotását, és segítséget nyújt a biztonsági protokollok kialakításához.

Max Kigler tanulmányában kifejtette, hogy a felkészülés fontos módja a jövőbeni támadásokat, ugyanis a feltérképező forgatókönyvek elkészítése révén feltárhatják a jelenlegi sérülékenységet azzal, hogy rávilágítanak a potenciális fenyegetésre, míg a terrorizmus esetén olyan infrastruktúrákra mutathatnak rá, amelyek az adott időpontban még nem kritikusak, de a predesztinálható folyamatok révén azzá válhatnak, és ez az eszközök biztonsági oldalának fejlesztését is segítheti, az elkészült dokumentumok a szabályozás irányára is rámutathatnak. Ezek a forgatókönyvek egy jelentős deficittel rendelkeznek: erősen technológiai alapúak és kevésbé figyelnek a kulturális, társadalmi és pszichológiai összetevőkre, tehát figyelmen kívül hagyják a humán faktort, annak ellenére, hogy a támadási láncolat központi eleme az egyén.[147]

Ha ezen szereplőket, akár mint magányos elkövetőket nézzük, vagy akár, mint bűnözői csoportokat, akkor a globális gazdasági és biztonsági jelentőségük minden korábbinál na-

145 R. James Clapper: Statement for the Record World wide Threat Assessment of the US Intelligence Community Senate Armed Services Committee (2015. 02. 26.), 2.
www.armed-services.senate.gov/imo/media/doc/Clapper_02-09-16.pdf?

146 Fontos megjegyezni, hogy az államhoz nemcsak hivatalos intézményei által megvalósított cselekmények köthetőek, hanem más személyek vagy csoportok azon cselekményei, amelyek az államnak betudhatóak. l. bővebben: Sulyok (2005): 30–56., Spitzer (2019a), Kecskés (2014) 289–301.

147 Kilger (2015): 693.

gyobb volumenű. Emellett persze tudjuk, hogy a támadó államok, a hibriditás során előszeretettel „alkalmaznak" olyan nem állami szereplőket, akik a megtámadott állam társadalmában valamely töréspontonhelyezkednek el, vagy vagyonszerzési potenciált látnak a támadó fél céljainak kiszolgálásában. A számok nyelvére lefordítva azt látjuk, hogy a kiberbűnözés globális költségei 2015 óta megduplázódtak, vagyis a 2015-ös 3 milliárd dollárról 2021-re 6 milliárd dollárra nőttek, és a Cybersecurity Ventures becslései szerint ez 2025-re 10,5 milliárd dollár lesz. A kiberbiztonsági kiadások pedig elérik az évi 1 milliárd dollárt.[148]

Az FBI 2021-es kiberbűnözéssel kapcsolatos jelentése is megerősíti ezt, hiszen 2021-ben végül a korábbi becsléseket meghaladva 6,9 milliárd dollár kárt eredményezett a kiberbűnözés, amelyhez 847 376 bejelentés társult.[149] Az FBI jelentését vizsgálva kirajzolódik, hogy ezen cselekmények – azon túlmenően, hogy a globális gazdaságnak kiemelkedően jelentős kárt okoznak (nagyobbat, mint a természeti katasztrófák) – az emberek életterét is jelentősen veszélyeztetik. Ugyanis például a zsarolóvírus (ransomware) támadásokkal leginkább érintett szektorok az energiaszektor, a víz- és szennyvízrendszer, a pénzügyi szolgálatások, az élelmiszeripar, a mezőgazdaság és leinkább az egészségügy voltak.[150] A támadással érintettek korfáját vizsgálva pedig az látszik, hogy a leginkább kitett csoport a hatvanéven felülieké, de a 30 éves korosztálytól minden dekád mellé egy milliárd dollár kár társul, továbbá a gyermekek is kicsit több mint száz milliárd dollárnyi károkozást szenvedtek el. Tehát a társadalom valamennyi rétege kitett a kiberbűnözők cselekményének. Országos összevetésben a legnagyobb kárt az Egyesült Államok szenvedte el, de mellette jelentős veszteséget könyvelhetett el az Egyesült Királyság, Kanada, India, Ausztrália, Franciaország, Dél-Afrika, Németország, Mexikó, Brazília, Fülöp-szigetek, Hollandia és Görögország is,[151] tehát a glóbusz minden része érintett a problémában.

Jellegüket tekintve azon cselekményeket emel ki a jelentés, amely fiskális értelemben is hátrányt okoz, ezek közül is kihangsúlyozza a zsarolást, az identitáslopást, az adatvédelmi incidenseket és az adatlopást. Ezzel szemben az Europol más típusú csoportosítást alkalmaz, jelentésében sokkal inkább a társadalomra veszélyességet emeli ki egy cselekményi körrel kapcsolatban. Ennek során lehatárolnak tipikusan kibertérhez köthető cselekményeket, így a zsaroló vírusos támadások, a mobil alapú rosszindulatú szoftverek általi támadások, illetve a DDos alapú támadásokat, szintén zsarolási célzattal. Emellett az Europol-jelentés rámutat a gyermekek szexuális kizsákmányolására irányuló kiber cselekményekre, az online csalásokra, amelyek a Covid19 pandémia nyomán jelentkező fokozott digitális aktivitás miatt jelentősen elszaporodtak. Nem konkrét cselekményként, de rámutat arra, hogy legalább ilyen jelentős probléma a darknet egyre nyilvánvalóbb iparági jellegű szerveződése, amelyet a szürke zónás eszközök csak tovább erősítenek, így a kriptovaluták is.[152] E megkülönböztetett figyelem ab-

148 Steve Morgan: *2019 Official Annual Cybercrime Report – Cybercriminal activity is one of the biggest challenges that humanity will face in the next two decades.* herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf

149 *Federa Bureau of Investigation Internet Crime Report 2021*. Internet Crime Complaint Center, 7. ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf (továbbiakban: FBI 2021-es jelentés)

150 FBI 2021-es jelentés, 15.

151 FBI 2021-es jelentés, 20.

152 Europol (2021), Internet Organised Crime Threat Assessment (IOCTA) 2021,
Luxemburg. Publications Office of the European Union, 2021. europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf

szolút indokolható és elvárható, mivel „a bűnözői tevékenység szinte minden formája (zsarolás, csalás, bántalmazás, prostitúció) megrendelhető”[153] a darknet weboldalain keresztül, ahol „a bitcoin a digitális birodalom színarany dublonja, de annyival még jobb is a régi spanyol pénzérménél, hogy tetten érhetetlen, névtelen valutaként (…) használható.”[154]

A kibertérben megvalósuló ártó jellegű cselekmények, abban az esetben is, jelentős károkat vonnak maguk után, ha nem államközi jelleget öltenek, tehát ebben az esetben ugyanúgy nemzetbiztonsági kockázatok és a társadalom egészét – a fiataltól az idősig, anyagi helyzettől függetlenül – a Föld valamennyi tájékán érintik. Így szükségszerű, hogy ne általánosságok szintjén kezeljük azt a személyi kört, akik ezeket a cselekményeket megvalósítják, és ne egy általános elkövető vagy hacker fogalom alá vonjuk be őket, mert ennek a buktatója, hogy ebből nem tudjuk megfelelően felmérni az elkövetői kör képességeit és motivációját, amely nélkül sem rendészeti, sem nemzetbiztonsági értelemben nem tudjuk megfelelően kezelni a problémát. Így ennek a fejezetnek a célja, hogy az általános hacker fogalmat kibontsa, és rávilágítson arra, hogy milyen tág merítésű akár képességben, akár motivációjában az egyéneknek az a köre, akik aktív szereplőként lépnek fel a kibertérben.

Érdemes először eloszlatni azt a téves képzetet, hogy mindenki, aki a kibertérben ártó módon tevékenykedik az hacker, illetve minden hacker ártó szándékkal lép fel. Több típusú csoportosítással találkozhatunk ezen a területen. Az egyik kézenfekvő felosztás a képességek szerinti megkülönböztetés. Ebben az esetben érdemes előbb leválasztani a hackerről azt a réteget, akik valójában a tényleges hackerhez képest gyengébb tudásúak, vagy más típusú készséggel bírnak. Az egyik kevésbé ismert kategória a phreakerek, akik eredetileg a telekommunikáció szakértői voltak, ebből kifolyólag inkább távközlési rendszerekre szakosodtak, azok hiányosságait kihasználva ingyen vették igénybe a szolgáltatásokat, illetve hallgattak le másokat.[155] Mára a mobiltelefonos operációs rendszereket célozzák, vagyis például androidos telefonokra írt alkalmazásokon keresztül valósítják meg ártó tevékenységüket (spoofing[156] lehallgatás,[157] szolgáltatásmegtagadásos támadások, túlszámlázások formájában).[158] Szintén egy más kört takarnak a crackerek. A cracker és a hacker közötti különbség legkézenfekvőbben abban ragadható meg, hogy „a cracker feltör, a hacker betör”[159], azonban a tudásukban is releváns eltérés van, ugyanis a tapasztalatuk és szakértelmük nem éri el a hackerekét.[160] Fogalmilag nézzük akkor két jelentéssel találkozhatunk: „elsődleges jelentése szerint olyan

153 Aiken (2020): 289.

154 Uo., 295.

155 Kazári (2003): 20.

156 A spoofing egy olyan típusú csalás, amelyben a bűnöző álcázza az e-mail címet, a megjelenített nevet, a telefonszámot, a szöveges üzenetet vagy a weboldal URL-címét, hogy meggyőzze a célpontot arról, hogy egy ismert, megbízható forrással lép kapcsolatba. A hamisítás gyakran csak egyetlen betű, szám vagy szimbólum megváltoztatását jelenti a kommunikációban, hogy az egy gyors pillantásra érvényesnek tűnjön. L. Jean Folger: What Is Spoofing? How Scam Works and How To Protect Yourself. *Investopedia,* 2022.09.07. investopedia.com/terms/s/spoofing.asp

157 A spoofing lehallgatás olyan technikát jelöl, amelyben az illetéktelen személyek meghamisítják vagy átverik a kommunikációs rendszerek vagy eszközök azon képességét, hogy átvigyenek vagy rögzítsenek információkat, ezáltal a támadók képesek lehetnek mások kommunikációját lehallgatni, illetve manipulálni azt. L. Jake Frankenfield: Eavesdropping Attack. *Investopedia,* 2022.02.11. investopedia.com/terms/e/eavesdropping-attack.asp

158 Jeremy Kirk: Is it still possible to do phone phreaking? Yes, with Android on LTE. *PCWorld,* 2015.10.19. pcworL.com/article/424063/is-it-still-possible-to-do-phone-phreaking-yes-with-android-on-lte.html

159 Forrest (2005): 206.

160 Raymond (1996): 22.

kárt okozó személy, aki számítógépes rendszereket rongál, illetve adatokat tulajdonít el, vagy bármilyen egyéb módon kárt okoz."[161] A cracker másodlagos jelentése viszont az, hogy a kereskedelmi forgalomba hozott szoftverek kódját módosítva lehetővé teszi, hogy az szabadon másolható és ezáltal terjeszthető legyen.[162] Lényeges kritérium itt a specializáció, mivel míg a hacker átfogó ismeretekkel rendelkezik a kibertérről, addig ezen szereplők csak egy-egy területen rendelkeznek kimagasló tudással. Egyes felosztások szerint a script kiddie-k egy kvázi hacker társadalom előszobáját jelentő kategória, ugyanis ők általában 14–16 éves iskolás fiúgyerekek, akik főként csak mulatják az időt a kibertérben, azonban van elég tudásuk ahhoz, hogy kárt okozzanak, igaz legtöbb esetben akaratlanul, sokan közülük meglépik a következő lépcsőt és hackerekké válnak.[163]

Mondhatni megérkeztünk a hackerek kategóriájához.

> „Az elnevezés az 50-es évekből származik, a MIT nagygépeket programozó végzős diákok és szakemberek kezdték magukra alkalmazni ezt a kifejezést, mégpedig azért, mert az akkori gépek korlátaival találkozva (nagyon kevés memória volt a számítógépekben akkoriban), megpróbálták minél kisebbre „összenyomni" a programokat és az operációs rendszereket, tehát belenyúltak a programokba, rendszerekbe, illetve átírták azokat."[164]

A szűk értelemben vett hackernek tekinthető kategória esetében is számos osztályozással találkozunk, mivel a kibertér legnagyobb tudású képviselőjeként szintén nem heterogén kategória, az tovább tipizálható az egyes hackerek tudása szerint. Képeségek alapján egyes szerzők négy kategóriába sorolják a hackereket: 1) a guru (guru hacker); 2) alkalmi/hétköznapi (casual hacker); 3) a tanuló (learning hacker); és 4) kezdő hacker (novice hacker).[165] A kezdő és tanuló hackerek, bár próbálják rendszerszinten szemlélni a kiberteret, még valós tudásuk nincs, hogy annak alapfolyamataiban változást idézzenek elő, sokkal inkább összefüggéseket keresnek, néhány ismert gyenge pontra, területre fókuszálnak. Az alkalmi hacker már képes programok megírására; fő jellemzője e csoportnak, hogy képes megkerülő eszközök (Circumvention Tool)[166] segítségével láthatatlanul manőverezni a kibertérben és kommunikálni más számítógépekkel.[167] A guru a legnagyobb tudású hacker, aki saját maga ír programokat (például vírusokat, férgeket) – amiket megoszt gyengébb tudású társaival –, tevékenységét rendkívül magas, szinte művészi szintre fejlesztette. Ténykedése során nemcsak rendszerszinten átlátja a kibertér folyamatait, hanem azokba aktívan beavatkozik.[168]

Egy másik, közismert megkülönböztetése a hackereknek az ún. kalapos felosztás, amely már tudáson túl a tevékenység szándékát is a csoportosítás alapjává teszi. Eredeti formájában három csoportot különítettek el: white hat hacker, grey hat hacker, black hat hacker. A white hat hacker az, aki a teljes legalitás talaján áll, hiszen tevékenységét a rendszer üzemeltetőjé-

161 Kazári (2003): 19.
162 Uo., 21.
163 Barber (2001): 15.
164 Kazári (2003): 18.
165 Zhang et al. (2015): 1245.
166 Ilyen eszközök többek között az egyszerű web proxyk, a HTTP/SOCKS proxyk, blokkolást gátlók, virtuális magánhálózat szolgáltatások. L. bővebben: Roberts et al. (2010): 1–13.
167 Zhang et al. (2015): 1247–1249.
168 Uo., 1246–1247.

nek megbízása alapján végzi, és ennek során hívja fel a figyelmet a biztonsági résekre. A grey hat hacker megbízás nélkül végzi eme tevékenységet, erről csak utólag értesíti a rendszer üzemeltetőjét. A black hat hacker az illegalitás talaján a rendszereket támadja, keresi annak hiányosságait, réseit, és azokat céljának megfelelően kihasználja.[169]

A „kalapos" felosztás az elmúlt években bővült a green, a yellow, a blue, és a red hat hackerek körével. A green hat hackerek sokkal inkább megfeleltethetők a fenti kategóriák közül a tanuló és kezdő hacker körrel. A yellow hat hackerek, akiket neveznek közösségi média hackereknek is, mivel a közösségi média fiókok és felhasználói fiókok feltörésére szakosodtak. Céljuk az egyes fiókokhoz való hozzáféréssel egy-egy márka lejáratása, rosszindulatú programok terjesztése, bosszúállás vagy személyes adatokkal való visszaélés.[170] A blue hat hackerek a white hat körhöz vannak legközelebb, tevékenységük során felkérésre sebezhetőségeket keresnek a rendszerekben. Ezért is szervez a Microsoft BlueHat konferenciákat. Egy másik értelmezés szerint viszont csupán bosszúra törekvő hackerek körét teszik ki, akiket kizárólag a céljuk elérése érdekel. A red hat hackerek pedig a Linux rendszereket célozzák tevékenységük során. Céljuk a black hat hackerek lefegyverzése, azonban a white hat hackerektől eltérően ők nem a hatóságok kezére kívánják juttatni őket, hanem önbíráskodásba kezdenek, és a black hat hackerek teljes ellehetetlenítésére fókuszálnak, amely során erőforrásaikat is meg kívánják semmisíteni.[171]

Újabban – igaz nem kalapos elnevezéssel – ehhez a körhöz vonnak három további személyi kört: cryptojackers-t, a gaming hacker és large-scale hacker kategóriákat. A cryptojackers és a large-scale hacker nagyon hasonló fogalomkört takar, ugyanis mindkettő egy idegen számítógép erőforrását kívánja a saját céljára megszerezni, azonban míg az előbbi – nevéből is következőleg – bányászatra használja azt, addig az utóbbi bot hálózat létrehozására, hogy azzal nagy volumenű támadást hajtson végre.[172] A gaming hackert a játékipar óriási fejlődése hozta magával, mivel ezekben a játékokban nagyon sokan rengeteg pénzt költenek. Ezen hackerek pedig ezt használják ki: vagy az ellenfelet akarják kivonni a játékból, például DDoS tipusú támadással, vagy a másik által a játékban megszerzett – és ma már materiális értékkel bíró – játéktartozékokat veszik el.[173] Egy másik csoportosítás alapja az általuk megvalósított tevékenység. E tipizálás már a script kiddies kört is ide vonja. Elfogadhatónak tűnik a két csoport közötti átfedés abból adódóan, hogy az életkori sajátosságok ellenére már találkozhatunk közöttük magasan képzett egyénekkel is.[174] A „fekete kalapos" megvalósíthatnak államok által finanszírozott cselekményeket, hírszerző tevékenységet, kiberterrorizmust, vagy belső, intézményen belüli rosszindulatú tevékenységet. Utóbbi jelenlegi vagy volt alkalmazottak káros tevékenységére utal.[175]

Sean Atkinson a The SecOps Group alapítója és a Lancaster University oktatója elemzésében a hackerek csoportosításánál az ártó szándékot vette alapul, és ennek alapján elkülöní-

169 Long (2012): 4–6.

170 Yellow hat hacker definition. nordvpn.com/cybersecurity/glossary/yellow-hat-hacker

171 Sharon Shea: 6 different types of hackers, from black hat to red hat. *TechTarget, SearchSecurity,* October 2019. techtarget.com/searchsecurity/answer/What-is-red-and-white-hat-hacking

172 What is Cryptojacking? – Definition and Explanation. kaspersky.com/resource-center/definitions/what-is-cryptojacking

173 14 Types of Hackers to Watch Out For. *panda/mediacenter,* 2021 pandasecurity.com/en/mediacenter/security/14-types-of-hackers-to-watch-out-for

174 Ilyen volt például az orosz hacker Ilja Hofman is, aki társaival a 1990–es évek végén körülbelül 97 000 dollárt utalt saját bankszámláikra 16 amerikai és néhány orosz bankból. Ilja történetét lásd bővebben: Turovszkij (2020): 34–39.

175 Nasr et al. (2016)

tette a script kiddiest, a rosszindulatú bennfenteseket, a kiberaktivistákat, a kiberkémeket, a kiberterroristákat és a kibertéri szervezett bűnözőket. A kiberterroristákkal kapcsolatban megjegyezte, hogy ezek lehetnek állam által finanszírozott ügynökök, ideológiai csoportok, vagy egyének, akiket a bosszúvágy hajt. A kiberkémek lehetnek vállalati vagy állami célokat kiszolgálók, míg a kibertéri szervezett bűnözök motivációja a pénzszerzés és a kaotikus helyzetek előidézése.[176] Általánosságban megállapította, hogy mindegyik csoport azonos körülményeket használ ki, vagyis a felhasználói képzetlenséget, hogy nincsenek tisztában a veszéllyel vagy nem törődnek azzal, emellett pedig az emberi természetből fakadó hanyagságot, lustaságot és naivitást. Az emberek jelentős része, mivel az adatot nem tudja materiális értelemben megfogni, kézbe venni, ezért nem is képes olyan tudatosan kezelni az azokhoz kötődő értékeit úgy, mint a hagyományos térbeli értékeit. Emellett e területre jellemző, hogy magas marad a látencia, hiszen sokan nem is tesznek feljelentést a nyomozóhatóságok felé, illetve fel sem fedezik a támadást, ami köthető ahhoz is, hogy a kibertérben sok felhasználónak sokkal fokozottabb a bizalma, mint a hagyományos térben, amit e szereplők ki is használnak, nem beszélve arról, mikor valamilyen potenciális függőség nyit lehetőséget számukra arra, hogy a szembenálló adatvagyonához, és azon keresztül, akár hagyományos értékeihez is hozzáférjen.[177]

Nem véletlen, hogy a tudományos gondolkodás területén a hacker csoportosítások elrugaszkodnak a kalapos rendszertől, és sokkal inkább folytatatják a motivációs irányba való tolódást. A szingapúri szerzők nevéhez köthető felosztás már tizenhárom különféle hackertípust különböztet meg: script kiddies, tanuló, cyberpunk, old guard, rosszindulatú bennfentes, piti tolvaj, profik, nemzetállamok hackerei, hacktivisták, kiberragadozók, digitális kalózok, crowsourcere, kiber bűnsegédek. A tanuló annyiban különbözik a script kiddies-től, hogy nincs ártó szándéka, a tanulás és a kíváncsiság hajtja. A cyberpunk alacsony vagy közepes képességű hacker, akinek a célja a pusztítás. Az old guard-ok nem rosszindulatú hackerek, őket a kíváncsiság és a hírnév ösztönzi. A kalapos felosztásból ide tartozik a fehér és a szürke kalapos hacker. A rosszindulatú bennfentes elégedetlen a helyzetével a szervezetben, ahol dolgozik, vagy ahol dolgozott: cselekményét haszonszerzési céllal, bosszúból vagy ideológiai megfontolásból viszi véghez. A piti tolvaj az, aki hagyományos téri cselekményeit menti át kibertérbe. A profik a magasan képzett hackerek. A nemzetállamok hackerei közvetlenül vagy közvetve dolgoznak a kormányoknak, tevékenységükkel destabilizálva más államokat, zavart keltve vagy információt szerezve a megbízónak. Kiegészítve a szerzők leírását, hozzá kell tenni, hogy a közvetlenül az állami szervnél dolgozó hackerek láthatják el az egyes kritikus infrastruktúrák és egyéb rendszerek védelmét is. A hacktivisták politikai vagy ideológiai céltól vezérelve valósítanak meg cselekményeket. A kiberpredátorok szexuális ragadozók, és ezen belül is főként pedofilok. A digitális kalózok lényegében a szerzői jogi jogsértő tevékenységet realizáló szereplők. A crowsourcerek egy probléma megoldása érdekében összefogó hackerek átmeneti csoportja. A kiber bűnsegéd különböző eszközöket biztosítnak másoknak kiber(bűn) cselekmények megvalósításához; kiemelkedő tudásúak egy-egy speciális szakterületen.[178]

Segíti az átfogóbb kép alkotását, ha ezen csoportosítás mellé megnézzük az egyes hackerek lehetséges motivációját is. Alice Hutchings felosztása szerint ezek a következők lehetnek: kíváncsiság, önfejlesztés, szórakozás; erő érzete, demonstrálása, kihívás; társadalmi státusz

176 Atkinson (2015): 4–9.
177 Uo., 12–13.
178 Chng et al. (2022): 3.

kiharcolása; ökológiai, politikai aktivisták (hacktivism); pénzügyi nyereség; külső nyomás (terrorista vagy bűnözői csoportok részéről).[179] Ezt Barber kiegészíti az ipari kémkedéssel, a kiberhadviseléssel,[180] a zsarolással és a csalással.[181]

John van Beveren fejlődési modelljében a Csíkszentmihályi Mihály által megalkotott flow elméletet használta fel a hackerek motivációjának feltérképezésére. A flow-élmény az elme olyan állapotát jelenti, amikor a cselekvésbe annyira belefeledkezünk, hogy a figyelem osztatlan lesz és ez az időérzetet elnyomja, maga a cselekvés pedig boldoggá teszi az embert.[182] Beveren szerint a hackerek ebbe az állapotba kerülnek tevékenységük során, és ez segíti bennük kialakulni a kontrollérzetet, az összpontosítást és felerősíti a kíváncsiságot. Ez pedig állandó fejlődésre sarkallja őket. Így bár megkülönbözteti a motiváció esetében a belső kényszert a hackelésre, a kíváncsiságot, a hatalom és kontroll iránti vonzalmat, valamint a társak elismerését, de rögzíti azt is, hogy flow-élmény révén megvalósuló fejlődés megváltoztatja az eredeti szándékukat és motivációjukat.[183] E felosztás annyiban rugaszkodott el a valóságtól, hogy idealizálja a hackereket, ezért a hagyományos térből átszűrődő motivációkat és főként az anyagi jellegűeket nem veszi számításba. Előnye, hogy felmérte egy szubkultúra sajátosságát, mivel a szereplők legtöbbjét ezek a tényezők hajtják, és a flow-élmény is megkerülhetetlen sajátja a közegnek, mivel a hackerek többsége egyfajta játéknak fogja fel a hackelést. Ezáltal megjelennek a klasszikus gamifikáció személyes (personal), mechanikus (mechanical) és érzelmi (emotional) elemei,[184] utóbbi flow-élményként jelenik meg náluk, vagyis egyfajta boldogságérzetet vált ki belőlük a pozitív megerősítések miatt.

A hackereket „hajtó" motivációk széleskörű cselekménykört ölelhetnek fel. Így ezek realizálása jelenthet egyszerűen egy információs rendszerbe való betörést, az ott lévő információ megismerését, módosítását, megsemmisítését, vagy az információs rendszer elérhetetlenné tételét, továbbá a megszerzett információ kiszivárogtatását, személyes adat megszerzését és az azzal való visszaélést, valamint legsúlyosabb esetben a kritikus infrastruktúrák elleni támadást. Ezen motívumok által vezérelt személyek kibertérben realizált cselekményei komoly problémát jelentenek az államok számára. Eme cselekményeknek a társadalomra, államra veszélyessége szintén rendkívül széles skálán helyezhető el, hiszen teljesen más hatásfokú egy szórakozásból vagy kihívásból elkövetett kibertámadás, mint egy nagyobb volumenű csalást, egyéb vagyoni célú bűncselekményt megvalósító cselekmény, vagy azon támadások, amelyek az egyes állami feladatellátások diszfunkcióját tűzik ki célul. A skálához rendelve lehet meghatározni az állami és jogi ellenlépéseket, válaszokat, valamint a fellépésre jogosított ágazatokat, ágazatokon belül pedig a fellépésre feljogosított szervet/szerveket. Kiemelt jelentőséggel kell kezelni azon motívumokat, amelyek az államok egy vagy több részfunkcióját, a társadalom és a gazdaság hétköznapi mechanikáját jelentősen veszélyeztetik, így kifejezetten azokat, amelyek a bűnszervezetekhez, terrorista csoportokhoz, valamint más államokhoz köthetők.

Max Kigler ennél földhözragadtabb felosztást dolgozott ki az ún. MEECES-elmélettel, amely hat különböző motivációt határolt el: a pénz (money), az ego (ego), a csoporthoz való

179 Hutchings (2013): 95.

180 A Barber információs hadviselésről ír tanulmányában, azonban az jóval szélesebb kört ölel fel, mint amire ő gondolhatott eme tárgykörben. L. bővebben: Kelemen (2017b): 117–122.

181 Barber (2001): 15.

182 Csíkszentmihályi (1997)

183 van Beveren (2001): 4–6.

184 Xu et al. (2021): 444–465.

csatlakozás igénye (entrance to social group), a személyes indítékok (cause), továbbá a szórakozás és a státusz (entertainment and status).[185] A szingapúri szerzők már ezt is ötvözve hét különböző motivációt különítenek el: a kíváncsiságot, a haszonszerzést, a hírnevet, a bosszút, a kikapcsolódást, a világnézetet és a szexuális ösztönt.[186]

A legátfogóbb motivációs térképet egy szerzői triász állította össze az ENSZ Régióközi Bűnügyi és Igazságügyi Kutatóintézete felkérésére. A hackerek – egyszerre akár több is – a következők motiválják: a kíváncsiság, a technológia szeretete, a bizonyítási vágy, a szórakozás, a problémamegoldás vágya, a technológia javításának a vágya, a hálózatok és gépek biztonságának a növelése, a szabadságjogok védelme, a szolgálatatások hozzáférhetetlenné tétele, a magánélet védelme, a rendszerellenesség, a lázad az állam szervei vagy a saját környezete ellen, a kalandvágy, az unalom, mert menő, a médiafigyelem, a düh és a frusztráció, a politikai okok.[187] Előnye ennek a felsorolásnak, hogy belevonja a társadalomra való pozitív hatás oldalát is hacker tevékenységének.

Mindamellett helyesnek vélem, hogy a fenti csoportosításokat egy saját megközelítés szerint összegezzem, amely azonosnak vélt kategóriákat összevon, de emellett rögzíteni kell, hogy egyes célzatok nem zárnak ki más célzatokat, tehát egy-egy hackernek ezek közül több motiváció is sajátja lehet. Következő motivációkat különítem el: a tanulás vágya; a kíváncsiság; a hírnév iránti vágy; a szórakozás; a hatalom érzete; a kihívás; a bosszú; a szexuális ösztön; a társadalmi/szubkulturális státusz; a világnézet: vallás, politika, ideológia, rendszerellenesség; a haszonszerzés; a nemzetállam szolgálata; az informatikai rendszer védelme. (lásd lenti ábra)

Hacker típus/ motiváció	tanulás vágya	kíváncsiság	hírnév iránti vágy	szórakozás	hatalom érzete	kihívás	bosszú	szexuális ösztön	társadalmi státusz	világnézet	haszonszerzés	nemzetállam szolgálata	informatikai rendszer védelme
script kiddies	–	+	+	+	+	+	–	–	+	–	+	–	–
tanuló	+	+	–	+	–	+	–	–	+	–	–	+	+
cyberpunk	–	+	+	+	+	+	+	–	+	+	+	–	–
old guard	–	+	+	–	–	+	–	–	+	+	–	+	+
rosszindulatú bennfentes	–	–	–	–	+	+	+	–	+	+	+	–	–
piti tolvaj	–	–	–	–	–	–	–	–	–	–	+	–	–
profik	–	+	+	+	+	+	+	–	+	+	+	+	+
nemzetállamok hackerei	–	–	–	–	–	–	–	–	–	+	+	+	+
hacktivista	–	–	–	–	–	–	–	–	+	+	–	–	–
kiberragadozó	–	–	–	+	+	–	–	+	–	–	+	–	–
digitális kalózok	–	–	–	+	–	–	–	–	+	–	+	–	–
crowsourcere	–	–	–	–	–	–	–	–	–	–	–	+	+
kiber bűnsegédek	–	–	–	–	–	+	–	–	+	–	+	–	–

1. ábra: Hacker típusok motivációs beosztása (saját szerkesztés)

185 Kilger (2015): 694.
186 Chng et al. (2022): 3.
187 Chiesa–Ducci–Ciappi (2009): 145–159.

A motivációkat összevetve a kibertér biztonságra gyakorolt hatásaival, valamint a hibrid konfliktusok alapjellemzőivel, látható, hogy a hackerek jól mozgósíthatóak egy-egy katonai szembenállás vagy hibrid szcenárió során.[188] A hactivisták a társadalmi, politikai törésvonalak mentén, akár direkt módon is hajlamosak lehetnek az államnak ártó kibertevékenység végrehajtására, valamint egyes szervezetek finanszírozásának kibertéri lebonyolítására. A gazdasági haszonszerzés célzattal működő szereplők elősegíthetik az ellenőrzött káosz kialakulását, mivel külső támogatással élve, felhasználók tömegeinek okozhatnak a kisebbtől a különösen jelentősig terjedő anyagi károkat. De az is lehetséges, hogy pontosan az ellenőrzött káoszt használják fel arra, hogy tevékenységüket a lehető leghatékonyabban hajtsák végre. Mivel a támadó fél eszközparkjába abszolút illeszkedik, hogy a politikai mellett a gazdasági környezetet is károsítsa, így kézenfekvő, hogy a ma már jelentősen digitalizált gazdaságba és kereskedelembe vetett fogyasztói vagy befektetői bizalmat leépítse, ezzel is elősegítve a gazdasági káosz kialakulását is. Emellett nem elhanyagolható az a körülmény sem, hogy mivel nemcsak a kibertér hat a hagyományos térre, hanem a hagyományos tér folyamatai is megjelennek a kibertérben, így a hagyományos térben megjelenő illegális csoportok (bűnszervezetek, terrorszervezetek) kibertéri cselekményeket is megvalósítanak, vagy még inkább a hagyományos térben elkövetett cselekményeket támogatják kibertéri cselekményekkel.

Ez az elmúlt évtized gyakorlatában tökéletesen ki is rajzolódott. A Hamász a 2010-es évek elején dezinformációs és a tömeghangulatot befolyásoló módszereket alkalmazott, izraeli és nem izraeli e-mail címekre és telefonokra küldött álhíreket tartalmazó e-mailekkel, szöveges üzenetekkel, valamint propaganda tartalmakkal. [189] Az Iszlám Állam már tovább fokozta ezt a tevékenységet: kifinomult és meglehetősen agresszív marketing kampányt folytattak, és magas szintre fejlesztették a kibertérben megjelenő pszichológiai hadviselést.[190] Pakisztáni terroristák 2008-ban pedig arra is rávilágítottak, hogy valós idejű információgyűjtésre és koordinálásra is alkalmas a közösségi média figyelése és az okostelefonon történő kommunikáció. [191] Ezeket a lehetőségeket az állami szereplők is felismerték, így saját hibrid terveik kidolgozása során e csoportok alkalmazásának a lehetősége, és kiemelten a kibertéri tevékenységük fokozása a listák élén szerepelt. A hagyományos tér terrorista csoportjai exportálják nézeteiket, ideológiájukat és tevékenységüket a kibertérbe.

> „A különböző fegyveres terrorista csoportok a politikai és katonai céljaik eléréséhez képessé váltak a világ teljes lakosságának megszólítására (…) A hagyományos műveleteik támogatására egyre jobban és eredményesebben használják fel az információs technológiák adta lehetőséget. A tapasztalatok dinamikus beépítése az alkalmazott műveletekbe, valamint annak széleskörű megjelenítése, propagálása mind a kibertér többrétű kihasználását tükrözi."[192]

A radikális szervezetek és tagságuk megjelenik a kibertérben is, és akár fel is használhatóak egy-egy hibrid szcenárió során. Ezen szervezetek hálózatalkotó képessége kimagaslóan re-

188 L. az orosz–ukrán háború esetében a mindkét fél álltal igénybe vett szabadúszó hackereket, amely során kiemelt figyelmet érdemel az ukrán IT Army felállítása: cfr.org/cyber-operations/ukrainian-it-army

189 Bachmann–Gunneriusson (2015): 82.

190 Hermann (2015)

191 Bachmann–Gunneriusson (2015): 83.

192 Magyar–Simon (2017): 58.

leváns, mivel nagyon jól felmérték a kibertér jelentette lehetőségeket.[193] A közösségimédia-platformokon keresztül ingyen, vagy elenyésző anyagi ráfordítás mellett tudják terjeszteni nézeteiket. Tökéletes példa erre a Notre-Dame-i tűzvész, amikor az orosz és kínai dezinformációs tevékenység mellett már a tűz estéjén a szélsőjobboldali Fdesouche.com azt kezdte el terjeszteni, hogy a bevándorlók által végrehajtott terrortámadás történt, amelyet több külföldi portál át is vett, [194] amelynek hatására széles tömegek reflexszerűen terrorakcióról[195] beszéltek, és sürgették a bevándorlás kérdésének megoldását.

Érdemes megemlíteni azt is, hogy a terrorista csoportoknak és szakadár szervezeteknek az 1990-es évektől alternatív bevételi forrásokhoz kellett jutniuk a tevékenységük finanszírozása érdekében, mivel a külső támogatók, így az Egyesült Államok vagy a Szovjetunió ekkor ebben már nem voltak érdekeltek. Így e csoportok a szervezett bűnözés lehetőségeit kihasználva jutottak bevételekhez, amely többek között lehetett kábítószerkereskedelem, műtárgyak illegális értékesítése, de kiberbűncselekmények megvalósítása is.[196] Ennek során nem egy kiberbűnöző – de más tagok is, vagy akár beépített szereplő[197] – került kapcsolatba nemzetbiztonsági szervekkel, és működött velük együtt. Ez különösen jellemző volt a posztszovjet térség államaira, így Oroszországra, Ukrajnára vagy Fehéroroszországra is.[198] Nem véletlen, hogy az oroszok rendkívül sikeresek voltak az ukránok elleni hibrid konfliktus során, hiszen tökéletesen tudták alkalmazni a korábbi évtizedek tapasztalatait és kapcsolati hálóját.[199]

Bűnszervezetek esetében két elkülönült típusú csoportról beszélhetünk. Az egyik csoportba tartoznak azok a szereplők, akik szinte tisztán kibertérben jelennek meg, vagy tevékenységünk főként ahhoz kötődik, a másik csoportot pedig a klasszikus bűnszervezetek alkotják, akik egyre inkább kihasználják a kibertér – lásd darknet – nyújtotta lehetőségeket. A motivációk közül kiemelendő a pénz, mivel a cselekmények túlnyomó többsége nyilvánvalóan haszonszerzésre irányul, emellett azonban a státusz megőrzése, fenntartása, esetlegesen kiterjesztése sem elhanyagolható.[200] Az is tetten érhető, hogy a kibertérben tevékenykedő bűnszervezetek mindegyike a hagyományos térben is realizálni kívánja a megszerzett előnyöket.

A fenti motivációkkal és képességekkel felvértezett szereplők a motivációjukhoz közelebb álló csoportokhoz könnyebben csatlakoznak, mintha a hagyományos térben kellene ezeket a tevékenységeket realizálni, hiszen a hackereknél is fennáll annak az ösztönző ereje, hogy az anonimitás valószínűsége jóval magasabb ezen tevékenységeknél is, mint a hagyományos

193 L. Malkovics (2013)

194 Makela (2019): 12.

195 L. a pszichológiai hatását és reakciókat bővebben: Kardos Gábor: Miért tűnik akkor is terrorakciónak a Notre-Dame tűzvész, ha nem az? azonnali.hu/cikk/20190415_miert-tunik-akkor-is-terrorakcionak-a-notre-dame-tuzvesz-ha-nem-az

196 Steenkamp (2017): 1–18.

197 Mészáros Bence (2019)

198 Ilyen volt például a Script nevű hacker, amely nagyobb hálózatot működtetett, de közben munkakapcsolatban volt az ukrán titkosszolgálattal. L. Turovszkij: (2020): 65.

199 Káncz Csaba: Az orosz titkosszolgálatok és a szervezett bűnözés ijesztő kapcsolatrendszere. privatbankar.hu/cikkek/makro/az-orosz-titkosszolgalatok-es-a-szervezett-bunozes-ijeszto-kapcsolatrendszere.html

200 L. például Olaszországban, ahol a rendőrség korábbi vezetője Alessandro Pansa, úgy fogalmazott: „A kibertér részévé vált a maffia mindennapi életének. Nem szabályozza senki, ellenőrzés sincs, és mi is most kezdjük észrevenni az itt történő bűnözés szofisztikált formáinak körvonalazódását." Ezt erősítik a korábbi olasz igazságügy miniszter Andrea Orlando szavai is: „Mikor a bűnszervezetek átköltöztetik a cégeiket egy bizonyos ágazatba, akkor az egész szektort magukhoz rántják." *Az olasz maffia is beszáll a virtuális bűnözésbe.* hirek.sk/kulfold/az-olasz-maffia-is-beszall-a-virtualis-bunozesbe

cselekmények esetében, továbbá az átlagnál nagyobb a siker valószínűsége. A támadások fejlesztése vagy új típusú eszközök alkalmazásának költsége pedig viszonylag alacsony a potenciális haszon, illetve okozható károk mértékéhez képest, amelyek amúgy jóval meghaladják a hagyományos térben okozható kár mértékét. Emellett a kiberterrorista akcióban való részvétel (esetleges haszonszerzési motívum mellett) azt az érzetet kelti az egyénben, hogy – a történelem során először – az egyén hatékonyan támadhat egy államot.[201] Tehát alkalmas eszköz a civilek mozgósítására, hiszen valójában úgy érezhetik, hogy a lebukás veszélye nélkül tehetnek valami olyat, amely tényleges befolyással bírhat a történelmi folyamatokra, segíthet megbuktatni a szembenálló államot vagy az ellentétes politikai nézeteket valló hatalom birtokosait.

3. A társadalmi hálózatok kibertéri evolúciója és hatásuk a biztonságra

Az eddigi fejezetek rámutattak arra, hogy a kibertér a hagyományostól eltérő térjellemzőinek, és az ahhoz kapcsolódó szociológiai hatásoknak is köszönhetően, valamint a gazdasági és biztonsági folyamatokba való rendkívül mély beágyazottsága révén átalakította az egyének hétköznapi életét, megváltoztatta a társadalmi hatóerejüket. Az átlagos felhasználóét sajnos negatív értelemben, azáltal, hogy sérülékenysége soha nem látott mértékben növeli a társadalmi sérülékenységet is. Gondoljunk itt csak az előző fejezetben felvillantott, 2021-es évben a kiberbűncselekményekből eredő, 6,9 milliárd dolláros globális kárra. Emellett pontosan ez az a szám, amely megmutatja, hogy az aktív egyéni szereplők – tehát a hackerek és a hozzájuk közvetlenül kötődő szereplők – tevékenységük révén mekkora mértékben hatnak a globális gazdasági, társadalmi és biztonsági alrendszerekre, és ezeken keresztül az állam működésére. A következő fejezetek arra kívánnak rámutatni, hogy a kibertérnek a jellemzői, és a benne zajló folyamatok miként befolyásolják a társadalmat és az államot, illetve azok biztonságát.

E fejezet a társadalmi hatások feltérképezéséhez egy relatíve fiatal diszciplinát hív segítségül a hálózatkutatás képében. E tudományterület csupán a 20. század második felében alakult ki, azonban a mögöttes hálózatelmélet históriája sem nyúlik vissza egy évszázadnál messzebbre. Ennek ellenére a hálózatkutatás egyik részterülete, a társadalmi hálózatok kutatása már historikus alapokon is megkezdődött, ugyanis főként a nyugati történelemtudomány felmérte a potenciálját annak, hogy az adott korszak folyamatait, eseményeit mélységében jobban megismerhetjük, teljesebb képet kaphatunk róluk, ha az adott korban élők viszonyrendszerét át tudjuk tekinteni.[202] E szemlélet segítséget nyújthat abban is, hogy a jelenkor kibertérhez erősen kötődő társadalmi hálózatait ne csak kvantitatív módon tudjuk jellemezni, hanem kvalitatív jellemzőit is felismerjük.

A társadalmi hálózat azonban, bár fogalmilag fiatalnak tekinthető, végigkíséri az emberi társadalmak történetét. Bár e hálózatok intenzitása, mérete, jellemzői jelentősen átalakultak az évszázadok során, de mindvégig befolyással voltak a közösség és az állam működésére, valamint a biztonságára. E hálózatok összekapcsolódtak a társadalmi totalitás más alrendszereivel, sőt egyes korszakokban kiemelkedő fontossággal bírtak a társadalmi totalitás egészében. Mint a társadalmi totalitás részkomplexuma, a társadalmi hálózatok is szükségszerűen

201 Kilger (2015): 694.
202 Kovács Bálint (2012): 188–190.

befolyásoltak, illetve befolyásolva voltak más részkomplexumok által.[203] Ilyen részegységnek tekinthető a fegyveres védelmi ágazat[204] (vagy annak egyes funkcióit megvalósító előképi szervek) is. A hadviselés generációinak vizsgálata során is láthatóvá vált,[205] hogy egyes társadalmi hálózatok az évszázadok során, a társadalmi struktúrához igazodva (gondoljunk a nemesi rendre mint társadalmi hálózatra és a nemesi inszurrekcióra)[206] mennyire eltérő szerepet töltöttek be a védelmi tevékenység tényleges megszervezése, működtetése során. Hasonló módon az általuk, vagy rajtuk keresztül használt egyes eszközök hatásfoka is eltérően alakult a korszak által biztosított technikai képességekhez mérten. Tökéletes példája ennek a hibrid konfliktusok és annak eszközparkja, amely lényegében – egészét tekintve – legalább évszázados, míg egyes eszközeire nézve, akár évezredes múltra tekint vissza. Ennek ellenére helyes az a megállapítás, hogy

> „amivel ma a hibridnek nevezett hadviselés vagy fenyegetés valóban újszerűnek tűnhet, az inkább a korábban is alkalmazott nem katonai tényezők tárházának robbanásszerű gyarapodásából és ezáltal kialakulni látszó stratégiai dominanciájából, illetve ezek hatóerejének a társadalmi- és technológiafejlődés miatti megerősödéséből következik."[207]

Kiemelendő e gondolatok közül, hogy a régi ismerősként kezelhető hibrid eszközpark sikeressége azokból a nem elhanyagolható körülményekből adódik, hogy egyik oldalról a modern technológia soha nem látott módon erősíti fel a korábbi eszközök hatékonyságát (lásd például az információs műveletek hatókörének bővülését), illetve másik oldalról a modern technológia jelentős hatást gyakorolt a társadalmi totalitásra, struktúrára és magukra a társadalmi hálózatokra is. Ahhoz azonban, hogy e hatást ne csak kvantitatív tudjuk elemezni, szükségesnek érzem a társadalmi hálózatok történeti vizsgálatát is, hiszen ezzel átfogóbb képet kaphatunk arról, hogy a társadalmi hálózatok mely jellemzői alakultak át a modern technológiának, dedikáltan a kibertérnek köszönhetően.

3.1. A társadalmi hálózatok és a társadalmi struktúra fogalmi, történeti vizsgálata

A társadalmi totalitás részkomplexumai közül e fejezetben részletesebben a társadalmi struktúra és a társadalmi hálózatok fogalmi rendszerével és történeti viszonyával foglalkozom, amelyek révén képet kívánok adni a társadalmi hálózatok tradicionális, prekibertéri fejlődéséről, jellemzőiről. Mindenekelőtt viszont érdemes azokat a fogalmakat tisztázni, amelyek a vizsgálódás alapját fogják jelenteni. Mind a társadalmi struktúra, mind pedig a társadalmi hálózatok rendkívül gyakran használt kifejezések. A sokszori alkalmazás és az interdiszciplináris jellegük miatt fogalmaik esetében már-már definíciós „bábeli sokféleségről" beszél-

203 Peschka Vilmos a jog mint részkomplexum esetében a következő módon fogalmazta ezt meg: „ha a jog mint a társadalmi totalitás egyik részkomplexusa létezik, akkor nyilvánvalóan rá nézve is érvényes az a társadalomontológiai törvényszerűség, hogy létét, helyét, működését és hatását… a többi részkomplexussal való szakadatlan kapcsolata határozza meg." – Peschka (1988): 33.

204 Farkas Ádám (2019a)

205 Kelemen (2020a): 65–81., Simicskó (2017): 3–16.

206 Keserű (2012): 14–25.

207 Farkas–Resperger (2020): 132.

hetünk.[208] E tanulmány keretei között célszerűnek tartom a hosszas fogalmi összevetések helyett olyan munkafogalmak átvételét, amelyek az egyes tudományterületeken átívelően képesek keretet adni a későbbi vizsgálódásnak.

A társadalmi struktúra – Farkas Zoltán fogalma szerint – kifejezi „az adott társadalom tagjainak társadalmi viszonyait és társadalmi helyzeteit, kiemelve e viszonyok és helyzetek leglényegesebb vonásait"[209]. E fogalomban a társadalmi viszony a társadalomban jelenlévő érdek- és erőviszonyok összességét jelenti. A társadalmi kapcsolat (helyzet) az egyének közötti tényleges, vagy hallgatólagos megállapodás, amely arra irányul, hogy ezáltal elősegítsék az érdekeik érvényesülését.[210] A társadalmi struktúra a fentiek alapján olyan intézményes és intézményes kereteken túli működési mechanizmusait öleli fel a társadalomnak (szűkebben az államnak), amelynek központi eleme az egyes egyének hatalomhoz való viszonyának definíciója, és e definíció mentén való társadalmi kapcsolatok (megállapodások) kialakítása. Ezzel szemben a társadalmi hálózatok sokkal lazább kereteket ölelnek fel:

> „[A] társadalmi hálózatot úgy értelmezhetjük, mint »a szereplők olyan csoportját, amelyek egymással valamilyen társadalmi kapcsolatban vannak« (…) Minden szereplő a hálózatban legalább két másik szereplővel van kapcsolatban (…) valamilyen közös célja, közös érdekeik vannak."[211]

Míg előbbi fogalom szükségszerűen összefonódik az állam hatalmi jellegével, addig utóbbi a társadalom akár lazább kapcsolódásait is felölei. Érdemes kérdésként megfogalmazni, hogy akkor egy, a társadalmi hálózatokat vizsgáló tanulmány keretei között miért jelenik meg a társadalmi struktúra kérdésköre is. A válasz erre a történeti vizsgálatban rejlik, ugyanis évszázadokon keresztül a társadalmi struktúra és a társadalmi totalitás szempontjából jellegadó, jellemző társadalmi hálózatok a legtöbb esetben egybeestek, de legalábbis rész-egész viszonyt jelentettek, amely – mint látni fogjuk – csak a modernitással kezdett megszakadni.

A korai társadalmak esetében, akár a nomád államról[212] beszélünk, akár a kora ókori államalakulatokról (ezt volt megfigyelhető a korai hellén időkben,[213] vagy mezopotámiai államfejlődés korai szakaszaiban is),[214] az alapvető vérségi viszonyon alapuló társadalmi hálózatok, vagyis a család, a nemzetség jelentették a társadalmi struktúra központi elemeit is. Hiszen ezen kapcsolatok mentén valósult meg az önfenntartás, a közösségi élet jelentette a fennmaradás egyedüli lehetőségét, e vérségi kapcsolatok léptek magasabb fejlettségi szintekre, így váltak törzsé, törzsszövetséggé, ahol a hatalom legitimációja továbbra is a vérségi kapcsolatokon nyugodott.

A feudális államfejlődés egyes szakaszaiban a szabadság kis körei[215] részére biztosított előjogok mentén szerveződő államban és a társadalomban ezen előjogokat birtokló szereplők kapcsolatai jelentették a társadalmi struktúra részegységeit, ezen előjogok birtokosai között

208 Kovács Bálint (2012): 190.
209 Farkas Zoltán (2019): 109.
210 Uo., 114.
211 Kovács Bálint (2012): 191.
212 Tőkési (1983), Kristó (2000): 116–120.
213 Szoboszlai-Kiss (2018), Szoboszlai-Kiss (2017): 95–116.
214 Jany (2016): 35–52.
215 Bibó (1979): 84.

alakultak ki a legfontosabb társadalmi hálózatok. E társadalmi hálózatok mindegyike érdekelt volt abban, hogy – bár a hatalom egyes szegmenseit a saját érdekeik mentén módosítsák (például Magna Charta mozgalom, az Aranybulla kikényszerítése, vagy a zsarnokölés kérdéskör̈e),[216] de – a status quo-t jelentősen ne alakítsák át, sőt abban az esetben, ha egy másik – a társadalmi struktúrában kevésbé jelentős – társadalmi hálózat azt érdemben támadta (például jobbágylázadás), akkor az ellen közösen léptek fel.[217] A korszak legjelentősebb teoretikusai ennek megfelelően az állami rendet és annak legitimációját úgy határozták meg, hogy ezen társadalmi hálózatok szerződést kötöttek egymással és/vagy egy külső szereplővel annak érdekében, hogy a fennálló társadalmi struktúrát meg tudják őrizni, vagyis az a közös célnak megfelelően működjön.[218]

Ebben tényleges változást a polgári forradalmakat követő átalakulások eredményeztek. Ekkortól a társadalmak tagjai sokkal inkább egyes uralkodó eszmék (liberalizmus, szocializmus, nacionalizmus, konzervativizmus), vagy más szemszögből a termelési tényezők megoszlása mentén szerveződtek. Egyre több és jelentősebb olyan társadalmi hálózat jött létre, amely a kialakult társadalmi struktúrában lényegében nem találta a helyét, perifériára szorult. Ebben az időszakban – ahogyan arra Wallerstein, Braudel, Szigeti és Pongrácz is felhívta a figyelmet[219] – kifelé bár egységesnek, homogénnek hatottak ezek az államalakulatok, és az imperializmus által vezetve kialakították a centrum-, félperiféria- és perifériaállamok egyfajta rendszerét, azonban belső társadalmi struktúrájukban legalább ennyire heterogének voltak. E heterogenitást pedig csak ideig-óráig tudta kezelni a hatalmi közeg, mivel vele szemben jelentős társadalmi hálózatok jöttek létre (munkásosztály és szervezetei, nemzetiségi törekvések), amelyek már ténylegesen tudták befolyásolni az állam működését és biztonságát, mondhatni helyet követeltek a Nap alatt. E társadalmi hálózatokat végső soron be kellett illeszteni a társadalmi struktúrába, emellett pedig ki kellett alakítani a védelmi jog azon intézményeit, amelyek jogállami keretek között kezelni tudták a szélsőséges törekvéseket.[220]

Ezen folyamatok mellett az egyre jobban kibontakozó globalizáció, az egyéni jogok térnyerése, a liberalizmus eszméjén alapuló individuum jelentőségének hangsúlyozása következtében az egyén szerepe felerősödött a társadalomban. A társadalmi hálózatok egyre inkább egyénközpontúvá váltak. Ami nem jelenti azt, hogy a társadalmi hálózat triádjellege innentől eltűnt volna, hanem sokkal inkább az látszik, hogy a társadalmi hálózat célja az egyén oldaláról vált definiálhatóvá, és ezek az egyéni célok értek össze. Ugyanis míg a feudális társadalomban a rendekhez tartozó egyének, bár nyilvánvalóan rendelkeztek saját, önálló célokkal, ezek viszont csak akkor voltak elérhetőek, ha a társadalmi struktúrában való helyzetük megkérdőjelezhetetlenül fennállt, amely a társadalmi hálózataik által definiált közös érdekek és célok mentén volt biztosítható. Az individuum térnyerése egyre inkább polarizálta a társadalmat, amelyben az egyén sokszor egyedül találta magát, ami nem egy esetben szélső-

216 Egresi (2016): 43., Szaniszló (2016): 75–77.

217 Büntetőjogi eszközparkot l. Barna (2017): 51–57., Barna (2013): 9–16.

218 Takács (2016): 43., Pongrácz (2019a): 33–35., Pongrácz Alex: A Leviatán mint politikai szimbólum az államelméleti gondolkodásban. *Ludovika kormányzás és tudomány blog,* 2022.04.12. ludovika.hu/blogok/kormblog/2022/04/12/a-leviatan-mint-politikai-szimbolum-az-allamelmeleti-gondolkodasban/, Pongrácz (2017a): 171–174., Pongrácz (2018b): 131–135.

219 Braudel (2008), Wallerstein (2010), Szigeti (2005), Pongrácz (2014a): 275–291., Pongrácz (2019a)

220 L. a jogállami különleges jogrendi szabályanyag kialakulását: Farkas Ádám (2019b), Kelemen (2022a): 4–59., Kelemen (2020b): 43–79.

séges válaszokat szült (eklatáns példái ennek az egyes terrorcselekmények). A másik oldalról azonban a vélemények ütköztetése sokszínűbbé vált,[221] a társadalmi felelősség pedig egyre inkább tartalmat nyert olyan társadalmi hálózatok képében, amelyekben a célok sokszor jóval túlmutattak a hálózat tagjainak érdekein, és magasabb szintű társadalmi jó érdekében léptek fel. Ilyen társadalmi hálózatok voltak azok, amelyek többek között követelték a rabszolgaság eltörlését, vagy a gyermekmunka betiltását, szervezték az árvasegélyezést – és még hosszasan lehet sorolni a 19–20. század ezen társadalmi hálózatait.[222] A második világháború idején, majd befejezése után azt értékelve újradefiniálták az egyén szerepét a társadalomban, úgy vélték, hogy az ember „ csak saját lendületében, mintegy saját hajánál fogva tudja kihúzni magát a semmiből és tud védekezni a semmi szakadatlan fenyegetése ellen (…) És az ember nemcsak magának és magáért felelős, hanem egyben mindig a másiknak és a másikért."[223] Az interszubjektivitás – mely fontossága a második világháború során vált igazán világossá – révén az ember próbálja megismerni és alakítani a társadalmi, politikai életet, így a mikroszint aktívan reagál a makroszint eseményeire.[224] Amely lényegében annyit jelent, hogy az ember annyit tesz, hogy „amit meg kellett tenni, és amit a terror és lankadatlan fegyvere ellen meg kell majd tenniük, egyéni meghasonlásaik ellenére",[225] azt megteszik. Vagyis az egyén létezését önmagán túli érdekek fölé is emeli, kiemelve, hogy az egyén létezése társadalmi realitás is egyben, így az egyén már nemcsak szűk értelemben vett közösségre van hatással, hanem a társadalmi struktúrára is.[226]

Eme felismerés a nyugati társadalmak esetében lehetővé tette, hogy a társadalmi hálózatok következetesen végig próbálják vinni céljaikat, akár a legitim társadalmi struktúra kárára is. Utóbbi viszont már jelentős társadalmi és nemzetbiztonsági kockázatokkal is járt. Számos példa közül kiemelhető például a német RAF csoport tevékenysége.[227] A 20. század második felére tehát egyértelműen kimutathatóvá vált, hogy azok a társadalmi hálózatok is képesek jelentős hatást gyakorolni a társadalmi totalitásra, amelyeknek a társadalmi struktúrában már nincs jelentős szerepük. E társadalmi hálózatok kiszélesítették a demokratikus nyilvánosságot, vagy valós társadalmi problémákat próbáltak megoldani (gondoljunk itt például a polgárjogi mozgalmakra az Egyesült Államokban), azonban szélsőséges esetekben reális veszélyt jelentettek a biztonságra.

221 Gosztonyi (2022): 55–58.

222 Szépvölgyi (2021): 316–323., Szépvölgyi (2020): 101–116.

223 Störig (2005): 483.

224 Pongrácz (2021a): 141–158.

225 Camus (1965): 387.

226 Ezt érzékelteti David Mitchell Felhőatlasz című művének záró monológja: „Hohó, ezek valóban szép whig érzések, Adam. De ne papolj nekem igazságról! Ügess szamárháton Tennesse–be, és győzd meg a déli fehér fajankókat, hogy ők csupán kifehérített négerek, a négereik pedig befeketített fehérek! Hajózz az Óvilágba, mondd el nekik, hogy császári rabszolgáik jogai elidegeníthetetlenek, akár Belgium királynőjéé! Ő, be fogsz rekedni, szegény leszel, és megőszülsz a jelölőgyűléseken! Leköpnke, rád lőnek, meglincselnek, megbékítenek kitüntetésekkel, elkergetnek a telepesek! Keresztre feszítenek! Naiv, álmodozó Adam. Aki hadakozna az emberi természet sokfejú hidrájával, a fájdalom valóságos világával fizet, és vele együtt fizet a családja is! És utolsó leheleteddel érted majd meg, hogy az életed nem ért többet a határtalan óceán egyetlen cseppjénél!
Ámde mi az óceán, ha nem cseppek sokasága?" Mitchell (2012): 323.

227 Papp László Tamás: Miért lett fiatal német értelmiségiekből kegyetlen terrorista a diáklázadás idején? szakirodalom.atlatszo.hu/2020/07/16/miert-lett-fiatal-nemet-ertelmisegiekbol-kegyetlen-terrorista-a-diaklazadasok-idejen/

A fenti változások mellett viszont e társadalmi hálózatoknak több közös jellemzője is kimutatható. Egyik ilyen jellemző a lokális jelleg, vagyis ezen hálózatok földrajzilag körül határolható, egymáshoz közel eső területen élők között jöttek létre. Így általában lokális célok és érdekek mentén szerveződő egyének hoztak létre társadalmi hálózatokat. E társadalmi hálózatokban az egyének közötti kapcsolatok intenzívek voltak, a bizalom a közös lokális ismeretségen nyugodott. A földrajzi térben nagyobb területet felölelő hálózatok esetében a bizalom és az intenzitás jóval csekélyebb volt, gyengébb kapcsolatok jöttek léte.[228] A hagyományos vagy lokális hálózatok zártak voltak, amelyek erősen védték a határaikat, és emiatt nehezen fogadtak be új tagokat. Ezen társadalmi hálózatok méretüket tekintve kötődtek a helyi szinthez, vagyis a hálózathoz csatlakozók száma lehatárolt volt. A tagok kapcsolata erős volt, így fluktuáció elhanyagolható mértékű volt. A kapcsolati háló sűrű szövésű volt, a tagok közvetlenül ismerték egymást, amihez hozzájárult a nyilvános terek kiemelt szerepe.[229] A 19. századig a technológia fejlettsége determinálta a társadalmi hálózatok java részében a szűk értelemben vett lokalitást, hiszen az emberek többsége falusias környezetben élt, amelyet élete során alig hagyott el, akkor is leginkább a szomszédos településeket érték el. Ez az arány csupán a 19. század közepén billent át Nyugat-Európában.[230] Számos technológiai változás volt hatással az egyén társadalomban betöltött helyére, szerepére, így a nyomtatott sajtónak a századfordulóra jelentős mérvű térnyerése volt megfigyelhető (ami az oktatás prioritássá válásából következő csökkenő analfabetizmusnak is köszönhető), valamint a távközlés, a közlekedés területén tapasztalható robbanásszerű technológia fejlődés, valamint a gazdasági átalakuláshoz köthető jelentős urbanizáció kiemelték az egyént a lokálisan szerveződő közösségből. E közösségre jellemző rendkívül erős köteléket és sűrű szövésű kapcsolati hálót egyre inkább felváltotta a flexibilis, laza szövésű gyengébb kötelék, illetve a közös érdekekre épülő hálózatok.[231] Ezek társadalmi struktúrára gyakorolt hatása fokozatosan erősödött a lokális jelleg leépülésével párhuzamosan, így már a 19. században is tetten érhető volt a társadalmi struktúra torzulása, azonban lényeges változásokat csak a második világháború hozott. Mindemellett meg kell jegyezni, hogy ez régiónként eltérő dinamikát öltött annak fényében, hogy a lokális jelleg milyen ütemben gyengült meg az adott nemzetállami társadalmi totalitásban.

Már itt is jelentős átalakulása figyelhető meg a hálózatoknak, hiszen megjelent a közös érdek és érdeklődés mint a hálózati szerveződés mozgatórugója. Ezen állítás még akkor is igaz, ha a korszak tömegszervezeteire gondolunk, akár a munkásmozgalmakra, akár a tömegpártokra, hiszen bár központi szereplőt követtek, azonban ezek a szervezetek továbbra is földrajzilag lehatárolható társadalmi hálózatokra épültek, amelyeket a centrumból próbáltak irányítani, mozgatni. Nem véletlen, hogy a forradalmi munkásmozgalmak legtöbbje lokális társadalmi hálózatokra épült, és azok összességét tekintették a legfőbb szervnek.[232] Még akkor is, ha valójában ezek vezetőinek komplexuma egy saját társadalmi hálózatot képezett.

A szűken vett lokalitáshoz kötött jellemvonás még, hogy a közösségen belül a *magatartási minták terjedése lineáris volt, vagyis diadikus* a mintakövetés, ami annyit jelent, hogy egy-egy ilyen magatartási minta kizárólag egyenes vonalban tud terjedni, két ismerős között. Ez egy

228 Kovács Bálint (2012): 194.
229 Vályi (2004): 50.
230 Hobsbawm (1988): 16–17., Armour (2012): 15–19., 22–27.
231 Vályi (2004): 47.
232 Nagy Szabolcs (2020): 9–27., Nagy Szabolcs (2016)

nagyobb társadalmi hálózat esetében hiperdiadikus jelleget ölt, vagyis a cselekvési mintákat már nem lineárisan veszik át az egyének, hanem a hálózaton belül bármilyen formában terjedhetnek ezek a sémák, vagyis ismerős ismerősén keresztül is. Fontos, hogy ezen hálózatok még mindig lehatároltak voltak, vagyis az egyes minták terjedése visszakövethető volt.

Az utolsó jellemzője a prekibertéri társadalmi hálózatoknak, hogy az egyén felől jellemezhetők voltak. Bár a fentebb felvillantott egyes társadalmi hálózatok esetenként heterogének voltak, azonban az egyéni jellemvonások így is visszaadták a hálózat makrovonásait. Hiszen ezen egyének hálózatai vagy a társadalmi struktúrához kötődtek, vagy lokális célok, attitűd mentén szerveződtek, illetve jól körül fogható ideológiai közösséget alkottak. Előbbi és utóbbi esetében a status quo fenntartása, illetve változtatásának az igénye szükségessé tett egyfajta homogenitást még heterogén közegben is, míg a lokális jellegű hálózatok esetében alapvetően homogén hálózatok voltak a jellemzőek. Szintén az egyén felöli meghatározhatóságot erősítette a magatartási minták diadikus vagy hiperdiadikus terjedése is, ugyanis a közösséghez mérten szélsőséges minta terjedésének bázisa visszakövethető volt.

3.2. Társadalmi hálózatok a kibertér vonzásában

Az elmúlt közel fél évszázadban – a posztfordista új gazdasági mechanizmus megjelenésétől – azonban ugrásszerű változás következett be a társadalmi totalitás egészében, amely nem hagyta változatlanul az egyes részkomplexumokat, így a társadalmi struktúrát és a társadalmi hálózatokat sem. Alvin Toffler elmélete szerint az emberi történelem három hullámra osztható. Az első hullámban a gazdasági termelés alapja a földművelés, ahol – mint fentebb is láttuk – a társadalmi struktúra és a leginkább jellegadó társadalmi hálózatok egybeestek. A második hullámot az ipari társadalom korának tekinti. Ezen időszakban felerősödött az egyén társadalmi szerepe, a társadalmi hálózataiknak hatóereje már nem feltétlenül függött a társadalmi struktúrában betöltött helyüktől. Végül a harmadik hullámot jelentve megjelent az információ kora, vagyis az információs társadalom térnyerése.[233] Fontos elméleti alapja volt annak a felismerése, hogy az információ, illetve az arra épített tudás a társadalmi struktúrában betöltött szerepet, viszonyokat alapjaiban határozza meg.[234] Ugyanis az információ már önálló értékké vált, annak megszerzése és birtoklása tett valakit, illetve valakiket tényleges hatalmi tényezővé. E folyamatban a technológiai robbanás mellett óriási szerepe volt a globalizáció kiteljesedésének is. E körben „a globalizációt akként gondolhatjuk el, mint a jelenkori társadalmi élet világméretű összekapcsoltságának szélesedő, mélyülő és gyorsuló valóságát, annak kulturális, kriminális, pénzügyi, spirituális, és számos egyéb aspektusával."[235] Ehhez viszont elengedhetetlen attribútummá vált a kibertér, tudniillik a kibertér kiépülésének köszönhetően váltak ténylegesen globálissá az emberi interakciók, a gazdaság és a kultúra. Fontos felismerés, hogy a technológia önmagában nem határozza meg a történelmi fejlődést és a társadalmi változásokat, viszont a technológia felhasználásának, vagy fel nem használásának a módja megmutatja egy társadalom alkalmazkodási képességét.[236] Egyes államok e

233 Toffler (2001)
234 Machlup (1962), Z. Karvalics (2009): 20–34.
235 Pongrácz (2018a): 43.
236 Castells (2010): 7.

technológia révén elmozdultak egy orwelli világ irányába, más társadalmak mindeközben megpróbálták a technológia pozitív, jólélti funkcióit hangsúlyozni, és továbbra is erős gátak között tartani az állami információéhséget.[237] Így egyre nagyobb teret nyertek az államoktól elkülönült szereplők.

> „Korunkra a nemzetállamok riválisaivá nőtték ki magukat többek között a tőke-, a termelési, a kommunikációs, bűnözői hálózatok, a nemzetközi intézmények, a szupranacionális katonai gépezetek, a nem kormányzati szervezetek, a nemzetek feletti vallások, sőt, még a különböző társadalmi mozgalmak is."[238]

A tudás (és információ)-intenzív társadalomban tehát az állam másodlagos szereplővé kezd válni a transznacionális tényezők mellett (tekintsünk e körben a közösségimédia-platformok tevékenységére irányuló állami szabályozás kialakításának eredendő lehetetlenségére). Furcsa kettőssége ennek társadalmi oldalról, hogy az állam információhoz jutását korlátozzák és hangosan tiltakoznak egy-egy hírszerzési kiszivárgás esetében (lásd Wikileaks, Snowden-ügy), de eközben a többség a hallgatásba burkolózik azzal kapcsolatban, hogy

> „az információ (…) kifürkészése és az adatok felhasználók hozzájárulásával, de az átadott adatkör mélységére és súlyára kiterjedő átfogó ismeret hiányában történő rendelkezésre bocsátása a legnagyobb tech-cégek részére milyen visszaélési lehetőséget biztosít akár (…) az Amazon, a Facebook és a Google"[239]

számára. Ezzel a társadalmi struktúra – amely korábban maximum nemzetállami értelmezést jelentett – annak az igénynek megfelelve, vagy azt felhasználva, kiszolgálva, hogy az állam hatalmi tényezőként a másodvonalba kerüljön, valamint annak köszönhetően, hogy életünk minden területe lényegében összekapcsolódott és a szerveződés világméretűvé vált, így már sokkal inkább értelmezhető transznacionális vagy globális közegben, semmint államon belül. Ez a társadalmi struktúrát megkettőzi, és a nemzeti társadalmi struktúra mellett kialakul egy transznacionális vagy globális társadalmi struktúra is. Ebből adódóan viszont az egyének társadalmi hálózatainak is e kettős struktúra irányába kell igazodniuk, amely már eredendően konfliktusok forrása, és a nemzeti társadalmakon belüli törésvonalakat eredményez.

Tovább fokozzák ezt az állapotot a kibertér alapjellemzői, valamint a diszruptív technológiák, ugyanis átalakították az emberek hétköznapjait, a szolgáltatóközpontú gondolkodás átvette az uralmat a korábbi tradicionális működés felett. Az IoT vagy IoD[240] rendszerek már szükségszerűen módosították az emberek egymás közötti, és az ember-gép közötti, sőt a gép-gép közötti interakciókat is. Ezzel a kibertér egyértelműen képes befolyásolni az éntudatot, képes azt módosítani, „átprogramozni". Mindez azért alakulhat így, mert a kibertér egyes szegmensei lényegében szándékosan úgy vannak tervezve, hogy az egyén sajátos világnézete, érdeklődési köre, tervei, céljai, függőségei mentén kapjon információt, érjen el felületeket, jusson hozzá kapcsolódó termékekhez. Lényegében a közösségimédia-platformok ezen fel-

237 Pongrácz (2022): 3–8.
238 Pongrácz (2014b): 158.
239 Farkas Ádám (2022a): 41.
240 Baranyi et al. (2021a): 225–240., Baranyi et al. (2021b): 91–104.

ismerés mentén szervezik saját üzleti modelljüket. Mindez úgy történik, hogy ez a speciális közeg új esélyt kínál az egyénnek: egy más közösséghez tartozást, a lehetőségek tárházát, akár úgy is, hogy látszatra a hagyományos létezése nem változik, valójában azonban teljesen felülírja azt. Tudniillik a kibertér „lehetővé teszi, illetve hatékonyan támogatja a közösségek spontán szerveződését."[241] Minden adat, minden eszköz és minden személy valós időben elérhetővé vált a világ bármely pontján, amely nyilvánvalóan átalakította a társadalmi hálózatok dinamikáját is. Hiszen ezzel lényegében egy-egy nagyobb társadalmi hálózat sohasem alszik, vagyis a kapcsolatok egy része mindig aktív magatartást tanúsít, mindig képes arra, hogy a célnak megfelelő reakciót adjon egy-egy felmerülő jelenségre, hírre, információra, és akár ennek megfelelően „riassza" a hálózat többi tagját. A kiberteret – legalábbis érzetre – az időbeli és térbeli korlátlanság, az azonnaliság, a mindenhol ottlevés jellemzi és a csatlakozás önkéntessége,[242] vagy annak a látszata, így a

> „cyberkörnyezetben csökken az ítélőképesség és nő az impulzivitás, némileg hasonlóan ahhoz, ahogyan az alkohol hat ránk. A cyberközeg sajátos jellemzői – a külső kontroll vagy felügyelet hiánya, a névtelenség, a távolság, a fizikai elkülönültség érzete – elősegítik a gátlások levetkőzését."[243]

Ez a kontrollvesztés önmagában növeli az ismeretlenek közötti szindikalizáció lehetőségét. Mivel a kibertér lehetővé teszi az egyéni kapcsolatok bővülését, akár a személyes, akár a karrierépítés területén, emellett elősegíti a különböző régiók együttműködését.[244] Ez egy olyan robbanásszerű kvantitatív változást jelent, amely ennek köszönhetően kvalitatív jellemzőit is módosítja a társadalmi hálózatoknak. Ugyanis az új hálózatok méretüket tekintve minden korábbi társadalmi kapcsolati hálót meghaladnak, számuk és méretük folyamatosan gyarapodik. Ehhez hozzájárul, hogy míg korábban a közösség egy földrajzilag jól lehatárolható területre összpontosult, és ezen belül tudtak kialakulni az azonos elvek mentén cselekvő személyek kapcsolatrendszerei is, mára ez átalakult. Így bár a hagyományos térben az egyéni kapcsolatok visszaszorulása, elsorvadása figyelhető meg, addig a kibertérben az emberi létezés fokmérője a hálózathoz tartozás lett.[245] Mindemellett viszont az is tényszerű, hogy ezek a társadalmi hálózatok is térbeli és társadalmi kötöttségűek. Az online közösség kiépülésében a térbeli tényezők is lényeges jelentőséggel bírnak. Két véletlenszerűen választott egyén esetében, ha nagyobb a földrajzi távolság, akkor kisebb az esélye, hogy tagjai legyenek egyazon hálózatnak. Ha mégis, akkor érdeklődési körük hasonló. Ebből adódóan a kibertéri kapcsolatok javarészt az offline kapcsolatok átemelései, így „az online közösségi hálók a valódi világ hálózatainak torzult, módosított változatai."[246]

E torzulást az adja, hogy a társas kapcsolatok mélységét szélességre cserélik, vagyis a személyes kapcsolatot sok esetben felváltják az online kapcsolatok. Így ezek a hálózatok kvantitatív nagyobbak, azonban kevésbé mélyek, kevésbé jellemző rájuk az érzelmi és értelmi racionalitás. Az érzelmi jólét megteremtéséhez már nem a kapcsolatok kvalitatív jellege dominál,

241 Vályi (2004): 48.
242 Klement (2015): 118–119.
243 Aiken (2020): 35.
244 Jain–Sahoo–Kaubiya (2021): 2157–2158.
245 Pintér Róbert (2007): 25.
246 Coget–Yamauchi–Suman (2002): 184.

hanem azok szélessége, ezáltal a kibertér gyengíti az emberi kapcsolatok minőségét,[247] és a társadalmi kohézió csökkenéséhez vezet.[248] Aminek köszönhetően csökken a társadalmi normákat közvetlenül átadó, fenntartó közösség szerepe is.[249]

Az alaptényezője változik meg mindezek által a társadalmi hálózatnak, hiszen korábban a társadalmi hálózatok bizalmi oldalát a lokalitás, a kölcsönös ismeretség adta, ebből adódóan voltak erősek a kisebb helyi hálózatok és gyengébbek a nagyobb, regionális vagy országos hálózatok; ez viszont átalakul, mivel ezeknél a hálózatoknál a hálózat erőssége már nem földrajzilag körülírható, sokkal inkább a benne megjelenő erősebb individuumok jelenléte, vagy egy mindenek fölé helyezett cél primátusa jelenti az összetartó és bizalmi kapcsolatot. Erős vezető(k), tagok vagy egy vallásként tisztelt cél rendkívüli kötőerőt jelent ezekben a hálózatokban. Előbbiek maguk determinálják a hálózat makrotulajdonságait, utóbbi viszont a tagok kollektív tudata mentén alakulhat, mert egy magasztos cél lehet pozitív, de szélsőséges mentalitással társulva biztonsági kockázatot is jelenthet. Utóbbiak megfigyelhetőek voltak a korábbi társadalmi hálózatok esetében is, azonban itt – ha emellé rendeljük a kvantitatív és technológiai jellemzőket is, valamint a társadalmi struktúra egy részének a társadalmi totalitáson kívülre kerülését, amely lehetővé teszi az egyes cselekmények relativizálását – lehet olyan cél, amit a belső társadalmi struktúra ellenérzéssel fogad, míg a külső akár támogat is (erre alkalmas példa lehet a migrációval kapcsolatos állásfoglalások, Black Lives Matter mozgalomra és utóhatásaira adott eltérő válaszok). Így a hatalmi viszonyban lévők részéről érzékelhetően jelentősebb potenciállal/kockázattal bíró hálózatok rajzolódnak ki, amit a lentebb ismertetésre kerülő tulajdonságok tovább erősítenek.

Tovább vizsgálva a hálózatokat formáló körülményeket, meg kell állapítani, hogy a kibertér növeli a kialakított hálózatok testreszabottságát is, mivel a kialakult közösségek tagjai közötti interakciók a kibertérnek köszönhetően már országhatárokat, sőt kontinenseket is átlépnek. A hasonlóan gondolkodó egyének határok nélkül tudnak kommunikálni, egymással információkat megosztani, csoportokat létrehozni, közösségeket szervezni. Ami tovább erősíti a határokon átnyúló társadalmi struktúráknak a hatalmi pozícióját, hiszen lehetőséget ad, hogy akár információs műveletek mentén alakíthassák egy-egy társadalmi hálózat szemléletét.

Ezzel párhuzamosan pedig nyilvánvalóan fokozódik ezeknek a hálózatoknak a közösségformáló szerepe. Hozzájárul ehhez a hálózatok hiperdiadikus jellege is. A hagyományos térben a viselkedési minták átvétele családtagok, barátok, osztálytársak, kollégiumi szobatársak stb. szokásainak másolásával történik meg, vagyis egy-egy viselkedési minta terjedése a legtöbbször lineárisan valósul meg. Ha ez a lineáris lánc megszakad, akkor ennek az új magatartási formának az átadása is meghiúsul. Azonban a hiperdiadikus terjedés egy szervezetben, így például egy munkahelyen, kollégiumi közösségben, egyetemen már horizontálissá válik, bonyolultabb, és nehezebben visszakövethetőbbek a hatások, viszonthatások. Akkor ezt most helyezzük át a kibertérbe, ahol a hálózat tagjainak száma több ezerre, tízezerre, sőt akár millióra is emelkedhet. A minta terjedése így már nem egyszerűen hiperdiadikus, hanem szuper hiperdiadikus. Itt egy-egy viselkedési minta átadásához, vírusszerű terjedéséhez nem

247 Molnár–Kollányi–Székely (2007): 64.
248 Peikari–Lotfi –Makhdomi (2015): 48.
249 Jakobi–Lengyel (2014): 43.

kell az, hogy minden szereplő azt magáévá tegye, támogassa, elsajátítsa.[250] Az így kialakított hálózatoknak létrejönnek olyan tulajdonságai és funkciói, amelyek az egyéntől elszakadnak, azokra nincsen valós befolyásuk.[251] Hozzájárul ehhez a kibertérnek a gátlásokat háttérbe szorító jellege, valamint az is, hogy egyes csoportokon belül eltérő aktivitású, eltérő célú és eltérő végletekben gondolkodó szereplők vesznek részt. Ezekből adódóan a kibertérben létrejövő kapcsolati hálózatokban az egyén radikalizálódása rendkívül felgyorsul.

Az egyén radikalizálódása a csoporton belüli aktivitás fokozódása mellett a csoporton túlra ható (kiber)tevékenységekben figyelhető meg, így például közösségi oldalakon történő toborzás, az elveiknek, nézeteiknek megfelelő hírek terjesztése, saját nézeteik igazolása, akár – még nem hagyományos értelemben vett – agresszív módon is. A kontrollt vesztett egyén a legtöbb esetben ezzel az agresszióval még jogi normát nem sért. A kiberagresszió fogalma viszont rendkívül szemléletes:

> „A cyberagresszió úgy értelmezhető, mint minden olyan, az egyén negatív érzelmeiből fakadó, cybertérben megnyilvánuló manifesztáció, ami magára a cselekvőre vagy másra nézve negatív hatású, vagy valamely normát sért, de még nem tartalmazza a fenyegetést és a kényszerítést, hanem azok megelőző, bevezető szakasza"[252]

Mindez kifejezésre juttatja, hogy az egyén itt lépi át a Rubicont, vagyis teszi meg az első olyan lépéseket, amelyek a későbbi, már akár bűncselekményi tényállást megvalósító cselekményhez vezethetnek. Sajnálatos módon a kibertér gátlásmódosító hatása okán az elkövető legtöbbször – bár hagyományos térben legtöbbjük ilyent nem tenne – nem is érzékeli, hogy rendkívüli mértékben átlépte az emberek között kialakult kommunikáció hétköznapi normáit.

A radikalizálódása a hálózathoz kapcsolódó szereplőknek eltérő fokozatot ölt, pontosan abból adódóan, hogy eltérő magatartási mintákat vesznek át a szereplők a csoport többi tagjától. Eltérő lesz az is, hogy miként viszonyul egy-egy tag a belső vagy külső társadalmi struktúrához, vagy azok mindegyikéhez. Ugyanis már a korábbi történeti közegben kialakult az az ereje az egyes társadalmi hálózatoknak, hogy a társadalmi struktúrában kevésbé jelentősek is hatni tudnak a kialakult társadalmi viszonyrendszerre. Így az a társadalmi hálózat, amely a belső társadalmi struktúrával szembehelyezkedik, de a külső társadalmi struktúrát támogatja, lehetőségként jelenik meg a külső tényezők számára, mégpedig olyan lehetőségként, amely később támogatható, erősíthető társadalmi töréspontot eredményezhet. Emellett a mindkét struktúrát bíráló, támadó és tagadó hálózatok radikalizálhatóságában rejlik a legnagyobb potenciál, hiszen ezen csoportok kisebb ráfordítással is szélsőséges radikalizmusra hajlamosak.

A fentiek okán megállapítható, hogy ezek a szuper hiperdiadikus mintakövetésen alapuló nagyméretű hálózatok esetében, a hálózat méretéből adandóan kevésbé jellemző a homogén magatartási minták átvétele. A csoport attitűdje, a radikalizmusának szintje tehát nem az egyén felől határozható meg, mivel „a kapcsolati hálóknak makrószintű tulajdonságai vannak. A mak-

250 Gondoljunk bele, a közösségi hálón mennyi olyan „kihívással" (ilyenek voltak többek között a dezodor–, a koronavírus–, a koponyatörő–, a kiki–, vagy a tüzes–kihívás) találkoztunk az elmúlt években, amely a digitális közösséghez tartozó egyének legtöbbjét sokkolta, azonban mégis óriási számú követőre talált. L. bővebben: Coronavirus challenge és a legveszélyesebb netes kihívások, 2020. blog.generalielorelatok.hu/biztonsag/coronavirus–challenge–es–veszelyes–internetes–kihivasok/

251 Christakis–Fowler (2010): 38–41.

252 Kiss Tibor (2020): 28.

roszintű tulajdonságok olyan, az egészre jellemző új vonások, amelyek a részek közötti kölcsönhatásokra és köztük fennálló kapcsolatokra vezethetők vissza."[253] Ez pedig adódik a kvantitatív jellemzőkön túl abból is, hogy az egyes tagok a korábban meghatározott célok mentén eltérően reagálnak a társadalmi struktúrákra. Ez a makrotulajdonságok mentén való definiálhatóság realizálja azt is, hogy a szereplők egy része erős szálak mentén kapcsolódik a hálózat egészéhez, emellett viszont az igazán kiemelkedő biztonsági kockázatot jelentő hálózatokhoz sok gyenge szálú kapcsolat is tartozik. A gyenge szál az, amelynek „hozzáadása vagy elvétele nem befolyásolja statisztikailag kimutatható mértékben a hálózat külső paramétereit."[254] Ez azért kell, mert a gyenge szálak stabilizálják a hálózatot. Ez ezen társadalmi hálózatok esetében azt jelenti, hogy van egy magja (erős szálak) a közösségnek, akik meghatározzák a makro jellemzőket, ők a csoport vezetői, aktivistái, a kifejezetten aktív és radikalizálható tagok. Viszont a hálózat megfelelő dinamikájához sok gyenge kapcsolat szükséges, mivel ebben az esetben a szereplők sűrűn kötődnek egymáshoz, így kisebb a fluktuáció, a hálózat integrált, egészként viselkedik és stabil. Amint a gyenge szálak száma megcsappan, úgy csökken a tagok kötődése, ez növeli a fluktuációt, amely eredményeként a hálózat részekre szakad.[255] Tehát egy erős kibertéri társadalmi hálózat esetében legalább olyan fontosak a gyenge szálak, mint az erősek, hiszen növelik a hálózat kohézióját. Azonban, ha szélsőséges radikalizmus irányába akarják elmozdítani – például egy hibrid szcenárió részeként – az adott hálózatot, akkor a gyenge szálak számát vissza kell építeni, ugyanis „ha a rendszer túl stabil, akkor nem fejlődik, nem mozog".[256] Ebből adódóan egy társadalmi hálózat stabil és hosszútávú működéséhez elengedhetetlen a nagyszámú gyenge szál léte, azonban a makrotulajdonság szélsőséges irányba történő elmozdítása esetében a számukat leépítik, mivel így könnyebben alakítható a teljes hálózat makrojellemzője.

A fentiek összessége rámutat arra, hogy míg korábban a jelentősebb társadalmi hálózatok vagy közvetlen kapcsolatban voltak a társadalmi struktúrával, vagy törekedtek arra, hogy abba beolvadjanak, addig az elmúlt évtizedekben ezen hálózatok egy része kimondottan alkalmassá vált arra, hogy ezen struktúrák valamelyikét felszámolja.

Melyik társadalmi hálózat tud ilyen potenciált magában hordozni? Érdemes itt idézni a világhírű magyar hálózatkutató, Barabási Albert László szavait:

> „Igen, tényleg van szólásszabadság a hálón. Azonban annak nagyobb a valószínűsége, hogy hangunk túl gyenge ahhoz, hogy meghallják. Azokat az oldalakat, amelyeknek csak kevés bejövő mutatója van, lehetetlen véletlen barangolással megtalálni. Ehelyett örökké a középpontokhoz vagyunk irányítva."[257]

Ezen következtetést erősíti a korábban már ismertetett Avaaz-jelentés, amely a 2020-as amerikai elnökválasztással kapcsolatos dezinformációt dolgozta fel, és rámutatott arra, hogy a Meta állásfoglalása ellenére mekkora volumenű dezinformációt valósítottak meg (162 milliós nézettség a száz legnézettebb fake news poszt esetében).[258] Barabási gondolata az Avaaz-

253 Christakis–Fowler (2010): 42.
254 Barabási (2011): 98.
255 Uo., 94.
256 Uo., 97.
257 Barabási (2020): 191.
258 Facebook from Election to Insurrection: How Facebook Failed Voters and Nearly Set Democracy Aflame, *Avaaz Report* 18/3/2021. secure.avaaz.org/campaign/en/facebook_election_insurrection

jelentés mellé állítva rámutat, hogy a kibertérben a társadalmi hálózatok soha nem látott mértékben formálhatóak és állíthatóak szembe a társadalmi struktúrával, amelyhez hozzájárul a közösségimédia-platform szolgáltatók üzleti gyakorlata, és amit eszközként használnak a hibrid konfliktusok ellenérdekű felei is.

