TANULMÁNY

FARKAS ÁDÁM

A kibertér műveleti képességek kialakításának és fejlesztésének egyes szabályozási és államszervezési alapvonalai *

I. BEVEZETÉS

A 21. század dinamikus változásainak egyik leginkább érezhető és mindent átható dimenzióját a kibertér és az infokommunikáció fejlődése, életvitelre, társadalmi-, politikai-, gazdasági- működésre gyakorolt hatásai jelölik. Ez a változás pozitív és negatív értelemben is érvényesül. A valós idejű kommunikáció és ezzel a kommunikációra épülő tevékenységek hatásfokának növekedése, vagy épp a személyiség kibontakoztatásának újabb lehetőségei mellett ugyanis a kibertér bűnözésre, befolyásolásra, kémkedésre, illetve hadviselésre is használható.

Igaz ugyan, hogy még nem rendelkezünk egy vitán felül álló kibertér fogalommal,[1] az azonban biztosnak tűnik, hogy egy olyan virtuális, infokommunikációs alapokon álló térként értelmezhetjük azt, amely közvetlen visszahatási képességgel és kapcsolódásokkal rendelkezik a valós, fizikai életünkre.

Ez a fizikai realitással való kapcsolat és visszahatási potenciál jelentős mértékben képes fokozni a kibertérben rejlő fenyegetések jelentőségét, hatóképességét. Ez pedig értelemszerűvé teszi a kibertérből érkező fenyegetésekkel szembeni védelem szükségességét, vagyis az államok számára olyan képességek kialakítását, amelyek a kibertérben képesek az állam védelmi rendszerének ágazati tagozódása szerint katonai, nemzetbiztonsági, illetve rendészeti műveleteket megvalósítani. Ezeket nevezhetjük összefoglalóan kibertér műveleti képességeknek, kialakításuk megkerülhetetlenségét tükrözik azok a tendenciák, amelyek mind a kiberbűnözés elleni fellépés, mind a kibertérben végzett hírszerzés-elhárítás, mind pedig a kibertérrel összefüggő katonai képességek terén intézményesítési törekvéseket mutatnak a világban.

A transzatlanti térségben fontos alapvetés, hogy ami elválasztja a bűnös magatartásokat a jogszerű, vagy engedélyezett cselekményektől, az a jogállamiság követelményéből adódóan a jogi szabályozás általi

* A tanulmány a szerzőnek a Smart Law Research Group (www.smartlawresearch.hu) keretei között végzett kutatása eredményeként készült.

[1] A téma kapcsán lásd például: Schmitt, 2017; Schmitt, 2013;, Munk, 2018, 113–131.; Szkála – Munk, 2018, 344–355.; Kelemen – Németh, 2018, 147–170.

minősítés, illetve az adott cselekmény megvalósítására való felhatalmazás. Ez az alapelv értelemszerűen a kibertérben végzett védelmi, biztonsági tevékenységekre is igaz, így jogállami keretek között legalább annyira fontos egy ilyen újszerű, dinamikusan fejlődő terület megfelelő jogi szabályozása és államszervezetben való cizellált leképzése, mint a konkrét képességek fejlesztése, hiszen az utóbbiak a jog megfelelő keretei nélkül nem, vagy esetleg bűnösen lesznek alkalmazhatók.

A jogi szabályozottság követelményére tekintettel megkerülhetetlen, hogy a kibertérben végzett tevékenységek jogi keretei újszerűek, illetve megújítottak legyenek. Ehhez a szakmai és jogi követelmények szinkronizálása, a szakemberek együttműködése és együtt gondolkodása nélkülözhetetlen. Önmagában a kibertérhez kapcsolódó — műszaki — tudományok és szakmák nem tudják jogállami keretek között megoldani a kibertér áldásai mellett megjelenő fenyegetések kezelését, míg a szakmai támogatás nélkül a jogalkotó sem tudja kezelni az előtte álló kihívást. Fontos azonban e téren látni, hogy amiképp a kibertér nem egy szeparált, kizárólag virtuális, azaz a valós élettől és annak területeitől külön létező valóság, hanem egy olyan újszerű síkja a létezésnek, ami lényegében minden tevékenységre képes jelentős mértékben ráhatni, úgy a szabályozás sem lehet kizárólag elkülönülő jellegű, vagyis a kibertér viszonyait önállóan rendező. A kibertérben végzett tevékenységek szabályozásának a sajátos törvényi keretek mellett meg kell jelennie a védelem klasszikus szabályrendszereiben és jogszabályaiban is, sőt idővel minden olyan kapcsolódó terület és viszonyrendszer szabályozásában és fogalomrendszerében, amelyre a digitalizáció érdemi hatást gyakorol és ez által tartalmában módosít.[2]