4. A kibertér államra gyakorolt hatása

Annak gondolata, hogy a kibertér és a hozzá kapcsolódó rendszerek felhasználhatóak az állam működése során, az egyes alrendszerek pedig eredményesebbé válhatnak ezáltal, nem újkeletű gondolat. Gregory M. Kaladijan 1996-os Journal of Children and Poverty-ben megjelent Welfare vs. Cyberfare című cikkében arra vállalkozott, hogy a welfare state (jóléti állam) reformjának szükségét felvázolja. A tanulmányban az elektronikus rendszerek szociális igazgatásban történő felhasználása mellett érvelt, melyek a már működő szociális struktúrát véleménye szerint átláthatóbbá és igazságosabbá, a rendszer működését pedig ezáltal eredményesebbé tették volna.[259]

Kaladijan a kibertér fejlődésének egy korai időszakában ismerte fel annak államigazgatást, állami alrendszereket, az állami funkciókat hatékonyabbá tevő képességét, igaz, ő csak egy területre, a szociális igazgatásra és annak hosszú ideje visszásan működő rendszerének megújítására látott benne fantáziát. Szavai azonban akkor – valószínűsíthetően a fókuszált terület társadalmi érzékenysége és a kibertér fejlődésének korai szakasza okán – lényegi változást nem eredményeztek. Mára viszont az államigazgatás teljes rendszere, így vagy úgy, de megjelent a kibertérben, a gazdasági szereplők tevékenysége elképzelhetetlen a virtuális tér nyújtotta lehetőségek nélkül, az emberek pedig a hétköznapjaik nagy hányadát töltik e közegben. Ez azonban nem egyszerűen a welfare state reformját eredményezte, azon lényegesen túlmutat hatásában, hiszen egy teljesen átalakult struktúrájú társadalmi-gazdasági közeget hozott létre ez a folyamat, amely az állami funkciók összességét is érintette. E folyamat alapjaiból kiforgatta a társadalmi totalitás egészét,[260] így annak minden egyes részkomplexumát: a gazdaságot, a jogot, a közigazgatást és a fegyveres védelem ágazatait[261] is. Az „evolúció" sajátja, hogy nemcsak a welfare state jegyeit vette át, módosította és szelektálta a szereplők hatalmi igényei szerint, hanem a geopolitikai környezet átalakulásának és a technológia fejlődés jelentette biztonsági problémáknak köszönhetően egyes államok visszanyúltak a warfare state (hatalmi állam) jegyeihez is. Warfare state esetében ki kell emelni, hogy ez nem a jó állammal – a welfare state-tel – szembenálló rossz állam, hanem olyan államfejlődési stáció(k), amely megjelent a transzatlanti térség államaiban is. Jelentősége abban fogható meg, hogy az államot ért impulzusokra, kiemelten a biztonságot érintő társadalmi vagy külső hatásokra való válaszreakcióként megjelenő állami (működési, szervezeti, funkcionális) racionalizációt, a védelmi, biztonsági aktorok centralizációját jelentette.[262] Bruce D. Porter tanulmányában az Egyesült Államok államfejlődésével kapcsolatban ki is fejtette, hogy ez az államfelfogás kellett az erős szövetségi állam létrejöttéhez, mivel a külső – vagy a polgárháborús – fenyege-

259 Tanulmányát l. Kaladijan (1996): 93–104.
260 Peschka (1988): 33.
261 Farkas Ádám (2018b), Farkas Ádám (2019a).
262 L. Sparrow (2011)

tettség minden esetben szükségessé tette az állam működésének átgondolását, adott esetben racionalizálását.[263] Emellett azonban nem elhallgatható, hogy ezen államfelfogás az 1945 előtti nemzetközi jogi környezetében kedvezett a nemzetközi konfliktusok eszkalálódásának, ha a jogállami kereteket nem tudták megerősíteni, illetve garantálni a békés működést.

A 21. század első évtizedeiben világossá vált, hogy a digitalizáció jelentős hatást gyakorol a társadalmakra, az államra, annak minden funkciójára. A pozitív hatások erősítik a jóléti funkciókat, emellett számos területen fejtenek ki jótékony hatást (lásd kommunikáció, okos városok stb.), mindazonáltal a negatív oldala is egy újfajta fellépést kíván az állam intézményeitől.

Jelen fejezet célja, hogy bemutassa a kibertér államra és állami alrendszerekre gyakorolt hatását, mind pozitív, mind pedig negatív oldalról; mivel kizárólag ez eredményezheti egy olyan átfogó kép megalkotását, mely révén megfelelő jogi, biztonsági válaszokat tudunk adni a kialakult vagy kialakulóban lévő folyamatokra.

4.1. A welfare state digitalizációja, a technológia pozitív hatása a 21. század államára

A jóléti állam a szervezett kormányzati hatalom tudatos alkalmazását jelenti annak céljából, hogy a piaci erőhatásokat egyfajta társadalmi igazságossági és elosztási eszmény mentén módosítsák. Ezt kifejezetten három területen kívánták érvényre juttatni: (1) egyéneknek és családoknak minimális jövedelmet garantálva (munkától, munkabértől függetlenül); (2) szűkíteni a gazdaság bizonytalanságait, és ezzel elérve bizonyos társadalmi kockázatok kezelését; (3) meghatározott szolgáltatások esetében a lehető legmagasabb szintű ellátás biztosítása. Az első kettőt már korlátozottan, de a szociális állam is képes volt megvalósítani.[264] Azonban a harmadik cél ezen állammodellen már túlmutatott, és az egyenlő bánásmód irányába kívánta módosítani a rendszert. Ez pedig a piacgazdaság negatív hatásainak a figyelem középpontjába kerülése miatt történhetett meg, hiszen szükségessé vált azok enyhítése, rendezése. Azonban, eltérően a szociális államtól, már nem a minimum garantálására törekedett, hanem az optimum irányába mozdult el a rendszer.[265]

Magának a jóléti államnak a létrejöttét a fenti felismeréseken túl több tényező együttállása tette lehetővé, így kifejezetten: az általános választójog kialakulása; a politikai demokrácia kompetitív logikája; a korábbinál tagoltabb és komplexebb társadalmi rétegződés; az érdekcsoportok növekvő befolyása; valamint a szocialista állammodellek jóléti ígéreteivel szembeni hatékony alternatíva állítása.[266] Ezen állammodell „a demokratikus jogok kiterjesztése és kiszélesítése részeként komplex jóléti rendszereket alakított ki".[267] Ezzel pedig több funkciót kívánt érvényre juttatni, így többek között a társadalom által okozott, azonosítható hátrányok enyhítését (munkanélküliség, üzemi balesetek, háborús nyugellátás stb.), a társadalom által nehezen azonosítható, vis maior jellegű hátrányok tompítását (légszennyezés, városok

263 Porter (1994a), Porter (1994b): 7. fejezet. War and the American Goverment
264 L. többek között: Szépvölgyi (2020): 101–116., Szépvölgyi (2021): 316–323, Kelemen (2019b): 149–174.
265 Briggs (2006): 16–17., 27.
266 Pongrácz (2019a): 55.
267 Pongrácz–Téglási (2021): 299.

pusztulása), indokolatlan társadalmi hátrányok kompenzációját (pl. szolgáltatás a hátrányos helyzetű gyermekek részére), valamint befektetést a jövő generációiba (pl. oktatás), továbbá a személyes jólét alapfeltételinek megteremtését (saját ingatlan, közművek stb.).[268] Megvalósítás eszközeként foghatók meg a társadalombiztosítás, a pénzbeli juttatások, a természetbeni juttatások, a partnerségi együttműködés kialakítása egyes szervekkel, és a helyi önkormányzatok szociális tevékenységének erősítése. [269] Az eszközök szerkezetére, tartalmára eltérő megoldások születtek az államról való gondolkodás, a társadalmi tradíciók és a történelmi hagyományok nemzeti sajátosságai mentén.[270] Az érintett területek, szakpolitikák köre soha nem rögzült taxatív módon, azok folyamatos változásokat mutatnak, igazodva az adott kor aktuális kihívásaihoz is.

A 21. század társadalmi folyamatai ismét próbára teszik a jóléti rendszerek és az állam alkalmazkodóképességét. Így például a munka világában megjelenő, szolgáltatás alapú gazdaság jelentős változásokat eredményez. A World Economic Forum (WEF) szerint 2015–2020 között közel 7,1 millió állás szűnt meg 15 gazdasági ágazatban.[271] Ez pedig csak az első lépés volt, ugyanis szintén a WEF által kiadott dokumentum, a Future of Jobs 2020 című jelentésében található becslés szerint 2025-re 85 millió munkahely szűnik meg, mert a gépekkel olcsóbb és hatékonyabb lesz az egyes feladatok ellátása, ezzel párhuzamosan pedig kialakul 97 millió új típusú feladat, szerepkör,[272] amelyek alapja a hatékonyabb alkalmazkodás az emberek és gépek közötti interakciókban.[273] Horváth Zoltán a Széchenyi István Egyetem Gépészmérnöki, Informatikai és Villamosmérnöki Kar (SZE GIVK) dékánjának a szavai mutatják, hogy ez a folyamat a következő években nem, hogy nem enyhül, hanem rohamtempóra fog kapcsolni. Beszéde szerint ugyanis – amit SZE GIVK diplomaátadóján mondott – „a társadalom- és jövőkutatók szerint harminc év múlva a szakmák nyolcvan százaléka olyan lesz, ami most még nem is létezik. Nagy eséllyel Önök olyan szakmában dolgoznak majd, ami jelenleg még nincs is, csak elképzelésünk van róla."[274] Ennek természetszerűleg részét képezi a munkahelyi környezet átalakulása, hiszen a vállalkozások szükségszerűen költséghatékonyságra törekednek, amelynek egyre inkább részét képezi a demonetizáció mint digitális következmény: vagyis a növekvő digitalizációs szint kevesebb fizikai költséghez vezet,[275] ami versenyelőnyt eredményez egyik oldalról, másik oldalról az okos munkahelyek megteremtése egyes hagyományos szakmák megszűnését eredményezheti, de legalábbis átképzést, fejlesztést követel meg. Így a tudás- és készségintenzív gazdaság hátrányos társadalmi következményeinek elkerülése érdekében az államnak jelentős beruházásokat kell eszközölnie ezen csoportok oktatására, átképzésére.

A változó és fejlődő technológiák, a fokozódó globális integráció és az ezekhez való alkalmazkodás képessége, a szolgáltató szektor túlságos dominanciája és az általa szült

268 Titmuss (2006): 42–43.
269 Briggs (2006): 18.
270 Esping-Andersen (2002): 1.
271 Ferencz (2019): 322.
272 Ezt igazolja vissza a robotika területe is. L. Hajdú (2020): 3–9.
273 *The Future of Jobs Report 2020 – October 2020*. World Ecnomic Forum, 5. www3.weforum.org/docs/WEF_Future_of_Jobs_2020.pdf
274 Nimsz Zsuzsanna: Szombaton is sokan vették át a diplomájukat a SZE-n. gyorplusz.hu/gyor/szombaton-is-sokan-vettek-at-diplomajukat-a-sze-n/
275 Gyekiczky (2021): 112.

tudásintenzív gazdaság együttesen szakadékot teremtenek társadalmakon belül, illetve ezek a tendenciák az államok között is fokozzák a polarizáltságot. Szükségszerűvé vált az államról alkotott felfogásunk újragondolása is.[276] „A szabadversenyes korszak be nem avatkozó, éjjeliőr államával szemben – amely az állami szerepvállalást a közrend és a közbiztonság fenntartására és a gazdaság működési feltételeinek biztosítására korlátozta – a jóléti állam tevékeny állam volt."[277] E megváltozott, az államot aktív cselekvésre ösztönző környezetben kézenfekvő, hogy eme jóléti állam egyes attribútumait erősítő államfelfogás tud csak eredményesen fellépni a korszak kihívásaival szemben.

Ennek egyik úttörője volt a bevezetésben már citált Kaladijan is, aki a jóléti állam reformjának lehetőségét a digitalizációban látta. A technológia hihetetlen fejlődése a 21. század első évtizedeiben arra a szintre jutott, hogy az élet szinte minden területén megkerülhetetlen tényezővé vált. Ebből a fejlődésből is kiemelkedik a kibertér által generált lehetőségek és változások tárháza, amelynek köszönhetően Kaladijan eszménye a digitálisan hatékonyabbá, igazságosabbá tett jóléti rendszerről részint megvalósulni látszik. Ez szintén a jóléti államok sajátos államfelfogásán is alapszik, hiszen annak megteremtése a társadalom oldaláról igényt támasztott a minőségi közigazgatás kialakítására, fejlesztésére, ezáltal „a közigazgatás ennek következtében megszűnt a jogszabályok puszta végrehajtója és a hatósági jogalkalmazó közigazgatás kizárólagos terepe lenni",[278] létrehozva ezzel a szolgáltató közigazgatást. Így a technológia forradalma a jóléti állam szükségszerű átalakulását is eredményezte, tehát szintén szükségszerűen magával hozta a közigazgatás, végső soron a teljes államműködés reformját is.

Az állami intézményrendszernek fel kellett vennie a versenyt az átalakult szolgáltatóiparral, amely lehetővé tette, hogy a saját otthonainkból szinte minden elérhetővé váljon az okoseszközök használatának köszönhetően. Az e-közigazgatás fokozatos kialakításával és fejlesztésével lépett e verseny pástjára az állam, amelynek köszönhetően hatékonyabbá, naprakészebbé és nem utolsó sorban polgárbaráttá (felhasználóbaráttá) vált a rendszer.[279] Az egyes szolgáltatások könnyebben elérhetővé váltak,[280] és a legtöbb esetben az eljárások is jelentősen felgyorsultak.

Az átalakulás azonban itt nem állt meg. A kibertér megjelenése hatott, illetve folyamatosan hat az – Titmuss fentebb ismertetett – állami (jóléti) funkcióknak valamennyi szegmensére. A kibertéren alapuló technológiai újítások robbanásszerű változásokat idéztek elő, illetve elővetítenek olyan generális átalakulásokat a tudományos vagy társadalmi alrendszerekben, amelyek révén az emberiség óriási lépéseket tehet az eddig megoldhatatlan problémák kezelése tekintetében.[281] Jól illusztrálja ezt a kvantumszámítógépek megjelenése, és folyamatos, gyors fejlődése és hasznosíthatósága is. Az első, 2019-ben a Google által fejlesztett gép 54 qubites processzorra épült, amely 200 másodperc alatt végzett el olyan műveletet, amely a korábbi technológiai csúcsot jelentő szuperszámítógépeknek tízezer évbe telt volna.[282] Alig telt

276 Esping-Andersen (2006): 434., 447–448.
277 Szigeti (2011): 262.
278 Pongrácz (2019a): 163.
279 L. Budai (2017)
280 Gondoljuk itt például Magyarország tekintetében az internetes ügyfélkapu rendszerre, amelynek köszönhetően számos szolgáltatást az otthonunkból ki sem mozdulva tudunk elérni.
281 Harari (2016)
282 Bognár Zsolt: Egy új korszak kezdete: A Google elérte a kvantumfölényt. qubit.hu/2019/09/24/egy-uj-korszak-kezdete-a-google-elerte-a-kvantumfolenyt

el három év, és 2022 őszén az IBM bejelentette Osprey nevű kvantumszámítógépét, amely 433 qubittel rendelkezik. Ezen gépek sajátja, hogy

> „a kvantumbitek a hagyományos bitekkel ellentétben egyszerre vehetik fel a 0, az 1 vagy akár egyszerre mindkettő értékét, ami lehetővé teszi olyan számítások elvégzését, amelyek még a legmodernebb szuperszámítógépeknek is túl bonyolultak – ilyen például a kémiai reakciók szubatomi részletességgel történő szimulálása".[283]

Amúgy az Egyesült Államok és Kína között e területre is kiterjed a verseny. Kína 2021-ben jelentette be a világ akkori legnagyobb teljesítményű kvantumszámítógépét, így feltételezhetjük, hogy a távol-keleti állam esetében sem ez volt a fejlesztés csúcsa.[284] Hasonló volumenű fejlesztés a kaliforniai Stanford Egyetemen működő Stanford Linear Accelartor Center laboratóriumában kifejlesztett óriás digitális kamera, amely 189 érzékelőt tartalmaz és 3,2 gigapixelre képes. Az eszköz a távoli galaxisok feltérképezését fogja segíteni, és várhatóan 20 milliárd galaxist fog katalogizálni, eközben éjszakánként 15 terabájtnyi adatot gyűjt. Az eszköznek köszönhetően a kutatók közelebb kerülhetnek az univerzum kialakulásának megértéséhez, illetve az univerzum és a sötét anyag működési hátterének feltérképzéséhez.[285]

Kézzelfogható eredményeket lehet felmutatni az oktatásban, kutatásokban, az egészségügyben, a szociális szférában, ahol megjelent az IoT,[286] az IoD[287] és az okoseszközök,[288] a mesterséges intelligencia pedig egyre jelentősebb teret foglal el. A kibertérhez csatlakozó eszközök (az állam, a gazdaság és az egyén oldaláról), valamint a korábbi évszázadok tudásának és a folyamatoknak, tevékenységeknek a digitalizálása, óriási adatmennyiséget (big data) generálva, forradalmi átalakulást hoztak a fenti területeken is.

Ez az egészségügyben többek között csökkentette a diagnosztikából eredő hibákat, lehetővé tette a korábban fel nem fedezett összefüggések felismerését, új módszerek kidolgozását, alkalmazását.[289] Ezek közül érdemes kiemelni pár példát. A Semmelweis Egyetem részvételével valósult meg az a kutatás-fejlesztési tevékenység, amelynek köszönhetően a mellkasi CT-felvételeket kiértékelő mesterséges intelligencia felhasználásával javul a korai daganatos megbetegedések felismerésének a lehetősége.[290] A digitalizáció e területen is átalakítja a hagyományos interakciókat, így az orvos-beteg kapcsolatot is. Ennek egy területe az E-Health

283 Bognár Zsolt: Az IBM megépítette a világ legnagyobb, 433 qubites kvantumszámítógépét. qubit.hu/2022/11/09/az-ibm-megepitette-a-vilag-legnagyobb-433-qubites-kvantumszamitogepet

284 Bognár Zsolt: Kína bemutatta a világ legnagyobb teljesítményű kvantumszámítógépét. qubit.hu/2021/07/14/kina-bemutatta-a-vilag-legnagyobb-teljesitmenyu-kvantumszamitogepet

285 Kun Zsuzsi: A világ legnagyobb 3,2 gigapixeles digitális kamerája magasabb egy autónál, és galaxisok milliárdjait örökítheti meg. qubit.hu/2022/10/28/a-vilag-legnagyobb-32-gigapixeles-digitalis-kameraja-magasabb-egy-autonal-es-galaxisok-milliardjait-orokitheti-meg

286 Korunk egyik nóvuma, konvergáló technológiája a tárgyak internete (IoT – Internet of Things), amely az információtudomány fejlődésével, a szenzorok használatának fokozódó térnyerésével (ami magával hozza az árak rapid csökkenését) egyre inkább a mindennapi életünk részévé válik mind az otthonokban, mind pedig a közszférában. L. Németh (2019): 307–325.

287 Baranyi et al. (2021a): 225–240., Baranyi et al. (2021b): 91–104.

288 G. Karácsony (2020)

289 Bőgel (2015): 22–24.

290 Mesterséges intelligencia segíti a tüdőrák hatékonyabb felismerését. *Semmelweis Egyetem – A Semmelweis Egyetem polgárainak lapja,* 2022. október 18.

rendszer, ami arra hivatott, hogy könnyebbé tegye az egészségügyi szolgáltatásokhoz való hozzáférést például az alacsonyabb jövedelműek részére vagy akik a központoktól távolabb élnek, ezzel pedig a rendszer infrastrukturális hiányosságait próbálja orvosolni.[291] Forradalminak hat az okostelefonok bevonása a mentális betegségek nyomon követése, felmérése és felismerése területén is, mivel az eszközökre telepített alkalmazások révén lehetőség van valós idejű értékelésre.[292] Hasonlóan eredményesnek mutatkozik a mesterséges intelligencia a járás elemzésben is, ahol meglehetősen hatékonyan szűri ki a kóros járást, így segítve egyes betegségek felismerését.[293]

Az oktatásban és kutatásban is lehetővé vált, válik a modern, kibertérhez kapcsolódó technológia alkalmazása. Az okoseszközök használata és algoritmusok révén a személyre szabott tanulás, tudásanyag átadása komoly potenciált jelent.[294] Ennek az egyik legvitatottabb megjelenési formája Kínához köthető, ahol kísérleti jelleggel megkezdték olyan EEG (elektromos aktivitást mérő elektroenkefalográf) használatát, amely iskolai órák közben vizsgálja a tanulók agyi funkcióit. Az eszköz segítségével a tanár valós időben látja, hogy a gyermek megfelelően koncentrál (fehéren világít a led), vagy unatkozik, mással foglalkozik (pirosan világít a led). A rendszerhez tartozik egy kamera rendszer is, ami a pontosabb képalkotáshoz szükséges. Az adatokból mind az oktatók, mind pedig a szülők valósidejű képet kapnak a gyermekek figyelmi szintjéről. De Kína emellett fejleszti és teszteli az óvodai óvórobotokat, valamint a mesterséges intelligencia alapú intelligens tutorokat is. Az Egyesült Államokhoz köthető a Tomorrow Advancing Life (TAL), ahol a gyártó cég (TAL Education Group) azon dolgozik, hogy a valós időben adatokat szolgáltató rendszernek köszönhetően az egyéni fejlesztésekre kerüljön a hangsúly, ahol az MI inkább digitális asszisztens szerepét tölti be.[295] India Kínához hasonlóan hatalmas lehetőséget lát az oktatás digitalizációjában, és óriási forrásokat költ arra, hogy az oktatás minél nagyobb területén jelenjenek meg az okoseszközök.[296] A big data-nak köszönhetően a kutatások soha nem látott, országhatárokat átlépő, kontinenseket összekötő hálózatokat generálnak, felgyorsítva az innovációt. Ezen innovációnak a gyorsaságát mutatja, hogy Moore-törvénye,[297] amely szerint az integrált áramkörök összetettsége körülbelül 18 havonta megduplázódik, napjainkban egyre inkább megdőlni látszik, hiszen ez a tendencia gyorsulóban van.[298]

Úgyszintén domináns a diszruptív technológiák térnyerése, amely még összetettebbé, sérülékenyebbé, de látszólag mindenképpen könnyebbé teszi az emberek hétköznapjait,[299] így a dolgok internetéhez 2020-ban már több mint 26 milliárd eszköz csatlakozott. A mesterséges intelligencia pozitív hatásai a technológiai fejlődéssel 2030-ra megsokszorozódnak. A Stanford Egyetem által közzétett előrejelzés szerint a mesterséges intelligencián alapuló innováció majd elérhetővé teszi, hogy még összetettebben működő okosvárosok jöjjenek létre,

291 Incze–Pesuth (2020): 247–250.
292 Lakhtakia et al. (2022)
293 Lim et al. (2022)
294 Tilesch– Hatamleh (2021): 65–68.
295 Kolozsi Ádám: Beelektródázták a gyerekeket az iskolapadban. index.hu/techtud/2019/11/14/mesterseges_intelligencia_kina_oktatas/
296 Seethal–Menaka (2019)
297 Moore (1965)
298 Justin Viktor: Vajon valóban elbukik a Moore-törvény, vagy van még tovább? raketa.hu/vajon-valoban-elbukik-a-moore-torveny-vagy-van-meg-tovabb
299 Majumdar–Banerji–Chakrabarti (2018): 1247–1255.

ahol autonóm járművek könnyítik az utazást, az áruszállítást,[300] és az orvosi diagnosztika területén a vérnyomást, vércukorszintet és egyéb jellemzőket monitorozó, adatokat gyűjtő szenzorok a páciensek életét menthetik meg.[301] A gyorsuló megtérülés törvénye[302] pedig csak erősíti ezt a folyamatot, hiszen elvárja, hogy új technológia jöjjön létre, ami gyorsabb fejlődést eredményez, és az természetszerűleg még újabb technológiákat szül. Ez pedig öngerjesztő folyamat, egyfajta pozitív visszacsatolást generál, amely következtében az egyik részterület gyorsítja a másik terület fejlődését, például a robotika, MI, kvantum- és nanotechnológiák, bioinformatika, blokkláncok, VR területén és így tovább.

Az állam működésének átalakulása nem állt meg a jóléti rendszerek modernizálásánál, a modern technológia alapjaiban alakította át a teljes állami működési mechanizmusokat, valamint az állam és a gazdasági szereplők, továbbá az állam és a polgárok közötti interakciókat. A modern technológia ennek köszönhetően behatolt az élet minden szintjére, és azokra jelentős hatást gyakorolt, így egyebek mellett a rendészetre,[303] az igazságszolgáltatásra,[304] a közlekedésre,[305] az energiahasználatra és az önkormányzatiságra, [306] és nem utolsósorban a védelem és biztonság világára is.[307]

Ezek a megoldások sok tekintetben sokkal élhetőbbé tették és fogják tenni az emberek hétköznapjait, az állam működését pedig racionalizálják, felhasználóközpontúbbá tették és fogják tenni. Mindemellett azonban a szolgáltatásközpontúság, az adatokhoz, a képességekhez való hozzáférés lehetősége a klasszikus welfare state egyenlőségre törekvő oldalát elmozdította egy elitista működés irányába, ahol ezen erőforrások feletti tényleges rendelkezés lehetősége teremti meg a döntéshozásnak az alapjait.[308] Tökéletes példái ennek a magántulajdonban álló okos városok, ahol az adatok szinte teljességéhez hozzáférnek az olyan nagyvállalatok, mint az Amazon Seattle-ben, vagy Facebookville, Zucktown esetében a Meta, de többek között ilyet tervez létrehozni a Tesla Ausztráliában Yarrabend néven.[309] Szintén az adatok garmadája felett diszponálnak a közösségi média vállalatok, azokat tényleges termékként kezelik. Érdekes módon tehát a nyugati államokban a gazdaság – főként a kibertérben tevékenységet realizáló – transznacionális szereplői tömegesen férnek hozzá az egyénekhez fűződő adatokhoz,[310] míg az alkotmányos struktúrájukban kialakított korlátoknak és fékeknek köszönhetően az államok számára ezeknek az elérhetősége erősen korlátozva van. Látni fogjuk ezzel szemben a keleti autoriter államalakulatok maguk is végrehajtották – igaz sajátos módon – az államaik

300 Bucko et al. (2021), Fandáková et al. (2020) 1680–1684.

301 Tom Abate: Smarter Hospitals: How AI-Enabled Sensors Could Save Live hai.stanford.edu/news/smarter-hospitals-how-ai-enabled-sensors-could-save-lives, Dunn at. al. (2021): 1105–1112.

302 Kurzweil (2014): 58–72.

303 L. Prakash (2018b): 97–108.

304 Nogel (2022): 481–503., Vajda (2022): 20–22.

305 Bhuyan (2021)

306 L. Kovács László (2018): 19–118.

307 Példaként ebben a körben érdemes megjegyezni, hogy több szerzői is kiemelte már a digitális adatokkal történő rendelkezés biztonságra, védelemre gyakorolt hatását, illetve fake news társadalmi kohéziót romboló hatását, továbbá az erre épített dezinformációs tevékenység nemzetbiztonsági vonatkozásait. L. Cattaruzza (2020), Kelemen (2021c): 71–85.

308 L. Árva–Pásztor–Pyanatova (2019): 57–81.

309 Mosco (2019): 137–145. L. még: Dusek (2018): 1–3., Krasznay (2022): 8–36.

310 Ezen vállalatok az adatokhoz való hozzáférést követően nem kizárólag felhasználják ezeket az információkat, hanem kereskedelmi és politikai célokra áruba bocsátják, ezzel is erősítve az adatok geopolitikai jelentőségét. L. Engel (2019): 70–76., Gellén (2020): 127–140., Farkas Ádám (2021a): 1–13.

digitális (jóléti) reformját, addig viszont az adatok lehető legteljesebb köre felett kívánnak rendelkezni.

4.2. A warfare state digitalizációja – A kibertérben realitássá vált totális biztonsági kihívások

A keleti államok, főként Kína és Oroszország jelentős mértékben kiaknázzák a technológiai újításokból fakadó biztonsági képességeket. Ennek eklatáns példája az okos város nyújtotta jóléti lehetőségekbe burkolt totális megfigyelés és adatgyűjtés lehetősége. Ilyen rendszer kiépítését kezdte meg Kína a 2010-es évek elejétől. *Megdöbbentő módon a világban jelenleg futó körülbelül ezer okos város-projekt közel fele Kínához köthető.* Ennek központi eleme a Citizen Cloud,

> „ez egy felhőalapú platform, és egyben mobil alkalmazás is, amely egyesíti a kormányzati szolgáltatások legnagyobb részét, és megkönnyíti a városlakók számára az ezekhez való hozzáférést, ide számítva az egészségügyi nyilvántartásokat, a jogosítványkérelmeket és -megújításokat, és más közösségi programokat is… a Huawei (…) gyártmányai teszik lehetővé az autósok számára a szabad parkolóhelyek megtalálását (…) A rendszer nagyon megkönnyíti a betegek és a kórházak számára a releváns nyilvántartások elérését".[311]

A kiépülő rendszer tökéletes példája lehet az előző fejezetben elérni kívánt állami működésnek, vagyis az olyan szolgáltató államnak, amely képes jóléti intézményeit átemelni a digitális környezetbe, sőt fokozni is képes ezáltal azokat. Azonban ott van egy hatalmas „de" a mondat végén, hiszen e rendszerek révén nem csupán erre képes Kína, hanem az emberek nyomon követésére, osztályozására és adataik tényleges birtoklására is.[312] Érdemes eme megoldásoknál kicsit elidőzni. A Kínai Aranypajzs projekt, ahogy arra a Freedom House 2020-as internetszabadságról szóló jelentése felhívja a figyelmet, a glóbusz legmodernebb és legösszetettebb rendszere. Fontos hangsúly van azon, hogy ez egy összetett rendszer, mivel már nem csupán a kibertéri tevékenységet figyeli és korlátozza, hanem számos rendszert kapcsol össze. Így a közterekre, az otthonokba, a munkahelyekre, de mint fentebb láttuk, már az általános iskolákba vagy óvódákba telepített megfigyelő kamerákat, a Covid19 terjedését megakadályozandó hőérzékelési rendszerek, egészségügyi állapottal és kontaktkutatással kapcsolatos applikációk, valamint a big data-alapú elemző rendszerek, az online tevékenységet korlátozó algoritmusok, és természetesen az arcfelismerést szolgáló technológiákat.[313] Nem lehet megfeledkezni a Kínai Nagy Tűzfalról sem, amely a külső tartalmakat elérhetetlenné tételét szavatolja. Az állami cenzúrát meg szűken vége maga a Pajzs. Ennek köszönhetően egyre nagyobb terjedelmében teremtődik meg az alapja a társadalmi kreditrendszernek, ami a politikai és társadalmi status quo rögzülését eredményezi, ahol csak az lehet a társadalom hasznos tagja és csak az léphet előre, aki megfelelően teljesít a pontok/kreditek rendszerében.[314]

311 Mosco (2019): 111–112.
312 Kollár (2020): 79–97.
313 *Freedom ont he Net 2020 – The Pandemic's Digital Shadow.* Freedom House, 2020. 21. (továbbiakban: Freedom House) freedomhouse.org/sites/default/files/2020-10/10122020_FOTN2020_Complete_Report_FINAL.pdf
314 Szikszai (2020): 21–26.

Gosztonyi Gergely felhívja arra a figyelmet, hogy ez a jelenség nem példa nélküli és egyre több követőre talál.

> „Nyilvánvalóan nem lehet társadalmi, szociális vagy akár politikai helyzet kapcsán egy kalap és egy szabályozási modell alá helyezni az összes ázsiai országot, az mégis látható, hogy – az eltérések ellenére – az internet szabályozásával és a tartalomszabályozással kapcsolatos felelősségi kérdésekben egy sokkal szigorúbb utat választottak, mint Európa vagy az Amerikai Egyesült Államok (…) A fő cél természetesen politikai: megakadályozni, hogy az online világban olyan gondolatok terjedjenek, amelyek esetlegesen politikai ellenállást szülhetnének a való életben."[315]

Ahogy Gosztonyi is kifejti, ez nem egy homogén csoportja az államoknak, azonban egyre nyilvánvalóbbá válik, hogy egyre több állam választja annak a lehetőségét, hogy a polgárait kibertérben a kapcsolódó eszközök révén „kordában" tartsa, az internetét pedig a lehető legteljesebb mértékig kontrollálja.

Szingapúr is hasonló példát mutat az Okos Nemzet projektjével, amely felhasználásával „kezdetektől fogva tervezeték (…) egy centralizált műveleti központ létrehozását, a polgárokról és a látogatókról összegyűjtendő nagy mennyiségű adat kezelésére", ez pedig lehetővé teszi „ az átfogó megfigyelést és az egyének magatartásának szigorú szabályozását".[316] A megvalósítás hivatalos céljai között szerepel a betegségek terjedésének a gyorsabb feltérképezése vagy a terrorista támadásokra való gyorsabb reagálás lehetősége. Megvalósításán fúzióban dolgoznak az állami intézmények és a magánszféra vállalatai, akárcsak Kína esetében. A rendszerek kialakításában és az üzemeltetésében történő közreműködésért cserébe a kormányzat „megosztja az adatokat a gazdaságfejlesztés és a kereskedelmi sikerek ösztönzése céljából".[317] Két szereplő, vagyis az állam és a technológiai vállalatok együttesen érdekeltté válnak a status quo fenntartásában, hiszen egyfelől totális felügyelet alá helyezték az egyéneket, másfelől a gazdasági fejlődés folyamatos fenntartását teszik lehetővé az állami megrendelések, harmadsorban a meglévő adatok birtokában a gazdasági szféra is meg tudja hozni a szükséges intézkedéseket, stratégiát a profit folyamatos növelése érdekében. Mit nyer ezzel a felhasználó? Javuló közszolgáltatásokat a szabadságáért cserébe, de lényegében a választás lehetősége egy másodpercig sincs biztosítva a részükre. Ilyen város kialakítását tűzte ki célul az Egyesült Arab Emirátus Dubaj esetében, de ezt látjuk Rio de Janeiro-ban, Malajzia és a Fülöp-szigetek jelentősebb városaiban, valamint India is meghirdette ezen programját All India City Challenge néven, amelynek alakításába azonban a helyi közösségek aktívan bele kívánnak szólni.

A rendszert a saját internet létrehozása és annak totális felügyelete tette teljessé, mint a kínai Aranypajzs rendszer vagy az orosz internet,[318] ezzel ezen államalakulatok képesek szinte totális ellenőrzés alatt tartani saját polgáraikat, hiszen minden olyan tartalmat képesek blokkolni, amely az államhatalom szempontjából nem kívánatos. Ezen megoldás az okos város projektekhez hasonlóan szintén követőkre talált. Irán közvetlenül kínai know-how fel-

315 Gosztonyi (2022a): 157., 165.
316 Mosco (2019): 109.
317 Uo., 110.
318 Gosztonyi (2021a): 87–99.

használásával kíván „halal”[319] internetet kiépíteni, amelyet Zambia is követ a kritikus tartalmak blokkolása területén. Emellett a kormányellenes, kormánykritikus hangok blokkolása is bevett gyakorlattá vált a közösségi média felületeken, ezt alkalmazza Kuba, Nigéria, Kolumbia, Banglades, Szenegál, illetve a teljes internet elérhetőségét megakadályozva a Kongói Köztársaság, Csád, Örményország vagy Mianmar.[320] Ezen államok fellépésének az alapja a korábban Kína vagy Oroszország által megfogalmazott elv: a szuverén internet elve, amely szerint minden állam szabadon rendelkezik a hozzá tartozó kibertér felett, ebbe más állam nem avatkozhat be, ott szabadon határozhatja meg az elérhető tartalmakat, az azokhoz való hozzáférést. A Freedom House fent már említett jelentése erre kitérve rámutat, hogy Kína és Irán a leginkább zárt saját internet tekintetében, de ehhez a táborhoz közelít Oroszország, Törökország és Vietnám is,[321] a tábor pedig folyamatosan bővül.

Az elmúlt években az is világossá vált, hogy az államok a technológia újdonságait legalább ilyen, aktív módon használják más államokkal szemben is. A hibrid konfliktusok eszközparkjába beemelt kibertéri műveletek rendkívül széles tárházát adják a szembenálló állam egyes rendszereinek támadására. Folyamatos fenyegetést jelentenek a dezinformációs kampányok, amelyek érdemben az államalakulatok mindegyikével szemben alkalmazhatóak. Az oroszok folyamatos dezinformációs tevékenysége figyelhető meg az elmúlt évtizedben. Ennek során beavatkoztak a 2016-os amerikai elnökválasztásba, akár álhírek terjesztésével, akár a szembenálló jelöltekkel kapcsolatos kompromitáló információk kiszivárogtatásával, vagy a közösségimédia-platformokon keresztül megfelelően időzített hírcsomagokat juttattak el a felhasználókhoz.[322] A francia sárgamellényes tüntetés időszakában hamis híreket terjesztettek német, spanyol, holland, lengyel, svéd és olasz nyelven. Az RT orosz állami hírcsatorna néhány riportere részt vett a tüntetéseken, és úgy ábrázolta a helyzetet, mintha Párizs háborús övezet volna. A dezinformációs kampányból nem maradhatott ki a hagyományos média munkatársainak lejáratása sem, őket korruptnak, megbízhatatlannak, a kormánnyal mindenben összejátszónak mutatták be.[323] A legyártott és azonosított száz álhírt, több mint 4,1 millióan osztották meg és 105 millióan tekintették meg.[324] De mindkét állam rendkívül erős dezinformációs kampányt folytatott a Covid19 járvánnyal és a nyugati vakcinák hatékonyságával kapcsolatban, ezzel is nehezítve a térség járvány elleni védekezését.[325] A könyv megjelenésének idején is zajló orosz–ukrán háború is élesen rávilágít erre a problémakörre. A háború szinte, vagy inkább a láttatni kívánt szinte minden pillanatát követni tudjuk a közösségi média felületein.[326] Ennek célja mindkét oldalról, hogy a hadviselő felek megfelelően

319 A halal fogalom az iszlám vallásban fontos értéket képvisel, jelentése megengedett vagy tiszta. Az iszlám jog szerint minden tevékenység megfelel a halal–nak, amely megengedett és az előírásoknak, dogmáknak megfelel. Ennek felhasználásával kontrollált internetes információ áramlást nevezhetjük halal internetnek. L. Iran creates „Halal Internet” to control online information. rsf.org/en/news/iran-creates-halal-internet-control-online-information

320 Gosztonyi (2021a): 97–98.

321 Freedom House, 2.

322 Rosenstedt (2021): 5.

323 Makela (2019): 10–13.

324 *Yellow Vests Flooded by Fake News – Over 100M Views of Disinformation on Facebook. Avaaz Report.* avaazimages.avaaz.org/Report%20Yellow%20Vests%20FINAL.pdf

325 Dubow–Lucas–Morris (2020)

326 Pató Viktória Lila: A háború hatása a közösségi médiára. eustrat.uni-nke.hu/hirek/2022/03/01/a-haboru-hatasa-a-kozossegi-mediara

tudják tálalni az érdekeiket a saját, illetve a világ más társadalmai irányába, vagyis mindkét oldal él a dezinformáció eszközével.[327] Földi László biztonságpolitikus ezt a következőképpen foglalta össze:

> „Nagyon álságos ez a helyzet, a közvéleményt afelé tolják, hogy tendenciózusan döntsünk, miközben gyakorlatilag kihúzzák a lábunk alól azt a lehetőséget, hogy objektívek maradjunk (…) megjegyezve, hogy az egyik fél amerikai, a másik fél pedig orosz propagandáról beszél, miközben valójában mindkét hatalomnak megvannak a maga eszközei a befolyásolásra."[328]

Legalább ilyen jelentős a különböző intenzitású kibertámadások elkövetése akár civil, gazdasági célpontok ellen,[329] akár állami intézmények rovására. Ezek közül legismertebb a 2007-es Észtországot és a 2008-as Grúziát ért támadás,[330] azonban ezenfelül számos kisebb volumenű szcenáriót tudunk feljegyezni az elmúlt évtizedből. Ilyennek tekinthetjük a Észak-Koreához köthető WannaCry zsarolóvírus támadást is, amely jelentős károkat okozott több államnak, gazdasági szereplőnek.[331] Az okozott anyagi károk mértékét már felvázoltuk a korábbi fejezetekben, annyit érdemes ismét felvillantani, hogy az elkövetkező években a kiberbűncselekmények által okozott kár mértéke, jelenleg 6,9 milliárd dollár,[332] a Cybersecurity Ventures becslései szerint ez 2025-re 10,5 milliárd dollár lesz, ami megközelítőleg az Európai Unió vagy Kína éves nominális GDP-jének az összege.[333] Szintén megfigyelhető ennek az eszköznek az alkalmazása a könyv megjelenésekor zajló orosz–ukrán háborúban is, amikor az orosz haderő legalább annyira aktív a kibertérben, mint a hagyományos hadviselés területén.[334] Ezzel kapcsolatban érdemes leszögezni, hogy a kibertér nem hozott létre önmagában új konfliktuskategóriákat, nem eredményezett a korábbitól ismeretlen had-

327 Huszák Dániel: Példátlan információs háború zajlik Ukrajna körül - Elképesztő mennyiségű hazugság ömlik a világra. portfolio.hu/global/20220226/peldatlan-informacios-haboru-zajlik-ukrajna-korul-elkepeszto-mennyisegu-hazugsag-omlik-a-vilagra-529377

328 Holló Bettina: Földi László a háborúról: Állásfoglalásra késztetnek, de az igazság magjától is eltántoríthatnak. *Index,* 2022.03.06. index.hu/belfold/2022/03/06/haboru-ukrajna-alhirek-biztonsagpolitika-foldi-laszlo-demko-attila/

329 „A 2020–as évben pusztító útjára indult Covid-19 járvány az informatikai biztonság területén is kifejtette hatását – globális szinten jelentősen megnövekedett a kibertámadások száma. A Kaspersky felmérése szerint »az Európai Unióban az internetet használó számítógépek 13,7 százalékán tapaszaltak legalább egy böngészőalapú, rosszindulatú programtámadást", (és a támadások számát tekintve) „az első tíz között találjuk Magyarországot is«. Nagyságrendileg ugyan az otthoni gépek vannak leginkább kitéve kémkedésnek, adatlopásoknak, rongálásnak és egyéb támadásoknak, de céges környezetben a statisztikák nem kevésbé lesújtóak. Az amerikai CSI egy korábbi felmérése szerint a válaszadók 85%–a észlelt már számítógépes betörési kísérleteket az adott naptári évben, sőt, 64% esetében ez anyagi veszteséget is jelentett." Németh (2021a): 48.

330 Kelemen–Pataki (2015): 53–90.

331 *North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions*. justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and

332 *Federa Bureau of Investigation Internet Crime Report 2021*. Internet Crime Complaint Center, 2021. ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

333 Steve Morgan: *2019 Official Annual Cybercrime Report – Cybercriminal activity is one of the biggest challenges that humanity will face in the next two decades.* herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf

334 Joe Tidy: Ukraine crisis: ‚Wiper' discovered in latest cyber–attacks. www.bbc.com/news/technology-60500618

viselési metódusokat, hanem ez valójában a hadiviselés korábbi eszköztárának a fejlesztését jelentette: a hatékonyság és az erő sokszorozását, műveleti képességek fokozását.[335] Az orosz–ukrán konfliktus korábbi szcenáriói is visszatükrözik ezt. A West Point-i katonai szakértők szerint az oroszok szinte példa nélküli módon egymást kiegészítve, kombinálva alkalmazzák a kiberhadviselés, az elektronikus hadviselés és az információ műveletek eszközparkját.[336] Ahogy ezt Kiss Álmos Péter kifejtette:

> „az oroszok egyáltalán nem osztják fel az információs teret. Nincs különálló kibertér, nem tesznek különbséget a számítógép-hálózatokat érintő műveletek és más információszerző, információfeldolgozó és információáramlást zavaró tevékenység között. Az orosz információs hadviselés harctere tehát a teljes kognitív tartomány."[337]

Látható, hogy a kibertéri eszközpark beépült a haderő tevékenységébe, legyen az akár befolyásolás, akár hírszerzés, akár támadó eszköz, amely így a békeidős összhaderőnemi felkészítésnek, majd pedig eszközparkjának immanens részét képezi. Így lehetséges az, hogy a hagyományos háborúnak is vannak – lásd orosz–ukrán – hibrid szcenáriói.

A kibertér a fentieken túl lehetőséget biztosít a szakadár és terrorista csoportok anyagi támogatására, szervezésére, amelyek így képesek lehetnek későbbi akciókhoz kapcsolódó információszerzésre, az ilyen akciók kibertéri támogatására, az akciók kibertéri előkészítésére és adott esetben – ahogy Lewis fogalmazott[338] – a közlekedési hálózatokkal, finomítókkal, gátakkal, katonai létesítményekkel, kórházakkal, bankokkal, kormányzati intézményekkel stb. szembeni támadás lefolytatására. Az oroszok rendkívül sikeresek voltak az ukránok elleni hibrid konfliktus során, hiszen tökéletesen tudták alkalmazni a korábbi évtizedek tapasztalatait és kapcsolati hálóját.[339]

A kibertér és a hozzá tapadó technológiai újdonságok pozitív hozadékai mellett olyan, az államok biztonságát, biztonsági környezetét befolyásoló természettel bír, amely így számos ponton tépázza meg az 1945 utáni nemzetközi jogi rezsimet, sok esetben feloldva azt a napi politikai realitások folyamában. A kibertérben alkalmazott vagy támogatott hadászati eszközök nem újak, azonban a korábbi eszközöket a végletekig tudják fokozni, eredményesebbé és hatékonyabbá tenni. Jól bizonyítják ezt a hibrid konfliktusok, kiemelten az ISIS ténykedése, valamint 2014-től az oroszok ukrajnai tevékenysége volt az egyik mintapéldánya ennek a hadviselésnek, amelynek magasabb fokozatba kapcsolását jelentette a 2022 februárjában kirobbant nyílt háború. A korábbi szcenáriók esetében is már egyértelművé vált, hogy a technológiai újításokat alkalmazva, egyre fokozottabb mértékben kezdődött meg az ENSZ Alapokmányban lefektetett erőszak általános tilalmának eróziója. Főként annak köszönhetően, hogy a polgári és kombattáns elkülönítése a harcászat nem klasszikus terepén szinte lehetetlenné vált, így a betudhatóság korábban kiforrott és többnyire a felek által betartott szabályait nem, vagy csak nagyon nehézkesen lehet alkalmazni. Az ukrán háború rávilágított arra is, hogy a népek önrendelkezése és külső állam beavatkozásától mentes létezése is feloldódni

335 Bachmann–Gunneriusson (2015): 82.
336 Brantly–Cal–Winkelstein (2017): 24.
337 Kiss Álmos (2019): 31.
338 Lewis (2002)
339 Káncz Csaba: Az orosz titkosszolgálatok és a szervezett bűnözés ijesztő kapcsolatrendszere. privatbankar.hu/cikkek/makro/az-orosz-titkosszolgalatok-es-a-szervezett-bunozes-ijeszto-kapcsolatrendszere.html

látszik a nagyhatalmi törekvésekben, amelyeket akár későbbi nemzetközi szerződésekkel is megerősítenek,[340] illetve végső esetben nagyhatalmi deklarációkkal legitimálnak.[341] A háború és a béke határa elmosódott az elmúlt években, a legtöbb konfliktus esetében nem tudjuk, hogy az „éppen még" vagy az „éppen már" állapotában vagyunk. Erre szintén rávilágított az orosz–ukrán válság, hiszen a tényleges harci cselekmények a felek között már jóval a 2022-es inváziót megelőzően megindultak.

Ezek összessége eredményezi a biztonság és védelem újradefiniálását, a totális biztonság irányába történő elmozdulást.[342] A nemzetközi közösség államainak egyik pólusa már megtette ezt, és ezen államalakulatok – főként a kibertér révén – már sokkal közelebb helyezkednek a warfare state államához, amely saját biztonságának szavatolását csak a hatalom révén, az erő által látja biztosítottnak.[343] Ezen államokban a haderő folyamatos erősítése mára létérdekké vált, a politikai hatalom, haderő és gazdaság hármasa egyetlen érdeket szolgál: a status quo minimum fenntartását, vagy még inkább a hatalmi szféra kiterjesztését.

5. A digitális állam modelljei: A cyberfare state

Stumpf István az Erős állam – alkotmányos korlátok című könyvében felhívja a figyelmet arra, hogy az államnak vannak olyan alapvető, nélkülözhetetlen funkciói, amelyeket mindenképpen el kell látnia. „Nincs olyan más, a legitim erőszak monopóliumával felvértezett intézmény, amely a szervezett közösségi együttéléshez nélkülözhetetlen alapfeltételeket az államot helyettesítve biztosítani tudja."[344] Ezen alapfunkciók első köre között tartja számon a joguralom, a magántulajdon biztosítását (belbiztonság), valamint a honvédelmet, vagyis a külső biztonságot.

Az előző fejezetek érzékeltetik, hogy a kibertér oly mértékben alakította át a társadalmi totalitás, azon belül az egyén életét és hatófokát, a társadalmi hálózatokat, az állam működését, valamint a biztonsági – természetesen a hagyományos térhez kapcsolódó egyéb kihívások sem felejtendők el ebben körben[345] – környezetet, hogy az államok több esetben, igaz leggyakrabban csak átmenetileg, a korábbi mércéhez képest kisebb terrénumban tudnak megfelelni ezeknek a követelményeknek. Márpedig, ha

> „a társadalmi félelemek eszkalálódnak (…) Ez egy negatív spirált eredményez. Minél inkább teszik ezt, annál nagyobb a zűrzavar és az erőszak, és minél nagyobb a zűrzavar és az erőszak, annál kevésbé képesek az államok a helyzet kezelésére, következésképp annál több ember vonja meg a bizalmát az államtól".[346]

Azaz a közrendbe és azt szavatoló katonai karakterű szervekbe vetett bizalom elvesztése annulálná a biztonságot, ezáltal felszámolná a normál állapotot.

340 L. a minszki szerződéseket az ukrán konfliktusban. Bővebben: Póti (2017)
341 Vlagyimir Putyin elismerte a két szakadár népköztársaságot. hirado.hu/kulfold/kulgazdasag/cikk/2022-02-22/vlagyimir-putyin-elismerite-a-ket-szakadar-nepkoztarsasagot
342 Farkas Ádám (2021c): 65–80.
343 Cook (1964): 102–109., Nelson (1971): 127–143., Edgerton (2006): 59–107.
344 Stumpf (2014): 27.
345 Juhász–Petruska (2022): 4–46.
346 Szigeti (2001)

Az államok mára a kibertér jelentette lehetőségeket és kihívásokat tökéletesen érzékelik (nem véletlen például, hogy a NATO a kiberteret hadszíntérré minősítette), azok biztonságot érintő hatására megpróbálnak választ adni. Azonban ezt a választ az egyes államok történeti és társadalmi hagyományai, valamint a politikai és az állam- és jogtudományi tradíciói, nagyhatalmi törekvései erősen befolyásolják. A kibertér biztonsága szempontjából az egyik fő ágens az egyén, akár passzív, akár aktív szereplőként figyelünk rá, mely az előző fejezetekben látható módon soha nem látott mértékben tud hatni a nemzet biztonságára. Nem véletlen, hogy a tradíciók, politikai rendszerek mentén az egyén szerepére történő reagálás az egyik legfontosabb választóvonal a vizsgált államok között. Ennek köszönhetően két modell értékű rendszer alakult ki. Az egyik modell a jogállami keretek között gondolkodó államok halmaza, míg a másik, a kibertérben és a kapcsolódó eszközökben lehetőséget látó és kihasználó, a társadalmának lehető legteljesebb ellenőrzésére törekvő államok foglalata. Természetesen a két halmaz egyike sem homogén, azokon belül eltérő mértékben valósul meg egyik oldalról a technológiai rendszerekre épülő totális kontroll, míg a másik halmaz államai között sem azonos mértékben veszik figyelembe a jogállami paradigma egyes pilléreit. Ennek ellenére érdemes elkülöníteni ezeket a modelleket és alapjaiban elemezni azokat.

5.1. A smart total control cyberfare state

Az előző fejezet rámutatott arra, hogy az államok egy köre a technológiai fejlesztések révén nemcsak a jóléti funkciókat erősíti a kibertérhez kötődő eszközök révén, hanem a lehető legteljesebb kontrollra törekszik polgárai felett. Az is látható volt, hogy ennek a gondolkodásnak az alapja a szuverén[347] internet elvének vagy kiberszuverenitásnak a megalkotása, amely körben minden állam rendelkezik saját, lehatárolható kibertérrel, amelybe nyilvánvalóan a hagyományos térben tapasztalható állami szabályozási, rendészeti és védelmi atitűdjét ülteti át.[348]

Adam Segal neves amerikai kiberbiztonsági szakértő rávilágít arra, hogy a kiberszuverenitás eszméjét Kína igen nagy mértékben azért fogalmazza meg és kívánja lehető legteljesebben kialakítani, mert e területen is globális hatalmi pozícióra tör, így az sem meglepő, hogy e koncepciónak egy belső és egy külső aspektusa van. Azonban nem feltétlenül ez az indoka annak, hogy a tézis elfogadottabbá válik, hanem az, hogy egyre több államnak okoz jelentős problémát a dezinformáció, a magánéletet és a magántulajdont fenyegető veszélyek, a gazdasági hozadékai a kiberbűncselekményeknek, és nem utolsó sorban sok állam visszásnak tekinti a nagy technológiai vállalkozások hatalmi koncentrációját, amely a szabályozatlan vagy alulszabályozott kibertérből ered. Azonban egy ilyen rendszer működtetéséhez megfelelő gazdasági és technológiai kapacitás is szükséges, mivel az elv kimondása önmagában nem fogja létrehozni a technológiai hátteret és az fejleszteni, működtetni, így az jelentős gazdasági forrással jár.[349] Kína mindezt sikeresen tudta kivitelezni, így a kínai kiberdiplomáciának egyértelmű és működő elvi alapja a kiberszuverenitás.[350] A modell egyértelműen következőkre talált azon államok között, amelyek hajlamosak amúgy is az kibertér elérésének korlátozására, il-

347 Szuverenitás fogalmáról l. bővebben: Horváth (1943), Pongrácz (2016): 108–119., Pongrácz (2020): 98–113.
348 Gosztonyi (2022b): 7–8.
349 Segal (2020): 86.
350 Molnár Dóra (2020): 357–371., Gosztonyi (2021b): 91–101., Gosztonyi (2021a): 87–99.

letve osztják a fenti aggályokat, és Kína a globális törekvései nyomán hajlandó is megosztani azt. Nem véletlen, hogy a kínai know-how átvételét láthatjuk vagy arra való törekvést Etiópiában, Egyiptomban, Jordániában, Libanonban, Líbiában, Marokkóban, Szaúd-Arábiában, az Egyesült Arab Emírségekben. De ez nem csupán a technológiában és az intézményrendszerben ölt testet, hanem a jogi szabályozás másolásában is. Tanzánia a kínaihoz hasonló kiberbiztonsági törvény fogadott el. Egyiptom, Laosz, Pakisztán, Uganda, Vietnam és Zimbabwe olyan törvényt fogadott el, amely kínai mintára lehetővé tette a weboldalak blokkolását, a valós név regisztrációját, az adatmegosztást és a tartalom eltávolítását.[351] Tehát Kína valós és működő alternatívát kínál mind szabályozás, mind technológiai vívmányok tekintetében. Tőle részben függetlenül, de ezen az úton jár Észak-Korea, Oroszország és Irán is. Ha nem is ekkora terrénumban, de lépéseket tett ebbe az irányba Törökország és Szingapúr is. Tehát azt kell mondani, hogy egyértelműen modellértékű a kínai kiberszuverenitás-felfogás, és nemcsak technológiai oldalról, hanem jogi, valamint szervezeti rezsim oldaláról is.

A kibertér és az ahhoz kapcsolódó rendszerek ilyen rendkívül sikeres – még, ha európai szemmel nézve, rendkívül visszás – kiaknázása, felhasználása és alkalmazása, amely főként Kínában vagy Oroszországban, Szingapúrban, illetve akár egyes aspektusokban Észak-Koreában figyelhető meg – de mint láttuk, emellett számos követő államra talált legalább részmegoldásaiban –, megteremtette a cyberfare state hatalmi államon nyugvó almodelljét. Ennek keretében az állam a birtokolt erőhatalom révén ténylegesen vagy jelentős terrénumában létrehozza a saját szuverén kiberterét, azt a lehető legteljesebb egészében birtokolja, ellenőrzi, az ettől elkülönült külső kibertérben megjelenő államok technikai, szabályozási, védelmi hiányosságait kihasználva pedig soha nem látható eredményeséggel tudja befolyásolni, eszkalálni más társadalmak töréspontjait, illetve tudja megbénítani egyes alrendszereit. Mindezeket anélkül, hogy legtöbb esetben ténylegesen fegyveresen konfrontálódna a megtámadott állammal.

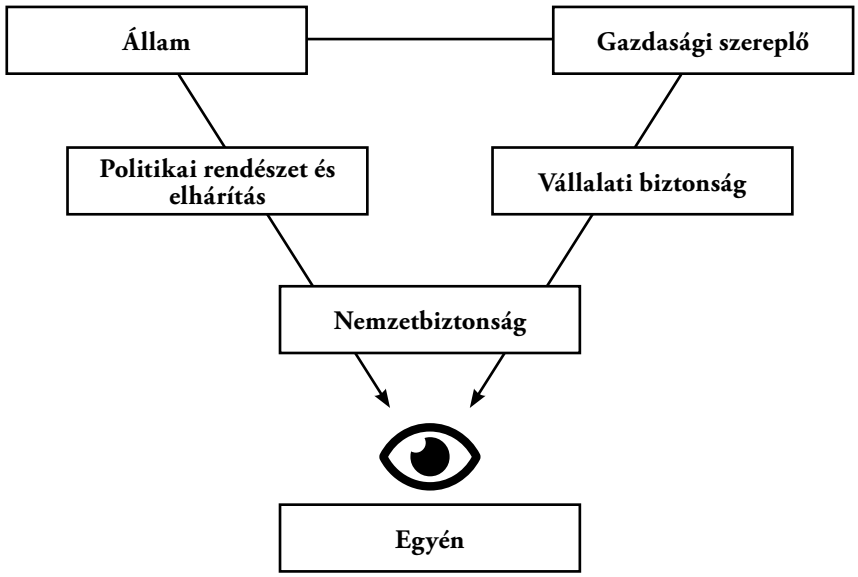
Ezt a rendszert azért működtetik, a tevékenységet azért valósítják meg, mert a kialakult új biztonsági környezetben meglátásuk szerint a totális felügyelet és totális „erőszak-monopólium a béke és a kiszámítható rend legfőbb biztosítéka"[352]. Ennek kialakításában pedig – mint láttuk – fúzióban tevékenykednek, működnek és fejlesztenek az egyes államok és gazdasági szereplőik. Az egyén ezekben az államokban a lehető legteljesebb kontroll alatt éli hétköznapjait, lényegében kizárólag egyes részobjektumok üzemeltetője (munkája révén) és fogyasztója a rendszer által engedett és kínált szolgálatásoknak, de valódi döntéssel nem rendelkezik adatvagyona felett sem. Ebben a közegben tehát az állam hatékony működését, biztonságának szavatolását az állam és a gazdasági szereplők összefonódása, érdekközössége teremti meg, ahol e közös cél érdekében az egyént mint a (kiber)biztonság legtörékenyebb láncszemét[353] megpróbálják kivonni, szerepét a lehető legcsekélyebb mértékűvé tenni, ennek pedig eszköze a személye feletti totális kontroll és adatai feletti állami és gazdasági rendelkezés totalitása.

Ezen államok (kiber)biztonság szavatolását jelentő legjobb gyakorlat kialakítása, folyamatos nyomkövetése és szükséges korrekciója az állam és az ebben érintett gazdasági szereplők közös érdeke és együttműködésük gyümölcse, amelyben az egyén nem érdekeltként, hanem kizárólag irányított, kontrollált erőforrásként jelenik meg. Ebben a legjobb gyakorlatban a kiber-

351 Segal (2020): 94–95.
352 Pongrácz (2017b): 9.
353 Informatikai szempontból l. Németh (2020): 23–41.

térre támaszkodó technológiai újításokon nyugvó szociális, jóléti intézményeket, végső soron szolgálató közigazgatás javítását, modernizálását társítják a totális kontroll és adatok feletti totális rendelkezés lehetőségével, amelyekhez sok esetben támadó potenciál kiépítése kapcsolódik. A cyberfare state ezen hatalmi jellegű attribútumokat felmutató államait a fentiek okán smart total control cyberfare statenek nevezhetjük.

SMART TOTAL CONTROL CYBERFARE STATE



2. ábra: Smart total control cyberfare state (saját szerkesztés)

5.2. A totális biztonság és védelem (jog)állami adaptációjának a lehetséges irányai

Ezzel szemben a nyugati államoknak a saját cyberfare state modelljük kialakítása során teljesen más alapokról kellett, kell indulniuk. A digitalizáció jóléti reformját már megkezdték a 2000-es évek elején, és ebben, ha nem is minden területen, de látványos sikereket értek el. Az előző fejezetben látható volt, hogy sikerrel alakították át a szolgáltató közigazgatást, nagy volumenű innováció jelent meg többek között az oktatás, a kutatás, az egészségügy területén, emellett rendkívül sikeres okos város programok[354] is futnak, de az önvezető járművekkel kapcsolatos projektek,[355] vagy az MI programok[356] is számos előnnyel kecsegtetnek.

354 A nyugati államok okos város projektjeiről, azok elvi alapjairól l. bővebben: Szalai (2020): 88–107., Rab–Szemerey (2018)

355 Ezzel kapcsolatos jogi dilemmákat l. bővebben: Somkutas–Kőhidi (2017): 232–269., Csitei (2020): 55–73.

356 Keserű (2019): 109–123.

Azonban itt is jelentős eltéréseket lehet kimutatni a másik pólus államaihoz képest, ugyanis ebben kulcsfontosságú, sőt élenjáró szereplők voltak a technológiai óriásvállalatok, azonban – szemben például Kínával – ez nem jelentette az állam és a gazdasági szereplők fuzionális összefonódását, ellenben sok esetben jelentős érdekellentétek alakultak ki, ami adódik a piacok struktúrájából, az állam és a gazdasági szereplők közötti kapitalista államfelfogás tradicionális ellentéteiből.[357] Szintén teljesen más képet mutat az egyéni adatok kezelhetősége ezen államok esetében. Sok esetben a transznacionális vállalatok gazdasági érdekeik fokozott érvényesítése érdekében a kezelt adatokkal visszaéltek, amely bár jelentős bírságot eredményezett, azonban gazdasági helyzetükben, társadalomban betöltött szerepükben ez nem jelentett változást. Itt az állam, vagy azok közössége próbál egyre szigorúbb szabályokat alkotni.[358] Másik oldalról az állam, a biztonsági környezet átalakulása miatt, próbálja a nemzetbiztonság sebezhetőségét csökkenteni, és az ehhez kapcsolódó információ éhséget csillapítani. Ez pedig ellentétes a gazdasági és az egyéni szereplők érdekeivel, emellett az alkotmányosan körülhatárolt állami működés miatt jelentős akadályokba ütközött, melyet sok esetben hangos ellenkezés, nemzetközi bírói fórumok előtti fellépés követett.[359] Ebben a közegben elképzelhetetlen volna az egyén, vagy akár a gazdasági szereplők feletti felügyelet még közel hasonló szintjének a kialakítása is, mint amit Kínában láthattunk. A kontrolleszközökön túl, a kibertérhez való hozzáférés korlátozása sem képzelhető el olyan mértékben, mivel egyes államok egyenesen alapjogoként tekintenek az internethez való hozzáférésre, de más államok esetében is garanciák garmadája védi azt.[360] Nem beszélve arról, hogy ez jelentősen szembemenne gazdasági szereplők profitorientált érdekeivel is. Ezek a megállapítások a békeidős, normál működésre igazak, ezeket jelentősen transzformálná egy klasszikus államközi konfliktus vagy a belső rendet támadó szélsőséges események, amelyeket egy teljesen más felhatalmazási közegben kellene az államnak megoldania. Egy ilyen helyzet elkerülése azonban minden érdekelt számára elsődleges érdekké kezd válni.

Az elmúlt évek konfliktusai, társadalmi feszültségei világossá tették, hogy valamiféle elmozdulás szükséges a biztonság digitális terrénumának fokozása frontján is, hiszen lassan a hétköznapok részévé válnak a zsarolóvírusok, a szolgáltatás megtagadó támadások, trollok tevékenysége,[361] amelyek más államokhoz vagy sok esetben a szervezett bűnözéshez kapcsolódtak.[362] A Covid19 járvány mellett megjelent az infodémia,[363] vagy a social media platformok

357 Szigeti (2017): 1–59., Pongrácz (2017a): 168–195.

358 Például GDPR rendelet szabályanyaga és gyakorlata. L. bővebben: Sepsi (2019). Egyéb területeken is akut problémák forrása: G. Karácsony (2021): 25–38.

359 L. a svéd és brit példát: Catalin Cimpanu: Sweden and UK's surveillance programs on trial at the European Court of Human Rights. zdnet.com/article/sweden-and-uks-surveillance-programs-on-trial-at-the-european-court-of-human-rights/

360 Gosztonyi (2020): 134–140.

361 Aro (2021)

362 Mezei (2019): 125–147.

363 A fogalmat a WHO vezette be és a következőképpen határozta meg: „az infodémia egy problémával kapcsolatos túlzott információáradat, amely megnehezíti a megoldás azonosítását. Magában foglalja az egészségügyi szükséghelyzet során terjedő félretájékoztatást, dezinformációt és pletykákat. Az infodémia hátráltathatja a hatékony népegészségügyi válaszintézkedéseket, továbbá zavart és bizonytalanságot kelthet az emberek körében." L. WHO: Coronavirus disease 2019 (COVID–19) Situation Report, 45. who.int/docs/default-source/coronaviruse/situation-reports/20200305-sitrep-45-covid-19.pdf

szűrőbuborék gyakorlata,[364] a fake news, a deepfake tartalmak már olyan irányba vitték el a véleménynyilvánítás szabadságát, ahol az egyén már sokszor nem tud különbséget tenni valós és valótlan tartalmak között. Az átlagos felhasználót jelentősen befolyásolják a véleményük, döntésük kialakítása során. Az ezekkel szembeni – jogállai keretek közötti – fellépés fontosságát mutatja, hogy az Európai Unió is szorosabb jogi keretek közé kívánja helyezni a közösségimédia-platformok működését, és átláthatóbbá kívánja tenni a szűrési mechanizmusokat is.

Ezek a feszültségek pedig egyértelműen kéz a kézben járnak a hagyományos tér biztonságának korróziójával is, mivel főként a külső szereplő általi szcenáriók abba az irányba is hatnak, hogy negatívan befolyásolják a közbizalmat. Ezeknek a kampányoknak a hatását erősítik, illetve létrejöttét lehetővé teszik egyik oldalról a lawfare, vagyis a joggal való rosszindulatú visszaélés,[365] valamint az államok jogi sérülékenysége[366] is, amelynek köszönhetően „kételyt, bizalmatlanságot szítsanak és megosszák a társadalmat".[367] Vagyis a transzatlanti térség jogállamisági garanciáit szükségszerűen figyelembe vevő nemzetbiztonsági szabályrendszere ismét a figyelem középpontjába került, ugyanis „ha a védelmi és biztonsági funkciók szabályozása nem kellően korszerű, nem kellően konzisztens, nem kellően stabil és kiszámítható, akkor az az állammal szembeni bizalom erózióját eredményezheti".[368] Ezzel az általános mechanizmust és az ahhoz kapcsolódó jogrendet is megkérdőjelezik. Így eljutnánk abba a helyzetbe, amit a fejezet felvezetőjében Szigeti Pétert idézve megfogalmaztam, hogy az állami szervek elveszítik társadalmi támogatottságukat, és az egyes szereplők végsősoron saját kézbe kívánnák venni a biztonságuk szavatolását, amely anarchiához vezetne, de legalábbis jelentős társadalmi törést hozna létre azok között, akik meg tudják fizetni a saját biztonságukat és azok között, akik nem. Ami elvezethet ahhoz, hogy a ma ismert alapjai tűnnének el vagy alakulnának át rendszerszinten a transzatlanti térséghez tartozó államoknak.

Ezzel pedig meg is érkeztünk ahhoz az indokhoz, amiért a nyugati pólus államainak három fontos szereplője az állam, a gazdasági aktorok és az egyén az együttműködés terepére kell, hogy lépjenek. A cyberfare state a transzatlanti térségben úgy formálható, alakítható ki tehát, hogy közben mindenféleképpen szavatolni kell a jogállam alapvető szegmenseit, de mindeközben meg kell teremteni a biztonsággal való egyensúlyt. Vagyis szemben a smart total control cyberfare state-tel, a totális biztonság felé való elmozdulás nem eredményezheti a szabadság felolvadását. Emellett azonban egyensúlyba kell hozni az egyéni és gazdasági érdekeket a valós biztonsági környezettel. Ugyanis a gazdasági szféra érdeke is a működőképes állami, gazdasági és társadalmi alrendszerek, amelyek nélkül elképzelhetetlen volna a kapitalista gazdálkodás megfelelő működése, a befektetések biztonságának a szavatolása. Ezt jól mutatják az ukrán–orosz háború jelenlegi gazdasági hatásai és visszásságai, továbbá a már jelzett hosszútávú hatások és törekvések (például Európa energetikai és védelmi önállósítása, mezőgazdasági hatásai stb.), de ezt erősítették a Covid19 világjárvány gazdasági hatásai is, illetve jelentősebb terrortámadásokat

364 Koltay (2019): 1–56.

365 A lawfare egy régóta ismert napjainkban folyamatosan szélesedő, de a hadviselési felfogásból kinövő értelmezési keret, amely a jogi normákat, vagy azok lehetséges értelmezését fordítja a szembenálló fél ellen. L. Petruska–Vikman (2021): 1–18., Hódos (2020): 49–64., Farkas–Resperger (2020): 132–149., Vikman (2021a): 44–56.

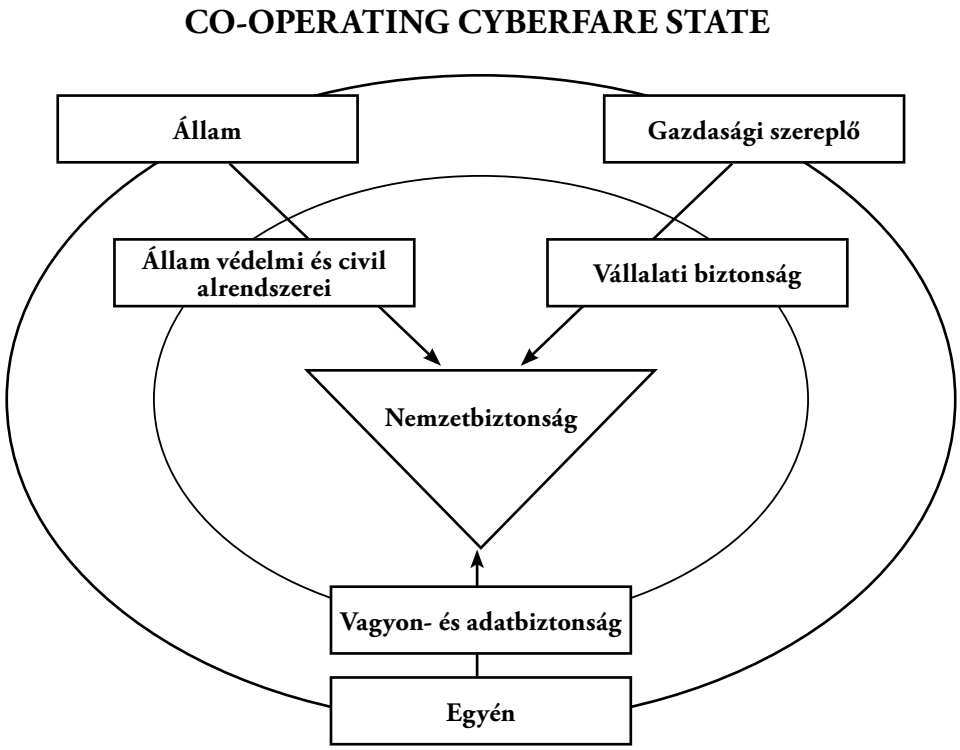
366 Szemben a lawfare esetkörével a jogi sérülékenység a komplex biztonsági felfogáshoz illeszkedő kategória, amely a társadalmi rezíliencia egyik fontos összetevője. L. Sari (2019a), Farkas Ádám (2022)

367 Hofstetter (2020): 85.

368 Farkas Ádám (2021d): 4.

követő tőzsdei reakciók is. Az egyén szempontjából az adatai integritása, a tulajdon védelme, a normális életmechanizmusok biztosítása csak működő állami intézményrendszer mellett képzelhető el. Az elmúlt években átalakult biztonsági környezet már alapjaiban támadja ezeket az alrendszereket, aminek rendkívül veszélyes fordulópontját jelenti az orosz–ukrán háború.

Az állam-gazdaság-társadalom kölcsönhatásos fungálására előnyként építő almodellt együttműködő vagy co-operating cyberfare state-nek nevezhetjük, ahol az együttműködés kiindulópontja szintén a jóléti, szociális digitalizáció. Ennek során a felek között olyan multidiszciplináris megközelítésen nyugvó legjobb gyakorlatot kell kialakítani, amely a jogállami garanciák mellett, a biztonság hatékonyságát is előtérbe helyezi. Ennek a legjobb gyakorlatnak magába kell foglalnia az állami szereplők, ezen belül a civil és katonai karakterű szervek[369] tapasztalásait, elvárásait, elméleti megközelítéseit, továbbá a gazdasági szereplők ugyanezen aspektusait, valamint a kutatói, innovációs oldalról nem kizárólag a műszaki tudományok képviselőit, hanem a társadalomtudományok (jogász, szociológus, közgazdász) és a hadtudomány művelőit is be kell vonni a munkába.[370]



3. ábra: Co-operating cyberfare state modellje (saját szerkesztés)

A deklarációk, a policyk, a stratégiaalkotás vonalán számos ilyen együttműködés megvalósulását vetítették előre, amelyek közül több már a megvalósítás pályájára is lépett. Ilyennek

369 Katonai karakterű szervek fogalmáról l. bővebben: Farkas Ádám (2012): 3–6.
370 Farkas Ádám (2021e): 22–28., Farkas Ádám (2022b)

tekinthető az egyes kiberbiztonsági stratégiák,[371] a NATO reziliencia programjai,[372] egyes államok kibervédelmi képességeinek kialakítása.[373] Az olyan össztársadalmi problémákat orvosló programok azonban, mint amilyenek például az Európai Unió többször meghirdetett, a dezinformációval szembeni média tudatos nevelése több év elteltével is csak a deklarációk szintjén létezik.[374] E területen érdemi elmozdulást jelenthet az új digitális szolgáltatókkal kapcsolatos jogalkotás,[375] illetve az állami hozzáállás változása.[376] Az egyén szintjéig ható, ténylegesen megvalósuló programokkal azonban nem igazán találkozhatunk, talán azért, mert eddig igazán akuttá a probléma nem alakult, káros hatásai viszont jelentős számban most is megfigyelhetőek.[377]

A jogállami keretek között működő cyberfare state esetében, a 21. század biztonsági környezetében nem hagyható figyelmen kívül az egyén szerepe sem. Nem véletlen, hogy a konkuráló államok mindent megtesznek annak érdekében, hogy az egyént, az egyéni döntés szabadságát kikapcsolják, hiszen a rendszer szempontjából a legjelentősebb biztonsági kockázatot továbbra is az emberek, az egyének jelentik. Ebből adódóan a co-operating almodell államaink jogállami keretek közötti válaszokat kell találniuk erre a kérdésre is, jelenleg azonban az látszik, hogy nem igazán tudnak mit kezdeni az egyéni szereplők tömegével, nem igazán tudják a helyüket definiálni a biztonsági környezetben, annak ellenére – ahogy a lenti ábrán látszik is –, hogy mind az állam, mind pedig a gazdasági szereplők alrendszereiben aktívan közreműködnek.

371 Vikman (2022a)

372 L. Molnár Ferenc (2021), Farkas–Spitzer (2021), Keszely (2018): 29–62., Vikman (2021b)

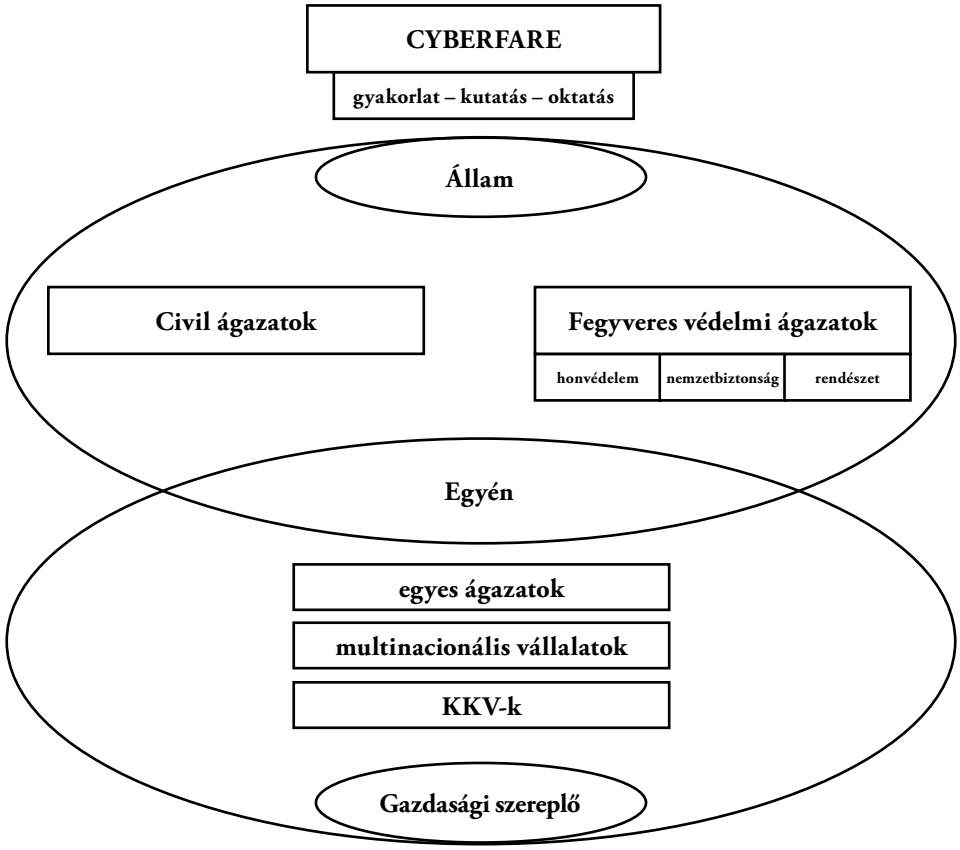
373 Farkas Ádám (2021b), Vikman (2021c)

374 Az Európai Bizottság és az Unió Külügyi és Biztonságpolitikai Főképviselőjének közös közleménye – Cselekvési terv a félretájékoztatással szemben, Join(2018)36. Final, Az Európai Bizottságnak közleménye az Európai Demokráciára vonatkozó cselekvési tervről. COM(2020) 790 Final.

375 Az Európai Parlament és a Tanács (EU) 2022/2065 Rendelete (2022. október 19.) a digitális szolgáltatások egységes piacáról és a 2000/31/EK irányelv módosításáról (digitális szolgáltatásokról szóló rendelet).

376 Gosztonyi (2021c): 40–54.

377 Aiken (2020), Murray (2020)



4. ábra: Az egyén relevanciája kibertérben a co-operation cyberfare state esetében (saját szerkesztés)

Az egyének munkaerőként és fogyasztóként is aktív szereplők, akik mindkét szerepükben potenciális veszélyforrások az állami és gazdasági rendszerekre, és természetesen ugyanekkora mértékben a saját adatvagyonukra vagy hagyományos tulajdonukra. Így szükségszerű volna meghaladni azt a felfogást, hogy az egyéni felelősség szintjére engedjük ezeknek a problémáknak a megoldását, amelyben még magára is hagyjuk az egyes szereplőket, azoknak tényleges tudása, képzettségi szintjétől függetlenül. E körben az együttműködés állami vonatkozásai és különösen a védelmi-biztonsági szegmense kapcsán is komoly lemaradást kell ma behozni a biztonságtudatosság szintjén, amivel a kibertérrel összefüggő biztonságfelfogást is szinkronizálni kell.[378]

Ezen államok esetében átfogó oktatási projekteket kell kidolgozni az iskolarendszer minden szintjén, hiszen ma már nemcsak kizárólag a magas kvalifikációt megkövetelő munkakörökben kerülnek az emberek kapcsolatba a kibertérrel és annak egyes alrendszereivel, hanem azok

378 Bányász–Krasznay–Tóth (2021): 130–149., Beláz–Krasznay–Szabó (2020): 242–252., Kiss–Krasznay (2017): 55–71., Farkas Ádám (2022c)

a hétköznapok részévé is váltak.[379] Fájdalmasan kijózanító jelenségként lehetett elkönyvelni, hogy az okoseszközök világában, például a Covid19 ellen védő vakcinákra történő regisztrációs rendszer elérése, kitöltése egyes egyének számára megoldhatatlan feladatot jelentett (itt nem a rendszer eléréséhez szükséges infrastruktúra hiányára kell gondolni vagy az idős állampolgárokra), míg ugyanők a hétköznapok során számos rendszerhez férnek hozzá. Ma már a felsőoktatásban sincs olyan oktatási terület, amelynek képzésébe ne volna feltétlenül szükséges beépíteni ezeket a készségeket, mert adott esetben vezetőként fog ezek hiányában dönteni az egyén a területet is érintő fontos kérdésekről, vagy ezeket nem ismerve működtett társadalmi alrendszert a potenciális veszélyforrásokat fel nem ismerve, ismertetve (például óvodai, iskolai nevelés). S legalább ugyanilyen fontos ezekben a problémákban a nyomon követés kérdése, hiszen a mindenkori új kihívásokhoz kell igazítani magát a képzést is. Ezek megvalósítása tovább már nem várathat magára,[380] hiszen a káros hatások már ténylegesen megindítottak akár deviáns folyamatokat is a társadalmon belül,[381] amelyek a halogatás révén nehezen visszafordíthatóak. Nem feledve az alapfelvetést, ha ezeket a társadalmi, biztonsági kihívásokat nem tudják kezelni a transzatlanti régió államai, abból végső soron az ellenpólus államainak intézményes győzelme is kialakulhat, amellyel önön képét veszítheti el a régió.

****

A cyberfare state mindegyik modelljében a kiindulópont a kibertérhez kapcsolódó rendszerek által az állam jóléti, szociális rendszereinek reformja, valamint a szolgáltató közigazgatás újradefiniálása. Emellett viszont jelentős eltérések mutatkoznak abban, hogy miként viszonyulnak ezeknek a rendszereknek a védelem és biztonság-szavatolás (angolszász megközelítésben: nemzetbiztonság) területén történő alkalmazásához.

A smart total control cyberfare state államfelfogása e körben visszanyúl a warfare state egyes jegyeihez, fúziót képez a gazdasági szereplők és az állam között, amelynek eredményeként a lehető legteljesebb mértékben kívánja kontrollálni polgárait és a kiberterét. Ennek során kidomborítják az állam hatalmi aspektusait, és saját biztonságuk szavatolását csak a hatalom révén, az erő által látják biztosítottnak. Így a „külső" kibertérben is aktívan használják a modern technológia által biztosított eszközöket.

A nyugati államok esetében is jelentős mértékű volt a digitalizáció, így eme folyamatok jelentős hatást gyakoroltak a társadalomra, gazdaságra és beágyazódtak a közigazgatási alrendszerekbe is. Az államra gyakorolt hatásuknak köszönhetően megteremtették a co-operating cyberfare state alapjait, vagyis a szereplők közötti folyamatos interakciót. Azonban a pozitív

379 A sérülékenységet és az oktatás szükségességét jól példázza az alábbi megállapítás: „Minden IT-biztonsági szakértő tisztában van vele, hogy a kibertérben a leggyengébb láncszem a humán faktor; a munkavállalók, akik – emberi természetükből fakadóan – jóhiszeműek, megtéveszthetőek, megfélemlíthetőek, nincsenek is tisztában a lehetséges kockázatokkal; éppen azért az ún. social engineering támadások célpontjai. Napjaink digitalizált világában minden munkavállaló kapcsolatba kerül számítógépes rendszerekkel, bizalmas adatokat kezel, és éppen ezért potenciális rizikóforrás. Ez a kockázat tovább növekszik azáltal, ha a munkavállaló a céges környezeten kívül, mérsékelt ellenőrzés mellett tevékenykedik." Németh (2021b): 101.

380 Erre is tökéletes példa az infodémia kérdésköre, amikor az emberek jelentős hánya hitt el olyan fake news híreket, amely szerint az oltások HIV-et okoznak, chipet ültetnek az emberi szervezetbe, népírtást követnek el velük stb. L. Sándor Judit: Az oltásellenes mozgalom érvei és a valódi válaszok – Tévhitek és tények. webbeteg.hu/cikkek/fertozo_betegseg/17762/tenyek–es–tevhitek–az–oltasokrol

381 Kiss (2020), Kiss–Pari–Prazsák (2019)

hozadékok mellett, mint fentebb láttuk, számos negatív biztonsági tapasztalás is hatással volt ezen típusú államokra is, így az állami és nem állami szereplők által képviselt erőszakos, jogellenes fenyegető fellépések és támadások kibereszközökkel való felerősítése, illetve a hagyományos fenyegetések kibertéri lehetőségekkel való kombinálása, amely szükségszerűvé teszi, hogy ezen államok esetében fokozódjon az egyes szereplők közötti együttműködés. Ebben viszont jelentős eltérés mutatkozik a másik almodellhez képest, hiszen az egyénhez való viszonyulás teljesen más képet mutat, ugyanis a jogállami keretek (békeidős) megtartása nem teszik lehetővé a polgárok fenti mértékű korlátozását. Sajátos, hogy szemben a másik almodellel, ebben az almodellben az egyes szereplők alapvetően ellenérdekeltek, mégis a megváltozott környezetben szükségszerű az együttműködésük. Ezen kooperációnak a biztonsággal kapcsolatos területek valamennyi szegmensére ki kell terjednie, kiemelten a modern technológia vívmányaira. Az együttműködésnek pedig egy legjobb gyakorlatot kell létrehozni, megújítva a jelenlegi alrendszereket.

A kialakított rendszernek nem eseti jelleggel, nem pillanatnyi kihívásokat kell kezelnie, hanem átfogó, rendszerszintű és hosszútávú megoldást kell létrehoznia, mindezt a jogállami attribútumok fenntartása mellett.

> „Rendeltetése ugyanis a totálissá váló biztonsági kihívások megelőzésén, elhárításán, illetve felszámolásán túl pontosan az, hogy kitörjünk a my lai-i, abu ghraibi, guantanamoi és egyéb árnyékokból, s valóban rendezett, átgondolt, a kor kihívásaihoz igazodó, de egyben jogállami”[382]

biztonsági modellt, legjobb gyakorlatot teremtsünk meg.

Azt is látni kell, hogy univerzális, minden államra, régióra alkalmazható megoldások nincsenek. A transzatlanti térség államai kulturálisan és történeti hagyományaikat tekintve rendkívül sokszínűek, így a kialakítandó rendszer esetében a nemzeti sajátosságokat, történeti, társadalmi tradíciókat szükséges figyelembe venni. Emellett az egyes megoldásoknak idomulniuk kell az alkalmazott szinthez, hiszen más igény formálódik meg egy multinacionális vállalatnál és egy KKV esetében, illetve egy helyi önkormányzat vagy országos szerv esetében. Az ellenőrzés, visszacsatolás, elemzés szükségszerű velejárója a rendszernek. A cooperating cyberfare state legjelentősebb kihívása az egyén elhelyezése ebben a rendszerben, tudatosságának kialakítása, megerősítése alapvető fontosságú a rendszer fenntartása, védelme és működtetése érdekében, amelyben a képzés, oktatás kiemelten hangsúlyos szerephez jut.

Ezen co-operating cyberfare state rendszereinek kialakítása átfogó reformot igényel, ami nélkül az átalakult biztonsági környezet kihívásaival (például hibrid konfliktusok ezen belül is kibertámadások, dezinformációk, radikalizmus, [kiber]terrorizmus stb.) hosszú távon nem tudnak eredményesen megküzdeni a transzatlanti térség államai. A reformnak pedig ténylegesnek és átfogónak kell lennie, és az orosz–ukrán háború geopolitikai történéseit látva azonnal meg kell indítani, ahol – az elmúlt évtizedek tapasztalásaival szemben – a reform nem abban rejlik, hogy a múlt fáradt és kopott ötleteit leporoljuk és újracsomagoljuk. Az igazi reform csak akkor valósulhat meg, ha elfogadjuk az új paradigmát és újradefiniáljuk az állam szerepét.[383]

382 Farkas Ádám (2018a): 70.
383 Kaladijan (1996): 103.

6. A kibertér állami-társadalmi-egyéni biztonsági szintjeinek metszéspontja: a reziliencia[384]

Az ellenállóképesség a komplex biztonsághoz való alkalmazkodás transzatlanti/nyugati slágertémájának is nevezhető az elmúlt évtizedben, aminek azonban mind társadalmi, mind pedig az egyénre vonatkoztatott pszichológiai értelmezése, irodalma is erősödő tendenciát mutat. Ha mélyebben belegondolunk, mind az egyénre, mind pedig a társadalomra vetített pszichológiai gondolkodás kapcsán kulcskérdés a reziliencia annak e néven nevezése nélkül is, hiszen a psziché torzulásaival kapcsolatos vizsgálódások célja tulajdonképpen ezek megelőzhetősége, illetve bekövetkezés esetén az egyensúlyi állapot, a mentális egészség helyreállítása, illetve a további állapotromlás fékezése.

Innen nézve a reziliencia kérdésköre a kibertér és humán vonatkozások tekintetében kulcskérdés, és jól kapcsolható az előzőekben leírt társadalmi és egyéni viszonyulások kérdésköreihez. Az ellenállóképesség ugyanis – épp úgy mint az immunrendszer – egy rendkívül sokrétű és összetett szisztéma, amelyben számos eltérő terület, viszonyulás, keret és intézmény együttes hatásaként érhető el egyrészről a változó körülményekhez és kihívásokhoz rugalmasan alkalmazkodó működés/magatartás, másrészről pedig az evolúciós értelemben egészséges veszélyérzetre épülő tudatosság kialakítása, amely a nem adekvát reakciók, illetve a nem kellően körültekintő viszonyulások kihasználását teszi megelőzhetővé. Úgy is mondhatnánk, hogy jelen kötet szolgálni kívánja az egyéni, társadalmi és állami reziliencia fejlesztését, hiszen a kibertér vonatkozásában a szélesebb megértés és a sokrétű kapcsolódások felvázolása útján kíván ismereteket közvetíteni, amelyek aztán a rugalmas és adekvát reagáláshoz felhasználhatók.

Egyértelműnek mutatkozik az is, hogy a komplex biztonság szinte mindenre kiterjedő felfogásából és ennek a kibertér miatt hatványozottan végbemenő kibontakozásából szükségképpen következik a társadalom kihívásokkal, fenyegetésekkel szembeni ellenállóképességének fontossága is az információs, a gazdasági, az egészségi, az ellátásbiztonsági, a bizalmi-érzelmi és számos más viszonyítási keretek tekintetében egyaránt. Ezt jelentősen felerősíti, hogy az információs társadalom korában talán soha nem látott mértéket ölt a tömegek információéhsége, digitális információs függősége, illetve ezen rendszereken keresztül történő befolyásolhatóságának lehetősége és hatástere. A kibertér azáltal, hogy a fizikai tér korlátairól részint elszakadni képes, számos értelemben nehezen ellenőrizhető információgenerálást és -áramlást biztosítani tudó, illetve valós idejű globalitást szavatoló „alternatív" térként jelenik meg, történelmi léptékben is sorsfordító hatáserősítője az információs tevékenységeknek mind pozitív, mind pedig negatív értelemben. Innen nézve a kibertér azonban megkerülhetetlen kulcsterülete az ellenállóképesség egyéni, társadalmi és állami dimenzióinak is, hiszen az új kihívási mátrixhoz igazodó új reagálási és felkészülési – ezáltal pedig ellenállási – megoldásokat is magában rejti, vagy hatásfokukban erősítheti.

A biztonsággal összefüggő ellenállóképesség fokozása azonban ma még inkább egy tág értelmezési keret, mint konkrét cselekvési renddel, eljárásrendszerrel vagy intézkedés-gyűjteménnyel leírható szisztéma. Úgy is mondhatjuk, hogy a reziliencia ma inkább követelmény és szemléleti séma, mint megoldási mátrix, de a cél az utóbbi felé való elmozdulás. A jelen állapot, vagyis a követelményrendszer-jelleg azonban azt erősíti, hogy a kibertér vonatkozásában is tekintsük át a kérdést, mivel az később háttértudásként segíthet értelmezni mind az EU, mind a NATO,

384 A téma kapcsán bővebben l. Farkas Ádám (2022a)

mind pedig a nemzeti szabályozási lehetőségek tekintetében felvázolásra kerülő gondolatokat. Ehhez azonban megkerülhetetlen az ellenállóképesség védelmi-biztonsági vonatkozásainak áttekintése.

Védelmi szempontból ez a témakör alapvetően a NATO-hoz köthető, és egyre inkább elterjed a tagállamok nemzeti szintű működésében, szabályozásában. Előzménye az átfogó megközelítés,[385] illetve a polgári komponensek szövetségi felkészülésbe történő fokozódó súlyú becsatolása, amelyek azonban a szövetség hagyományosan katonai jellegéhez igazodó civil-katonai együttműködésre helyezték a hangsúlyt. A reziliencia pont emiatt tekinthető jelentős újdonságnak, hiszen a szövetség hagyományosan katonai-védelmi súlyozottságán túlmutatva az ellenállóképesség kérdése már egy széles spektrumú, össztársadalmi felkészültség követelményrendszerét tárja elénk. Úgy is mondhatnánk, hogy a védelmi értelemben vett reziliencia egyfajta állami-társadalmi immunrendszer kialakítására, megerősítésére irányul, melynek számos megfogalmazása született az elmúlt években, sőt amely a NATO hivatalos fejlesztési irányultságában is kulcsszerepet kapott.[386]

Természetesen ez a fajta komplex felkészültség és ellenállóképesség számos nem katonai területre kiterjed az élelmezéstől az egészségügyön, a közlekedésen, a kommunikáción át a közrend fenntartásáig. Az információs technológia robbanásszerű fejlődése és az egyénekre, társadalmakra gyakorolt jelentős hatása, illetve az ebben rejlő lehetőségek szuverén államok destabilizálását szolgáló kihasználása[387] azonban kiemelkedő jelentőséget ad a reziliencia vonatkozásában a kibertérnek és az információs tevékenységeknek.[388] A kibertér kiterjedtsége, egyéni és társadalmi életre gyakorolt sokrétű hatásai mellett ugyanis az egyes társadalmak, állami-politikai rendszerek működésének nyílt szembenállás nélküli, információs-dezinformációs kampányok útján való befolyásolása napjaink biztonsági környezetében egyre jelentősebb teret nyer magának. Ahhoz tehát, hogy a kibertér és a nemzeti biztonság viszonyát megfelelően értelmezzük, nem elég arra törekednünk, hogy megértsük a kiberteret fogalmi oldalról, és hogy annak állami-társadalmi-egyéni vonatkozásait is áttekintsük, hanem szükséges az is, hogy annak szerepét a biztonságot fenyegető, illetve veszélyeztető jelenségekkel szembeni ellenállóképesség tekintetében megfelelően értelmezzük.

A reziliencia kérdés különösen a NATO tagállamok körében mutat fokozódó jelentőséget a politikai kommunikációban és a különféle szakpolitikai dimenziókban. Fontos azonban látni, hogy a szövetségi szintű iránymutatások és általános követelménytámasztások lefordítása, majd szakmai és tudományos parafrazálása legfeljebb abban lehet segítségünkre, hogy

385 A téma kapcsán l. Jakobsen (2008), Ringsmose–Rynning (2011), Keszely (2013), Molnár Ferenc (2012): 10–23.

386 L. NATO: *Strengthened Resilience Commitment. 14. Juny 2021.* nato.int/cps/en/natohq/official_texts_185340.htm, NATO: *Commitment to enhance resilience. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw, 8-9 July 2016.* nato.int/cps/en/natohq/official_texts_133180.htm, Molnár Ferenc (2021)

387 A téma kapcsán l. Aro (2022), McIntyre (2018), Farkas–Spitzer (2021)

388 A NATO megközelítés jobb érthetősége érdekében ki kell emelni, hogy a szövetségben a katonai gondolkodás jelentős súlya miatt a műveleti szemlélet meghatározó. A NATO tehát a különféle műveletek végzése, illetve az azokkal szembeni védekezés felől közelít. Ebben a megközelítésben pedig az információs műveletek jelentik a tágabb kategóriát, melynek része a kibertérben zajló műveletek csoportja, de ezen túl még számos más terület is, például a pszichológiai műveletek, az elektronikai hadviselés vagy az információ biztonság. Vö. NATO: AJP-3.10. Allied Joint Doctrine for Information Operations. NATO, November 2009, NATO: AJP-3.20. Allied Joint Doctrine for Cyberspace Operations. NATO 29 Janury 2020.

a témakört tudatosítjuk mind a szakmai közösségekben, mind pedig a döntéshozókban. A valódi nemzeti szintű ellenállóképesség erősítéséhez, illetve az erősítést megalapozó attitűd kialakításához azonban jelentősen meg kell haladnunk ezt a szintet, és mélyebben kell a témakört vizsgálnunk. Célszerű elgondolkoznunk azon, hogy az ellenállóképesség milyen horizonton és milyen mélységben kíván beavatkozást az állami és társadalmi rendszereinkbe azáltal, hogy a biztonság teljes spektrumára kiterjedő képesség- és működésrendszer kialakítására irányul. Ez a kiterjedtség ugyanis számos jogállami, értékbeli, gondolkodásbeli és bizalmi vonatkozással is egybe esik, amelyek miatt az eseti jellegű, legfeljebb adott intézményekre, szabályokra, témákra fókuszáló célzott beavatkozások, illetve a deklaratív rendelkezések önmagukban elégtelennek bizonyulnak a valós előrelépéshez. Az ellenállóképesség bázisa ugyanis innentől a társadalom, amelynek valódi bevonása egy sokrétű hatások kivédését segítő „immunrendszer" kialakításába szükségképpen együttműködést feltételez, kiterjesztve ezt annak a működési közegére és szemléletmódjára is, amelyben a kibertérnek megkülönböztetett jelentősége van napjainkban.

Ebben a megközelítésben a biztonságot megerősíteni kívánó felfogás, melynek szabályozási és működési mentalitása alapvetően imperatív/követelménytámasztó, vagy korlátokat és szankciókat meghatározó jellegű, szemben találja magát a polgári társadalom jogos szabadságigényével és kockázatvállalási lehetőségeivel, a különféle gazdasági érdekekkel és törekvésekkel, a fogyasztói és egyben információs társadalom újszerű és sajátos működési jellemzőivel, melyek évtizedek óta mélyen áthatják mindennapi életünket és amelyek tekintetében meg kell találni a hatékony működéshez egy többségi támogatottságot biztosító modust. E modus viszonylatában az információs tér jelentősége talán fel sem mérhető igazán, mivel a reziliens működéshez ez egyszerre jeleníthető meg információs csatornaként, vezetés-irányítási keretrendszerként vagy közegként, olyan környezeti halmazként, amelyben reagálást igénylő események valósulhatnak meg, illetőleg olyan platformként, ahol megfelelő megoldások mellett hatékonyan alakítható ki, tartható fenn, illetve erősíthető és védhető meg a társadalmi kooperáció és ezáltal az állami fellépés többségi legitimációja is. Ez pedig az állami cselekvés és szervezés számára jelentős működési kihívás, hiszen a hagyományos és vegytisztán parancsoló-szabályozó megoldásokkal a viszonyrendszerek ilyen széles körébe jelentősen beavatkozni demokratikus jogállamban, tartósan hatékony és támogatott módon kevéssé lehet. Hovatovább, a kibertér részben alternatív tér jellegéből, ha nagyon egyszerűen akarunk fogalmazni, akkor virtuális vagy tükörtér jellegéből adódóan az átfogó beavatkozás, illetve kontroll még autoriter, vagy diktatórikus rezsimekben is komoly kihívás jelent a mai kor színvonalán,[389] mind a társadalmi hatások, mind pedig a digitális tér folyamatos fejlődése, illetve az érintett államokra is kiterjedő fejlődési kényszer kölcsönhatásossága miatt.

Ha tehát a reziliencia védelmi és biztonsági vonatkozásait a maguk teljességében és az információs korszak sajátosságainak, azon belül pedig különösen a kibertér specialitásainak súlyozásával közelítjük meg, akkor magától értetődő, hogy egy elvi-szemléleti alapproblémával állunk szemben, amit a NATO szövegpanelek átvétele és ismétlése épp úgy nem old fel, mint az egyes eseti, ad hoc beavatkozások szisztematikus reziliencia-építésként való kommunikálása. Ez az alapprobléma abban ragadható meg, hogy a reziliencia előfeltétele a társadalom együttműködése, viszont a társadalom biztonságtudata, az időszakos és félelemalapú kilengésektől eltekintve, alapvetően nem a biztonsági szféra parancsoló/korlátozó szemléletmódjára van kondicionálva.

389 A téma kapcsán l. Kelemen (2022b)

Ezt a helyzetet pedig európai viszonylatban felerősíti két összefüggő történelmi tény. Az egyik, hogy a totalitarizmus-tapasztalat miatt Európában az állam védelmi és biztonsági képességeinek megerősítése a békés és szabadabb világrenddel szembeni eretnekségnek számított társadalmi-politikai szempontból mindaddig, amíg az új típusú, és emberáldozatokat, illetve biztonságerőziót követelő fenyegetések sora közvetlenül el nem érte Európát. A másik az, hogy az európai térségben a biztonság kemény – katonai, rendőri, titkosszolgálati – eszközökkel és képességekkel való fenntartása és megerősítése, mint költséges, de rendszerszerűen és hatékonyan piaci alapon nem szervezhető közszolgáltatás, az elmúlt évtizedekben nem volt prioritás, sőt negatív érzetű témakör volt a gazdasági, jóléti-fogyasztói fejlődést szolgáló forrásallokációhoz képest. Ezt a két történelmi tényt a társadalmi, információs-működési kondicionáltság terén pedig jelentős mértékben tudja felerősíteni a kibertér és az abban megjelenő rendkívüli mennyiségű, de lényegét tekintve legfeljebb csak kis részben kontrollált, validált információk áramlása, amelyek lehetővé teszik bármely érdekcsoportnak, hogy a védelmi és biztonsági képességek és megközelítés erősítésével szembeni érzéseit terjeszteni, sulykolni tudja a felhasználók körében. Ez utóbbi körben ugyanis a véleménynyilvánítás szabadságából fakadó gondolatközlésektől a különféle – egyáltalán nem/részben/egészben – megalapozott elméleteken át az európai államok kemény hatalmi karakterének újjáépítésében egyáltalán nem érdekelt gazdasági vagy hatalmi szereplők leplezett törekvéseiig terjedhet az információs csomagok mögött álló motivációs skála.

Akkor tehát, amikor a NATO resilience szemléletét kívánjuk tényleges – nemzeti szintű – immunirendszerré transzformálni, és ebben az információs korszak sajátosságaira is figyelemmel kívánunk lenni, szükségszerű, hogy fokozott figyelmet fordítsunk az állami-társadalmi kooperáció újragondolása mellett a kibertér egyéni, társadalmi és állami kiaknázásának kérdésköreire is. Ha úgy tetszik, akkor egy működőképes és valóban rendszerként működő reziliencia kialakításához a szövetség által meghatározottakat ezekre az alapvetésekre kell ráépítenünk, hiszen az előzőekben láttuk, hogy milyen sokrétűek a kibertér biztonsági vonatkozásai, illetve annak egyéni, társadalmi és állami megvalósulása között a különféle kölcsönhatások.

A NATO a reziliencia koncepcióját a washingtoni szerződés harmadik cikkére alapozza, mely szerint „jelen Szerződésben kitűzött célok hathatósabb elérése érdekében a Felek különkülön és együttesen, folyamatos és hathatós önsegély és kölcsönös segítség útján, fenntartják és fejlesztik egyéni és kollektív védelmi képességüket fegyveres támadással szemben”.[390] Erre a fajta kooperációs kötelezettségvállalásra építve a resilience azonban tartalmilag – akárcsak maga a NATO a hidegháború végét követő útkeresés után – túllép az eredeti, katonai szövetségi kereteken és a fegyveres támadással szembeni felkészülésen, mikor rögzíti, hogy

> „Minden NATO-tagországnak ellenállónak kell lennie ahhoz, hogy ellen tudjon állni egy nagyobb megrázkódtatásnak, például természeti katasztrófának, a kritikus infrastruktúra meghibásodásának, illetve hibrid vagy fegyveres támadásnak, és ki tudjon lábalni azokból. Az ellenálló képesség egy társadalmi képesség a sokkhatásokkal szembeni ellenállásra és az azokból való felépülésre, ami kombinálja a polgári felkészültséget és a katonai kapacitásokat.”[391]

390 A Magyar Köztársaságnak az Észak-atlanti Szerződéshez történő csatlakozásáról és a Szerződés szövegének kihirdetéséről szóló 1999. évi I. törvény. 3. cikk. net.jogtar.hu/jogszabaly?docid=99900001.tv

391 NATO: *Resilience and Article 3.* nato.int/cps/en/natohq/topics_132722.htm

Ebből a megfogalmazásból egyértelműen látható, hogy a resilience fókuszába, persze a kapcsolódó politikai döntések függvényében, de lényegében bármely nagyobb hatóképességű biztonsági kihívás vagy fenyegetés beleérthető. Különösen igaz ez akkor, ha az ellenállóképességet, hasonlóan az immunitáshoz, egy fokozatos reakciókra épülő rendszerként fogjuk fel, vagyis nem csak a sokkhatások szintjét elérő, azaz válságként azonosítható eseményekre nézve kívánjuk kialakítani, hanem már ezek kialakulását megelőző, az eszkaláció hatékonyságát és gyorsaságát mérséklő képességként is értelmezzük. Az immunrendszer analógiaként használása esetén a kiberteret az információs társadalom korában, ha nem is teljességgel, de nagy átfedéssel feleltethetjük meg a vérkeringés és a nyirokrendszer együttesének, amelyben a fennmaradáshoz szükséges anyagok áramlanak és a szervezet védekezésének is jelentékeny része megvalósul. A kibertér tehát a reziliencia szempontjából megkerülhetetlen, egyszerre jelenti az ellenállóképesség megerősítésének terét és lehetőségét, és egyben azt a teret is, amelyben számos károkozó áramolni, érvényesülni tud.

A szövetségi irányok jobb megértése érdekében célszerű kitekinteni a NATO resilience felfogásának főbb témaköreire, jelesül:

– a kormányzat és a kritikus kormányzati szolgáltatások folytonosságának biztosítására;
– az országon belüli és határokon átnyúló tartaléktervekkel és tartalékhálózatokkal számoló rugalmas energiaellátásra;
– az emberek ellenőrizetlen mozgásainak hatékony kezelésére;
– a megszakításokkal és szabotázzsal szemben is ellenállni képes rugalmas élelmiszer- és vízkészletezésre;
– a tömeges – egészségügyi jellegű – veszteségek kezelésének képességére;
– a reziliens – válsághelyzetben is működni képes – polgári kommunikációs rendszerek kialakítására; valamint
– a reziliens, NATO erők és polgári képességek gyors és folyamatos mozgását biztosítani képes közlekedési rendszerek kialakítására.[392]

A NATO által meghatározott hét fő resilience terület vagy irány a problémahorizontot egyértelműen mélyíti.[393] Ezt mind a NATO, mind az egyes államok azonosították, hiszen a reziliencia kialakítása, erősítése érdekében megkezdték a különféle koordinációs szerveik kialakítását, fejlesztését, illetve szabályozásaik korszerűsítését.[394] A társadalmi együttműködés és befogadóképesség fundamentális jelentősége is azonosításra került, mégis elsődlegesen úgy látszik, hogy az ellenállóképesség építésében jelenleg még inkább az állami fejlesztések és cselekvések rendjének kialakítása dominál. Ennek bázispontja pedig még, úgy fest, a klaszszikusan fegyveres, vagy más módon szuverenitást sértő behatásokon van, amit Wolf-Diether Roepke és Hasit Thankey[395] következő gondolata is tükröz:

392 Vö. NATO: *Resilience and Article 3* nato.int/cps/en/natohq/topics_132722.htm
393 A téma kapcsán l. Townsend–Agachi (2020), NATO CDS: *Enhancing the Resilience of Allied Societies through Civil Preparedness* nato-pa.int/download-file?filename=/sites/default/files/2021-04/011%20CDS%20 21%20E-%20RESILIENCE%20THROUGH%20CIVIL%20PREPAREDNESS_0.pdf, Hamilton (2016)
394 Kibertér tekintetében l. bővebben: Kelemen (2019c): 29–50.
395 A szerzők álláspontja kapcsán l. Roepke–Thankey (2019): 50–53.

> „Az ellenállóbb országok – ahol az egész kormányzat, valamint a köz- és a magánszektor részt vesz a polgári felkészülés tervezésében – kevesebb olyan sebezhető ponttal rendelkeznek, amelyeket egyébként kihasználhatnak, vagy amelyeket az ellenfelek célba vehetnek. Az ellenálló képesség ezért a tagadással történő elrettentés fontos szempontja: az ellenfél meggyőzése arról, hogy a támadás nem éri el a kívánt célokat."[396]

Elvitathatatlan és fontos elem természetesen az ellenérdekelt tevékenységektől való elrettentés, azonban ez a fajta megközelítés és mögötte egy indirekt vagy hibrid katonai stratégiai retorika talán eltereli a figyelmet a megcélzott területek nagyobb szabályozási és ebből következő állami-társadalmi kooperációs és politikai kulturális kérdéseiről, továbbá arról a tényről is, hogy az információs korszak kihívási palettáján egyszerre vannak jelen a szervezett, hálózatos vagy centralizált ellenérdekelt törekvések, valamint a szervezetlen, egyéni vagy kis csoportos indíttatású, de nagy számban halmozódó cselekmények, amelyekre a hagyományosan államközi fellépésre kialakított narratívák nem alkalmazhatók megfelelően. További mérlegelési szempont kell, hogy legyen az is, hogy a kibertér kulcsszerepe a mai társadalmi, gazdasági és biztonsági térben magával hozza azt is, hogy fejleszteni kell az állam kibertéri jelenlétét, de egyúttal alkalmazkodni kell a kibertér határokon, kultúrákon átívelő, rendkívül dinamikus és a társadalmi működésbe ágyazott globális működési elveihez. Ez ugyanis egyszerre teszi szükségessé az állam hagyományos reagálási képességének a kibertér irányában történő fejlesztését, de másik oldalról azt is, hogy az állam építeni tudjon a társadalmi kooperációra, illetőleg működését jobban elfogadhatóvá tudja tenni ebben a társadalmi dominanciájú közegben. Ezt az irányultságot jól tükrözi az Egyesült Királyság az elmúlt években, ahol évszázados állami funkcióelválasztásokat és titkosszolgálati hagyományokat kezdtek megbontani[397] annak a felismerésnek a talaján, hogy a kibertérben zajló biztonságszavatolás a régi, 19–20. századi alapokon álló megoldásokkal és szemléletmóddal nem tartható fenn hosszú távon.

Mivel jelen kötet célja a kibertér és a nemzeti biztonság kapcsolódásaira fókuszálni, ezért a NATO resilience irányai kapcsán is erre kívánjuk a hangsúlyt helyezni. E körben ki kell emelni, hogy a hét irány egyértelműen komoly kihívást jelent az elmúlt évszázadok fejlődésében a funkcionális tagozódás és a funkcionális felelősségmegosztás elvei felé elmozduló kormányzati rendszereknek is. Úgy is fogalmazhatnánk, hogy a valódi előrelépés kulcsa állami oldalról feltehetően ezen az irányon nyugszik, hiszen, ha az állam az információs korszak sajátosságaihoz igazodó módon nem tudja saját működését sem tartalmilag megújítani, akkor nehezen képzelhető el, hogy a többi hat – külső tényezők sokaságára építkező területen – valódi áttörést tudna elérni egy érdemi stressztest során. A nemzeti biztonság-kibertér-reziliencia hármasságban tehát a whole of government szemléletnek már államszervezésileg és ehhez kapcsolódva a kormányzati funkciók és felelősségek szabályozásának viszonylatában is jelentős súlya van, mivel úgy kell hatékony és koordinált megoldásra jutni, hogy közben a funkcionális elkülönülésben rejlő napi szintű, illetve a szakterület-specifikus előnyök megmaradjanak, de ne jöjjön létre se egy valóban hatékony működésre a 21. század dinamikájában képtelen ágazatok feletti mamutszervezet/vízfej, se pedig egy ágazatokon átívelő, de az ágaza-

396 Wolf-Diether Roepke – Hasit Thankey: Resilience: the first line of defence. nato.int/docu/review/articles/2019/02/27/resilience-the-first-line-of-defence/index.html

397 A téma kapcsán l. Farkas Ádám (2021b), Petruska–Vikman (2021)

tok érdekei miatt jól koordinálni képtelen „béna kacsa" állapot. Ezt a képletet tovább színezi, hogy a két véglet közé pozícionálandó összkormányzati szakértői képességnek/intézménynek tudnia kell önmérsékletet tanúsítania, vagyis nem elvonni a generalista és koordinatív szintre olyan feladatokat, amely stabil megalapozásához specializált és funkcionlista válaszok kellenek, hiszen akkor nem az átfogó szemléletű összekapcsolás, hanem a specializált szakmai alapok meggyengítése történik meg a valóságban.

Ebben a kérdéskörben a digitalizációnak szintén kimagasló szerepe van, hiszen az állam funkcionális diverzifikációját nem öncélú törekvések, hanem az állam által felügyelt környezet mind inkább fokozódó összetettsége indukálta az elmúlt másfél évszázadban. A digitalizáció rohamléptékű erősödése miatt az állami működésben is exponenciálisan nő a keletkező, elemzés-értékelésre váró, vagy közszolgáltatások miatt kezelendő adatok mennyisége, amelyek egy részét aztán megfelelően be is kell csatornázni az állam különféle specifikus szervei között. A whole of government szemlélet tehát digitalizációs kihívást is hordoz magában a hatékony digitális információmenedzsment, illetőleg a kormányzati működés irányításának biztonságos digitális módozatai, illetve a környezeti adatok elemzése terén, amely környezeti halmazban maga a kibertér is egy rendkívül jelentős szeletet képvisel rendkívül összetett és sokrétű folyamataival és jelenségeivel. Az összkormányzatiság dimenziójában ugyanis egyszerre van szükség a kibertér specializált értelmezésére, amit a kiberbiztonsági szakterületek tudnak megjeleníteni, illetőleg egy komplex értelmezésre is, amely a kormányzás összes többi szegmensét a kibertér útján érintő jelenségek megfelelő értékelését és reagálását tudja biztosítani, ami viszont már egy generalista szemléletet feltételez még hozzá a kormányzati központ szintjén.

E megközelítésben azt is mondhatnánk, hogy az a nemzeti ellenállóképesség koncepció, amely nem számol jelentős súllyal a kibertér egyszerre specializált és generalista szemléletű megközelítésével és reagálásával, illetve amely a kormányzati működésben nem tud egy egészséges egyensúlyt kialakítani a funkcionális-specializált szférák és a generalista-összkormányzati koordinációs szint között a politikai döntések valóban hatékony és reális alapokon nyugvó támogatása érdekében, az nehezen lehet korszerű és hatékony a 21. század információs korszakában. Ezt pedig tovább erősíti az az alapfeltevésünk, hogy a whole of government irányvonal a kibertér sajátosságaira megfelelően reflektálva a reziliencia tűzpróbája, hiszen amíg ez nem ölt testet egy valóban új és hatékony működési modellben, addig nem képzelhető el az sem, hogy a többi, valamilyen módon szakosított, specializált reziliencia irány vonatkozásában átfogó áttörést érhessen el az az állami irányítás, amely önnön működése terén nem lépett még szintet az információs korszak követelményei szerint. Ezen feltevésünket a nemzetközi környezet és a szövetség különféle példái egyaránt alátámasztják. Az észt digitalizációs modell, az egyes nemzetek különféle információfúziós és védelmi-biztonsági koordinációs modelljei, illetve a NATO madridi csúcstalálkozóján a kibertér fontosságának további hangsúlyozása, vagy éppen a Tallinnban működő NATO Cooperative Cyber Defence Centre of Excellence szakértői anyagai is ezt tükrözik.

III. rész

A kibertér biztonságának nemzetközi kapcsolódásai – Az egyes releváns Uniós és NATO dokumentumok tükrében

1. A kibertér és NATO

Hazánk 1999 óta tagja a NATO-nak, így a kibertérrel kapcsolatos biztonsági kérdésekben is iránytűként szolgálnak a szövetség szabályai, fejlesztési irányai. A NATO 2016-ban, Varsóban nyilvánította végérvényesen az ötödik hadszíntérré a kiberteret, amely mutatja, hogy a benne zajló folyamatok már alapvető fontosságúak a nemzetek biztonsága szempontjából is. A NATO kibertérrel összefüggő tevékenysége emellett nem csak hazánk, de a két szervezet közötti szoros együttműködés révén az Európai Unió kiberbiztonsági felfogására, stratégiájára és joganyagára is kihatnak. Ezek okán mindenképpen érdemes bemutatni, hogy a szövetség miként viszonyul a kibertérhez mint a társadalmi totalitás egy részéhez, illetve a kibertérhez mint műveleti térhez.

1.1. A NATO alapvető rendeltetésének a kollektív biztonságnak az értelmezése a kibertérben a Tallinn Manual 2.0 alapulvételével

A kollektív védelem lehetőségének jogi hátterét az Alapokmány 51. cikke jelenti. Olyan jellegű megállapodások és szervezetek létrehozását, amelyek „a nemzetközi béke és biztonság fenntartásának regionális jellegű tevékenységre alkalmas kérdéseivel foglalkoznak, feltéve, hogy az ilyen megállapodások és szervezetek, valamint tevékenységük az Egyesült Nemzetek céljaival és elveivel összhangban állanak”,[398] az 52. cikk kifejezetten lehetővé teszi.

Az Alapokmány előkészítése során azonban felmerült, hogy az erőszak általános tilalmát megfogalmazó 2. cikk (4) bekezdés annulálná azokat a törekvéseket, amelyeket a kollektív védelemi megállapodások létrehozása érdekében tettek az egyes államok. Így

> „az önvédelmi jogot és a kifejezést az amerikai államok az Alapokmány elfogadása előtt megkötött chapultepeci nyilatkozata miatt vették be az Alapokmányba annak érdekében, hogy a 2. cikk (4) bekezdése ne okozhasson zavart az oly nehezen kialkudott első amerikai biztonsági rendszerben.”[399]

Eme okból, az erőszak általános tilalma alóli kivételként az Alapokmányba emelt önvédelem és kollektív védelem lehetőséget teremtett egyéb védelmi típusú szervezetek létrehozására, amelyek közül a leginkább kiemelendő/kiemelkedő az 1949. április 4-én Washingtonban,

398 *ENSZ Alapokmány* 52. cikk (1) bekezdés
399 Kajtár (2015): 66.

tizenkét állam által aláírt szerződéssel létrehozott Észak-atlanti Szerződés Szervezete (North Atlantic Treaty Organization, továbbiakban: NATO).

Sulyok Gábor megfogalmazása szerint „a kollektív védelem tartalma prima facie elég egyértelműnek tűnik: a megtámadott, önvédelmi helyzetben levő államot más államok segítenek – katonailag vagy más módon – az agresszor elleni harcban."[400]

A Washingtoni Szerződés 5. cikke szerinti kollektív védelmi klauzula a következőképpen fogalmazza meg a fentieket:

> „A Felek megegyeznek abban, hogy egyikük vagy többjük ellen, Európában vagy Észak-Amerikában intézett fegyveres támadást valamennyiük ellen irányuló támadásnak tekintenek és ennél fogva megegyeznek abban, hogy ha ilyen támadás bekövetkezik, mindegyikük az Egyesült Nemzetek Alapokmányának 51. cikke által elismert jogos egyéni vagy kollektív védelem jogát gyakorolva, támogatni fogja az ekként megtámadott Felet vagy Feleket azzal, hogy egyénileg és a többi Féllel egyetértésben azonnal megteszi azokat az intézkedéseket – ideértve a fegyveres erő alkalmazását is –, amelyeket a békének és biztonságnak az észak-atlanti térségben való helyreállítása és fenntartása érdekében szükségesnek tart. Minden ilyen fegyveres támadást és ennek következtében foganatosított minden intézkedést azonnal a Biztonsági Tanács tudomására kell hozni. Ezek az intézkedések véget érnek, ha a Biztonsági Tanács meghozta a nemzetközi béke és biztonság helyreállítására és fenntartására szükséges rendszabályokat."[401]

Az 5. cikk részben keretjellegű rendelkezés, amely visszahivatkozik az Alapokmány 51. cikkére. Többletként jelenik meg benne, hogy az „egyéni vagy kollektív önvédelem" joga kötelezettségé alakul, ugyanis „a NATO tagállamai kötelesek egymásnak segítséget nyújtani, amennyiben bármelyiküket olyan fegyveres támadás éri, ami megfelel a washingtoni szerződésben foglalt feltételeknek"[402] ugyanis az 5. cikk felállítja azt a vélelmet, hogy „ha bármelyik tagot fegyveres támadás éri, akkor az valamennyi tag ellen irányuló fegyveres támadásnak minősül. Következésképpen egy tag – vélhetően – akkor is önvédelmi helyzetbe kerül, ha nem őt, hanem valamelyik másik szövetségesét éri fegyveres támadás"[403].

Az 5. cikk alkalmazhatóságáról azonban dönteni kell, amelyre a NATO legfőbb döntéshozó szerve, az Észak-atlanti Tanács jogosult, vagyis a casus foederis-be foglaltak fennállását meg kell vizsgálni és a klauzulát életbe kell léptetni.

> „Ezen a plénumon a többi tagállam is állást foglal arra nézvést, hogy valóban fennáll-e a megfelelő fegyveres támadás ténye, a kollektív védelmi kötelezettség gyakorlati érvényre juttatását pedig bárki »megakaszthatja«. Fontos körülmény tehát, hogy az egyes tagállamok csak együttesen kötelezhetők a kollektív védelem gyakorlására, egyenként nem."[404]

400 Sulyok (2002): 115.

401 *North Atlantic Treaty*, Washington D. C., 4 April 1949. A szerződés szövegét hazánkban kihirdette: 1999. évi I. törvény a Magyar Köztársaságnak az Észak–atlanti Szerződéshez való csatlakozásáról és a Szerződés szövegének kihirdetéséről. (továbbiakban: Észak–atlanti Szerződés).

402 Sulyok (2002): 120.

403 Uo., 122.

404 Pongrácz (2017b): 14.

Eme jogosultság/kötelezettség terjedelmére tekintettel meg kell jegyezni, hogy „a kollektív önvédelmi jog, amelyre teljes mértékben vonatkoznak az 51. cikk megkötései, azonban a nemo plus juris elve miatt nem ad többletjogosítványt az államoknak."[405] Ebből következőleg tehát a szükségesség, arányosság és időbeliségi kérdések a kollektív védelem esetében is irányadóak.

Érdemes emellett megvizsgálni az Észak-atlanti Szerződés 6. cikkét, amely rögzíti:

> „Az 5. cikk alkalmazása szempontjából egy vagy több Fél ellen irányuló támadásnak kell tekinteni fegyveres támadást
> a Felek egyikének területe ellen Európában vagy Észak-Amerikában, Franciaország algériai megyéi ellen, Törökország területe ellen vagy a Felek egyikének joghatósága alá tartozó, az észak-atlanti térségben a Ráktérítőtől északra fekvő szigetek ellen vagy a Felek egyikének hajói vagy repülőgépei ellen ugyanebben a térségben;
> a Felek egyikének fegyveres erői, hajói vagy repülőgépei ellen, ha a fenti területeken vagy azokon kívül bármilyen más olyan európai területen tartózkodnak, amelyen az egyik Fél a Szerződés hatálybalépésekor megszálló erőket tart."[406]

Mint az e könyv első fejezetében megállapítottuk, a kibertér a földrajzi tér egy speciális szelete, amely jelentősen eltérő térjellemzőkkel bír, amelyek okán nehezen feleltethető meg a hagyományos földrajzi tér fogalmaknak. Így a 6. cikkben található hagyományos földrajzi fogalmakra (és eszközparkra) alapított hatály meghatározás – a szöveg szószerinti értelmezését véve alapul – nem terjeszthető ki a kibertérre. Lehetséges támpontot ad eme szakasz kibővített alkalmazására – amit Kajtár Gábor a falklandi háborúval kapcsolatban állapított meg –, hogy „az állam elleni közvetlen támadás akkor is megvalósul, ha az az állam szuverenitása alá tartozó egyéb területeken következik be."[407]

Ennek okán rendkívül időszerű volt, hogy a NATO és tagállamai – főként az Észtországot ért támadást követően – szükségesnek ítéljék a kiberhadviselés nemzetközi jogi definiálását és esetlegesen a megfelelő jogi környezet kialakítását. Eme igény korporálódásának eredménye a Tallinni Kézikönyv első és második kiadása, valamint az a tény is – amely lehetővé tette a fenti okán a 6. cikk szerinti fogalmak kibertérre való értelmezését is –, hogy a NATO a kiberteret harctérré minősítette, amely révén a tagállamok védelmi kötelezettségét már ezen sajátos harctérre is kiterjesztette.

A nemzetközi jogi rezsim átalakítása vagy inkább kialakítása a kibertérre vonatkozóan még várat magára, ugyanis a jelenleg uralkodó álláspont szerint analógia útján a nemzetközi jogi rezsim szabályai alkalmazhatók a kibertérre is.[408] E vélekedés azonban nincs tekintettel arra, hogy a kibertérnek számos olyan jellemzője van, amelyek esetében nehezen alkalmazhatók a hagyományos hadviselés szabályai.[409]

405 Kajtár (2015): 68.
406 *Észak–atlanti Szerződés, 6. cikk*
407 Kajtár (2015): 101.
408 Almási (2009): 293.
409 Gondolok itt az állami szuverenitás problematikájára, a hagyományos tértávolságok feloldására, harcosok és hadviselők azonosíthatóságának kérdésére (lásd például zombihálózatok), célpontok katonai jellegének megállapíthatóságára, betudhatóság kérdéskörére, eszközpark sajátosságára stb.

A NATO szakértők által összeállított Tallinni Kézikönyv is az analógiát követve rögzíti, hogy a védelem jogát lehet kollektíven gyakorolni. Kifejti emellett, hogy fegyveres támadásnak minősülő kibertámadás esetében a kollektív védelem csak a megtámadott állam kérésére és a kérelemben foglaltak körén belül gyakorolható.[410] A Tallinni Kézkönyv 2.0 az első kiadáshoz képest már a kibertérre specifikusan próbálja értelmezni a kollektív védelmet. Ennek során kifejti, hogy a kollektív védelmi jogosultság lehetővé teszi, hogy egy vagy több tagállam éljen ezzel a joggal, ha fegyveres támadásnak minősülő kibertámadás éri a szövetség összes tagját (mindegyiküket [an attack launched against all of them] vagy annak egyes tagjait).[411] Aláhúzandó a kibertéri cselekmények sajátosságaként, hogy a szakértők szerint elképzelhető egy olyan támadás, amely akár a szövetség valamennyi tagállama ellen is irányulhat azonos idősíkban, amely a hagyományos térben folytatott hadviselés esetében nehezen volna elképzelhető.

A Tallinn Kézikönyv 2.0 a kollektív védelemről szóló alfejezetében – megegyezően az első kiadással – megfogalmazza, hogy a védelmi segítségnyújtás kereteit és határait a megtámadott állam rögzíti. Hangsúlyosabb ennél a két kiadás szóhasználata közötti különbség, ugyanis míg a korábbi kiadás – a nem kinetikus eszközökön túl[412] – a passzív kibervédelmi eszközökről aktív kibervédelmi eszközökre való átállás lehetőségét fekteti le (to passive rather than active cyber defences),[413] addig a második kiadás már sokkal gyakorlatiasabb módon azt mondja ki, hogy a megtámadott állam korlátozhatja azokat a célrendszereket, amelyek számítógépes műveletek tárgyát képezhetik (restrict the types of targets that may be made the object of cyber operations).[414] Tehát utóbbi esetében már fel sem merül, hogy önmagában a passzív kibervédelmi eszközpark alkalmas volna arra, hogy visszaverjen egy fegyveres támadás szintjét elérő kibertámadást.

Az Alapokmány 51. cikke által megalapozott kollektív védelem, valamint a NATO működésének alapjait lefektető Észak-atlanti Szerződés rendelkezései – bár néhol kitágított értelmezéssel, de – alkalmasak arra, hogy a kiberhadviseléssel szembeni védelem jogi alapjait jelentsék, azonban emellett – a szabályozás analóg jellege okán – szükséges a védelmi közösség szintjén kialakítani a kizárólag kibertérhez kötődő önálló mechanizmusokat. Ugyanis

> „figyelembe véve a NATO-nak a kiberhadviseléssel való találkozásait és az endemikus politika nehézségeit, a Szövetségnek olyan mechanizmust kell kidolgoznia, amely olyan egyértelmű jogi normákat hozhat létre, amelyek iránymutatásul szolgálhatnak a NATO személyzetének, ügynökségeinek és tagországainak."[415]

1.2. A kibertérrel kapcsolatos NATO törekvések

A NATO a kibertámadások létével először szövetségi szinten Szerbia 1999-es bombázása során szembesült, amikor a szerb (Fekete Kéz), az orosz (From Russia with Love) és a kínai

410 Schmitt (2013): 67.
411 Schmitt (2017): 354.
412 Nem kinetikus eszközökről l. bővebben: Rózsa (2017): 44–53.
413 Schmitt (2013): 67.
414 Schmitt (2017): 355.
415 Check (2015): 500–501.

hacker csoportok támadták a NATO és a tagállami kormányzati rendszereket. Volumenét tekintve ekkor ez még inkább volt alkalmas figyelemfelhívásra, mintsem egy olyan esemény, ami a szövetség, vagy egyes tagállamok működését jelentősen befolyásolni tudta volna. Azonban arra mindenképpen alkalmas volt, hogy érzékelje a szervezet, hogy a kibetér a későbbiekben releváns veszélyforrás lehet. Így a 2002-es prágai csúcson elindították a NATO kibervédelmi programját, amelynek részét képezte a NATO Számítógépes Incidens Reagáló Központ kialakítása, amely képessé tette a szervezetet arra, hogy érzékelje a NATO rendszereibe történő behatolást. Emellett azonban a tagállami hálózatok és rendszerek védelme továbbra is az adott állam feladata maradt.[416] Ezekben az években – nem felroható módon – a figyelem középpontjába a terrorizmus (9/11 és a 2004-es madridi terrortámadás) állt, és erre a kihívásra próbált választ adni a szövetség.

A kibertérrel kapcsolatos fejlesztések továbbvitelére és nagyobb ütemben való megvalósítására irányuló tényleges szándékot az Észtországot 2007-ben és Grúziát 2008-ban ért támadás váltotta ki a NATO-ban és tagállamaiban, ugyanis először ekkor vált láthatóvá, hogy milyen is lehet a kiberhadviselés valós arca. Ennek következtében a 2007 júniusi brüsszeli védelmi miniszteri csúcson megfogalmazták az igényt a tagállami kibervédelemi törekvések egységesítésére. Ezen törekvések egyik fontos állomásaként 2008 januárjában, Bukarestben új Kibervédelmi Irányelvet fogadtak el, amelynek célja a nemzeti eljárások összehangolása volt, mivel a „nemzeteknek is meg kell védeniük a kulcsfontosságú informatikai rendszereiket, meg kell osztaniuk a legjobb gyakorlatokat és olyan képességekkel kell rendelkezniük, hogy egy szövetséges állam segítségére siethessenek egy kibertámadás elhárítására."[417] Emellett szintén ezen év májusában felállították a NATO Kooperatív Kibervédelmi Kiválósági Központját Tallinnban, amely a NATO kutatási és oktatási központjaként funkcionál ezen a területen. Ezt további tizenöt kiválósági központ felállítása követte, amelyekhez Magyarország 2010-ben csatlakozott támogató országként.[418]

Ezzel párhuzamosan kezdte meg működését a Cyber Defence Management Authority (továbbiakban: Hatóság), amely a Cyber Defence Management Board-nak (NATO Kibervédelmi Irányító Testület) alárendelve végezi tevékenységét. A Hatóság feladatai a szövetségi szintű centralizált kibervédelem irányításának a megteremtése, valamint reagálás a tagállamokat érő támadásokra, továbbá segítségnyújtás a nemzeti kibervédelmek kialakításában. Emellett, a Számítógépes Incidens Reagáló Központnak alárendelve kialakították a Rapid Reaction Team-et, egy ún. gyorsreagálású csapatot, amely nemzeti szinten nyújt segítséget a támadások ellen, rövid idő alatt települve az adott országba. Nemzeti szinten pedig elkezdték kiépíteni a Computer Emergency Response Team-et (CERT – Számítástechnikai Sürgősségi Reagáló Egység).[419]

A 2009 novemberében kiadott információs műveletekről szóló doktrína (Allied Joint Doctrine for Information Operations AJP-3.10.) minden kétséget eloszlatott afelől, hogy a NATO innentől kezdve kiemelt területként kezeli a kiberteret és a hozzá kapcsolódó rendszereket. A dokumentum kiadásának a célja az volt, hogy közös alapot adjon az információs műveleteknek és megpróbálja átfogni az egyes nemzetek információs műveleti tevékenysé-

416 L. bővebben: Molnár Ferenc (2008): 50–51.
417 Siposné Kecskeméthy (2017): 117.
418 Szentgáli (2012): 79–82.
419 Szentgáli (2012): 83.

gét.[420] Kiadását azzal indokolták, hogy az új információs környezet kialakulásának a kezelése érdekében a NATO új doktrínák, koncepciók, folyamatok kidolgozásán fáradozik, ebbe beleértve az információs műveleteket. Ugyanis az információra támaszkodás és az információ iránti vágy egyre nagyobb, valamint a támadások a megújuló média miatt valós idejűek a közvetítő közeget felhasználva, manipulálva. Mivel az információ létfontosságú a stratégiai szinttől egészen a taktikai szintig, valamint a katonai műveletek teljes skáláján, ezért kiemelten fontos az információáramlás befolyásolása. A NATO felismerte azt is, hogy az információs technológiára épülő függősége egyre nagyobb, mivel a számítógépes rendszerek áthatják a társadalmat és ezek alkotják a legtöbb katonai rendszer magját is. Ez pedig új lehetőségeket, de új sebezhetőségeket is teremt. Az információs műveletek esetében kiemelt tény, hogy az internet kiemelt információforrás, amelyet ellenőrizetlenül, szűretlenül vesznek át az egyének és sok esetben nagy hitelt adnak neki, főleg a kevésbé szabad sajtóval rendelkező államokban. Amit, ha hozzárendelünk ahhoz, hogy az információ soha nem látott sebességgel terjed, az internet pedig korlátlan, alig szabályozott és világszerte elérhető, akkor ez egy kiemelkedő potenciál, azonban az ellenség is legalább ilyen hatékonysággal tud vele élni.[421]

Pontosan ezért, a műveletek során a számítógépes hálózatok felhasználását össze kell hangolni és szinkronizálni a többi eszközzel, ezzel javítva a támadási potenciált. Emellett legalább ennyire fontos a műveleti biztonság is, amelynek kiemelt részévé vált az információs biztonság, így minden katonai művelet szerves része a számítógépes biztonság (COMPUSEC), a számítógépes hálózat védelme (CND) és a számítógépes hálózati művelet (CNO), amiket a művelet során mindvégig figyelembe kell venni. A doktrína kiemeli, hogy a számítógép-hálózati műveletek hatékonysága arányos az ellenség informatikai függőségével. Ami lényegében annyit tesz, hogy a NATO tagállamok esetében kifejezetten nagy veszélyt jelentenek ezek a műveletek a digitalizáció magas foka okán. A számítógépes-hálózati műveletek három területre osztották fel: a számítógépes-hálózati támadásra (CNA), a számítógép-hálózatok kihasználására (CNE) és a számítógépes-hálózatok védelmére (CND). A CNA a szoftver-hardver sebezhetőségre épít, célja a rombolás, az adat manipuláció, az eszközteljesítmény megváltoztatása, amiket kifejezetten fokoz a kereskedelmi forgalomban lévő eszközök katonai rendszerekbe való alkalmazása. A CNE lényegében az információszerzést jelenti. A CND pedig az előző kettő elleni védelmet, mivel alapvetően fontos a döntéshozatali képesség fenntartásához a rendszer integritásának a megőrzése.[422] A doktrína jelentős előrelépés volt, hiszen rendkívül fontos területeken, az információs műveletek hatékonyságánál, a műveleti integritásnál, az információs rendszerek védelménél ismerte fel az akkor még lényegében kiépülés alatt lévő új típusú biztonsági kihívások egyik kiemelt pillérét jelentős kibertéri rendszereket, illetve az azokban rejlő potenciált.

A 2010. novemberi lisszaboni csúcs újabb lendületet adott a folyamatoknak, ugyanis itt elfogadták a NATO új Stratégiai Koncepcióját, amelynek immanens részét képezték a kibertéri folyamatok. A Stratégiai Koncepció a biztonsági környezetet vizsgálva leszögezte, hogy

> „a kibertámadások egyre gyakoribbá, szervezettebbé, illetve a kormányok, vállalkozások, gazdaságok és potenciálisan a közlekedési és ellátási hálózatok, valamint más kritikus inf-

420 NATO Allied Joint Doctrine for Information Operations AJP-3.10., XV. info.publicintelligence.net/NATO-IO.pdf (továbbiakban: AJP-3.10)

421 AJP-3.10., 1/1–3.

422 AJP-3.10., 1/8–11.

rastruktúrák számára is egyre nagyobb károkat okoznak. Elérhetik azt a küszöböt, ami már a nemzeti és euro-atlanti prosperitást, biztonságot és stabilitást veszélyezteti."[423]

Ennek elkerülése érdekében a Koncepció célul tűzte ki, hogy (1) továbbfejlesztik azon képességeket, amelyek szükségesek a kibertámadások megelőzése, felismerése, az ellenük való védelem hatékonysága és a helyreállítás terén, beleértve NATO tervezési folyamatának használatát a nemzeti kibervédelmi képességek növelésében és koordinálásában; (2) centralizált kibervédelem alá szükséges vonni minden NATO szervezetet, és e téren jobban össze kell hangolni a NATO tájékoztatási, előrejelzési és válaszadási képességét a tagországokkal.[424] Ennek megfelelően a 2011. júniusi brüsszeli védelmi miniszteri találkozón az új stratégiához igazították a Kibervédelmi Irányelvet és elfogadták az azt gyakorlatba átültető Cselekvési Tervet.

A 2012. májusi chicagói csúcstalálkozón ismét megerősítette a NATO a kiberhadviselés fontosságát. Leszögezték, hogy

„a kibertámadások továbbra is jelentősen növekedni fognak, mind számukat, mind kifinomultságukat és komplexitásukat tekintve. Megerősítjük a lisszaboni csúcstalálkozón tett kibervédelmi kötelezettségvállalásainkat (…) Vállaljuk, hogy biztosítjuk az anyagi forrásokat és véghez visszük a szükséges reformokat ahhoz, hogy minden NATO szerv központosított kibervédelem alá kerüljön annak érdekében, hogy a fokozott kibervédelmi képességekkel megvédjük a közös NATO értékeket (…) Továbbra is fejleszteni fogjuk azon képességeinket, amelyekkel képesek vagyunk a megelőzésre, a felderítésre, a védelemre és a kibertámadások következményeinek a felszámolására. A kiberbiztonsági fenyegetések kezelése és a közös biztonságunk fejlesztése érdekében elkötelezettek vagyunk, hogy párbeszédet folytassunk az érintett partnernemzetekkel, illetve nemzetközi szervezetekkel, mint az Európai Unióval, az Európa Tanáccsal, az ENSZ-szel és az EBESZ-szel annak érdekében, hogy erősítsük a konkrét együttműködést."[425]

A fejlesztési irányok kiolvashatók a 2012-es tallinni CyCon konferencián elhangzott előadásokból is, ezek egyike szerint

„a NATO kiberbiztonság területén az elosztott felelősség elvét alkalmazza, így szükség van a NATO és a nemzeti elkülönített kiberbiztonsági követelmények pontos megfogalmazására, illetve lehatárolására. Minimum követelményeket kell meghatározni azon nemzeti infrastruktúrák kiberbiztonságára, amelyek NATO műveleteket is támogatnak annak érdekében, hogy ne legyen biztonsági rés a NATO és a nemzeti infrastruktúrák védelmi szintje között."[426]

423 *Aktív Szerepvállalás, Modern Védelem – Az Észak–atlanti Szerződés Szervezetének Stratégiai Koncepciója Tagállamainak Védelméről és Biztonságáról.* (továbbiakban: *Stratégiai Koncepció, Védelem és elrettentés)* 5. oL.biztonsagpolitika.hu/documents/1291766875_NATO_Strat_Koncepcio_2010_hun_BSZK.pdf

424 *Stratégiai Koncepció, Védelem és elrettentés*, 19. pont, 8. bekezdés, 6.

425 *Chicago Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Chicago on 20 May 2012*. 49. pont nato.int/cps/en/natolive/official_texts_87593.htm#cyber

426 Ágota–Kassai–Tóth (2013): 185.

Mindezek folyományaként 2012. decemberében megjelent a nemzeti kiberbiztonsági keretrendszert bemutató kézikönyv,

> „amely részletes háttérinformációkat és elméleti kereteket biztosít a nemzeti kiberbiztonság különböző vetületeinek megértéséhez (…) iránymutatást nyújt a nemzeti kiberstratégia megalkotásához, az alkalmazási terület kijelöléséhez, az együttműködés dimenzióinak meghatározásához és a szabályozásra szoruló kritikus kérdések azonosításához."[427]

A 2014-es walesi csúcs meghozta a szükséges áttörést, ugyanis a záródokumentum 72. pontja deklarálta, hogy ahogy

> „a Szövetség a jövőbe tekint, a számítógépes fenyegetések és támadások egyre gyakoribbá, kifinomultabbá válnak, és potenciálisan károsak lesznek. E kialakulóban lévő kihívásnak való megfelelés érdekében támogatunk egy továbbfejlesztett kibervédelmi politikát, amely hozzájárul a Szövetség alapvető feladatainak a teljesítéséhez. A politika megerősíti a szövetségesek biztonságának, valamint a megelőzésnek, a felderítésnek, a rugalmasságnak, a helyreállításnak és a védelemnek az megosztására vonatkozó elveket. Emlékeztet arra, hogy a NATO alapvető kibervédelmi felelőssége, hogy megvédje saját hálózatait, és hogy a szövetségeseknek nyújtott segítséget a szolidaritás szellemében kell kezelni, hangsúlyozva a szövetségesek felelősségét a nemzeti hálózatok védelméhez megfelelő képességeik fejlesztése érdekében. Irányelveink továbbá elismerik, hogy a nemzetközi jog – beleértve a nemzetközi humanitárius jogot és az ENSZ Alapokmányát – a kibertérben is érvényesül. A számítógépes támadások elérhetik azt a küszöbértéket, amely veszélyezteti a nemzeti és az euro-atlanti jólétet, biztonságot és stabilitást. Ezek hatása ugyanolyan káros lehet a modern társadalmak számára, mint a hagyományos támadások. Ezért megerősítjük, hogy a számítógépes védelem része a NATO alapvető kollektív védelmi feladatának. Az Észak-atlanti Tanács eseti alapon dönt arról, hogy egy kibertámadás mikor vezetne az 5. cikk felhívásához."[428]

Erre azért is szüksége volt a NATO-nak, mivel Oroszország az elmúlt évtizedben bizonyította, hogy rendkívül jól kombinálja többek között a hagyományos hadviselést a kibertéri cselekményekkel.[429]

A 2016-os varsói csúcstalálkozón elfogadta a Szövetség a Kibervédelmi Fogadalom (Cyber Defence Pledge) elnevezésű dokumentumot. Eme dokumentumban a NATO tagállamok állam- és kormányfői elismerték a kiberfenyegetéseket mint a biztonsági fenyegetések új realitását, amellyel szemben megóvják nemzetüket. Ennek érdekében megerősítették kötelezettségvállalásukat, hogy minden tagállam a lehető legmagasabb szintű kibervédelmet alakít ki és együttműködik a többi tagállammal. Emellett elismerik az EU kibervédelem területén tett törekvéseit és tovább kívánják erősíteni a két szervezet közötti együttműködést. A NATO kibervédelmi potenciáljának növelése és a kibervédelem hatékonysága érdekében többek kö-

427 Beláz–Berzsenyi (2017): 7.
428 *Wales Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales* nato.int/cps/en/natohq/official_texts_112964.htm#cyber, 72. pont
429 L. bővebben: Szenes (2014): 3–26.

zött vállalták, hogy (1) a nemzeti kibervédelmet a lehető legmagasabb szintre fejlesztik és a lehető legteljesebb mértékben kiterjesztik; (2) a nemzeti kibervédelem területén kialakult gyakorlatok, szisztémák, fenyegetéssekkel kapcsolatos ismeretek, tapasztalatok cseréjét és a „legjobb gyakorlat" kialakítását; (3) hogy támogatják a képzéseket, tréningeket és a közös gyakorlatokat, amely segít egy közös tudásbázis kialakításában. Vállalták, hogy a dokumentumban foglaltak megvalósulása érdekében létrehoznak egy értékelési és nyomonkövetési rendszert, amely mentén a következő csúcstalálkozón megvizsgálják az előrehaladást.[430]

A szervezeti megoldások tekintetében – a fentebb már említetteken túl – rögzíteni kell, hogy a kibervédelemmel kapcsolatos válságkezelés felett is az Észak-atlanti Tanács látja el a felügyeletet. A Tanácsnak alárendelten működik a Kibervédelmi Bizottság (Cyber Defence Committee), amely a tagállamok tevékenységét felügyeli. A 2008-ban felállított Kibervédelmi Irányító Testület (Cyber Defence Management Board) felelős a gyakorlatban a kibervédelem összehangolásáért a polgári és a katonai szervek között. A NATO Tanácsadó, Vezetési és Irányítási Ügynökség (NATO Consultation, Command and Control Agency) felelős a kibervédelem technikai megvalósításáért.[431] Ezt a rendszert tökéletesít a védelmi miniszterek által 2017. november 8-án hozott elvi megállapodása alapján létrehozott Kiberműveleti Központ, amely a NATO korszerűsített vezetési struktúrájának a része. E szervezeti elem feladata, hogy megerősítse a NATO kibervédelmét, és elősegítse annak a NATO tervezési és műveleti rendszerébe való integrálását.[432] A feladata az elrettentés, a védelem, a reziliencia javítása, kapcsolattartás a nemzeti szervekkel és a tallinni kiberkiválósági központtal.

A 2018-as brüsszeli csúcson kiadott nyilatkozat szerint a nemzetközi biztonsági környezet veszélyes és kiszámíthatatlan, amelyek keretében a NATO-nak tartós kockázatokkal és veszélyekkel kell szembenéznie, ezek egyike a kibertámadás, de ehhez kapcsolódva a hibriditás is. Így kinyilvánította a szövetség, hogy továbbra is a legalapvetőbb funkciója, a kollektív védelmi tevékenysége kiterjed a kibertérre is. Mivel a szövetség biztonságát fenyegető kiberfenyegetések egyre gyakoribbá, összetettebbé, pusztítóbbá és kényszerítőbbé válnak, ennek során nem tehet mást a NATO, mint hogy folyamatosan alkalmazkodik a változó kiberfenyegetettségi környezethez. A kibervédelem része a NATO kollektív védelmi alapfeladatának, így képesnek kell lennie arra, hogy a kibertérben ugyanolyan hatékonyan működjön, mint a többi hagyományos műveleti területen. Ebből kifolyólag folytatják a lépéseket a kibertér mint műveleti terület megvalósítása irányába. Ennek a műveleti térnek pedig immanens része, hogy a képességek teljes skáláját alkalmazva a kiberfenyegetések egészével szemben tanúsítják az elrettentést, beleértve a hibrid szcenáriók részeként végrehajtott fenyegetéseket is. A műveleti tér fontos részeként meg kell erősíteni a hírszerzésen alapuló helyzetfelismerést, mivel csak ezzel tudják megfelelően támogatni a NATO döntéshozatalát és fellépését. A tagállamok pedig eltökéltek abban, hogy a Kibervédelmi Fogadalom teljes körű végrehajtása révén erős nemzeti kibervédelmet alakítsanak ki, mivel ez központi szerepet játszik a kibertámadásokkal szembeni reziliencia fokozásában. Kiemelte a csúcsot záró dokumentum, hogy a szövetség tovább kívánja fejleszteni a partnerségeit a szövetségesek iparával

430 *Cyber Defence Pledge* www.nato.int/cps/en/natohq/official_texts_133177.htm
431 Kovács László (2023): 128.
432 Cyber Defence nato.int/cps/en/natohq/topics_78170.htm#

és tudományos testületekkel, hogy az innováció révén lépést tudjon tartani a technológiai fejlődéssel.[433]

Ezen megállapítások egyik eredménye, hogy 2018-ban ténylegesen felállításra került a NATO Kiberműveleti Központja a belgiumi Monsban – Vass Sándor dandártábornok révén magyar vezetés alatt[434] – amely a kibertérben végzett NATO-műveleti tevékenység helyzetfelismerését és koordinálását biztosítja.[435] „Létrehozását a tervezők a különleges erők vezetési központja evolúciós modelljének mintájára képzelik el: először központ, majd önálló csoportfőnökség, végül független NATO parancsnokság jönne létre." [436]

2019 augusztusában terjesztette elő a Tudományos és Technológia Bizottság Susan Davis főelőadó jelentéstervezetét a NATO Parlamenti Közgyűlése elé. A jelentéstervezet A NATO a kiberkorszakban: a kiberbiztonság és védelem megerősítése, az elrenettentés stabilizálása című dokumentumot, amely egy rendkívül alapos helyzetjelentés mellett, kitér a lehetséges fejlesztési irányokra is. A dokumentum megállapítja, hogy az emberi társadalom minden területen összekapcsolódott, ahol a kiberfenyegetések száma rendkívüli, amire a NATO-nak is reagálnia kell, méghozzá ez egy sűrgősségi kérdés.[437] A jelentés, mivel a kibertámadások rendkívül sokszínűek, így kizárólag azokra koncentrál, amely a szövetség területi integritását, politikai függetlenségét vagy a nemzetbiztonságot fenyegetik, mégpedig oly mértékben, hogy akár a casus föderis is felhívhatóvá válhat. Ezt látszik igazolni Healey és Singh tanulmánya[438] is, ahol felvázolják, hogy a feszültségek fokozódásához hozzájáruló uralkodó tendenciák miatt a jövőbeni nyomáscsökkentő akciók már nem tekinthetők hatékonynak a feszültség enyhítésére, főként, ha az egyes államok a korábbi incidenseket oknak tekintik saját képességeik fejlesztésére, vagy a kibertéri műveleteket provokatívnak kezdik tekinteni. Véleményük szerint a támadó kiberműveletek ezáltal nagyobb valószínűséggel eszkalálódnak nyílt fegyveres támadássá, így a mérsékeltebb műveletek is egyre súlyosabbá válnak.[439]

Következik az előzőekből is, de maga a jelentés szerint is kétfelé lehet osztani a jelentősebb támadásokat: az egyik csoport, amely önmagában nagyon jelentős online, illetve offline hatással bír, illetve azon támadások, amikor a különböző rosszindulatú műveletek között a

433 *Brussels Summit Declaration. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels 11–12 July 2018.* 20. pont (tovabbiakban: *Brussels Summit Declaration*) nato.int/cps/en/natohq/official_texts_156624.htm

434 Kovács László (2021): 133.

435 *Brussels Summit Declaration*, 29. pont

436 Szenes (2018)*:* 59.

437 Science and Technology Commitee (STC) – *NATO in the Cyber Age: Strengthening Security & Defence, Stablising Deterrence.* (Draft General Report) by Susan Davis (United States) General Rapporteur. 13 August 2019. 1. (tovabbiakban: *NATO in the Cyber Age*) nato-pa.int/download-file?filename=/sites/default/files/2019-10/REPORT%20148%20STC%2019%20E%20rev.%201%20fin%20%20-%20NATO%20IN%20THE%20CYBER%20AGE.pdf

438 E tanulmányt azért érdemes itt beemelni a jelentés ismertetésébe, mivel a NATO Kooperatív Kibervédelmi Kiválósági Központ kutatói által készített, a 2020-as évtized végéig prognosztizált változásokat vázolja fel, amely nyíltan vállalja előszavában, hogy tartalmával célja, hogy segítse tájékoztatni a döntéshozókat, hogy azok jobban megértsék a kiberfenyegetések jellemzőit. Így az e kötetbe rögzített állítások bár nem a szervezet állásfoglalásai, de azok a kibertérrel, kiberbiztonsággal, kiberműveletekkel kapcsolatos lehetséges gondolkodási irányait felvázolják. Szemben a jelentéssel pedig már az orosz–ukrán háború kirobbanása után, annak realitásaival számolva adta közre gondolatait.

439 Healey–Singh (2022): 29.

határok elmosódnak és tartós kiber szcenáriót eredményeznek. A tartós szkenáriók veszélye, hogy lassan felemésztik a megtámadott erőforrásait.[440]

Healey és Singh a folyamatosan fennálló magas eszkalálódási veszély elkerülésére a nemzetközi együttműködés fokozását látja szükségesnek, emellett viszont lehetséges megoldásként fogalmaznak meg olyan eszközöket, amelyek sokkal inkább a NATO-val szembenálló blokkra jellemző, így a magánszektor egyes szereplőivel történő fúziószerű együttműködést, valamint a szuverén internet kialakítását, a keményebb virtuális határok feállítását.[441]

A tervezet mint lehetséges megoldás a folyamatos szerepvállalás stratégiáját említi meg, amelyet az Egyesült Államok kiberparancsnoksága dolgozott ki. A folyamatos szerepvállalás stratégiáját tartalmazó Achieve and Maintain Cyberspace Superiorty – Comman Vision for US Cyber Command című dokumentumot 2018-ban adták közre. E szerint a stratégia lényege, hogy az állandóságon keresztül ragadja meg a kiberfölényt és tartja fenn a kezdeményezést a kibertérben azáltal, hogy folyamatosan részt vesz az ellenség elleni harcban és vetélkedésben, ezzel bizonytalanságot okoz. A stratégia négy kérdésre épül:

– hogyan? védelem és támadás között manőverez
– hol? globálisan, lehető legközelebb az ellenséghez
– mikor? folyamatosan a harctér alakításával
– miért? hogy a műveleti előnyt szerezzen, ezzel gátolva, hogy más ilyent ki tudjon alakítani.

Kiemelik, hogy a műveleti fölény törékeny, mindig veszélyben van, ezért folyamatosan növelni kell a rugalmasságot, folyamatosan védekezni kell és folyamatosan fel kell venni harcot, mivel ez csökkenti a támadási felületet. Jelentős hangsúlyt helyeznek arra, hogy együttműködjenek más szereplőkkel, beleértve nem katonai kormányzati szerveket és a magánszektor kiválasztott szereplőit.[442]

A békeidős kibertámadások mellett kitér a jelentéstervezet arra, amikor a támadásokat válságok és konfliktusok során alkalmazzák, mivel a kibertámadások más katonai műveletekhez integrálva jelentős katonai hatásokkal járnak. Felhívja a figyelmet arra, hogy az alábbi intézkedések révén lehetséges a védelmi és támadó kiberképességeket integrálni a műveleti tervezésbe:

– kiberképesség fejlesztésével,
– parancsnoki struktúra átszervezésével,
– kiberdoktrinák kidolgozásával és beágyazásával az általános doktrínába,
– nemzeti és nemzetközi jog alkalmazhatóságának feltárása a műveletekhez.[443]

Kifejezetten problémás az ilyen műveletek során, amikor meglévő konfliktusban a kibereszközök révén aláássák a közbizalmat, mivel ez magasabb eszkalációs fokot eredményez

440 *NATO in the Cyber Age*, 2–3.
441 Healey–Singh (2022): 30.
442 Achieve and Maintain Cyberspace Superiorty – Comman Vision for US Cyber Command. United States Cyber Command, 6. cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010
443 *NATO in the Cyber Age*, 4.

a válságban, így a fentieken túl a NATO-nak az eszkaláció dinamikájára is több figyelmet kell fordítania.

A NATO-nak pedig ehhez kell igazítania a kiberpolitikáját, amelyben konkrét célokat és határidőket kell megfogalmazni, és ezt rendszeresen frissítenie kell. Ennek pedig a következő részei vannak:

– kibertámadások elhárítására irányuló stratégia,
– kiberképesség fejlesztése,
– kiberképességek NATO tervezésbe integrálása,
– konkrét együttműködés a NATO-n belül és
– NATO partnerség aktív építése.[444]

Az átfogó stratégiának három területre kell kitérnie: a jogi normákra, a kiberbiztonságra és védelemre, valamint az elrettentésre. A jogi normák esetén a NATO fenntartja, hogy a kibertérre a nemzetközi jog normáit kell alkalmazni, azokat kell továbbfejleszteni. A kibervédelem esetében a tagállami fejlesztés hangsúlyos, és lehetőséget lát az amerikai példában. Az elrettentés esetében a NATO fenntartja a kiberelrettentés kétértelműségét: egyfelől nem húz egyértelmű határt, hogy mikortól tekinti fegyveres támadásnak a támadást, másfelől pedig nincs operatív meghatározása arra, hogy mi lenne ebben az esetben a kollektív válasz. A tervezett kiemelt partnerként tekint az Európai Unióra és az CERT-EU-ra.[445]

Összességében a javaslat úgy véli, hogy az egyes tagállamoknak egyéni felelőssége van a kibertámadásokkal szembeni ellenállóképesség fenntartásában és fejlesztésében, amely a fentebb ismertet Fogadalom révén valósítható meg. A NATO erőfeszítéseinek viszont ennél összetettebb képet kell mutatni és ki kell térnie az alábbi területekre:

– kiberképességek fejlesztése,
– kibervédelmi kiadások növelése,
– NATO struktúra kiigazítása,
– kiberhatások integrálása a katonai műveletekbe,
– kiberstratégia és politika finomítása,
– együttműködés és a legjobb gyakorlat cseréje,
– információmegosztás,
– készségek és tudatosság fejlesztése nemzeti és NATO szinten,
– oktatás, képzés és gyakorlat,
– hatékony partnerség.[446]

Ezen területek visszaköszönnek a co-operating cyberfare state rezilienciájának kialakításához szükséges feltételek megteremtése körében. Ezért itt érdemes legalább röviden kitérni a reziliencia kérdéskörére. A társadalmi reziliencia kialakítása során csak az utóbbi években indult meg annak felismerése, hogy az állami, önkormányzati és gazdasági szereplőkön túlmutató ellenállóképességet növelő programokat, szabályozásokat kell kialakítani. Azonban

444 *NATO in the Cyber Age*, 5.
445 Uo., 5–11.
446 Uo., 12–13.

ezek, például a kínai, az orosz vagy a szingapúri rendszerekhez képest időbeli csúszásban vannak, és sok esetben még csupán bábállapotban léteznek. Már az is üdvözölendő, hogy a NATO néhol megcsúszva, de elkezdett fejlődési programokat kidolgozni. Ezt tükrözi vissza a NATO modern technológiákkal kapcsolatos Emerging Disruptive Technology (EDT) rendszere, amelyhez kapcsolódó tanácsadó csoport 2020-as jelentésében hangsúlyozta ezen technológiák társadalmi hatásait, valamint azt, hogy szükségszerű ezen a területen az oktatás és a képességfejlesztés. Utóbbiak azért elengedhetetlenek, mert ezek a technológiák rendkívül bonyolult rendszereket eredményeznek, ahol a politikai, gazdasági döntéshozóknak, illetve az egyéneknek úgy kell eligazodniuk, hogy nem rendelkeznek átfogó ismeretekkel, ami viszont elengedhetetlen volna a NATO versenyképességéhez akár szervezeten belül, akár azon kívül is. Ami viszont nem jelent egyet azzal, hogy minden szereplőnek mély műszaki ismeretekkel kell rendelkeznie, vagyis a cél sokkal inkább a tudatosság, az alapismeretek szintjének növelése, vagyis a technológiai műveltség magasabb szintre helyezése. A szervezeten belüli képesség növelésére kínálnak lehetőséget az egyes NATO képzési központok. Emellett elkerülhetetlennek vélik az együttműködés kialakítását a magánszektorral és a felsőoktatással is. Szintén kiemelik, hogy ezen együttműködések lehetőséget teremthetnek külsős ismeretterjesztő projekteknek, továbbá egyetemi képzések fejlesztésének, amelyek keretében a NATO mester- és doktori képzések esetében ösztöndíj-programokat hozhatna létre, ezzel növelve társadalmi elfogadottságát is.[447] A NATO, bár a gazdasági és akadémiai szférára irányultan megkezdte az együttműködés kereteinek kialakítását (ilyen a DINA-hoz [Defence Innovation Accelerator for the North Atlantic] és az EDT-hez kötődő tudományos tanácsadó testület is), azonban az egyénekre irányuló programok a gyakorlatban még váratnak magukra, pedig a szakértők között egyre inkább világossá vált, hogy „az emberek tömeges adatainak (…) elemzésével és felhasználásával cselekvésünk, gondolkodásunk befolyásolható (…) technikailag lehetővé vált az egyes társadalmak integritásának, az állami intézmények iránti bizalom kártékony befolyásolása is."[448]

A NATO egyértelműen megkezdte azt az építkezést, amire a fenti jelentéstervezet is felhívta a figyelmet, így nem véletlen, hogy 2020 januárjában kiadta a kibertéri műveletekre vonatkozó doktrínáját, amely a kibertéri műveletek tervezésének, végrehajtásának és értékelésének egységesítésére szolgál.[449] A dokumentum első része lényegében a doktrína megalkotásának alátámasztásául szolgál. Ebben kiemelik, hogy a szövetség egyre inkább összekapcsolt környezetben tevékenykedik, ahol az adatok szabad áramlása és a hálózatok zökkenőmentes működése kritikus fontosságú a civil társadalom és a katonai erők szempontjából. Az állami és nem állai szereplők e rendszerek sérülékenységét próbálják kihasználni, melynek során a céljuk a pusztítás, az adatszivárogtatás, a presztízs, a politikai vagy katonai előny- vagy haszonszerzés. És pontosan ezért kell kihangsúlyozni, hogy a kibertér több mint az internet, hiszen a kapcsolódó eszközök révén a hagyományos élettérre is hatnak, így minden ilyen eszköz potenciális veszélyforrás. Egy nemzet sebezhetősége tehát a kibertérben attól függ, hogy

447 NATO Advisory Group on Emerging and Disruptive Technologies – Annual Report 2020. Brussels, NATO Emerging Security Challenges Division, 2020. 10, 14–15. nato.int/nato_static_fl2014/assets/pdf/2021/3/pdf/210303–EDT–adv–grp–annual–report–2020.pdf

448 Molnár Ferenc (2021): 6.

449 Allied Joint Publication-3.20 Allied – Joint Doctrine for Cyberspace Operations. NATO standard, January 2020. (továbbiakban: AJP. 3.20.) XIV. assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf

mekkora az állam, a társadalom kitettsége, függősége a kibertéri eszközöktől. Ebből adódóan e területen alapvető fontosságú a képességek folyamatos fejlődése és fejlettebbé válása, amely eredményeként a rendszereknek reziliensnek kell lenniük.[450]

A kibertér jellemzői azonban megnehezítik a doktrína alkotását, ugyanis a kibertér tér jellemzői miatt nagyon nehéz a klasszikus műveleti határok kijelölése, annak ellenére is, hogy ez egy olyan globális tér, amelyben a földrajzi határok és a nemzeti hatáskörök érvényesülnek. Szintén a probléma összetettségét eredményezi, hogy a tér jellemzők során korábban felhozott különböző (fizikai, logisztikai, tartalmi) rétegek mindegyikét érinthetik a támadások, ezeken belül a logikait pedig biztosan érintik is. Emellett azonban a doktrína nem túl szerencsés kibertér fogalma is lehatárolná a mozgásteret – üdvözölendő, hogy a dokumentum többi része mégsem teszi, legalábbis nem ennyire –, mivel annak ellenére, hogy korábban és a dokumentum más részein is hangsúlyozza a kibertér társadalmi jellegét, ennek ellenére a fogalom kizárólag technológiai alapú, ezzel némiképpen kizárva a társadalmi realitás beemelését.[451]

A kibertér katonai kontextusainál viszont már kiemeli, hogy különböző társadalmi és technológia változások miatt a NATO hagyományos műveleti környezete bővült a kibertérrel, így szükséges a műveleti átállás a küldetésbiztonság/biztosítás területén is.[452] A szereplők (állam, nem állami szereplő, bűnözők, bennfentes) és az általuk kifejtett hatás is indokolja a sajátos kezelését a területnek, ugyanis az kibertér összekapcsolt jellege miatt alacsony költségű képességek aránytalanul nagy kárt tudnak okozni egy technológiafüggő nemzet esetében. Bennfentesek esetében hangsúlyozza a doktrína, hogy a kibertérben a személyzet minden tagja frontvonalban van.[453]

A doktrína áttekinti a kiberműveletek egyes kiemelt lehetséges részeit. Rögzíti, hogy a kibertérben a hagyományos célpontok mellett a kiberműveletek potenciális lehetőségekkel bővítik a célpontok körét (logika és tartalmi réteg entitásai), amelyekkel abszolút befolyásolni lehet az ellenfél harci hatékonyságát. Ezért a világosabb és átláthatóbb kiberműveletek érdekében egyes részterületeket érdemes áttekinteni. Kiemelt területek a kiberműveleten belül a következőek: manőver, tűz, parancsnokság és irányítás, hírszerzés, információ, fenntartás, erővédelem és a polgári-katonai együttműködés. A manőver az erőknek a harctéren való alkalmazása tűzzel vagy tűzpotenciállal kombinált mozgás révén. A kiberműveletek új teret nyitnak és kiterjesztik a parancsnok eszközeit a hadműveleti célok előfeltételeinek megteremtése és más manőverek támogatása tekintetében is. A tűz mindhárom réteg esetében elképzelhető. Oda és vissza, vagyis a kiberműveletet szükséges esetben támogathatja hagyományos tűz is, amikor olyan előfeltétellel kell teljesülnie, amely csak így teljesülhet. A tűz lehet támadó, védekező, támogató és támogatott. Ezeket be kell vonni a közös tervezési folyamatba a szinkronizáció és a közös koordinálás érdekében. A parancsnokság és irányítás területén a kibertér a hatékony parancsnokság tervezésének, összehangolásának és végrehajtásának az eszköze, amelyből következik, hogy a kiberműveletnek minden katonai területen hatása lehet. A hírszerzés esetében hangsúlyos, hogy a kibertér alapvető fontosságú az információk rendelkezésre állása és megosztása szempontjából, és így kiemelt szerepe van e körben. Az

450 Uo., 1.

451 Uo., 2–4.

452 Érdemes röviden elhatárolni az információs biztonságot a küldetésbiztonságtól. Előbbi az információk és rendszerek védelmével kapcsolatos biztonsági és védekező magatartást hangsúlyozza, míg utóbbi a kibertérben vagy azon keresztül folytatott tevékenységek operatív hatását foglalja magába.

453 *AJP. 3.20.* 5–6.

információ az olyan fő támogató tényezők, mint a stratégiai kommunikáció, az információs művelet, a pszichológiai művelet és a katonai közügyek elengedhetetlen eleme. A fenntartás esetében a haditechnika, a logisztika, az orvosi támogatás létfontosságúak, és ezek a kibertérre is támaszkodnak. Ma már az erővédelem, vagyis személyzet, létesítmény, művelet és tevékenység fenyegetésekkel és veszélyekkel szembeni sebezhetőségének minimalizálhatósága sem képzelhető el kibereszközök nélkül, mivel például a kibertéren keresztüli információszerzéssel megalapozható a művelet tervezése, formálása, hiszen naprakész adat szerezhető az ellenség képességeiről és szándékáról. Az egyik leginkább átformálódott terület a polgári-katonai együttműködés, amely lehetővé teszi a művelet átfogó megközelítését, amit a kibertér soha nem látott módon felerősít.[454]

A kiberműveletek karakterisztikája is eltér a hagyományos műveletektől, mivel eltérő a tér jellege, más a hatótávolság, hiszen a többi térre jellemző korlátok javarészt nincsnek jelen, emellett aszimmetrikus hatást gyakorol, mivel könnyű, gazdaságos és globális a hozzáférés, ahol az egyén vagy kis szervezet megfelelő tudással, motivációval és erőforrással a kibertérre vagy azon keresztül jelentősen nagy kárt tud okozni. Szintén sajátja az anonimitás, az időtényező átalakulása és a gyorsaság, illetve a sokoldalúság és az újrafelhasználhatóság.[455]

Ezeknek köszönhetően a kiberművelet lehet védekező (támadó kiberműveletre reagálás, esetleges visszatámadás kezelésére is szükséges terv) és támadó (önálló vagy más műveletek része). Ezek a kiberműveletek az alábbi hatásokat tudják elérni:

– biztonság (saját rendszereké),
– izolálás (ellenség és rosszindulatú kódja közötti kommunikáció blokkolása),
– elszigetelés (a kód tovább terjedésének a megakadályozása),
– semlegesítés,
– helyreállítás,
– manipulálás,
– szivárogtatás,
– lerontás,
– zavarás vagy
– megsemmisítés.

A NATO kiberműveleti doktrínája átfogó képet ad a problémáról, illetve annak lehetséges kezeléséről, azonban a biztonsági, védekezési oldalon továbbra sem hangsúlyos a polgári (civil) oldal rezilienciája, annak erősítése csak sporadikusan jelenik meg a dokumentumban.