Az önálló és emellett főként a védelem már meglévő jogi kereteibe beépülő szabályozás meglátásom szerint csak úgy valósítható meg, ha a kibertérben végzett tevékenységeket nagyrészt sikerül koherens módon elhelyezni a nemzetközi és a nemzeti jog szöveteiben. Ez egyrészről nemzetközi összehasonlító elemzést, másrészről komplex stratégiai szemléletet, harmadrészről pedig a nemzeti szabályozásunk széles látókörű megújítására való nyitottságot feltételez. Ezek, és különösen az ezekhez szükséges szakemberek, tudományos kutatók és komplex tudományos kutatások a megfelelő jogi keretek kialakításának zálogai, amelyek szükségesek a nemzeti katonai kibertér műveleti képesség kialakítására irányuló stratégiai döntések szempontjából is.[3] Jelen tanulmány a fegyveres védelemmel összefüggő komplex kutatások élénkülésére[4] is tekintettel e kérdések egyes aspektusaira tér ki.

[2] Ennek egyik példáját adhatják az emberi jogokkal kapcsolatos háttértanulmányok, illetve Kelemen Roland gondolatai az alapvető jogok és a derogáció vonatkozásában. Vö.: AHRC 2013; Kelemen 2018, 52–58.
[3] Dr. Böröndi Gábor altábornagy, a Magyar Honvédség parancsnokának helyettese 2019. március 19-én a parancsnoki országjárás fővárosi állomásán beszélt erről. A bejelentést közlő hír szerint altábornagy úr rögzítette, hogy a „kiberképességet is fejlesztik, s már nemcsak a védekezésre, de a támadásra is hangsúlyt fektetnek, egy kiberakadémiát is létrehoznak Szentendrén". Nyulas Szabolcs: Az ütőképes hadsereg létrehozása nem szlogen. *honvedelem.hu*, 2019. március 20. https://honvedelem.hu/cikk/115130_az_utokepes_hadsereg_letrehozasa_nem_szlogen (2019.03.25.)
[4] E tekintetben példaként lásd: Spitzer, 2019; Farkas, 2018a; Farkas, 2018b.

II. A SZAKMAI KÖVETELMÉNYEK, A NEMZETKÖZI JOG ÉS A NEMZETÁLLAMI SZABÁLYOZÁS HÁROMSZÖGÉBEN

A kibertér műveleti képességek fejlesztése és szabályozása tekintetében fontos rögzíteni, hogy több szempontból is adódik a komplex és multidiszciplináris megközelítés megkerülhetetlensége és vele az egyes — szakmai, vagy épp ágazati — szereplők kizárólagosságának értelmezhetetlensége. A *szakmai dimenzió* tekintetében fontos ugyanis kiemelni, hogy nem csak a szűken értelmezett kibervédelmi és -biztonsági funkciókat ellátó szakterületekre, hanem a tágabb IT szakterületre, sőt még az ehhez kapcsolódó szakterületekre — szervezés, jog, műszaki támogatás, stb. — is fokozott figyelmet kell fordítani, idekapcsolva az innováció kérdéseit és nemzeti szintű szervezését is. Nyilván az egyes szakmai rétegeknek, vagy szegmenseknek nem lehet azonos a súlyozása akkor, amikor kifejezetten a kibertér műveleti képességek kialakításáról van szó, másik oldalról viszont a biztonsági és védelmi karakter hangsúlyozása nem eredményezheti a kapcsolódó szakmai kritériumok súlytalanodását sem. Ez mind a szakmai-kidolgozói, mind pedig a kormányzati, irányítói, illetve szabályozói szintű teendők szempontjából fontos alapvetés, ami a fejlesztendő képességekkel érintett tér, azaz a kibertér sajátosságaiból következik.