Az Észak-atlanti Tanács a Covid19 járvány kezelése során felmerült kibertámadásokra, kiberártalmakra hivatkozva (gondoljuk itt a WHO által is azonosított infodémiára) 2022. június 3-án nyilatkozatot adott ki a rosszindulatú kibertámadásokról. Ebben kimondták, hogy elítélik a destabilizáló és rosszindulatú kibertevékenységet, amelyek a járvány elleni védekezés alapját jelentő kritikus infrastruktúrákra irányultak, így az egészségügyi szolgáltatásokra, kórházakra és kutatóintézetekre. A szövetség pedig támogatja az ezek elleni támadásokra való reagálást. Emellett pedig a Kibervédelmi Fogadalom alapján a tagállamok továbbra is elkötelezettek amellett, hogy a kritikus infrastruktúrák védelmét, ellenállóképességét kiépí-

454 Uo., 8–10.
455 Uo., 13–14.

tik megerősítik, fejlesztik. Továbbá a NATO fenntartja a 2018-as brüsszeli csúcstalálkozón elhangoztat: a kibervédelem a NATO kollektív védelemmel kapcsolatos alapvető feladatának a része. E tevékenység fontos eleme az elrettentés – lásd kiberműveleti doktrína – viszont szükséges volna a kibertérre vonatkozó nemzetközi normák kialakítása mivel ez minden állam érdeke, ezzel elkerülhetőek lennének az ilyen típusú incidensek.[456]

2021. június 14-én a NATO kiadta Kötelezettségvállalás az ellenállóképesség megerősítéséről című nyilatkozatot. A szövetség állam- és kormányfői kijelentették, hogy a nemzeti és kollektív ellenálló képesség a hiteles elrettentés és védelem, valamint a szövetség alapvető feladatainak hatékony teljesítéséhez nélkülözhetetlen és ezért megújították és megerősítették a 2016-ban Varsóban tett kötelezettségvállalásukat. A dokumentum kimondja, hogy az ellenállóképesség nemzeti felelősség és kollektív kötelezettségvállalás. A NATO nemzeti ellenálló képességre vonatkozó alapkövetelményeit folyamatosan frissíti a felmerülő kihívások és prioritások tükrében, ez pedig átfogó keretet biztosít fegyveres erők és a NATO alapvető feladatainak. Az eddig eredmények ellenére e követelmények területén kötelezik magukat arra, hogy fokozzák erőfeszítéseiket. Ennek fényében megállapodtak a NATO 2030 keretében abban, hogy növelik az ellenálló képességüket a tagállamok. Megállapították, hogy az ellenállóképesség továbbra is nemzeti hatáskör, azonban szükséges integráltabb és jobban összehangolt megközelítés, amely összhangban van a NATO 3. cikke szerinti kollektív kötelezettségvállalással. A szövetség tagjai javaslatot dolgoznak ki a következők létrehozására: értékelésre, felülvizsgálatra és nyomon követésre az ellenálló képességgel kapcsolatos célkitűzések terrénumában. Minden tagállamnak meg kell határoznia, hogy miként alakítja ki és teljesíti a nemzeti ellenálló képességgel kapcsolatos célokat és végrehajtási terveket.[457]

Az ellenállóképességet fenyegető, állami és nem állami szereplők által megvalósított fenyegetések változatos formákat öltenek. Ezek közé tartoznak a hagyományos, nem hagyományos és hibrid fenyegetések és tevékenységek; a terrortámadások; a növekvő és egyre kifinomultabb rosszindulatú kibertevékenységek; a társadalmak destabilizálására irányuló, egyre inkább elterjedt ellenséges információs tevékenységek, beleértve a dezinformációt; valamint a demokratikus folyamatokba való beavatkozásra irányuló kísérletek. A tagállamok elkötelezték magukat, hogy fokozni fogják az ellátási láncok, a kritikus infrastruktúrák és a kulcsfontosságú iparágak ellenállóképességét. Kiemelt terület az újonnan megjelenő technológiák hatásainak kezelése, így a következő generációs kommunikációs rendszerek, a technológia és a szellemi tulajdon védelme, valamint az energiabiztonságot érintő kihívások kezelésére, illetve az éghajlatváltozás hatásainak kezelése. Fokozni kívánja a szövetség az ellenálló képességet a szilárd, rugalmas és interoperábilis katonai képességekbe történő beruházások megerősítésével.[458]

Kifejtették, hogy az ellenállóképesség megerősítése széles körű megközelítést igényel, amibe be kell vonni a kormányzat egészét, a magán- és a nem kormányzati szektorokat, a szakértői központokat, valamint társadalmi szervezeteket és lakosságot, de a partnerségi és együttműködési területen is előre kell lépnie a szövetségnek. Ide tartozik az Európai Unió is, fenntartva a közös értékeket kölcsönösen kiegészítő és előnyös koordinációt a reziliencia

456 *Statement by the North Atlantic Council concerning malicious cyber activities* nato.int/cps/en/natohq/official_texts_176136.htm

457 *NATO – Strengthened Resilience Commitment. 14. Jun. 2021.* 1–6. pont nato.int/cps/en/natohq/official_texts_185340.htm

458 Uo., 7–9. pont

erősítése érdekében. Kiemelten fontos gondolatokkal zárul a nyilatkozat, hiszen úgy fogalmaztak, hogy az ellenállóképesség alapja az egyéni szabadság, a demokrácia, az emberi jogok és a jogállamiság elvei iránti közös elkötelezettség. Amely egyértelmű szembehelyezkedés a másik pólus államainak már megtett intézkedéseivel.[459]

A 2022-es madridi csúcs központi témáját egyértelműen az orosz–ukrán háború adta, így az Ukrajna melletti kiállás, valamint a háborúval kapcsolatos megoldáskeresés kiemelt témák voltak. A kibertér ennek okán, illetve ellenére továbbra is központi terület volt. A csúcsot záró deklaráció kimondta – hasonlóan a korábbiakhoz –, hogy a kiber-, űr-, hibrid és egyéb aszimmetrikus fenyegetésekkel, valamint az új és bomlasztó technológiák rosszindulatú használatával kell szembenéznie a szövetségeknek.[460] A szervezet elkötelezett amellett is, hogy folytatja Ukrajna támogatását Oroszországgal szemben, ennek részét képezi a nem halálos védelmi felszerelések szállítása, ezzel például javítja Ukrajna kibervédelmét és ellenálló képességét.[461]

Ezen deklarációnak is kiemelt eleme a reziliencia. Továbbra is hangsúlyozzák, hogy az ellenállóképesség nemzeti felelősség és egyben kollektív kötelezettségvállalás. Meg kell erősíteni az ellenállóképességet, ennek eszköze – a korábban ismertetett nyilatkozat szerinti – nyomonkövetési rendszer. Az orosz–ukrán háborúval kiemelt jelentőségűvé vált az energiabiztonság is. Fel kívánják gyorsítani a szövetség alkalmazkodását, és növelni az ellenállóképességet a kiber- és hibrid fenyegetésekkel szemben. Ennek érdekében a politikai és katonai eszközöket integráltan fogják alkalmazni. A NATO jelentősen meg akarja erősíteni a kibervédelmét a fokozott polgári-katonai együttműködés révén. Bővíteni fogják ezért az iparral való partnerséget is. Ami egyértelműen kiemelt figyelmet érdemel, hogy a szövetségesek önkéntes alapon és nemzeti eszközök felhasználásával virtuális gyors reagálású kiberképességet fognak létrehozni és törekszenek a folyamatos gyakorlatokra a rosszindulatú kibertevékenységekre való reagálás érdekében.[462]

A szövetség ugyanezen a napon kiadta a NATO 2022 stratégia koncepció című dokumentumot. Ebben öt cél és elvet jelölt meg. (1) A NATO tántoríthatatlan szándéka, hogy megvédje a szövetségesek szabadságát és biztonságát, minden irányú fenyegetéssel szemben. (2) A szövetség lét nélkülözhetetlen a régió biztonságához, ez pedig az azonos értékekre épül, mint az egyéni szabadság, az emberi jogok, a demokrácia és a jogállamiság. Így tekintenek az Európai Unió céljaira és elveire is. (3) A NATO egyedülálló és nélkülözhetetlen fórum arra, hogy koordináljon és cselekedjen az egyéni és kollektív biztonsággal kapcsolatos valamennyi kérdésben. E tekintetben pedig a szövetség oszthatatlan a biztonság, szolidaritás és egymás védelme iránti elkötelezettség területén. E kötelezettségvállalás gerincét a szövetség elrettentő és védelmi képessége adja. (4) A NATO három alapvető feladatot lát el: elrettentés és védelem; válságmegelőzés és kezelés; valamint az együttműködés biztonság érdekében. (5) A NATO fokozni fogja egyéni és kollektív ellenálló képességet és növelni akarja a technológiai előnyét, mivel ezek döntő fontosságúak a szövetség alapvető feladatainak teljesítéséhez.[463] Jól látható, hogy a 2018 utáni dokumentumok

459 Uo., 10–11. pont

460 *Madrid Summit Declaration. Issued by NATO Heads of State and Government participating in the meeting of the North Atlantic Council in Madrid 29 June 2022.* (továbbiakban: Madrid Summit Declaration). 6. pont nato.int/cps/en/natohq/official_texts_196951.htm

461 Uo., 8. pont

462 Uo., 10. pont

463 *NATO 2022 Strategic Concept*. Adopted by Heads of State and Government at the NATO Summit in Madrid, 29 June 2022. 3. (továbbiakban: *NATO 2022 Strategic Concept*) nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf

mindegyikében hangsúlyos a közös transzatlanti értékrend, amire a szövetség épül, valamint az együttműködés az Európai Unióval, továbbá a reziliencia kérdése.

A dokumentum a biztonsági környezet elemzése során kitér arra, hogy az ellenséges pólus tekintélyelvű államai kihasználják a szövetség államaira, társadalmaira jellemző összekapcsoltságot, nyitottságot és a magasfokú digitalizációt, így rosszindulatú tevékenységet folytatnak kibertérben, dezinformációs szcenáriókat támogatnak. A legjelentősebb és legközvetlenebb fenyegetés az euróatlanti térségben Oroszország, amely hagyományos, kiber- és hibrid eszközöket is használt a szövetséggel szemben. A kibertér önmagában is kiemelten fontos terület, ugyanis a rosszindulatú szereplők arra törekednek, hogy lerombolják a kritikus infrastruktúrákat, zavarják a kormányzati szolgáltatásokat, hírszerzési információkat szereznek, szellemi tulajdont lopnak és akadályozzák a katonai tevékenységeit a NATO-nak.[464]

A NATO fő feladatai közül kibertér szempontjából a dokumentum az elrettentést és a védelmet emeli ki. Hangsúlyozza, hogy a NATO egy védelmi szövetség, de senki sem kételkedhet erejében és elszántságában azon a téren, hogy megvédi a szövetséges területeit és annak minden egyes centiméterét. Ebben a biztonsági környezetben a NATO fokozni fogja a globális tudatosságát és hatókörét az elrettentés, a védelem és az elhárítás érdekében, összhangban a 360 fokú megközelítéssel. A NATO elrettentő és védelmi pozíciója a következők megfelelő kombinációján alapul: a nukleáris, a hagyományos és a rakétavédelmi képességek, kiegészítve az űr- és a nukleáris védelemmel és a kiberképességekkel. Ennek érdekében a szövetség felgyorsítja a digitális átalakulást, a NATO parancsnoki struktúráját az információs korszakhoz igazítják, és megerősítik a kibervédelmet, hálózatokat és infrastruktúrákat. A cél érdekében elősegítik az innovációt, és növelni fogják a beruházásokat az újonnan megjelenő és bomlasztó jellegű technológiák területén a katonai előny fenntartása érdekében. Visszatérő elemként itt is megjelenik, hogy a szövetség együtt fog dolgozni az új technológiák átvétele és integrálása érdekében, fokozni fogják az együttműködést a magánszektorral. A dokumentum szerint a világűr és a kibertér biztonságos használatának és az ahhoz való korlátlan hozzáférésnek a fenntartása kulcsfontosságú a hatékony elrettentés és védelem tekintetében. A NATO fokozni fogja a képességek fejlesztését a kibertérben azért, hogy megelőzzék, felderítsék, ellensúlyozzák és reagálni tudjanak a fenyegetések teljes spektrumára, minden rendelkezésre álló eszközt felhasználva. A rosszindulatú kiberfenyegetések egyszeri vagy folyamatos alkalmazása elérheti a fegyveres támadás szintjét, és arra késztetheti az Észak-atlanti Tanácsot, hogy alkalmazza a Szerződés 5. cikkét.[465] A stratégiai koncepció nem tartalmaz alapvető újdonságokat az elmúlt évekhez képest, de egyértelműen jelentősebb hangsúlyt kaptak a modern technológiák jelentette kihívások a szövetség életében, mint korábban. Emellett az is üdvözölendő, hogy a reziliencia már egyértelműen többrétegűvé vált, amiben kiemelt jelentőségű a társadalom és az egyén védelme.

464 Uo., 3–4.
465 Uo., 6-7.

2. Az Európai Unió szerepe a kibertér biztonsági aspektusaiban

Hazánk, az egyes tagállamok és közösség egészének biztonsága szempontjából kiemelkedő fontosságú az Európai Unió kibertér biztonságával kapcsolatos integratív, standardizáló és iránymutató tevékenysége, amelynek fontos részét képezik az e területen működő intézmények, kiadott jogi dokumentumok és azokon nyugvó legjobb gyakorlat meghatározása. Emellett az előző fejezetekben már érintett olyan problémák orvoslásában, mint amilyen a dezinformáció vagy a közösségimédia-platformok tevékenysége, az államok önállóan nem is tudnak megfelelő eredményeket elérni, a kívánt állapot eléréséhez szükségszerű a közösségi szervek tevékenysége, mert e transznacionális vállalatok számára a tagállamok többsége túl kicsi piac ahhoz, hogy alkalmazkodjanak a helyi sajátosságokhoz, tehát ezt csak és kizárólag közösségi szinten lehet elérni és megvalósítani az egyes szükséges, optimálisnak értékelhető működési mechanizmusokat. Jelen fejezetnek a célja, így abban áll, hogy legalább nagyvonalakban bemutassa az Európai Unió kiberbiztonsággal kapcsolatos törekvéseit.

2.1. A kiberbiztonsággal kapcsolatos törekvések kezdőlépései az Európai Unióban

Kezdetekben a kibertérrel kapcsolatos aggodalmak kizárólag a kibertérben realizálódó bűncselekményekkel kapcsolatban merültek fel, és főként azok kártékony gazdasági hatásai ösztönözték a tagállamokat a fellépésre.[466] Ezen szándék intézményi korporálódása volt a 2004-ben felállított Európai Hálózati és Információbiztonsági Ügynökség (ENISA). Az ENISA létesítésének a célja az volt, hogy „fokozza a Közösség, a tagállamok, és következésképpen az üzleti szféra képességét a hálózat- és információbiztonsággal kapcsolatos problémák megelőzésére, kezelésére és az azokra történő reagálására."[467] Feladatkörei azonban csupán tanácsadásra, tagállami tevékenységek összehangolására, adatgyűjtésre és jelentések elkészítésére[468] terjedt ki, tehát nem nevezhető sem a védelem, sem pedig a biztonság valós idejű koordináló vagy azt biztosító szervének.

A 2004. március 11-i madridi terrortámadás után az Európai Unió Tanácsa felszólította a Bizottságot, hogy dolgozzon ki átfogó stratégiát a kritikus infrastruktúrák területén.[469] 2005-ben ez öltött testet az Európai Unió Tanácsának kerethatározatában is, amely akként fogalmazott, hogy „egyre nagyobb aggodalmat okoz a tagállamok kritikus infrastruktúrájának részét képező információs rendszerek elleni terrortámadások lehetősége".[470] Eme kerethatározat ekkor még csupán a kibertérben megvalósuló sajátos bűncselekményeket és azok szankcióit kívánta meghatározni, valamint az egységes tagállami fellépését megalapozni. A kerethatározatot 2013-ban felváltották az információs rendszerek elleni támadásról szóló irányelvvel, amely lényegében a kiberbűncselekmények körét szélesítette ki, továbbá a társa-

466 Ilyen volt például a nem készpénzes fizetőeszközökkel összefüggő csalás és hamisítás elleni küzdelemről szóló Európai Unió Tanácsa által elfogadott kerethatározat 2001-ben (2001/413/IB).

467 Európai Parlament és Tanács 460/2004/EK Rendelete az Európai Hálózat– és Információbiztonsági Ügynökség létrehozásáról, 2. cikk

468 Európai Parlament és Tanács 460/2004/EK Rendelete az Európai Hálózat– és Információbiztonsági Ügynökség létrehozásáról, 3. cikk

469 Nyitrai (2017): 247.

470 Európai Unió Tanácsának 2005/222/IB kerethatározata (2005. február 24.) az információs rendszerek elleni támadásokról, Preambulum 2. bekezdés

dalomra való veszélyességük fokozódása révén azok szankcióit kívánta súlyosbítani.[471] Ezen irányelv egészen 2017-ig volt hatályban, éveken át az uniós kiberpolitika egyik sarokköve volt, így a később bemutatása kerülő kiberbiztonsági stratégia és hálózat- és információbiztonsági irányelv mellett ismertetésre kerül.

2006-ban a Bizottság által kiadott Biztonságos információs társadalomra irányuló stratégia: „párbeszéd, partnerség, felvértezés és felelősségvállalás" elnevezésű közlemény még mindig a kibertér gazdasági potenciálját és az abban okozott károkat hangsúlyozta, és a hálózati és információs biztonság (NIS – network and information security) gazdasági dimenziókon túlterjedő veszélyét a szektorba vetett bizalom elvesztésében látta, és ezáltal fejlődésének visszaesését, valamint az alapvető jogok online érvényesülésének akadályokba ütközését vizionálta.[472]

A 2007-es Észtországot és a 2008-as Grúziát ért kibertámadások világossá tették, hogy a kibertérben véghez vitt cselekmények kockázata az államok szemszögéből nem merül ki a gazdasági károkban vagy korlátozott hozzáférésű adatok illetéktelen kézbe kerülésében, hanem egy-egy nagyobb volumenű támadás akár az állam – és közösségeik – működését is veszélyezteti. Ennek ellenére az Európai Unió 2008-as kritikus infrastruktúrákat és azok kezelésével kapcsolatos feladatokat meghatározó irányelve preambulumában még csak megvizsgálandó kérdésnek tekintette azt, hogy szükséges-e egyáltalán az információs és kommunikációs technológiák ágazatát is bevonni a kritikus infrastruktúrák körébe.[473]

Fontos azonban rögzíteni – mivel ezen irányelv alapelvi szinten vonatkozik a később kritikus infrastruktúrának nyilvánított más rendszerekre is –, hogy ezen infrastruktúrák védelmének „elsődleges és végső felelőssége a tagállamokat és az infrastruktúrák tulajdonosait/üzemeltetőit terheli."[474]

A kritikus infrastruktúrákról szóló irányelv preambulumában felvetett vizsgálat eredményeit foglalta össze a Bizottság 2009-ben egy közlemény formájában. Ebben már rögzítette, hogy az információs és kommunikációs technológiák, vagyis

> „IKT-rendszerek, -szolgáltatások, -hálózatok és -infrastruktúrák (együttesen IKT-infrastruktúrák) egy része létfontosságú az európai gazdaság és társadalom számára (…) Az ilyen infrastruktúrák működésében bekövetkező zavar, illetve azok megsemmisülése súlyos hatással lenne az alapvető társadalmi funkciók működésére nézve, ezért létfontosságú informatikai infrastruktúrának számítanak".[475]

471 Európai Parlament és Tanács 2013/40/EU irányelv az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról.

472 A Bizottság közleménye a Tanácsnak, az Európai Parlamentnek, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának – A biztonságos információs társadalomra irányuló stratégia: „párbeszéd, partnerség, felvértezés és felelősségvállalás" SEC(2006) 656, 6.

473 Európai Unió Tanácsának 2008/114/EK Irányelve az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről, Preambulum 5. bekezdés

474 Európai Unió Tanácsának 2008/114/EK Irányelve az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről, Preambulum 6. bekezdés

475 A Bizottság Közleménye az Európai Parlamentnek, a Tanácsnak, az Európai gazdasági és Szociális bizottságnak és a Régiók Bizottságának a kritikus informatikai infrastruktúrák védelméről – „Európa védelme a nagyszabású számítógépes támadások és hálózati zavarok ellen: a felkészültség, a védelem és az ellenálló képesség fokozása" SEC(2009) 399, SEC(2009) 400. (továbbiakban: Európa védelme a nagyszabású számítógépes támadások és hálózati zavarok ellen: a felkészültség, a védelem és az ellenálló képesség fokozása) 2.

Maga a dokumentum terveket, célkitűzéseket fogalmazott meg, emellett még mindig a védelem leghangsúlyosabb okaként a kibertérben rejlő gazdasági potenciál kiaknázásának veszélyeztetését jelölte meg.[476] Ennek megóvása érdekében szándékként fogalmazták meg, hogy a nemzeti szemléletmódokat összehangolják, egy közös európai irányítási modell dolgoznak ki – amely nem más, mint a tagállami magánszféra és közszféra működő kapcsolatainak Uniós szintre fejlesztése az ENISA révén –, továbbá célként jelölték meg a nemzetközi és tagállami együttműködés erősítését, valamint a gyenge korai figyelmeztető és reagáló képesség fokozását.[477]

Létrehozták a köz-magán partnerséget (EP3R), valamint az Európai Információmegosztási és Figyelmeztető Rendszert (EISAS), amelynek feladata a lakosság és a kritikus infrastruktúrák figyelmeztetése. Utóbbi részeként funkcionál a korai észlelést és fellépést segítő, az információcsere hatékonyságának növelését a tagállamok között elősegítő CERT-ek (számítástechnikai katasztrófaelhárító csoportok),[478] amely közös Uniós alapképességek kialakítását kívánja elősegíteni, valamint az EGC, vagyis az Európai Kormányzati CERT-ek Csoportja hatáskörének kiterjesztését szolgálja.[479] 2011-ben felállították a CERT-EU-t, amelyet 2012-ben véglegesítettek. E szerv szoros kapcsolatot ápol a tagállami CERT-ekkel, az egyéb uniós kibertérrel foglalkozó szervekkel, valamint az ilyen típusú gazdasági vállalkozásokkal. A CERT-EU létrehozásának célja a legfontosabb Uniós intézmények (a Bizottság, a Titkárság, a Parlament, a Régiók Bizottsága, a Gazdasági és Szociális Bizottság) kibervédelmének uniós szintű megoldása.

2.2. A 2010 évek uniós kiberbiztonsági rendszere: kiberbiztonsági stratégia (2013, 2017), NIS (2016), kiberbiztonsági jogszabály és a kiberbiztonsági szakpolitika kerete (2014, 2018)

A 2010-es évek elején lépett túl az Európai Unió a politikai jellegű deklarációkon, amely nem választható el attól, hogy eddigre már a közösséget javarészét lefedő katonai biztonsági tömörülés, a NATO is lépéseket tett a kibertér biztonságának hatékonyabb szavatolása érdekében, emellett felismerte, hogy elengedhetetlen egy olyan területen a közbelépése, amely határokon átnyúló problémákat kíván megoldani, vagyis együttműködő, támogató, iránymutató, koordináló és a közös fellépést elősegítő fellépése nélkül a tagországok hosszútávon hatékonyan nem tudják megoldani a kiberbiztonságból eredő problémákat, kihívásokat.[480]

476 Uo., 4–5.

477 Európa védelme a nagyszabású számítógépes támadások és hálózati zavarok ellen: a felkészültség, a védelem és az ellenálló képesség fokozása, 5–7.

478 A CERT-ek vagy ma már szinonimaként használt CSIRT-ek (számítógépbiztonsági katasztrófaelhárító csoport) olyan állami vagy magán intézmények összefoglaló elnevezése, amelyeknek feladata állami vagy ágazati információs hálózatok védelmének biztosítása. Az elnevezés először Carnegie Mellon Egyetem CERT Coordination Center-re használta. Ma már globális és regionális szervei is vannak. Globális szerve a FIRST, amelynek tagja a magyar GovCERT (Kormányzati Eseménykezelő Központ), amely a Nemzetbiztonsági Szakszolgálat keretei között működik, valamint a magán szférából a HUN-CERT. Regionális szervként említendő az EGC, amely egyes Európai Uniós tagállamok kormányzati CERT-jeit tömöríti. A magyar kormányzati CERT tovább tagolt ágazati CERT-kre, ilyen például a Katonai Nemzetbiztonsági Szolgálat keretében működő katonai CERT.

479 Európa védelme a nagyszabású számítógépes támadások és hálózati zavarok ellen: a felkészültség, a védelem és az ellenálló képesség fokozása, 5–9.

480 Carrapico–Barrinha (2018): 299–303.

Ez az évtized a konkrét lépések megtétele mellett még mindig az útkeresés jegyében zajlott. Nem véletlen, hogy erre az évtizedre két kiberbiztonsági stratégia mellett, egy kiemelkedően fontos irányelv és rendelet kiadása (NIS – a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló kiberbiztonsági jogszabály) mellett a szakpolitikai keretrendszert is kétszer alakították át.

A NIS irányelvet kodifikációs folyamata 2013-ban indult meg, ezzel párhuzamosan a Bizottság, valamint a külügyi és biztonságpolitikai főképviselő közösen dolgozta ki az Európai Unió kibervédelmi stratégiáját. A stratégia már-már a kétezres évek elejére, a web 2.0 megjelenése idejére jellemző utópikus víziót[481] fest a kibertérről, amely szerint az „előmozdította a politikai és társadalmi integrációt; ledöntötte a határokat az országok, a közösségek és a polgárok között,"[482] és amelyben

> „az Unió nemzetközi kiberpolitikájának egyik legfontosabb eleme, hogy a virtuális teret a szabadság és az alapvető jogok érvényesülésének helyszínévé igyekszik formálni. Az internethez való hozzáférés folyamatos bővülésének világszerte elő kell segítenie a demokratikus reformot és annak ösztönzését."[483]

A stratégia alapelvként fogalmazta meg, hogy a kibertér eme küldetését azonban csak abban az esetben teljesítheti be, ha az Unió hagyományos térbeli normái itt is maradéktalanul érvényesülnek, vagyis az alapvető jogok, a szólásszabadság, a személyes adatok védelme, a mindenki számára biztosított hozzáférés, a demokratikus és hatékony irányítás, biztonság területén a közös felelősségvállalás megvalósul.[484] Megfogalmazott öt stratégiai prioritást is az alapelvek érvényesülése érdekében. Ezek a következőek voltak: kibertámadásokkal szembeni ellenálló képesség elérése; a számítástechnikai bűnözés drasztikus csökkentése; kibervédelmi politika és képességek kifejlesztése a közös biztonság- és védelempolitika (KBVP)[485] tekintetében; kiberbiztonsági ipari és technológiai erőforrások kifejlesztése; összefüggő nemzetközi szakpolitika létrehozása a kibertér vonatkozásában az Európai Unió számára, és az Unió alapértékeinek támogatása.[486] Az előző fejezetekben felvillantott károkból és a fennálló problémákból kiviláglik, hogy tényleges elmozdulást az elmúlt közel egy évtizedben nem sikerült elérni ezen területek javarészén.

A kiberbiztonsági stratégia nagyvonalakban rögzíti a támadások lehetséges indítópontjait, így a bűncselekményeket elkövető személyeket vagy azok csoportjait, a terrorista csoportokat, a politikai jellegű, valamint az államilag támogatott kibercselekményeket. Előbbi kettővel szembeni határozottabb és eredményesebb fellépés érdekében maga az Unió is alkotott jogi normákat, addig utóbbiak esetében rögzíti, hogy „az Unió nem várja el a nemzetközi jogi eszközök létrehozását a kibertérrel kapcsolatos kérdésekben".[487] Ennek a hibás álláspontnak a következményeit az évtized végén, kiemelten pedig az orosz–ukrán szembenállás világította meg, főként a 2022 februárjában kirobbant háború és annak eszközparkja.

481 Gosztonyi (2022c): 168–173.

482 Közös közlemény az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér /JOIN/2013/01 final/, 2.

483 Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér (2013), 17.

484 Uo., 4.

485 Knapp (2020): 106., Knapp (2019)

486 Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér (2013), 5.

487 Uo., 18.

A stratégia hiányosságaként értékelhető, hogy nem kívánja legalább jellemzőiben megfogni a kibertér sajátosságait, a hagyományos tértől eltérő jellegét, így nem is adhatja meg az egyes alapjogok, vagy ahogy a közleményben többször is megjelenik, az uniós alapértékek kibertérre vonatkoztatható térképét, ebből adódóan nem jelenik meg azok kizárólag a kibertérben érzékelhető sajátosságainak rögzítése, azok jogszerű korlátozhatóságának mikéntje, határai, sem pedig az azokkal kapcsolatos uniós intézmények hatásköreinek rögzítése. Az Unió ezen túlmenően a kibertér országhatárokon átnyúló jellege, valamint az államok különböző szabályozási keretei miatt nem látta kivitelezhetőnek egy központi európai felügyelet kialakítását, így a felelősség – ahogy az a korábbi dokumentumokban is megjelent – az egyes tagállamokat és a magánszektort terheli. [488] Az Európai Uniónak eme hozzáállása rendkívül visszás, mivel pontosan a szabályozás összehangolása lenne – és lett volna ebben az időszakban is – a legalapvetőbb feladata ezen a területen, amelyhez elengedhetetlenül szükséges egy, az ENISA-nál jóval szélesebb hatásköri felhatalmazással rendelkező központi uniós intézmény, amely képes összehangolni az egyes tagállami hatóságok tevékenységét, képes egységes védelmi protokoll kialakítására és működtetésére. Ilyen jellegű intézményre azért is van égető szükség, mivel a stratégiában megfogalmazott célokra irányuló együttműködési formák – vagyis az információcsere vagy tanácsadás – kizárólagos alkalmazása már idejétmúlttá vált a kibertér gyors fejlődése, valamint az ott megjelenő harmadik államok vagy terrorcsoportok által bírt potenciál okán. Ezt a hibás korai álláspontot kívánja az Unió átlépni például a közösségimédia-platformok térnyerése, üzletpolitikája, valamint annak biztonsági és társadalmi hatásainak egyre világosabbá válása miatt,[489] valamint az orosz és kínai hibrid szcenáriók elszaporodása következtében az évtized végétől. Egyértelmű előrelépés volt viszont a kibertér biztonságának szavatolása, fontosságának felismerése a hagyományos tér szempontjából.

A stratégia nagyon fontosnak tartotta a végfelhasználói tudatosság javítását, mivel fontos szerepet játszanak a hálózati és információs rendszerek biztonságában. Erre pedig programokat kívánt létrehozni, ezek közül kiemelték a 2012 októberétől megszervezett európai kiberbiztonsági hónapot, valamint a gyermekek internetes védelmére összpontosító Biztonságos Internet programot.[490] Sajnos egyik sem éri el megfelelően azokat a társadalmi csoportokat, akiknek a tudatosságának javítására kiemelt szükség volna a társadalmi reziliencia javítása érdekében, így az idősebb, de kibertérben aktív korosztályt, a gyermekeket[491] és az őket nevelő pedagógusokat,[492] valamint az informatika területén kevésbé jártas és képzett egyéneket.

2014-ben készült el az Európai Unió kibervédelmi szakpolitikai kerete című dokumentum. A feladat dedikált szerve az Európai Külügyi Szolgálat. A dokumentum rögzíti, hogy a kiberbiztonság a közös biztonság- és védelempolitika (KBVP) egyik alapvetően fontos szegmense, amely – ismételve a NATO korabeli megállapításait – legalább olyan fontos, mint a szárazföldön, a tengeren, a légtérben és a világűrben megjelenő biztonsági kockázatok. Ezért e dokumentum rendeltetése, hogy meghatározza a KBVP keretébe tartozó kibervédelem területeit, pontosítsa az európai szereplők feladatait úgy, hogy közben tiszteletben tartja a tagál-

488 Uo., 19.

489 Bányász (2016): 61–81., Bányász (2015): 11–12., Bányász (2017b): 59–77., Gosztonyi–Huszár (2022): 141–152., Kovács-Szépvölgyi (2022a): 227–236.

490 Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér (2013), 8–9.

491 Krasznay–Varga-Perke (2013): 179–202.

492 Krasznay–Som (2016): 235–240., Krasznay (2013): 105–109.

lami és más uniós szervek feladatait és hatásköreit. Az uniós kibervédelmi szakpolitikai keret öt prioritását állapították meg: a (1) KBVP vonatkozású tagállami kibervédelmi képességek fejlesztésének támogatását; az (2) uniós szervek által a KBVP keretében használt kommunikációs hálózatok védelmének növelését; a (3) polgári-katonai együttműködésnek, illetve a tágabb uniós kiberpolitikákkal, az érintett uniós intézményekkel és ügynökségekkel, valamint a magánszférával fennálló szinergiáknak az előmozdítását; a (4) képzési, oktatási és gyakorlati lehetőségek javítását; a (5) nemzetközi partnerekkel folytatott együttműködés elmélyítését. Ezek keretében többek között a tagállamoknak lehetőségük van segítséget kérni az ENISA-tól a kibervédelmi képességeik fejlesztéséhez, a tagállami katonai CERT-ek közötti együttműködések önkéntes javítására; kidolgozni a KBVP keretében folyó katonai műveletek egységesített kibervédelmi koncepcióját; a meglévő uniós szintű tapasztalatok hasznosításának megszilárdítását; közös kiberbiztonsági és védelmi kompetenciaprofilok kidolgozását a legjobb nemzetközi gyakorlatok és uniós minősítés alapulvételével; a kiberbűnözés megelőzésére és feltérképezésére irányuló, valamint forenzikus képességek formálását; képzési programok létrehozását, akkreditálását, a kiberspecifikus katonai Erasmus kialakítását.[493] Sajnos a képzésre, oktatásra irányuló paletta a 2013-as stratégia ellenére nem össztársadalmi, hanem főként az érintett szektorok állományának képességbeli javítására irányult, de fontos előrelépés a tekintetben, hogy egyre inkább összehangolt fellépést mutatott az Unió a kiberbiztonság tekintetében, azonban ez javarészt még ekkor is csak az alapok lehelyezését jelentette.

Az orosz–ukrán konfliktus kiéleződése 2014–15-ben, és annak kibertéri következményei lépésre kényszerítették az Uniót is.[494] Az Európai Unió Tanácsa 2015-ben kiadta a Cyber Diplomacy-ra vonatkozó következtetését, melyben kimondta, hogy a kiberbiztonság, az emberi jogok, a nemzetközi jogi és jogállamisági normák biztosítása a kibertérben folyamatos kihívást jelent a közös kül- és biztonságpolitika számára, amelyeket, úgy vélték, csak egy átfogó, sokrétű, koherens nemzetközi kibertér politikával lehet kezelni. Mindeközben viszont fontos, hogy továbbra is szem előtt tartsák az egységes, nyitott, szabad és biztonságos kibertér előmozdítását és védelmét, amely csak úgy valósítható meg, hogy közben teljes mértékben tiszteletben tartják a demokrácia, az emberi jogok és a jogállamiság uniós alapértékeit. Ehhez viszont a dokumentum szerint ki kell dolgozni egy kiberdiplomáciára vonatkozó egységes és átfogó uniós megközelítést, amelyre még további két évet kellett várni.[495] A kitűzött célok, így az alapvető (uniós, jogállamisági) értékek megőrzése, a szabadságjogok tiszteletben tartása, a nemek közötti egyenlőség, a versenyképesség és a jólét megőrzése szignifikáns különbségek mutattak az ekkor is már egyre jobban kirajzolódó geopolitikai törésvonal nyugati és keleti államai között a kiberbiztonság rendeltetése terén is.[496]

Nagy jelentőségű volt az uniós kiberbiztonság előmozdításának területén a 2016-os hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló irányelv (továbbiakban: NIS). Ez az első kiberbiztonsággal kapcsolatos uniós jogforrás, így önmagában is kiemelkedő jelentőségű. Az irányelv keretében az Unió kiberbiztonsággal kapcsolatos jogalkotási, politikai folyamatainak fejlődése tetten

493 Uniós kibervédelmi szakpolitikai keret, Brussels, 18. November 2014, 15585/14.

494 Farkas Ádám (2020a): 11–23., Padányi–Tomolyka (2017): 29–42.

495 Brussels, 11 February 2015 (OR. en) 6122/15 Európai Unió Tanácsa Council Conclusions on Cyber Diplomacy.

496 Krasznay (2019): 25–29., Gosztonyi (2022b): 27–36., Baer–Koponen (2022), Krasznay (2022): 37–56.

érhető, hiszen annak gazdasági veszélyeit megfelelően tudták már azonosítani. Megfogalmazása szerint, ugyanis „a hálózati és információs rendszerek és szolgáltatások létfontosságú szerepet játszanak társadalmunkban. Megbízhatóságuk és biztonságuk alapvetően lényeges a gazdasági és társadalmi tevékenységek, és különösen a belső piac működése szempontjából".[497] Rendkívül pontosan felmérve, az irányelv megállapította azt is, hogy a kiadásakor a meglévő kapacitások nem voltak elegendőek ahhoz, hogy a rendszerek biztonságát és megfelelő működését garantálják, és ezért uniós szinten szükséges, a korábbitól eltérő, globális megközelítés a képességek, kapacitások, minimumkövetelmények létrehozása terén. Cél lényegében tehát az volt, hogy meghatározzon egy közös struktúrát és eszköztárat a tagállamok számára, valamint megrajzolja az uniós szintű együttműködés alapjait. Így az irányelvnek természetszerűleg vannak tagállamokra vonatkozó rendelkezései és vannak közösségi szintre tartozó szabályhelyei is.

A tagállamokkal szembeni elvárás volt, hogy 2018. november 9-ig azonosítaniuk kellett a területükön letelepedett, alapvető szolgáltatásokat nyújtó szereplőket, vagyis amelyek a kritikus társadalmi és/vagy gazdasági tevékenységek fenntartásához alapvető szolgáltatást nyújtanak; az adott szolgáltatás nyújtása hálózati és információs rendszerektől függ; és az említett szolgáltatást érintő biztonsági esemény jelentős zavart okozna a szolgáltatás nyújtásában.[498] Az érintett ágazatok az energia, a közlekedés, a banki szolgáltatások, a pénzügyi piaci infrastruktúrák, az egészségügy, az ivóvízellátás és -elosztás, valamint a digitális infrastruktúra.[499] Ez pedig azért kiemelten fontos, mert lényegében ezen szereplőkre állapított meg az irányelv különleges kötelezettségeket.

Az irányelv a tagállamok számára előírta, hogy saját hálózati és információs rendszerek biztonságára vonatkozó nemzeti stratégiákat kell létrehozniuk, amelyek többek között megfogalmazzák a nemzeti stratégia prioritásait, céljait, azok megvalósításához szükséges irányítási keretrendszert, érintve a kormányzati szerveket és egyéb szereplőket, azonosítják a felkészülésre, reagálásra vonatkozó szükséges intézkedéseket, beleértve a köz- és magánszektor együttműködését, továbbá érintik az ehhez kapcsolódó oktatási, tájékoztatási és képzési programokat, kutatási és fejlesztési terveket.[500] Kifejezett előírás volt a tagállami hálózati és információs rendszerek biztonságáért felelős hatóság(ok) kijelölése, amelyeknek a fentebbi szereplők, valamint digitális szolgáltatók (online piactér, online keresőprogram, felhőalapú számítástechnikai szolgáltatás) tekintetében az irányelv megvalósulásának a monitorozása. Emellett ki kellett jelölniük a tagállamoknak egyedüli kapcsolattartó pontot is, amelynek feladata a tagállamok és a CERT szervek közötti együttműködés biztosítása.[501]

Az irányelv előírta nemzeti CERT-ek felállítását, amelyek feladata a fenti szereplőkkel kapcsolatos kiberbiztonság szavatolása. A tagállami CERT-ek között a bizalom erősítése, a legjobb gyakorlatok megismerése és megosztása érdekében CERT-ek hálózata jött létre. A CERT-ek hálózata a tagállami CERT-ek és a CERT-EU képviselőiből áll. A háttér adminisztrációt az ENISA biztosítja a megfelelő működéshez.

497 Az Európai Parlament és a Tanács (EU) 2016/1148 Irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről. (továbbiakban: 2016/1148 Irányelv) Preambulum (1).

498 2016/1148 Irányelv Preambulum (2).

499 Uo., II. melléklet

500 Uo., 7. cikk

501 Uo., 8. cikk

A CERT-ek I. számú melléklete tartalmazza a CERT-ek feladatait: (1) alapvető funkciók: (a) a biztonsági események nemzeti szintű monitoringja; (b) a kockázatokkal és biztonsági eseményekkel kapcsolatos korai előrejelzés, riasztás, bejelentéstétel és információterjesztés a releváns érdekeltek számára; (c) reagálás a biztonsági eseményekre; (d) dinamikus kockázat- és eseményelemzés, valamint helyzetkép nyújtása; (e) a CSIRT-ek hálózatában való részvétel. (2) A CERT-eknek együttműködési kapcsolatokat kell kialakítania a magánszférával. (3) Az együttműködés megkönnyítése érdekében a CERT-eknek közös vagy szabványosított gyakorlatok elfogadását és alkalmazását kell szorgalmaznia az alábbiakra vonatkozóan: (a) a biztonsági események és a kockázatok kezelésére vonatkozó eljárások; (b) a biztonsági események, kockázatok és információk osztályozására szolgáló rendszerek.[502]

A felsorolt feladatok szerint a CERT-ek hatáskörei részben lefedik az ENISA hatásköreit (például ismeretterjesztés, társadalomtudatosság fejlesztése, együttműködések kialakítása), azonban emellett tényleges kibervédelmet is ellátnak, továbbá eljárások, esemény osztályozások révén próbálják megvalósítani az egységes fellépést az Unióban.

A fentebb ismertetett szereplők esetében az irányelv elvárja, hogy „megfelelő és arányos műszaki és szervezési intézkedéseket tesznek a működésük során általuk használt hálózati és információs rendszerek biztonságát fenyegető kockázatok kezelése érdekében".[503] Ezt pedig a tagállami hatóságoknak kötelezettségük ellenőrizni, illetve a szereplők kötelezettsége, hogy tájékoztassák a hatóságokat arról, ha működést veszélyeztető támadás éri őket. Erről a nemzeti kapcsolattartó pontnak a többi tagállami kapcsolattartót is értesítenie kell.[504] Az irányelv révén az Unió óriási lépést tett a hálózatbiztonság egységes kezelése felé, lehatárolta a tagállami és uniós feladatokat, egységesítési törekvései voltak a tagállami kiberbiztonsági stratégiák tartalma tekintetében, azonban két és féléves elfogadási folyamata miatt már elfogadásakor sem tudott lépést tartani a digitalizáció jelentős ütemével és az abból fakadó kiberfenyegetettségek jelentős erősödésével.

A Bizottság 2016-os, a kibertérrel kapcsolatos közleményében rögzítette, hogy a pozitív fejlemények ellenére az EU továbbra is sérülékeny a kiberbiztonsági incidensekkel szemben. A Bizottság kiemelte, hogy különösen veszélyesek azok a kibertérből indított műveletek, amelyek a hibrid támadások eszközének tekintendők, vagyis amelyeket a hibrid fenyegetések elkövetői alkalmazhatnak,[505] mivel ezen támadások „akár országok vagy politikai intézmények destabilizációjához is vezethetnek".[506] A közlemény azonban ezen túlmenően jelentősebb újdonságot nem tartalmaz, továbbra is a politikai deklarációk szintjén mozogva kívánta előmozdítani a kiberbiztonság kérdését az Európai Unióban.

Nem véletlen, hogy a fentiek után a közösség úgy érezte, hogy szükséges a 2013-as stratégia kiigazítása, aktualizálása, amely 2017-ben meg is történt. A stratégia bevezetője rögzíti, hogy a kiberbiztonság alapvető és kiemelt a mindennapjaink biztonságának fenntartása körében, azonban a fenyegetések az évek során exponenciálisan növekedtek. A támadások

502 Uo., I. melléklet

503 Uo., 14. cikk (1) bekezdés

504 Uo., IV. fejezet melléklet

505 Közös Közlemény az Európai Parlamentnek és a Tanácsnak A hibrid fenyegetésekkel szembeni fellépés közös kerete JOIN/2016/018 final, 4.4. pont.

506 Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának Európa kibertámadásokkal szembeni ellenálló képességének erősítése, valamint a versenyképes és innovatív kiberbiztonsági ágazat támogatása, COM(2016) 410 final, 2.

pedig – a hibriditásnak is köszönhetően – egyaránt köthetőek állami és nem állami szereplőkhöz, elmosódott a határ a hagyományos és a kibertéri szereplők között. Hangsúlyozza, hogy egyes államok geopolitikai érdekeiket kibertéri műveletekkel kényszerítik ki, és amennyiben nem sikerül az EU-nak jelentősen javítani a kiberbiztonságán, akkor a kockázat a digitalizáció kiterjedtségével egyre nagyobb lesz. A stratégia megállapítása szerint az Unió kibertámadásokkal szembeni rezilienciája a következő megvalósítása esetén reális cél: az ENISA megerősítése; az egységes kiberbiztonsági piac felé való elmozdulás; a NIS teljeskörű végrehajtása; az ellenállóképesség kulcsa a gyors vészhelyzeti reagálás; a Kiberbiztonsági kompetenciahálózat és az Európai Kiberbiztonsági Kutatási és Kompetenciaközpont, vagyis a kutatás és fejlesztés erősítése; a kiberkészségbázis kiépítése, tehát az oktatás erősítése; a kiberhigiénia és -tudatosság elősegítése. Ezekhez többek között kell egy egységes uniós kiberbiztonsági tanúsítási keretrendszer kialakítása, amelyet az IKT szabványok meghatározása és kötelezővé tétele révén lehet megvalósítani. Kiemelt fontosságú célként jelenik meg a kiberbiztonsági kutatások fokozása, amelyek segíthetnek megérteni és felkészülni az új típusú kihívásokra. Oktatás területén felmérték, hogy már nemcsak a katonai kapacitás a fontos, hanem a civil is, főként, mivel felmérésük szerint óriási szakemberhiány várható a területen. Emellett sikerült azonosítani, hogy az incidensek sikerét az emberi faktor teszi lehetővé, mégpedig az esetek 95%-ban. Így szükségesek tájékoztató kampányok ezen a területen. Sajnos ez még mindig nem érte el a társadalom jelentős részét, ahogy az oktatás esetében is szükséges volna a kiberbiztonság generális, minden oktatási szinten és minden felsőoktatási szakon megjeleníteni, hiszen a tudatosság csak és kizárólag így érhető el. Ezeken túlmenően rögzíti a dokumentum, hogy szükséges hathatós uniós kibertámadás-elhárítás létrehozása, ami már önmagában megkésett volt ekkor is. Ennek részeként határozták meg a rossz szándékú szereplők azonosítását, a bűnüldözési reagálás fokozását, az állami és a magánszféra közötti együttműködés növelését, a politikai válaszlépések erősítését, a tagállami védelmi kapacitások javítását, emelését.[507]

2017-ben, két évvel az egységes uniós Cyber Diplomacy kinyilvánítása utána, az Európai Unió Tanácsa életre hívta a Cyber Diplomacy Toolbox-ot, vagyis az EU kiberdiplomáciai eszköztárát, a rosszindulatú kibertevékenységekre adott közös válaszlehetőségeket. Eme eszköztár hivatott a konfliktusmegelőzésre, a kiberbiztonsági fenyegetések mérséklésére és a nemzetközi kapcsolatok stabilizálására. Az uniós diplomáciai válasz az egyes kibertevékenységek terjedelmével, mértékével, időtartamával, intenzitásával, összetettségével, kifinomultságával és hatásával arányos választ tesz lehetővé. Az eszköztárat tartalommal 2019-ben töltötte fel a Tanács rendeletével és határozatával. Mindkettő szabályait akkor kell alkalmazni, ha külső, jelentős hatású kibertámadás vagy annak kísérlete éri az Uniót vagy annak tagállamát. Támadásnak tekintik azokat a jogellenes tevékenységet, ami információs rendszerhez hozzáfér, abba beavatkozik, vagy megfigyel. Veszélyesnek minősítik többek között a kritikus infrastruktúrát, az alapvető társadalmi, gazdasági tevékenységet biztosító rendszert, a kritikus állami funkciót biztosító rendszert, a kormányzati veszélyelhárító csoportot ért támadásokat. A jelentős hatás megállapításához vizsgálják az előidézett zavar hatókörét, léptékét, a támadott természetes vagy jogi személyek, szervezetek, tagállamok számát, az okozott gazdasági veszteséget, az érintett adatvagyon mennyiségét, léptékét. Az Unió számára lehetővé

507 Közös közlemény az Európai Parlamentnek és a Tanácsnak Ellenálló képesség, elrettentés, védelem: az Unió erőteljes kiberbiztonságának kiépítése, Brüsszel, 2017.9.13., Join(2017) 450 final.

teszi, hogy megakadályozzák, hogy az ilyen támadást megvalósító az Unió területére lépjen, azon átutazzon, valamint hogy a tulajdonában lévő pénzeszközt és gazdasági erőforrást befagyasszák.[508] E rendelkezések határozott kifejezése az Unió szándékának a külső támadók szankcionálása érdekében, amely a 2010-es évek második felében elszaporodott támadásokra kíván reagálni, mégpedig úgy, hogy a kiberdiplomáciai eszköztár a közös kül- és biztonságpolitikán keresztüli szankciós modellt alkalmazó jogrendet hozott létre. A kiberdiplomáciai eszköztárat eddig két alkalommal alkalmazták. 2020 júliusában az Európai Unió Tanácsa szankciókat vetett ki a kibertámadásokban, például a „Wannacry" és „NotPetya" támadásokban részt vevő orosz, kínai és észak-koreai hackerekkel szemben, míg 2020 októberében azon orosz hackerek ellen, akik részt vettek a német parlamentet 2015-ben ért kibertámadásokban, amelynek során nyolc személyt és négy szervezetet súlytottak szankcióval.[509]

A stratégia megújítását és a kiberdiplomácia eszközpark kialakítását követte az Uniós kibervédelmi szakpolitikai keret naprakésszé tétele is. Ebben is kiemelték, hogy az intézményi és tagállami kiberrezilienciát meg kell erősíteni, ahogy a biztonsági és védelmi képességeket is. Már tényként rögzíti – a NATO doktrínája után –, hogy a kibertér az ötödik műveleti tér, ami kiemelt, mivel az uniós missziók sikere nagyban függ a kibertér használatának biztonságától és zavartalanságától. Így a dokumentum megújításának a célja az elmúlt évek tapasztalataihoz és realitásaihoz való igazítás. A szakpolitikai keretdokumentum több helyen is kiemeli az együttműködést a NATO-val, valamint azt is, hogy az együttműködés gördülékenysége és saját kiberbiztonságának hatékonysága érdekében ezt az együttműködést tovább kell erősíteni, fokozni és új területekre is kiterjeszteni. A fentiek érdekében pedig hat prioritást fogalmaztak meg: a tagállami kibervédelmi képességek fejlesztésének támogatása; az uniós szervek által a KBVP keretében használt kommunikációs és információs rendszerek védelmének növelése; a polgári-katonai együttműködés előmozdítása; kutatás és technológia; a képzési, oktatási és gyakorlati lehetőségek javítása; a releváns nemzetközi partnerekkel folytatott együttműködés elmélyítése. Ez utóbbi a NATO, az EBESZ és az ENSZ közötti együttműködést takarja. Az oktatást és a képzést pedig el kell mozdítani abba az irányba, hogy egy közös uniós kibervédelmi kultúra kialakulhasson.[510] Ez egy óriási elmozdulás abból a korábbi nézőpontból, hogy a kiberbiztonság csak gazdasági jelentőségű, így ez a gondolata a dokumentumnak jól érzékelteti, hogy a kiberbiztonság és a kibertér megfelelő használata már össztársadalmi problémává vált. Ezen dokumentumok révén jelentős elmozdulás történt az Unió kibertér és kiberbiztonság felfogásában, amelyet az elmúlt évek társadalmi abúzusai, valamint a hibriditás térnyerése, továbbá a politikai és gazdasági realitások is eredményeztek.

Érdemes még megemlíteni a 2019-ben elfogadott rendeletet, amely az ENISA és IKT technológiákra vonatkozó szabályt alkotta meg. Ehelyütt az ENISA-ra vonatkozó szabályt tekintem át röviden. Az ENISA az Unió szerve és jogi személyiséggel rendelkezik. Feladata, hogy a rendelet által rábízott feladatok elvégzése révén egy egységes, magas szintű kiberbiztonság jöjjön létre az egész Unióban. Ennek során főként támogatást nyújt a tagállamoknak vagy az uniós szerveknek a kiberbiztonság javításához, valamint a tagállami jogi környezetek egy-

508 A Tanács (EU) 2019/796 Rendelete (2019. május 17.) az Uniót vagy annak tagállamait fenyegető kibertámadások elleni korlátozó intézkedésekről; A Tanács (KKBP) 2019/797 Határozat (2019. május 17.) az Uniót vagy annak tagállamait fenyegető kibertámadások elleni korlátozó intézkedésekről.

509 Khausar–Ras (2023): 29–58.

510 Uniós kibervédelmi szakpolitikai keret (2018. évi naprakésszé tett változata), Brussels, 19. November 2018, 14413/18.

máshoz közelítésén munkálkodik. Célként határozza még meg a rendelet, hogy az ENISA egyfajta független szakértői központként működve, járuljon hozzá a kiberbiztonsági képességek fokozásához, támogassa az Unión belüli kapacitásépítést és felkészülést, mozdítsa elő az Unión belüli együttműködést a kiberbiztonság területén, segítse a vállalkozások és a polgárok kiberbiztonsági tudatosságának fejlődését. Feladata az uniós szakpolitika és jogszabályok kidolgozása és végrehajtása, a kapacitásépítés, az uniós szintű operatív együttműködés támogatása, valamint elő kell mozdítania a kiberbiztonsági tanúsításra, valamint szabványosításra vonatkozó uniós szakpolitikát és annak végrehajtását. Kiemelt feladata még az ismeretterjesztés és tájékoztatás, valamit ehhez kötődően a tudatosítás és az oktatás, a kutatás és az innováció is.[511]

2.3. Az Európai Unió fellépése a dezinformációs tevékenységgel szemben

Szükséges röviden kitérni a dezinformációval kapcsolatos dokumentumokra, hiszen ezek élesen kirajzolják a fenti hangsúlyeltolódás okait, valamint a következő fejezetben tárgyalt új joganyagok megalkotásának hátterét is világosabbá teszik.

Oroszország Ukrajna elleni tevékenységének hatására az Európai Unió is felismerte a hibriditás, ezen belül a dezinformáció jelentőségét, ezért 2015-ben felállították az East StratCom Task Force elnevezésű munkacsoportot, amelynek célja, hogy javítsa az Unió képességeit a külső szereplők által előállított dezinformáció előrejelzése, felderítése és a reagálás területén.

2018-ban cselekvési tervet fogadtak el a félretájékoztatással szemben, amely osztott tagállami és Uniós intézményi fellépésről rendelkezett. A koordinált válasz négy pilléren nyugszik: (1) az uniós intézmények képességeinek javítása a félretájékoztatás eseteinek észlelése, elemzése és leleplezése területén; (2) a félretájékoztatással kapcsolatos koordinált és együttes válaszlépések megerősítése; (3) a magánszektor mozgósítása a félretájékoztatás elleni küzdelem érdekében; (4) tudatosságnövelés és a társadalom rezilienciájának javítása. A tervezet azt az elvárást állította fel, hogy meg kell erősíteni azokat az Uniós szerveket, amelyek a területen feladattal bírhatnak, emellett létre kell hozni egy riasztási rendszert, amely valós időben képes jelezni a dezinformációs tevékenységet, és a tagállamoknak ki kell jelölnie kapcsolattartó pontot. A magánszektor mozgósítása alatt a dokumentum a platformok szerepének hangsúlyozását és felelősségük kiemelését értette, mivel ezek nem kezelték megfelelően az érintett problémakört. A társadalmi ellenállóképesség növelése érdekében előirányozták a független tényellenőrzőkből álló csoportok létrehozását, akiknek feladata a dezinformálás feltárása és a közvélemény tájékoztatása.[512]

Ennek érdekében elfogadtak egy önszabályozó gyakorlati kódexet, amelynek aláírói többek között vállalták, hogy elősegítik a megbízható tartalmak láthatóságát, mégpedig a félrevezető tartalmak csökkentése révén, valamint fokozzák a hamis fiókokkal szembeni fellépést,

511 Az Európai Parlament és a Tanács (EU) 2019/881 rendelete (2019. április 17.) az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről (kiberbiztonsági jogszabály). III. fejezet. 13–45. cikk

512 Az Európai Bizottság és az Unió Külügyi és Biztonságpolitikai Főképviselőjének közös közleménye – Cselekvési terv a félretájékoztatással szemben, Brüsszel, 2018.12.15., Join(2018)36. Final.

továbbá növelik a hirdetések és szponzorált tartalmak átláthatóságát.[513] Magyarországon 2021 tavaszán indult el a tényellenőrzők programja, a Facebook erre a feladatra az APF hírügynökséget vonta be. Az ilyen csoportok hatékonysága mindamellett megkérdőjelezhető. Abból kiindulva, hogy a hibrid konfliktusok rendkívül összetett, nemcsak a dezinformálásból álló cselekményeket ölelik fel, hanem számos soft, medium és hard eszköz és módszer is a tárházában van, így példának okáért a gazdasági és pénzügyi műveletek, a kiberműveletek, valamint a bűnszervezetek, terrorista csoportok tevékenységének ösztönzése, finanszírozása, támogatása. Ezeket a komplex – mondhatni totális – kihívásokat a fegyveres védelem ágazatai (honvédelem, rendészet, nemzetbiztonsági tevékenység) külön-külön sem tudják megfelelően kezelni. Szükségszerű az ilyen totális biztonsági kihívásokra az ágazatok összehangolt, koordinált, információmegosztáson alapuló fellépése. Ez értelemszerűen becsatornázza a nemzetbiztonsági ágensek által megszerzett adatokat, amelyek mentén átfogóbb döntést tud hozni a megtámadott állam. Míg a civil, polgári tényellenőrök ezen információk hiányában hozzák meg döntéseiket, javaslataikat, egy magánvállalat számára. Nem beszélve arról, hogy ezen magánvállalat az esetek többségében nem ismeri az adott társadalmi valóságot és/vagy politikailag, ideológiailag elfogult. Az is kérdéses, hogy a magánszektor által kiválasztott, felkért tényellenőrök mennyiben függetlenek, vagy tudják magukat függetleníteni a magánvállalati célok, attitűd alól.

A cselekvési tervnek megfelelően 2019-ben létrehozták a Rapid Alert System-et. Célja megkönnyíteni az információcserét és összehangolni a tagállami és uniós intézmények fellépését a dezinformációval szemben. Ennek érdekében 27 tagállami kapcsolattartó pontból álló hálózatot hoztak létre, amelyek feladata a koordinálás és a legjobb gyakorlatok megosztása. A megosztott hatáskörök miatt nehézkes a problémamegoldás, továbbra is fennmaradt a tagállami eszközpark.[514] A Covid19[515] által okozott pandémiás helyzet ismét előtérbe helyezte a kérdéskört, mivel generált egy ún. infodémiát.[516] Az infodémia kapcsán az Unió számára is világossá vált, hogy különbséget kell tenni hamis vagy félrevezető tartalmak különböző formái között, így a jogellenes és a káros, de nem jogellenes tartalmak között. Utóbbiak esetében a dezinformálás akkor áll fent, ha megtévesztés, közérdeknek való károkozás vagy gazdasági károkozás szándékával tették közzé. Az ebből adódó dezinformációs tevékenység leküzdésének alapjául a korábbi cselekvési terv, a gyakorlati kódex és a gyors reagálású csoport gyakorlata szolgál. Ez nem több azonban, mint célirányos cáfolatok, mítoszrombolás és médiatudatossági kezdeményezések.[517] A fellépés tényleges eszközparkja tehát továbbra is a platformszolgáltatónál maradt. Annak ellenére, hogy a tartalmak fentebbi osztályozása, vagyis annak eldöntése, hogy a káros tartalom dezinformálás céljából került e megosztásra, kizárólag tagállami hatáskörben valósulhat meg.

513 Klein (2018): 246.

514 Makela (2019): 15.

515 Covid19 által okozott helyezett sajtóra gyakorolt hatását l. Cendic–Gosztonyi (2020): 14–29.

516 A fogalmat a WHO vezette be és a következőképpen határozta meg: „az infodémia egy problémával kapcsolatos túlzott információáradat, amely megnehezíti a megoldás azonosítását. Magában foglalja az egészségügyi szükséghelyzet során terjedő félretájékoztatást, dezinformációt és pletykákat. Az infodémia hátráltathatja a hatékony népegészségügyi válaszintézkedéseket, továbbá zavart és bizonytalanságot kelthet az emberek körében." who.int/docs/default–source/coronaviruse/situation–reports/20200305–sitrep–45–covid–19.pdf?sfvrsn=ed2ba78b_4.

517 Az Európai Bizottságnak és az Unió Külügyi és biztonságpolitikai főképviselőjének közös közleménye A Covid19–cel kapcsolatos dezinformáció kezelése – lássuk a valós tényeket, Brüsszel, 2020.6.10. Join(2020)8. Final.

2020 decemberében az Európai Bizottság előterjesztette az Európai Demokráciára vonatkozó cselekvési tervet. Ennek negyedik pontja szól a dezinformáció elleni küzdelemről. Szorosabb együttműködés kialakítása mellett érvel a magánszektorral, a civil társadalommal, a tudományos élettel és az Unió nemzetközi partnereivel, azonban még mindig csak a hibrid konfliktus jobb megértése érdekében. Vagyis továbbra is csak ígéretként fogalmazták meg az eljárásrend hatálybaléptetését, a közös módszertani keret kidolgozását. A platformok esetében az általuk használt algoritmusok átláthatatlanságát, a hírekkel kapcsolatos – fentebb ismertetett – gyakorlatát kritizálta, amely problémákat a dokumentum szerint furcsa mód csak a gyakorlati kódex értékelése során azonosítottak. A Bizottság véleménye szerint a dezinformálás elleni hatékony fellépés záloga a platformszolgáltatók erőteljesebb és világosabb kötelezettségvállalása, valamint a megfelelő felügyeleti mechanizmuson alapuló megközelítés kialakítása. A Bizottság álláspontja abban nem változott, hogy a dezinformálás elleni küzdelem egyik legfontosabb terepe a polgárok médiatudatos nevelése.[518]

A cselekvési tervnek megfelelően a Bizottság 2020-ban előterjesztette a digitális szolgáltatások egységes piacáról szóló rendelet javaslatát, amelyet 2022 őszén fogadtak el. A rendelet célja az Alapjogi Chartában biztosított jogokat tiszteletben tartó, de biztonságos, kiszámítható és megbízható online környezet kialakítása.

A rendelet meghatározza a jogellenes tartalom fogalmát:

> „bármely olyan információ, amely önmagában vagy egy tevékenységgel kapcsolatban, beleértve a termékek értékesítését vagy a szolgálatások nyújtását, nem felel meg az uniós jognak vagy bármely tagállam – az uniós joggal összhangban álló – jogának, függetlenül az adott jog pontos tárgyától vagy jellegétől."[519]

E jogellenes tartalmakra tekintettel engedi meg a rendelet a tagállami igazságügyi vagy közigazgatási szerv határozatán nyugvó tartalom elleni fellépést. A végzésnek többek között pontosan meg kell jelölnie annak uniós vagy nemzeti jog szerinti jogalapját, a jogellenesség indoklását, a jogellenes tartalom pontos azonosíthatóságát.[520] A végzést pedig továbbítani kell a kibocsátó hatóság szerinti állam digitális szolgáltatási koordinátorának.[521] Emellett a tárhelyszolgáltató olyan mechanizmusokat köteles alkalmazni, amely bármely személy vagy szervezet számára elérhető szolgáltatás keretében tapasztalt jogellenes tartalom bejelentését lehetővé teszi számára.[522] Emellett a rendelet továbbra is lehetővé teszi a tartalommoderálást a platformok részéről. A tartalommoderálással kapcsolatban pedig előírja, hogy évenként egyszer erről köteles jelentést tenni, amelynek része például az önálló tartalommoderálásról adott érdemi és érthető tájékoztatás, beleértve az automatizált eszközök alkalmazását, a felelős személyeknek nyújtott képzéseket, a szolgáltatást igénybevevő által nyújtott információ láthatóságát és hozzáférhetőségét érintő intézkedések számát és típusát, a szolgáltatás igénybe vevőinek a szolgáltatáson

518 Az Európai Bizottságnak közleménye az Európai Demokráciára vonatkozó cselekvési tervről. Brüsszel, 2020.12.3. COM(2020) 790 Final

519 Az Európai Parlament és a Tanács (EU) 2022/2065 Rendelete (2022. október 19.) a digitális szolgáltatások egységes piacáról és a 2000/31/EK irányelv módosításáról (digitális szolgáltatásokról szóló rendelet) (továbbiakban: DSA), 3. cikk, h) pont

520 Eljárásokat és a teljes szabályozást l. bővebben: Ződi (2023)

521 DSA 9. cikk

522 Uo., 16. cikk

keresztüli információszolgáltatásra való képességét, a szolgáltatás egyéb kapcsolódó korlátozásait, valamint a belső panaszkezelésre vonatkozó adatokat, így a panaszok számát, a panaszok alapját, az e panaszokra vonatkozó döntéseket, továbbá a tartalommoderlásra használt automatizált eszközöket és azok minőségi leírását.[523] A platformoknak a korábbitól eltérően átlátható belső panaszkezelési rendszert kell működtetniük, aminek része az eltávolítás, a hozzáférhetetlenné tétel, a szolgáltatás felfüggesztése vagy a megszűntetésével kapcsolatos döntések felülvizsgálata és indokolása. Ennek során pedig „az online platformot üzemeltető szolgáltatók időben, megkülönböztetéstől mentesen, kellő gondossággal és nem önkényesen eljárva kezelik a belső panaszkezelési rendszerükben benyújtott panaszoka". [524]

Ezek már önmagukban olyan előrelépések, melyek a hibrid fenyegetések dezinformációs műveleteinek hatékonyságát csökkenthetik. Ilyennek tekinthető a rendelet 22. cikke is, amely létrehozza a megbízható bejelentő intézményét, akinek/aminek a bejelentését kiemelten kell kezelnie a szolgáltatónak. Ezt a státuszt pedig a digitális szolgáltatási koordinátor ítéli oda a szakértelemmel, hozzáértéssel rendelkezőnek, aki emellett független és kellő gondossággal, pontossággal végi tevékenységét. E tevékenységéről pedig évente köteles jelentést tenni.[525] Szintén segíti az ezen tevékenységekkel szembeni fellépést az, hogy az online platformoknak fel kell függeszteniük a szolgáltatás nyújtását olyan igénybevevőnek, aki gyakran oszt meg nyilvánvalóan jogellenes tartalmat. Ezt szolgálja még az online hirdetések átláthatósága is, hiszen visszakövethetőbbé teszi az egyes félrevezető tartalmakat.[526] Az online óriásplatformokkal szembeni plusz elvárás a kockázatértékelés, amely kiterjed olyan tartalmak megjelenhetőségére, ami alapvető jogok gyakorlását érintő tényleges vagy várható negatív hatásokat eredményezhet, amelyek a társadalmi párbeszédre, a választási folyamatokra, vagy a közbiztonságra negatív hatással vannak, továbbá közegészséggel, kiskorúakkal kapcsolatban tényleges negatív hatást eredményeznek. Ezen esetekben a kockázatcsökkentési intézkedésekkel megtörténhet többek között tartalommoderálás vagy szolgáltatás korlátozása.[527]

A rendelet rendelkezik arról, hogy ki kell dolgozni egy Uniós válságkezelési protokollt, amely lehetővé teszi a hatékony, átlátható fellépés lehetőségét közbiztonságot vagy közegészségügyet veszélyeztető helyzetekben. Válsághelyzet fennállása esetében a Bizottság a Testület ajánlása alapján határozatot fogad el, amelyben előírja, hogy a szolgáltató értékelje, hogy szolgáltatása (valószínűleg) jelentős mértékben hozzájárul-e a súlyos fenyegetéshez és milyen mértékben, továbbá azonosítsa a konkrét, eredményes és arányos intézkedéseket és alkalmazza is azokat, emellett pedig az első kettőről időszakonként készítsen jelentést a Bizottság számára. Az intézkedések, ha megkívánják, az Alapjogi Chartába foglaltakat is sérthetik.[528] Ami így számos kérdést vet fel – még akkor is, ha erre lényegében a Bizottságtól kap utasítást –, legfőképpen azt, hogy nem állami szerv korlátoz alapvető jogot ezáltal, mégpedig a védelmi alkotmány, belső válságkezelés területét érintő kérdéskörben, ahol az Unió hatásköre is erősen vitatható. Emellett megjelenik a rendeletben a válságkezelési protokoll is, amely szintén közbiztonságot vagy közegészségügyet érintő rendkívüli körülmény esetére vonatkozik. E protokollt kidolgozásában a szolgáltatóknak közre kell működniük. A Bizottságnak lehetősége van

523 DSA 15. cikk
524 Uo., 20. cikk
525 Uo., 22. cikk
526 Uo., 24–26., 39. cikk
527 Uo., 34–35. cikk
528 Uo., 36. cikk

a válságkezelési protokoll kidolgozásába bevonni a tagállami hatóságokat is. Érdekes módon a Bizottságnak csak törekednie kell arra, hogy a protokoll a lehető legkonkrétabban határozza meg, hogy mi minősül rendkívüli körülménynek, vagy mik az egyes résztvevőknek a szerepük és milyen intézkedéseket hozhatnak meg, továbbá milyen eljárásban nyilváníthatják ki a válságkezelési protokoll alkalmazását és milyen időszakra vonatkozik ez a felhatalmazás.[529] Itt érdekes összeütközés lehet az Uniós és tagállami hatáskörök között, hiszen a közbiztonság, belbiztonság alapvetően tagállami hatáskör. Kérdéses az is, hogy a válsághelyzet azonosítható-e a belső jogrendi különleges jogrenddel, annak egy digitális verziója, mondhatni egy kibertéri különleges jogrendje. Ezen esetekben nehezen elfogadható, hogy egy tagállam hibrid támadás esetében, ahelyett, hogy önállóan intézkedjen és kérje a platformszolgáltatótól, hogy korlátozzon bizonyos tartalmakat, helyette az Uniós válsághelyzeti protokoll hatályba léptetését kivárva a Bizottságon keresztül próbálja érdekeit érvényesíteni. Kérdéses, hogy egy tagállamot érintő politikai jellegű különleges jogrend esetében, amilyen alapvetően egy hibrid szcenárió elő kíván idézni, az Uniós mechanizmus beindítható-e késleltető politikai csatározások nélkül. További problémát jelent, hogy a rendelet a jogellenes tartalmakkal foglalkozik. Azonban egy hamis információ, ahogy fentebb a demokrácia cselekvési terv esetében az Unió is megjegyezte, nem feltétlen jogsértő. Vagyis a nem jogsértő hamis információk elleni fellépés lehetőségét az óriásplatform szolgáltató kockázatelemző tevékenységi körében szabályozza csak a rendelet, így tagállami közbenjárásra ilyen tartalom moderálása maximum az eszkaláció magasabb fokát jelentő válságkezelési protokoll aktiválása után lesz lehetséges. Mivel ez egy Uniós intézmény lesz, ebből adódóan nem, vagy csak részlegesen tud illeszkedni az egyes tagállamok társadalmi valóságához, nem feltétlen tudja kezelni azokat a töréspontokat, amelyeket hibrid támadás esetében kezelnie kell a megtámadott államnak.

2.4. A fordulat éve(i) – A kiberbiztonság egységesítése az Unióban

Nem véletlen tehát, hogy 2020-as év végére kifejezett szándék jelent meg az Unióban arra, hogy a kiberbiztonság területén is erősíteni kell az integrációt. Ez a digitális rendeletcsomagon túl, a stratégia ismételt megújítását jelentette, valamint több jogszabálytervezet elkészítése és 2022-ben történő elfogadása. Így többek között a NIS2, a European Cyber Resilience Act kiemelkedő jelentőséggel bírnak a következő évek tekintetében.

Az új stratégia rendkívül erős mondatokkal nyitva érzékelteti, hogy az Európai Unió már egészében látja azt a problémát – a nagyszámú lehetőség mellett –, amit a kibertér jelent. A stratégia szerint

> „a kiberbiztonság az európaiak biztonságának szerves része (…) A közlekedés, az energiaügy, az egészségügy, a telekommunikáció, a pénzügy, a biztonság, az űrpolitika, a védelem és a demokratikus folyamatok nagymértékben függenek az egyre inkább összekapcsolt hálózati és informatikai rendszerektől."[530]

529 DSA 48. cikk

530 Közös közlemény az Európai Parlamentnek és a Tanácsnak Az EU kiberbiztonsági stratégiája a digitális évtizedre, Brüsszel, 2020.12.16. JOIN(2020) 18 final (továbbiakban: Az EU kiberbiztonsági stratégiája a digitális évtizedre) 1.

És ezeket a folyamatokat a Covid19 járvány tovább erősítette, hiszen egyes folyamatok, így a munkavégzés digitalizációja is felgyorsult. Jelentős problémát jelent, hogy a kibertér globális és nyílt, ami a háttér technológia területén tapasztalható ellátási lánc visszásságai mellett geopolitikai feszültségekhez vezet, továbbá óriási probléma, hogy az elmúlt években a kritikus infrastruktúrákat folyamatosan növekvő számú rosszindulatú támadás éri, és ezek az aggodalmak akadályozzák az online szolgáltatások igénybevételét, végső soron pedig gazdasági károkat okoz. A területen – mint korábban is kifejtésre került – óriási a látencia, és a bűncselekmények feltérképezése pedig kis százalékban tud eredményes lenni. Szembetűnő a stratégia azon kijelentése, hogy egyik oldalról folyamatosan bővülő ágazat a kiberbűnözés, másik oldalról a vállalkozások és az egyének kiberfelkészültsége és kibertudatossága alacsony, a munkaerő tekintetében a kiberbiztonsági készségek jelentős hiánya figyelhető meg. Utóbbiak tekintetében azért meg kell jegyezni, hogy ezért a tagállamok mellett az Uniót is felelősség terheli, mert mindeddig az egyének felzárkóztatására kevés programot hoztak létre, azok legtöbbje is igencsak holisztikus megközelítésű.[531] Emellett az EU rendkívül nagy utat járt be az elmúlt évtizedben, mivel korábban hangsúlyozta, hogy ezek a fenyegetések valójában leginkább gazdasági jellegűek, mára azonban egyértelműen felmérte, hogy ez egy össztársadalmi probléma, amit kezelni kell. Ami viszont még kevésbé látható, hogy ez nem csak technológiai oldalról megoldandó kérdés, hanem multidiszciplináris megközelítést igényel, főként az oktatás és kutatás, valamint a szabályozás területén.

A korábbi stratégiák eredményeire építve három fő (szabályozási, beruházási és szakpolitikai) eszköz alkalmazását az uniós fellépés három területén látja fontosnak: 1. reziliencia, technológiai szuverenitás és vezető szerep, 2. operatív kapacitásépítés a megelőzés, elrettentés és reagálás érdekében és 3. a globális és nyílt kibertér előmozdítása.[532] A megvalósítás a következő hét év jelentős digitális beruházásaihoz fog kötődni, amelyek számos ösztönzőt, kötelezettséget, teljesítménymérőt fognak integrálni a digitális beruházásokba, amelynek kiemelt területe a mesterséges intelligencia, a titkosítás és a kvantum-számítástechnika. A folyamat egyik fő támogatója pedig az Európai Védelmi Alap (EDF) lesz.

A három fő terület alterületekre bontható. A reziliencia, technológia szuverenitás és vezető szerep a következőkre épül: a) reziliens infrastruktúrára és kritikus szolgáltatásokra; b) az Európai kiberpajzs létrehozására; c) ultrabiztonságos kommunikációs infrastruktúrára; d) a következő generációs széles sávú mobilhálózatok biztonságának biztosítására; e) az IoT után a biztonságos dolgok internetére; f) nagyobb globális internetes biztonságra; g) megerősített jelenlétre a technológiai ellátási láncban; h) kiberkészzségekkel rendelkező uniós munkaerőre.[533] Ezek egy része Uniós szinten megvalósíthatónak tűnik, így a szabályozási környezet átalakítását, például a NIS irányelvet, digitális rendeletcsomag révén, illetve a társadalmi reziliencia, az egyéni fejlesztési programok. Azonban egyes megfogalmazások propagandisztikusak, így az ultrabiztos rendszer, az Európai kiberpajzs, a globális internet biztonságának növelése, amelyre egyre kevésbé van ráhatása a közösségnek, így nem tűnik reális célnak.

Az operatív kapacitásépítés a megelőzés, elrettentés és reagálás érdekében az alábbi területeket fogja össze: a) közös kiberbiztonsági egység; b) a kiberbűnözés kezelése; c) az uniós kiberdiplomácia eszköztárának aktív használata; d) a kibervédelmi képességek fejlesztése. Eb-

531 Uo., 1-4.
532 Uo., 5.
533 Uo., 6–14.

ből igazán újdonság erejével hat a közös kiberbiztonsági egység létrehozása, ugyanis eleddig az Unió ódzkodott ilyen típusú szerv létesítésétől, viszont maga a dokumentum is kiemeli, hogy ez egy fontos lépés lenne az európai kiberbiztonsági válságreagálás területén. A közös kiberbiztonsági egység három fő célt szolgálna: a kiberbiztonsági közösségek felkészülését, a hatékonyabb információmegosztáson alapuló helyzetismeretet, valamint a koordinált válasz megerősítését.[534] A 2021 októberében az Európai Unió Tanácsa által kiadott következtetésekben megerősítették, hogy a tagállamok is egyetértenek egy hasonló intézmény felállításával, azonban az ahhoz való csatlakozást csak önkéntes alapon tudják elképzelni.[535]

A globális és nyílt kibertér előmozdítása területén az EU vezető szerepet kíván elérni a kibertérre vonatkozó szabványok, előírások és keretrendszerek kialakítása, fokozása terén. Ez az EU jelenlegi geopolitikai szerepét vizsgálva egész utópisztikusnak tűnik, hiszen mind az USA, mind pedig Kína jelentősen nagyobb erőforrásokkal bír ezen a területen. Ezeken túlmenően az ENSZ égisze alatt egy felelős állami magatartásokra vonatkozó önkéntes, nem kötelező érvényű norma megalkotásának az irányába szeretnének elmozdulni, amely terv megint csak olyan jellegű, amely lényegi elmozdulást nem eredményezne ezekben a folyamatokban, mert tényleges szankciók hiányában az eseti hatalmi és politikai érdek felülírná a magatartási kódexbe foglaltakat. A további pontok visszatérő jellegűek, így az együttműködés és annak erősítése a partnerekkel, valamint a reziliencia fokozása, még globális köntösben sem jelent újdonságot.[536]

Az új kiberbiztonsági stratégia jelentős elmozdulást jelent a realitások irányába, legalábbis a felismerések területén, illetve a közös egység létrehozásának igényével, azonban egyes célok utópisztikus jellegűek, amely talán abból is fakad, hogy az EU nem jól méri fel a jelenlegi geopolitikai helyzetét és a globális geopolitikai viszonyokat. Ezeken túlmenően viszont az új szabályozás ténylegesen elmozdíthatná a közösséget a működőképesebb kiberbiztonság irányába.

Érdemes tehát röviden áttekinteni ezeket a jogszabályokat. A NIS2 irányelv preambuluma hangsúlyozza, hogy a NIS óta jelentős eredményeket ért el a közösség a kiberreziliencia területén, amely lehetővé teszi, hogy a következő szintre emeljék a kiberbiztonsági szabályozást, emellett a megjelenő új kihívások és a korábbiak fokozása ezt szükségessé is teszik. Nem véletlen, hogy a NIS2 az alapvető szereplők körét kibővíti, míg új csoportként hozza be a fontos szervezetek, ugyanis itt túlnyomóan szereplő ellátási láncok biztonsága mára össztársadalmi létérdek lett. Alapvető szervezetek esetében az energia területén megjelent külön alpontként a távfűtés, a -hűtés és a hidrogén, fő területként pedig a szennyvíz, a közigazgatás és a világűr. Fontos területek köre pedig szinte egészében lefedi az egyének hétköznapjait: postai és futárszolgáltatások, hulladékgazdálkodás, vegyszerek gyártása, előállítása és forgalmazása, élelmiszer előállítása, -feldolgozása és forgalmazása, gyártás (például: orvostechnika, diagnosztikai eszközök, számítógépek, elektronikai és optikai termékek, gépjárművek), digitális szolgáltatások.[537] E szervekről az ENISA nyilvántartást vezet.

534 Uo., 14–22.

535 A Tanács következtetései a nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt uniós reagálás kiegészítéseként szolgáló, a közös kiberbiztonsági egységre vonatkozó kezdeményezésben rejlő lehetőségek feltárásáról, Brüsszel, 2021. október 8., 12534/21.

536 Az EU kiberbiztonsági stratégiája a digitális évtizedre, 22–28.

537 Az Európai Parlament és a Tanács (EU) 2022/2555 Irányelve (2022. december 14.) az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (továbbiakban: NIS 2 irányelv), I–II. melléklet

Az irányelv kimondja azt is, hogy ezek a kiberbiztonsági rendelkezések a minimális harmonizációt teremtik meg, így ennél inkább csak magasabb szintű bizonságot szavatóló szabályozást fogadhatnak el a tagállamok. A korábbiakhoz képest a nemzeti kiberbiztonsági stratégiáknak ki kell egészülniük többek között az alapvető és fontos szervezetek által használt IKT-termékek kiberbiztonsági kérdéseire, így az ezekkel kapcsolatos követelményekre a közbeszerzés folyamán, a kiberbiztonsági készséges népszerűsítésére, fejlesztésére, kutatás és fejlesztés témakörére, a nyílt internet nyilvános magjának, általános elérhetőségének és integritásának a fenntartására, a vállalatok közötti önkéntes kiberbiztonsági információmegosztásra. Emellett a biztonsági rések összehangolt közzétételére egy eljárásrendet és egy nyilvántartást hoznának létre. Minden tagállamnak saját nemzeti kiberbiztonsági esemény- és válságkezelési tervet kell kidolgoznia. A szervek és együttműködések keretében új szerveként létrehozza az Európai Kiberválságügyi Kapcsolattartó Szervezetek Hálózatát, amelynek feladata a nagyszabású kiberbiztonsági események és válságok operatív szintű összehangolása, valamint az érintett tagállami és közösségi szervek közötti rendszeres információmegosztás biztosítása. Az alapvető és fontos szerveknek pedig kiberbiztonsági, kockázatkezelési és jelentéstételi kötelezettséget ír elő, amelyet a szervezet vezető testületének jóvá kell hagynia, így az abba foglaltak nem teljesítése esetén számonkérhetővé válnak. Újdonság, hogy foglalkozik az ellátási láncok és a beszállítói kapcsolatok biztonságával is. A korábbiaktól eltérően pedig részletesen szabályozza a tagállami hatóságok felügyeleti tevékenységét az érintett alapvető és fontos szervek körében, az irányelvben foglaltak minél hatékonyabb megvalósulása érdekében. Így nem meglepő, hogy a rendelet az ezek meg nem valósítása esetén kifejezetten előírja a közigazgatási bírság kiszabását. Nem titkolt célja a szigorúbb felügyelet, a szigorúbb végrehajtási követelmények mellett a szankciórendszer harmonizálása a tagállamokban.[538]

A NIS2 tehát jelentős előrelépést jelentene, hiszen sokkal nagyobb körben határozza meg a szabályozással érintett szereplők körét, így a társadalom tagjai által igénybe vett szolgáltatás jelentős része a szabályozás hatálya alá kerül. A nemzeti kiberbiztonsági stratégiák hatókörét is kibővíti az IKT-termékek átláthatóbb és szabványosítottabb felhasználásának kialakítására, az ismeretterjesztés, az oktatás, a kutatás területére. A szereplőktől pedig elvájra, hogy felépítsék saját képességüket, arról jelentést tegyenek. Összességében egy erősebb kockázat- és eseménykezelési együttműködést alapoz meg a javaslat (amely a szabályok hatályát jelentősen kiterjesztette), amellyel az Európai Unió Tanácsának a szándéka egyértelműen az, hogy az uniós kiberbiztonsági képességet és kiberrezilienciát megerősítse.

A Cyber Resilience Act (a digitális elemeket tartalmazó termékekre vonatkozó horizontális kiberbiztonsági követelményekről) lényegében azt a felismerését ülteti jogi keretek közé, hogy a hardver- és szoftvertermékek egyre gyakrabban válnak kibertámadás célpontjaivá. Két fő oka van ennek: az egyik a kiberbiztonság alacsony szintje, ami a széles körben elterjedt sebezhetőségekben és az ezek kezelésére szolgáló biztonsági frissítések elégtelenségében és következetlenségében nyilvánul meg, a másik oldal, hogy a felhasználók nem ismerik eléggé az információkat, és nem férnek hozzá eléggé az információkhoz, ami megakadályozza őket abban, hogy megfelelő kiberbiztonsági tulajdonságokkal rendelkező termékeket válasszanak, vagy azokat biztonságos módon használják. Így kifejezetten aggodalomra ad okot, hogy ezekre a termékekre javarészt nem vonatkoznak a kiberbiztonságot kezelő uniós jogszabályok. Így a jogszabálytervezet két fő célt határozott meg: a hardver- és szoftvertermékek kevesebb sebez-

538 NIS 2. irányelv

hetőséggel kerüljenek forgalomba és az életciklusuk során a gyártók végig komolyan vegyék a biztonságot, másik oldalról pedig olyan feltételrendszer kialakítása, hogy a felhasználók már a termék kiválasztásakor, vagy használata során fel tudják mérni annak kiberbiztonsági vonatkozásait. Ezt pedig négy konkrét területhez kötik: 1. biztosítani kell, hogy a gyártók már a tervezés, fejlesztés fázisától figyelembe vegyék a termékük biztonságát; 2. koherens kiberbiztonsági keretrendszer, amely egyértelművé teszi, hogy a gyártók miért felelősek; 3. maguknak a termékek biztonsági tulajdonságai átláthatóságának a megteremtése; 4. maguknak a termékek biztonságos használatának a megteremtése.[539]

Az elmúlt években az Európai Unió kiberbiztonsággal kapcsolatos hozzáállása jelentős, mondhatni 180 fokos fordulaton esett át. Hiszen az egy évtizeddel ezelőtti állapothoz képest felmérték, hogy a kibertér és a kapcsolódó rendszerek biztonsága nemcsak gazdasági kérdés, hanem a társadalmi totalitás egészét érintő kérdéskör, amely mind az állami, mind a gazdasági, mind pedig az egyén életét, életterét jelentősen befolyásolja, így arra jóval komplexebb stratégiát, szabályozást kell megalkotni. A 2010-es évtized végére a stratégiai irányvonal egyértelműen visszatükrözi ezt, amelyben fontos szereplővé váltak az egyének és csoportjaik mint a társadalmi reziliencia alappillérei. Ennek köszönhetően az oktatás, a fejlesztés és a kutatás, valamint az innováció minden eddiginél hangsúlyosabb kérdéskörré vált. Emellett lépéseket tett az Unió a hibriditásból eredő kiberártalmak csökkentésére, így a dezinformáció visszaszorítására is, amely végül elvezethet a közösségimédia-platformok hatékonyabb szabályozásához is, bár itt még rendkívül hosszú utat kell bejárni.

539 Javaslat Az Európai Parlament és a Tanács rendelete a digitális elemeket tartalmazó termékekre vonatkozó horizontális kiberbiztonsági követelményekről és az (EU) 2019/1020 rendelet módosításáról, Brüsszel, 2022.9.15. COM(2022) 454 final

IV. rész
A védelmi jog és kibertér

1. A jogi szabályozás szerepe a 21. századi biztonság fenntartásában és erősítésében

A biztonság fenntartása, a biztonsági célok meghatározása, valamint a védelem mint a biztonságot szavatoló tevékenységek összessége tekintetében a transzatlanti térségben az állam és a jog szerepe kiemelkedő fontosságú, de nem kizárólagos.[540] A komplex biztonság egyértelműen magával hozza egyik oldalról a társadalmi szereplők felelősségét és biztonságtudatosságának felértékelődését, másik oldalról pedig az állami-társadalmi kooperáció korszakos fokozásának megkerülhetetlenségét. Azáltal ugyanis, hogy a biztonság tematikus horizontja – ha úgy tetszik, dimenzióinak száma – rendkívüli mértékben bővült a huszadik század második felétől, illetve mélysége is fokozódott, hatékonyan nem képzelhető el, hogy az állam kizárólagosan tudja szavatolni a biztonság legjelentősebb részét. Az állam és a jog kiemelkedő szerepe egyrészről a piaci alapon nem, vagy hatékonyan és tartósan nem szervezhető közszolgáltatások (például a honvédelemi, a rendészeti, a titkosszolgálati, az élelmezés-, egészség-, ipar-, energia-, ellátásbiztonsági követelmények egységesítését és ellenőrzését szolgáló képességek) fenntartásában, fejlesztésében, másik oldalról pedig a komplex védelem megfelelő szervezésében, a különféle társadalmi, gazdasági és más érdekek fejlődést megalapozó becsatornázásában, illetve a biztonságtudatosság fejlesztésének hiteles megalapozásában van.

E tekintetben a kibertér jelentette kihívás már önmagában is újszerű,[541] hiszen egyik oldalról magától értetődő, hogy az államnak a védelmi képességei körében fejlesztésekkel kell alkalmazkodnia ahhoz a tényszerű változáshoz, hogy a kibertérben számos olyan cselekmény is történik, amire a hagyományos védelmi képességekkel adott esetben reagálni kell. Az információs térben zajlik a bűnözés, történnek katonai és hírszerzési műveletek, egyértelműen megvalósul a geopolitikai érdekérvényesítés és befolyásolás, vagy a gazdasági nyomásgyakorlás. Az ehhez való alkalmazkodás már önmagában jelentős kihívás, mivel ez nem csak technikai, hanem szemléletbeli és szervezeti fejlesztéseket is feltételez, amelyek hatékonyságát jelentős mértékben befolyásolja az is, hogy az állam védelmi és biztonsági képességei, struktúrája a hagyományos feladatrendszer tekintetében mennyire korszerű és hatékony. Fokozza azonban a kihívást az is, hogy a kibertérrel kapcsolatos piaci alapon nem szervezhető védelmi tevékenységek ellátása terén a piaci környezetben jelentős értékkel bíró szaktudásra van szükség, amelynek az állami szférába történő bekapcsolása eleve jelentős innovativitást igényel mind szervezeti-működési, mind pedig humánerőforrás-menedzsment oldalról.

---

540 A téma kapcsán l. Kádár (2022a): 61–73., Kelemen (2022b), Farkas Ádám (2022a), Farkas Ádám (2023): 17–31., Farkas Ádám (2022d): 113–124.

541 Példaként l. Török–Ződi (2022), Török–Ződi (2021), Tóth András (2018), Klein (2021): 129–166., Vikman (2022a), Vikman (2022b)

A legjelentősebb kihívást azonban mégis az adja, hogy a kiberbiztonság terén az állammal szemben jogos elvárás, hogy felzárkózzon a kor kihívásaihoz, miközben az érintett állami rendszerek ezer szálon kapcsolódnak nem állami szereplőkhöz – a felhasználóktól a szolgáltatást nyújtó vállalatokon át egészen az állammal információs kapcsolatba lépő külső szereplőkig –, amelyek biztonságtudatos tényked ése jelentős mértékben visszahat az állam kiberbiztonsági feladatellátásának hatékonyságára.

A kibertér kapcsán tehát az állam feladataiban rejlő kihívás rendkívül jelentős, és az erőforrások, intézmények és eljárások szisztematikus fejlesztésén túl megkerülhetetlenné teszi azt is, hogy az állam a rajta kívül álló szereplők biztonságtudatosságának, biztonságot erősítő vagy legalábbis nem erodáló tényked ésének előmozdításáért is jelentős lépéseket tegyen. Ehhez azonban, ahogy az előzőekben is jeleztük már, az állam védelmi működésében a tradicionálisan jellemző imperatív/korlátozó szabályozás mellett az együttműködéses és adott magatartásra orientáló szabályozási karakternek épp úgy meg kell jelennie, mint a biztonság komplex felfogásának és társadalmi elfogadottságának, támogatottságának. Ezzel a követelményrendszerrel pedig a kibertér lényegében egy új szabályozási területet hív életre a kiberbiztonság szabályozásával, amiben a már tárgyalt EU-szintű szabályozás rendkívüli dinamikát mutat. A kibertér jogi leképezése azonban karakterében átmentet képez a hagyományos védelmi-biztonsági területek szabályozása és a civil viszonyok jogi keretei között. Egyik oldalról a hagyományos védelmi-biztonsági funkciók kibertérben való megvalósulása szorosan érinti a védelmi-biztonsági szabályozást és ezzel a tág értelemben vett nemzetbiztonság magját, míg másik oldalról a kibertér kiterjedt gazdasági és társadalmi kiaknázása miatt a kiberbiztonság túl is mutat a hagyományos védelmi-biztonsági funkciókon, és okkal tekinthető attól külön értelmezendő, új jogterületnek is.

Bárhogy is nézzük, a kibertér jelentette kihívások hagyományos védelmi és biztonsági, illetve azon túlmutató „önálló” kiberbiztonsági megközelítése során is fontos, hogy a technikai szemléletmód mellett felhívjuk a figyelmet a humán tényező és a társadalmi kapcsolódások fontosságára, kiemelve, hogy a technikai értelemben vett biztonságot leginkább szolgáló szabályozás hatékonysága is végletesen csorbulhat akkor, ha a szabályozási és intézményi rendszer nem tudja megfelelően kezelni az egyéni és társadalmi vonatkozásokat az edukációtól a különféle kommunikációs, képzési és érdekegyeztetési vonatkozásokig.

Másik oldalról nézve azonban, a jogállamiságból önmagában is következik, hogy a biztonság és védelem tekintetében a jognak is kimagasló szerepe van, hiszen egy jogállamban az állami fellépés arra terjedhet ki szisztematikusan és mindenki által követhető, elfogadható módon, amire jogszabályok felhatalmazzák, és ahogyan felhatalmazzák. Ebből következően a szabályozás jellege, keretei alapjaiban determinálják, hogy a különféle egyéni és társadalmi szintű jogok miként érvényesülnek, hiszen a biztonság szintjének romlása egyértelműen hátrányosan hat a jogok érvényesíthetősére és a polgári szabadságokra, ezáltal pedig a fejlődésre és a gazdaságra is. Ez az összefüggés azért is fontos, mert rávilágít arra, hogy az állam védelmi és biztonsági képességeit, intézményeit és szabályait akkor is a kor színvonalán kell tartani, ha az adott állam közvetlenül nincs jelentős hagyományos fenyegetésnek kitéve – a svájci, szingapúri, norvég hozzáállás ezt jól példázza –, mivel ezek a biztonság fenntartásához és ezáltal a jogérvényesüléshez, a gazdasági fejlődés alapját adó stabilitáshoz közvetlenül kapcsolódnak, emellett pedig nem katonai (például katasztrófakezelési, rendészet-támogatási, közcélú műszaki) tevékenységekre is használhatók, viszont elhanyagolás esetén még a szükséges anyagi erőforrások és politikai-társadalmi akarat ellenére sem pótolhatók kellő hatékonysággal és je-

lentős áldozatok nélkül egyik napról a másikra. Ez a sajátosság, amit Európa legtöbb országa az elmúlt harminc évben a saját kárán tanult meg a védelmi képességek, intézmények és szabályozások perifériára sorolásával, majd a fejlesztések újbóli elindításával.[542] Ennek a korábbi mulasztásnak a jövőbeni elkerülése a kiberbiztonság tekintetében kiemelt jelentőségű lesz. A digitalizáció dinamikája miatt ugyanis, ha ezt a területet mint konkrét szakterületet és mint az állam védelmi és biztonsági rendszerének egészét átható változási halmazt, időszakosan kevéssé fontos fejlesztési célként kezeljük, kérdéses, hogy a keletkező lemaradás behozható lesz-e a jövőben.

Érdemes azonban mind a biztonság-szavatolás jogállami determináltságát, mind pedig a kiberbiztonsági feladatrendszer újszerűségét és jelentőségét általánosságban összekapcsolni a komplex biztonság rendkívül tág fogalmával is. Ezen kapcsolódás révén ugyanis arra is rávilágíthatunk az előzőekben leírtak kapcsán, hogy a biztonság és a szabályozás közös horizontja messze szélesebb, mint amit eddig jellemzően a védelemmel mint aktív biztonságot szavatoló – az állam legitim kényszermonopóliumával összekapcsolt – tevékenységek hagyományosan a honvédelemre, rendészetre és titkosszolgálati tevékenységekre kiterjedő összességével azonosítva képzeltünk. A biztonság szabályozási alapjaiba ugyanis a legtágabb értelemben mindazon szabályok beleértendők, amelyek a különféle tevékenységek (például közlekedés, ipari termelés, gazdálkodás, egészségügyi szolgáltatás, kutatás stb.) gyakorlása kapcsán azért tartandók be, hogy mindaz ne eredményezzen biztonságot fenyegető, erodáló következményt. A biztonság különféle szektoraiban ugyanis számos olyan lehetséges biztonsági veszély vagy fenyegetés felmerülhet, amelyek bizonyos szint elérésekor kapcsolódhatnak a hagyományos védelmi tevékenységekhez, mert például katasztrófához vezetnek vagy lehetőséget teremtenek súlyos bűncselekmények vagy akár konkrét szuverenitás elleni támadás megvalósítására, de mind ezen szint alatt, mind pedig e felett sajátos szektorális fellépést, szabályozást, illetve szektorközi – a magyar megfogalmazásban inkább ágazatközi – koordinációt igényelnek ahhoz, hogy ne váljanak jelentős veszteségek forrásává.

Nem véletlen, hogy a huszadik század második felétől a komplex biztonság széleskörű értelmezése fokozatosan teret nyert a transzatlanti térség államainak szervezési és szabályozási törekvéseiben, és arra ösztökélte az államokat, hogy a szektorális/ágazati specialitások erősítése és fejlesztése mellett az összbiztonsági, összkormányzati koordinációt és összhangot is fokozzák. Ennek típuspéldája az amerikai nemzetbiztonsági felfogásból következő megközelítés,[543] de lényegében ide sorolható az a megoldási séma is, amely átfogó külön szabályozás nélkül a kormányzás-közigazgatás szintjén biztosítja az átfogó koordinációt a különféle államokban. Ezt a komplex biztonságra jellemző sokrétű, kölcsönhatásosságon és hálózatosságon alapuló kapcsolódási mátrixot, a komplex biztonság talán teljességében át sem fogható, nem taxálható vertikális és horizontális kiterjedését pedig tovább fokozza, ha úgy tetszik hatványozza a digitalizáció minden szektorra kiterjedő fejlődése, ami számos hatékonyságnövelő hozadéka mellett komoly biztonsági kockázatokat is rejt magában mind üzemeltetési, irányítási és ezáltal a fizikai térre közvetlenül is visszahatni képes vonatkozásban, mind pedig ezen szektorok információi és ezáltal információs sérülékenységei kapcsán. Akkor tehát, amikor a védelem és biztonság-szavatolás kérdésein gondolkodunk az információs korszak kapcsán, fontos látni ezt a komplexitást és azt, hogy erre az információs technológia hatványozó té-

542 Vö. Spitzer–Vikman (2022a), Spitzer–Vikman (2022b)
543 Farkas Ádám (2020b): 5–20.

nyezőként épül rá, ami a termeléshatékonysági és szolgáltatásminőségi hozadékok mellett a hagyományos védelmi szféráktól független területek, infrastruktúrák sérülékenységét is fokozni tudja.

Ez persze nem tekinthető teljesen újszerű jelenségnek a történelemben, hiszen a különféle szabotázsok vagy akár a természeti erőforrások és az ahhoz kapcsolódó építmények károsításának ártó célú, illegitim alkalmazása már jó ideje rámutatott arra, hogy klasszikusan nyílt fegyveres szembenállás nélkül is használhatók támadó célokra a társadalmi rendszer különféle alapvető fontosságú vagy létfontosságú alrendszerei, infrastruktúrái.

Az ipari társadalom, majd a technológia többlépcsős forradalmi fejlődése azonban a jóléti és fogyasztói életvitel révén jelentősen megemelte a transzatlanti társadalmak többségi komfortszintjét, amit az információs társadalomba való átlépés tovább fokozott, hiszen az információs infrastruktúra nyújtotta előnyöket nem csak életünk kényelmes részévé tette, hanem fokozatosan megkerülhetetlen elemévé teszi számos területen az oktatás-kutatás, az egészségügy, a pénzpiacok és a gazdasági tevékenységek körében. Ez a fajta fejlődés tehát sokakat nem csak vagy nem elsősorban életviteli, hanem biztonsági értelemben is függővé tett a magasabb komforttal járó újításoktól, illetve a társadalom egyre inkább technológia-bázisú ellátásoknak és működési rendszereknek való kitettségét is jelentős mértékben megnövelte. Ezt tükrözi a létfontosságú infrastruktúrák témakörének felértékelődése. Ahogy tehát a technológiai és vele a kutatási, termelési és szolgáltatási paletta rohamosan differenciálódik, úgy bővül az állami és társadalmi szabályozás köre és tagoltsága is, amely bővülés a biztonság tartalmára, szabályozására és szavatolására is hasonló hatást gyakorol, az információs korszakban kiemelt területté téve a kibertérben tapasztalható kihívások megfelelő kezelését, megelőzését.

Egyik oldalról tehát a biztonság és védelem a jogi szabályozás viszonylatában ugyanabban az erőtérben értelmezendő, amiben a jogrendszer és az államműködés egésze: felzárkózási kényszerben van a tág értelemben vett környezet dinamikus változásaival szemben. Ez nemcsak fejlődési verseny, hanem egyben újfajta biztonsági sérülékenység is, ha a szabályozás lehetséges hiányosságait az ellenérdekelt cselekvők ki tudják használni saját céljaikra, ahogy erre a következőkben a lawfare kapcsán még kitérek. Másik oldalról azonban a szabályozásnak a biztonság kapcsán és ezzel összefüggésben a védelemben történelmi és funkcionális okokból is kulcsszerepe van.[544] A biztonsági és védelmi rendszereknek ugyanis gyorsan és hatékonyan reagáló, jól begyakorolható részrendszerek konzisztens egészeként kell felépülnie. Ebben pedig történelmileg kimagasló szerepe van a szabályozásnak. Nem véletlen, hogy a haderők történetében a különféle rendtartások, regulamentumok és szabályzatok már a szervezett társadalmak és haderők hajnala óta azonosíthatók, illetve a fejlődés kapcsán fokmérők is úgy a védelem, mint a társadalmi működésre és vele az államra visszaható jelentőség tekintetében. Niccolò Machiavelli ezt úgy fogalmazta meg, hogy

> „ha az ókori rendszabályokat tanulmányoznánk; akkor a polgári és katonaéletnél egységesebb, azonosabb dolgokat nem is találhatnánk; sem azt, hogy szükségszerűen annyira szeresse egyik dolog a másikat, mint ezek; ugyanis minden művészetben, amelyet csak megszerveznek egy társadalomban az emberek közös javára, minden rendszabály, amelyet azért foganatosítanak, hogy az emberek Isten és a törvények félelmében éljenek, hiába való lenne, ha a védelméről nem gondoskodnánk előre; azok a művészetek amelyek jól szervezettek, fenntartják még azokat is, amelyek nincsenek jól megszervezve. A jó rendszabályok

544 Vö. Morris (2020), Farkas Ádám (2019a)

viszont katonai segítség nélkül úgy vesznének kárba, mint egy fenséges királyi palota termei, amelyek bár arannyal és ékkövekkel díszesek, de mert még befödve nincsenek, nincs, ami megvédje őket az esőtől."[545]

Az idő persze meghaladta a kizárólag és dominánsan katonai erőre építő felfogást, az üzenet lényegét azonban nem: a jogállam és annak szabályai, velük pedig az egyéni és társadalmi biztonság a védelem nélkül nem állhatja ki az idők próbáját.

Ebben azonban a digitalizáció komoly kihívás elé állít minket, hiszen egyik oldalról a jog jellemzően hosszabb időre statikus, szemléletmódjában és gondolkodásmódjában pedig inkább lassan, mint gyorsan változó jellegét kell összehangba hozni az információs technológiai dinamikus fejlődésével és ebből adódóan egy olyan szakmai közeggel, amelynek szemléletmódja jelentősen eltér a jogi gondolkodástól, másik oldalról viszont számos olyan ma még tételesen nem azonosítható kihívást rejt magában, amelyek kellő hatékonysággal nem kezelhetők merev jogi keretek alkalmazásával, ám a társadalom szabadságfoka és az állammal szembeni biztonságérzete miatt – ahogy erre a cyberfare state kérdése kapcsán jelen kötet is kitért – végtelenül generalizált és rugalmasított megoldásokkal sem orvosolható hosszú távon.

Ahhoz viszont, hogy az állam védelmi és biztonsági feladatrendszerének optimális fejlesztése felé mozdulhassunk el az információs korszakban, előbb el kell jutnunk addig, hogy helyén kezeljük a védelem és biztonság kérdéseit társadalmi, állami és jogi felfogásunkban, mivel a hidegháború utáni időszak Európa-szerte – az egykori szovjet érdekszférában pedig fokozottan – hátrányosan hatott ezekre a funkciókra. Érdemes tehát a jogi szabályozás szerepét a biztonság és védelem viszonylatában három aspektusból külön is hangsúlyozni annak érdekében, hogy segíteni tudjuk az állam védelmi és biztonsági tevékenységeinek, az ehhez kötődő társadalmi együttműködésének a rehabilitálását és józan mértékletesség szerinti visszavezetését a jogtudományi, államtudományi, politikatudományi és -szakmai diskurzusokba.

Elsőként arra érdemes felhívni e téren a figyelmet az előzőekben leírtakra kapcsolódva, hogy a világ változásait és fejlődését követő védelmi szabályozás a jogállamiság oldaláról megközelítve is kulcsfontosságú, hiszen az állam szervei és különösen erőszakszervei tekintetében nem a „mindent szabad, amit nem tilos" elve érvényesül,[546] hanem a törvényekben meghatározott felhatalmazásokhoz igazodó működés – azaz a védelmi alkotmányosság[547] – követelménye. Ezen nyugszik egyik oldalról az állam önkorlátozása. Fontos azonban látni, hogy ez másik oldalról a védelmi és biztonsági szervek szabályok közötti, kiszámítható, hatékony, tervezhető és ezekből adódóan a civil szféra által el is várható működésére építve a rend, a stabilitás és ezek által az egyéni jogok érvényesíthetősége, illetve a társadalmi szintű fejlődés, továbbá a gazdasági gyarapodás fundamentuma is. A szabályozottság – különösen a jól és a működésben is hatékony szabályozottság – tehát alapvető garancia mind az állam működése, mind annak kontrolláltsága felől, együttesen: annak megbízhatósága felől nézve. Nem véletlen, hogy ennek a civil-katonai kapcsolatok, valamint a rendészet, a közigazgatás és a civil szféra egymáshoz való viszonya tekintetében is egyre hangsúlyosabb a megjelenése.[548]

545 Machiavelli (2001): 6.

546 L. Patyi (2015): 72–75.

547 L. Patyi (2016): 233–249., Farkas–Till (2016): 40–71., Farkas Ádám (2018c): 227–255.

548 A téma kapcsán l. Huntington (1994), Nielsen–Snider (2009), Sztankai (2012), Szeles (2005): 67–77., Christián (2022), Jonathan-Zamir–Wisburd –Hasisi (2014)

Figyelemmel arra, hogy a transzatlanti térségben a jogállamiság a részletekbe menő meghatározás nehézkessége mellett is olyan minimumkövetelmény-halmazt jelent, amelynek főbb elemeit az államok ismerik és elfogadják, könnyen belátható, hogy a térségbe tartozóként a szabályozás megfelelősége nemzetközi relációban is komoly súllyal bír. Érdemes azonban ezt a kérdéskört egy rövid feltevéssel kiegészíteni, melynek fókuszában a valódi globalizáció és általa a transzatlanti térségen kívüli államokkal való valós idejű interakciók állnak. A fizikailag is valódi és valós idejű kölcsönhatásokra épülő globalizáció rendszerszintű alapjait a világkapitalizmus fektette le, felépítményét pedig a technológiafejlődés teljesítette ki. A kapitalizmus jellegéből fakadóan azonban szerződéses viszonyok sokaságát feltételezi, függetlenül attól, hogy az érintett felek a nyugati értelemben vett jogfelfogáshoz és ez által a jogállami garanciákkal operálók köréhez tartoznak vagy sem. Ennek folytán azonosítható, hogy még a transzatlanti értelemben vett jogállamiságot kulturális-tradicionális okokból nem vagy nem teljesen osztó államoknál is megerősödött a nyugati követelményekhez igazítható szabályozás szintje, hiszen ez a gazdasági kapcsolatokhoz szükséges bizalom alapját adja. Másik oldalról az is látható, hogy formálisan fejlődést mutatnak a különféle jogvédelmi mechanizmusok is a világ különféle tájain, hiszen ez garanciát jelent a gazdasági kapcsolatok építése, illetve a munkaerő globális mobilitása érdekében oda utazó, települő személyek számára. Ez szükségképpen érinti már az egyes államok védelmi és biztonsági szerveinek működését is, vagyis, ha rendkívül széles felhatalmazási skálán is, de látható, hogy bizonyos kiszámíthatósági és garanciális minimumok – a diktatúrákat, a pszeudo-államokat és az államkudarcokat leszámítva – világszerte megjelenőben vannak a védelmi és biztonsági funkciók terén. Igaz, ebben a képletben pont az információs technológia, az abból származó adatok megismerése és felhasználása, illetve a biztonsági célú megfigyelés kérdése komoly kérdéseket és aggályokat vet fel időről-időre az elmúlt két évtizedben.

Mindebből megfordítva azt kell látni, hogy ha a védelmi és biztonsági funkciók szabályozása nem kellően korszerű, konzisztens, stabil és kiszámítható, akkor az az állammal szembeni bizalom erózióját eredményezheti. Ez a bizalomvesztés értelmezhető az államalkotó nép egyénei és csoportjai, az állammal szövetségi, partneri viszonyban álló többi állam, továbbá az állam kapcsán gazdasági érdekekkel vagy tervekkel rendelkező szereplők viszonylatában is. A korszerűtlen, inkonzisztens és nem megfelelően érvényesített szabályozás ugyanis potenciális lehetőséggé teszi az állam megfelelő reagálóképességének gyengülését vagy akár hiányát is az egyes, új fajta vagy összetettebb fenyegetések és krízisek viszonylatában, kiszámíthatatlanná vagy legalábbis bizonytalanná teheti az állam válaszait a különféle eshetőségekre, végső soron pedig akár az állam vagy annak intézményei általi visszaélések rémét is reális közelségbe hozhatja.

Ezen bizonytalansági lehetőségek bármelyikének fennállása pedig az érintett állam szuverenitásának gyengülésével, gazdasági és társadalmi vonzerejének és stabilitásának aláásásával, végső soron ezek realizálódása és spirálba kerülése esetén pedig az adott állam válságával fenyegethet. Az információs korszakba lépve nem nehéz belátni, hogy a fenti hátrányok elkerülése érdekében az állam védelmi és biztonsági szisztémájának is alkalmazkodnia kell a kibertér jelentette változásokhoz, mind a hagyományos fellépés, mind az újszerű – kifejezetten kiberbiztonsági – működés, mind pedig a digitalizáció kiterjedtségéből következő többsíkú, szükség szerint imperatív/korlátozó és szükség szerint kooperatív megközelítés tekintetében.

Európai viszonylatban azonban ezek közül jelenleg – némileg talán szokatlan módon – a védelmi és biztonsági szabályozás korszerűségének, konzisztenciájának és kiszámíthatóságának fontossága kapcsán a gazdasági bizalomra gyakorolt hatást kell kiemelni. Fontos ugyanis látni, hogy gazdasági prosperitás – ideértve a befektetések növekedését, az innováció fokozódását és ezek kialakítását, majd működtetését is – nehezen képzelhető el olyan államban, ahol az alapvető biztonsági szinttel kapcsolatban kínos kérdések, illetve konkrét krízisek esetén bizonytalan megoldások tapasztalhatók. Ez fokozott jelentőségű az információs infrastruktúra tekintetében, amely korunk valamennyi fejlődést megalapozó kulcsterületén alapvető fontosságú.

A megfelelő szabályozás tehát a bizalmi kérdésen túl az állam felkészültségét, a biztonsági környezettel kapcsolatos szakértői gondolkodását és felkészültségét is tükrözi, ami minden értelemben kulcsfontosságú a fejlődés és az ehhez szükséges bizalom szempontjából. E bizalom megteremtése pedig nem a nagy- és középhatalmak kiváltsága, hiszen kis államok is rendelkeznek komoly és bizalomerősítő védelmi és biztonsági rendszerekkel, elég csak példaként állítani Svájcot vagy az ázsiai térségből Szingapúrt, méghozzá a biztonság meglehetősen tág értelmezési horizontjával és az ehhez illeszkedő komplex védelmi rendszerrel párosítva. Ha kifejezetten a digitalizáció és a biztonság horizontját szemléljük, akkor európai viszonylatban – igaz egy rendkívül széleskörű és kártékony információs támadáshullám következményeként, de – Észtország egyértelműen mintaállamként emelhető ki, méghozzá nem csak a biztonság, hanem az állami működés digitalizációja és az állami-társadalmi kooperáció tekintetében is.

Másodszor azt is hangsúlyozni kell, hogy minden jól strukturált és felkészült védelmi szervezet számára alapvető fontosságú a szabályozottság, vagyis ami a jogállam oldaláról egy optimális szabályozás esetén garancia, az a feladatellátás oldaláról hatékonysági előfeltétel. Előre meghatározott protokollok nélkül ugyanis nincs hierarchia, nincs parancsuralmi rendszer, vagyis nem építhető fel a vezetés és irányítás rendszere a hagyományos védelmi és biztonsági arhitektúrákban. Megfelelő szabályozás nélkül nem tervezhető a konkrét feladatellátás, hiszen a feladatrendszer megfelelő strukturálása, majd meghatározása és számonkérése is szabályozáson alapul. Végső soron pedig a hatékony szabályozás nélkül az erők felkészítése sem realizálható, hiszen annak előfeltétele a megfelelően meghatározott és adott esetekben követendő működési rend, ami végső, megismerhető és megkövetelhető formáját – a szóban forgó rendszerek összetettsége folytán – csak a szabályozásban tudja felölteni. Úgy is mondhatjuk tehát, hogy jó és hatékony védelmi rendszer csak a jól és korszerűen szabályozott védelmi rendszer lehet. Ebből következően a hiányos, idejétmúlt, inkonzisztens szabályozás közvetlenül képes negatív visszahatást kifejteni a védelmi erők hatékonyságára, ezzel pedig az egyéni és társadalmi szintű biztonságra is.

Ez a törvényszerűség azonban nem jogi eredetű, hiszen a védelem történelmileg vett intézményi bázisát jelentő haderők szabályozása a modern értelemben vett jogi szabályozást megelőzte, és egészen a polgári (jog)államiság kibontakozásig jellemzően a törvényi szabályozási szint alatt teljesedett ki. Ez azonban nem jelentett a funkciók szempontjából alulszabályozottságot. A szabályozás fontossága, fundamentális jelentősége ugyanis a védelem szervezésének természetéből fakad. Ezt jól tükrözi az is, hogy a hadtudomány egyik sarokpontját a hadtörténelem, annak részeként pedig a hadseregek és védelmi rendszerek szervezésének és szabályozásának, irányításának elemzése adta, amire különösen a kimagasló elvi összegzések, vagyis a törvényszerűséget adó gondolkodók munkásságának elemzése terén a hadelmélet és a témához

kapcsolódó társtudományos elemzések sora[549] is építkezett. Ez pedig egy olyan tradíció a védelem történelmileg sokáig domináns katonai dimenziójában, amelyet aztán a maga sajátosságai szerint, de szemléletében a rendészettudomány, majd a nemzetbiztonsági funkciókkal foglalkozó kutatások is így-úgy átvettek. Nem véletlen az sem, hogy a nemzetközi szakirodalomban is dinamikusan gyarapodnak azok a művek, amelyek a kibertér és az információs korszak védelmi és biztonsági vonatkozásainak átfogó, szisztematikus megközelítésére, feldolgozására törekednek, egyidejűleg pedig javaslatokat, mintákat nyújtanak e területek fejlesztése számára. Ezt a tendenciát a nemzeti törekvések mellett az Európai Unió és a NATO is erősíti, mind szabályozási, mind szakpolitikai és iránymutatási szinten, ahogy erre már korábban kitértünk. A NATO esetében külön kiemelendő az is, hogy a védelmi szférára történelmileg jellemző szisztematikusságot a kutatás, elemzés, gyakorlás viszonylatában is jelentős kapacitásokkal képviseli a Tallinnben működő NATO Cooperative Cyber Defence Centre of Excellence széleskörű kutatási és ajánlás-kidolgozó, illetve gyakorlatszervező tevékenysége révén.

A szabályozás fundamentális szerepe a védelem viszonylatában tehát magából a védelem szervezettség-igényéből, azaz belső természetéből fakad. E tekintetben tehát az, hogy a 17–19. századi Európában a védelmi rendszerek és hadseregek fejlesztésének egyik fő lenyomatát a szabályozás adta a katonai rendtartásokkal, nem elsősorban az állam és a szabályozás fejlődéséből, hanem a hadseregszervezés és az ezt segítő tudományok hagyományaiból következett. Innen nézve tehát az, hogy a polgári (jog)állam kialakulásával a haderők és a honvédelem szabályozása is egyre jelentősebb jogi kereteket, törvényi megalapozást kapott, az egyik oldalról nem újszerű jelenség, másik oldalról pedig – optimális jogalkotás és ezt támogató jogi szakmai apparátus mellett – nem azt jelenti, hogy a jog megszorította volna a szabályozással a védelmi rendszereket, hanem azt, hogy a haderőszervezés szabályozási-igénye a jogállamiság fejlődésével szintézisre lépve alkotott megfelelő szintű szabályokat. Ennek hazánkban kiváló példáját adta a 19–20. század fordulóján végbemenő, több lépcsős honvédelem szabályozási fejlesztési folyamat,[550] melyből ilyen-olyan módon, de a rendészet fejlődése, majd a nemzetbiztonsági funkciók önállósodási folyamata, majd később szabályozása is táplálkozott, még ha hazánk hányattatott történelme miatt a törvényi szintű szabályozás terén jóval később is.

Harmadszor, a 21. századi biztonsági környezetben az úgynevezett lawfare,[551] vagy ha úgy tetszik a joggal való hadviselés,[552] stratégiai befolyásolás eszközként történő használata az állami és nem állami szereplők által komoly jogállami és egyben biztonsági kihívás is egyben. Ez a jelenség nem tekinthető újkeletűnek, de stratégiai szintű eszközzé és könnyebben előkészíthetővé a jogforrások digitalizációjával és online elérhetőségével vált. Kiaknázhatóságának jó példáit adták az elmúlt évtizedekben különösen a drónhadviselés és az önvédelem kiterjesztésének jogi kérdései,[553] valamint a hibrid fenyegetések körében generált jogi viták.[554]

549 Példaként l. Szendy (2017): 106–129., Forgács (2020), Forgács (2017), Bellamy (2016)

550 Vö. Farkas Ádám (2019), Farkas Ádám (2018d): 31–57., Kelemen (2017c): 203–210.

551 Dunlap (2011), Bachmann–Mosquera (2015): 25–28., Ansah (2010): 87–119., Kearney (2010): 79–129., Sari (2019), Sari (2017)

552 A téma hazai megközelítése kapcsán l. Hódos (2020): 49–64., Hódos (2021a): 134–149., Petruska (2022a), Petruska (2022b), Petruska (2022c), Petruska (2021): 97–106.

553 A téma kapcsán l. Hasian (2016), Spitzer (2018.): 101–146., Spitzer (2020a): 172–190., Spitzer (2019a), Kis (2018a): 70–82., Kis (2018b): 16–29.

554 Sari (2018), Sari (2019), Hódos (2020): 49–64., Vikman (2021a): 44–56., Farkas–Resperger (2020): 132–149., Farkas Ádám (2020a): 11–23., Kelemen (2021a): 1–17.

A megismerhetőség mellett fontos azonban kiemelni, hogy a kibertér eleve komoly kihívást jelent azáltal, hogy a jogi szabályok miként és milyen hatékonysággal alkalmazhatók az ott történtekre, miközben az információs tér rendkívüli mértékben tudja fokozni a jogi keretek hiányosságaira, sérülkenységeire építkező befolyásoló-destabilizáló kampányok hatékonyságát, hiszen általa sokkal könnyebben elérhetők ma a társadalmi szereplők, mint a történelemben korábban bármikor. A lawfare és a jogi sérülékenység kérdése a kibertér viszonylatában külön is fokozott figyelmet érdemel, aminek megalapozásához célszerű e témát is áttekinteni.

Orde F. Kittrie a témakörről írt munkájában a fogalom felütéseként tekint ki arra a közkézen forgó véleményre, amely a lawfare fogalmát Charles Dunlap Jr. 2001-es munkájához köti, másik oldalról azonban a jog háborús eszközként való alkalmazását Grotiusig vezeti vissza. Kitér arra is, hogy az ezredfordulón – tegyük hozzá, a Geraszimov-doktrínát jóval megelőzően – publikált kínai „korlátok nélküli hadviselés" koncepcióban is megjelenik már a jog stratégiai eszközként való alkalmazása,[555] illetve ezt megelőzően is különféle megvilágításokban. Orde F. Kittrie értékes elemzése azonban a lawfare fogalom szemantikai eredetére, vagyis a law (jog/törvény) és a warfare (hadviselés) kombinálására építve a háborús/katonai szemléletre építkezik, és ennek adja sajátos és tanulmányozást érdemlő tipológiáját, majd esettanulmányait is. E megközelítés azonban a katonai stratégiához kapcsolja a jog eszközként való használatát, amit tipológiája is tükröz, hiszen egyrészről a katonai erőt kiváltó/pótló/helyettesítő hatású és célú eszközként tekint a lawfare-re, másrészről pedig a harci cselekményekkel összefüggésben nyomásgyakorlásra szolgáló eszközként a jogi keretek – jellemzően a hadijog – megsértésének publikálása, propagálása révén.[556]

A biztonság komplexitása és a hibrid hadviselésben új, 21. századi alakot öltő átfogó nyomásgyakorlás-befolyásolás-támadás különféle állami és nem állami módozatai miatt azonban fontosnak tartom idehaza részletesebb elemzés tárgyává is tenni[557] azt a gondolatot, hogy a jogi szabályozásban rejlő biztonsági relevanciájú hézagok, hiányosságok, ellentmondások vagy konzisztenciazavarok nem csupán a konkrét szembenállás időszakában, illetve a katonai stratégai térben jelenthetnek rendkívüli kockázatot, hanem a komplex biztonság tágabb, nem fegyveres szférák sokaságára kiterjedő keretrendszerben is. Amellett tehát, hogy a katonai stratégiai vonatkozásokban a lawfare kérdését továbbra is komoly elemzések tárgyává kell tenni mind jogi, mind katonai vonatkozásaiban, fontos lenne, hogy a jogi sérülékenységek mint biztonsági kockázatok értelmezését is elmélyítsük.

E tekintetben azt is láttatni kell, hogy a jogi szabályozás hibáinak biztonsági kockázatként való azonosítása tekintetében nem lehet „szűken" a védelmi és biztonsági funkciók szabályozására fókuszálni, hanem tágan kell értelmezni mindezt, kitérve a különféle stratégiai szabályozási területek biztonsági vonatkozásaira is. Alapvető fontosságú tehát, hogy egy állam védelmi és biztonsági funkcióinak szabályozása koherens, korszerű és hatékony legyen, de emellett éppilyen fontos a közlekedési, a kommunikációs, a pénzpiaci, az élelmiszerbiztonsági, a gyógyszerbiztonsági, az adatvédelmi, az információbiztonsági vagy épp a migrációs szabályozás biztonsági réseinek azonosítása, elemzése és korrigálása. A hibás szabályozás ugyanis adott esetben külső beavatkozás előzetes előkészítésének, azaz egyfajta beszivárgásnak, is terepet adhat. Ehhez a fedést gazdasági ügyletek, szervezett bűnözői fellépés vagy épp az ország-

555 L. Kittrie (2016): 4–8.
556 L. uo., 11–24.
557 L. Sari (2017)

gon belüli könnyebb letelepedési vagy akár civil szerveződési lehetőségek is adhatják. Ezek miatt tehát érdemes a lawfare – mint a jog és hadviselés angol megfelelőiből képzett, ezért gondolatilag hadviselés-kötött – fogalma helyett inkább a jogi reziliencia/a jog rezilienciája kérdéskörei felől közelítve a jogi sérülékenység (legal vulnerability) vagy a jog mint biztonsági sérülékenység (law as security vulnerability) gondolatkör felé haladni a jövőben.

A fogalmi kérdésektől visszatérve a védelmi és biztonsági szabályozás korszerűségének és hatékonyságának fontosságához, látni kell, hogy az állam működése belső és nemzetközi viszonyaiban is rendkívül széles körben szabályozott, és ez a joganyag nyilvánosan megismerhető. Ez egyik oldalról a jogérvényesülést és a jogbiztonságot szolgálja, másik oldalról azonban lehetőséget teremt arra is, hogy ha a szabályaink nem megfelelőek, akkor a konkrét védelmi intézkedések a szabályozás oldaláról nyilvánosan megkérdőjelezhetők legyenek. Egy avítt szabályozás melletti konkrét védelmi intézkedés tehát mind a hazai, mind pedig a nemzetközi közvélemény viszonylatában destabilizálhatóvá válik, amihez a világháló kiváló terepet ad a lakossághoz való közvetlen hozzáférés révén. Erre a jelenségre számos példát láthattunk kibertámadások, célzott dróncsapások, a Krím-félsziget elcsatolása, vagy épp egyes tengeri területeket érintő távol-keleti viták vonatkozásában.

E három megközelítést együtt szemlélve tehát a jogi szabályozás szerepe a biztonság fenntartásában és megerősítésében, ennek részeként pedig a védelmi funkciók ellátásában kulcsfontosságú, és korszerűen akkor elemezhető, fejleszthető és alkalmazható, ha abban a biztonsági és védelmi szakértelem, a biztonsági és védelmi kérdésekre szakosodott jogászok, a tág értelemben vett jogász társadalom, illetve e hármasra támaszkodva a társadalom és a politikai is felismeri a hiányosságokat, majd a szükséges és arányos cselekvési irányokat. Ebben a kibertérnek és az információs korszak sajátosságainak kiemelt jelentősége van, mivel egyik oldalról új és kiterjedt cselekvései területet nyitnak meg, másik oldalról azonban dinamikájukkal és a fizikai valóságra – és annak viszonyaira – visszaható képességükkel fel is erősítik azt a kényszert, amely az államokra és társadalmakra nehezedik a korszerű védelmi és biztonsági szisztéma és kooperáció kialakítása terén.

2. A védelmi és biztonsági szabályozás modelljei

A 21. század innovációja rendkívüli tempóban alakítja át a mindennapokat, a gazdaságot, a politikát és vele értelemszerűen a biztonságot és annak fenntartását, megóvását is. E hatástérből a honvédelem, sőt még tágabban az állam védelmi és biztonsági rendszere sem kivétel, sőt. Ahogy az előző fejezetben rögzítettük, a jogállami működést determináló szabályozás szerepe szükségképpen jelentős a 21. századi biztonsági környezethez való alkalmazkodás tekintetében, és ezt csak tovább erősíti az reagálási kényszer, ami az információs technológiák rohamos fejlődéséből és terjedéséből következik.

Látni kell azonban azt is, hogy a védelem és biztonság-szavatolás terén Európa-szerte tapasztalható felzárkózási és fejlődési kényszer régre nyúló és egymást metsző történelmi folyamatok sorába kell, hogy beágyazódjon. A változó társadalmi, politikai-kulturális, gazdasági és geopolitikai környezet mellett a jelenleg több európai államban zajló biztonsági és védelmi reformok, fejlesztési programok a védelmi és biztonsági szisztéma fejlődési sajátosságaira is rá kell, hogy épüljenek. E tekintetben természetesen minden nemzeti rendszer épp annyira sajátos, amennyire egyedi a történelmi-kulturális fejlődése, azonban tendenciák, nagybani osz-

tályozások mégis felvázolhatók arra nézve, hogy milyen megközelítések szerint alakulnak a védelmi és biztonsági rendszerek. Ezen csoportosítások szerepe nem csak az értékelhető minták adaptációs lehetőségeinek felmérése miatt fontos, hanem azért is, mert szemléleti oldalról segíthetnek azonosítani olyan megoldási sémákat, amelyekkel különféle államok a komplex biztonság jelentette kihíváshalmazt igyekeztek kezelni, és amely megoldások absztrakt módon a NATO szintjére is felkerültek az átfogó megközelítés, majd a reziliencia szemléletével.

2.1. Az európai katonai jogi rendszerek osztályozása mint szemléleti alap a komplex védelem-értelmezéshez

Figyelemmel arra, hogy a huszadik század első feléig a biztonságfelfogást a transzatlanti térségben a katonai dominancia jellemezte, és csak a század második felében indult meg a komplex biztonsági szemlélet kibontakozása– lényegében máig tart az államoknak az ehhez való intézményi és szabályozási alkalmazkodása –, nem ördögtől való a klasszifikáció során előzményként tekinteni a katonai jogi szabályozások európai modellezésére.

E tekintetben Georg Nolte meghatározó jelentőségű összehasonlító munkáját érdemes alapul venni, amely 2003-ban jelent meg és egy 2000-ben a német védelmi minisztérium által megrendelt elemzés főbb eredményeit adta közre az európai katonai jogi rendszerek összehasonlítására vállalkozva. A tanulmány megrendelésének időszaka egyértelműen egybeesik a védelmi képességek európai újragondolásának időszakával, ami a legtöbb államban racionalizálást, sok esetben képességcsökkentést is eredményezett. Utóbbi mögött azonban elsősorban anyagi és politikai megfontolások álltak, amelyek mellett minden állam érzékelte a biztonsági környezet és a technológiai közeg változásait, valamint azt, hogy ehhez az államnak és az állam védelmi alrendszereinek is alkalmazkodnia kell. Erre figyelemmel, a katonai fókusz ellenére is, fontos tehát Nolte munkáját a komplex biztonsághoz való viszonyulás állami és jogi reagálása terén figyelembe venni, különös tekintettel arra, hogy Németország történelmi múltját is e téren meglehetős kettősség jellemzi, ami mellett azonban az ország mérete és pozíciója a teljeskörű pacifizmust és semlegességet nem tette lehetővé.

Nolte a változó közeghez igazodva az európai államok katonai szabályozásainak osztályozása során is törekedett a komplex megközelítésre, ezért a hangsúlyt a (1) hatalmi ágak szétválasztása és államszervezet, (2) az egyenruhás állampolgár modell, (3) az alapvető jogok kérdése, (4) a katonai szolgálat, (5) a parancsnoklás hatalma és az utasításoknak való engedelmesség, (6) a szolgálati idő, kompenzáció a túlszolgáltért és eltávozás, (7) a közigazgatási felülvizsgálat joga, (8) az intézményesített képviselet joga, (8) a fegyelmi jog, (9) a katonai büntetőjog, valamint (10) az őr- és figyelő szolgálatok[558] szabályainak elemzése mentén határozta meg. Ezen kulcstémakörök révén ugyanis Nolte úgy vélte – meglátásunk szerint helyesen –, hogy messze nem csak, sőt talán nem is elsősorban a konkrét katonai szabályozások osztályozása történhet meg, hanem a sajátos katonai viszonyrendszerek jog- és államrendszer egészéhez, ezáltal pedig a társadalmi berendezkedéshez való viszonyulásának az osztályozása, ami már egy komplex strukturális megközelítés lehetőségét is magában rejtette.

Az egyes államok konkrét szabályozásának vizsgálata előtt azonban Nolte történeti kitekintést is tett, aminek bázisát a demokratikus tradíciók adták az összehasonlítás terén, vagyis

558 L. Nolte (2003): 1–17.

az egyes államok katonai jogát aszerint osztályozta, hogy az adott állam milyen jellegű és mélységű demokratikus tradíciókkal rendelkezik. Ennek oka alapvetően az, hogy a katonai – és egyébként tágabban a védelmi és biztonsági – intézmény- és szabályrendszer állami- és társadalmi beágyazottságát, jellegét és korszerűségét nagyban meghatározzák az adott állam történelmi előzményei, alapjai. Ott, ahol a vizsgálatot megelőző évszázad jelentős részében autoriter vagy diktatórikus berendezkedés volt, jellegében rendkívül eltérő – előbb domináns és corpus separatum státuszt öltő, utóbb perifériára sodródott – képet mutatott a védelmi architektúra. Míg ott, ahol részben-egészben demokratikus alapokon nyugodott a fejlődés, a védelmi és biztonsági rendszer jobban szinkronba tudott kerülni az állam és a társadalom „civil" fejlődésével. Ebben az osztályozási sémában Nolte csekély,[559] illetve jelentős[560] demokratikus tradíciójú, valamint poszt-autoriter[561] demokráciákat különböztet meg. Ennek hazánk, és a fegyveres védelem tekintetében lényegében még előttünk álló állam- és jogtudományi szemléletváltás tekintetében azért is van kiemelt fontossága, mert ez a klasszifikálás egyértelműen tükrözi a totalitarizmus-tapasztalat hatását mind a szabályozások, mind a védelmi és biztonsági szisztéma szerepfelfogása tekintetében. Amíg ugyanis a Nolte által is azonosított történelmi nehezékeket nem tudjuk magunk mögött hagyni mind az állami szemléletmód és a védelmi intézményeket jellemző gondolkodás, mind pedig a „civil" tudományos, szakmai és társadalmi gondolkodás terén, addig nehezen képzelhető el egy olyan tartalmilag is szisztematikusan megvalósuló fejlődési-fejlesztési folyamat,[562] amelynek talaján versenyképes, korszerű és társadalmilag is elfogadott és hasznosuló védelmi szisztémával kezdhetünk neki az információs korszak kihívás-kezelésének.

Természetesen ki kell emelni, hogy Nolte demokrácia-fókuszú elemzése ízig-vérig 20. századi és ezért bizonyos szempontból a védelmi funkciók sajátosságait háttérbe sorolta a hidegháború lezárása utáni demokrácia terjedést támogatása jegyében. Emiatt ma már nem tekinthető teljességgel reprezentatív elemzésnek az eltelt negyed évszázadra és a hagyományos demokráciák körében kialakult különféle hatalmi-védelmi kapcsolódású aggályos eseményekre figyelemmel. Mindemellett azonban vitán felül áll, hogy Nolte összehasonlító munkájában olyan komplex elemzésre törekedett, amely a fentieken túl a fegyveres erő alkalmazásának alapvető szabályaira, a demokratikus kontrollra, a műveletek szabályozására – beleértve a kivételes vagy minősített helyzeteket –, az alkotmányos hatalom-megosztás védelmi kérdéseire, a fegyveres erők struktúrájára, valamint az egyes szolgálati és alapjogi kérdésekre is kiterjedt.[563] Ez a megközelítés egyik oldalról alapot adhat újabb hasonló elemzések korrekciókkal történő elvégzéséhez, különösen a kibertérben, illetőleg az információs térben történő védelmi szerepvállalás jövőjének komplex elemzéséhez. Másik oldalról azonban Nolte azon megközelítése, amellyel a katonai jogi vonatkozásokon keresztül egy komplex állam- és jogrendszeri kapcsolódási hálózat megvalósulási formáinak osztályozása felé mozdult el, egyértelműen alapot ad a komplex biztonsághoz igazodó modellek klasszifikálásának előzetes felvázolásához. Ahhoz ugyanis, hogy az információs korszak biztonsági környezetének intézményi és jogi vonatkozásait megfelelően tudjuk értelmezni, át kell látni azt is, hogy milyen

559 Nolte (2003): 24–25.
560 Uo., 25–26.
561 Uo., 26–29.
562 Farkas Ádám (2021f): 37–52.
563 L. Nolte (2003): 23–182.

fogalmi és szemléleti keretben jelennek meg a szóban forgó konkrét intézmények és szabályok, illetve, hogy milyen is az az értelmezési séma, amelyhez a komplex biztonságból adódóan számos hagyományosan nem védelmi és biztonsági szférát valamilyen módon kapcsolni kellene a jövőben annak érdekében, hogy azok szektorális biztonsága is szavatolható legyen.

2.2. Az angolszász nemzetbiztonság-felfogás jelentősége a transzatlanti térségben

A transzatlanti térség államainak védelmi és biztonsági működését jelentős mértékben meghatározzák a NATO törekvései, a NATO fejlődési irányait pedig az Amerikai Egyesült Államokból származó komplex biztonsági megközelítés. Erre tekintettel szükségesnek mutatkozik a komplex biztonsághoz igazodó védelmi és biztonsági rendszer értelmezése terén az amerikai megközelítést részleteiben is áttekinteni. Ez a megközelítés a NATO-ban mintaértékűnek mondható jellege mellett a cyberfare state amerikai vonatkozásaira tekintettel a kibertér és a nemzeti biztonság relációjában is releváns.

A 20. század vége és a 21. század első két évtizede egyértelműen megerősíti azt a tendenciát, hogy a társadalmak és az államok biztonsága szempontjából egyre növekvő jelentőségre tesz szert a nemzetbiztonsági szféra. Ahogy már többször hangsúlyoztuk, az információs korszak dinamikus fejlődése számtalan technikai újítás, ezáltal gazdasági erősödés, ezzel pedig jóléti előrelépés alapja, azonban másik oldalról ezek a lehetőségek kihívásokat is jelentenek, hiszen azok mind egyéni, mind magasabb szinten szervezett visszaélésekre is hasznosíthatók, méghozzá titokban, leplezett módon és széles eszkalációs skálán mozogva, akár a nemzetbiztonság egészére kiterjedően. Ez utóbbit kifejezetten a kibertér vonatkozásában jól példázta az az összetett és a kibertérre jelentős mértékben építő behatási folyamat, amely 2007-ben Észtországot érte, és amelynek hatására Észtország azóta a kiberbiztonság és a biztonságos digitalizáció egyik úttörőjének számít. Ahhoz azonban, hogy helyesen tudjuk ezt a másik osztályozási és értelmezési irányt követni, szükségszerű először a nemzetbiztonság fogalmát az államrendszer, illetve az ellátandó funkciók jogrendszeri kapcsolódásai felől közelítve is értelmezni. A nemzetbiztonság fogalma esetében ugyanis az általános képzetek furcsa viszonyt mutatnak a témakör mélyebb elemzésének eredményeivel, mivel e fogalomhoz tulajdonképpen legalább két jelentéstartalmat társíthatunk a köznapi/politikai diskurzust figyelve. Ebben a terminusban ugyanis vegyülni látszik egy szervezetszintű/funkcionális és egy összkormányzati/rendszerszintű jelentéstartalom. Egyszerűbben fogalmazva, a nemzetbiztonság fogalmának használata során megjelenhet a köznapi értelemben vett titkosszolgálatok jelensége, illetve a nemzet biztonságának komplex jelenségegyüttese, melyet e kifejezéssel – például a 2022-es kormányalakítást követően Védelmi Tanáccsá átkeresztelt és -alakított magyar Nemzetbiztonsági Kabinet elnevezésében, vagy az USA nemzetbiztonsági törvényében[564] – egyfajta ernyőfogalomként, egy számos-számtalan funkciót egyesítő szisztéma leírására alkalmazunk. Ezt a fogalmi kettősséget jól tükrözi a köznapi/politikai tematizálás mellett a szakirodalom is, hiszen akár a konkrét nemzetbiztonsági szolgálatok nemzetközi áttekintésére[565] irányuló

564 National Security Act 1947.
565 Béres (2018b)

munkáról, akár a hazai nemzetbiztonsági funkció egyes szakkönyveiről[566] beszélünk, mindkét jelentéstartalom megtalálható.

A nemzetbiztonság fogalmához tehát legalább két értelmezési dimenziót párosíthatunk. E kettősség érdekessége az, hogy azok között jelentékeny kapcsolat, hovatovább rész-egész viszony áll fenn, aminek az eredője a 20. század forgatagaiban és az államszervezet ugrásszerű fejlődésében ragadható meg. A fogalmi kettősség kiindulópontja ugyanis egyik oldalról az, hogy a nemzetbiztonsági tevékenység – mint funkció, és az azt realizáló szervezetek összessége – a transzatlanti térség számos országában jelentős önállóságra és egyfajta ágazati elkülönülésre a múlt század technológiai, társadalmi és politikai változásai során tett szert. Ez az önállósodás azonban van, ahol egybeesett a totalitárius tapasztalatokkal, másutt pedig a totalitarizmus elleni erőteljes harc követelményeivel. Az előbbi esetben tehát a nemzetbiztonság fogalmával kellett felváltani azokat a meghatározásokat, elnevezéseket, amelyek a 20. században váltak bevetté, de kompromittálódtak[567] a totalitárius hatalomgyakorlással összefüggésben. Az utóbbi esetben pedig a nemzetbiztonság fogalmát kellett egy olyan gyűjtőfogalomként használni, amivel tükrözhető, hogy a szembenálló totalitárius ellenség a nemzet biztonságának bármely szektorában megjelenhet, ezért a fellépésnek is komplexnek, a nemzet biztonságának egészén átívelőnek kell lennie. Másik oldalról azonban ez az időszak egybeesik a biztonság fogalmának megváltozásával is, amely a korábban katonailag determinált biztonságfelfogásból egy komplex, a nemzet egészének differenciált viszonyaira kiterjedő biztonságszemlélet felé mozdult el, ezért a katonai megfogalmazások helyett önálló és átfogó megközelítést tükröző elnevezésre volt szükség.

A konkrét elnevezések bűvöletén túlhaladva azonban érdemes ezt a kettősséget előzetesen is átgondolni. Egyik oldalról a nemzetbiztonság a politikai-kormányzati szinten a legtágabb értelemben vett védelmi és biztonsági politikát, döntéshozatalt öleli fel, ahogy erre a következőkben kitérek. Ez tehát a legtágabb ernyőfogalomként értelmezendő, amelybe beleértendők olyan „civil" – tehát nem a védelmi és biztonsági szférákba tartozó – állami funkciók és viszonyrendszerek is, amelyek a biztonságban való sajátos szerepük és súlyuk miatt fokozott figyelmet kell, hogy kapjanak a biztonság tervezése, szervezése, szavatolása tekintetében. Másik oldalról azonban érdemes felhívni arra is a figyelmet, hogy a nemzetbiztonsági jelző szervezeti szinten való paralel megjelenéséből levonható az a következtetés, hogy az érintett szolgálatokat a jogalkotó olyanként hozta létre, amely a maga speciális eljárásaival, eszközeivel és módszereivel a nemzet és az állam biztonságának legszélesebb viszonyrendszerében hivatott ellátni a szolgálatát.

Meglátásom szerint tehát a szervezeti (mikro-) és a kormányzati (makro-) szintek nemzetbiztonsági fogalmait nem indokolt egymástól teljesen elkülönítve értelmezni, még ha az egyébként esetenként értelemzavaró is lehet, hogy egy adott szövegkörnyezetben a két szintet együtt kell megjeleníteni. A két eltérő szint fogalmi parkjának párhuzamosságát tehát úgy is felfoghatjuk, hogy azok a két szint közti kapcsolatot tükrözik, vagyis azt, hogy a makro-

566 Vö. Dobák (2014), Resperger (2018b), Resperger (2018c)

567 Típusosan ilyen Magyarországon az államvédelem, állambiztonság fogalma az Államvédelmi Hatóság, illetve a BM III. – állambiztonsági – főcsoportfőnökség öröksége, német területen pedig a biztonsági szolgálat (Sicherheitsdienst, röviden SD) vagy épp az államrendőrség (Geheime Staatspolizei, röviden Gestapo) elnevezés a náci örökség miatt, ami mellett az elnevezések politikai rendszerváltásokhoz való igazodására akár Oroszország esetében is fel lehet hívni a figyelmet (a GRU GU-vá alakulása, vagy a KGB nyomán létrejövő FSZB és SZVR tekintetében).

szinten megjelenő széles spektrumú biztonság-felfogás és „kezelés" szervezeti-funkcionális szinten történő leképeződése mutatkozik meg a fogalmi kettősségből.

A fogalom egyik – funkcionális – dimenziója tehát a szervezeti szint, ha úgy tetszik a titkosszolgálati[568] szféra, amelynek szervezeteit a 20. század önállósodási folyamatai óta számos államban,[569] és így a rendszerváltást követően[570] hazánkban is *nemzetbiztonsági szolgálatok* elnevezéssel illetik. Kiemelendő persze, hogy a nemzetbiztonsági jelző mellett számos államban meghatározó a hírszerző, az információs, a védelmi, a biztonsági vagy épp az államvédelmi jelző is. Ez a dimenzió az állam rendszerében mikroszintként is megfogható, hiszen az adott szervezetre való vonatkozással a legkisebb önálló strukturális elemet helyezi a fogalom középpontjába.

Erről a dimenzióról már elöljáróban érdemes rögzíteni, hogy hazánk gyakorlatától eltérően a nemzetbiztonsági szolgálatok elnevezés nem mindenhol jelent gyűjtőfogalmi jelleget a terminológiában. Azt is mondhatnánk, hogy Magyarországon a gyűjtőfogalmi jelleg inkább a jogalkotók történelmi-politikai reakciójának eredménye az 1989 előtti pártállami időszakra nézve, amelynek e körbe tartozó szervezeteit összefoglalóan állambiztonsági szerveknek vagy állambiztonsági szolgálatoknak nevezték. A szervezeti szint fogalmi megközelítése a transzatlanti térségben ettől eltérő képet mutat, amelyben a hírszerző, a biztonsági, illetve az információs jelzők tekinthetők a legjellemzőbbnek a szervezetek elnevezéseiben.

Részint az elnevezések, de még inkább a mikro-, azaz szervezeti szint jellemzően a nemzetbiztonsági feladatösszesség egy-egy csoportjának szervezésére, ellátási struktúrájára irányítja rá a figyelmet, hiszen a szervezet jellege, feladatrendszere és alárendeltsége szükségképpen tükrözi az általa ellátott fő funkciókat. A mikroszint szisztematikus áttekintése és elemzése tehát – a feladatellátás konkrétumainak ismerete nélkül is – alkalmas lehet arra, hogy megmutassa egy adott állam mit ért bele – a látható, jogi térben – a nemzetbiztonsági működésbe.

A mikroszint másik fontos visszatükröződését az egyes szervezetek profiljai adják, hiszen az adott állam viszonyainak, szemléletének, biztonságfelfogásának egyik lenyomatát jelenti, hogy a nemzetbiztonság mikroszintjén megjelenő szolgálatai milyen portfóliót képviselnek. Az, hogy egy államban méreteihez és geopolitikai potenciáljához mérten hány szolgálat és milyen profil-megosztással van, egyértelműen utal arra, hogy milyen az adott államban a hatalommegosztás rendszere, a nemzetbiztonsági funkciókkal szembeni kormányzati/

568 Már az jelzés értékű, hogy Magyarországon a titkosszolgálatok fogalmat „szakszerűtlennek" tekintjük arra hivatkozással, hogy a rendszerváltást követő jogalkotás nemzetbiztonsági szolgálatokká nevezte át ezen szerveinket. A szakmai diskurzus és annak a közérthetősége kapcsán érdemes lenne azonban mérlegelni a titkosszolgálati jelző rehabilitálását, példának okáért arra figyelemmel, hogy azt a nemzetközi szakirodalom is meglehetősen széles körben és elfogadottan használja, azaz eltérve a magyar történelmi tapasztalásoktól és traumáktól, nem társít hozzá általánosan pejoratív jelentéstartalmat. Emellett pedig hazai viszonylatban is fajsúlyos érvként hívható fel, hogy Magyarország Alaptörvénye a 46. cikkben jelenleg is használja a titkosszolgálati jelzőt.

569 Példa lehet erre az amerikai Nemzetbiztonsági Ügynökség (National Security Agency), a szlovák Nemzeti Biztonsági Hivatal (Národný bezpečnostný úrad), a bolgár Állami Nemzetbiztonsági Ügynökség (Държавна агенция „Национална сигурност), a montenegrói Nemzetbiztonsági Ügynökség (Agencija za Nacionalnu Bezbjednost), norvég Nemzetbiztonsági Hatóság (Nasjonal sikkerhetsmyndighet), az Örmény Köztársaság Kormányának Nemzetbiztonsági Szolgálata (Հայաստանի Ազգային Անվտանգության Ծառայություն), a spanyol Nemzetbiztonsági Hivatal (Departamento de Seguridad Nacional) vagy a svéd Polgári Nemzetbiztonsági Szolgálat (Sakerhetspolisen).

570 A gyűjtőfogalmi jelleget Magyarország Alaptörvényének 46. cikke, valamint a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény is egyértelműen jelzi, de ez visszatükröződik egyes szervezetek elnevezéséből is, így például a Nemzetbiztonsági Szakszolgálatéból, valamint a Katonai Nemzetbiztonsági Szolgálatéból.

törvényhozási/társadalmi bizalom, illetve, hogy a szolgálatok irányítását végző kormányzaton belül milyen erőközpontok, súlypontok léteznek. Másik oldalról ez a dimenzió azt is tükrözi, hogy az adott állam hozzávetőleg mekkora erőforrás-megoszlással, funkcionális részletezettséggel tekint a nemzetbiztonsági vonatkozásokra. Ez persze viszonylagos államismérvként értelmezendő, hiszen nincs törvényszerűség arra nézve, hogy mekkora államméretnek, illetve hatalmi potenciálhoz hány és milyen megoszlású szolgálat dukál. Az azonban jelzésértékű, hogy az e területen meghatározónak, jelentősnek tekinthető szereplők (és nem csak a nagyhatalmak, hogy példaként hozzuk adott esetben Izraelt) általában a heterogén, szakosított szervezeti mátrix felé mozdulnak el a komplex biztonsági környezethez – és ez által a nemzetbiztonság makroszintjéhez is – alkalmazkodva, és nem a minél kisebb számú szolgálati rendszer felé. Ezen a képleten pedig, biztosan állíthatjuk, hogy a kibertér jelentette kihívások sem változtattak, sőt egyik oldalról erősítették az információk leplezett megszerzése/megvédése miatt a titkosszolgálati funkciókat, másik oldalról pedig fokozták az állami szervek közti titkosszolgálati részvételű kooperáció igényét Európa-szerte.[571]

A nemzetbiztonság-fogalom másik – rendszerszintű – dimenziója az összkormányzati, a nemzet biztonságának nagy egészére irányuló döntéshozatallal azonosítható szint, amely fajsúlyosan a fegyveres védelmi funkciók súlyozásával, de a nem fegyveres tényezők sokaságára kiterjedő módon helyezi a döntés-előkészítés és a döntéshozatal homlokterébe a nemzet biztonságának és érdekérvényesítésének szavatolását. Ez a dimenzió az állam rendszerére vetítve makroszintként is megragadható, tehát már nem szakfeladatok és funkciók ellátására, hanem a kormányzás biztonsági tematizáltságára, illetve az állam biztonsági jellegű érdekeinek érvényesítésére rendszerszinten fókuszál.

Ezzel a nemzetbiztonság-fogalom makroszinten egy olyan absztrakt biztonsági szegmenset jelent, amelybe az egyes államok azokat a kihívásokat, fenyegetéseket sorolják, amelyek jelentős és súlyos mértékben tudják aláásni, illetve veszélyeztetni a társadalom rendjét, békéjét, biztonságát, illetve az állam működését, érdekeinek érvényesülését. E körbe elsődlegesen a katonai védelmi, a rendészeti, illetve a titkosszolgálati funkciók/ágazatok kooperációja, szemléletük fuzionálása, illetve működésük felsőszintű koordinációja jelenik meg, azonban fontos azt is kiemelni, hogy számos államban e területeken messze kívül eső, de a társadalmi biztonság szempontjából kulcsfontosságú ágazatok (járványügy, energetika, gyógyszer- és kábítószerügy, infokommunikáció stb.) is megjelennek. Leegyszerűsítő módon azt is mondhatnánk, hogy nemzetbiztonság e makroszintű dimenziója nem más, mint a 20. században kibontakozó komplex biztonság[572] politikai, kormányzati leképezése mind a szemléletmód, mind pedig a döntéselőkészítés és -hozatal tekintetében. Ha a biztonságot – helyesen – egy fokozódó komplexitású, és ez által adott szektor vagy dimenzió dominanciájával le nem írható jelenségként értelmezzük, akkor egyértelműnek és okszerűnek tűnik az a fejlődés, amivel a korábban domináns hadpolitikai, katonapolitikai szemlélet kormányzati jelentőségét egyre inkább az összetettebb és differenciáltabb nemzetbiztonsági politika veszi át. Erről azonban még célszerű jelen időben beszélni, mivel a transzatlanti térségben meglehetősen eltérő fej-

571 A téma kapcsán többek között l. Petruska–Vikman (2021), Vikman (2021c), Vikman (2022b), Spitzer (2021), Farkas Ádám (2021b)

572 Vö. Buzan–Waever–Wilde (2006), Dannreuther (2016), Deák (2009), Deák (2007), Szálkai–Stepper (2015)

lettségi, kiforrottsági, működési szintek tapasztalhatók ezen hangsúlyváltozás, vagy inkább szemléletváltás tekintetében.

A makroszint megközelítését, értelmezését Samuel P. Huntingtonnak a nemzetbiztonsági politikáról adott meghatározása mind a szisztéma és komplexitás, mind pedig a politikai determinációk szempontjából kiválóan tükrözi. Eszerint:

> „A nemzetbiztonsági politika célja az ország társadalmi, gazdasági és politikai intézményei biztonságának erősítése más független országok részéről jelentkező fenyegetésekkel szemben. A nemzetbiztonsági politika elvileg három formában és két szinten létezhet. A katonai biztonsági politika azon tevékenységek programja, amelyet arra terveznek, hogy minimalizálják, vagy semlegesítsék az ország meggyengítésére vagy megsemmisítésére irányuló erőfeszítéseket olyan fegyveres erők részéről, amelyek intézményi vagy területi határain kívül tevékenykednek. A belbiztonsági politika a felforgatás veszélye ellen veszi föl a küzdelmet – vagyis azon erőfeszítés ellen, amely az állam meggyöngítésére vagy megsemmisítésére irányul a területi vagy intézményi határain belül tevékenykedő erők részéről. A helyzeti biztonsági politika az állam viszonylagos erejének csökkentésére irányuló, a társadalmi, gazdasági, demográfiai és politikai viszonyokban bekövetkező hosszú távú változásokból fakadó lemorzsolódás veszélyével foglalkozik. E politika mindhárom formájának van operatív és intézményi szintje. Az operatív politika a biztonsági fenyegetéssel való szembeszállás céljából tett azonnali intézkedésekből áll. Az intézményi politika azzal a móddal foglalkozik, ahogyan megfogalmazzák és megvalósítják az operatív politikát."[573]

Ebből jól látható, hogy már messze szélesebb spektrumot ölel fel a biztonság dimenziói kapcsán, mint a katonai biztonságra fókuszáló korábbi időszakok szemlélete. Konstrukciójában az ágazati jellegű tagoltság (a katonai-belbiztonsági felosztással) még jelen van ugyan, de a helyzeti politikával egy ezeken átívelő, átfogó szemléletmódot is megjelenít, amelyekre aztán ráépíti azt a meggyőződését, hogy mind a nemzetbiztonsági politika mint nagy egész, mind pedig az egyes „rész" politikák tekintetében van azonnali reagálási szint, és van egy stratégiai távlatú, az ő szóhasználatában intézményi szint a megvalósításra.

Kiemelendő ezzel kapcsolatban, hogy Huntington gondolatvilága az 1947-ben megalkotott amerikai nemzetbiztonsági törvény szellemiségét és struktúráját tükrözte, vagyis lényegében tudományos absztrakcióját adta egy már megvalósulásba fordult szemléletváltásnak, amit a hidegháború kibontakozása jelentős részben kényszerített ki. Ebben a rendszerben az éles és bármikor eszkalálódó katonai szembenállás mellett napi szinten volt jelen a hírszerzési háború, a gazdasági versengés, a társadalmi modell-versengés és a társadalompszichológiai beavatkozások lehetősége, egyfajta kulturális és ideológiai feszültség kezelése, továbbá számos más ezekkel összefüggő (jóléti, egészségügyi, innovációs, külpolitikai, oktatási stb.) kérdés, amelyeket komplex módon kellett kezelni. Ehhez értelemszerűen a szembenállás sarokponti területeire, azaz a klasszikusan fegyveres karakterű biztonsági szektorokra épülő, de a komplexitást garantáló rendszert kellett felépíteni a szakmai tanácsadás vonatkozásában is. Ennek tudható be, hogy az Amerikai Egyesült Államok Nemzetbiztonsági Tanácsa rendkívül sokrétű feladatrendszerrel és szakmai összetétellel írható le, ami mellett dinamikusan fejlődtek a különféle biztonsági szektorokkal foglalkozó kutató, elemző think thankek, intézetek, tan-

573 Huntington (1994): 8.

székek az Egyesült Államokban az elmúlt évszázadban. A nemzetbiztonsági politika mint makroszint ugyanis nem csak azt jelenti, hogy az állam különféle területein működő funkcionáriusok álláspontjait kell kanalizálni és szintetizálni valamennyire, hanem azt is, hogy tudáshátteret és a közigazgatási/bürokratikus módszereken túllépő elemzési képességeket is ki kell alakítani a döntéshozatal mögött, majd azokat kapcsolni is kell a döntéshozatalhoz. Ez utóbbi jelentőségét az USA vonatkozásában talán jól szemlélteti, hogy a 20. század két meghatározó külpolitikai alakja, Henry Kissinger és Zbigniew Brzezinski is ebből a háttértudás-teremtésből épült fel és került a Fehér Házba.[574]

Fontos azonban azt is látni, hogy Huntington fogalommeghatározása 1957-ben, tíz évvel a National Security Act megalkotása után, de még jóval az információs és vele a biztonsági „forradalom" azon szakaszai előtt született, amelyek révén ma már információs társadalomról, online globalitásról és egyben a virtuális tereknek való kitettségről beszélhetünk. Korát jól tükrözi még a szembenállás állami szereplőkre szorítása, amihez mérten mára a nem állami szereplők súlya jelentősen felértékelődött a legtöbb új, vagy a globalitás és a technológiafejlődés miatt újszerűnek ható fenyegetés miatt. Mindezek mellett is az mondható azonban, hogy alapvonalaiban ez a modell egy olyan makroszintű rendszert és szemléletmódot alapozott meg, amire méltán építhető fel a multidimenzionális biztonság felfogása és lehetőség szerinti szavatolása. Elgondolkodtató azonban, hogy ha mind az amerikai törvényhozás, mind az annak eredményeit mélyebb kontextusba helyező tudományos gondolkodás a nemzetbiztonsági politika és az azzal összefüggő kormányzati működés tekintetében már a hidegháború elején is egy komplex, koordinált és széleskörű szakmaiságra épített működést igényelt, akkor milyen elvárásokkal, kritériumokkal kell ma szembenézni ezen a területen ahhoz, hogy azt egy állam korszerűnek nevezhesse az információs korszak kihívásai, illetőleg a társadalmi, gazdasági és állami célú digitalizáció fokozódása közepette.

Hogy jobban értsük mindezt: az amerikai szisztéma bázispontja szabályozási szempontból az az 1947-es nemzetbiztonsági törvény,[575] amely a második világháború utáni és azóta többszöri módosítással, de hatályban lévő törvényi keretként már a komplex biztonsághoz igazodott a múlt század első felének végén is és amellett, hogy rendszerszerűen közelítette meg a társadalom és az állam biztonságának megóvása és védelme szempontjából kiemelkedő fontosságú funkciókat és intézményeket, az ezek közti hatékony koordináció és az összehangolt irányítás szempontjából is fajsúlyos lépéseket tett az új korszak követelményeihez való felzárkózás terén.

Az amerikai nemzetbiztonsági törvény által létrehozott rendszer sok szempontból magán viselte az épp letűnőben lévő biztonságfelfogást, melyet a katonai elem dominált. Más szempontból azonban felismerte ennek a dominanciának a háttérbe szorulását és vele számos más tényező, különösen az információ, a hírszerzési hatékonyság – külső és belső – jelentőségét, és azt a tényt, hogy a nemzet biztonságának záloga az, ha a nemzet védelmére hivatott állami funkciók és intézmények koordináltan működnek. Nem véletlen, hogy a törvény első címe a nemzetbiztonság koordinációjára fókuszál,[576] és azon belül – folyamatos gyarapodás mellett, de már a megalkotáskori változat is – megjeleníti a végrehajtó hatalom szintjén a Nemzetbiz-

574 Vö. Gati (2014), Kissinger (2019)
575 L. National Security Act of 1947 dni.gov/index.php/ic-legal-reference-book/national-security-act-of-1947
576 Uo., Title I.

tonsági Tanácsot,[577] a megalkotáskor önállóságában újszerű titkosszolgálati szférában kiemelt feladatot kapó CIA-t,[578] valamint a Nemzetbiztonsági Erőforrás Testületet[579] mint a civil-katonai együttműködés és felkészülés koordinatív testületét. Az eltelt bő fél évszázad során ez a cím rendkívül jelentős fejlődésen, bővülésen ment át,[580] részint a koordináció hatékonyságának fokozása, részint a hírszerző szervezetek számának és funkcióinak gyarapodása, részint pedig garanciális szabályozási elemek beépítése révén, így mára egy sokrétű, de rendszerszerű komplex biztonsági koordinációs keretet ad az Amerikai Egyesült Államok védelmi és biztonsági rendszerének.

Komoly jelentőséggel bír az 1947-es eredeti modellben a védelmi ágazat (Magyarországon: honvédelem) második címben történő szabályozása,[581] ami az angolszász sajátosságok mellett, de úgy gondolom, hogy párhuzamba állítható a hazai honvédelmi szabályozás 1939-es szemléletével,[582] megerősítve azt, hogy a háborús helytállás csak akkor lehet sikeres, ha a felkészülés össztársadalmi, de abban a katonai elem sajátosságai megfelelő nyomatékkal jelennek meg. Úgy is mondhatnánk, hogy a nemzetbiztonsági (hazánkban: védelmi és biztonsági) átfogó megközelítés mellett a katonai védelmi (hazánkban: honvédelmi) szegmens egy sajátos pozíciót foglal el, amely része a nagy halmaznak, de bizonyos szempontból a katonai, és különösen a háborús sajátosságok miatt túlnyúlik azon, és emiatt egyfajta autonómiát, a nagy rendszeren belüli önálló működést szavatolni képes kialakítást élvez. Ezt az értékelést nem csak a katonai védelem kereteinek nemzetbiztonsággal paralel törvényi meghatározása erősíti meg, hanem az is, hogy a második címen belül előbb, vélhetően a háborús tapasztalatok és a korábbi, katonai dominanciájú biztonságfelfogás hatására, olyan közjogilag jelentős entitás is megjelent, mint a War Council,[583] azonban ez később, a National Security Council erősödésével, kikerült a szabályozásból. Jelen kötet szempontjából az is hangsúlyt érdemel, hogy a törvény a katonai védelem kereteiről szóló második részben külön rendelkezett 1947-ben a Kutatási és Fejlesztési Tanácsról,[584] tükrözve ezzel már 1947-ben – költői túlzással a maihoz mért fejlődés és innováció kezdetén –, hogy a külső környezettel való lépéstartás a védelem és biztonság kulcskérdése mind szabályozási, mind pedig intézményi értelemben. Szintén jelen kötet apropóján emelendő ki, hogy mára az amerikai nemzetbiztonsági rendszerben kulcsszerepet játszik a National Security Agency, amely irányítási szempontból a védelmi szféra alá tartozik, vezetője 2010 óta egyben az USA Kiber Parancsnokságának parancsnoka is,[585] de feladatrendszere a komplex biztonsághoz illeszkedik, míg szervezetétől külön, de fizikailag azonos parancsnokságon funkcionál a katonai kiberparancsnokság. Ez a fajta összenemzeti-összkormányzati nemzetbiztonsági szemlélet, és ezen belül a katonai vonatkozások sajátos szerepe tehát az információs korszakban is folyamatos megerősítés alatt áll, természetesen az

577 National Security Act of 1947 – July 26, 1947; Sec. 101. webcache.googleusercontent.com/search?q=cache:n4W7n4lxejoJ:https://global.oup.com/us/companion.websites/9780195385168/resources/chapter10/nsa/nsa.pdf+&cd=13&hl=hu&ct=clnk&gl=hu&client=firefox-b-d

578 Uo., Sec. 102.

579 Uo., Sec. 103.

580 Vö. National Security Act of 1947 Sec. 101A. – Sec. 119B.

581 National Security Act of 1947 – July 26, 1947; Title II.

582 Vö. Farkas Ádám (2018d): 31–57., Farkas Ádám (2019b)

583 National Security Act of 1947 – July 26, 1947; Sec. 210.

584 National Security Act of 1947 – July 26, 1947; Sec. 214.

585 L. U.S. Cyber Command cybercom.mil/About/History/

együttműködési keretek fokozásával együtt.[586] Ennek a viszonyulásnak az egészséges kétirányúságát tükrözi, hogy a kutatás-fejlesztés témaköre a nemzetbiztonsági, azaz a nagyrendszer szintű koordináció erősödésével mára az első címbe, a nemzetbiztonság koordinációjába került át, kiterjesztve ezzel a katonai védelmen túl a tudomány és az innováció fontosságát a teljes védelmi és biztonsági szférára. Ebben tágabb értelmezésben feltételezhető, hogy a kibertérrel összefüggő fejlődés is jelentős szerepet fog kapni a jövőben.

A megalkotás idejére nézve tehát az mondható, hogy az amerikai nemzetbiztonsági törvény a társadalom és az állam védelmére hivatott három fő ágazatból (katonai védelem/honvédelem; nemzetbiztonság/titkosszolgálat; rendészet) kettőre fókuszált a katonai és a titkosszolgálati elemmel. Ez azonban elsődlegesen talán annak tudható be, hogy a rendészet hagyományosan a büntető igazságszolgáltatás és a közigazgatás metszéspontjában áll, és ezért később válik – belbiztonságként – önálló fegyveres védelmi entitássá az állami gondolkodásban. E tekintetben azt is figyelembe kell venni, hogy a rendészet az angolszász jog- és államrendszerekben eltérő fejlődési pályát járt be, mint a kontinentális államfejlődésben, ami azonban egy közös pontot, a biztonság fegyveres szavatolásában ellátott kulcsszerepet és a katonai erőtől való elhatárolást soha nem írta felül.

Időközben az amerikai nemzetbiztonsági törvény a biztonsági környezet változásaihoz és az államfejlődés vívmányaihoz igazodva jelentős szabályanyaggal gyarapodott, különös tekintettel a hírszerző tevékenységek alkotmányos kereteire és az adatvédelemre. Kiemelendő azonban, hogy e törvény a mai napig keretként értelmezhető, amely az időközben törvényi szinten is önállósult belbiztonságra[587] is kiutal, bekapcsolva azt értelmezési keretébe. Mindebből pedig egy olyan minta rajzolódik ki, amely egy idővel belátó politikai kultúrával és a különféle történelmi nyomáspróbákkal párosulva felismerte a maga tökéletlenségét[588] – ami nem jelent alacsony hatékonyságot –, és folyamatos fejlődésben, gyarapodásban igyekezett a demokráciát összehangolni a biztonsági környezet kihívásainak és fenyegetéseinek kezelésével.

Persze ez a megközelítés, és különösen a hidegháború örve alatt zajló hírszerző háború, illetve a különféle proxy háborúk komoly jogkorlátozásokat tettek szükségessé, illetve jelentős anyagi és emberi áldozatokkal is jártak. Ezeket értelemszerűen korlátozások, racionalizálások is követték a megalkotáskori fenyegetési paletta változásakor, de törekedve a geopolitikai státusz megóvásához szükséges képességek fenntartására. Újabb ellenirányú – felhatalmazás bővítő – kilengést az amerikai modell szempontjából kulcsjelentőségű 9/11 utáni fellépés hozott ebben a rendszerben. Az Egyesült Államokat saját területén ért jelentős terrortámadás hatására a nemzetbiztonsági fellépés jelentős mértékű fokozása és ennek törvényesítése is megvalósult. Ez utóbbi emblematikus eleme a PATRIOT Act,[589] mely utóbb számos támadásnak adott alapot, és emiatt korrigálásra is került, de mégis olyan változásokat hozott,

586 Vö. President Biden Signs National Security Memorandum to Improve the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems. whitehouse.gov/briefing-room/statements-releases/2022/01/19/fact-sheet-president-biden-signs-national-security-memorandum-to-improve-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/

587 Homeland Security Act of 2002 dhs.gov/sites/default/files/publications/hr_5005_enr.pdf

588 A téma kapcsán L. Scott (2018), Stuart (2008), Brown (2008), Barnet (1985): 483–500, Ripsman–Paul (2005): 199–227.

589 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001 govinfo.gov/content/pkg/BILLS-107hr3162enr/pdf/BILLS-107hr3162enr.pdf

melyek arra hivatkozással nem kerültek teljes mértékben annulálásra, hogy a változó biztonsági környezetben változó eszközrendszerre van szükség. Ebben a környezeti változásban az info-kommunikáció fejlődésének is kiemelt szerepe van. Ezt a jogalkotási lépést – a különféle hírszerzési botárnyoktól messze nem érintetlenül – a hírszerzésre vonatkozó törvényi felhatalmazások cizellálása követte, és okkal feltételezhetjük, hogy ez a változási folyamat nem állt le napjainkra sem. A különféle vélt vagy valós hibák ellenére ugyanis az amerikai modellt a folyamatos megújulás és adaptáció jellemzi, amit nem titkoltan a nemzet biztonságának elsődlegessége és az ehhez kapcsolódó hatalmi törekvések táplálnak, de úgy, hogy ennek szellemi motorját a védelmi és biztonsági szakmák mellett egy nagyon széles társadalmi beágyazottság is áthatja.[590] Azt is ki kell e ponton emelni, hogy a nemzetbiztonsági modell körül élénk – és kritikáktól messze nem mentes – közéleti és tudományos diskurzus is kialakult amerikai körökben, amelyek mind-mind a rendszer finomhangolását is szolgálják.[591] A különféle tapasztalások után pedig látható az is, hogy az amerikai nemzetbiztonsági rendszer, hasonlóan a 2015-ös terrortámadások után szintén kilengésbe került, majd részint visszarendeződött francia jogrendszerhez,[592] képes arra is, hogy a túlzó lépéseket korrigálja, racionalizálja, ebből következően pedig – vitáktól sosem mentesen, de a hatékonyságra törekedve – arra is, hogy a kezelendő biztonsági környezet, így az információs korszak jelentette kihívásokhoz is rugalmasan alkalmazkodjon mind szabályozási, mind intézményi, együttműködési, irányítási és koordinációs oldalról.

2.3. Egy kortárs védelmi-biztonsági rendszerekre irányuló osztályozás lehetséges sémája

Az, hogy az európai államok védelmi és biztonsági rendszerei a kibertér hatásaitól függetlenül is fejlődési és változási kényszerbe kerültek a hidegháború után, már Nolte klasszifikációjából is egyértelműen következik. Ezt azonban tovább fokozza az a tény, hogy a Nolte munkája óta eltelt majdnem negyed évszázad dinamikusan változó, és sok tekintetben romló, pontosabban a hidegháborút követő idealista víziókhoz mérten romló biztonsági környezettel párosult, miközben a társadalmi, gazdasági, politikai-kulturális és geopolitikai közeg differenciálódása tovább folytatódott. Ez a jelenségegyüttes a klasszifikáció egy másik irányát, az

590 Az Amerikai Egyesült Államok védelmi és biztonsági szerveinek együttműködése a piaci és a tudományos-oktatási szereplőkkel külön kutatásokat érdemel. Jelen kötet vonatkozásában azonban fontos felhívni arra a figyelmet, hogy a védelmi és biztonsági témák a K+F szektorban is meghatározó jellegűek, illetve a felsőoktásban és az egyetemi kutatási szférában is kiterjedten jelen vannak a védelmi szféra intézményein túl is. Ez nem csak a különféle intézmények, kutatások, periodikák körén látszik, hanem azon is, hogy a védelmi és biztonsági szféra – korábbi katonai és titkosszolgálati vezetők – milyen módon tudnak átlépni a civil, illetve ezen belül az akadémiai szférába. Ezt az állami célú kutató, elemző és képző intézmények mellett a különféle kormányfüggetlen elemző központok és think-tankek is példázzák, mint a Center for Strategic and International Studies (csis.org), az MIT Center for International Studies (cis.mit.edu) vagy épp a Stratfor (worldvies.stratfor.com). Ezt erősíti azonban az is, hogy személyi értelemben is értékelik az átjárást a védelmi és biztonsági szféra, a gazdasági szféra, illetve a felsőoktatás között. Erről példaként l. Gates (2018)

591 A téma kapcsán l. Scott (2018), Stuart (2008), Brown (2008), Barnet (1985): 483–500, Ripsman–Paul (2005): 199–227.

592 E tekintetben l. Stollsteiner (2021): 322–340., Ságvári (2017): 179–188., Spitzer (2020b): 235–258., Spitzer (2020c): 69–93.

átfogó vagy komplex – angolszász megközelítésben: nemzetbiztonsági jellegű – védelmi és biztonsági megközelítés állami és jogi meghonosításának jellege szerintit alapozhatja meg.

Érdemes tehát kísérletet tenni arra, hogy Huntington nyomait fürkészve, és az amerikai modellt – illetve annak lényegében a NATO reziliencia megközelítése útján való érvényesülését – is figyelembe véve megpróbáljuk általánosítani a nemzetbiztonság makroszintű, azaz politikai-kormányzati megközelítését, és ezzel egy olyan új osztályozási séma alapjait letenni, amely segíthet helyesen értelmezni és a fejlesztés szempontjai szerint is elemezni a nemzeti szintű szabályozást a későbbi kutatások során.

A magam részéről ehhez egy olyan munkafogalmat javaslok, amely szerint a szektorálisan tagolt biztonság különféle dimenzióinak hatásai egymásra vetülve, egymást erősítve, egymással új eredményeket és hatásokat eredményező kölcsönhatásokra lépve közelítendő meg, és abba mindazon jelenségek relevánsként bevonhatók, amelyek közvetlen, vagy jól prognosztizálható időn belül közvetlenné váló visszahatási képességgel rendelkeznek a fizikai valóságra és vele az állam- és/vagy a társadalomműködés folyamataira, stabilitására.

Egy ilyen megközelítés persze szükségképpen rendkívül sokrétű, már-már végtelen számú releváns tényező bevonását eredményezheti, mindazonáltal megpróbál rávilágítani arra, hogy ma már a biztonság szempontjából éppoly jelentősnek tekinthető egy társadalom berendezkedése, jóléti kitettsége, iskolázottsága és átlag intellektusa, mint egészségügyi helyzete és ellátórendszere, az adott állam infrastrukturális fejlettsége és annak belső megoszlása, gazdasági jellemzői, kommunikációs ismérvei, innovációs lehetőségei, geopolitikai és geográfiai helyzete, vallási és kulturális sajátosságai, adaptációs képességei, katonai, nemzetbiztonsági, belbiztonsági képesség- és hatékonyság szintjei, közigazgatási korszerűsége, vagy épp politikai stabilitása és fejlődőképessége. A különféle fenyegetések és kihívások ugyanis egymással kölcsönhatásba hozzák az egyes aspektusokat, és így fejtik ki hatásukat az adott társadalmi és állami berendezkedésre.

Ennek megfelelően az az állam, amely nem komplexen közelít a kihívásokhoz és a fejlesztésekhez, az jelentős versenyhátrányra, hosszú távon pedig kudarcra van ítélve, hiszen a 21. században úgy fest, a biztonsági dinamika tovább gyorsul, és egy gazdasági válságot rövid időtávon belül követhetnek fegyveres konfliktusok, társadalmi-kulturális feszültségek, migrációs nyomások, járványok, természeti katasztrófák, terrortámadások, majd ezek ismétlődései különféle variációkban. Ezekre pedig összehangolt helyett részleges fejlesztésekkel, illetve az állam megújulási képességének fokozása – egy ehhez megfelelően alkalmazkodó állami humánpolitika, illetve kutatás-fejlesztési és oktatási politika – nélkül nem lehet megfelelő válaszokat adni. A szükséges összhang és előremutató fejlesztési célok azonosításában és koordinációjában pedig a nemzetbiztonság makroszintjének kiemelt jelentősége lehet, vagyis annak a „napi" szintű helyzetértékelés és művelet-irányítás mellett stratégiai tervező-szervező jelentősége is van, amihez a szükséges feltételeknek rendelkezésre kell állnia.

Ha a munkafogalomra tett javaslatomat mint a vizsgált politikai, kormányzási ernyőterületet tükrözőt elfogadjuk, akkor magától értetődő lesz számunkra, hogy ennek hatékony működéséhez

- rendszerszemlélettel felépített szabályozás,
- egy valódi kapcsolódásokra és kölcsönhatásokra épülő, tehát „nagy" rendszert alkotni képes szervezetalakítás és –fejlesztés,
- szakosított apparátus és ezt biztosító kutatási és képzési keretrendszer,

– átgondolt és komplex kommunikációs és biztonságtudatosító stratégia, valamint
– komplex és jól strukturált, mégis hatékony és adott esetben gyors reagálást biztosító döntés-előkészítési és döntés-hozatali rendszer szükséges.

Ezek a kritériumok – ahogy erre Huntington is felhívja a figyelmet – azonban nem lehetnek előzmények vagy történelmi alapok nélküliek. Mind a szakapparátus, mind a stratégiák, vagy a döntéshozatal vonatkozásában egyértelmű, hogy a biztonság 20. század előtti felfogása kitermelte már a különféle példákat, alapokat. A 20. század előtt a biztonság erőteljesen katonai dominanciájú felfogásban érvényesült, aminek fő oka az volt, hogy a járványok és a természeti csapások akkor még kevéssé befolyásolható jelenségei mellett a nem ritkán beálló háború volt az a fenyegetés, amely a legnagyobb mértékben képes volt aláásni egy társadalom, illetve egy állam működését, vagy akár fennmaradását is. Ebből adódott az állam azon evolúciós reakciója, hogy legjelentősebb fegyveres apparátusává a haderőt tette, amelynek sajátosságai mind a jogi szabályozásban, mind pedig az állami döntéshozatalban testet öltöttek.