Egyrészről a kibertér azon jellemzője, hogy az a valóságnak egy fizikai kötődésekkel rendelkező és a fizikai valóságra visszahatni képes, de nagyrészt virtuális része, egyértelművé teszi, hogy a hatásait a védelem terén a 20. századig megszokott külső/belső védelmi funkciófelosztástól függetlenül, átfogó jelleggel fejti ki. Ez meglátásom szerint a legtöbb új típusú kihívás, illetve a hadviselés változásai folytán általánosan jellemző a védelem terén,[5] de a különbséget megértetendő úgy is fogalmazhatnék, hogy a kibertérből érkező fenyegetések tekintetében a külső/belső védelmi felosztás éles elhatárolásának értelmezhetetlensége épp úgy esszenciális jellemző, mint a hálózatos jelleg. Ebből adódóan tehát egyik oldalról az érintett ágazatoknak, illetve katonai karakterű szervezeteknek[6] képesnek

[5] Az átfogó jelleg és ezzel szemben a reziliencia fejlesztése a NATO-ban is alapvetés ma már. Ezt a hatást a nemzetközi terrorizmus, a hibrid konfliktusok és ezekhez kapcsolódva, vagy épp önállóan a kibertérből érkező fenyegetések, támadások váltották ki. Azt is mondhatnánk, hogy a 21. század meghatározónak és újszerűnek tartott biztonsági fenyegetései komplexek, differenciáltak, a védelem szempontjából ágazatokon átívelők, azaz totálisak. A totális biztonsági kihívások, a hibrid konfliktusok alapjellemzője, illetve a nemzetközi terrorizmus kapcsán lásd: Treverton et al., 2018; Ferm, 2017; Chivvis, 2017; Weiss, 2015; Hermann, 2015; Napoleoni, 2015; Farkas, 2018c.

[6] Kutatásim során egyik fő munkafogalmam a katonai karakterű szervek fogalma. Katonai karakterű szervek alatt a legitim, szabályozott, monopolizált és szervezett állami erőszak érvényesítésére törvényileg feljogosított, — főszabály szerint — katonai rendfokozati hierarchiában, parancsuralmi vezetési rendszerben és a szervezet egészét általánosságban jellemző fegyveres jellegben működő testületeket értem. Ez a kategorizálás ebben a formában nem tesz különbséget sem aszerint, hogy az adott szervezet fő funkciója belső, vagy külső védelmi, sem aszerint, hogy mely védelmi ágazathoz tartozik a szervezet, sem pedig aszerint, hogy a szervezet beleérthető-e valamelyik már használt, bevett — de nem ritkán vitákkal terhelt — fogalmi körbe, mint amilyen a fegyveres erő, a rendészeti szervek, rendvédelmi szervek vagy a nemzetbiztonsági szolgálatok. Fontos azonban kiemelni, hogy ez egy rendszerező, tehát tudományos, elméleti fogalom és nem egy alternatíva a katonai, nemzetbiztonsági, illetve rendészeti szervek legális fuzionálására.

kell lennie a saját maguk tekintetében szükséges, speciális kibertér műveleti és védelmi feladatok ellátására, emellett viszont a fokozott együttműködésre is.