Értelemszerűnek tűnik tehát, hogy amikor a biztonság a technikai, gazdasági, társadalmi, politikai változások és fejlődés miatt a korábbinál jóval összetettebb, de egy adott terület dominanciájával már nem jellemezhető, akkor szükség van arra, hogy az egyébként minden más „civil" vonatkozásában is egyre bővülő feladatkörű állam a nemzetbiztonság komplex rendszerében is létrehozza a korszerűségre és hatékonyságra törekvő szabályozási, strukturális, döntéshozatali, illetve bürokratikus megoldásait. Ezek nélkül ugyanis a régi receptek, régi megoldások és régi beidegződések által determinált apparátus alkalmazására kényszerülne az állam, ami megújulási képességében kevéssé megfelelő, és egy idő után már hatásfokában is jelentékenyen hanyatló cselekvésekhez, tehát az állam funkcionális zavaraihoz és a biztonság eróziójának fokozódásához vezetne.

Ezt a kényszert az államok többsége felismerte. Nem véletlen, hogy a 20. század a nemzetbiztonság tekintetében a sajátos szabályozások, illetve a speciális szervezetalakítások időszaka volt, melyben már egyre fokozottabb figyelmet kapott a kormányzati döntéshozatal és -előkészítés szakosítása is a nemzetbiztonság aspektusából. Ennek köszönhető, hogy a nemzetbiztonság makroszintű fogalma számos állam sajátos döntéshozatali, illetve döntéstámogató fórumában visszaköszön (Nemzetbiztonsági Tanács, Nemzetbiztonsági Titkárság, Nemzetbiztonsági Bizottság stb. elnevezéssel) annak érdekében, hogy az egyes államok vezetői a nemzetbiztonságot érintő döntéseiket úgy tudják meghozni, hogy az érintett ágazatok vezetői mellett a döntéshozatalt szakosított, a komplex biztonság szakmai vonatkozásait és igazgatási sajátosságait is ismerő szervek és szakértők támogatják. Ezek az instrumentumok azonban még a 20. század vívmányai, vagyis ezek talaján mérlegelni kell a további fejlesztés lehetséges irányait, hogy a 21. századi körülményekhez igazodó és hatékonyabb rendszereket tudjunk kialakítani.

Egy, a biztonság komplex megközelítésének talaján álló, az állam- és jogrendszer viszonyulását vizsgáló osztályozás az előzőekben leírtakra építve segítheti az ez irányú gondolkodást és helyzetünk megfelelő felmérését is. A javasolt új osztályozás középpontjában a reziliencia kapcsán már említett „whole of government" megközelítés és annak megoldási módozatai állnak. A fenti példákra figyelemmel úgy pontosabb, ha a klasszifikáció központi elemeként azt tekintjük vizsgálati pontnak, hogy az adott osztályba tartozó államok a komplex megközelítést

– jogi, intézményi, együttműködési, irányítási és koordinációs;
– együttműködési, irányítási és koordinációs; vagy
– irányítási és koordinációs

keretben valósítják-e meg, szoros összefüggésben természetesen a nemzeti sajátosságokkal a politikai-kulturális és történeti dimenziókban. Fontos már itt kiemelni, hogy ez az osztályozás hallgatólagosan szinkronban áll Nolte demokrácia megközelítésével, de leválasztva arról a történeti kötöttségeket, hiszen a fenti osztályozás fentről lefelé haladva nem feltétlenül jelent hatékonysági különbséget, sokkal inkább azt tükrözi, hogy az adott rendszer mennyire átlátható, mennyiben társul egy államon belül, illetve állam-társadalom relációban érvényesülő komplex kooperációs kerettel.

A jogi, intézményi, együttműködési, irányítási és koordinációs modell mintáját egyértelműen az Egyesült Államok adja a nemzetbiztonsági rendszerrel. Ennek a megoldásnak a lényege, hogy mind szabályozási, mind intézményi, mind pedig működési oldalról beágyazott a komplex megközelítés. Ez nem rontja le az egyes specializált szakmai szervek működését, fejlesztésük fontosságát vagy adott esetben a kisebb intenzitású – napi feladatellátási – kihívások együttműködéses keretben való kezelésének lehetőségét. Ez a modell egyik oldalról azt tükrözi, hogy a nagyobb intenzitású vagy jellegéből adódóan számos szakterületet érintő kihívások kezelése nem ad hoc, hanem minden értelemben rendezett keretek között valósulhat meg. Másik oldalról az is következik ebből a modellből, hogy az állam védelmi és biztonsági funkciói kevéssé szeparáltak már – a szükséges sajátosságok, információvédelem és titkosság körétől eltekintve – a „civil" állami szervektől és a társadalomtól, mint korábban, hiszen egy egyértelműen átlátható, informatív webes megjelenésekkel párosuló, illetve törvényi keretekből is következően társadalmi együttműködésre építő intézményi struktúrát tükröz. Ez a modell egyszerre biztosít átlátható keretet, és ezzel egy értelmezési alapot a komplex biztonságfelfogás erősödéséhez, illetve a különféle képességek koordinált és egymást erősítő kiaknázásának lehetőségét, megerősítve azokat a szakmai, szakpolitikai, kormányzási-politikai szintű összekapcsoltság intézményi kereteivel is. Ebben a megközelítésben ez a komplex séma több olyan hozadékot is potenciálisan elérhetővé tesz, amelyek a szabályozási-intézményi-működési összekapcsoltság révén az „egész több, mint a részek összessége" hálózatkutatási tapasztalatából következik. Természetesen látni kell azt is, hogy ez a modell nagyobb személyi, intézményi és infrastrukturális igényekkel is párosul.

Az együttműködési, irányítási és koordinációs modell lényege, hogy bizonyos sajátos – különösen válságkezelési, kimagasló fenyegetés kezelési – feladatok szervezetek közti együttműködésen alapuló szabályozási megalapozása mellett a döntő szerepet a komplex biztonsághoz igazodó állami fellépésben a kormányzati szervek irányítási és koordinációs funkció kapják. E körben jellemző egyrészt, hogy az érintett minisztérium állami, illetve állami-társadalmi együttműködési feladatait fokozzák, továbbá jellemző az is, hogy a komplex biztonsági fellépéshez igazodó döntéselőkészítő vagy döntéshozatali szervek létesülnek, amelyek vagy sajátos irányítási megoldásokkal, vagy az eredeti irányítási jogkört gyakorlók együttes döntéseivel biztosítják a rendszer összehangoltabb működését. Ebben a modellben jellemzők a már említett védelmi, védelmi-biztonsági, nemzetbiztonsági stb. koordinációs tanácsok, titkárságok, munkacsoportok és bizottságok, amelyek legtöbbször nem vagy nem teljesen azonosak a kormányzati összetétellel. Ebbe a modellbe a legtöbb EU-s tagállam beletartozónak tekinthető, kiemelt példát hoz azonban az Egyesült Királyság, illetve Franciaország abban a tekintetben, hogy a kooperatív működést szabályozási és irányítási oldalról is megalapozzák, de nem lépnek – a nagyhatalmi törekvések ellenére sem – tovább az amerikai modell megvalósítása felé.

Az Egyesült Királyság közkeletű elnevezésű megoldása a COBRA,[593] amely azonban inkább csak tükröződése annak a modellnek, amelyben a különféle sajátos jogállású területek, illetve az eltérő kormányzati funkciókat ellátó szervek irányítóinak kooperációjára épül a krízismenedzsment, kiegészülve sajátos szabályzási megoldásokkal és állandó kormánykabinetekkel,[594] illetve annak a sürgetésével, hogy további erősítésre kerüljön a nemzetbiztonsági szemlélet.[595] Franciaországban hasonló – de a félprezidenciális jelleghez igazodóan sajátos modell azonosítható, melyben a különféle ágazati szabályozások biztosítják az együttműködést, az átfogó megközelítés azonban irányítási oldalról jelentkezik első sorban az államfő elnökletével működő Védelmi és Nemzetbiztonsági Tanács,[596] valamint a tárcaközi – részint kormányzási, részint szakpolitikai és szakmai – koordinációért felelős Védelmi és Nemzetbiztonsági Főtitkárság[597] működése révén. Ez a modell a különféle képességek egymást segítő-kiegészítő alkalmazására építve érhet el többlet hozadékokat, míg a komplex megközelítést döntően a szakpolitikai, illetve a kormányzás tisztán politikai dimenzióiban érvényesíti.

Az irányítási és koordinációs modellbe lényegében azok az államok sorolhatók, ahol, főként a központosított nemzeti működési hagyományok és/vagy megoldások miatt, az állam erőforrásainak, különféle funkcióinak, illetve társadalmi kapcsolódásainak összehangolt működtetése védelmi és biztonsági érdekből egyértelműen központi irányítási alapokon nyugszik. Ezekben az államokban nem ritka az az Európában korábban már ismert, döntően a katonai dominanciájú biztonságfelfogás korára jellemző megoldás, hogy az adott kihívástípushoz igazodó módon a központi irányító egy adott ágazat központi szervei útján gyakorolja az összes érintett funkció irányítását. Ebben a modellben is jelen van tehát a komplex biztonsághoz igazodó átfogó fellépés lehetősége, annak letéteményese azonban a végrehajtó hatalom központi szintje, míg megoldási módozata jellemzően a kezelendő fenyegetés szerint feladat- és hatáskörrel rendelkező ágazat, szervezet időleges kulcsszerepbe kerülése. Utóbbi kapcsán kiemelendő, hogy ez a megoldás hatalmi, illetve információs szempontból szenzitív területek fokozottabb elkülönítését is lehetővé teszi, vagyis az átfogó megközelítésű válságkezelését minden esetben a hatalmi struktúra fenntartásához szükséges megoldások fenntartása mellett tudja megvalósítani. Ez a modell azokban az államokban jellemző, ahol nem, vagy nem transzatlanti értelemben tűnik szükségesnek és bevettnek a jól átlátható szabályozási és működési rendszer kialakítása. E tekintetben egyértelmű példaként hozható fel Oroszország és a Kínai Népi Demokratikus Köztársaság. Oroszország esetében a centralizált irányítás hagyományaira építve általános keretnek tekinthető az elnöki hatalomból következő meghatározások szerint működő Polgári Védelemért, Rendkívüli Helyzetekért és a természeti katasztrófák következményeinek felszámolásáért felelős minisztérium, valamint a védelmi minisztérium és különösen annak Nemzeti Védelmi Irányítási Központja,[598] amely a könyv

593 A valós rövidítés COBR, ami a Cabinet Office Briefing Rooms elnevezést takarja és azokat a hivatali helységeket öleli fel, amelyekben a nemzeti vagy regionális válságkezelési megbeszélések szoktak zajlani az érintett irányítók között.

594 Vö. www.gov.uk/government/publications/the-cabinet-committees-system-and-list-of-cabinet-committees/list-of-cabinet-committees-and-their-membership

595 Vö. Devanny–Harris (2014)

596 Le Conseil de défense et de sécurité nationale. elysee.fr/en/french-presidency/defence-and-national-security-council

597 Secrétariat général de la défense et de la sécurité nationale. sgdsn.gouv.fr/accueil/sgdsn-in-english/

598 A téma kapcsán l. McDermott (2014) Cooper (2016), Perrin (2020)

megjelenésének idején is zajló orosz–ukrán háborúban is kulcsszerepet tölt be. Ezek a fórumok biztosítani tudják az elnöki döntések ágazatokon és szervezeteken átívelő megvalósítását, azonban inkább irányítási, és az irányítást segítő összekötőként értelmezhetők, mint nyugati értelmében vett koordinációs intézményi keretként. Kína tekintetében hasonló kép rajzolódik ki a felvállaltan pártállami működés sajátosságait figyelembe véve. Ebben a tekintetben egyértelmű, hogy a központi szerepet Kína védelmi és biztonsági működése vonatkozásában az elnök, és egyben a párt főtitkára játssza, a valós irányítás tekintetében pedig a párt szervei jelentik a kulcspozíciót, míg a formális kormányzati szervek a működtetés terepét. Kína azonban pártállami jellegének megőrzése ellenére sajátos utat jár be, ugyanis az információs technológia robbanásában is kulcsszereplő, amivel visszaigazolja a jelen klasszifikáció azon alapvetését, hogy az nem hatékonysági értékelést, hanem inkább működési csoportosítást tükröz. Ebben a modellben szükségszerű, hogy egyik oldalról a hatalmi pozícióhoz szükséges katonai erő megkülönböztetett szerepe jobban fennmaradjon, másik oldalról pedig az, hogy a jelentősen újnak ható kihívásokat kezelő képességek – például a huszadik században a titkosszolgálatok, ma a kibertérben tevékenységet ellátó szervezetek – is többlet felhatalmazásokat kapjanak, hiszen az átfogó kooperáció helyett nagyobb területen érvényesül e körben a szervezeti fellépés és esetleges célzott együttműködés.

3. A magyar védelmi és biztonsági szabályozási séma kibertér-fókuszú áttekintése

Ahogy az előző fejezetekben rögzítettük, a jogállami működést determináló szabályozás szerepe szükségképpen jelentős a 21. századi biztonsági környezethez való alkalmazkodás tekintetében, és ezt csak tovább erősíti az az alkalmazkodási és reagálási kényszer, ami az információs technológiák rohamos fejlődéséből és terjedéséből, ezeknek az egyénekre, társadalmakra és államokra gyakorolt hatásaiból következik. Ebben értelemszerűen Magyarország sem kivétel, sőt a védelmi és biztonsági szabályozás modelljei kapcsán azt is látni kell, hogy hazánk Nolte értékelésében egyértelműen a poszt-autoriter államok körébe tartozik, amit tovább nehezít, hogy hazánk történelmi és gazdasági helyzete is jelentős mértékben fokozta azt a politikai indíttatást, amely az elmúlt három évtizedeben pártpolitikai hovatartozástól függetlenül a védelmi képességekre inkább szükséges rosszként, mint optimálisan beárazott fejlesztési prioritásként és használható funkciókként tekintett.

Az elmúlt évek – döntően a biztonsági környezet rohamos változásával – Magyarországon is a védelmi és biztonsági rendszer megújítása, különféle rendészeti, titkosszolgálati és katonai képességek fejlesztése felé hatott, amely folyamatra aztán 2020. év végétől a védelmi és biztonsági rendszer reformjának megkezdése is ráépült. A fejlesztési tematikában[599] mind képességbeli, mind intézményi, mind pedig szabályozási és elméleti oldalról egyértelműen jelen van a kibertér jelentette kihíváshalmaz. Ez az elektronikus információbiztonság – EU-s alapokon nyugvó – nemzeti szabályozásától, a büntető jogi megoldásokon át, a nemzetbiztonsági, a katonai és a rendészeti szabályozásban, illetőleg az új, összkormányzati védelmi-

599 Példaként l. Kenedli (2020): 74–94., Dobák (2022a), Dobák–Tóth (2021): 195–212., Kovács László (2023), Christián (2022), Hódos (2022), Hódos (2021a): 134–149., Farkas Ádám (2021d), Farkas Ádám (2019c): 63–79.

biztonsági szabályozásban is jól azonosítható. Mindazonáltal ki kell emelnünk, hogy az előző gondolatban felvázolt tematikus láncolat nem egy egységes és koherens fejlesztési folyamat eredménye, ahogy azt is, hogy a 2020 végén megindult védelmi és biztonsági szabályozási reform még folyamatban van, így egyértelmű, hogy a konkrét szabályozás szintjén a következő időszakban további jelentős változások várhatók.

Kiemelendő a hazai szisztéma tekintetében az is, hogy egyik oldalról a magyar kiberbiztonsági szabályozás erősíti azt a korábbi megállapításunkat, miszerint a kiberbiztonság témaköre egyrészről szerves része a védelmi-biztonsági szabályozásnak, másrészről azonban azon túlmutató, ha úgy tetszik önállósuló vagy már önállóvá vált jogterület is. Ezt tükrözi hazai viszonylatban egyfelől az EU-s alapokon nyugvó Ibtv. és a kiberbiztonsági szabályozás, illetve legújabban a kiberbiztonsági tanúsításról szóló szabályozás[600] is, míg másfelől az a tény, hogy a kibertérrel összefüggő új szabályozási elemek mind a honvédelmi, mind a nemzetbiztonsági, mind pedig a büntető igazságszolgáltatást megalapozó szabályozásban megjelentek az elmúlt években. Ez a kettősség a kibertér és a tágabb értelemben vett nemzetbiztonság viszonylatában arra hívja fel a figyelmet, hogy a „civil" szférára is kiterjedő önálló szabályozásnak is jelentős szerepe van a biztonsági ökoszisztémában, de a hagyományos védelmi-biztonsági rendszer részeként a fókuszt – jelen kötetben is – elsődlegesen a védelmi-biztonsági képességek kibertér műveleti vonatkozásaira kell helyezni. Az összehangolt fellépés jegyében azonban magától értetődő, hogy mind a stratégiai döntési szinteken, mind pedig a konkrét események kezelése, illetve hatósági fellépések szintjén szükségszerű az érintett szervezetek közti hatékony kooperáció erősítése. Ennek folyományaként a jövőre nézve az is mérlegelendő, hogy az információs tér/kibertér szabályozásában elképzelhető-e egy olyan szabályozási irány, ami egy önálló kiberbiztonsági törvény megalkotásával a biztonsági dimenzió jelentőségét fokozza, és egyidejűleg erősíti a hagyományos védelmi-biztonsági funkciókhoz való kapcsolódásokat is.

Jelen kötet megközelítésére és korábbi fejezeteire figyelemmel nemzeti megoldásaink áttekintése körében egy olyan helyzetkép megadását tartjuk célravezetőnek, amely átfogóan mutatja be a komplex biztonság, és különösen a kibertér jelentette kihívások hatását a magyar állam- és jogrendszer tág értelemben vett nemzetbiztonsági vonatkozásaira, vagy ha úgy tetszik: védelmi-biztonsági szabályozására. Ehhez szükségesnek tartjuk hazánk megoldásainak elhelyezését az előző fejezet szerint javasolt klasszifikációban a szemléleti és intézményi vonatkozásokkal együtt tárgyalva, majd pedig a szabályozási dimenzió nagybani áttekintését a kibertér jelentette hatásokra fókuszálva és esetleges fejlesztési irányokat megjelölve.

3.1. A magyar megoldások klasszifikációs besorolása, különös tekintettel a védelmi és biztonsági rendszer szemléleti és intézményi dimenzióira

Az előző fejezet szerinti osztályozás tekintetében Magyarország álláspontunk szerint a jelenleg folyamatban lévő reformra figyelemmel az *együttműködési, irányítási és koordinációs* modellbe tartozik, de megkezdte elmozdulását a jogi, intézményi, együttműködési, irányítási és koordinációs modell felé, amely állapot önmagában véve is jelentős változásként értelmez-

600 L. Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (továbbiakban: Ibtv.), Bodó et al. (2020), Tóth András (2022), Tóth Tamás (2019): 97–115., A kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről szóló 2023. évi XXIII. törvény

hető, hiszen a magyar védelmi és biztonsági rendszer az 1989-es rendszerváltás után nem számított prioritási kérdésnek a 2010-es évek közepéig a hazai jogalkotásban és kormányzásban.

A jelenlegi pozíciót a szabályozás ágazati-funkcionális tagoltsága és az ehhez igazodó – funkcionálisan lehatárolt – döntés-előkészítési és döntéshozatali intézményi keretek dominanciája alapozza meg, amelynek elemeit a következőkben ismertetjük. Az elmozdulást azonban egyik oldalról az Alaptörvény kilencedik módosítása, másik oldalról pedig a védelmi és biztonsági tevékenységek összehangolásáról szóló 2021. évi XCIII. törvény elfogadása és 2022. november 1-jei hatálybalépése alapozza meg. Ez utóbbi folyamat ugyanis egyik oldalról egyértelműen az összkormányzati, és egyben a komplex biztonsághoz igazodó megközelítés felé mozdul el mind az alkotmányos szabályozás, mind pedig a törvényi szintű keretrendszer tekintetében, viszont figyelemmel arra, hogy ez az átállási folyamat még a szabályozás terén is kiteljesedőben van, és kérdéses, hogy intézményi tekintetben milyen irányt vesz, nem tekinthető még olyan tényezőnek, amely révén hazánk egyértelműen az osztályozás első kategóriájába tartozna. Jelenleg tehát Magyarország a folyamatban lévő átalakítások miatt egy hibrid, vagy átmeneti mintát mutat az osztályozásunk tekintetében, aminek fő oka a következő intézményi vonatkozásokban rejlik.

Az állam védelmi és biztonság funkcióinak tervezése, szervezése és irányítása tekintetében domináns szerepet tölt be a végrehajtó hatalom, azaz a mindenkori kormány. Természetesen a hatalommegosztás mindenkori rendszerében megvannak a sajátos védelmi és biztonsági vonatkozású jogkörei és feladatai a törvényhozásnak, az államfőnek és az igazságszolgáltatásnak is, de az operatív működés rendszerként való irányítása tekintetében Magyarországon is a kormányé a kulcsszerep, a működésben azonban sajátos döntéshozatali szervről – az amerikai National Security Council megoldásához hasonlóan – nem beszélhetünk, hanem a kormány tematikus munkamegosztási fórumaként értelmezhető kabinet rendszer, illetve az azt támogató vegyes jellegű – szervezeti, szakmai és politikai vezetőket is tömörítő – döntés-előkészítő fórumrendszerről beszélhetünk.

Hatályos szabályozásunkban 2022 nyaráig létezett a kormányzás – politikai-hatalmi – szintjén sajátos védelmi és biztonsági szakmai szerv Nemzetbiztonsági Kabinet (a továbbiakban: NBK) elnevezéssel és szakminiszteri – az utóbbi években belügyminiszteri – irányítással, amelynek helyét a Védelmi Tanács (a továbbiakban: VT) vette át a miniszterelnök vezetésével. Ez a testület az érintett szakminiszterek részvételével, szükség esetén szakmai/szervezeti vezetők vagy szakértők meghívásával kifejezetten a védelmi és biztonsági tárgyú kormányzati kérdések megvitatására szolgál, pro forma és de jure kötelező érvényű és kormányzati erejű döntést azonban nem hoz, hanem döntéseiről tájékoztatja a Kormányülést, amely azokat jóváhagyással emeli lényegében kötelező erőre. Ez a megoldás természetesen gyorsítja a kormányzati működést, hiszen a miniszterelnök vezetésével jóváhagyott döntések kormányülésen való megmásítása csak kapcsolódó, de nem védelmi jellegű jelentős érdekből képzelhető el, így a VT és annak adminisztratív támogatása dinamikusan tudja a VT döntéseinek végrehajtását a kormány irányítása alá tartozó szervek körében menedzselni. Mindazonáltal kiemelendő, hogy a VT sem egy sajátos jogállású döntéshozó szerv, hanem inkább egy sajátos kormány kabinet. A korábbi NBK, ma VT, illetve végső soron a Kormány munkáját több a politikai és a szakmai-funkcionális vezetés szintjeit ötvöző bizottság és munkacsoport segíti, ezek feladatrendszere, jellege és kormányzati struktúrában való elhelyezkedése azonban már nem mutat egységes képet, inkább ágazati érdekeket tükröz. A tagolt döntés-támogató, döntés-előkészítő rendszer egyik oka, hogy a korábbi NBK,

azaz a mai VT összetételéből következően döntően kormányzási – vagyis politikai-hatalmi súlyozottságú – működési jelleggel bír, amihez szükséges a funkcionális támogatás biztosítása a különféle szakterületi munkacsoportok és bizottságok révén. Ezek tagjai jellemzően a különböző ágazatok, szakmai szervek központi közigazgatási szintű felsővezető, vezető besorolású képviselői. Ezek a szervek azonban vegyes képet mutatnak rendeltetésük, tagjaik, alárendeltségük és végső soron a VT-hez és vele a Kormány védelmi-biztonsági szakosított működéséhez való viszonyuk vonatkozásában is. Ezen tanácsadó, döntéstámogató, koordinációs testületek közé sorolhatjuk

– a Nemzetbiztonsági Munkacsoportot (NBMUCS);
– a Honvédelmi és Rendészeti Munkacsoportot (HRMUCS);
– a Honvédelmi Igazgatási Koordinációs Tárcaközi Munkacsoportot (HIKOM);
– a Katasztrófavédelmi Koordinációs Tárcaközi Bizottságot (KKB);
– a Terrorellenes Koordinációs Bizottságot (TKB), valamint
– a Nemzeti Kiberbiztonsági Koordinációs Tanácsot (KIBKT).

Ezen intézmények mindegyike ellát döntéselőkészítő, döntéstámogató funkciókat, ezen túlmenően azonban messze nem tekinthetők egy egységes intézményi séma különféle funkcionális variánsainak. Van köztük olyan, amely dedikáltan a korábbi NBK, ma már VT, és van, amely a kormány alárendeltségébe tartozik, miközben feladatrendszerük egyértelműen védelmi-biztonsági tematikájú. A KKB és a TKB a tematikus döntéstámogatás mellett operatív feladatokat is ellát a konkrét védelmi intézkedések összehangolásával vagy riasztási fokozatok bevezetése érdekében, míg a HIKOM inkább a döntéstámogatási jelleget, különösen a kormányzati döntéshozatalt gyorsító – a közigazgatási egyeztetést kiváltó – funkcióval hivatott segíteni. A HIKOM tekintetében érdekes változás, hogy azt egy ágazati igazgatási fórumként úgy tartja fenn a döntéshozó, hogy párhuzamosan 2022. nyarán létrehozta a Honvédelmi és Rendészeti Munkacsoportot a Kormány ügyrendjében, amelyet a VT alárendeltségébe kapcsolt, míg a HIKOM a kormány döntéselőkészítő szerve.

A kibertér jelentette kihívások szerepét tükrözi, hogy az azzal kapcsolatos döntés-előkészítés különálló fórumhoz, a KIBKT-hoz tartozik, méghozzá az Ibtv-ből levezethetően. Az előzőekben vázoltakhoz ez a fórum is illeszkedik annyiban, hogy bár elnevezésében és funkciójában is biztonsági feladatrendszerrel bír, elnöki tisztségét pedig a Nemzeti Kiberbiztonsági Intézetet is magában foglaló Nemzetbiztonsági Szakszolgálat főigazgatója látja el, ennek ellenére a KIBKT mégis a kormány döntéselőkészítő szerve, és nem a VT munkáját támogatja. További érdekesség ebben a vonatkozásban, hogy bár a KIBKT munkáját további, alárendelt munkacsoportok, valamint felkért tudományos és szakmai szakértőkből álló Kiberbiztonsági Fórum segíti, annak láthatósága meglehetősen alacsony, ami a reziliencia kapcsán leírtak tükrében még további fejlesztési igényeket körvonalazhat ezen a téren.

Ezen felül az egyes fórumok abban sem mutatnak egységes képet, hogy tagjaik milyen szintű vezetőkből állnak össze, és ehhez mérten legalább elvi szinten milyen szintű döntési autonómiával bírnak az egyes szakterületek képviselői. Ennek a sokrétűségnek az a fő oka, hogy a szóban forgó intézmények nem egy átfogó és rendszerszintű koncepció folyományaként jöttek létre, illetve kerültek újraszabályozásra és racionalizálásra, hanem adott funkcionális vagy ágazati koordinációs törekvés összkormányzati szintre vetítése, vagy a TKB esetében egy konkrét biztonsági fenyegetésre adott válasz részeként a 2015-ös párizsi terrortámadások után.

A védelmi és biztonsági szakosítottságú, felsőszintű döntéshozatali és döntéselőkészítő fórumok mellett ki kell azonban még térni a védelmi és biztonsági funkciók ágazatokon átívelő összehangolásának szakigazgatási kérdésére. Ez egy rendkívül érdekes képet mutató intézményi és szabályozási megoldásra vezetett eddig Magyarországon, mivel a védelmi igazgatás fogalma létezett, azt lényegében ágazatokon átívelő módon elismerték. A védelmi igazgatást azonban ágazati törvény – jelesül a honvédelmi törvény – határozta meg a következőkkel:

> „a közigazgatás részét képező feladat- és szervezeti rendszer, amely a Kormány – a honvédelemért felelős miniszter útján gyakorolt – irányítása mellett a Magyarországot veszélyeztető fenyegetésekkel és támadásokkal szemben az állam feladatainak megvalósítására létrehozott, valamint egyes védelmi feladatok ellátásra kijelölt közigazgatási szervek által végzett tervező, végrehajtó, rendelkező tevékenység."[601]

A honvédelmi törvény általi meghatározottság egyik következménye, hogy a jogalkotó lényegében egy ágazatra telepítette az ágazatokon átívelő védelmi igazgatás komplex feladatrendszerét, amivel egy rendkívül sajátos és problémáktól messze nem mentes helyzetet alakított ki. A megoldással ugyanis egyrészről összemosódik a védelmi igazgatás és honvédelmi igazgatás[602] kérdése az értelmező rendelkezésekben való elhatároláson túl. Másik oldalról funkcionális értelemben egyértelmű, hogy az ágazatokon átívelő, ezért az egyes ágazatokat feladatok ellátásában irányító és ellenőrző védelmi igazgatás csak oly módon látható el teljes hatékonysággal egy adott ágazat által, ha ahhoz a jogalkotó – vagyis ez esetben plasztikusan a Kormány javaslatára az Országgyűlés – olyan többletjogosítványokat párosítana, amivel az adott ágazat primus inter pares-szé válik a kormányzati struktúrában. Ez nem lehetetlen megoldás ugyan, hiszen a kancelláriaminisztériumok és a kormányzati központok rendszerint ilyesfajta koordinatív funkciót hivatottak ellátni, és ezek a megoldások nem ismeretlenek a rendszerváltás utáni magyar kormányzati modellekben, de az, hogy egy szaktárcát expressis verbis a többi fölé emeljenek, az nem jellemző normál működési keretek között. További érdekessége az összkormányzati igazgatási bázist jellemző magyar megoldásnak, hogy miközben a védelmi igazgatást mint összkormányzati szakigazgatást a jogalkotó feladatként a honvédelmi tárcához telepítette, addig a védelmi igazgatás felett lévő szakosított összkormányzati döntéshozatal vezetésében a belügyminisztérium, illetve a belügyminiszter volt 2022 nyaráig túlsúlyban. 2022 nyarától ez a súlyozás egyik oldalról a miniszterelnök felé mozdult el a VT révén, másik oldalról pedig a miniszterelnök kabinetfőnöke és annak munkaszerve felé, hiszen a polgári nemzetbiztonsági szolgálatok mellett a védelmi és biztonsági igazgatás központi szervének irányítása is ide került, a nemzeti információs államtitkár feladatkörével együtt.[603]

601 A honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető rendkívüli intézkedésekről szóló 2011. évi CXIII. törvény 80. § 32. pontja

602 „12. honvédelmi igazgatás: a védelmi igazgatás részét képező feladat- és szervezetrendszer, amelynek keretében az ország védelmére létrehozott, valamint e feladatra kijelölt közigazgatási szervek, továbbá a honvédelemben közreműködő más szervek ellátják az 1. § (3) bekezdésében meghatározottak honvédelemre való felkészítésével, az országvédelemmel és a honvédelmi kötelezettségek teljesítésével kapcsolatos feladatokat". A honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető rendkívüli intézkedésekről szóló 2011. évi CXIII. törvény 80. § 12. pontja

603 L. a Kormány tagjainak feladat- és hatásköréről szóló 182/2022. (V. 24.) Korm. rendelet 29. §-át, valamint a Védelmi Igazgatási Hivatalról szóló 337/2022. (IX. 7.) Korm. rendelet 1. §-át

A kép tehát nem mutatott egységességet és konzisztenciát a Vbö.[604] 2022. november 1-jei hatálybalépéséig. Ezzel a fordulónappal a védelmi igazgatás helyét a védelmi és biztonsági igazgatás vette át, amely döntő részben függetlenné vált az ágazati szinttől, és a kormányzati központ részét képező Miniszterelnöki Kabinetiroda alárendeltségében létrehozott Védelmi Igazgatási Hivatal – mint a védelmi és biztonsági igazgatás központi szerve – szervezeti keretei közé került egy teljesen új, összkormányzati szemléletű törvényi megalapozottság mellett. Ezt a megközelítést erősíti az is, hogy az NBK helyét és szerepét a kormányzás politikai döntési szintjén átvevő VT vezetője sem a szakminiszter már, hanem a kormányfő, távollétében pedig ezen feladatait a miniszterelnök nemzetbiztonsági főtanácsadója[605] látja el, akinek feladatrendszere a nemzetbiztonság hazai és angolszász megközelítését ötvözi azáltal, hogy a kormányzati szintű titkosszolgálati felügyeleti és koordinációs feladatok mellett hadiipari, haderőfejlesztési, illetve a Vbö. szerinti komplex feladatrendszerrel kapcsolatos ellenőrző és koordináló jogosítványokat is kapott.

Az új rendszerre való átállás jelen sorok megírásakor még folyamatban van, elvi és szabályozási szinten azonban látható, hogy törekvés van a szakigazgatási háttér megteremtésére is a komplex biztonsághoz igazodó átfogó megközelítés érdekében. A kibertérből érkező kihívások kérdései kapcsán persze még tisztázást igényel a feladatrendszer és a működés, mivel az mind szabályozási mind pedig koordinációs szempontból sajátos képet mutat, melyben egyszerre jelenik meg ez önálló szabályozás és a védelmi funkciókon belüli speciális kibertérrel összefüggő tevékenységek szabályozása. Jelenleg tehát a kibertér vonatkozásában az látható, hogy a tág értelemben vett kiberbiztonság szabályozási alapját az Ibtv. és főbb végrehajtási szabályai adják egy saját koordinációs intézményrendszerrel, de eközben az alapvetően összkormányzati összehangolásra fókuszáló Vbö. is érinti a kibertér kapcsolódásait,[606] továbbá az ágazati törvényekben és rendeletekben is megjelennek kibertér műveleti rendelkezések és feladatok, továbbá ezekhez kapcsolódó koordinációs keretek.[607] A komplex biztonsághoz való alkalmazkodás azonban a jövőben nélkülözhetetlenné teszi, hogy a kibertérrel összefüggő – nem csak kiberbiztonsági, hanem azon túlmutató származtatott hatásokkal számoló – kihívások kezelése a komplex védelmi-biztonsági szisztémának is szerves része legyen.

3.2. A védelmi és biztonsági szabályozás változásai és az információs korszak sajátosságai

Az információs korszakkal, és különösen a kibertérrel összefüggően a szabályozás és az állami képességek fejlesztése nem csak hazánkban, hanem a transzatlanti térség egészében változásban van. Ez mind nemzetállami, mind szövetségi (NATO) és Európai Uniós viszonylatban megállapítható. A terület újszerűsége, a technológiai háttér és vele a társadalmi-gazdasági-biztonsági vonatkozások rendkívül differenciált és dinamikus változása ezt megkerülhetetlenné teszi.

604 A védelmi és biztonsági tevékenységek összehangolásáról szóló 2021. évi XCIII. törvény (továbbiakban: Vbö)
605 L. a Kormány ügyrendjéről szóló 1352/2022. (VII. 21.) Korm. határozat 108-115. pontjait
606 Példaként lásd a védelmi és biztonsági tevékenységek összehangolásáról szóló 2021. évi XCIII. törvény 5. § 15. pontját, V. fejezetét, 46. § (1) bekezdés j) pontját, XI. fejezetét
607 Példaként l. a rendőrségről szóló 1994. évi XXXIV. törvény, a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény, valamint a honvédelemről és a Magyar Honvédségről szóló 2021. évi CXL. törvény kibertérrel összefüggő rendelkezéseit

A kiberbiztonság szabályozásában jelentős kérdés már az is, hogy az állami szabályozás, felügyelet, illetve beavatkozás milyen esetekben jelentkezhet és meddig terjedhet. Erre a nemzetközi térben elég sokrétű megoldások mutatkoznak. Figyelemmel azonban arra, hogy az állami szabályozás és beavatkozás alapvetően kiberbiztonsági jellegű, a „címkéből" következő védelmi-biztonsági kötődés egyértelműen kapcsolódik az adott állam védelmi-biztonsági tudatosságához, kultúrájához, történetiségéhez. Ehhez érdemes hozzákapcsolni az EU-s és NATO-s vonatkozásokat, amelyek részint ajánlásként, részint kötelezettségként jelennek meg a tagállamokra nézve, miközben a kibertér biztonsága rendkívüli súlyú kérdése a nemzeti biztonság szavatolásának is. E tényezők együttesen eredményeztek azt a jelenleg tapasztalható megoldási sémát a transzatlanti térségben, amely egyik oldalról önállósítani látszik a kiberbiztonság területét, másik oldalról azonban a kibertérrel kapcsolatos új területeket ettől elkülönülten megjeleníti a „hagyományos" védelmi-biztonsági funkciók szabályozásában is.

Mindezeket egybevetve hazánk tekintetében látni kell, hogy a védelmi-biztonsági funkciók mellett a kiberbiztonság kérdése sem tekinthető egyszerűnek. Egyrészről a terület újszerűsége, sajátosságai eleve egyfajta szemléleti konfliktust eredményeznek a piaci szereplőkkel szemben, hiszen a biztonság kérdését mind szemléleti, mind működési szempontból máshogy közelíti meg egy kiberbiztonsággal foglalkozó piaci szereplő és egy olyan állami szervezet, amely a kibertéri tevékenységeket a biztonság tágabb terrénumához, és ezzel más funkciókhoz is kapcsolja. Másrészről azt is látni kell, hogy az állam védelmi és biztonsági funkcióinak társadalom- és politikatörténeti kényszerpályája valamiképp erre a területre, pontosabban a kibertéri tevékenységek „hagyományos" védelmi-biztonsági feladatlellátásba való bekapcsolására is kiterjed.

A konkrétumok szintjén jól értelmezhető, hogy a – túlzással talán, de – hazai kiberbiztonsági törvényként számon tartott az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény megalkotásához mérten a konkrét védelmi és biztonsági funkciók terén a kibertérben zajló műveleti tevékenység csak később, és alapvetően meglehetősen korlátozott szabályozási keretekkel, részint NATO kötődésekkel, majd sajátos intézményi kapcsolódásokkal jelent meg.[608] Az információs térrel összefüggő büntetőjogi eszközkészlet fejlődése folyamatosnak mondható, és e téren a szakirodalmi diskurzus is aktívnak tekinthető, mindazon által feltehető persze a kérdés, hogy ez a terület mennyiben tud adekvát megoldást és reakciót adni a gyors lefolyású, valós idejű kibertéri cselekményekre, illetve azok származtatott hatásaira a dezinformációtól a szándékolt pánikkeltésen át egészen a támadó jellegű, de nem csak katonai értelmezéssel bíró műveletekig.

A szabályozandó kérdés rendkívül összetett, az európai, illetve a nemzetközi és külföldi válaszok is fokozatosan fejlődnek, és egyre magasabb, erőteljesebb beavatkozási szintekre lépnek az adminisztratív-hatósági jellegű, majd a büntetőjogi természetű részmegoldások után már a szélesebb körű biztonsági szabályozás felé haladva. Mindez azonban még nyitott kérdések sorát tárja elénk, amelyek megválaszolása szorosan összefügg a nemzeti biztonság rendszerszerű szavatolásának karakterével. E tekintetben számos kritikus kérdés áll előttünk, melyek közül példaként emelhetők ki a következők:

608 Vö. A honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről szóló 2011. évi CXIII. törvény 40/A. címét, valamint a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény 8. § (7)-(10) bekezdéseit és 56. § e) pontját

– Megalkotandó/megalkotható-e egy átfogó, lényegében új és funkcionális értelemben különálló védelmi-biztonsági területet jelentő kiberbiztonsági törvény?
– A kibertér gazdasági, társadalmi és politikai hatásai, illetőleg a digitalizáció üteme és térhódítása tükrében a kiberbiztonság szabályozásának védelmi-biztonsági területként kell-e működnie vagy helyesebb a jelenlegi „civil" szabályozás és emellett a védelmi-biztonsági sajátosságok egyes funkcióknál történő jogi keretezése?
– A konkrét jogok érvényesülésének, illetve a nemzeti biztonság absztraktabb kategóriájának védelme, megerősítése érdekében milyen szintű, mértékű állami beavatkozások engedélyezhetők?
– Az infokommunikáció rohamos fejlődésével összefüggően meddig terjedhet az állam védelmi és biztonsági képességeinek felülvizsgálata és megújítása?
– Egy esetleges kiberbiztonsági törvény megalkotása miként viszonyuljon az összkormányzati biztonságszavatolás kibontakozó intézményrendszeréhez és a hagyományos védelmi és biztonsági képességek szabályozásához?

A kiberbiztonsági törvény egy inkább adminisztratív-hatósági szemléleti alapra helyezkedjen – hasonlóan például a minősített adatok védelméről szóló törvényhez –, vagy egy védelmi-biztonsági területekre jellemzőbb, államot felhatalmazó, intézményi és eljárási kereteket teremtő, ha úgy tetszik védelmi és műveleti arcélű bázisra?

A kérdések sora még hosszan folytatható, és ezzel a szakirodalom is hol mélyebben, hol inkább katalógusszerűen foglalkozik. Meglátásunk szerint pedig jelen kötet tematikájához a hagyományos védelmi és biztonsági funkciók terén megjelenő szabályok, illetőleg a kibontakozóban lévő összkormányzati védelmi-biztonsági szabályozás és működés kapcsolódásainak bemutatás illeszkedik a kibertér és kiberbiztonság kapcsán.

Megközelítésünk szerint az információs tér és társadalom bázisa az elnevezésből is következően az információ. A nemzeti biztonság és az információ kapcsolatában a legmélyebb összefonódást a nemzetbiztonsági szolgálatok által képviselt titkosszolgálati funkció képviseli, hiszen annak fő szerepe az információk megszerzése és megóvása, illetve sok tekintetben információs alapon a nemzetbiztonságot veszélyeztető cselekmények, törekvések felderítése, megelőzése, elhárítása. Áttekintésünket tehát itt indítjuk, majd innen az információs hadviselés témakörére, és annak az orosz–ukrán aktualitásaira figyelemmel, a honvédelem területével folytatjuk. Nem vitatva, hogy a kibertérnek és az információs vonatkozásoknak a bűnüldözés terén is rendkívül jelentős vonatkozásai vannak, kötetünk jelen kiadásában ezt a területet az adminisztratív-büntetőjogi területhez soroljuk és mellőzzük, hiszen a rendészeti fellépést döntően a büntetőeljárási szabályok, illetve a közigazgatási szankciós jelleget mutató szabálysértési vonatkozások határozzák meg. Ez a lehatárolás, úgy véljük, a külföldi irodalommal is korrelál, hiszen a kibertér műveletek kérdését a külföldi diskurzus, illetve szabályozási és szervezési megoldások is jellemzően a katonai és a titkosszolgálati dimenziókhoz kapcsolják.[609] A nemzeti biztonság és a kibertér szabályozási vonatkozásai kapcsán tehát a titkosszolgálati és a katonai funkciók után a záró elemet a kibontakozóban lévő összkormányzati védelmi-biztonsági megközelítés, illetve annak kibertérrel való kapcsolódásai adják, így mutatva egy reményeink szerint átfogónak mondható képet a nemzeti biztonságunk kibertéri vonatkozásait meghatározó szabályozási keretekről.

609 A téma kapcsán l. Lin–Zegart (2018), Farkas Ádám (2022e)

3.2.1. A nemzetbiztonsági szabályozás kibertéri kapcsolódásai

Ahogy az előzőekben már tisztáztuk, a nemzetbiztonsági szabályozás tartalmilag mást fed le az angolszász terminológiában, mint Magyarországon. Hazánkban a nemzetbiztonsági törvény lényegében a titkosszolgálatok szervezeti és eszköz-, illetőleg módszer-rendszer irányultságú szabályozását öleli fel. A két fogalmi vonatkozás közül a magyar irány a nemzetbiztonság mikroszintjeként ragadható meg. A klasszifikáció kérdésre visszautalva nemzetbiztonság mikroszintjének megszervezése és szabályozása az államrendszer elemzése vonatkozásában is releváns, és adott esetben jelentős markernek tekinthető. Az, hogy egy adott állam a szolgálatait például a polgári-katonai megoszlás tengelyén; a polgári vagy katonai szegmensen belül funkcionális vagy fegyvernemi tagoltságban; elhárító-hírszerző klasszifikációban; végrehajtó-szolgáltató megközelítésben; vagy épp klasszikusan humán alapú és elkülönült technikai portfóliókban szervezi meg, mind-mind jellemzését adja az adott állam nemzetbiztonsági rezsimjének, és távlatosan ugyan, de rendszerszintű működés-hatékonyságának és biztonságfelfogásának, továbbá politikai kultúrája egyes szegmenseinek és hagyományainak,[610] végső soron pedig akár Nolte módszerén, akár az általunk javasolt megközelítésen nyugvó osztályozásának is.

A transzatlanti térségben a funkcionális szint jelentőséget kaphat a titkosszolgálati szféra és a civil társadalom közti reláció vonatkozásában is, hiszen ezekkel a szervezetekkel szemben egyfajta társadalmi misztikum, illetve időszakosan bizalmatlanság már-már értelemszerűen minden államban felmerül az eljárások, módszerek, működés és részletes feladatok titkossága, fedettsége, illetve sajátos és nem minden elemében megismerhető motivációja és jellege miatt. Részint ennek is tudható be, hogy globális értelemben is jelentősnek mondható nemzetbiztonsági szolgálatok fokozatosan nyitnak a társadalom felé.[611] Ennek bevett csatornáját adhatják a múzeumok, a kommunikatív webfelületek, illetve a tudományos életben való részvétel és az adott szolgálat, illetve funkcionális ág történetének fokozatos (de szükségképpen részleges) feldolgozása és megismertetése. Úgy is mondhatnánk, hogy az adott államrendszer vonatkozásában a civil kontroll viszonylagos feltérképezésében is egy szempont lehet a titkosszolgálatok társadalommal való kapcsolatának informatív vagy kevésbé informatív jellege.

A civil kontroll és a bizalom dimenziójában egy másik aspektus lehet annak a megnyilatkozása, hogy az adott államban jelentős tudományos, kutatási, központi közigazgatási vagy akár politikai tisztségeket milyen arányban vállalnak (vállalhatnak) olyanok, akikről e funkciók betöltésekor nyilvánosan is kommunikálják, hogy korábban valamely nemzetbiztonsági szolgálat állományában szolgáltak. E tendencia érzékelhető vagy elhanyagolható volta egyik részről az adott állam szolgálatokkal szembeni bizalmát és elfogadását, másik részről pedig a szolgálatok nyilvánossággal kapcsolatos viszonyulását is tükrözi.

A nemzetbiztonsági szolgálatok, és általában a „titkosszolgálati" szféra elmúlt bő évszázados önállósulása és dinamikus fejlődése tekintetében persze látni kell, hogy a történeti gyökereknek még meghatározó jelentősége van/lehet, amivel jelen gondolatok között is indokolt foglalkozni. Visszakanyarodva tehát a történelmi determinációhoz: a legtöbb államban – bizonyos tekintetben a demokratikus tradícióktól függetlenül – él az az alapvető felosztás, amely a nem-

610 Vö. Béres (2018b), Farkas Ádám (2020b): 5–20.

611 A téma kapcsán példaként l. Dobák (2022c): 52–67., Dobák (2022b): 145–159., Petruska–Vikman (2021), Budavári (2023): 34-48.

zetbiztonsági szolgálatokat a katonai, illetve a polgári osztályokba sorolja feladataik, viszonyrendszerük és ezzel összefüggésben nem ritkán személyi állományuk jogállását is tükrözve. Ez a felosztás egyszerre tekinthető egyfajta tradíciónak, vagy evolúciós visszatükröződésnek, de egyben szakmai és jogállami garanciának is.

A hírszerzés, kémkedés, elhárítás történetével foglalkozó kötetek[612] sora emeli ki, hogy a ma ismert, önálló nemzetbiztonsági szolgálatok jó része a 20. században önállósult. Persze ezeket a funkciókat ezt megelőzően is el kellett látni az állam szervezetében, azonban ezek kiterjedtsége, jelentősége a 20. századot megelőző korok technológiai színvonala, illetve a katonai és ezen belül is háború-dominanciájú biztonságfelfogása miatt eltérő jellegű és jelentőségű volt. Értelemszerű tehát, hogy a hírszerző és elhárító funkciók a haderőn és a rendészeten belül jelentek meg mint speciális szolgálati formák. A 20. század technológiai, biztonsági és nem utolsó sorban politikai-társadalmi dinamizmusa volt az, ami a hadseregek és a különféle rendőrségek berkein belül lévő hírszerző és elhárító képességek felerősítése, majd szervezeti önállósítása, végül pedig ágazati jellegű elkülönülése felé hatottak. Ennek az eredetnek, vagy evolúciónak a tradicionalitása abban érhető tetten, hogy különféle nemzetbiztonsági szolgálatok feladatrendszerében a legtöbb államban a mai napig meghatározónak mondható az, hogy mely másik fegyveres testületből eredeztethetők. Az információs korszakban ez az eredet és funkcionális „evolúció" jelentős mértékben hat arra is, hogy az adott szolgálatnak milyen mérvű és jellegű feladatai vannak a kibertérrel és annak biztonságával, illetve más „hagyományos" védelmi-biztonsági funkcióhoz való kötődésével összefüggésben.

A *katonai nemzetbiztonsági szolgálatok* alapfeladatai között visszatérő módon jelenik meg a haderő művelet tervezésének és művelet végrehajtásának információkkal, titkosszolgálati eszközökkel, módszerekkel és képességekkel való támogatása, vagy épp a katonai állomány tekintetében a „belső" elhárítási feladatok ellátása, amelyen túl azonban a katonai védelemnél sokkal szélesebb körű, de a katonai viszonyokhoz ezer szálon kötődő feladatok is jelen vannak (például hadiipari tevékenységekkel összefüggők, katonadiplomáciaiak, a katonai szervezeteket veszélyeztető radikalizmusra irányulók, rádióelektronikai, terror-elhárítási vagy alkotmányvédelmi jellegűek stb.). Látni kell, hogy a katonai nemzetbiztonsági szolgálatok feladatai elsődlegesen nemzetbiztonsági-titkosszolgálati vonatkozásúak és „csak" másodlagosan katonai védelmi jellegűek, amely utóbbi azonban szervezeti-funkcionális kapcsolódások, és végső soron egy kettős rendeltetés vagy jogállás specialitását vonja maga után. A kibertérrel összefüggő feladatok és sajátosságok ebben a képletben is szükségképpen megjelennek a legtöbb államban. Magyarország viszonylatában sincs ez másként. A Katonai Nemzetbiztonsági Szolgálat (a továbbiakban: KNBSZ) alapvetően nemzetbiztonsági szolgálat az Alaptörvény 46. cikke és a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény (a továbbiakban: Nbtv.) szerint, de „másodlagosan" a honvédelemről és a Magyar Honvédségről szóló 2021. évi CXL. törvény (a továbbiakban: Hvt.) 3. § 14. pontja értelmében honvédelmi szervezet is a Hvt.-ben meghatározott feladataival összefüggésben. Ha mindezt a kibertér kapcsolódásai felől közelítjük meg, akkor egyrészről a KNBSZ nemzetbiztonsági feladatrendszerében önálló pontként jelennek meg a kibertérrel összefüggő speciális feladatok, másrészről azonban a katonai kibertér műveletekkel összefüggő feladatok is azonosíthatók a Hvt.-ben. Az Nbtv. 6. § g) pontja szerint a KNBSZ

612 Vö. Andrew (2018), Hughes–Colonel (2017), Jagadics et al. (2018), Árvai–Gyaraki (2019), Béres (2018a), Boda (2016), Pilch (1996), Piekalkiewicz (1998)

> „információkat gyűjt a honvédelmi érdeket veszélyeztető kibertevékenységekről és -szervezetekről, jogszabály keretei között ellátja a honvédelmi ágazat elektronikus információbiztonsági feladatait, biztosítja a honvédelemért felelős miniszter által vezetett minisztérium, valamint a Honvéd Vezérkar tervező munkájához szükséges, kibertérrel összefüggő nemzetbiztonsági jellegű információkat, továbbá kibertér műveleti képességeivel ellátja a honvédelmi érdekek nemzetbiztonsági jellegű védelmét és együttműködik a Magyar Honvédség kiberműveleti erőivel."[613]

E feladatrendszer jól mutatja, hogy a feladatellátásnak kötődései vannak a hagyományos katonai feladatellátáshoz, a kiberbiztonság adminisztratív-hatósági vonatkozásihoz, illetve a titkosszolgálati szféra sajátosságaihoz is. Fontos azonban kiemelni, hogy a szolgálatok feladatrendszerében még számos más kapcsolódás is lehetséges ebben a tekintetben, hiszen a technológia fejlődése miatt bármely más szolgálati alapfeladatánál is felmerülhet a kibertér kapcsolódása az ellenérdekelt/felderítendő cselekmények megvalósítása körében. Ez a fajta feladatkomplexitás mind a hazai, mind a nemzetközi viszonylatban szükségessé teszi, hogy a katonai nemzetbiztonsági szolgálatok feladataik ellátása körében fokozott figyelmet fordítsanak a kibertér nemzetbiztonsági, illetve katonai vonatkozásaira és fejlődésére. A konkrét műveleti fellépés kapcsán a külföldi mintákon az is látható, hogy a komplex kihívásokra figyelemmel a kibertér műveleti vonatkozásoknál sajátos együttműködési keretek jönnek létre, ahol a „titkosszolgálati" funkciók a katonaival, esetenként a bűnüldözésivel is összekapcsolják.[614]

A fenti logika alapján a *polgári nemzetbiztonsági szolgálatoknál* is jellemzően megmutatkozik, hogy mely másik állami szférából, illetve szervezetből nőttek ki. A diplomáciai testületekből eredő hírszerző szolgálatok jellemzően az információszerzési és érdekérvényesítési feladataikon túlmenően a diplomáciai testületek „titkosszolgálati" védelmében, információbiztonsági biztosításában is jelentős feladatokat látnak el, illetve más módon is aktívan támogatják a diplomaták munkáját. Magyarországon ezt a feladatrendszert az Információs Hivatal képviseli, melynek korábban a kibertér viszonylatában dedikált elektronikus információbiztonsági feladatai voltak, amelyeket aztán átvett a Nemzetbiztonsági Szakszolgálat. Ettől függetlenül azonban a katonai szolgálatoknál megfogalmazottak itt is érvényesíthetők, vagyis a kibertér jelentőségnek fejlődése révén szükségképpeni, hogy a polgári hírszerzés feladatrendszerében – nevesítés nélkül is – számos kapcsolódással bír a kibertér, amelyhez a feladatellátásnak alkalmazkodnia kell. A rendészeti szférából kiváló nemzetbiztonsági szolgálatok feladatrendszerében pedig a rendészeti, és különösen a bűnüldözést titkosszolgálati eszközökkel támogató funkciók vannak jelen az önálló, polgári viszonyokra irányuló, komplex nemzetbiztonsági feladatok mellett. Magyarországon ebbe a körbe az Alkotmányvédelmi Hivatal mint polgári elhárítás, illetve a Nemzetbiztonsági Szakszolgálat (a továbbiakban: NBSZ) mint technikai szolgáltató, és napjainkra már mint polgári kiberbiztonsági szervezet tartozik. A katonai szolgálatok és a polgári hírszerzés kapcsán rögzítettek a kibertér viszonylatában ezen szervezeteknél is irányadók, az NBSZ szerepe azonban még jelentősebb e tekintetben. Egyik oldalról a törvényi rendelkezések szerint az NBSZ „jogszabály rendelkezései szerint ellátja az elektronikus információbiztonsággal kapcsolatos feladatokat,"[615] ami értel-

613 A nemzetbiztonsági szolgálatokról szóló 1995. évi CCV. törvény 6. § g) pontja
614 L. Farkas Ádám (2022e)
615 Nbtv. 8. § (1) bekezdés i) pont

mezési szempontból a KNBSZ feladatrendszerével egybevetve azt jelenti, hogy mindazon feladatok hozzá tartoznak az adminisztratív-hatósági kiberbiztonsági körből, amelyek honvédelmi vonatkozásaik miatt nem tartoznak a KNBSZ-hez. Másik oldalról azonban az NBSZ feladatrendszerében törvény külön megjeleníti, hogy

> „A Nemzetbiztonsági Szakszolgálat - a 6. § *g)* pontjában foglaltak és a katonai kibertér műveletek kivételével - információbiztonsággal kapcsolatos feladatkörében
>
> a) ellátja az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvény hatálya alá tartozó szervek tekintetében az ott meghatározott hatásköri szabályok szerint a kibertérből érkező fenyegetésekkel és támadásokkal szembeni védelmet,
> b) a honvédelmi ágazat kivételével irányítja a kibertérből érkező fenyegetésekre történő felkészülést és a kapcsolódó biztonsági feladatokat,
> c) ellenőrzi - az azon folytatott kommunikáció megismerése nélkül - az elektronikus hírközlési hálózatok forgalmát, észleli a kibertérből érkező fenyegetéseket és támadásokat,
> d) végrehajtja vagy kezdeményezi a kibertérből érkező támadás megszakításához szükséges intézkedéseket."[616]

Ez a sajátos feladatrendszer egyszerre reagál a KNBSZ feladataira, ad egy sajátos – primus inter pares – pozíciót a polgári nemzetbiztonsági szolgálatok körén belül a kiberérrel összefüggő védelmi tevékenységek körében, illetőleg azáltal, hogy időben a honvédelmi törvény hasonló tárgyú rendelkezései után épült be az Nbtv. szövegébe, lényegében a nemzetbiztonsági dimenzióban szűkítve, de leképezi, és egyben viszonyításként reagálja a katonai kibertér műveleti vonatkozásokat is.[617] Ez utóbbi különösen azzal erősíti meg az Nbtv., hogy külön tételezi:

> „(8) A (7) bekezdés *d)* pontja szerinti intézkedés végrehajtására a Kormány által kijelölt személy erre vonatkozó döntése alapján van lehetőség. A támadás megszakítását követően meg kell vizsgálni a védelem fokozásához szükséges további intézkedések lehetséges körét, illetve az ország védelmével összefüggő további döntések szükségességét. (9) A (7) bekezdés *d)* pontja szerinti intézkedésnek *a)* az okozott sérelemmel vagy közvetlen fenyegetéssel arányosnak és szükséges mértékűnek kell lennie, és törekedni kell arra, hogy a támadás megszakításán túli eredményre vagy sérelemre ne vezessen, *b)* biztosítani kell az összhangot a nemzetbiztonsági, honvédelmi, bűnüldözési és külpolitikai érdekekkel és törekvésekkel. (10) Külföldről érkező jelentős kibertámadás esetén a foganatosított intézkedésekről és azok okairól tájékoztatni kell a külpolitikáért felelős minisztert a további intézkedések megtétele céljából."[618]

Ezek a szabályok ugyanis jellemzően a katonai szükségesség nemzetközi mintáira építő logikát követnek és honosítanak meg az Nbtv.-ben, sajátos szerepbe hozva ezzel az NBSZ-t, de mégsem kizárólagossá téve annak szerepét, hiszen a KNBSZ feladatkörén kívüli hatáskört tételezett a jogalkotó, illetve a külső engedélyhez kötött titkos információgyűjtő eszközök

616 Nbtv. 8. § (7) bekezdés
617 Farkas Ádám (2021d)
618 Nbtv. 8. § (8)–(10) bekezdései

alkalmazásánál is minden szolgálat számára nyitva hagyta az információs rendszerekkel kapcsolatos titkos információgyűjtés jogi lehetőségét, és e körben a kibertér műveleti cselekmények foganatosítását is.[619]

A konkrét feladatrendszerek kibertéri vonatkozásai kapcsán is mondhatnánk tehát, hogy egy nemzetbiztonsági szolgálat feladatrendszeréből, és e tekintetben a polgári/katonai klaszszifikációban való elhelyezkedéséből jó eséllyel következtetni lehet annak eredetére, tradicionális „hovatartozására", és ezáltal – jelen kötet fókusza alapján – a kibertérrel kapcsolatos feladataira is. A polgári-katonai felosztásnak azonban funkcionális és jogállami értelemben vett garanciális természete is van. Egyrészről ugyanis ez egyértelműen tükrözi, hogy sem a katonai, sem a rendészeti, sem a nemzetbiztonsági szférában nem alakulhat ki olyan fokú hatalomkoncentráció, ami a 20. század borzalmainak felderengéséhez vezethetne. A nemzetbiztonsági szolgálatok általi támogatás ugyanis azt mutatja, hogy a katonai és a rendészeti szféra információs szempontból képvisel kisebb potenciált, míg értelemszerű, hogy a nemzetbiztonsági szolgálatok oldalán a kiterjedt erőalkalmazás képessége az, ami nem tekinthető érdemi/bevett jellemzőnek, hiszen az szükség esetén a másik két szervtípus együttműködésével érvényesíthető. Ebből tehát az erőkoncentráció garanciális kizártsága mutatkozik meg, amihez érdemes hozzávenni, hogy a fent leírtak egyben funkcionális tagoltságot is jelentenek, ami pedig az adott szolgálati formára való szakosodás, vagyis a professzionalizáció alapja.

Ez persze együttműködést is feltételez, hiszen egyértelmű, hogy a komplex biztonság korában egyre több olyan kihívás és fenyegetés jelenik meg, amely a szolgálatok közötti, illetve a más állami szervekkel való kooperáció nélkül nem kezelhető megfelelően. Mégis ez a fajta tagoltság a kibertér viszonylatában is garanciát jelent, mivel a kibertérre reagáló felderítő, elemző, értékelő, műveleti, hatósági képességek nem egy ponton összpontosulnak. Másfelől nézve ez a sokrétűség a hatékonyság fokozását is szolgálja, hiszen a kibertér sok esetben a hagyományos cselekmények újszerű közvetítő közegeként érvényesül, ami egy központosított és kizárólag kiberbiztonsági fókuszú megközelítés esetén a hatékonyság csökkenésével járna, mivel a hagyományos cselekmények nem vesztik el hagyományos logikájukat és sajátosságaikat a kibertéri érvényesítés során, hanem kiegészítik azokat a kibertér által biztosított új elemekkel. Ez azt is jelenti, hogy az ilyen jelenségek kezelése szükségszerűvé teszi a hagyományos reagálási képességek és szemléletmódok diverzifikált, de mégis összehangolt kibertéri alkalmazását is úgy az állam védelmi és biztonsági funkcióinak egész rendszer, mint a nemzetbiztonsági-titkosszolgálati szféra tekintetében.

3.3. A katonai kibertér műveletek szabályozása

Ahhoz, hogy a katonai kibertér műveletek nemzetközi viszonylatban is egyre mélyebben és szélesebb körben elemzett és hazai viszonylatban is növekvő érdeklődésre számot tartó témájának hazai szabályozására kitekintsünk, fontos néhány alapvetést megfogalmaznunk az érthetőség érdekében. E körben elsődleges annak rögzítése, hogy a katonai tevékenységek központi és megkerülhetetlen részei a honvédelmi szabályozásnak, de utóbbi egy szélesebb halmazt jelent, mivel magában foglalja mindazon tervező, szervező, felkészítő és igazgatási tevékenységek kapcsolódásait, amelyek az ország egészének és a társadalomnak a katonai fe-

619 Vö. Nbtv. 56. § e) pont

nyegetésekkel szembeni védelméhez szükségesek. A katonai szabályozás közvetlenül a haderő tevékenységére, a honvédelmi szabályozás a katonai szabályozásra, és azon túl a kapcsolódó igazgatási, szervezési, oktatási, képzési stb. tevékenységekre is kiterjed, s mint ilyen, rendkívül jelentős történelmi evolúcióval, nemzeti sajátosságokkal rendelkezik.[620]

A honvédelem viszonylatában az erős tradicionalitás ethosza keveredik az előzménykötöttséggel a szabályozás terén. Ez alatt azt értjük, hogy a honvédelmi szabályozás megújulási képessége kevéssé látványos és dinamikus az egyes történelmi korszakhatárok között, mint más területeké. Ez részint abból a tényből fakad, hogy a honvédelem rendszere az állam kényszerapparátusának része, és így politikailag minden időszakban szenzitív kérdés annak fejlesztése, megújítása. Másik oldalról azonban látni kell, hogy a honvédelem egy piaci alapon nem szervezhető közszolgáltatás, amelynek ellátása az államon belül is egyedi szervezeti keretben jelenik meg, így – a nagyhatalmi szerepkör nélküli államok esetében – annak speciális tudással és egyben információ-monopóliummal párosuló belső rendszereiben a piaci közeg, de esetenként még a tágabb, civil közigazgatás intellektuális versenykényszere is mérsékelten vagy másként érvényesül. Ez a sajátosság egyes történelmi szituációkban értelemszerűen előny is lehet, hiszen kiszámítható, begyakorolható működést és rendszerszinten egységesülő gondolkodást alapozhat meg. A történelmi és/vagy biztonsági helyzetkép dinamikus változása során azonban ez a fajta megközelítés hátránnyá válhat, ha az intellektuális versenykényszer hiányára az innovativitás csökkenésével járó rutin működés alakul ki, és emiatt a szükséges szakmai, tudományos tartalékok és innovációs képességek nem kerültek kialakításra, illetve fenntartásra. A 2010-es évek második fele óta pedig biztosan állíthatjuk, hogy egy dinamikusan változó helyzetbe kerültünk, amelyre újszerű válaszokat kell adni. Nem véletlen, hogy Magyarországon is folyamatban van a honvédelmi és haderőfejlesztés, illetve annak biztonsági környezetre reagáló elemeként egyfajta katonai kultúraváltás,[621] valamint, hogy a honvédelem szabályozása is változó képet mutat.[622]

A kibertér, és tágabban a diszruptív technológiák, az autonóm fegyverrendszerek, a mesterséges intelligenciára épülő művelet- és információ elemzés mind-mind egyre bevettebb fogalmak, melyek jelentős mértékben alakítják a honvédelmi, katonai feladatellátást, de természetesen a biztonságszavatolás összes többi területét a hatósági feladatoktól a rendészeti funkciókon át a nemzetbiztonsági tevékenységekig. Ez a NATO szabályrendszeréből is érzékelhető. Egyértelmű tehát, hogy az az időszak, amelyet jelenleg átélünk, egy olyan történelmi szituáció, melyben a környezet – különösen a kibertér hatásaira és polgári felhasználása mellett érvényesülő katonai alkalmazhatóságára figyelemmel – jelentősen változik. Ez megkerülhetetlenné teszi az állami reagálás, így a honvédelem korszerűsítését is, a képességeken túl a rendszerszemlélet, a más állami szférákhoz való kapcsolódás, a működés és ezek jogállami kereteként a szabályozás terén is.

Kettős tehát a szorítás, amivel a honvédelem rendszerének – és általában az állam védelmi és biztonsági funkcióinak – szembe kell néznie, hiszen a technikai, képességfókuszú megújulás mellett szükséges egy szemléletmódbeli, működési, szabályozási reform is. Ennek szabályozási vertikumában pedig át kell gondolni, hogy a honvédelem jogának ágazati keretei milyen mértékben építenek az 1990-es évek során kialakított szabályozásra, az pedig milyen

620 Vö. Farkas Ádám (2019b)
621 Ezek kapcsán l. Korom (2020): 3–4., Kádár (2020): 3–10., Porkoláb (2019)
622 L. Balogh–Till (2022), Farkas–Till (2022)

mértékben jelentett tartalmi újítást – a jogállami elvek szerinti átvezetésen túl funkcionális értelemben is – a rendszerváltás előtti törvényi keretekhez képest. Ha ugyanis szabályozásunkat inkább az esetről-esetre, tapasztalatról-tapasztalatra reagáló részleges korrekciók és egyfajta előzmény-kötöttség jellemzi,[623] akkor egy olyan rendszerszintű reformra van szükség, amely egyszerre képes szintetizálni a szakmai és képességfejlesztési igényeket, a nemzetközi és külföldi hatásokat, a kormányzati célokhoz szükséges megoldásokat, de az állam- és jogfejlődés újításait, újítási igényeit is. Ez a fajta szorítás tehát az 1990-es évek szemléletmódjának apró korrekciójával, de még a 2000-es évek elején kialakított szemléleti dogmák új jelenségekre vetítésével sem kezelhető konstruktívan. A szorítás oldását nem segíti e körben a védelmi-biztonsági reform felgyorsítása – vagyis az AT9M[624] és a Vbö. hatálybalépésének előrehozása – sem, mivel az egyértelműen felgyorsította a kapcsolódó honvédelmi szabályozást is.[625] A 2021-ben elfogadott „új" honvédelmi törvény e tekintetben, sok újítása mellett, egy ilyen vizsgálatban okkal feltételezhető, hogy az AT9M és a Vbö. hatálybalépéséhez igazítás kényszerének erejét mutatná, amely feltevés helytállósága esetén a jelenleg is zajló kultúraváltás nem zárja ki a szabályozás további fejlesztését. Kérdés, hogy ez a további szabályozás témáról-témára, esetről-esetre, vagy immár komplex koncepcionális keretben valósul majd meg, hiszen a működési környezet változásai átfogónak tekinthetők.

A technológiai környezet forradalmi változása ugyanis a társadalom működését, egyéni és csoport szintű pszichológiáját, gondolkodás- és munkamódszereit is átformálja. Ebből egyértelműen következik, hogy az emberi eredetű kihívások és fenyegetések szemlélete, módszerei és dinamikája is jelentősen változik. Az állam védelmi és biztonsági rendszerének pedig az alapvető rendeltetése ezek megelőzése, elhárítása, megfelelő módon történő reagálása az egyéni és össztársadalmi jogérvényesülés fenntartása, ezáltal pedig a rend, a biztonság, a jólét és a gazdasági fejlődés lehetőségének, alapjainak biztosítása érdekében. Magától értetődő, hogy ha a megelőzésre és reagálásra hivatott állami rendszerek gondolkodása, rendszerszerű működése és dinamikája – az eszközökön túl – nem tudja felvenni a megújulás és innováció ütemét, akkor hátrányba kerül a kihívásokkal szemben. E körben azonban a katonai sajátosságok nem jelentenek mentességet, mivel jól látható a különféle konfliktusok, és az immár háborús fázisba lépett orosz–ukrán relációban, hogy a katonai szembenállást is áthatják az új fajta technikai, szemléleti és humán viszonyok a hagyományos szembenállási formák fennmaradása mellett. E körben a kibertér műveletek, a drónhadviselés, illetve ezekben a korábban aktív katonai szolgálati kötődéssel nem rendelkező személyek szerepe egy jelentős marker, ami mutatja, hogy a katonai védelem terén is meg kell találni az új időkhöz valóban igazodó megoldásokat.

A nemzeti szabályozás konkrétumai tekintetében e körben előrelépések tapasztalhatók az elmúlt években, hiszen a honvédelmi törvényekben viszonylag részletes, és a működést jól keretező együttműködési, illetve kibertér műveleti szabályok jelentek meg. E folyamatban elsőként az Nbtv.-nek a KNBSZ kiberbiztonsági feladatait meghatározó rendelkezésére[626] alapozva, és ebből a korábbi honvédelmi törvény szabályainak új elemekkel való gyarapítása felé lépve ment végbe a katonai és katonai nemzetbiztonsági kibertér műveleti képességek mű-

623 L. Till (2017), Farkas Ádám (2020c) 347–380.

624 Az Alaptörvény kilencedik módosítása.

625 E tekintetben érdemes összevetni a 2011. évi és a 2021. évi honvédelmi törvényeket.

626 Vö. Nbtv. 6. § g) pont, valamint ennek evolúciója kapcsán Hódos (2021b): 134–149.

ködtetésének törvényi megalapozása. Ennek fontos eleme a Magyar Honvédség és a KNBSZ relációjában a kifejezetten kibertér-fókuszú együttműködés honvédelmi vonatkozású előírása is. Ezt tükrözi az a korábbi honvédelmi törvényből az új Hvt.-be is átemelt rendelkezés, miszerint

> „Magyarország honvédelmi érdekeinek védelme és biztosítása, a kapcsolódó szövetségesi kötelezettségek teljesítése, valamint az országvédelem kibertér műveleti erőkkel történő fenntartása és fokozása érdekében a Honvédség és a KNBSZ kibertér műveleti erői közvetlenül együttműködnek egymással. A kibertér műveleti képességek fejlesztését, valamint a kapcsolódó tervezési, biztonsági és szabályozási feladatokat a Honvédség a KNBSZ-től kapott információk felhasználásával és a KNBSZ szakmai támogatásával látja el. Ha a kibertér műveleti képességek fejlesztése, a kapcsolódó tervezési, biztonsági és szabályozási feladatok nemzetbiztonsági vonatkozással bírnak, a végrehajtásukhoz a KNBSZ főigazgatójának egyetértése szükséges."[627]

A honvédelmi szabályozás katonai nemzetbiztonsági funkciókhoz való kapcsolása – és nemzetbiztonsági érintettség esetén egyetértéshez kötése – a nemzetbiztonsági szabályozásban már meglévő előzményeken túl tehát a biztonsági ésszerűségen is alapul. A kibertér, és az ott realizálható – honvédelmi érdeket érintő – fenyegetések jellege, más folyamatokhoz vagy fenyegetésekhez való kapcsolódási lehetőségei, illetve a reagálás sokféle tényező általi meghatározottsága miatt is teljesen egyértelmű kell, hogy legyen ennek az összekapcsolódásnak a szükségessége. Ennek fő oka, hogy a kibertérből érkező – honvédelmi érintettségű – fenyegetések és akár támadások is számtalan aspektusban túlmutathatnak a Magyar Honvédség alapvetően katonai védelmi, de még a honvédelem szélesebb felelősségi körén is, illetve biztosan szükségessé teszik a válaszlépésekkel kapcsolatos felelős politikai döntés meghozatalához – mások mellett – a nemzetbiztonsági vonatkozások áttekintését is.

Ezt a szemléletet erősíti az is, hogy a kibertérből érkező fenyegetések és támadások tekintetében nemzetközi és belső jogi értelemben is egy folyamatos változásban lévő szabályozási környezet tapasztalható, ami a reagálást eleve komolyabban megfontolandóvá teszi. Ennél is fontosabb azonban az a tény, hogy a fajsúlyos támadások prognosztizálhatóan országon kívüli indíttatásúak lesznek, amelyekre egy katonai típusú, nem kinetikus válaszlépés sem nemzetközi politikai, sem tágabb értelemben vett nemzetbiztonsági, sem pedig jogi értelemben nem alapozható meg automatizmusként.

Ha a konkrét normaszövegek felől közelítünk, akkor a fentebb már idézett együttműködési alapvetésen túl, a honvédelmi törvény konkrétan katonai kibertérműveltekre vonatkozó szabályai is ezt a fajta körültekintést tükrözik:

> „88. § (1) A Honvédség katonai kibertér műveleti erői jogszabályban meghatározottak szerint folyamatosan ellátják
> a) a honvédelmi szervezetek – ide nem értve a KNBSZ-t – és az e törvény szerinti katonai feladatok – ideértve az ezekre való felkészülést és a gyakorlatokat is – kibertérből érkező fenyegetésekkel és támadásokkal szembeni védelmét, az arra történő felkészülést

627 A honvédelemről és a Magyar Honvédségről szóló 2021. évi CXL. törvény 17. § (5) bekezdés

és – a jogszabályban meghatározott elektronikus információbiztonsági feladatokra figyelemmel – a kapcsolódó biztonsági feladatokat,

b) az a) pont szerinti feladatokkal összefüggésben a folyamatban lévő, kibertérből érkező támadás megszakításához szükséges intézkedések végrehajtását, vagy annak kezdeményezését, valamint

c) a Magyarország biztonságát, honvédelmi érdekeit, illetve szövetségesi kötelezettségeit sértő vagy fenyegető rendszerekkel szembeni katonai kibertér műveleti fellépést.

(2) Az (1) bekezdés a) pontja szerinti katonai feladatok ellátásának védelme kapcsán felmerülő részfeladatokat a Magyar Honvédség parancsnoka határozza meg.

(3) Az (1) bekezdés b) és c) pontja szerinti feladatok szakmai koordinációjáért – a kapcsolódó közjogi döntések keretei között – az ügyeletes kibervédelmi parancsnok felel.

(4) Ha az (1) bekezdés b) pontja szerinti intézkedéseket a Honvédség kibertér műveleti erői önállóan hajtják végre, akkor

a) az intézkedések végrehajtását a (3) bekezdés szerinti parancsnok, vagy annak helyettese, szükség esetén elöljáró parancsnoka rendelheti el,

b) az alkalmazott intézkedésnek a folyamatban lévő támadással arányosnak kell lennie és az a támadás megszakításán túli eredményre, sérelemre nem vezethet,

c) a szükséges intézkedések végrehajtásáról azonnal tájékoztatni kell a honvédelemért felelős minisztert, a Magyar Honvédség parancsnokát, valamint a KNBSZ kibertér műveleti szakfeladatokra kijelölt szervezeti egységét,

d) a támadás megszakítását követően meg kell vizsgálni a védelem fokozásához szükséges további intézkedések körét, illetve az ország védelmével összefüggő további döntések szükségességét a Magyar Honvédség parancsnokának történő egyidejű jelentéssel.

(5) A (4) bekezdés c) pontja szerinti értesítés esetén a KNBSZ kibertér műveleti szakfeladatokra kijelölt szervezeti egysége azonnal értesíti Magyarország jogszabályban kijelölt kibervédelmi szervezeteit.

(6) Külföldről érkező jelentős támadás esetén a megtett intézkedésekről és azok okairól – katonadiplomáciai úton, a külpolitikáért felelős miniszter egyidejű tájékoztatása mellett – értesíteni kell a támadók helye szerinti államot – érintettség esetén a NATO-t, az Európai Uniót, és a két- vagy többoldalú megállapodás alapján együttműködő feleket –, vagy kezdeményezni kell a hatáskörrel és illetékességgel rendelkező hatóságoknál a támadók felelősségre vonásához szükséges eljárásokat.

(7) Az (1) bekezdés c) pontja szerinti fellépésre az ott meghatározottak nemzetbiztonsági információkkal megerősített fennállása esetén – a kapcsolódó közjogi döntések keretei között –

a) szövetségi kötelezettség teljesítésének keretében,

b) nemzetközi művelettel összefüggésben, vagy

c) honvédelmi válsághelyzetben a kibervédelmi ügyeletes parancsnok döntése alapján van lehetőség.

(8) Az (1) bekezdés c) pontja szerinti fellépésre az ott meghatározottak nemzetbiztonsági információkkal megerősített fennállása esetén – a kapcsolódó közjogi döntések keretei között –

a) különleges jogrendben, valamint

b) a (7) bekezdéstől eltérő esetben a Kormány döntése alapján van lehetőség.

(9) Az (1) bekezdés c) pontja szerinti fellépés keretében megvalósuló cselekmények, intézkedések tekintetében
a) az okozott sérelemmel, vagy közvetlen fenyegetéssel arányosan kell fellépni,
b) biztosítani kell az összhangot a kapcsolódó műveleti, nemzetbiztonsági, diplomáciai érdekekkel és törekvésekkel,
c) olyan eljárásokat kell alkalmazni, amelyek a kibertéren keresztül tudják garantálni a sérelmek jövőbeni megismétlődésének megakadályozását, vagy a közvetlen fenyegetés elhárítását, és
d) figyelembe kell venni az alkalmazott módszerek és eljárások katonai szükségességét.
(10) A (7) bekezdésben meghatározott döntéshozatal rendjét a Kormány a 6. § (1) bekezdés l) pontjára figyelemmel határozza meg, különösen az elrendeléshez szükséges jelentések és információk körének, valamint a döntéshozatal folyamatának és jogosultjainak meghatározásával.
(11) Az (1) bekezdés szerinti feladatok ellátásához szükséges műveleti információkat a Honvédség kibertér műveleti erői a kibertérre irányuló önálló felderítő tevékenység, valamint a katonai egységes felderítő rendszer útján szerzik be.
(12) Az (1) bekezdés szerinti feladatok tervezése és végrehajtása érdekében az állami szervek és a 11. § (2) bekezdése szerinti állami szervnek nem minősülő, honvédelemben közreműködő szervek együttműködnek, a kapcsolódó szolgáltatási tevékenységet folytató gazdasági társaságok együttműködhetnek a Honvédség katonai kibertér műveleti erőivel."[628]

A normatív rendelkezések alapján látható tehát, hogy a kibertérben megvalósuló katonai fellépést a nemzetközi jog szabályaival és a hazai fogalomhasználattal összhangban a jogalkotó helyesen és okkal a védelemre, a támadás általi károkozás megszakítására hegyezte ki. Ez a megoldás illeszkedik a fegyveres erők feladatellátásának nemzetközi korlátozásaihoz, de ahhoz a valószínűséghez is, hogy egy jelentősebb kibertámadás soha nem önmagában való cselekmény, hanem valamely más viszonyrendszerek vagy cselekmények része, kapcsolódó tevékenysége. Nem utolsó értelmezési szempont az sem, hogy a katonai gondolkodás is elsődlegesen az összhaderőnemi harchoz – vagyis a különféle katonai szakterületek együttes műveleti fellépéséhez – kapcsolja a kibertér műveleti kérdéseket, és inkább a szakpolitika szintjén számol önálló katonai kibertér műveletek – elrettentő vagy demonstratív – lehetőségével.[629] Ennek megfelelően a szabályozás a Magyar Honvédség kibertérműveleti erőinek alapfeladatává a honvédelmi érdeket érintő támadások kivédését, elhárítását tette, míg a további fellépés vagy válaszadás lehetőségét már hazánk nemzetközi politikai törekvéseivel és nemzetbiztonsági érdekeinek mérlegelésével összehangoltan tette csak lehetővé.

Mindez azonban nem csak a kibertér műveleti képességek honvédelmi szabályozásban való újszerűsége miatt előrelépés. Jelentős ez az újítás azért is, mert egyrészről a NATO szempontjából fontos törekvési irányhoz alkalmazkodik, és eközben a hazai kiberbiztonsági fejlesztések terén is mintául szolgálhatott, amit egyes honvédelmi törvényi szabályok átvétele is mutat az egyes törvényeknek a polgárok biztonságát erősítő módosításáról szóló törvényben,[630] a polgári

628 2021. évi CXL. törvény 88. §
629 Lupovici (2011): 49–62., Bendiek–Metzger (2015), Brantly (2018): 31–54., Kovács László (2021): 119–137.
630 Vö. Egyes törvényeknek a polgárok biztonságát erősítő módosításáról szóló 2020. évi XXXI. törvény 22. § (2) bekezdés

szféra kiberbiztonsági erői tekintetében. Másrészről ez a szabályozás nem csak a konkrét – katonai és nemzetbiztonsági értelemben vett – műveleti keretekre tér ki, hanem a kibertér műveleti tevékenység kormányzati, jogi és diplomáciai sajátosságai kapcsán is előre vetíti a további fejlesztési lehetőségeket,[631] hiszen a külügyi, és a tágabb értelemben vett kormányzati felelősségek révén egyértelműen előre vetíti a kiberdiplomáciai, és különösen az attribúciós kérdések fejlesztését,[632] de végső soron további érvet adhat egy magyar kiberbiztonsági törvény kidolgozásának megkezdéséhez épp úgy, mint a védelmi-biztonsági reform kiberbiztonsági és kibertér műveleti vonatkozásainak erősítéséhez, és jövőbeni fokozásához.

3.4. A védelmi-biztonsági tevékenységek összehangolásának lehetőségei a kibertér viszonylatában

Ahhoz, hogy az előzőekben leírtakat, és általában a kibertér és a nemzeti biztonság összefüggéseit a hazai szabályozás és védelmi-biztonság működés viszonylatában megfelelően értelmezhessük, szükségszerű, hogy kitekintsünk a folyamatban lévő védelmi-biztonsági szabályozási reform[633] alapvető kérdéseire. E tekintetben a Vbö. állam- és jogrendszerben betöltött szerepének elemzése és értékelése[634] a kibertéri vonatkozásokkal kiegészítve adhat egy olyan olvasatot, amely egyrészről a 2022. november 1-je óta hatályban lévő működési rendre vetítve segít értelmezni a kibetér és a magyar nemzet biztonságának szabályozási kapcsolatait, másik oldalról pedig lehetőséget teremt további kapcsolódások vizsgálatára is.

Innen nézve tehát a Vbö. szerepének tisztázása során különféle történeti és elméleti, rendszertani vonatkozásokra építve indokolt a normatív szabályok elemzését megalapozni annak érdekében, hogy lehetőség szerint egy olyan képet kapjunk, amely a szabályozás jelen állapotában is helytálló, de az esetleges további fejlesztésekhez is alapokat tud adni. Egy ilyen szemüvegen át kialakított kép figyelemmel tud lenni egyebek mellett arra is, hogy a Vbö. bár önálló törvény, nem önmagában álló jogalkotási produktum, hanem – a jogalkotó megnyilatkozásaiból következően is, elvileg – egy védelmi és biztonsági reform-folyamat része. Ezt a reform folyamatot az Alaptörvény kilencedik módosításának indokolása a következőkkel vezette fel:

> „Az Alaptörvény kilencedik módosításával megvalósul a különleges jogrend alkotmányos szabályozásának reformja, ennek keretében pontosulnak a védelemmel és biztonsággal összefüggő alkotmányos kötelezettségek, a különleges jogrendi helyzetek változása révén az Országgyűlés kapcsolódó jogai, az országos népszavazási tárgykörök, a Magyar Honvédségre vonatkozó alkotmányos szabályozás, továbbá a katonai műveletekkel kapcsolatos döntéshozatal. A módosítás nyomán a hatályos hat helyett három esetkörre – a hadiállapotra, a szükségállapotra és a veszélyhelyzetre – változik a különleges jogrendi esetkörök rendszere, amely *egy korszerűbb, a változó biztonsági környezethez jobban al-*

631 L. Farkas Ádám (2019c): 63–79.
632 L. Molnár Anna – Molnár Dóra (2022), Mártonffy (2020): 307–320., Nyáry (2020): 321–341., Legárd (2020): 125–140., Páll-Orosz (2021): 66–84.
633 A téma kapcsán l. Kádár (2022b): 65–90., Kádár (2022a): 61–73., Kádár (2022c) Kádár (2022d): 3–19., Till (2021), Keszely–Varga (2022a), Keszely–Varga (2022b), Farkas Ádám (2022f), Farkas Ádám (2022g)
634 L. Kádár–Till (2022), Farkas Ádám (2022h), Farkas Ádám (2022i)

kalmazkodó és az elmúlt évek válságkezeléseinek tapasztalataira építő, hatékony rendszer jövőbeni kialakítását szolgálja."[635]

„A Javaslat rendszerszintű célja, hogy *a különleges jogrendi szabályozás átláthatóbb legyen, a normál jogrendi működés és válságkezelés szabályaihoz igazodva illeszkedjen a fokozatosság elvéhez* és ezáltal a legsúlyosabb kihívásokra és fenyegetésekre fókuszáljon, de mindezt korszerű módon, a változó biztonsági környezethez igazodva és a hatályos szabályozáshoz mérten további garanciák beiktatásával valósítsa meg."[636]

Erre építve a Vbö. általános indokolása úgy fogalmaz, hogy

„E törvénnyel a jogalkotó az eddigi ágazati működést kiegészíti az összkormányzati koordináció és az ágazati elhatárolást felváltó hatékony együttműködés kereteivel, kiemelt területté téve a társadalom felkészültségének és biztonságtudatosságának erősítését, továbbá a normál jogrendi válságkezelés és a különleges jogrendi szabályozás hatékonyabbá tételét. *Az Alaptörvény kilencedik módosítása és jelen törvény egy védelmi és biztonsági reform alapját teszi le*, melyre az elkövetkezendő években felépíthető lesz a technológia és a biztonsági környezet prognosztizálható változásaiból adódóan az egyes ágazatok összehangolt fejlesztése is."[637]

Ezen jogalkotói iránymutatásokat azonban már elöljáróban is érdemes kiegészíteni azzal a figyelemfelhívással, hogy a módosított, illetve az újólag megalkotott szabályozási elemekben is számos ponton közvetve vagy közvetlenül megjelent a kibertér jelentette kihívások halmaza. E körben a hadiállapot támadással egyenértékű cselekményekre való kiterjesztése, a szükségállapot korábbi szabályozásban meglévő fegyveres vagy felfegyverkezett elkövetéshez való rögzítésének korrigálása, vagy épp a Vbö. kibertér műveletekkel kapcsolatos kormányzati szabályai csak példákat tárnak elénk annak megvilágítására, hogy a jogalkotó jelentős mértékben számol(t) a védelmi-biztonsági reform során a kibertér jelentette – nem kinetikus és nem klasszikusan fegyveres – kihívásokkal és fenyegetésekkel is, miközben azokat a komplex biztonság összkormányzati szemléletébe is integrálni kívánja. Ez pedig már az elvi megközelítéstől egy normatívabb irányhoz vezet el minket, ami a Vbö. jellegéből adódóan a komplex biztonságra fókuszál, amibe a kiberbiztonság is szükségképpen beleértendő.

A Vbö. és vele a komplex biztonsághoz alkalmazkodó, átfogó szemlélet hazai szabályozási rendszerben betöltött szerepének elvi megközelítése kulcsfontosságú. Ezt segíti, hogy a Vbö. általános indokolása röviden maga is kitekint a történeti és államfejlődési előzményekre[638] a következő megfogalmazással:

„A polgári magyar állam jogfejlődésében a védelem és a biztonság kérdése meghatározó helyet foglalt el az alkotmányos fejlődés nagy fordulópontjai tekintetében, hiszen az önálló és szuverén államiság szempontjából kulcsfontosságú kérdés Magyarország védelme és a nemzet biztonságának megóvása. Ebben az évszázados fejlődésben azonban szük-

635 Kiemelés az Alaptörvény kilencedik módosításának általános indokolásából
636 Kiemelés az Alaptörvény kilencedik módosításának 11. cikkéhez készült részletes indokolásból
637 Kiemelés a Vbö. általános indokolásából
638 Bővebben l. Farkas–Kelemen (2022)

ségképpen voltak a politikatörténeti és alkotmánytörténeti sajátosságoktól függetlenül is korszakfordulók, melyek a védelem és biztonság technikai, társadalmi és ezek folytán jogi vonatkozásainak változásából következtek. 1848-ban a nemzet védelmi szabályozásának alapjait tette le a jogalkotó, majd az 1867-től kezdődő első tartós polgári parlamentáris időszakban főként szervezeti és tevékenységforma szerinti megközelítésben elkezdte felépíteni egy modern védelmi és biztonsági rendszer kereteit, kirajzolva ezzel a ma is létező főbb védelmi szervezetek elődeit. 1912-ben kialakításra került a kivételes hatalom intézménye, amely a mai különleges jogrendi szabályozás alapjait adta, majd a két világháború között megszületett a légvédelem szabályozása a hadviselés technikai feltételeinek változása miatt, megalapozva ezzel a mai polgári védelem elődintézményét. Az 1939. évi II. törvénycikkel, első nemzeti honvédelmi törvényünk megalkotásával aztán a törvényhozás jelentős szemléletváltást hajtott végre a védelem és biztonság szabályozása terén, hiszen a korábbi szervezeti, illetve tevékenységi fókuszú szabályozást felváltva az ágazati szabályozás első bástyáját építette ki, amely még a jogrendszer államszocialista átalakításában is hosszú időn át mértékadónak mutatkozott. Ekkor azonban még a rendvédelmi szervek szabályozása nem volt teljes körűen törvényi szinten garantált, míg a titkosszolgálati működés a haderő és a rendvédelem részeként valósult meg és az államszocialista fordulat szerte is foszlatta a polgári elvek szerinti törvényi szabályozási fejlődés folytatását. Az első honvédelmi törvénnyel azonban az ágazati szabályozási megközelítésnél több valósult meg, hiszen az a 20. század első felének végéig jellemző katonai dominanciájú biztonságfelfogásra figyelemmel lényegében a honvédelemre való összkormányzati felkészülés kereteit is meghatározta, vagyis az ország és a nemzet védelmét a katonai védelem ernyője alatt ugyan, de tárcákon átívelő és folyamatos feladattá tette."[639]

Ezzel a megfogalmazással a jogalkotó egy fejlődési narratívát vázolt fel, amelyben azonban a polgári alkotmányos fejlődés, és az azt kísérő komplex környezeti változás államszervezeti hatásainak mátrixa csak említés szintjén jelenik meg. Ez érthető, hiszen az indokolás nem tudományos elemzés, hanem a szóban forgó jogforrás megalkotására, céljaira irányuló értelmezési iránymutatás vagy segédlet. Ahhoz azonban, hogy a Vbö. helyét és szerepét átfogó módon tudjuk értelmezni, szükséges, hogy a tudományos vizsgálódás keretei között kitekintsünk a tágabb kontextusra is.

A 19. század második, illetve a huszadik század első felére felerősödő tudományos, technológiai, majd ezekre támaszkodó társadalmi és kulturális fejlődés – jelentékeny előzmények után,[640] de mégis koncentrált kibontakozással – rendkívül dinamikus fejlődést hozott az állam funkciói, belső strukturáltsága és nem utolsó sorban jogi karaktere tekintetében is. Hazánkban ezt az alkotmánytörténeti jelentőségű változásokkal szorosan összekapcsolódva, de az államszervezet komplexitását feltáró céllal jól példázza a szakirodalom is. Ferdinandy Gejza,[641] Tomcsányi Móricz,[642] Kmety Károly,[643] Concha Győző,[644] Egyed István[645] és szá-

639 Kiemelés a Vbö. általános indokolásából
640 A téma kapcsán l. Kelemen (2022c): 1–9., Kelemen (2017a): 81–102.
641 Ferdinandy (1902), Ferdinandy (1911)
642 Tomcsányi (1932), Tomcsányi (2018)
643 Kmety (1902), Kmety (1911)
644 Concha (1907), Concha (1905)
645 Egyed (2016), Egyed (2017)

mos más szerző vizsgálta különféle aspektusokból az államrendszert, és annak fejlődését is, kitekintve sok esetben az adott korszakban jelentkező kihívásokra, új intézményekre. Az állam funkciónak fejlődése szempontjából azonban kimagasló magyarázó erővel bír Magyary Zoltán munkássága a közigazgatás fejlődése és fejlesztése kapcsán. A változás szükségességét Magyary a közigazgatás gazdaságosságának, hatékonyságának,[646] racionalizálásának[647] vizsgálata után úgy vezette fel, hogy „Államéletünk válságát mindenki érzi, de a közvélemény még nincs eléggé, tisztában azzal, hogy ezt mi okozza. A válság lényege az, hogy a XIX. századi államnak át kell alakulnia XX. századi állammá."[648] Ennek a kihívásnak a kereteit és különösen a magyar állam funkcióinak gyarapodását Magyary példásan szemléltette a Magyar közigazgatás[649] című korszakos művében, míg az állam környezet által kikényszerített funkciógyarapodását jól szemléltette.

A Magyary által válságosnak tekintett időszak nemzeti történelmünkben a polgári alkotmányos államiság évtizedeken át tartó kibontakozásával esik egybe, amely a hatalmi ágak szétválasztására, illetve a jog által kötött államhatalmi működésre épülő berendezkedés megszilárdulásával egyébként a differenciált – tehát már nem a haderő dominanciájára épülő – és jogi keretek között egyre kiterjedtebben szabályozott védelmi szisztéma kialakulását is magában hordozta.[650] Azt mondhatjuk tehát, hogy a szóban forgó időszakban – bonyolultan egymásra ható folyamatokként – egyszerre bontakozott ki az alkotmányosan korlátozott államműködés politikai modellje, a társadalom tömegesedésre és ipari termeléssel járó körülményjavulásra épülő fejlődése, a köz- és magáncélú tevékenységeket is hatékonyabbá és gyorsabbá tevő technológiai fejlődés, valamint mindezekre reagálva az állam funkcionális és intézményi differenciálódása. A válságosság oka tehát egyfelől az államműködés környezetének és feladatrendszerének dinamikus változásából, és a „régi megoldások" ezzel való találkozásából is következett. Ez a jelenségegyüttes tehát számos vonatkozásban szükségessé tette az állam különféle feladatrendszerinek ellátása és intézményei közti koordináltabb feladatellátást, amely tendenciában a második világháború lezárultáig megkülönböztetett szerepet töltött be a katonai célú koordináció is.

Ki kell azonban emelni, hogy bár a két totális háború rendkívüli történelmi eseményként határozza meg a mai napig a 20. századról való gondolkodásunkat, nem lehet figyelmen kívül hagyni, hogy a 20. század további részében is rendkívül dinamikus fejlődés valósult meg a gazdasági, technológiai, társadalmi és biztonsági dimenziókban. Az állam és a jog a külső környezet intenzív fejlődésére és egyre sokrétűbbé válására szükségképpen meglévő működésének fejlesztésével, új funkciók azonosításával és intézményesítésével, új szabályozási keretek kialakításával reagál. Ezt a jog oldaláról a hagyományos jogterületeken túl a 19. század végétől szemlélve számos ma már bevett, vagy dinamikusan megerősödő jogterület létrejötte igazolja, melyek sorát – igaz még kezdeti állapotában, de – a védelmi és biztonsági tevékenységek koordinált ellátásának szabályozása is zárhatja, hiszen a külső környezet szinte minden változása valamiképp módot ad az újítások társadalmi rend és stabilitás sérelmével, veszélyeztetésével járó alkalmazására, vagyis védelmi reakciót, és napjainkban egyre inkább

646 Magyary (1931a)
647 Magyary (1930)
648 Magyary (1939): 3.
649 Magyary (1942)
650 Vö. Farkas Ádám (2019b)

koordinált, ágazatokon és szakterületeken átívelő reakciót indukálhat. Az államfejlődés aspektusából nézve tehát a Vbö. szerepe kapcsán felismerhető lehet, hogy amiképp sokasodnak és differenciálódnak a potenciális fenyegető és veszélyeztető cselekvési lehetőségek és az ezekre adott különböző eszköz-, módszer- és eljárásrendszerre épülő állami-társadalmi reakciók, úgy válik mindinkább fontossá az állam védelmi és biztonsági tevékenységeinek összehangolt működtetésének fokozása. Ez pedig akár egy új jogterületté is kinőhetné magát, feltéve, hogy a törvényi és szervezeti keretek mellett a szakmai és tudományos háttér is – a napi közigazgatási gyakorlat és szereplők feladatain messze túlmutató, elméleti és rendszerszemléleti mélységű önállósággal[651] – kialakításra kerül. Ennek az elméleti, tudományos és képzési vonatkozásai kapcsán Magyary szintén értékes példákat nyújthat nekünk a tudományos megalapozottság kérdésétől[652] a közigazgatási vezérkar témájáig[653] terjedően. Ezeknek ma is jelentős aktualitása lehetne, és a közigazgatáson túl akár a honvédelmi és haderőfejlesztésre, akár a rendészet, illetve a nemzetbiztonsági rendszer további fejlesztésére is termékenyítően hathatnának.

Ezt az irányultságot megerősíti az a tény is, hogy a huszadik század második felétől a biztonság felfogása és fogalma is a katonai dominanciától a komplex, szektorálisan tagolt felfogás felé mozdult el. Igaz ugyan, hogy a hidegháború katonai szembenállása és versengése – különösen a szovjet érdekszférában – továbbra is kiemelt szerepet adott a katonai védekezésnek, de az is magától értetődő, hogy ez az időszak, illetve az ezredforduló számos újszerű kihívása, és ezek mellett nem kis mértékben a kibertér dinamikus fejlődése a titkosszolgálati tevékenységek megerősítésével, illetve a stratégiai gondolkodásban mások mellett a DIME,[654] majd a MIDFIELD[655] megközelítés kibontakozását is magával hozta.

A biztonság komplex, nem katonai és nem is hagyományosan fegyveres karakterű dimenziók és szereplők sokaságára kiterjedő, a kibertér révén új érvényesülési dimenzióval – vagy domain-nel – is gyarapodó megközelítése szükségképpen magával hozza azt is, hogy az államnak polgárai és nemzetbiztonsági érdekei védelme érdekében fel kell készülnie arra, hogy az ártó törekvésekre a nem fegyveres szférákban is megfelelően, a biztonságszavatolás és a védelem elveinek is megfelelő módon, de a „civil" közeghez igazodóan tudjon reagálni.

Ezt az irányultságot jelen kötet a kibertér, a digitalizáció, az információs társadalom és a nemzeti biztonság számos-számtalan szálon történő sajátos kapcsolódásaival, úgy véljük, megfelelő módon igyekezett megvilágítani. Hasonlóan fontos azonban, hogy a védelem és biztonság-szavatolás szabályozásában is megjelenjenek a nem fegyveres elemek, kialakuljon egy egységes tervezési és képzési-felkészítési keretrendszer, illetve egy gondolati séma, amelyet a döntéshozók és a döntéseiket támogató különféle szakértők is el tudnak sajátítani. Ez egy meglehetősen jelentős kihívás, hiszen egyik oldalról a komplexitás nem oldja fel a

651 A téma kapcsán l. Farkas Ádám (2022c), Farkas Ádám (2022b)

652 Magyary (1927), Magyary (1931b), Mezey (2011)

653 Magyary (1938)

654 Amerikai betűszó, amely a stratégiai gondolkodásban a Diplomatic, Informational, Military, and Economic vagyis diplomáciai, információs, katonai és gazdasági tényezők együttes alkalmazásának megkerülhetetlenségére hívja fel a figyelmet.

655 Szintén amerikai betűszó, amely a DIME továbbfejlesztéseként is értelmezhető és lényegesen szélesíti a releváns területek körét a Military, Informational, Diplomatic, Financial, Intelligence, Economic, Law, and Development, azaz a katonai, információs, diplomáciai, pénzügyi, hírszerzési, gazdasági, jogi és fejlesztési területek összekapcsolásával.

szakterületi sajátosságokat, hanem ráépül azokra, ami azonban szükségképpen szemléleti és érdek-konfliktusokkal jár. Másik oldalról a komplex biztonsághoz alkalmazkodó gondolkodás, államszervezés és jogi szabályozás előfeltétele egy teljesen újszerű gondolkodás, amelyhez a biztonság-szavatolás fegyveres karakterű gondolati és szervezeti súlyozottsága ellenére a mintákat a civil szférából lehet meríteni. Ezek a minták a hálózatkutatás, a teljesítmény- és kreativitáskutatás területeiről, sőt a filozófiából és a politikatudományból is meríthetők. Ezt példázza Barabási-Albert László komplexitás felfogása és ennek viszonyítása az egyszerűsítéshez,[656] Christopher Andrew hírszerzés-történeti szemléletében a történeti jellegű és stratégiai távlatú gondolkodás szerepe,[657] Steven Kotler csúcsteljesítmény-kutatása[658] és ebben a specializáció megítélése, vagy épp David Epstein sokoldalúságot propagáló munkája.[659] Ha mélyebben belegondolunk azonban, akkor a filozófiai eredetek révén a generalista gondolkodás megkerülhetetlensége felé mutat az Artha-sásztra[660] épp úgy, mint Machiavelli a Fejedelemben[661] vagy épp Carl Schmitt a politikai fogalmában, különösen a partizán elméletével.[662]

A Vbö. helyének és szerepének értelmezése kapcsán tehát át kell gondolni annak a lehetőségét is, hogy amiképp a biztonság komplex tartalmúvá vált, és ezáltal nem dominálható fegyveres szemléletmóddal és karakterisztikával, úgy az összehangolt védelmi és biztonsági tevékenységhez is komplex, generális gondolkodásmód kell, ami a koordináló szakmai szerveknél sajátos elemző és javaslat-kidolgozó képességek kialakítását épp úgy indokolja, mint a koordináló – praxishoz kötött – szervektől független think tank képesség kialakítását és ezek vezetői döntéstámogatásba történő közvetlen bekapcsolását. Ez a fajta működési modell és háttér-szisztéma a külföldi mintákban Nyugaton és Keleten egyaránt azonosítható, ami azt sugallhatja, hogy az államszervezet napi működési gyakorlata megfelelő megoldásokkal összebékíthető a napi rutintól elszakadtabb, rendszerszemléletű és perspektivikus szakmai-kutatási háttér látásmódjával.

Ezt a sokrétű elvi megközelítést és alapvetést érdemes összevetni a klasszifikációs kísérletünk kapcsán már megidézett amerikai modell szemléletével, illetőleg a cyberfare state problémakörével is ahhoz, hogy lássuk, milyen horizonton és vertikumban kell gondolkodnunk akkor, amikor a kibertér komplex állami biztonság-szavatoláshoz való kapcsolódásait próbáljuk elemezni. Ez az út azonban sok éven át tartó multidiszciplináris kutatásokhoz vezet reményeink szerint, ami miatt viszont jelen kötet olvasói inkább „csak" pillanatkép érvényű válaszokat várhatnak a hazai védelmi-biztonsági szabályozás vonatkozásai és kibertéri kötődései kapcsán.

E pillanatkép megalkotásához szükségszerű a konkrét normatív kapcsolódásokra is kitekinteti. E körben magától értetődőnek mutatkozik (1) az alaptörvényi kötődések azonosítása, (2) a Vbö. önmeghatározására való kitekintés, vagyis annak azonosítása, hogy a jogalkotó a Vbö.-n belül milyen szerepet – is – tükröző rendelkezéseket helyezett el, továbbá szükséges lesz egy későbbi kutatásban annak áttekintése is, hogy (3) a Vbö. miként jelenik meg a biz-

656 Barabási (2008), Barabási (2016)
657 Andrew (2021)
658 Koetler (2021)
659 Epstein (2021)
660 Pandit (2015)
661 Machiavelli (2006)
662 Schmitt (2002)

tonság különféle dimenzióit és szektorait meghatározó törvényi szabályozásokban, különös figyelmet fordítva kibertéri kötődések átültetésére.

A Vbö. Alaptörvénnyel való összefüggései, kapcsolódásai tekintetében nehezen képzelhető el egy tételes, és főleg vitán felül álló taxáció számbavétele, hiszen a különféle alapjogok érvényesíthetőségéhez való hozzájárulástól az állami szervek működéséhez való kapcsolódáson keresztül egészen a különleges jogrendi szabályrendszerig terjedően rendkívül kiterjedt hálózatként képzelhető el az a normaösszesség, amelyhez legalább közvetett módon a Vbö. kapcsolódhat. Ezek közül számos ponton legalább közvetett mértékben feltételezhető, sőt bizonyos pontokon szükségszerűen azonosítható is a kibertéri kihívások kötődése, így jelen kötet irányultsága miatt a hangsúlyt ezen kapcsolódásokra kívánjuk helyezni.

Egy ilyen irányultságú áttekintéshez kézenfekvő elemzési iránynak mutatkozhat a törvény sarkalatossági záradékából kiindulni, hiszen az egyértelműen rögzíteni hivatott az Alaptörvény egyes kiemelt szabályozási követelményt támasztó passzusaihoz való kapcsolódást. A Vbö. 85. §-a az Alaptörvény sarkalatosságra vonatkozó követelményének való megfelelés körében

– 6. § (1) bekezdés *a)–d)* pontja és 7. §-a tekintetében az Alaptörvény XXXI. cikk (4), (5) és (6) bekezdését,
– 4. alcíme kapcsán az Alaptörvény XXXI. cikk (5) bekezdését,
– 5. alcíméhez az Alaptörvény XXXI. cikk (6) bekezdését,
– 79–81. §-aihoz az Alaptörvény 52. cikk (5) bekezdését és 54. cikk (8) bekezdését,
– 82. §-ához pedig az Alaptörvény T) cikk (1) bekezdését

jelöli meg alaptörvényi kapcsolódásként, kiegészülve a Vbö. által végrehajtott módosítások sarkalatossági kapcsolódásaival, különösen a Magyar Honvédség, a rendőrség, a nemzetbiztonsági szolgálatok, valamint az Országgyűlés viszonylatában.

Ezekhez az alaptörvényi rendelkezésekhez tehát a jogalkotó maga mondta ki az egyértelmű kapcsolódást, amelyek körében a XXXI. cikknek a honvédelmi munkakötelezettségre, a polgári védelmi kötelezettségre, valamint a gazdasági és anyagi szolgáltatás teljesítésére irányuló kötelezettségre vonatkozó szabályai kiemelt jelentőségűek a szerepmeghatározás tekintetében, hiszen ezek Vbö.-s keretei egyértelműen átfogó szerepet tükröznek azzal, hogy a korábban honvédelmi és katasztrófavédelmi szabályozásban párhuzamosan megjelenő rendelkezéseket egységes keretbe, az említett ágazatok által alkalmazandó közös szabályként rögzítette a jogalkotó. Az Alaptörvény vonatkozó szabályainak törvényi alábontásával tehát ez a kötődési keret egyértelműen mutatja az átfogó, az érintett ágazatok számára is keretet adó jelleget. Ehhez a szabályozási körhöz fontos hozzátenni, hogy jelentőségük a kibertérben zajló műveleti tevékenységek viszonylatában sem elhanyagolható, hiszen a hazai kiberökoszisztéma, illetve hazánk globális kibertérbe kapcsolódása számos hazai, de nem állami szereplő részvételével valósul meg, akikre nézve a legsúlyosabb esetekben ez a szabályozás relevanciával bírhat például egy átfogó kibertámadás esetén.

A kibertéri érintettséget tovább erősíti e körben az Alaptörvény 2022. november 1-jével hatályba lépő 52. és 54. cikkeire való hivatkozás, amelyek a különleges jogrendi szabályozás Vbö.-ben való elhelyezése miatt voltak szükségesek. Ezek kapcsán fontos kiemelni, hogy az új különleges jogrendi szabályozás a kihirdetés okai terén a biztonsági környezet differenciáltságára és dinamikus változására, ezen belül pedig magától értetődő módon a kibertérrel összefüggő kihívások változékonyságára és eszkalációs képességeire figyelemmel is törekedett rugalmasítani

a kereteket. E körben a kibertér szerepe – ahogy arra a kötet korábbi fejezeteiben már kitértünk – a szervezett bűnözői, terrorista, ellenérdekelt titkosszolgálati vagy katonai tevékenységektől a nem állami szereplők által elkövetett, de nagy hatású támadásokig terjedő széles skálán mozog, amelyekre a szabályozásnak reagálóképesnek kell lennie, különös tekintettel arra, hogy ezek pontos prognosztizálhatósága és hatóképesség-elemzése is még bizonytalanságokkal terhelt. E tekintetben tehát a Vbö. különleges jogrendi szabályozásban betöltött szerepe nem csak a biztonság komplex megközelítése terén jelenthet előrelépést a megfelelő jogalkalmazás és felkészülés esetén, hanem a komplex kibertéri kihívások és fenyegetések kezelése terén is.

A sarkalatossági kapcsolódások apropóján erőteljes alaptörvényi kötődést mutat az is, hogy a Vbö. 5. § 18. pontja védelmi és biztonsági szervezetként azonosítja a Magyar Honvédséget, a rendvédelmi szerveket, a nemzetbiztonsági szolgálatokat, valamint az Országgyűlési Őrséget, míg ugyanezen szakasz 8. pontja rendvédelmi szervként tételezi a rendőrséget, a Nemzeti Adó- és Vámhivatalt, a büntetés-végrehajtási szervezetet, valamint a hivatásos katasztrófavédelmi szervet, hogy aztán a törvény ezeknek több ponton lényegében feladatokat határozzon meg. E rendelkezés kapcsán egyértelműnek mutatkozik a Vbö. és az Alaptörvény 45. és 46. cikkei közti szoros kapcsolat, amely azáltal, hogy a feladatmeghatározást a Vbö.-ben generálisan hajta végre, és az ágazati, illetve szervezeti szabályozókban utaló megoldásoknak nyit teret, tovább erősíti az ágazatokon átívelő keretjellegű szerepértelmezést, ezzel pedig adott esetben az ágazati sajátosságok szerinti kiberbiztonsági és kibertér műveleti feladatok hatékonyabb összekapcsolásának lehetséges módozatait.

Az Alaptörvény 45. és 46. cikkeinek érintettsége egyéb okból is figyelmet érdemel. A Vbö. a védelmi és biztonsági funkciókra fókuszáló szabályozás, illetve annak az összkormányzati koordinációs megközelítése révén egyik oldalról közvetlen kapcsolatban áll a Kormánynak a Honvédség, a rendőrség és a nemzetbiztonsági szolgálatok viszonylatában fennálló működés irányítói feladatkörével. Másik oldalról azonban a védelmi és biztonsági tevékenységek összehangolásával járó azon törekvés, hogy a komplex biztonsághoz igazodó módon a kapcsolódó koordináció és kormányzati tevékenység a fegyveres szférákon messze túlmutató jelleggel valósuljon meg, egyértelműnek tűnik a Vbö. kapcsolódása az Alaptörvény 15. cikkéhez, ezen belül pedig a Kormány feladatrendszeréhez, amit a komplex biztonsághoz kapcsolódó összehangolási jellegen túl a Vbö. 46. §-a is megerősít a Kormányra irányuló rendelkezésekkel. A kibertér biztonsági vonatkozásai kapcsán ez az ágazatokon átívelő összehangoló jelleg azért is kiemelkedő fontosságú, mert a kiberbiztonság és a kibertéri műveletek technikai bázisú vonatkozásai mellett a hatékony kibertéri érdekérvényesítés szempontjából nélkülözhetetlen a különféle humán, társadalmi, állami kapcsolódások összehangolt erősítése, fejlesztése és felkészítése is, amely kapcsán a Vbö. és annak intézményi keretei egy összkormányzati keretet biztosíthatnak.

A súlyozottnak tekintett alaptörvényi vonatkozások mellett jelen keretek között arra vállalkozhatunk, hogy azokat a főbb törvényi elemeket azonosítsuk még, amelyek a szerepmeghatározás vagy szerepértelmezés szempontjából kiemelt jelentőséggel bírhatnak, és a kibertér biztonsági vonatkozásai terén is jelentős elemként ragadhatók meg.

E vállalásunk vonatkozásában a konkrét jogszabályhelyeket megelőzően már a *preambulum* is irányt mutat számunkra. Akkor ugyanis, amikor a preambulum úgy szól, hogy

„Az Országgyűlés
Magyarország és a magyar nemzet védelme, biztonságának fenntartása, fejlesztése és ezekkel összefüggő érdekeinek érvényesítése,

az erre hivatott képességek összehangolt és hatékony irányítása és működtetése,
a 21. századi biztonsági környezet sokrétű és összetett kihívásainak és fenyegetéseinek kezelhetősége,
a természeti, a civilizációs eseményekkel, továbbá az emberi cselekményeken alapuló fenyegető, ártó, befolyásoló, támadó magatartásokkal szembeni összehangolt felkészülés és védekezés, valamint
a válságkezelés és a különleges jogrend idejével összefüggő feladatok átfogó megközelítésének erősítése
érdekében"[663]

alkotta meg a Vbö.-t, lényegében előirányozta annak rendeltetését, kiemelve e körben a szabályanyag megfelelő alkalmazásával elérni kívánt főbb célokat. Ezzel egyértelműen egy olyan célrendszert azonosít, amely a biztonság átfogó, passzív – tehát védekezésen – és aktív – tehát érdekérvényesítésen – alapuló fenntartását és fokozását kívánja előmozdítani a különféle ezzel összefüggő állami funkciók hatékonyabb működés-koordinációjával és összehangolásával. Az első két tétel a Vbö. szerepének meghatározása kapcsán kiemelt fontosságú, hiszen a védelem és a biztonság fenntartása, illetőleg fejlesztése a kapcsolódó érdekek érvényesítésével együtt jelenik meg, hogy aztán elvárásként fogalmazódjon meg az erre hivatott képességek összehangolt és hatékony irányítása, működtetése. Ez a kibertér vonatkozásában egyértelműen kulcsjelentőségű annak sokrétűsége és differenciált felhasználhatósága miatt, amire már a társadalmi, állami vonatkozásokon túl az EU-s és NATO-s kapcsolódások terén épp úgy rámutattunk, mint jelen részben a titkosszolgálati és a honvédelmi kapcsolódások terén. Fontos kiemelni, hogy a preambulum ezen megközelítése a biztonság teljes spektrumára kiterjedő összhang-fokozást és irányítást tükröz, ami szükségképpen magával hozza azt az értelmezést, hogy ennek érdekében a jogalkotó a Vbö.-ben az érintett szakterületek szabályozására ráépülő, többlet követelményeket, feladatokat és működési kereteket határoz meg. Innen nézve tehát a Vbö. rendelkezései a kibertérrel összefüggő ágazati specialitásokra, illetve a sajátos szabályozásra is ráépülő elemként értelmezhető, ami a kormányzás politikai szintjén, illetve az azt segítő szakmai, de központi szintű döntéselőkészítés terepén is előmozdíthatja a kibertérrel összefüggő vonatkozások megfelelő összhangját és rendszerszerűvé tételét a hazai védelmi-biztonsági szisztémában.

A preambulumot követően a jogalkotó a Vbö. 1. §-ában rögzítette, hogy

„Magyarország védelme és biztonsága nemzeti ügy, amelyen a nemzet fennmaradása és fejlődése, a közösségi és az egyéni jogok érvényesülése alapszik, ezért *a magyar nemzet védelmével és biztonságának fenntartásával és fejlesztésével összefüggő jogszabályi rendelkezéseket e törvényre figyelemmel kell meghatározni*."[664]

E rendelkezéssel kapcsolatban persze felhívható lenne a figyelem arra, hogy a jogforráshierarchia értelmében a Vbö. egy törvény a többi közül, vagyis nem helyezheti a jogalkotó sem – alaptörvény-konform módon – a többi vonatkozó törvényi rendelkezés fölé. Ez az állítás természetesen igaz, bár kiemelése szükségtelen, hiszen a rendelkezés nem pozícionálja magasabbra a

663 Kiemelés a Vbö. preambulumából
664 Vbö. 1. §

Vbö.-t a jogforráshierarchiában. A rendelkezés lényege egy olyan kötelezettség meghatározása, amelyet a jogalkotó magára nézve is, de a jogszabályok előkészítésének folyamatából következően szükségképpen a Kormányra, illetve annak szakosított szerveire nézve súlyozva abban határoz meg, hogy a Vbö. elfogadását és hatálybalépését követően a kapcsolódó jogszabályok kialakítása a Vbö.-re figyelemmel kell elvégezni. Ez természetesen nem szigorú alkalmazkodást irányoz elő, hiszen a Vbö. figyelembevételét határozza meg, egyértelművé teszi azonban, hogy a preambulumban, illetve az alaptörvényi kapcsolódások szellemében meghatározott hatékonysági, és ezáltal széles értelemben vett biztonsági célok csak akkor érhetők el, ha a Vbö. által megjelenített új, összkormányzati védelmi és biztonsági szabályokhoz a kapcsolódó ágazati, szervezeti, szakterületi rendelkezések megfelelően alkalmazkodnak a jövőben. Ez a rendelkezés a kibertérrel összefüggő védelmi és biztonsági vonatkozások terén egyaránt érintheti a már meglévő ágazati szabályozások jövőbeni fejlesztését, illetve egy esetlegesen megalkotásra kerülő új kiberbiztonsági törvény tartalmát is, ami meglátásunk szerint előnyös változást hozhat a kiberbiztonság és kibertér műveleti szabályozás jelenlegi fragmentált és laza kooperációkra épülő fejlődésében.

A magyar jogrendszerből ez eddig – az Alaptörvény I. cikkében szereplő védelmi kötelezettség meglehetősen absztrakt keretét ide nem értve – hiányzó védelmi és biztonsági rendszerszint jelleget a Vbö 3. §-ával is egyértelműen megerősítette a jogalkotó. Ezzel ugyanis az (1) bekezdésben egyik oldalról kimondta, hogy az egymástól külön funkcionális, ágazati és szervezeti rendszereket képező katonai védelem, rendvédelem és nemzetbiztonsági tevékenységek együtt alkotják az állam fegyveres védelmének szisztémáját, másik oldalról pedig a (2) bekezdéssel egyértelműen rögzítette, hogy a közigazgatási szervek kötelesek együttműködni ezekkel a törvény 1. §-ában meghatározott célok érdekében. Ezzel a Vbö. egyértelműen, és a feladatszabás jellegét tekintve az ágazati/szakterületi szabályozáshoz mérten felülről, átfogó jelleggel kapcsolta össze a védelem és biztonság-szavatolás kulcs szereplőit az állami szférában mind a fegyveres, mind pedig a nem fegyveres karakterű szereplők tekintetében, méghozzá egy Vbö. specifikus együttműködési kötelezettség meghatározásával. Ez a megoldás nem idegen a magyar jogrendszertől, hiszen a feladatrendszerrel összefüggő, mégis tág együttműködési kötelezettség megjelenik a honvédelmi törvényben,[665] a rendőrségről szóló törvényben,[666] illetve a nemzetbiztonsági szolgálatokról szóló törvényben[667] is. Ez a megoldás tovább erősíti azt a szerepértelmezést, miszerint a Vbö. egyik oldalról összekapcsolja az érintett ágazatokat, másik oldalról azonban ráépítkezik azokra, és egyúttal új, az ágazati feladatellátás feletti, összkormányzati érdekű feladatokat is képez azok számára. Ez a vonatkozás a kibertér viszonylatában kiemelt jelentőséggel bírhat, hiszen egyik oldalról a kibertérben zajló cselekmények egyre több állam stratégiai deklarációi alapján válthat ki a fegyveres szervek által foganatosított választ, másik oldalról azonban a kiberbiztonság jellemzően nem fegyveres karakterisztikájú, amely kettősség a maga teljességében tud a Vbö. megközelítésébe beépülni, és ezzel a hazai kiberbiztonsági és kibertér műveleti szabályozás terén új kooperációs és összehangolt szabályozás- és működés-fejlesztési perspektívákat megnyitni.

665 L. pl. a honvédelemről és a Magyar Honvédségről szóló 2021. évi CXL. törvény 6. címét, 11. § (1) beklezdés c) pontját, valamint 58. § (2) bekezdését

666 L. pl. a rendőrségről szóló 1994. évi XXXIV. törvény 2. § (2) bekezdés a) pontját, 2. § (4) bekezdését, valamint 7/F-7/G. §-ait

667 L. pl. a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény 9. § a) pontját, valamint 28. § (2) bekezdését

A Vbö. összehangoló és összekapcsoló keretet adó szerepénél erősebb, összkormányzati szintű feladathatározó jellegét erősíti megítélésünk szerint a törvénynek a védelmi és biztonsági tervezésre vonatkozó szabályanyaga is. Ezt erősíti a 20. § (2) bekezdés azon rendelkezése, miszerint

> „A védelmi és biztonsági tervezési rendszer rendeltetése a védelmi és biztonsági szervezetek, valamint a védelmi és biztonsági feladatok ellátásában részt vevő, Kormány irányítása alatt álló szervek eseménykezelésre való felkészítése, kapcsolódó működésük, fejlesztésük stratégiai meghatározása és az együttműködés kereteinek biztosítása."[668]

E rendelkezésben ugyanis a stratégiai meghatározás többet feltételez a magyar nyelv szabályai szerint mint iránymutatást. Ezt az értelmezést pedig tovább erősíti ugyanezen szakasz (3) bekezdése, amikor kimondja, hogy a

> „védelmi és biztonsági tervezési rendszerben központilag meghatározott szempontrendszer szerint, ágazatilag elkülönülten, de kormányzati szinten összehangolt módon, a költségvetési források tervezésére is kiterjedő stratégiai és végrehajtási szintű tervdokumentumok kerülnek kialakításra."[669]

Ezzel ugyanis a jogalkotó egyértelműen azt határozta meg, hogy a különféle tervezési és policy jellegű dokumentumok kialakításához imperatív módon legyen egy központi követelménytámasztás, ami szükségképpen több mint koordinatív összehangolás. Ez a fajta megközelítés a kiberbiztonság terén komoly előrelépéseket indukálhat, hiszen hazánk kiberbiztonsági stratégiája mind a magasabb szintű stratégiák megújulása, mind pedig a környezet változása miatt már megérett a megújításra, amely cselekvésnek azonban már ebbe az új tervezési keretrendszerbe, és ezáltal egy rendszerszerű megközelítésbe is illeszkednie kell.

Az eddigiekben rögzítetteken túl azonban a Vbö. koordinatív keretadó jellegén túlmutató, sajátos, összkormányzati szintű, védelmi és biztonsági fókuszú szakmai irányítást megalapozó jellegét legjobban a Kormány Vbö. szerinti feladatai tükrözik. E feladatrendszerben ugyanis vannak a Kormány önmaga működésére vonatkozó koordinatív tételek, de ezeken túlmenően vannak egyértelműen kötelezéssel, irányítással járó elemek is, amelyek felvezetése is irányítási fókuszú a következők szerint: „A Kormány a védelmi és biztonsági feladatok összehangolt irányítása és ezzel összefüggésben a Kormány irányítása alá nem tartozó szervekkel való együttműködés biztosítása érdekében"[670] látja el a törvény 46. §-ában szereplő feladatokat. E körben a kiberbiztonság hatékonyabb nemzeti biztonsági integrációját és egyúttal kooperatív garantálását egyértelműen segíthetik a következő kormányzati feladatok a Vbö. felsorolásából:

> „a) az Országgyűlés elé terjeszti a Biztonság- és Védelempolitika Alapelveiről szóló határozati javaslatot és irányítja a védelmi és biztonsági célú tervezés további dokumentumainak kidolgozását, (…)
> c) meghatározza a Kormány tagjainak és a Kormány irányítása alá tartozó állami szerveknek a védelmi és biztonsági célú felkészítéssel és feladatellátással összefüggő feladatait; (…)

668 Vbö. 20. § (2) bekezdés
669 Vbö. 20. § (3) bekezdés
670 Vbö. 46. §

h) meghatározza a nemzeti ellenálló képesség fejlesztésének programját és irányítja annak összehangolt végrehajtását,

i) meghatározza a Honvédség, a rendvédelmi szervek, a nemzetbiztonsági szolgálatok összehangolt felkészülésének és feladatellátásának fő irányait, valamint az ezekkel összefüggő kivételes döntéshozatal kereteit,

j) meghatározza a katonai és a polgári kibertér műveleti erők védelmi, támadásmegelőzési és nemzetközi műveletekkel, továbbá felkészüléssel összefüggő feladatait, valamint az ezekkel összefüggő kivételes döntéshozatal kereteit."[671]

Az „irányítja" és a „meghatározza" fordulatokkal a jogalkotó egyértelműen a Kormány működés irányítási, illetve államigazgatási csúcsszervi minőségére kívánt építeni, ami messze túlmutat a koordináció inkább mellérendeltségre épülő keretein. Ezek kapcsán fontos arra is felhívni a figyelmet, hogy a fent kiemelt feladatok mindegyike jelentős lehet a kiberbiztonságot érintő hatékonyabb állami és állami-társadalmi működés hazai vonatkozásaiban, kiemelve, hogy a jogalkotó fontosnak tartotta külön egységes alapra helyezni a Vbö. keretei között a katonai és a polgári kibertér műveleti erők feladatainak kérdését, amely egyértelmű ernyőként szolgál az előzőekben áttekintett nemzetbiztonsági és honvédelmi vonatkozásokhoz.

Ezekhez a konkrét kötődésekhez pedig célszerű hozzávenni, hogy a Vbö. a tervezés, felkészülés, összkormányzati kiterjedtségű védelmi-biztonsági szakigazgatás, illetve a normál jogrendi válságkezelés, a NATO válságreagálási rendszer szabályai, valamint a különleges jogrendi szabályanyagok révén is további számos-számtalan közvetett kötődési pontot biztosít a kiberteret érintő biztonsági tevékenységek hazai fejlesztéséhez és koordináltabb megvalósításához.

Mindezek a szerepértelmezések azonban alapvetően elvi jellegűek, ami egyfelől a történeti és biztonságfogalmi aspektus elméletiségéből épp úgy következik, mint abból a tényszerűségből, hogy a Vbö. rendelkezéseinek értelmezéséből felállított szerepmeghatározás is alapvetően a Vbö. alkalmazása, különösen a kormányzati és az azt jelentős mértékben meghatározó döntés-előkészítő jellegű alkalmazásba vétele révén tud majd kiteljesedni. E tekintetben tehát mindazon újítások, történelmi jelentőségek, illetve állam- és jogrendszerben betöltött szerepelemek, amelyeket jelen fejezet felvázolt, hipotézisnek tekinthetők, amit elsődlegesen a védelmi és biztonsági igazgatás központi szervének tevékenysége, és annak állami és nem állami fogadtatása és kapcsolódásai, illetve kormányzati támogatottsága tud majd visszaigazolni a valóságban. A Vbö. helye és szerepe a jogrendszerben tehát úgy is mondhatnám, hogy egy történelmi távlatokban is korszakos ígéret, amelyet az alkalmazás válthat be, és akkor egy új korszakba léphet Magyarország védelmi és biztonsági rendszere a szabályozáson messze túlmutató kontextusba szemlélve is, méghozzá a kibertérrel összefüggő megannyi biztonsági teendő tekintetében is. Ez utóbbi kapcsán azonban arra is fel kell hívni a figyelmet, hogy az összkormányzati szint mellett talán nagyobb a szerepe az ágazati, speciális szervezeti szereplőknek, hiszen az ő megfelelő felzárkózásuk és mégis együttműködésre való nyitottságuk nélkül nehezen képzelhető el a gyorsan és jelentősen változó közeghez igazodni képes megfelelő szabályozási keret a magyar kiberbiztonság számára, ami jogállami keretek között azt is jelenti, hogy nehezen lesz elképzelhető a korszerű és hatékony működés-együttműködés a hazai kiberbiztonság terén.

671 Vbö. 46. §

Felhasznált irodalom

Acsai (2020) = Acsai György: Cybercrime. In: Ruzsonyi Péter (szerk.): *Közbiztonság. Fenntartható biztonság és társadalmi környezet tanulmányok III.* Budapest, Ludovika Egyetemi Kiadó, 2020. 1484–1500.

Ágota–Kassai–Tóth (2013) = Ágota András – Kassai Károly – Tóth Gergely: A kiberkonfliktusok aktuális kérdései, nemzetközi kitekintésben. *Sereg Szemle* 2013/2–3. 184–197.

Aiken (2020) = Mary Aiken: *Cyber-csapda – Hogyan változtatja meg az online tér az emberi viselkedést*, Budapest, Harmat – Új Ember Kiadó, 2020.

Almási (2009) = Almási Ferenc: A nemzetközi humanitárius jog alkalmazását érintő kihívások az informatikai és technológiai fejlődés, valamint a magánszféra katonai célú bevonásának következtében. In: Ádány Tamás – Bartha Orsolya – Törő Csaba (szerk.): *A fegyveres összeütközések joga*. Budapest, Zrínyi Kiadó, 2009. 283–309.

Ambrus (2021) = Ambrus István: *Digitalizáció és büntetőjog.* Budapest, Wolters Kluwer Hungary, 2021.

Andrew (2018) = Christopher Andrew: *The Secret World. A History of Intelligence.* New Heaven and London, Yale University Press, 2018.

Andrew (2021) = Christopher Andrew: *Titkos világ I–II.* Budapest, Európa Könyvkiadó, 2021.

Ansah (2010) = Tawia Ansah: Lawfare: A Rhetorical Analysis. *Case Western Reserve Journal of International Law*, 2010/1. 87–119.

Aral (2020) = Sinan Aral: *The Hype Machine: How Social Media Disrupts Our Elections, Our Economy, and Our Health--and How We Must Adapt.* New York, Currency, 2020.

Arató et al. (2022) = Arató Nikolett – Zsido András Norbert – Rivnyák Adrienn – Péley Bernadett – Lábadi Beatrix: Risk and Protective Factors in Cyberbullying: The Role of Family, Social Support and Emotion Regulation. *International Journal of Bullying Prevention,* 2022/4. 160–173.

Armour (2012) = Ian D. Armour: *A History of Eastern Europe 1740–1918 – Empires, Nations and Modernisation*, London, Bloomsbury Academic, 2012.

Aro (2021) = Jessika Aro: *Putyin trolljai – Igaz történetek az orosz infoháború frontvonalából*. Budapest, Corvina, 2021.

Árvai–Gyaraki (2019) = Árvai Zoltán – Gyaraki Károly: *100 éves az önálló magyar katonai felderítés, hírszerzés és elhárítás 1918–2018.* Budapest, Zrínyi Kiadó, 2019.

Árva–Pásztor–Pyanatova (2019) = Árva László – Pásztor Szabolcs – Victoria Pyanatova: A multinacionális vállalati stratégiák és a változó világkereskedelem kapcsolatáról. *Gazdaság és Pénzügy*, 2020/1. 57–81.

Ash (2022) = Timothy Garton Ash: *Szólásszabadság.* Budapest, Európa Könyvkiadó, Budapest, 2022.

Assa (2011) = Haim Assa: *Cyberspace and its effect on cultural-political and social processes.* Tel Aviv, Tel Aviv University, 2011.

Atkinson (2015) = Sean Atkinson: Psychology and the hacker – Psychological Incident Handling. *SANS Whitepaper,* 2015.
giac.org/paper/gcih/20948/psychology-hacker-psychological-incident-handling/129780

Babos (2011) = Babos Tibor: „Globális közös terek" a NATO–ban. *Nemzet és biztonság* 2011/3. 34–46.

Bachmann–Gunneriusson (2015) = Sascha-Dominik Bachmann – Hakan Gunneriusson: Hybrid Wars: The 21st Century's New Threats to Global Peace and Security. *South African Journal of Military Studies,* 2015/1. 77–98.

Bachmann–Mosquera (2015) = Sascha Dov Bachmann – Andres B. Munoz Mosquera: Lawfare and hybrid warfare – how Russia is using the law as a weapon. Amicus Curiae. *Journal of the Society for Advanced Legal Studies*, Summer 2015. 25–28.

Baer–Koponen (2022) = Katarina Baer – Kalle Koponen: *Kínai való világ – A legjobban kontrollált ország.* Budapest, HVG könyvek, 2022.

Bagge (2019) = Daniel P. Bagge: *Unmasking Maskirovka: Russia's Cyber Influence Operations.* New York, Defense, 2019.

Bainbridge (2020) = William Sims Bainbridge: *The Social Structure of Online Communities*. Cambridge, Cambridge University Press, 2020.

Baji (2014) = Baji Péter: Az internet, a tér és az új gazdaság Budapesten. *Tér,* 2014/4. 117–137.

Balaban–Mielniczek (2019) = Mariusz Balaban – Pawel Mielniczek: Hybrid Conflict Modeling. In: *WSC ,18: Proceedings of the 2018 Winter Simulation Conference.* Gothenburg. IEEE, 2019. 3709–3720. dl.acm.org/doi/proceedings/10.5555/3320516

Balogh–Till (2022) = Balogh András József – Till Szabolcs: Új szabályozás – régi gondolatok, avagy aktuális kérdések a (hon)védelmi tevékenység hatékonyságának jogi alapjai kapcsán: A honvédelem közjogi kereteinek kapcsolódása a védelmi és biztonsági reformhoz. *Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok* 2022/29. 1–43.

Bányász (2015) = Bányász Péter: A terrorizmus jelenléte a közösségi médiában. In: Bányász Péter – Kiss Dávid – Orbók Ákos (szerk.): *Hadszíntér előkészítés, létfontosságú rendszerelemek védelme, honvédelmi érdekek érvényesítése: Poszterkiadvány.* Budapest, Magyar Hadtudományi Társaság, 2015.

Bányász (2016) = Bányász Péter: A közösségi média szerepe a lélektani műveletekben az elmúlt időszak válságainak tükrében. *Szakmai Szemle,* 2016/1. 61–81.

Bányász (2017a) = Bányász Péter: A közösségi média mint az információs hadszíntér speciális tartománya. *Hadmérnök*, 2017/II. különszám. 108–121.

Bányász (2017b) = Bányász Péter: Kiberbűnözés és közösségi média. *Nemzetbiztonsági Szemle,* 2017/4. 55–74.

Bányász–Krasznay–Tóth (2021) = Bányász Péter – Krasznay Csaba – Tóth András: A NATO kibervédelmi szakpolitikája. In: Szenes Zoltán (szerk.) *A mai NATO: A szövetség helyzete és feladatai.* Budapest, HM Zrínyi Térképészeti és Kommunikációs Szolgáltató Nonprofit Kft., 2021. 130–149.

Barabási (2011) = Barabási Albert-László: A gyenge kapcsolatok stabilizálják a komplex rendszereket. In: Varga V. Attila (szerk.): *Társadalmi kapcsolathálózatok elemzése*. 2011. dtk. tankonyvtar.hu/xmlui/bitstream/handle/123456789/7380/0010_2A_08_Kapcsolathalo_elemzes_szerk_Takacs_Karoly.pdf?sequence=1&isAllowed=y

Barabási (2016) = Barabási Albert-László: *A hálózatok tudománya.* Budapest, Libri Könyvkiadó, 2016.

Barabási (2018) = Barabási Albert-László: *Behálózva.* Budapest, Libri Kiadó, 2018.

Barabási (2020) = Barabási Albert-László: *Behálózva – A hálózatok új tudománya.* Budapest, Libri Kiadó, 2020.

Baranyi et al. (2021a) = Baranyi Péter – Csapó Ádám – Budai Tamás – Wersényi György: Introducing the Concept of Internet of Digital Reality – Part I. *Acta Politechnica Hungarica,* 2021/7. 225–240.

Baranyi et al. (2021b) = Baranyi Péter – Csapó Ádám – Budai Tamás – Wersényi György: Internet of Digital Reality: Infrastructural Background – Part II. *Acta Politechnica Hungarica,* 2021/8. 91–104.

Barber (2001) = Richard Barber: Hackers Profiled – Who are they and what are their motivations? *Computer Fraud&Security*, 2001/2. 14–17.

Barna (2013) = Barna Attila: „Kik a' Király' és Haza ellen való hűtlenséggel vádoltatnak": Az 1830. évi büntetőkódex-tervezet felségsértésre és hűtlenségre vonatkozó szabályainak megalkotása. In: Máthé Gábor – Révész T. Mihály (szerk.): *Állam–, egyház–, jogtörténeti*

magyarázatok: Ünnepi tanulmányok Rácz Lajos tiszteletére 65. születésnapja alkalmából, Budapest, Multiszolg Bt., 2013. 9–16.

Barna (2017) = Barna Attila: Rendes és rendkívüli bíróságok a hűtlenségi perek perjogi szabályozásában és ítélkezésében a középkori Magyar Királyság felosztásáig. *Jogtörténeti Szemle,* 2017/1–2. 51–57.

Barnet (1985) = Richard J. Barnet: The Ideology of the National Security State. *The Massachusetts Review,* 1985/4. 483–500.

Bartkó (2017a) = Bartkó Róbert: Challenges of fight against terrorism with reference to the last amendment of the New Hungarian Criminal Code. *Polish Political Science Yearbook,* 2017/1. 315–327.

Bartkó (2017b) = Bartkó Róbert: Az Európai Unió büntetőjogi reformja a terrorizmus elleni küzdelemben. *Ügyészek Lapja,* 2017/3–4. 5–18.

Bartkó (2019) = Bartkó Róbert: A hazai polgári nemzetbiztonsági szolgálatok a terrorizmus elleni küzdelemben. *Katonai Jogi és Hadijogi Szemle,* 2019/2. 37–57.

Bartkó–Gál (2022) = Bartkó Róbert – Gál István László: A kibertérben megjelenő büntetőjogi kihívások és fenyegetések büntetőjogi kezelésének tendenciái. *Military and Intelligence CyberSecurity Research Paper* 2022/12. 1–30.

Bartkó–Sántha (2018) = Bartkó Róbert – Sántha Ferenc: Az Európai Unió jogalkotása és hatása a terrorcselekmény hazai büntetőjogi szabályozására. In: Homoki–Nagy Mária (szerk.): *Ünnepi kötet Nagy Ferenc egyetemi tanár 70. születésnapjára.* Szeged, SZTE ÁJK, 2018. 83–100.

Batty (1997) = Michael Batty: Virtual Geography. *Futures*, 1997/4–5. 337–352.

Beláz–Berzsenyi (2017) = Beláz Annamária – Berzsenyi Dániel: Kiberbiztonsági Stratégia 2.0 – A kiberbiztonság stratégiai irányításának kérdései. *Stratégiai Védelmi Központ Elemzések,* 2017/3. 1–15.

Beláz–Krasznay–Szabó (2020) = Beláz Annamária –Krasznay Csaba –Szabó Zsolt: Cybersecurity Strategy and Leadership Managment Issues. In: Živan Živković (szerk.): *An international serial publication for theory and practice of Management Science – IMCSM Proceedings (2020)*, Bor, University of Belgrade, Technical Faculty in Bor, Engineering Management Department (EMD), 2020. 242–252.

Bell (2007) = David Bell: *Cyberculture Theorists – Manuel Castells and Donna Haraway*. London – New York, Routledge, 2007.

Bellamy (2016) = Christopher Bellamy: *The Evolution of Modern Land Warfare*. London – New York, Routledge, 2016.

Bendiek–Metzger (2015) = Annegret Bendiek – Tobias Metzger: Deterrence theory in the cyber-century. *Working Paper RD EU/Europe*, 2015/02. Berlin, German Institute for International and Security Affairs, 2015.

Bereczkei (2008) = Bereczkei Tamás: *Evolúciós pszichológia*. Budapest, Osiris kiadó, 2008.

Bereczkei–Plég–Csányi (2001) = Bereczkei Tamás – Plég Csaba – Csányi Vilmos: *Lélek és evolúció – Az evolúciós szemlélet és a pszichológia*. Budapest, Osiris kiadó, 2001.

Béres (2018a) = Béres János (szerk.): *A Válogatás a magyar katonai felderítés és hírszerzés történetéből: szemelvénygyűjtemény, 1918–2018.* Budapest, Katonai Nemzetbiztonsági Szolgálat, 2018.

Béres (2018b) = Béres János (szerk.): *Külföldi nemzetbiztonsági szolgálatok.* Budapest, Zrínyi Kiadó, 2018.

Bérzina (2019) = Ieva Bérzina: Total Defence as a Comprehensive Approach to National Security. In: Nora Vanaga – Toms Rostoks (szerk.): *Deterring Russia in Europe. Defence Strategies for Neighbouring States.* London, Routledge, 2019. 71–90.

Bhuyan (2021) = Bhuyan Atanu Bhuyan: Designing optimal welfare policies for intermediate public transportation systems: A developing country perspective. *Academia Letters,* 2021. academia.edu/44905958/Designing_optimal_welfare_policies_for_intermediate_public_transportation_systems_A_developing_country_perspective

Bibó (1979) = Bibó István: A magyar társadalomfejlődés és az 1945. évi változás értelme (1947). *Magyar Füzetek,* 1979/4. 79–93.

Blount (2016) = P. J. Blount: *Reporgramming the World: Cyberspace and the Geography of Global Order* (disszertáció). Newark, The State University of New Jersey, 2016.

Boda (2016) = Boda József: *„Szigorúan Titkos!"? Nemzetbiztonsági almanach.* Budapest, Zrínyi Kiadó, 2016.

Bodó et al. (2020) = Bodó Attila Pál – Palicz Tamás – Joó Tamás – Deák Veronika (szerk.): *Az IBTV. gyakorlata: Éves továbbképzés az elektronikus információs rendszerek védelméért felelős vezető számára* 2020. Budapest, Nemzeti Közszolgálati Egyetem Közigazgatási Továbbképzési Intézet, 2020.

Bőgel (2015) = Bőgel György: *A big data ökoszisztémája.* Budapest, Typotex, 2015.

Brantly (2018) = Aaron F. Brantly: The Cyber Deterrence Problem. In: T. Minárik – R. Jakschis – L. Lindström (szerk.): *2018 10th International Conference on Cyber Conflict.* Tallinn, NATO CCD CoE, 2018. 31–53.

Brantly–Cal–Winkelstein (2017) = Aar Aaron F. Brantly – Nerea M. Cal – Devlin P. Winkelstein: *Defending the Borderland – Ukrainian Military Experiences with IO, Cyber, and EW.* Army Cyber Institute at West Point, West Point, 2017.

Brattberg–Maurer (2018) = Erik Brattberg – Tim Maurer: *Russian Election Interference – Europe's Counter to Fake News and Cyber Attacks.* Washington, Carnegie Endowment for International Peace, 2018.

Braudel (2008) = Fernand Braudel: *A kapitalizmus dinamikája.* Budapest, Európa Könyvkiadó, 2008.

Briggs (2006) = Asa Briggs: The Welfare State in Historical Perspective. In: Christopher Pierson –Francis G. Castel (szerk.): *The Welfare State Reader (Second Edition).* Cambridge, Polity Press, 2006. 16–29.

Brown (2008) = Cody M. Brown: *The National Security Council. A Legal History of the President's Most Powerful Advisers.* Washington, Project On National Security Reform Legal Working Group, 2008.

Bucko et al. (2021) = Boris Bucko – Martin Michálek – Katarina Papierniková – Katarína Zábovká: Smart Mobility and Aspects of Vehicle-to-Infrastructure. *Applied Sciences,* 2021/11. 1–18. mdpi.com/2076-3417/11/22/10514/htm

Budai (2017) = Budai Balázs: *Az e–közigazgatás fogalma, jogi és stratégiai keretei.* Budapest, Dialóg Campus, 2017.

Budavári (2023) = Budavári Krisztina: A védelmi ipar és a nemzetbiztonság kapcsolata az aktuális 21. századi környezetben. *Nemzetbiztonsági Szemle* 2023/1. 34–48.

Buzan–Waever–Wilde (2006) = Barry Buzan – Ole Waever – Jaap De Wilde: A biztonsági elemzés új keretei. In: Póti László (szerk.): *Nemzetközi biztonsági tanulmányok. Önértelmezés és viták a hidegháború utáni korszakban.* Budapest, Zrínyi Kiadó, 2006. 53–112.

Camus (1965) = Albert Camus: A pestis. In: Köpeczi Béla (szerk.): *Az egzisztencializmus.* Budapest, Gondolat Kiadó, 1965. 379–388.

Carrapico–Barrinha (2018) = Helena Carrapico – Andre Barrinha: European Union Cyber Security as an Emerging Research and Policy Field. *European Politics and Society,* 2018/3. 299–303.

Castells (2005) = Manuel Castells: *A hálózati társadalom kialakulása.* Budapest, Gondolat Kiadó, 2005.

Castells (2006) = Manuel Castells: *Az információ kora: Gazdaság, társadalom és kultúra – Az identitás hatalma.* Budapest, Gondolat Kiadó, 2006.

Castells (2007) = Manuel Castells: *Az információ kora: Gazdaság, társadalom és kultúra III. kötet – Az évezred vége*. Budapest, Gondolat Kiadó, 2007.

Castells (2010) = Manuel Castells: *The Information age – Economy, Society, and Culture – Volume I. The Rise of the Network Society (second edition).* Oxford, Blackwell Publishing,2010.

Cattaruzza (2020) = Amaël Cattaruzza: *A digitális adatok geopolitikája.* Budapest, Pallas Athéné Könyvkiadó, 2020.

Cavanagh (2007) = Allison Cavanagh: *Sociology in the Age of the Internet.* Maidenhead, McGrawHill Open University Press, 2007.

Cendic–Gosztonyi (2020) = Kristina Cendic – Gosztonyi Gergely: Freedom of Expression in times of Covid-19: chilling effect in Hungary and Serbia. *Journal of Liberty and International Affairs, Institute for Research and European Studies – Bitola,* 2020/6. 14–29.

Check (2015) = Terence Check: Book Review: Analyzing the Effectiveness of the Tallinn Manual's Jus Ad Bellum Doctrine on Cyberconflict: A NATO–Centric Approach. *Cleveland State Law Review,* 2015/2. 495–513.

Chiesa–Ducci–Ciappi (2009) = Raoul Chiesa – Stefania Ducci – Silvio Ciappi: *Profiling Hackers - The Science of Criminal Profiling as Applied to the World of Hacking.* Boca Raton, Taylor & Francis Group, 2009.

Chng et al. (2022) = Samuel Chng – Han Yu Lu – Ayush Kumar – David Yau: Hacker types, motivations and strategies: A comprehensive framework. *Computers in Human Behavior Reports,* 2022/5. 1–8.

Christakis–Fowler (2010) = Nicholas A. Christakis – James H. Fowler: *Kapcsolatok hálójában: Mire képesek a közösségi hálózatok, és hogyan alakítják sorsunkat?* Budapest, Typotex, 2010.

Christián (2022) = Christián László: *Komplementer rendészet.* Budapest, Ludovika Egyetemi Kiadó, 2022.

Clausewitz (2014) = Carl von Clausewitz: *A háborúról.* Budapest, Zrínyi Kiadó, 2014.

Coget–Yamauchi–Suman (2002) = Jean-Francois Coget – Yutaka Yamauchi – Michael Suman: The Internet, Social Networks and Loneliness. *IT@Society,* 2002/1. 180–201.

Concha (1905) = Concha Győző: *Politika. II. Kötet. Közigazgatástan.* Budapest, Grill Károly Könyvkiadóvállalata, 1905.

Concha (1907) = Concha Győző: *Politika. I. Kötet. Alkotmánytan.* Budapest, Grill Károly Könyvkiadó Vállalata, 1907.

Connolly et al. (2016) = Irene Connolly – Marion Palmer – Hannah Barton – Gráinne Kirwan (szerk.): *An Introduction to Cyberpsychology*. London – New York, Routledge, 2016.

Cook (1964) = Fred J. Cook: The Warfare State. *The Annals of the American Academy of Political and Social Scince*, 1964/1. 102–109.

Cooper (2016) = Julian Cooper: *If War Comes Tomorrow. How Russia Prepares for Possible Armed Agression.* London, Royal United Service Institute for Defence and Security Studies, 2016.

Cucumano–Corbe (2018) = Eugenio Cucumano – Marian Corbe (szerk.): *A Civil–Military Response to Hybrid Threats.* Cham, Palgrave Macmillan, 2018.

Cullen (2018) = Patrick Cullen: *Hybrid threats as a new 'wicked problem' for early warning.* Helsinki, The European Centre of Excellence for Countering Hybrid Threats, 2018.

Curtis (2011) = George Curtis: *The Law of Cybercrimes and Their Investigation.* Boca Raton, CRC Press, 2011.

Cs. Kiss (2001) = Cs. Kiss Lajos (szerk.): *Carl Schmitt jogtudománya.* Budapest, Gondolat Kiadó, 2004.

Cs. Kiss (2022) = Cs. Kiss Lajos (szerk.): *Carl Schmitt fogadtatása a társadalomtudományokban.* Budapest, Ludovika Egyetemi Kiadó, 2022.

Csíkszentmihályi (1997) = Csíkszentmihályi Mihály: Flow: Az áramlat – A tökéletes élmény pszichológiája. Budapest, Akadémiai Kiadó, 1997.

Csitei (2020) = Csitei Béla: Az önvezető járművek és az Európai Unió joga. In: Lévayné Fazekas Judit – Kecskés Gábor (szerk.): *Az autonóm járművek és intelligens rendszerek jogi vonatkozásai.* Győr, Universitas–Győr Nonprofit Kft, 2020. 55–73.

D. Horváth (2022) = D. Horváth Vanessza: Cyberbullying a jogterületek metszéspontjában. *Infokommunikáció és jog* 2022/1. 46–50.

Dannreuther (2016) = Roland Dannreuther: *Nemzetközi biztonság.* Budapest, Antall József Tudásközpont, 2016.

Deák (2007) = Deák Péter: *Biztonságpolitikai kézikönyv.* Budapest, Osiris kiadó, 2007.

Deák (2009) = Deák Péter: *Biztonságpolitika a hétköznapokban.* Budapest, Zrínyi kiadó, 2009.

Desewffy (2019) = Desewffy Tibor: *Digitális szociológia.* Budapest, Typotex Kiadó, 2019.

Devanny–Harris (2014) = Joe Devanny – Josh Harris: *The National Seucirty Council. National security at the centre of government.* London, Institute for Government, 2014.

Dewar–Keller–Malhotra (2022) = Carolyn Dewar – Scott Keller – Vikram Malhotra: *CEO Vezetés felsőfokon.* Budapest, 21. Század Kiadó, 2022.

Dobák (2014) = Dobák Imre (szerk.): *A nemzetbiztonság általános elmélete.* Budapest, Nemzeti Közszolgálati Egyetem, 2014.

Dobák (2022a) = Dobák Imre (szerk.): *Nemzetbiztonság a 21. század elején.* Budapest, Ludovika Egyetemi Kiadó, 2022.

Dobák (2022b) = Dobák Imre: A nemzetbiztonság fejlődő egyetemi kapcsolatai. In: Dobák Imre (szerk.): *Nemzetbiztonság a 21. század elején.* Budapest, Ludovika Egyetemi Kiadó, 2022. 145–159.

Dobák (2022c) = Dobák Imre: Társadalom – Technológiai környezet – Nemzetbiztonság. In: Dobák Imre (szerk.): *Nemzetbiztonság a 21. század elején.* Budapest, Ludovika Egyetemi Kiadó, 2022. 52–67.

Dobák–Tóth (2021) = Dobák Imre – Tóth Tamás: Régi módszerek a kibertérben? (CYBER-HUMINT, OSINT, SOCMINT, Social Engineering). *Belügyi Szemle* 2021/2. 195–212.

Dodge–Kitchin (2001) = Martin Dodge – Rob Kitchin: *Mapping Cyberspace.* London – New York, Routledge, 2001.

Dubow–Lucas–Morris (2020) = Ben Dubow – Edward Lucas – Jake Morris: *Jabbed in the Back: Mapping Russian and Chinese Information Operations During Covid–19.* The Center for European Polidy Analysis (CEPA), 2020.

Dunlap (2011) = Charles J. Dunlap Jr.: *Law and Military Interventions: Preserving Humanitarian Values in 21 st Conflicts.* people.duke.edu/~pfeaver/dunlap.pdf

Dunn et al. (2021) = Jessilyn Dunn – Lukasz Kidzinski – Ryan Runge – Daniel Witt – Jennifer L. Hicks – Sophia Miryam Schüssler – Fiorenza Rose – Xiao Li – Amir Bahmani – Scott L. Delp – Trevor Hastie – Michael P. Snyder: Wearable sensors enable personalized predictions of clinical laboratory measurements. *Nature medicine,* 2021/27. 1105–1112

Dusek (2018) = Dusek Tamás: Az okos városok komplex mutatószámainak egyes tartalmi és módszertani problémái. In: Kovács Gábor – Völgyi Katalin (szerk.): *„Üzleti vállalkozások, makro- és mikrokörnyezetük gazdálkodási és menedzsment sajátosságai" c. kutatás tanulmányai.* Győr, Széchenyi István Egyetem Kautz Gyula Gazdaságtudományi Kar, 2018. 1–3.

Edgerton (2006) = David Edgerton: *Warfare State – Britain, 1920–1970.* Cambridge, Cambridge University Press, 2006.

Egresi (2016) = Egresi Katalin: Keresztény és a középkori politikai bölcselet főbb jellemzői. In: Egresi Katalin – Pongrácz Alex – Szigeti Péter – Takács Péter: *Államelmélet.* Győr, SZE DF ÁJK Jogelméleti Tanszék, 2016. 31–44.

Egyed (2016) = Egyed István: *A mi alkotmányunk.* Budapest, Dialóg Campus, 2016.

Egyed (2017) = Egyed István: *A magyar közigazgatási jog alaptanai.* Budapest, Dialóg Campus, 2017.

Engel (2019) = Engel Péter: A Bundeskartellamt Facebook–döntése – az adatgyűjtés versenyjogi kockázatai. *Verseny Tükör*, 2019/1. 70–76.

Epstein (2021) = David Epstein: *Sokoldalúság.* Budapest, HVG Könyvek Kiadó, 2021.

Escobar (1994) = Arturo Escobar: Welcome to Cyberia – Notes on the Anthropology of Cyberculture. *Current Anthropology*, 1994/3. 211–231.

Esping-Andersen (2002) = Gøsta Esping-Andersen: Towards the Good Society, Once Again? In: Gøsta Esping-Andersen (szerk.): *Why We Need a New Welfare State.* Oxford – New York, Oxford University Press, 2002. 1–25.

Esping-Andersen (2006) = Gøsta Esping-Andersen: A Welfare State for the Twenty–first Century. In: Christopher Pierson –Francis G. Castel (szerk.): *The Welfare State Reader (Second Edition).* Cambridge, Polity Press, 2006. 434–454.

Fandáková et al. (2020) = Mariam Fandáková – K. Zabovska – Boris Bucko – Michal Zábovsky: Improvements of Computer Assisted Virtual Environment (CAVE). In: *2020 43rd International Convention on Information, Communication and Electronic Technology (MIPRO)*. Opatija, Croatia, 2020. 1680-1684.

Farkas Ádám (2012) = Farkas Ádám: A katonai büntetőjog és igazságszolgáltatás helye, szerepe, létjogosultsága az állam és társadalom rendszereiben. *Hadtudomány*, 2012/elektronikus szám. mhtt.eu/hadtudomany/2012/2012_elektronikus/2012_e_Farkas_Adam.pdf

Farkas Ádám (2015) = Farkas Ádám: A totális államtól a totális háborún át a totális védelemig. *MTA Law Working Papers* 2015/34. 1–20.

Farkas Ádám (2016) = Farkas Ádám: *Tévelygések fogásában?: Tanulmányok az állam fegyveres védelmének egyes jogtani és államtani kérdéseiről, különös tekintettel Magyarország katonai védelmére.* Budapest, Magyar Katonai Jogi és Hadijogi Társaság, 2016.

Farkas Ádám (2017a) = Farkas Ádám: Adalékok az állam fegyveres védelmének rendszertani megközelítéséhez. *Honvédségi Szemle*, 2017/1. 44–58.

Farkas Ádám (2017b) = Farkas Ádám: A terrorizmus elleni harc, mint kiemelt ágazatközi fegyveres védelmi feladat. *Szakmai Szemle*, 2017/3. 5–20.

Farkas Ádám (2018a) = Farkas Ádám: *A totalitás kora? A 21. század biztonsági környezetének és kihívásainak totalitása és a totális védelem gondolatkísérlete.* Budapest, Magyar Katonai Jogi és Hadijogi Társaság, 2018.

Farkas Ádám (2018b) = Farkas Ádám: *A fegyveres védelem mint állami alrendszer és annak szabályozási sajátosságai.* Budapest, Magyar Katonai Jogi és Hadijogi Társaság, 2018.

Farkas Ádám (2018c) = Farkas Ádám: Adalékok a védelmi alkotmány és a védelmi alkotmányjog hazai értelmezéséhez és történetiségéhez. *Hadtudományi Szemle*, 2018/4. 227–255.

Farkas Ádám (2018d) = Farkas Ádám: A honvédelmi jog polgári szabályozási előzményei Magyarországon. In: Farkas Ádám (szerk.): *A honvédelem jogának elméleti, történeti és kortárs kérdései.* Budapest, Dialóg Campus, 2018. 31–58.

Farkas Ádám (2019a) = Farkas Ádám: *Az állam fegyveres védelmének alapvonalai.* Budapest, Katonai Nemzetbiztonsági Szolgálat, 2019.

Farkas Ádám (2019b) = Farkas Ádám: *A [hon]védelmi alkotmány polgári evolúciója Magyarországon 1867–1944.* Budapest, Zrínyi Kiadó, 2019.

Farkas Ádám (2019c) = Farkas Ádám: A kibertér műveleti képességek kialakításának és fejlesztésének egyes szabályozási és államszervezési alapvonalai. *Jog Állam Politika* 2019/2. 63–79.

Farkas Ádám (2020a) = Farkas Ádám: Komplex biztonság, hibrid konfliktusok, összetett válaszok. *Honvédségi Szemle,* 2020/4. 11–23.

Farkas Ádám (2020b) = Farkas Ádám: Gondolatok a nemzetbiztonság fogalmáról. *Szakmai Szemle – A Katonai Nemzetbiztonsági Szolgálat tudományos–szakmai folyóirata*, 2020/3. 5–20.

Farkas Ádám (2020c) = Farkas Ádám: Egy lehetséges narratíva a védelem-szabályozási szemléletünk megújításához. In: Farkas Ádám – Kelemen Roland (szerk.): *Szkülla és Kharübdisz között. Tanulmányok a különleges jogrend elméleti és pragmatikus kérdéseiről, valamint nemzetközi megoldásairól*. Budapest, Magyar Katonai Jogi és Hadijogi Társaság, 2020. 347–380.

Farkas Ádám (2021a) = Farkas Ádám: Biztonság – Geopolitika – Digitalizáció, avagy Amaël Cattaruzza „A digitális adatok geopolitikája" című kötetének főbb üzenetei. *SmartLaw Research Group Working Paper,* 2021/1. 1–13.

Farkas Ádám (2021b) = Farkas Ádám: Kibertér művelet: Hírszerző, rendészeti és katonai műveltek elegye? Gondolatok az angol National Cyber Force kapcsán. *Military and Intelligence CyberSecurity Research Paper*, 2021/1. 1–8.

Farkas Ádám (2021c) = Farkas Ádám: Gondolatok a totalitás 21. századi esszenciájához. In: Pongrácz Alex (szerk.): *Ünnepi tanulmányok a 65 éves Cs. Kiss Lajos tiszteletére. Út vocatio scientia.* Budapest, Ludovika Egyetemi Kiadó, 2021. 65–80.

Farkas Ádám (2021d) = Farkas Ádám: A kortárs technológia-fejlődés és innováció viszonya a honvédelmi szabályozással. *MTA Law Working Papers* 2021/4. 1–15.

Farkas Ádám (2021e) = Farkas Ádám: A multidiszciplinaritás helye, szerepe a védelem és biztonság szabályozásának és szervezésének komplex kutatásaiban. *Közjogi Szemle,* 2021/4. 22–28.

Farkas Ádám (2021f) = Farkas Ádám: Bábeli Zűrzavar?: Avagy a védelmi és biztonsági kihívások jogállami adaptációjának rendszerszintű kérdései, különös tekintettel az Eurázsia-gondolatra. *Jog Állam Politika,* 2021/3. 37–52.

Farkas Ádám (2022a) = Farkas Ádám: *A védelem és biztonság-szavatolás szabályozásának alapjai Magyarországon.* Budapest, Magyar Katonai Jogi és Hadijogi Társaság, 2022.

Farkas Ádám (2022b) = Farkas Ádám: A történelmi tapasztalat és a tudomány helye, szerepe a 21. századi védelmi és biztonsági gondolkodásban. *Védelmi-Biztonsági Szabályozási és Kormányzástani Műhelytanulmányok,* 2022/1. 1–29.

Farkas Ádám (2022c) = Farkas Ádám: A védelmi-biztonsági gondolkodás és képzés megújításának elméleti és kulturális alapjai. *Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok,* 2022/2. 1–16.

Farkas Ádám (2022d) = Farkas Ádám: The Status and Role of Law and Regulation in the 21st-Century Hybrid Security Environment. *Acta Universitatis Sapientiae Legal Studies,* 2022/2. 113–124.

Farkas Ádám (2022e) = Farkas Ádám: The UK'S National Cyber Force - Beginning of a Hybrid Trend or a New Answer for Cyber Domain. *Military and Intelligence CyberSecurity Research Paper,* 2022/2. 1–10.

Farkas Ádám (2022f) = Farkas Ádám: Az Alaptörvény új, védelmi és biztonsági tárgyú rendelkezéseinek elemzése I. *Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok,* 2022/38. 1–22.

Farkas Ádám (2022g) = Farkas Ádám: Questions and Options for the Emerging Reform of the Hungarian Security and Defence Regulation. *MTA Law Working Papers,* 2022/14. 1–11.

Farkas Ádám (2022h) = Farkas Ádám: A védelmi és biztonsági tevékenységek összehangolásáról szóló törvény helye, szerepe a jogrendszerben. *Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok,* 2022/39. 1–26.

Farkas Ádám (2022i) = Farkas Ádám: A védelmi és biztonsági tevékenységek összehangolásának alapvetései, ezek viszonyrendszerének feltárása. *Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok,* 2022/36. 1–30.

Farkas Ádám (2023) = Farkas Ádám: Babelic confusion?: Systemic issues in the adaptation to defence and security challenges in the transatlantic states, with special regard to the Eurasia-idea as a special aspect of hybridity. *Iustum Aequum Salutare,* 2023/1. 17–31.

Farkas Zoltán (2019) = Farkas Zoltán: A társadalmi struktúra fogalma, összetettsége és a társadalmi hálózatok. *Jel–Kép,* 2019/2. 100–123.

Farkas–Kelemen (2022) = Farkas Ádám – Kelemen Roland: Az Alaptörvény kilencedik módosítása, valamint a védelmi és biztonsági tevékenységek összehangolásáról szóló 2021. évi XCIII. törvény megalkotásának történelmi előzményei. *Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok,* 2022/37. 1–39.

Farkas–Resperger (2020) = Farkas Ádám – Resperger István (2020): Az úgynevezett „hibrid hadviselés" kihívásainak kezelése és a nemzetközi jog mai korlátai. In: Farkas Ádám – Végh Károly (szerk.): *Új típusú hadviselés a 21. század második évtizedében és azon túl. Intézményi és jogi kihívások.* Budapest, Zrínyi Kiadó, 2020. 132–149.

Farkas–Spitzer (2021) = Farkas Ádám – Spitzer Jenő: Az információs korszak és az állami reziliencia egyes kérdései. *Védelmi-Biztonsági Szabályozási és Kormányzástani Műhelytanulmányok*, 2021/18. 1–27.

Farkas–Till (2016) = Farkas Ádám – Till Szabolcs: A honvédelmi alkotmány és alkotmányosság alapkérdései Magyarországon. In: Farkas Ádám – Kádár Pál (szerk.): *Magyarország katonai védelmének közjogi alapjai.* Budapest, Zrínyi Kiadó, 2016. 40–71.

Farkas–Till (2022) = Farkas Ádám – Till Szabolcs: A honvédelem közjogi szabályozásának megújítását indokló körülmények áttekintése. *Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok,* 2022/26. 1–37.

Farkas–Vilics (2022) = Farkas Ádám – Vilics Tünde: A társadalmi rezíliencia és a pszichológia találkozási pontjai. *Védelmi-Biztonsági Szabályozási és Kormányzástani Műhelytanulmányok,* 2022/15. 1–19.

Ferdinandy (1902) = Ferdinandy Gejza: *Magyarország közjoga.* Budapest, Politzer Zsigmond és Fia kiadása, 1902.

Ferdinandy (1911) = Ferdinandy Gejza: *A magyar alkotmányjog tankönyve*. Budapest, Franklin-Társulat, 1911.

Ferencz (2019) = Ferencz Jácint: Az információ és a technológia kettős arca a munkajogban. In: Baranyiné Kóczy Judit – Fehér Ágota (szerk.): *Pedagógusképzés, oktatás a Kárpát–medencében, társadalmi kontextusok. XXII. Apáczai–napok Tudományos Konferencia tanulmánykötet.* Győr, Széchenyi István Egyetem Apáczai Csere János Kar, 2019. 322–329.

Forgács (2017) = Forgács Balázs: *Hadelmélet. A magyar katonai gondolkodás története és a hadikultúrák.* Budapest, Dialóg Campus, 2017.

Forgács (2020) = Forgács Balázs: *Gerillák, partizánok, felkelők - Az irreguláris hadviselés elméletének története – korunk kihívásai.* Budapest, Zrínyi Kiadó, 2020.

Forrest (2005) = Dave Forrest: *Barát vagy ellenség? – A totális kontroll forgatókönyve*. Budapest, Focus Kiadó, 2005.

Fridman–Kabernik–Pearce (2019) = Ofer Fridman – Vitaly Kabernik – James C. Pearce (szerk.): *Hybrid Conflicts and Information Warfare. New Labels, Old Politics.* Boulder–London, Lynne Rienner, 2019.

Fuchs (2019) = Yeshimabeit Christian Fuchs: Towards Dialectical Digital Modernity: Reflections on David Chandler's Chapter. In: Dave Chandler – Christian Fuchs (szerk.): *Digital Objects, Digital Subjects: Interdisciplinary Perspectives on Capitalism, Labour and Politics in the Age of Big Data*. London, University of Westminster Press, 2019. 43–52.

G. Karácsony (2020) = G. Karácsony Gergely: *Okoseszközök - okos jog?* Budapest, Ludovika Egyetemi Kiadó, 2020.

G. Karácsony (2021) = G. Karácsony Gergely: A videójátékok adatkezelési gyakorlata: kommunikáció és profilalkotás. In: G. Karácsony Gergely (szerk.): *A videojátékok jogi kérdései*. Győr, Széchenyi István Egyetem, 2021. 25–38.

Gagliarducci et al. (2017) = Stefano Gagliarducci – Massimilano Gaetano Onorato – Francesco Sobbrio – Guido Tabellini: War of the Waves: Radio and Resistance during World War II. *IZA Discussion Paper Series,* 2017.

Gates (2018) = Robert M. Gates: *A vezetés szenvedélye*. Budapest, Antall József Tudásközpont, 2018.

Gati (2014) = Charles Gati: *Zbig. Zbigniew Brzezinski a stratéga.* Budapest, Noran Libro, 2014.

Gellén (2020) = Gellén Klára: Tisztességtelen kereskedelmi gyakorlatok az online térben – fókuszban a közösségi média. *In Medias Res*, 2020/1. 127–140.

Giannopoulos–Smith–Theocharidou (2021) = Georgios Giannopoulos – Hanna Smith – Marianthi Theocharidou (szerk.): *The Landscape of Hybrid Threats: A Conceptual Model. Public Version.* Luxembourg, European Union, 2021.

Gibson (1984) = William Gibson: *Neuromancer*. New York, ACE Publishing Group, 1984.

Gosztonyi (2020) = Gosztonyi Gergely: The European Court of Human Rights: Internet access as a means of receiving and imparting information and ideas. *International Comparative Jurisprudence Research Journal,* 2020/2. 134–140.

Gosztonyi (2021a) = Gosztonyi Gergely: Special Models of Internet and Content Regulation on China and Russia. *ELTE Law Journal*, 2021/2. 87–99.

Gosztonyi (2021b) = Gosztonyi Gergely: Az internet-hozzáférés korlátozásának gyakorlata az Emberi Jogok Európai Bírósága előtt. *In Medias Res,* 2021/1. 91–101.

Gosztonyi (2021c) = Gosztonyi Gergely: Az internetes tartalomszabályozással kapcsolatos új gondolkodási irányok az Amerikai Egyesült Államokban. *Miskolci Jogi Szemle*, 2021/4. 40–54.

Gosztonyi (2022a) = Gosztonyi Gergely: *Cenzúra Arisztotelésztől a Facebookig – A közösségi média tartalomszabályozási gyakorlatának komplexitása.* Budapest, Gondolat Kiadó, 2022.

Gosztonyi (2022b) = Gosztonyi Gergely: A kínai internetcenzúra modellje. *Pro Futuro,* 2022/1. 27–36.

Gosztonyi (2022c) = Gosztonyi Gergely: Aspects of the History of Internet Regulation from Web 1.0 to Web 2.0. *Journal on European History of Law,* 2022/1. 168–173.

Gosztonyi–Huszár (2022) = Gosztonyi Gergely – Huszár Daniella: Az anonim kommentelés aktuális jogi megítélése az Emberi Jogok Európai Bírósága és az ausztrál legfelső bíróság gyakorlata alapján. *In Medias Res,* 2022/2. 141–152.

Gyekiczky (2021) = Gyekiczky Tamás: *Olvasmányok a Digitális társadalomról – jogászoknak. Kézirat.* Budapest, 2021. academia.edu/49694295/Olvasm%C3%A1nyok_a_Digit%C3%A1lis_T%C3%A1rsadalomr%C3%B3l_Jog%C3%A1szoknak

Gyuris–Meskó–Tisljár (2014) = Gyuris Petra – Meskó Norbert – Tisljár Roland: *Az evolució árnyoldala. A lelki betegségek és az alternatív szexualitás darwini értelmezése*. Budapest, Akadémiai kiadó, 2014.

Haig et al. (2014) = Haig Zsolt – Kovács László – Ványa László – Vass Sándor: *Elektronikus hadviselés*. Budapest, Nemzeti Közszolgálati és Tankönyv Kiadó Zrt., 2014.

Hajdú (2020) = Hajdú József: A mesterséges intelligencia hatása a munkaerőpiacra, avagy elveszik-e a robotok az ember munkáját. *Infokommunikáció és Jog,* 2020/2. 3–9.

Hamilton (2016) = Daniel S. Hamilton (szerk.): *Forward Resilience. Protecting Society in an Interconnected World.* Washington, Center for Transatlantic Relations – Johns Hopkins University, 2016.

Harari (2016) = Yuval Noah Harari: *Homo Deus. – A holnap rövid története*. Budapest, Animus Kiadó, 2016.

Hasian (2016) = Marouf Hasian Jr.: *Drone Warfare and Lawfare in a Post-Heroic Age*. Tuscaloosa, The University of Alabama Press, 2016.

Hausner (2017) = Hausner Gábor: Zrínyi Miklós. In: Gőcze István (szerk.): *Állam és katona.* Budapest, Dialóg Campus Kiadó, 2017. 61–86.

Hazelwood–Koon-Magnin (2013) = Steven D. Hazelwood – Sarah Koon-Magnin: Cyber Stalking and Cyber Harassment Legislation in the United States: A Qualitative Analysis. *International Journal of Cyber Criminology,* 2013/2. 155–168.

Healey–Singh (2022) = Jason Healey – Virpratap Vikram Singh: Situational Cyber Stability and the Future of Escalating Cyber Conflict. In: Pirek Pernik (szerk.): *Cyberspace Strategic Outlook 2030 – Horizon Scanning and Analysis.* Tallinn, NATO CCDCOE Publications, 2022. 19–31.

Hermann (2015) = Rainer Hermann: *Az Iszlám Állam – A világi állam kudarca az arab világban.* Budapest, Akadémiai Kiadó, 2015.

Hobsbawm (1988) = Eric J. Hobsbawm: *A forradalmak kora*. Budapest, Kossuth Kiadó, 1988.

Hódos (2020) = Hódos László: A hibrid konfliktusok felívelési szakasza, avagy a fenyegetés észlelésének, megelőzésének és kezelésének nemzetbiztonsági aspektusa. *Honvédségi Szemle,* 2020/4. 49–64.

Hódos (2021) = Hódos László: A nemzetbiztonsági szolgálatok közelmúltbeli tevékenységét befolyásoló mérföldkövek, avagy az új típusú biztonsági kihívások jelentette veszélyek és az azokra adott kormányzati, illetve jogalkotói válaszok 2010 és 2020 között. *Szakmai Szemle*, 2021/1. 134–149.

Hódos (2022) = Hódos László: A kibertér és a mesterséges intelligencia jelentősége és kihívásai a jogállamok nemzetbiztonsági feladatellátásában. *Military and Intelligence CyberSecurity Research Paper,* 2022/11. 1–17.

Hofstetter (2020) = Yvonne Hofstetter: *Láthatatlan háború, avagy miképpen fenyegeti a digitalizáció a világ biztonságát és stabilitását.* Budapest, Corvina, 2020.

Horváth (1943) = Horváth Barna: *Angol jogelmélet.* Budapest, A Magyar Tudományos Akadémia Kiadása, 1943.

Hughes–Colonel (2017) = John Hughes – Wilson Colonel: *The Secret State: A History of Intelligence and Espionage.* New York, Pegasus Books, 2017.

Huntington (1994) = Samuel P. Huntington: *A katona és az állam.* Budapest, Zrínyi – Atlanti Kiadó, 1994.