Másrészről maga a kibertér is egy hatalmas és rendkívül összetett hálózat. Az onnan érkező fenyegetések is hálózatos jellegűek, aminek az is egy fontos következménye, hogy a kibertérben való közvetítésen túl ezek mind módszerük, mind célpontjaik, mind hatásterületük és hatásaik tekintetében differenciálódhatnak. Ennek megfelelően a kibertérből érkező fenyegetésekkel szembeni fellépésnek is differenciáltnak és hálózatosnak kell lennie, azaz a kibertér műveleti képességeknek — az interoperabilitásra való alkalmassággal — meg kell jelennie a klasszikus rendészeti, katonai, nemzetbiztonsági feladatokat ellátó szervezeteken belül, illetve akár az egyes ágazatok vonatkozásában új, önálló szervezeti keretekben is. Ez a fajta, a fegyveres védelem rendszerének egészét érintő megjelenés, vagy leképeződés azonban szintén a multidiszciplináris szemlélet felé mutat, hiszen az egyes védelmi ágazatoknak és szervezeteknek eltérő igényei, céljai, eszközei, eljárásai és szervezeti keretei lesznek. Ennek a fajta fejlesztésnek tehát az ágazatok vonatkozásában hasonló ívet kell bejárnia, mint a nemzetbiztonsági szolgálatok fejlődése volt a 20. században, ami az önállóvá válás mellett a meglévő védelmi funkciókat támogató jelleggel, azokhoz igazodó — polgári-katonai — differenciálódással épült ki a világ számos pontján. A kibertér műveleti képességek fejlesztésének a szakmai erőterét tehát egy nagy fokú multidiszciplinaritás és differenciáltság is jellemzi.

A differenciált és hálózatos szakmai igények és megoldások mellett, illetve ahhoz szorosan kapcsolódó módon a nemzetállami és a nemzetközi jogi vonatkozásokban is komoly erőterek fedezhetők fel, amelyekhez a kibertér műveleti képességek fejlesztésének alkalmazkodnia kell. Ez a tagolás azonban nem értelmezhető a szakmai/ágazati differenciáltságtól függetlenül, hiszen magától értetődő, hogy mind a nemzeti, mind a nemzetközi jog terén rendkívül eltérő szabályozási anyag vonatkozik például a rendészeti, a katonai, illetve a nemzetbiztonsági funkciók ellátására. Ez a jogi értelemben vett differenciáltság azonban a kibertér műveleti képességek kiaknázása, illetve az azokkal kapcsolatos garanciák terén komoly jelentőséget nyer.

A *nemzetközi jogi vonatkozások* terén ugyanis látható az a tendencia, hogy a *katonai funkciók* tekintetében egy meglehetősen erőteljes és kiforrott szabályozás, mind a korlátozások, mind a lehetőségek, mind a cselekmények értékelése tekintetében. Ennek megfelelően a katonai kibertér műveleti erők a nemzetközi jog vonatkozásában osztják a katonai erők sorsát és szabályozását. Ezt a témát mindenképp fontos Magyarországon is részletekbe menően elemezni, azt azonban a jelen áttekintés szintjén sem lehet elmulasztani, hogy a NATO-ban is terjed az az értelmezés, miszerint a kibertér műveleti erőkkel végrehajtott beavatkozások is elérhetik azt a szintet, amit a nemzetközi jogi értelemben vett fegyveres

támadásként lehet felfogni.[7] Nem véletlen, hogy a NATO hadszíntérré nyilvánította a kiberteret és a nemzetközi jog vonatkozó szabályait alapvetően alkalmazhatónak tekinti az ott folyó műveletekre is.[8] Ennek megfelelően egy ilyen kibertér műveleti csapásra az önvédelem keretében — az arányosság fokmérőihez igazodva — akár kinetikus választ is lehet adni. A katonai kibertérműveleti erők szabályozása, alkalmazása, illetve ezekhez igazodó felépítése terén tehát a nemzetközi jogi szabályozásra és korlátozásra a politikai, diplomáciai, gazdasági, illetve adott esetben egy fegyveres konfliktusból eredő hatások miatt fokozott figyelmet kell fordítani. Ez a még formálódó, mégis több tekintetben kiforrott, illetve jól beazonosítható nemzetközi jogi keretrendszer értelemszerűen determinálja a nemzeti szintű szabályozást is a katonai kibertér műveleti erők vonatkozásában. Lényegi elem tehát, hogy az országon kifelé ható, egy állam által megvalósított, vagy az államnak betudható, ártó/károkozó cselekmények a nemzetközi térben fegyveres támadásként is értelmezhetők, ha olyan hatásúak, hogy teljesítik az egyes államok által az erőalkalmazás szintjének ehhez társított kritériumait.

Hasonlóan korlátos azonban *a rendészetre* vonatkozó nemzetközi szabályrendszer is, hiszen azt a nemzetközi jog a szuverenitás klasszikus belső megnyilvánulásaként fogja fel. A határokon átívelő fenyegetésekkel kapcsolatos bűnügyi egyezmények közül persze kiemelhető itt a Budapesti Konvenció,[9] fontos azonban azt rögzíteni, hogy sem a Konvenció, sem más bűnügyi egyezmények alapvetően nem írják felül azt a tényt, hogy a rendészet alapvetően a szuverenitás belső funkcióihoz tartozik. A rendészeti kibertér műveleti erők mozgástere tehát — főszabály szerint — a nemzetállamon belül, a nemzeti eljárások vonatkozásában értelmezhető. Azon túl csak kifejezett, szabályozott és határozottan erre is kiterjedő nemzetközi bűnügyi, rendészeti együttműködés keretében valósulhat meg[10] a rendészeti fellépés, vagyis a szuverenitás belső szegmensének a külsőbe való átmozdulása. E tekintetben azt is ki kell emelni, hogy bár a fegyveres erő alkalmazása és fegyveres támadás kapcsán joggal asszociálunk klasszikusan katonai cselekményekre, azonban a kibertérben megvalósuló ilyen cselekmények kapcsán elsődlegesen az adott államnak való betudhatóság dominál (attribúció). Ennek megfelelően a határon kívülre irányuló, egy állam rendészeti kibertér műveleti képességével végrehajtott támadó jellegű műveletek fegyveres erőalkalmazásnak, illetve súlyosabb esetben akár fegyveres támadásnak is minősíthetők a sértett állam részéről, függetlenül attól, hogy azt pro forma nem katonai, hanem rendészeti szervezet hajtotta végre, hiszen a kifelé irányuló cselekményeknél az

[7] A kinetikus hatások és válaszok kérdései kapcsán lásd például: Applegate, 2013, 163–177.; Geers, 2015; Wallace, 2018.; Kelemen – Pataki, 2015, 53–90.; Lattmann, 2018, 39–51.; Klimburg, 2012.

[8] E tekintetben lásd: Csiki – Tálas – Varga, 2014, 112–128., NATO: Wales Summit Declaration (letöltve: 2019.04.23., https://www.nato.int/cps/ic/natohq/official_texts_112964.htm), Tálas,2016, 97–101., NATO: Warsaw Summit Communiqué, https://www.nato.int/cps/en/natohq/official_texts_133169.htm (2019.04.23.)

[9] Budapest Convention on Cybercrime (ETS No. 185), Budapest, 23/11/2001.

[10] A téma alapvonalai kapcsán lásd: Blaskó – Budaházi, 2019; Finszter, 2018, 460–472.

államnak való betudhatóság és a cselekmény hatásai határozzák meg a minősítést, nem a nemzetállamon belüli szervezeti osztályozás. Erre figyelemmel alakul ki az a jellemző megoldás a transzatlanti térségben, hogy a kifejezetten támadó képességek a nemzetközi és nemzeti jog korábbi korlátozó szabályrendszereihez jól igazodó fegyveres erőkhöz kerülnek telepítésre, míg a rendészeti szerveknél alapvetően a bűnfelderítést támogató, a rendészeti rendszerek védelmét szolgáló, illetve az esetleges nemzetközi bűnügyi együttműködésben is alkalmazható képességek kialakítása valósul meg.