Hutchings (2013) = Alice Hutchings: Hacking and Fraud: A Qualitative Analysis of Online Offending and Victimisation, In: Karuppannan Jaishankar – Natti Ronel (szerk.): *Global Criminology: Crime and Victimization in a Globalized Era*, London, CRC Press, 2013. 93–114.

Incze–Pesuth (2020) = Incze Norbert – Pesuth Tamás: E-Health – Digitalizálódik az egészségügy? *Köz-Gazdaság,* 2020/4. 247–250.

Jagadics et al. (2018) = Jagadics Péter – Rajos Sándor – Simon László – Szabó Károly: *A magyar katonai elhárítás története 1918–2018.* Budapest, Univerzum Könyvek, 2018.

Jain–Sahoo–Kaubiya (2021) = Ankit Kumar Jain – Somya Ranjan Sahoo – Jyoti Kaubiya: Online Social Networks Security and Privacy: Comprehensive Review and Analysis. *Complex & Intelligent System*, 2021/7. 2157–2177.

Jakobi (2002) = Jakobi Ákos: A virtuális világ terei. *Magyar Tudomány*, 2002/11.

Jakobi–Lengyel (2014) = Jakobi Ákos – Lengyel Balázs: Egy online közösségi háló offline földrajza, avagy a távolság és a méret szerepének magyar empíriái. *Tér*, 2014/1. 40–61.

Jakobsen (2008) = Peter Viggo Jakobsen: *NATO's Comprehensive Approach to Crisis Response Operations: A Work in Slow Progress*. DIIS Report 2008/15. Copeanhagen, Danis Institute for International Studies, 2008.

Jany (2016) = Jany János: *Jogi kultúrák Ázsiában – Kultúrtörténet, jogtudomány, mindennapok.* Budapest, Typotex, 2016.

Jegede–Ovia–Idam (2016) = Ajibade Ebenezer Jegede – E. Ovia – SC. Idam: Cyberspace and Crime Engineering: A Sociological Review. *International Journal of Forensic Sciences,* 2016/1.

Jonathan-Zamir–Wisburd –Hasisi (2014) = Tal Jonathan-Zamir – David Wisburd – Badi Hasisi: *Policing Terrorismt, Crime Controll, and Police-Community Relations*. Cham, Springer, 2014.

Juhász–Petruska (2022) = Juhász István – Petruska Ferenc: A védelmi-biztonsági szabályozási reformot indukáló biztonsági környezet-változás elemeinek beazonosítása, szakmai értékelése. *Védelmi-biztonsági Szabályozási és Kormányzástani Kutatóműhely,* 2022/32. 1–46.

Kádár (2020) = Kádár Pál: A hibrid kihívások és a működő államszervezet – gondolatok egy konferencia margójára. *Honvédségi Szemle,* 2020/4. 3–10.

Kádár (2022a) = Kádár Pál: A short overview of the reform of Hungarian defence and security regulations. *Hadtudomány,* 2022/1. 61–73.

Kádár (2022b) = Kádár Pál: A különleges jogrendi szabályrendszer reformja. *Katonai Jogi és Hadijogi Szemle,* 2022/3. 65–90.

Kádár (2022c) = Kádár Pál: A védelmi-biztonsági szabályozási reform rendszer alapelgondolásának elemzése és lehetséges perspektívái. *Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok,* 2022/8. 1–32.

Kádár (2022d) = Kádár Pál: Gondolatok a védelmi-biztonsági szabályozás reformjának egyes kérdéseiről. *Honvédségi Szemle,* 2022/1. 3–19.

Kádár–Till (2022) = Kádár Pál – Till Szabolcs Péter: A védelmi és biztonsági tevékenységek összehangolásának biztosítékai a Vbö. tükrében. *Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok,* 2022/21. 1–58.

Kajtár (2015) = Kajtár Gábor: *A nem állami szereplők elleni önvédelem a nemzetközi jogban.* Budapest, ELTE Eötvös Kiadó, 2015.

Kaladijan (1996) = Gregory M. Kaladijan: Welfare vs Cyberfare. *Journal of Children and Proverty*, 1996/1. 93–104.

Kalpokas (2019) = Ignas Kalpokas: *A Political Theory of Post-Truth.* Cham, Palgrave Pivot, 2019.

Karácsony (2016) = Karácsony András: *A jogtudomány teológusa. Carl Schmitt politikai teológiája.* Gödöllő–Máriabesnyő, Attraktor Kiadó, 2016.

Kassai (2012) = Kassai Károly: Kiberveszély és a Magyar Honvédség. *Hadmérnök,* 2012/4. 135–137.

Kazári (2003) = Kazári Csaba: *Hacker, cracker, warez. A számítógépes alvilág titkai.* Budapest, Computer Panoráma, 2003.

Kearney (2010) = Michael Kearney: Lawfare, Legitimacy and Resistance: The Weak and the Law. In: Ardi Imseis (szerk.): *The Palestine Yearbook of International Law.* Martinus Nijhoff Publishers, Leiden, 2010.

Kecskés (2014) = Kecskés Gábor: Az államfelelősség és a szankciók nemzetközi jogi kérdéskörének megjelenése a magyar jogirodalomban. In: Blutman László – Homoki-Nagy Mária (szerk.): *Ünnepi kötet Dr. Bodnár László egyetemi tanár 70. születésnapjára.* Szeged, Szegedi Tudományegyetem Állam- és Jogtudományi Kar, 2014. 289–301.

Kelemen (2017a) = Kelemen Roland: A kettős forradalom hatása a 19. század eleji geopolitikai viszonyokra – Avagy a polgári jogállam születése. In: Keserű Barna Arnold (szerk.): *Doktori Műhelytanulmányok*, Győr, 2017, Széchenyi István Egyetem, 2017. 81–102.

Kelemen (2017b) = Kelemen Roland: Cyber Attacks and Cyber Intelligence in the System of Cyber Warfare, In: Szabó Miklós (szerk.): *Doktoranduszok Fóruma: Állam– és Jogtudományi Kar szekciókiadványa.* Miskolc, Miskolci Egyetem, 2017, 117–122.

Kelemen (2017c) = Kelemen Roland: A katonai jog, a katonai büntetőjog helye a dualizmus kori magyar államban. In: Kis Norbert – Peres Zsuzsanna (szerk.): *Ünnepi tanulmányok Máthé Gábor oktatói pályafutásának 50. jubileumára: Studia sollemnia scientiarum politico-cameralium.* Budapest, Dialóg Campus Kiadó, Nordex Kft., 2017. 203–210.

Kelemen (2019a) = Kelemen Roland: Az Alaptörvény szükségállapot szabályozásának kritikai áttekintése az egyes európai uniós tagállamok alkotmányainak figyelembevételével – különös

tekintettel a visegrádi államok alkotmányaira. In: Bartkó Róbert (szerk.): *A terrorizmus elleni küzdelem aktuális kérdései a XXI. században.* Budapest, Gondolat, 2019. 9–35.

Kelemen (2019b) = Kelemen Roland: A polgári kor társadalombiztosítása – Társadalombiztosítási bíráskodás a polgári korban. In: Molnár Andrea – Széplaki László (szerk.): *Tanulmányok a győri felsőbíráskodás történetéből a XIX–XX. század fordulóján.* Győr, Győri Ítélőtábla, 2019. 149–174.

Kelemen (2019c) = Kelemen Roland: A kibertámadások nemzetközi jogi olvasata és a NATO értelmezése, különös tekintettel a válaszlehetőségekre. In: Farkas Ádám (szerk.): *Az állam katonai védelme az új típusú biztonsági kihívások tükrében.* Budapest, Nemzeti Közszolgálati Egyetem Közigazgatási Továbbképzési Intézet, 2019. 29–50.

Kelemen (2020a) = Kelemen Roland: A kibertérből érkező fenyegetések jelentősége a hibrid konfliktusokban és azok várható fejlődése. *Honvédségi Szemle,* 2020/4. 65–81.

Kelemen (2020b) = Kelemen Roland: A különleges jogrend történeti modelljeinek kialakulása és fejlődése a 20. század második évtizedének végéig. In: Farkas Ádám – Kelemen Roland (szerk.): *Szkülla és Kharübdisz között – Tanulmányok a különleges jogrend elméleti és pragmatikus kérdéseiről, valamint nemzetközi megoldásairól.* Budapest, Magyar Katonai Jogi és Hadijogi Társaság, 2020. 43–79.

Kelemen (2020c) = Kelemen Roland: A biztonsági környezet alakulása a hosszú 19. században. *Vélemények a Katonai Jog Világából*, 2020/3. 1–9.

Kelemen (2021a) = Kelemen Roland: A nem állami kibertéri műveletek egyes szereplőinek jelentősége a hibrid konfliktusokban. *SmartLaw Research Group Working Paper*, 2021/2. 1–17.

Kelemen (2021b) = Kelemen Roland: A legitimációs kivételes hatalom fogalmi rendszere. In: Pongrácz Alex (szerk.): *Ünnepi tanulmányok a 65 éves Cs. Kiss Lajos tiszteletére. Ut vocatio scientia.* Budapest, Ludovika Egyetemi Kiadó, 2021. 177–186.

Kelemen (2021c) = Kelemen Roland: Radikalizálás, dezinformálás és tömegpszichózis modern köntösben: a hibrid konfliktus kibertérben. *Jog Állam Politika*, 2021/3. 71–85.

Kelemen (2022a) = Kelemen Roland: A jogállami kivételes hatalom gyökerei és az eredeti modellek kialakulása. *Védelmi–biztonsági Szabályozási és Kormányzástani Műhelytanulmányok*, 2022/4. 4–59.

Kelemen (2022b) = Kelemen Roland: Cyberfare Sate – Egy hibrid állammodell 21. századi születése. *Military and Intelligence CyberSecurity Research Paper*, 2022/1. 1–32.

Kelemen–Farkas (2020) = Kelemen Roland – Farkas Ádám: To the margin of the theory of a new type of warfare: Examining certain aspects of cyber warfare. In: Szabó Marcel –Gyeney Laura –Láncos Petra Lea (szerk.): *Hungarian yearbook of international law and European law (2019).* Hague, Eleven International, 2020. 203–226.

Kelemen–Németh (2019) = Kelemen Roland –Németh Roland: Vulnerabilities of the cyberspace due to its social nature. In: Rastislav Funta (szerk.): *Počítačové právo, UI, ochrana údajov a najväčšie technologické trendy.* Sládkovičovo, Vysoká škola, Danubius, 2019. 51–66.

Kelemen–Pataki (2015) = Kelemen Roland – Pataki Márta: A kibertámadások nemzetközi jogi értékelése. *Katonai Jogi és Hadijogi Szemle*, 2015/1. 53–90.

Kelemen–Simon (2020) = Kelemen Roland – Simon László: A kibertérben megjelenő fenyegetések és kihívások kezelésének egyes nemzetközi jogi problémái. In: Farkas Ádám – Végh Károly (szerk.): *Új típusú hadviselés a 21. század második évtizedében és azon túl – intézményi és jogi kihívások.* Budapest, Zrínyi, 2020. 150–170.

Kenedli (2020) = Kenedli Tamás: A Katonai Nemzetbiztonsági Szolgálat szakmai fejlődésének legfontosabb sajátosságai az elmúlt években. *Nemzetbiztonsági Szemle,* 2020/1. 74–94.

Keserű (2012) = Keserű Barna Arnold: Jogtörténeti töredékek az 1809. évi nemesi felkelés Fejér megyei eseményeiről. *Diskurzus,* 2012/2. 14–25.

Keserű (2019) = Keserű Barna Arnold: A mesterséges intelligencia néhány magánjogi aspektusáról. In: Glavanits Judit (szerk.): *A gazdasági jogalkotás aktuális kérdései.* Budapest, Dialóg Campus, 2019. 109–124.

Keszely (2013) = Keszely László (szerk.): *Az átfogó megközelítés és a védelmi igazgatás.* Budapest, HM Zrínyi Média Közhasznú Nonprofit Kft., 2013.

Keszely (2018) = Keszely László: Hibrid hadviselés és nemzeti ellenálló képesség (resilience), avagy átfogó megközelítés újratöltve. *Katonai Jogi és Hadijogi Szemle*, 2018/1. 29–62.

Keszely–Varga (2022a) = Keszely László – Varga Attila: A nemzeti és NATO szintű válságkezelés új szabályozási keretrendszerének elemzése. *Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok,* 2022/27. 1–33.

Keszely–Varga (2022b) = Keszely László – Varga Attila: A védelmi és biztonsági igazgatás új szabályrendszerének elemzése. *Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok,* 2022/28. 1–42.

Khausar–Ras (2023) = Miftahul Khausar – Abdul Rivai Ras: Establishment of The Cyber Diplomacy Toolbox (CDT) as a Joint Diplomatic Response to the European Union Against the Threat of Cyber Attack activity. *Politicon – Jurnal Ilmu Politik,* 2023/1. 29–58.

Kilger (2015) = Max Kilger: Integrating Human Behavior into the Development of Future Cyberterrorism Scenarios, In: *2015 10th International Conference on Availability, Reliability and Security.* Toulouse, IEEE, 2015. 693–700.

Kis (2018a) = Kis Kelemen Bence: Drónok háborúja (1.): A dróntámadások jus ad bellum jogszerűségi vizsgálata. *Honvédségi Szemle*, 2018/1. 70–82.

Kis (2018b) = Kis Kelemen Bence: Drónok háborúja (2.): A dróntámadások jogszerűségének vizsgálata a humanitárius nemzetközi jog és az emberi jogok tükrében. *Honvédségi Szemle*, 2018/2. 16–29.

Kiss Álmos (2019) = Kiss Álmos Péter: A hibrid hadviselés természetrajza. *Honvédségi Szemle*, 2019/4. 17–37.

Kiss Tibor (2020) = Kiss Tibor: *Agresszió a cybertérben.* Budapest, Nemzeti Közszolgálati Egyetem, 2020.

Kissinger (2019) = Henry Kissinger: *Fehér házi éveim I–III.* Budapest, Antall József Tudásközpont, 2019.

Kiss–Krasznay (2017) = Kiss Attila – Krasznay Csaba: A felhasználói viselkedéselemzés kiberbiztonsági előnyei és adatvédelmi kihívásai. *Információs Társadalom: Társadalomtudományi Folyóirat*, 2017/1. 55–71.

Kiss–Pari–Prazsák (2019) = Kiss Tibor – Pari Katalin – Prazsák Gergő: *Cyberdeviancia.* Budapest, Dialóg Campus, 2019.

Kittrie (2016) = Rode F. Kittrie: *Lawfare: Law as a Weapon of War.* New York, Oxford University Press, 2016.

Klein (2018) = Klein Tamás: Harmadik rész: Cyberjog I. fejezet: Az online nyilvánosság alkotmányjogi vonatkozásai. In: Klein Tamás – Tóth András (szerk.): *Technológia jog – Robotjog – Cyberjog.* Budapest, Wolters Kluwer, 2018. 219–261.

Klein (2021) = Klein Tamás: Pillanatfelvétel az online (közösségi média) platformok szabályozásának új európai koncepciójáról. In: Homicskó Árpád Olivér (szerk.): *Modern technológiák a jog egyes részterületein.* Budapest, Károli Gáspár Református Egyetem, Állam- és Jogtudományi Kar, 2021. 129–166.

Klement (2015) = Klement Mariann: Online és offline közösségek szerveződésének sajátosságai egy kutatás tükrében. In: Nádasi András (szerk.): *Agria Media 2014:XI. Információtechnikai és Oktatástechnológiai Konferencia és Kiállítás: nemzetközi konferencia.* Eger, Eszterházy Károly Főiskola Médiainformatikai Intézet, 2015. 114–126.

Kmety (1902) = Kmety Károly: *A magyar közigazgatási jog kézikönyve.* Budapest, Politzer Zsigmond és Fia Könyvkereskedése, 1902.

Kmety (1911) = Kmety Károly: *A magyar közjog tankönyve.* Budapest, Grill Károly Könyvkiadó Vállalata, 1911.

Knapp (2019) = Knapp László: A terrorizmus elleni küzdelem az Európai Unió jogában: A terrortámadásra adandó válasz a szolidaritási és a kollektív védelmi klauzula tükrében. In: Bartkó Róbert (szerk.): *A terrorizmus elleni küzdelem aktuális kérdései a XXI. században.* Gondolat, Budapest, 2019. 119–137.

Knapp (2020) = Knapp László: Az Európai Unió jogi személyisége. Gondolat, Budapest, 2020.

Koetler (2021) = Steven Koetler: *A lehetetlen művészete*. Budapest, HVG Könyvek Kiadó, 2021.

Kollár (2020) = Kollár Csaba: Kína és a társadalmi kredit rendszere. *Hadtudomány*, 2020/2. 79–97.

Koltay (2009) = Koltay András: *A szólásszabadság alapvonalai.* Budapest, Századvég Kiadó, 2009.

Koltay (2017) = Koltay András: Az internetes kapuőrök és az emberi jogok európai egyezményének 10. cikke: A sajtószabadság új alanyai. *Állam és Jogtudomány*, 2017/különszám. 129–140.

Koltay (2018) = Koltay András: Az újmédia kapuőreinek hatása a médiaszabályozásra. In: Koltay András (szerk.): *Tíz tanulmány a szólásszabadságról.* Budapest, Wolters Kluwer, 2018. 267–292.

Koltay (2019) = Koltay András: A social media platformok jogi státusa a szólásszabadság nézőpontjából. *In Medias Res*, 2019/1. 1–56.

Korom (2020) = Korom Ferenc: Feladataink egy új, hatékony, modern haderő létrehozása érdekében. *Honvédségi Szemle,* 2020/1. 3–4.

Kósa (1998) = Kósa László (szerk.): *Magyar művelődéstörténet.* Budapest, Osiris Kiadó, 1998.

Kovács Bálint (2012) = Kovács Bálint: A hálózatelemzés alkalmazásáról a történelemtudományban. *Világtörténet,* 2012/3–4. 187–204.

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

Kovács László (2021) = Kovács László: Offenzív kiberműveletek II.: Kibererők és képességeik. *Hadmérnök,* 2021/3. 119–137.

Kovács László (2023) = Kovács László: *Hadviselés a 21. században: kiberműveletek.* Budapest, Ludovika Kiadó, 2023.

Kovács-Szépvölgyi (2022a) = Kovács-Szépvölgyi Enikő: A digitális gyermekvédelem egyes aspektusai. In: *Széchenyi István Egyetem Új Nemzeti Kiválóság Program Tanulmánykötet 2021/2022.* Győr, Széchenyi István Egyetem, 2022. 227–236.

Kovács-Szépvölgyi (2022b) = Kovács-Szépvölgyi Enikő: Az európai uniós reklámszabályozás és a kiskorúak védelme – a digitalizáció kihívásai. *Külgazdaság,* 2022/5–6. 109–122.

Krasznay (2013) = Krasznay Csaba: Önkéntes oktatási tapasztalatok a Biztonságosabb Internet Programban. In: Gabos Erika (szerk.): *A média hatása a gyermekekre és fiatalokra. VII.* Budapest, Nemzetközi Gyermekmentő Szolgálat Magyar Egyesület, 2013. 105–109.

Krasznay (2019) = Krasznay Csaba: Kiberbiztonság a negyedik ipari forradalom korában. *Híradástechnika: Hírközlés-informatika,* 2019/1. 25–29.

Krasznay (2022) = Krasznay Csaba: *Kiberbiztonság a 21. században.* Budapest, Katonai Nemzetbiztonsági Szolgálat, Nemzeti Közszolgálati Egyetem, 2022.

Krasznay–Som (2016) = Krasznay Csaba – Som Zoltán: A szülői tudatosság megteremtése a közigazgatási információbiztonsági képzések segítségével. In: Gabos Erika (szerk.): *A média hatása a gyermekekre és fiatalokra VIII.* Budapest, Nemzetközi Gyermekmentő Szolgálat Magyar Egyesület, 2016. 235–240.

Krasznay–Varga-Perke (2013) = Krasznay Csaba – Varga-Perke Bálint: Ifjúságvédelem a hacker szubkultúrában. In: Bíró A. Zoltán – Gergely Orsolya (szerk.): *Ártalmas vagy hasznos internet? A média hatása a gyermekekre és fiatalokra.* Csíkszereda, Státus Könyvkiadó, 2013. 179–202.

Krekó (2018) = Krekó Péter: *Tömegparanoia. Az összeesküvés-elméletek és álhírek szociálpszichológiája.* Budapest, Atheneum Kiadó, 2018.

Krekó (2021) = Krekó Péter: *Tömegparanoia 2.0. Összeesküvés-elméletek, álhírek, dezinformáció.* Budapest, Atheneum Kiadó, 2021.

Kristó (2000) = Kristó Gyula: A magyar nomád államtól Szent Istvánig. *Aetas,* 2000/3. 116–120.

Kulesza (2020) = Joanna Kulesza: *International Internet Law.* London, New York, Routledge, 2012.

Kurzweil (2014) = Ray Kurzweil: *A szingularitás küszöbén.* Budapest, Ad Astra, 2014.

Lakhtakia et al. (2022) = Tanyi Lakhtakia et al.: Smartphone digital phenotyping, surveys, and cognitive assessments for global mental health: Initial data and clinical correlations from an international first episode psychosis study. *Digital Health*, November 2022. journals.sagepub.com/doi/10.1177/20552076221133758

le Bon (2018) = Gustave le Bon: *A tömegek lélektana.* Budapest, Hermit Könyvkiadó Bt., 2018.

Legárd (2020) = Legárd Ildikó: A barát és ellenség megkülönböztetése a kibertérben. *Jog Állam Politika,* 2020/3. 125–140.

Leigher (2021) = William E. Leigher: *Cyber Conflict in a Hybrid Threat Environment: Death by a Thousand Cuts.* Helsinki, Hybrid CoE 2021.

Lewis (2002) = James A. Lewis: Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats. *Center for Strategic and International Studies*, 2002. steptoe.com/images/content/4/5/v1/4586/231a.pdf

Lieberman (2017) = Ariel Victoria Lieberman: Terrorism, the Internet, and Propaganda: A Deadly Combination. *Journal of National Security Law & Policy*, 2017/1. 95–124.

Lim et al. (2022) = Ashley Cha Yin Lim – Pragadesh Natarajan – R Dineth Fonseka – Monish Maharaj – Ralph J. Mobbs: The application of artificial intelligence and custom algorithms with inertial wearable devices for gait analysis and detection of gait-altering pathologies in adults: A scoping review of literature. *Digital Health,* January 2022. journals.sagepub.com/doi/full/10.1177/20552076221074128

Lin–Zegart (2018) = Herbert Lin – Amy Zegart: *Bytes, Bombs and Spies. The Strategic Dimensions of Offensive Cyber Operations.* Washington, Brooking Institute, 2018.

Long (2012) = Larisa April Long: Profiling Hackers. *Sans Institute Reading Room*, 26th January 2012. 2–21.

Ludendorff (1935) = Erich von Ludendorff: *Der totale Krieg.* München, Ludendorffs, 1935.

Ludendorff (1940) = Erich von Ludendorff: Apostle of the „total war". *The Living Age,* 1940/March.

Lupovici (2011) = Amir Lupovici: Cyber Warfare and Deterrence: Trends and Challenges in Research. *Military and Strategic Affairs* 2011/3. 49–62.

Lupton (2015) = Deborah Lupton: *Digital Sociology.* London – New York, Routledge, 2015.

Machiavelli (2001) = Niccolò Machiavelli: *A háború művészete.* Szeged, Szukits kiadó, 2001.

Machiavelli (2006) = Niccolò Machiavelli: *A fejedelem.* Budapest, Caraphilus Kiadó, 2006.

Machlup (1962) = Fritz Machlup: *The Production and Distribution of Knowledge in the United States.* Princeton University Press, 1962.

Magyar–Simon (2017) = Magyar Sándor – Simon László: A terrorizmus és indirekt hadviselés az EU kibertérben. *Szakmai Szemle – A Katonai Nemzetbiztonsági Szolgálat tudományos–szakmai folyóirata*, 2017/4. 57–68.

Magyary (1927) = Magyary Zoltán: *A magyar tudománypolitika alapvetése.* Budapest, Királyi Magyar Egyetemi Nyomda, 1927.

Magyary (1930) = Magyary Zoltán: *A magyar közigazgatás racionalizálása.* Budapest, Királyi Magyar Egyetemi Nyomda, 1930.

Magyary (1931a) = Magyary Zoltán: *A magyar közigazgatás gazdaságosságának és eredményességének biztosítása.* Budapest, Athenaeum, 1931.

Magyary (1931b) = Magyary Zoltán: *A magyar tudományos nagyüzem megszervezése.* Budapest, Danubia Könyvkiadó, 1931.

Magyary (1938) = Magyary Zoltán: *Közigazgatási vezérkar*. Budapest, Dunántúl Pécsi Egyetemi Könyvkiadó és Nyomda, 1938.

Magyary (1939) = Magyary Zoltán: *Államéletünk válsága.* Budapest, Klny. „Egyedül vagyunk", 1939/6.

Magyary (1942) = Magyary Zoltán: *Magyar közigazgatás. A közigazgatás szerepe a XX. sz. államában. A magyar közigazgatás szervezete működése és jogi rendje.* Budapest, Királyi Magyar Egyetemi Nyomda, 1942.

Majumdar–Banerji–Chakrabarti (2018) = Debashis Majumdar – Pradipta Kumar Banerji – Satyajit Chakrabarti: Disruptive technology and disruptive innovation: Ignore at your peril! *Technology Analysis & Strategic Managment,* 2018/11. 1247–1255.

Makela (2019) = Jarmo Makela: Countering Disinformation: News Media and Legal Resilience. *Hybrid CoE Paper,* 2019/1. 1–25.

Malkovics (2013) = Malkovics Tibor: A magyar jobboldali (nemzeti) radikálisok és a hazai „gárdák" az internetes kapcsolathálózati elemzések tükrében, *Médiakutató,* 2013/nyár. 29–50.

Mártonffy (2020) = Mártonffy Balázs: Bevezetés a kiberdiplomáciába: alapfogalmak és elméleti viták. In Török Bernát (szerk.): *Információ- és kiberbiztonság.* Budapest, Ludovika Egyetemi Kiadó, 2020.

Maszaaki (2022) = Imai Maszaaki: *Kaizen stratégia*. Budapest, HVK Könyvek Kiadó, 2022.

McDermott (2014) = Roger McDermott: Russia Activates New Defense Management Center. *Eurasia Daily Monitor,* 2014/196. jamestown.org/program/russia-activates-new-defense-management-center/

Mcintyre (2018) = Lee C. McIntyre: *Post-Truth*. Cambridge, The MIT Press, 2018.

Mercier (2005) = Arnaud Mercier: War and media: Constancy and convulsion. *International Review of the Red,* 2005/87. 649–659.

Mészáros Bence (2019) = Mészáros Bence: *Fedett nyomozó alkalmazása a bűnüldözésben*. Budapest, Dialog Campus Kiadó, 2019.

Mészáros Rezső (2006) = Mészáros Rezső: A kibertér, mint új földrajzi tér. In: Kiss Andrea – Mezősi Gábor – Sümeghy Zoltán (szerk.): *Táj, környezet és társadalom – Ünnepi tanulmányok Keveiné Bárány Ilona professzor asszony tiszteletére.* Szeged, SZTE Éghajlattani és Tájföldrajzi Tanszék, 2006. 489–496.

Mezei (2019) = Mezei Kitti: A szervezett bűnözés az interneten. In: Mezei Kitti (szerk.): *A bűnügyi tudományok és az informatika.* Pécs, Budapest, Pécsi Tudományegyetem, MTA TK, 2019. 125–147.

Mezei (2021) = Mezei Kitti: Az online gyermekpornográfia és a büntetőjog. *Ügyészek Lapja*, 2021/4. 19–30.

Mezei (2022a) = Mezei Kitti: Új tendenciák a kiberbűnözés büntetőjogi megítélésében. In: Gárdos Orosz Fruzsina (szerk.): *A magyar jogrendszer rezilienciája 2010–2020.* Budapest, ORAC Kiadó, 2022. 529–549.

Mezei (2022b) = Mezei Kitti: *A kiberbűnözés aktuális kihívásai a büntetőjogban.* Budapest, L'Harmattan Kiadó – MTA Társadalomtudományi Kutatóközpont, Jogtudományi Intézet, 2022.

Mezey (2011) = Mezey Barna (szerk.): *Magyary Zoltán – „A tudományos versenyben megállás nincs". Válogatott tanulmányok.* Budapest, Gondolat kiadó, 2011.

Mitchell (2012) = David Mitchell: *Felhőatlasz,* Budapest, Cartaphilus Kiadó, 2012.

Molnár Anna – Molnár Dóra (2022) = Molnár Anna – Molnár Dóra: *Kiberdiplomácia.* Budapest, Ludovika Egyetemi Kiadó, 2022.

Molnár Dóra (2020) = Molnár Dóra: Nagyhatalmi kiberdiplomácia – az Egyesült Államok, Kína és Oroszország a nemzetközi kiberporondon. In: Török Bernát (szerk.): *Információ- és kiberbiztonság.* Budapest, Ludovika Egyetemi Kiadó, 2020. 357–373.

Molnár Ferenc (2008) = Molnár Ferenc: NATO-csúcstalálkozók Washingtontól Bukarestig. *Nemzet és Biztonság,* 2008. április. 48–57.

Molnár Ferenc (2012) = Molnár Ferenc: Egy sikeresebb válságkezelés felé: A civil szakértelem szükségessége a NATO stabilizációs és újjáépítési feladatai során. *Nemzet és Biztonság*, 2012/4. 10–23.

Molnár Ferenc (2021) = Molnár Ferenc: A reziliencia kérdése és a NATO. *Védelmi-Biztonsági Szabályozási és Kormányzástani Műhelytanulmányok,* 2021/15. 1–14.

Molnár–Kollányi–Székely (2007) = Molnár Szilárd – Kollányi Bence – Székely Levente: Társadalmi hálózatok, hálózati társadalom. In: Pintér Róbert (szerk.): *Az információs társadalom – Az elmélettől a politikai gyakorlatig.* Budapest, Gondolat – Új Mandátum, 2007. 64–81.

Moore (1965) = Gordon E. Moore: Cramming more components onto integrated circuits. *Electronics,* 1965/8. 82–85.

Morris (2020) = Ian Morris: *Háború!* Budapest, Antall József Tudásközpont, 2020.

Mosco (2019) = Vincent Mosco: *Okosvárosok a digitális világban.* Budapest, Pallas Athéné, 2019.

Munk (2018) = Munk Sándor: A kibertér fogalmának egyes, az egységes értelmezést biztosító kérdései. *Hadtudomány,* 2018/1. 113–131.

Murphy–Kondrasov–Bailey (1998) = David E. Murphy – Szergej A. Kondrasov – George Bailey: *A láthatatlan front.* Budapest, Kossuth Kiadó, 1998.

Murray (2020) = Douglas Murray: *A tömegek tébolya – Áldozatok a politikai korrektség oltárán?* Budapest, Alexandra, 2020.

Murray–Mansoor (2012) = Williamson Murray – Peter R. Mansoor: *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present.* Cambridge, Cambridge University Press, 2012.

Nagy Károly (1999) = Nagy Károly: Titok és biztonság az információs társadalomban. *Belügyi Szemle,* 1999/4–5. 172–183.

Nagy Szabolcs (2016) = Nagy Szabolcs: *Muli püspök temet: Tanácsköztársaság Pápán.* Pápa, Jókai Mór Városi Könyvtár, 2016.

Nagy Szabolcs (2017) = Nagy Szabolcs: Igazságosság vagy jogbiztonság? Rendszerváltozások utáni büntetőjogi felelősségre vonások a 20. századi magyar történelemben. In: Keserű Barna Arnold (szerk.): *Doktori Műhelytanulmányok 2017.* Győr, Széchenyi István Egyetem Állam- és Jogtudományi Doktori Iskola, 2017. 183–198.

Nagy Szabolcs (2020) = Nagy Szabolcs: Adalékok a Tanácsköztársaság dunántúli történetéhez. In: Paksy Zoltán (szerk.): *Tanácsköztársaság Zala megyében.* Zalaegerszeg, Magyar Nemzeti Levéltár Zala Megyei Levéltára, 2020. 9–27.

Nasr et al. (2016) = Elie Nasr – Elie Kfoury – Maya Kfoury – Liliane Karam: *An Analytical Approach to Psychological Behavior of Hackers' Motives* ce.sc.edu/cyberinfra/docs/publications/An_Analytical_Approach_to_Psychological.pdf

Nelson (1971) = Keith L. Nelson: The Warfare State: History of Concept. *Pacific Historical Review,* 1971/2. 127–143.

Németh (2019) = Németh Richárd: Kibertámadások gazdasági vonatkozásai a vállalati szférában. In: Dernóczy-Polyák Adrienn (szerk.): *Kutatási jelentés 1. Győr.* Universitas-Győr Nonprofit Kft., 2019. 307–325.

Németh (2020) = Németh Richárd: Kiberfenyegetettség nagyvállalati környezetben. *Magyar Bűnüldöző*, 2020/2. 23–41.

Németh (2021a) = Németh Richárd: A kibertérből érkező fenyegetések elleni védekezés vállalati környezetben. *GIKOF Journal*, 2021. 15–26.

Németh (2021b) = Németh Richárd: A COVID–19 járvány okán bevezetett home office munkavégzés hatása a munkakörülményekre és szervezeti kommunikációra nagyvállalati környezetben. *Jog Állam Politika*, 2021/4. 87–109.

Nielsen–Snider (2009) = Suzanne C. Nielsen – Don M. Snider (szerk.): *American Civil-Military Relations. The Soldier and the State in a New Era.* Blatimore, The Johns Hopkins University Press, 2009.

Nogel (2022) = Nogel Mónika: Bűnös vagy ártatlan? Igazságügyi genetikus szakértői vélemények relevanciája a védelem számára. *Belügyi Szemle,* 2022/3. 481–503.

Nolte (2003) = Georg Nolte: *European Military Law Systems*, Berlin, De Gruyter Recht, 2003.

Nyáry (2020) = Nyáry Gábor: Kiberdiplomácia: Hatalom, politika és technológia a geopolitika ötödik dimenziójában. In: Török Bernát (szerk.): *Információ- és kiberbiztonság.* Budapest, Ludovika Egyetemi Kiadó, 2020. 321–342.

Nyitrai (2017) = Nyitrai Mihály: Összehasonlító tanulmány az Európai Unió és az Egyesült Államok kritikus infrastruktúra védelem szabályozása és megvalósítása területén. *Hadtudományi Szemle,* 2017/2. 232–253.

O'Hara–Hall (2018) = Kieron O'Hara – Wendy Hall: *Four Unternets. The Geopolitics of Digital Governance. CIGI Papesrs No. 206.* Waterloo, Centre for International Governance Innovation, 2018.

Ortega y Gasset (2019) = José Ortega y Gasset: *A tömegek lázadása.* Budapest, Helikon Kiadó, 2019.

Oteren et al. (2016) = Suleyman Oteren – M. Salih Elmas – Hakan Hekim – Halil Ibrahim Canbegi: *ISIS inf Cyberspace: Findings From Social Media Research.* Ankara, GLOBAL Policy and Strategy Report 7, 2016.

Padányi–Tomolyka (2017) = Padányi József – Tomolyka János: Háború és béke Ukrajnában, avagy keleten a helyzet változatlan. *Hadtudományi Szemle,* 2017/3-4. 63–83.

Páll-Orosz (2021) = Páll-Orosz Piroska: Attribúció (betudás) a kibertérben. In: Kenedli Tamás (szerk.): *Nemzetbiztonsági Tanulmányok II.* Budapest, Katonai Nemzetbiztonsági Szolgálat, 2021. 66–84.

Pandit (2015) = Chanakya Pandit: *Artha-sásztra.* Budapest, Danvantara Kiadó, 2015.

Pataki–Kelemen (2014) = Pataki Márta – Kelemen Roland: Kiberterrorizmus: A terrorizmus új arca. *Magyar Rendészet,* 2014/5. 103–116.

Patyi (2015) = Patyi András: Demokratikus legitimáció, választási felhatalmazás és alkotmány a haderő mögött. *Hadtudomány,* 2015/1–2. 72–75.

Patyi (2016) = Patyi András: A védelmi alkotmány alapkérdése: A fegyveres erő rendeltetése. In: Csefkó Ferenc (szerk.): *Közjog és jogállam: Tanulmányok Kiss László professzor 65. születésnapjára.* Pécs, PTE Állam- és Jogtudományi Kar, 2016. 233–249.

Pavelec (2015) = S. Michael Pavelec: Cyber Warfere in the Professional Military Education System. In: Paul J. Spinger (szerk.): *Cyber Warfare*. Santa Barbara–Denver–Oxford, ABC–CLIO, 2015. 120–124.

Peikari–Lotfi–Makhdomi (2015) = Naser Peikari – Rasoul Lotfi – Hadi Makhdomi: Social Networks, Cyberspace and Formation of Virtual Identity of the Users. *International Journal of Advanced Studies in Humanities and Social Science,* 2015/1. 92–101.

Perrin (2020) = Cédric Perrin: *Russian Military Modernisation: Challanges ahead for NATO Allies.* Brussels, NATO Parliamentary Assembly Defence And Security Committee, 2020.

Peschka (1988) = Peschka Vilmos: *A jog sajátossága*, Budapest, Akadémia Kiadó, 1988.

Petruska (2021) = Petruska Ferenc: A Lawfare fogalma. *Katonai Jogi és Hadijogi Szemle*, 2021/3. 97–106.

Petruska (2022a) = Petruska Ferenc: A lawfare tipológiája. *Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok*, 2022/16. 1–12.

Petruska (2022b) = Petruska Ferenc: Lawfare a védelmi szférában. *Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok*, 2022/18. 1–16.

Petruska (2022c) = Petruska Ferenc: A jogi hadviselés eszköztára. *Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok*, 2022/17. 1–16.

Petruska–Vikman (2021) = Petruska Ferenc – Vikman László: Egy formabontó hírszerzési nyilatkozat a jogi sérülékenységek szempontjából. *Military and Intelligence CyberSecurity Research Paper*, 2021/4. 1–22.

Piekalkiewicz (1998) = Janusz Piekalkiewicz: *A kémkedés világtörténete I–II.* Budapest, Zrínyi Kiadó, 1998.

Pilch (1996) = Pilch Jenő: *A papirusz titkai: a kémkedés története I–III.* Budapest, Kassák Kiadó, 1996.

Pintér István (2016) = Pintér István: A virtuális tér geopolitikája. In: Pintér István (szerk.): *A virtuális tér geopolitikája – Geopolitikai Tanács Műhelytanulmányok*. Budapest, Geopolitikai Tanács Közhasznú Alapítvány, 2016. 285–366.

Pintér Róbert (2007) = Pintér Róbert: Úton az információs társadalom megismerése felé. In: Pintér Róbert (szerk.): *Az információs társadalom – Az elmélettől a politikai gyakorlatig.* Budapest, Gondolat – Új Mandátum, 2007. 11–28.

Pirisi–Trócsányi (2015) = Pirisi Gábor – Trócsányi András: *Általános társadalom– és gazdaságföldrajz.* 2015. tamop412a.ttk.pte.hu/files/foldrajz2/ch01s02.html

Pirisi–Trócsányi (2019) = Pirisi Gábor – Trócsányi András: *Fejezetek a társadalomföldrajz világából*. Pécs, Publikon Kiadó, 2019.

Pongrácz (2014a) = Pongrácz Alex: The Tropes of Globalization. In: Kálmán János (szerk.): *Legal Studies on Contemporary Hungarian Legal System.* Győr, Universitas-Győr Nonprofit Kft., 2014. 275–291.

Pongrácz (2014b) = Pongrácz Alex: A globalizáció toposzai. In: Kecskés Gábor (szerk.): *Doktori Műhelytanulmányok 2014.* Győr, Széchenyi István Egyetem Állam– és Jogtudományi Doktori Iskola, 2014. 157–168.

Pongrácz (2015) = Pongrácz Alex: Globalizáció: államelhalás vagy államépítés? In: Takács Péter (szerk.): *Az állam szuverenitása: eszmény és/vagy valóság: Interdiszciplináris megközelítések.* Budapest–Győr, MTA Jogtudományi Intézet – Gondolat Kiadói Kör, 2015. 222–237.

Pongrácz (2016) = Pongrácz Alex: Szuverenitás és alkotmányosság a globális erőtérben. *Pro Publico Bono,* 2016/1. 108–119.

Pongrácz (2017a) = Pongrácz Alex: Az állam gazdaságpolitikai szerepvállalásának változásai. *Pro Publico Bono: Magyar Közigazgatás,* 2017/3. 168–195.

Pongrácz (2017b) = Pongrácz Alex: A politika folytatása más eszközökkel? Avagy gondolatok az állam és az erőszak kérdésköréről. *Államtudományi Műhelytanulmányok*, 2017/17. 1–24.

Pongrácz (2018a) = Pongrácz Alex: A hálózat csapdájában? Globalizáció és totalitás. In: Farkas Ádám (szerk.): *Védelmi alkotmányosság az új típusú biztonsági kihívások erőterében.* Budapest, Magyar Katonai Jogi és Hadijogi Társaság, 2018. 41–62.

Pongrácz (2018b) = Pongrácz Alex: A szuverenitásfogalom változásának 21. századi fejleményei. *Pro Publico Bono,* 2018/2. 128–153.

Pongrácz (2019a) = Pongrácz Alex: *Nemzetállamok és új szabályozó hatalmak a globális erőtérben – avagy megszelídíthető–e a globalizáció?* Budapest, Dialóg Campus, 2019.

Pongrácz (2019b) = Pongrácz Alex: Államkudarc és államépítés, avagy egy valós kihívás koncepcionális értelmezései és a katonai kezelés állami aspektusai. In: Farkas Ádám (szerk.): *Az állam katonai védelme az új típusú biztonsági kihívások tükrében.* Budapest, Nemzeti Közszolgálati Egyetem Közigazgatási Továbbképzési Intézet, 2019. 19–28.

Pongrácz (2020) = Pongrácz Alex: Mozaikok a magyar szuverenitásfelfogás történetéből. In: Karácsony András (szerk.): *Szuverenitáskérdések. Elméletek, történetek.* Budapest, Gondolat Kiadó, 2020. 98–113.

Pongrácz (2021a) = Pongrácz Alex: Az egyén az állam ellen (?) Aktuálisak–e Spencer nézetei a 21. században? In: Tóth J. Zoltán (szerk.): *Herbert Spencer öröksége: Tanulmányok, reflexiók Herbert Spencer születésének 200. évfordulója alkalmából.* Budapest, Károli Gáspár Református Egyetem, Állam– és Jogtudományi Kar, 2021. 141–158.

Pongrácz (2022) = Pongrácz Alex: Variációk hibrid állammodell–építésére. *Military and Intelligence Cybersecurity Research Paper*, 2022/3. 1–12.

Pongrácz–Téglási (2021) = Pongrácz Alex – Téglási András: Szociális állam, jóléti állam – Elméleti és történeti alapvetés. In: Bódi Stefánia – Schweitzer Gábor (szerk.): *Az emberi jogok alkotmányos védelme Magyarországon.* Budapest, Ludovika Egyetemi Kiadó, 2021. 295–311.

Porkoláb (2015) = Porkoláb Imre: Hibrid hadviselés: Új hadviselési forma, vagy régi ismerős? *Hadtudomány,* 2015/3–4. 36–48.

Porkoláb (2019) = Porkoláb Imre: *A Stratégia Művészete: Szervezeti innováció kiszámíthatatlan környezetben*. Budapest, HVG Könyvek, 2019.

Porter (1994a) = Bruce D. Porter: The Warfare State. *American Heritage*, 1994/4. szám americanheritage.com/warfare–state#1

Porter (1994b) = Bruce D. Porter: *War and the Rise of the State – The Military Foundations of Modern Politics.* New York, The Free Press, 1994.

Póti (2017) = Póti László: Minszk–2 után két évvel: Hol tart a békefolyamat? *KKI Elemzések*, 2017/5.

Prakash (2018a) = Abishur Prakash: *Új geoplitika – A világ jövője technológia, I–II. kötet.* Budapest, Pallas Athéné Könyvkiadó, 2018.

Prakash (2018b) = Abishur Prakash: *Go. AI – A mesterséges intelligencia geopolitikája.* Budapest, Pallas Athéné Könyvkiadó, 2018.

Price (2018) = Caterine Price: *Digitális detox*. Budapest, Libri Könyvkiadó, 2018.

Puddephatt (2006) = Andrew Puddephatt: *Voices of war: Conflict and the role of the media.* Denmark, International Media Support, 2006.

Pyhnöniemi (2021) = Katri Pyhnöniemi: The Concept of Hybrid War in Russia: A National Security Threat and Mean of Strategic Coercion. *Hybrid Coe Strategis Analysis*, 2021.

Rab–Szemerey (2018) = Rab Judit – Szemerey Samu: *Az okos város fejlesztési modell módszertani alapjai.* Budapest, Lechner Nonprofit Kft, 2018.

Ramge–Mayer-Schönberger (2018) = Thomas Ramge – Viktor Mayer-Schönberger: *Reinventing Capitalism in the Age of Big Data*. London, Basic Books, 2018.

Raymond (1996) = Eric S. Raymond: *The newhacker's dictionary.* Cambridge, MIT Press, 1996.

Renz–Smith (2016) = Bettina Renz – Hanna Smith: *Russia and Hybrid Warfare – Going beyond the Label.* Helsinki, Aleksanteri Institute, 2016. helda.helsinki.fi/bitstream/handle/10138/175291/renz_smith_russia_and_hybrid_warfare.pdf

Resperger (2018a) = Resperger István: *A válságkezelés és a hibrid hadviselés.* Budapest, Dialóg Campus, 2018.

Resperger (2018b) = Resperger István (szerk.): *A nemzetbiztonság elmélete a közszolgálatban.* Budapest, Dialóg Campus Kiadó, 2018.

Resperger (2018c) = Resperger István (szerk.): *Nemzetbiztonsági alapismeretek.* Budapest, Dialóg Campus, 2018.

Ringsmose–Rynning (2011) = Jens Ringsmose – Sten Rynning: *NATO's New Strategic Concept: A Comprehensive Assessment.* DIIS Report 2011:02., Copenhagen, Danish Institute for International Studies, 2011.

Ripsman–Paul (2005) = Norrin M. Ripsman – T. V. Paul: Globalization and the National Security State: A Framework for Analysis. *International Studies Review*, 2005/2. 199–227.

Roberts et al. (2010) = Hal Roberts – Ethan Zuckerman – Rob Faris – John Palfrey: Circumvention Tool Usage Report, *Digital Acces to Scholarship at Harvard*, 2010. dash.harvard.edu/handle/1/5366727

Roepke–Thankey (2019) = Wolf-Diether Roepke – Hasit Thankey: Resilience: The First Line of Defence. *The Three Sword Magazine*, 2019/34. 50–53.

Rosenstedt (2021) = Lina Rosenstedt: Improving Cooperation with Social Media Companies to Counter Electoral Interference. *Hybrid Coe Paper*, 2021/5. 1–13.

Rózsa (2014) = Rózsa Tibor: A befolyásolás művészet. *Hadtudományi Szemle,* 2014/2. 44–53.

Ságvári (2017) = Ságvári Ádám: Különleges jogrend a francia jogban: Állandósult különlegesség. *Iustum Aequum Salutare,* 2017/4. 179–188.

Sari (2017) = Aurel Sari: *Hybrid Warfare, Law and the Fulda Gap.* Exeter, University of Exeter Law School, 2017.

Sari (2018) = Aurel Sari: Blurred Lines: Hybrid Threats and the Politics of International Law. Helsinki. *The European Centre of Excellence for Countering Hybrid Threats*, 2018/4. 1–9.

Sari (2019) = Aurel Sari: Hybrid Warfare, Law and the Fulda Gap. In: Christopher M. Ford – Winston S. Williams (szerk.): *Complex Battle Spaces – The Law of Armed Conflict and the Dynamics of Modern Warfare.* New York, Oxford University Press, 2019. 161–190.

Sari (2019) = Aurel Sari: *Legal Resilience in an Era of Gray Zone Conflicts and Hybrid Threats*. Exeter, Exeter Centre for International Law, 2019.

Sari (2019a) = Aurel Sari: Legal Resilience in an Era of Gray Zone Conflicts and Hybrid Threats. *Exeter Centre for International Law Working Paper Series* 2019/1. socialsciences.exeter.ac.uk/media/universityofexeter/collegeofsocialsciencesandinternationalstudies/lawimages/research/Sari_-_Legal_Resilience_ECIL_WP_2019-1.pdf

Schmitt (2002) = Carl Schmitt: *A politikai fogalma.* Budapest, Osiris – Pallas Stúdió – Attraktor, 2002.

Schmitt (2013) = Michael N.Schmitt: *Tallinn Manual on International Law applicable to cyber warfare.* Cambridge, Cambridge University Press, 2013.

Schmitt (2017) = Michael N. Schmitt (szerk.): *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations – Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence*. Cambridge, Cambridge University Press, 2017.

Schühly–Becker–Klein (2020) = Andreas Schühly – Frank Becker – Florian Klein: *Valós idejű stratégia – Amikor a stratégiai előrejelzés és a mesterséges intelligencia találkozik.* Budapest, Pallas Athéné Könyvkiadó, 2020.

Scott (2018) = Paul F. Scott: *The National Security Constitution.* London, Hart Publishing, 2018.

Seethal–Menaka (2019) = K. Seethal – B. Menaka: Digitalisation Of Education In 21st Century: A Boon Or Bane. *International Journal for Research in Engineering Application & Management,* 2019. 140–143.

Segal (2020) = Adam Segal: China's Vision for Cyber Sovereignty and the Global Governance of Cyberspace. In: Nadége Rolland (szerk.): *An Emerging China-Centric Order – China's Vision for a New World Order in Practice.* Seattle, The National Bureau of Asian Research, 2020. 85–100.

Segura–Waisbord (2018) = María Soledad Segura – Silvio Waisbord: Between Data Capitalism and Data Citizenship. *Television & New Media,* 2018/4. 412–419.

Sepsi (2019) = Sepsi Tibor: *GDPR útikalauz adatkezelőknek.* Budapest, Wolters Kluwer, 2019.

Siboni–Cohen–Rotbart (2013) = Gabi Siboni – Daniel Cohen – Aviv Rotbart: The Threat of Terrorist Organizations in Cyberspace. *Military and Strategic Affairs,* 2013/3. 3–29.

Simicskó (2017) = Simicskó István: A hibrid hadviselés előzményei és aktualitásai. *Hadtudomány,* 2017/3–4. 3–16.

Simon (2015) = Simon László: A fokozódó terrorizmus Európában és annak hatása a katonai tömegrendezvények biztosítására. *Szakmai Szemle – A Katonai Nemzetbiztonsági Szolgálat tudományos–szakmai folyóirata*, 2015/2. 145–162.

Simon (2016a) = Simon László: A titok speciális értelmezése az elmúlt 25 év kihívásainak, kockázatainak és fenyegetéseinek tükrében. *Felderítő Szemle*, 2016/1. 67–87.

Simon (2016b) = Simon László: Az információ mint fegyver? *Szakmai Szemle*, 2016/1. 34–60.

Simon (2017) = Simon László: A partizán elmélete a premodern virtuális korban. *Jog, Állam, Politika,* 2017/4. 233–242.

Simon (2022) = Simon László: Az egyén mint nem állami szereplő a kibertérben megjelenő fenyegetési palettán, avagy a kiberpartizán kérdése. *Military and Intelligence CyberSecurity Research Paper,* 2022/10. 1–24.

Simon–Magyar (2017a) = Simon László – Magyar Sándor: A terrorizmus és indirekt hatása a kibertérben. *Nemzetbiztonsági Szemle*, 2017/3. 89–101.

Simon–Magyar (2017b) = Simon László – Magyar Sándor: A terrorizmus és indirekt hadviselése az EU kiberterében. *Szakmai Szemle,* 2017/4. 57–68.

Singer–Brooking (2018) = P. W. Singer – Emerson T. Brooking: *Likewar: The Weaponization of Social Media.* Boston – New York, Houhton Mifflin Harcourt, 2018.

Siposné Kecskeméthy (2017) = Siposné Kecskeméthy Klára: NATO-csúcstalálkozó az elrettentés és a védelem jegyében (Varsó, 2016. július 8–9.). *Hadtudomány,* 2017/1–2. 114–126.

Smith, T. E. (2017) = Tory E. Smith: The Specter of Cyber in the Service of the Islamic State. *American Intelligence Journal*, 2017/1. 54–58.

Smith, Z. M. (2017) = Zachary M. Smith: Cyber Security. In: Paul J. Spinger (szerk.): *Encyclopedia of Cyber Warfare*. Santa Barbara–Denver, ABC–CLIO, 2017. 62–66.

Somkutas–Kőhidi (2017) = Somkutas Péter – Kőhidi Ákos: Az önvezető autó szoftvere magas szintű szellemi alkotás vagy kifinomult károkozó? *In Media Res*, 2017/2. 232–269.

Somodi–Kiss (2019) = Somodi Zsolt – Kiss Álmos Péter: A hibrid hadviselés fogalmának értelmezése a nemzetközi szakirodalomban. *Honvédségi Szemle,* 2019/6. 22–28.

Sorbán (2020) = Sorbán Kinga: A bosszúpornó és deepfake pornográfia büntetőjogi fenyegetettségének szükségességéről. *Belügyi Szemle*, 2020/10. 81–104.

Sørensen–Nyemann (2018) = Heine Sørensen – Dorthe Bach Nyemann: *Going beyond resilience: A revitalized approach to countering hybrid threats.* Helsinki, The European Centre of Excellence for Countering Hybrid Threats, 2018.

Sparrow (2011) = James T. Sparrow: *Warfare State – World War II Americans and the Age of Big Government*. Oxford, Oxford University Press, 2011.

Spitzer (2018) = Spitzer Jenő: A dróntámadások nemzetközi joggal való összeegyeztethetőségének egyes kérdései, kitekintéssel a drónok védelmi célú alkalmazásának más perspektíváira. In: Farkas Ádám (szerk.): *Védelmi alkotmányosság az új típusú biztonsági kihívások erőterében.* Budapest, Magyar Katonai Jogi és Hadijogi Társaság, 2018. 101–146.

Spitzer (2019a) = Spitzer Jenő: *Önvédelem versus terrorizmus – Az erőszak tilalma és az önvédelem joga a nemzetközi jogban, különös tekintettel az Iszlám Állam elleni nemzetközi fellépés lehetőségeire*. Magyar Katonai Jogi és Hadijogi Társaság, Budapest, 2019.

Spitzer (2019b) = Spitzer Jenő: A különleges jogrend szabályozása az egyes alkotmányokban IV. – Különleges jogrendi szabályozás a francia jogrendszerben. *Vélemények a katonai jog világából,* 2019/4. 1–13.

Spitzer (2020a) = Spitzer Jenő: A felfegyverzett drónok alkalmazásának egyes nemzetközi jogi kérdései. In: Farkas Ádám – Végh Károly (szerk.): *Új típusú hadviselés a 21. század második évtizedében és azon túl. Intézményi és jogi kihívások.* Budapest, Zrínyi Kiadó, 2020. 172–190.

Spitzer (2020b) = Spitzer Jenő: Különleges jogrendi szabályozás a francia jogrendszerben. In: Farkas Ádám – Kelemen Roland (szerk.): *Szkülla és Kharübdisz között – Tanulmányok a különleges jogrend elméleti és pragmatikus kérdéseiről, valamint nemzetközi megoldásairól.* Budapest, Magyar Katonai Jogi és Hadijogi Társaság, 2020. 281–316.

Spitzer (2020c) = Spitzer Jenő: A nemzetbiztonsági szolgálatok helye, szerepe Franciaország védelmi és biztonsági rendszerében. *Katonai Jogi és Hadijogi Szemle,* 2020/4. 69–93.

Spitzer (2021) = Spitzer Jenő: A francia kibervédelmi és -biztonsági rendszer egyes stratégiai aspektusai. *Military and Intelligence CyberSecurity Research Paper,* 2021/3. 1–16.

Spitzer–Vikman (2022a) = Spitzer Jenő – Vikman László: Katonai és nemzetbiztonsági képességfejlesztések és azok jogi, jogpolitikai háttere egyes transzatlanti államokban. *Military and Intelligence CyberSecurity Research Paper,* 2022/13. 1–34.

Spitzer–Vikman (2022b) = Spitzer Jenő – Vikman László: A honvédelmi szabályozás egyes lehetséges külföldi mintáinak áttekintése. *Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok,* 2022/31. 1–27.

Steenkamp (2017) = Christina Steenkamp: The Crime-Conflict Nexus and the Civil War in Syria. *Stability – International Journal of Security & Development,* 2017/1. 1–18.

Stokes (2009) = Christopher Stokes: Chapter 2 – OSI Model and Then Some. In: Dale Liu (szerk.): *Next generation SSH2 implementation: securing data in motion.* Burlington, Elsevier, 2009. 15–40.

Stollsteiner (2021) = Stollsteiner Gabriel: Franciaország: Folyamatosan különleges jogrend, koronavírus idején is. In: Nagy Zoltán – Horváth Attila: *A különleges jogrend és nemzeti szabályozási modelljei.* Budapest, Mádl Ferenc Összehasonlító Jogi Intézet, 2021. 322–340.

Störig (2005) = Hans Joachim Störig: *A filozófia világtörténete.* Budapest, Helikon Kiadó, 2005.

Stuart (2008) = Douglas T. Stuart: *Creating the National Security State. A History of the law that transformed America*. Princeton, Princeton University Press, 2008.

Stumpf (2014) = Stumpf István: Új államalapítás? Alkotmányos és kormányzati kihívások. In: Stumpf István (szerk.): *Erős állam – alkotmányos korlátok*. Budapest, Századvég Kiadó, 2014. 17–48.

Suler (2015) = John R. Suler: *Psychology of the Digital Age: Humans Becoma Electric.* Cambridge, Cambridge University Press, 2015.

Sulyok (2002) = Sulyok Gábor: Az egyéni vagy kollektív önvédelem joga az Észak-Atlanti Szerződés 5. cikkének tükrében. *Állam és Jogtudomány*, 2002/1–2. 99–136.

Sulyok (2005) = Sulyok Gábor: A terrorcselekmény elkövetéséhez használt polgári légi jármű lelövésének nemzetközi jogi és alkotmányjogi megítélése. *Fundamentum*, 2005/3. 30–56.

Sulyok (2019) = Sulyok Gábor: A terrorcselekmény elkövetéséhez használt polgári légi jármű lelövésének alkotmányjogi megítélése az új szabályozási környezetben. In: Bartkó Róbert (szerk.): *A terrorizmus elleni küzdelem aktuális kérdései a XXI. században.* Budapest, Gondolat, 2019. 35–60.

Szalai (2020) = Szalai Ádám: Az okosváros-koncepciók kritikai földrajzi vizsgálata – elméleti háttér és lehetséges kutatási irányok. *Tér és Társadalom*, 2020/2. 88–107.

Szálkai–Stepper (2015) = Szálkai Kinga – Stepper Péter (szerk.): *A biztonság szektorális értelmezése. Új kihívások a kutatás napirendjén.* Pécs–Budapest, Publikon kiadó, 2015.

Szaniszló (2016) = Szaniszló Krisztián: A hatalommegosztás államelméleti előképei – Hatalomkorlátozás az európai állambölcseletben az antikvitás korától a felvilágosodásig. *Acta Humana,* 2016/1. 63–88.

Szeles (2005) = Szeles Péter: A civil-katonai együttműködés public relations aspektusai. *Kard és toll*, 2005/3. 67–77.

Szendy (2017) = Szendy István: A hadviselés, mint tudományelméleti és tudomány-rendszertani kategória. *Hadtudomány,* 2017/3–4. 106–129.

Szenes (2014) = Szenes Zoltán: Előre a múltba? A NATO Wales után. *Külügyi Szemle,* 2014/ősz 3–26.

Szenes (2018) = Szenes Zoltán: Transzatlanti „Super Bowl". *Hadtudomány,* 2018/3–4. 43–65.

Szentgáli (2012) = Szentgáli Gergely: A NATO kibervédelmi politikájának fejlődése. *Bolyai Szemle,* 2012/2. 79–93.

Szépvölgyi (2020) = Szépvölgyi Enikő: A dualizmuskori állami gyermekvédelem és a szegénység összefüggései. *Jog Állam Politika,* 2020/3. 101–116.

Szépvölgyi (2021) = Szépvölgyi Enikő: Gondolatok az állami gyermekvédelemről szóló törvénycikkek 120. évfordulójára. In: Mezey Barna (szerk.): *Kölcsönhatások. Európa és Magyarország a jogtörténelem sodrásában.* Budapest, Gondolat Kiadó, 2021. 316–323.

Szigeti (2001) = Szigeti Péter: Vázlat a közbiztonság három dimenziójáról: világrendszer – nemzetállami szint és lokalitás. In: Szigeti Péter: *A valóság vonzásában – Jogelméleti* és *Jogtudományi Közlöny,* Győr, ELTE–SZIF ÁJK, 2001. mek.oszk.hu/04200/04241/04241.htm#16

Szigeti (2005) = Szigeti Péter: *Világrendszernézőben: globális „szabad verseny" – A világkapitalizmus jelenlegi stádiuma.* Budapest, Napvilág Kiadó, 2005.

Szigeti (2011) = Szigeti Péter: *Társadalomkutatás – Mi végre? Politikatudomány, alkotmányjog, világrendszerelmélet.* Győr, Universitas, 2011.

Szigeti (2017) = Szigeti Péter: Kapitalizmusfogalmak és a tőkés termelési mód elmélete. *Eszmélet*, 2017/ősz/melléklet.

Szikszai (2020) = Szikszai Marcel: Disztópia Kínában? Tanulmány a társadalmi kreditrendszer a kínai jogfejlődés tükrében. *Infokommunikáció és Jog,* 2020/1. 21–26.

Szkála–Munka (2018) = Szkála Károly – Munka Sándor: A kibertér fogalma, értelmezése és fejlődése. *Földrajzi Közlemények*, 2018/4. 344–355.

Szoboszlai-Kiss (2017) = Szoboszlai-Kiss Katalin: Bevezetés a klasszikus görög államtudományi kutatáshoz: Az antik görög államfejlődés legkorábbi forrásai. *Jog Állam Politika,* 2017/2. 95–116.

Szoboszlai-Kiss (2018) = Szoboszlai-Kiss Katalin: *Alvó demokrácia – Kormányzásról, törvényről, erkölcsről Homérosztól Szókratészig.* Győr, Universitas–Győr Nonprofit Kft., 2018.

Szretykó (2005) = Szretykó György (szerk.): *Tömegkultúra és tömegmanipuláció a modern társadalomban.* Pécs, Comenius Kiadó, 2005.

Sztankai (2012) = Sztankai Krisztián: A civil-katonai együttműködés, a lélektani műveletek és a kulturális antropológia kapcsolata. *Hadtudomány*, 2012/elektronikus szám. 1–7.

Szun Ce (2006) = Szun Ce: *A háború művészete.* Budapest, Carthaphillus, 2006.

Taddeo–Glorioso (2017) = Mariarosaria Taddeo – Ludovica Glorioso (szerk.): *Ethics and Policies for Cyber Operations*. Springer, 2017.

Taj Kung (2016) = Taj Kung: *A háború törvényei.* Budapest, Helikon Kiadó, 2016.

Takács (2016) = Takács Péter: Társadalmi szerződések elméletei. In: Egresi Katalin – Pongrácz Alex – Szigeti Péter – Takács Péter: *Államelmélet.* Győr, SZE DF ÁJK Jogelméleti Tanszék, 2016. 66–86.

Techet (2013) = Techet Péter: *Carl Schmitt. Egy szellemi kalandor.* Máriabesnyő, Attraktor Kiadó, 2013.

Tilesch–Hatamleh (2021) = Tilesch György – Omar Hatamleh: *Mesterséges intelligencia – Vegyük kezünkbe a sorsunkat az MI korában.* Budapest, Libri, 2021.

Till (2017) = Till Szabolcs: *A honvédelmi alkotmányosság 30 éve Magyarországon 1988–2017.* Budapest, Zrínyi Kiadó, 2017.

Till (2021) = Till Szabolcs Péter: Az Alaptörvény kilencedik módosítása szerinti intézményrendszer előzetes értékelése a megvalósítási átmeneti idő első évi fejleményei alapján. *Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok,* 2021/19. 1–39.

Titmuss (2006) = Richard Titmuss: Universal versus Selection. In: Christopher Pierson – Francis G. Castel (szerk.): *The Welfare State Reader (Second Edition).* Cambridge, Polity Press, 2006. 40–48.

Toffler (2001) = Alvin Toffler: *A harmadik hullám (információs társadalom A–tól Z–ig).* Budapest, Typotex, 2001.

Tomcsányi (1932) = Tomcsányi Móricz: *Magyarország közjoga.* Budapest, Királyi Magyar Egyetemi Nyomda, 1932.

Tomcsányi (2018) = Tomcsányi Móricz: *A magyar közigazgatási jog alapintézményei.* Budapest, Dialóg Campus Kiadó, 2018.

Tóth András (2018) = Tóth András (szerk.): *Az infokommunikációs és technológia jog alapjai.* Budapest, Nemzeti Közszolgálati Egyetem, 2018.

Tóth András (2022) = Tóth András: *A digitális állam információbiztonsági kihívásai.* Budapest, Ludovika Egyetemi Kiadó, 2022.

Tóth Tamás (2019) = Tóth Tamás: Az Európai Unió tervezett kiberbiztonsági tanúsítási keretrendszerének bemutatása. *Szakmai Szemle – A Katonai Nemzetbiztonsági Szolgálat tudományos–szakmai folyóirata* 2019/1. 97–115.

Tóth Zoltán (2016) = Tóth Zoltán Balázs: Az Iszlám Állam online térhódítása. *Nemzetbiztonsági Szemle*, 2016/4. 26–42.

Townsend–Agachi (2020) = Jim Townsend – Anca Agachi: Build Resilience for an Era of Schocks. In: Christopher Skabula (szerk.): *NATO 20/2020. Twenty Bold Ideas to Reimagine the Alliance after the 2020 US Election.* Washington, The Atlantic Council, 2020.

Tőkési (1983) = Tőkési Ferenc (szerk.): *Nomád társadalmak és államalakulatok.* Budapest, Akadémia Kiadó, 1983.

Tömösváry (2017) = Tömösváry Zsigmond: Pjotr Alekszandrovics Rumjancev tábornagy – A hadvezér és az állam. In: Gőcze István (szerk.): *Állam és katona.* Budapest, Dialóg Campus, 2017. 87–106.

Török–Ződi (2021) = Török Bernát - Ződi Zsolt (szerk.): *A mesterséges intelligencia szabályozási kihívásai. Tanulmányok a mesterséges intelligencia és a jog határterületeiről.* Budapest, Ludovika Egyetemi Kiadó, 2021.

Török–Ződi (2022) = Török Bernát – Ződi Zsolt (szerk.): *Az internetes platformok kora.* Budapest, Ludovika Egyetemi Kiadó, 2022.

Treverton et al. (2018) = Gregory F. Treverton – Andrew Thvedt – Alicia R. Chen – Kathy Lee – Madeline McCue: *Adressing hybrid threats.* Stockholm, Swedish Defence University, 2018.

Turkle (2011) = Sherry Turkle: *Alone Together – Why We Expect more from Technology and Less from Each Other.* New York, Basic Books, 2011.

Turovszkij (2020) = Danyiil Turovszkij: *Orosz hekkerek – Így lettek lázadókból Putyin katonái.* Budapest, Athenaeum Kiadó, 2020.

Vajda (2022) = Vajda János: Álmodnak-e az androidok elfogult bírókkal? Kognitív torzítások és önbeteljesítő jóslatok a mesterséges intelligencia peres előrejelzéseiben. *Infokommunikáció és Jog,* 2022/1. 20–22.

Vályi (2004) = Vályi Gábor: Közösségek hálózati kommunikációja. *Szociológiai Szemle,* 2004/4. 47–60.

van Beveren (2001) = John van Beveren: A conceptual model of hacker development and motivations. *Journal of E-Business*, 2001/2. 1–9.

van der Putten et al. (2018) = Frans-Paul van der Putten – Minke Meijnders – Sico van der Meer – Tony van der Togt: *Hybrid Conflict: The Roles of Russia, North Korea and China.* The Hague, Clingendael Institute, 2018.

van der Staak–Wolf (2019) = Sam van der Staak – Peter Wolf (2019): *Cybersecurity in Elections – Models of Interagency Collabiration.* Stockholm, International Institute for Democracy and Electoral Assistance, 2019.

Vikman (2021a) = Vikman László: A műveléttervezés jogi feladatai. *Honvédségi Szemle*, 2021/2. 44–56.

Vikman (2021b) = Vikman László: A közműszolgáltatások és a reziliencia egyes kérdései, különös tekintettel a kiberbiztonságra, *Védelmi–biztonsági Szabályozási és Kormányzástani Műhelytanulmányok*, 2021/14. 1–26.

Vikman (2021c) = Vikman László: A német kiberbiztonsági szisztéma áttekintése. Szervezeti keretek, különös tekintettel a nemzetbiztonsági szolgálatok és a hadsereg szerepére és kapcsolatára, valamint a szabályozási háttér alakulására. *Military and Intelligence CyberSecurity Research Paper,* 2021/2. 1–24.

Vikman (2022a) = Vikman László: Gondolatok a kiberbiztonsági stratégiák fejlesztésére vonatkozó nemzetközi útmutató kapcsán. *SmartLaw Research Group Workin Paper*, 2022/1. 1–12.

Vikman (2022b) = Vikman László: Szempontok a kibertér egyes aktuális fenyegetéseinek jogi értékeléséhez. *Military and Intelligence CyberSecurity Research Paper,* 2022/4. 1–14.

Wallace (2002) = Patricia Wallace: *Az internet pszichológiája.* Budapest, Osiris kiadó, 2002.

Wallerstein (2010) = Immanuel Wallerstein: *Bevezetés a világrendszer-elméletbe*. Budapest, L'Harmattan Kiadó, 2010.

Werbach (2006) = Kevon Werbach: A Layered Model for Internet Policy. *Journal on Telecommunications and High Technology Law,* 2006/2. 37–67.

Winterfeld–Andress (2013) = Steve Winterfeld – Jason Andress: *The Basics of Cyber Warfare Understanding the Fundamentals of Cyber Warfare in Theory and Practice*. Waltham, Elsevier, 2013.

Wither (2020) = James Kennet Wither: Back to the Future? Nordic total defence concepts. *Defence Studies,* 2020/1. 61–81.

Xu et al. (2021) = Joy Xu – Aaron Lio – Harshdeep Dhaliwal – Sorina Andrei – Shakthika Balakrishnan – Uzhma Nagani – Sudipta Samadder: Psychological interventions of virtual gamification within academic intrinsic motivation: A systematic review. *Journal of Affective Disorders,* October 2021. 444–465.

Z. Karvalics (2009) = Z. Karvalics László: „A tudás termelése és elosztása az Egyesült Államokban": Fritz Machlup újraértékelése az információs társadalom elmélettörténetében. *Információs Társadalom,* 2009/2. 20–34.

Zarembo–Solodkyy (2021) = Kateryna Zarembo – Segiy Solodkyy: *The Evolution of Russian Hybrid Warfare: The Case of Ukraine.* Washington, Center for Europan Policy Analysis, 2021. cepa.org/comprehensive-reports/the-evolution-of-russian-hybrid-warfare-ukraine/

Zhang et al. (2015) = Xiong Zhang – Alex Tsang – Wei T. Yue – Michael Chau: The classification of hackers by knowledge exchange behaviors, *Information Systems Frontiers*, 2015/6. 1239–1251

Ződi (2023) = Ződi Zsolt: *Platformjog.* Budapest, Ludovika Egyetemi Kiadó, 2023.

NATO források

Achieve and Maintain Cyberspace Superiorty – Comman Vision for US Cyber Command. United States Cyber Command
cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010

Aktív Szerepvállalás, Modern Védelem – Az Észak-atlanti Szerződés Szervezetének Stratégiai Koncepciója Tagállamainak Védelméről és Biztonságáról
old.biztonsagpolitika.hu/documents/1291766875_NATO_Strat_Koncepcio_2010_hun_BSZK.pdf

Allied Joint Publication-3.20 Allied – Joint Doctrine for Cyberspace Operations. NATO standard, January 2020.

assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf

Brussels Summit Declaration. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels 11–12 July 2018. www.nato.int/cps/en/natohq/official_texts_156624.htm

Chicago Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Chicago on 20 May 2012. www.nato.int/cps/en/natolive/official_texts_87593.htm#cyber

Cyber Defence www.nato.int/cps/en/natohq/topics_78170.htm#

Cyber Defence Pledge www.nato.int/cps/en/natohq/official_texts_133177.htm

Joint Publication 1–02 Department of Defense Dictionary of Military and Associated Terms fas.org/irp/doddir/dod/jp1_02.pdf

Madrid Summit Declaration. Issued by NATO Heads of State and Government participating in the meeting of the North Atlantic Council in Madrid 29 June 2022. www.nato.int/cps/en/natohq/official_texts_196951.htm

NATO – Strengthened Resilience Commitment. 14. Jun. 2021. www.nato.int/cps/en/natohq/official_texts_185340.htm

NATO 2022 Strategic Concept. Adopted by Heads of State and Government at the NATO Summit in Madrid, 29 June 2022. www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf

NATO Advisory Group on Emerging and Disruptive Technologies – Annual Report 2020. Brussels, NATO Emerging Security Challenges Division, 2020. www.nato.int/nato_static_fl2014/assets/pdf/2021/3/pdf/210303–EDT–adv–grp–annual–report–2020.pdf

NATO Allied Joint Doctrine for Information Operations AJP-3.10. info.publicintelligence.net/NATO-IO.pdf

NATO CDS: Enhancing the Resilience of Allied Societies through Civil Preparedness www.nato-pa.int/download-file?filename=/sites/default/files/2021-04/011%20CDS%2021%20E-%20RESILIENCE%20THROUGH%20CIVIL%20PREPAREDNESS_0.pdf

NATO: Commitment to enhance resilience. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw, 8–9 July 2016. www.nato.int/cps/en/natohq/official_texts_133180.htm

NATO: Resilience and Article 3 www.nato.int/cps/en/natohq/topics_132722.htm

North Atlantic Treaty, Washington D. C., 4 April 1949. A szerződés szövegét hazánkban kihírdette: 1999. évi I. törvény a Magyar Köztársaságnak az Észak–atlanti Szerződéshez való csatlakozásáról és a Szerződés szövegének kihirdetéséről

Science and Technology Commitee (STC) – NATO in the Cyber Age: Strengthening Security & Defence, Stablising Deterrence. (Draft General Report) by Susan DAVIS (United States) General Rapporteur. 13 August 2019.
nato-pa.int/download-file?filename=sites/default/files/2019-09/148%20STC%20Davis%20-%20NATO%20IN%20THE%20CYBER%20AGE%20-%20fall%20revision%20-%20clean%2011.9.19.pdf

Statement by the North Atlantic Council concerning malicious cyber activities www.nato.int/cps/en/natohq/official_texts_176136.htm

Wales Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales
www.nato.int/cps/en/natohq/official_texts_112964.htm#cyber

EU források

A Bizottság közleménye a Tanácsnak, az Európai Parlamentnek, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának – A biztonságos információs társadalomra irányuló stratégia: „párbeszéd, partnerség, felvértezés és felelősségvállalás" SEC(2006) 656

A Bizottság Közleménye az Európai Parlamentnek, a Tanácsnak, az Európai gazdasági és Szociális bizottságnak és a Régiók Bizottságának a kritikus informatikai infrastruktúrák védelméről – „Európa védelme a nagyszabású számítógépes támadások és hálózati zavarok ellen: a felkészültség, a védelem és az ellenálló képesség fokozása" SEC(2009) 399, SEC(2009) 400

Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának Európa kibertámadásokkal szembeni ellenálló képességének erősítése, valamint a versenyképes és innovatív kiberbiztonsági ágazat támogatása, COM(2016) 410 final

Brussels, 11 February 2015 (OR. en) 6122/15 Európai Unió Tanácsa Council Conclusions on Cyber Diplomacy

Az Európai Bizottság és az Unió Külügyi és Biztonságpolitikai Főképviselőjének közös közleménye – Cselekvési terv a félretájékoztatással szemben, Brüsszel, 2018.12.15., Join(2018)36. Final; Az Európai Bizottságnak közleménye az Európai Demokráciára vonatkozó cselekvési tervről. Brüsszel, 2020.12.3. COM(2020) 790 Final

Az Európai Bizottság és az Unió Külügyi és Biztonságpolitikai Főképviselőjének közös közleménye – Cselekvési terv a félretájékoztatással szemben, Brüsszel, 2018.12.15., Join(2018) 36. Final

Az Európai Bizottságnak és az Unió Külügyi és biztonságpolitikai főképviselőjének közös közleménye A Covid19–cel kapcsolatos dezinformáció kezelése – lássuk a valós tényeket, Brüsszel, 2020.6.10. Join(2020) 8. Final

Az Európai Bizottságnak közleménye az Európai Demokráciára vonatkozó cselekvési tervről. Brüsszel, 2020.12.3. COM(2020) 790 Final

Az Európai Parlament és a Tanács (EU) 2016/1148 Irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről

Az Európai Parlament és a Tanács (EU) 2019/881 rendelete (2019. április 17.) az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről (kiberbiztonsági jogszabály)

Az Európai Parlament és a Tanács (EU) 2022/2065 Rendelete (2022. október 19.) a digitális szolgáltatások egységes piacáról és a 2000/31/EK irányelv módosításáról (digitális szolgáltatásokról szóló rendelet)

Az Európai Parlament és a Tanács (EU) 2022/2555 Irányelve (2022. december 14.) az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv), I–II. melléklet

Európai Parlament és Tanács 2013/40/EU irányelv az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról

Európai Parlament és Tanács 460/2004/EK Rendelete az Európai Hálózat– és Információbiztonsági Ügynökség létrehozásáról

Európai Unió Tanácsának 2005/222/IB kerethatározata (2005. február 24.) az információs rendszerek elleni támadásokról

Európai Unió Tanácsának 2008/114/EK Irányelve az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről

Javaslat Az Európai Parlament és a Tanács rendelete a digitális elemeket tartalmazó termékekre vonatkozó horizontális kiberbiztonsági követelményekről és az (EU) 2019/1020 rendelet módosításáról, Brüsszel, 2022.9.15. COM(2022) 454 final

Közös Közlemény az Európai Parlamentnek és a Tanácsnak A hibrid fenyegetésekkel szembeni fellépés közös kerete JOIN/2016/018 final

Közös közlemény az Európai Parlamentnek és a Tanácsnak Az EU kiberbiztonsági stratégiája a digitális évtizedre, Brüsszel, 2020.12.16. JOIN(2020) 18 final

Közös közlemény az Európai Parlamentnek és a Tanácsnak Ellenálló képesség, elrettentés, védelem: az Unió erőteljes kiberbiztonságának kiépítése, Brüsszel, 2017.9.13., Join(2017) 450 final

Közös közlemény az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér /JOIN/2013/01 final/

A Tanács (EU) 2019/796 Rendelete (2019. május 17.) az Uniót vagy annak tagállamait fenyegető kibertámadások elleni korlátozó intézkedésekről; A Tanács (KKBP) 2019/797 Határozat (2019. május 17.) az Uniót vagy annak tagállamait fenyegető kibertámadások elleni korlátozó intézkedésekről

A Tanács következtetései a nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt uniós reagálás kiegészítéseként szolgáló, a közös kiberbiztonsági egységre vonatkozó kezdeményezésben rejlő lehetőségek feltárásáról, Brüsszel, 2021. október 8., 12534/21.

Uniós kibervédelmi szakpolitikai keret (2018. évi naprakésszé tett változata), Brussels, 19. November 2018, 14413/18.

Uniós kibervédelmi szakpolitikai keret, Brussels, 18. November 2014, 15585/14.

Belső jogforrások

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény

Egyes törvényeknek a polgárok biztonságát erősítő módosításáról szóló 2020. évi XXXI. törvény

A honvédelemről és a Magyar Honvédségről szóló 2021. évi CXL. törvény kibertérrel összefüggő rendelkezéseit

A honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető rendkívüli intézkedésekről szóló 2011. évi CXIII. törvény

A honvédelmi miniszter 60/2013. (IX. 30.) HM utasítása a Magyar Honvédség Kibervédelmi Szakmai Koncepciójának kiadásáról

A kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről szóló 2023. évi XXIII. törvény

A Kormány tagjainak feladat- és hatásköréről szóló 182/2022. (V. 24.) Korm. rendelet

A Kormány ügyrendjéről szóló 1352/2022. (VII. 21.) Korm. határozat

A Magyar Honvédségről szóló 2021. évi CXL. törvény

Magyarország Alaptörvénye

National Security Act of 1947
www.dni.gov/index.php/ic-legal-reference-book/national-security-act-of-1947

A nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény

A nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény

A rendőrségről szóló 1994. évi XXXIV. törvény

A védelmi és biztonsági tevékenységek összehangolásáról szóló 2021. évi XCIII. törvény

A Védelmi Igazgatási Hivatalról szóló 337/2022. (IX. 7.) Korm. rendelet.

A sorozatban eddig megjelent kötetek

1. Apró István (szerk.): *Határon túli magyar nyelvű médiumok 2010/2011* (2012)
2. Dobos Ferenc: *Nemzeti identitás, asszimiláció és médiahasználat a határon túli magyarság körében 1999–2011* (2012)
3. Csink Lóránt – Mayer Annamária: *Variációk a szabályozásra. Önszabályozás, társszabályozás és szabályozó hatóság a médiajogban* (2012)
4. Sarkady Ildikó – Grad-Gyenge Anikó: *A média-értéklánc szerzői jogi vonatkozásai* (2012)
5. Koltay András (szerk.): *A médiaszabályozás két éve (2011–2012)* (2013)
6. Paál Vince (szerk.): *Magyar sajtószabadság és -szabályozás 1914–1989* (2013)
7. Horváth Attila: *A magyar sajtó története a szovjet típusú diktatúra idején* (2013)
8. Koltay András – Nyakas Levente (szerk.): *Összehasonlító médiajogi tanulmányok. A „közös európai minimum" azonosítása felé* (2014)
9. Dobos Ferenc – Megyeri Klára: *Nemzeti identitás, asszimiláció és médiahasználat a határon túli magyarság körében 2.* (2014)
10. Grad-Gyenge Anikó – Sarkady Ildikó: *Közös jogkezelés az audiovizuális médiában* (2014)
11. Apró István (szerk.): *Média és identitás* (2014)
12. Pruzsinszky Sándor: *Halhatatlan cenzúra* (2014)
13. Kóczián Sándor: *Gyermekvédelem a médiajogban* (2014)
14. Apró István – Paál Vince (szerk.): *A határon túli magyar sajtó Trianontól a XX. század végéig* (2014)
15. Kiss Zoltán – Szivi Gabriella: *A közszolgálati médiaszolgáltatás és a szellemi tulajdonjogok kapcsolódási pontjai és szabályozási környezete* (2015)
16. Dobos Ferenc: *A médiahasználat változása az erdélyi, felvidéki, kárpátaljai és vajdasági magyarság körében 2001–2014* (2015)
17. Grad-Gyenge Anikó: *Az audiovizuális archívumok szabályozási kerete – különös tekintettel a médiajogi és szerzői jogi rendelkezésekre* (2015)
18. Dobos Ferenc: *A médiahasználat változása az erdélyi, felvidéki, kárpátaljai és vajdasági magyarság körében 2001–2014/2* (2015)
19. Apró István (szerk.): *Média és identitás 2.* (2016)
20. Mezei Péter : *Jogkimerülés a szerzői jogban* (2016)
21. Koltay András – Andrej Školkay (szerk.): *Comparative Research on the Approaches of Administrative Judiciaries to Sanctions Issued by Media Regulators in V–4 I.* (2016)
22. Koltay András – Andrej Školkay (szerk.): *Comparative Research on the Approaches of Administrative Judiciaries to Sanctions Issued by Media Regulators in V–4 II.* (2016)
23. Makkai Béla: *Határon túli magyar sajtó – Trianon előtt* (2016)
24. Grad-Gyenge Anikó: *Film és szerzői jog – A megfilmesítési szerződés* (2016)
25. Kőhidi Ákos: *Fájlcsere és felelősség* (2016)
26. Hajdú Dóra: *A törvény által előírt közös jogkezelés a magyar és a francia szerzői jogban* (2016)
27. Tóth J. Zoltán: *A büntetőjogi rágalmazás és becsületsértés* (2017)
28. Kelemen Roland: *Az első világháború sajtójogi forrásai – Sajtójog a kivételes hatalom árnyékában* (2017)
29. Apró István (szerk.): *Határon túli magyar médiumok 2016* (2017)
30. Klein Tamás (szerk.): *Tanulmányok a technológia- és cyberjog néhány aktuális kérdéséről* (2018)

31. Kiss Zoltán Károly: *A kulturális tevékenységekre, valamint a médiaszolgáltatásra vonatkozó köztehervise lési és jogdíjfizetési szabályok* (2018)
32. Merkovity Norbert: *A figyelemalapú politika a közösségi média korában* (2018)
33. Csapody Miklós: *Az „irányított nyilvánosság" és a „szerkezet megváltoztatása" Magyarországon* (2018)
34. Apró István (szerk.): *Média és identitás 3.* (2019)
35. Mák Ferenc: *Sajtó a Birodalom határán. Hírlapok és a nemzeti újjászületés a kiegyezés utáni Délvidéken* (2019)
36. Paál Vince: *Tanulmányok a magyar sajtószabadság történetéhez 1867–1944* (2019)
37. Kiss Zoltán Károly – Kiss Dóra Bernadett: *A vizuális művészetek és a jog – 1. A képzőművészet szabályozása* (2019)
38. Gálik Mihály – Csordás Tamás (szerk.): *A média gazdaságtanának kézikönyve* (2020)
39. Klestenitz Tibor: *Fejezetek az egyházi sajtó történetéből* (2020)
40. Klestenitz Tibor – Paál Vince (szerk.): *Médiatörténeti tanulmányok 2020* (2020)
41. Apró István (szerk.): *Média és identitás 4.* (2021)
42. Kiss Zoltán Károly: *A vizuális művészetek és a jog 2. Az építészet, a fotóművészet és az alkalmazott művészetek jogi szabályozása* (2021)
43. Apró István (szerk.): *Magyar médiaműhelyek a Kárpát-medencében* (2021)
44. Grad-Gyenge Anikó: *Egy modern szerzői jog* (2022) (Online kiadvány!)
45. Szadai Károly (szerk.): *VV10 – Egy valóságshow valósága* (2022)
46. Dobos Ferenc: *Isaurától az 5G-ig. (A médiahasználat változása 2001 és 2021 között a határon túli magyarság körében)* (2022)
47. Gyulay Dániel: *Becsület csorbításának vizsgálata a tényállásszerű és jogellenességet nélkülöző cselekmények körében* (2023)
48. Paál Vince (szerk.): *Médiatörténeti mozaikok 2022* (2023)
49. Kiss Zoltán Károly: *A vizuális és az audiovizuális alkotók díjazása* (2023)

Médiatudományi Intézet, Budapest
A kiadásért felel Nyakas Levente
Tördelő: Varga Ákos
Megjelent 11,75 (B/5) ív terjedelemben, 300 példányban
Médiatudományi Könyvtár: ISSN 2063-5222
Médiatudományi Könyvtár 50.: ISBN 978-615-5302-46-6