A nemzetközi jogi szabályozás terén *a nemzetbiztonsági, pontosabban a hírszerző és elhárító funkciók* vonatkozásában találkozunk a legalacsonyabb szintű, tehát egyik oldalról bizonytalanságot okozó, másik oldalról a rugalmasságot lehetővé tevő szabályozással. A kibertérben végzett hírszerzés és elhárítás is osztja a klasszikus hírszerző — kémkedő —, illetve elhárító tevékenységek sorsát a nemzetközi jog tekintetében. E körben — szemben a katonai fellépésre, vagy épp a más ország szuverenitását sértő túlterjeszkedő rendészeti fellépésre vonatkozó szabályokkal — kiforrott és részletes nemzetközi jogi szabályrendszerről nem beszélhetünk. A fő rendező elv az, hogy a kémkedéssel szemben a nemzetállam jogosult jogi eszközökkel fellépni, míg kimunkált nemzetközi jogi rendszer e mögött érdemben nem áll. Ez persze nem zárja ki, hogy egy nagyhatású, kibertérben végrehajtott nemzetbiztonsági művelet ne lehetne utóbb fegyveres erőalkalmazásként vagy extrém esetben fegyveres támadásként értékelhető a sértett állam által, de az e szint alatti cselekményeknél általában a hangsúly a nemzetállam védekezésén, illetve a nem jogi következményeken van. Egy kiber-hírszerző[11] (adott esetben hibrid hadviselésbe illeszkedő, de még nem nagy intenzitású befolyásoló) művelet a dekonspiráció esetén is csak további feltételekkel valósíthat meg fegyveres erőalkalmazást. Ez azonban egyértelműen nem eredményezi az ellenérdekelt fél önvédelmi helyzetbe kerülését. E tekintetben külön kérdéses és vizsgálandó, hogy a betudhatóság megáll-e az adott— sokszor áttétekkel, nem állami szereplők felhasználásával megvalósuló — cselekmények vonatkozásában. Erre nézve vannak ugyan az egyes államoknak rugalmasabb értelmezési lehetőségei, de azt a nemzetközi bírói gyakorlat keretek közé tereli és egyik fő elemeként a tényleges és bizonyítható irányítást határozza meg. A betudhatóság kérdésessége, és a hírszerző cselekmény fegyveres erőalkalmazási szintet el nem érő volta persze sem a hírszerzési, sem a diplomáciai, sem a gazdasági válaszokat nem zárja ki, a katonai értelemben való jogszerű fellépést azonban mindenképp, illetve a gazdasági és diplomáciai szankcionálás terén is korlátozza a lehetőségeket. Ennek köszönhető az, hogy számos NATO tagállam a kibertér műveleti képességeit mind a polgári, mind pedig a katonai oldalon beágyazza a nemzetbiztonsági szolgálatok feladatrendszerébe, hiszen azokra nézve elsősorban a nemzeti jogszabályi környezet irányadó, míg a nemzetközi jogi terén egy rugalmasabb, bizonytalanabb keretrendszer ragadható csak meg.

[11] A téma kapcsán példaként lásd: Ziolkowski, 2013, 425–464.

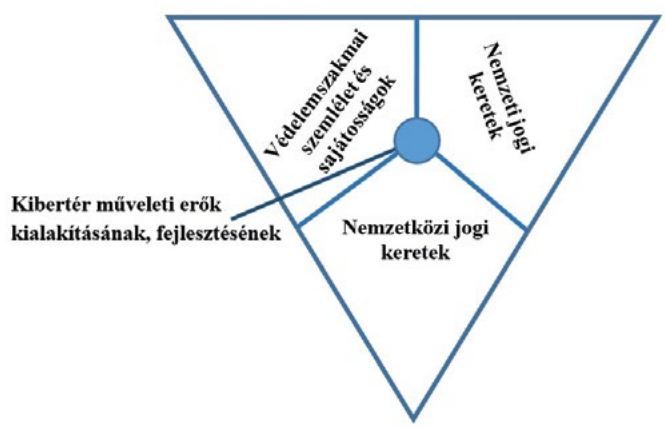
A nemzetközi jogi keretekre figyelemmel *a nemzetállami jogi szabályozás*ra, mint a kibertér műveleti erők fejlesztését és alkalmazását determináló erőtérre kell kitekintenünk, úgy hogy arra egyszerre hatnak a szakmai erőtér és a nemzetközi jogi erőtér vonatkozásai is. Egyrészről ugyanis nyilvánvaló, hogy az adott állam fegyveres védelmi rendszerén belül az ágazati tagozódás, a szervezeti mátrix és az ehhez kapcsolódó hatáskör- és képességmegosztás, valamint az ezeket irányító kormányzati felelősségi és döntéshozatali szisztéma is a nemzeti jog által meghatározott. Ez a nemzetállami jogi szabályozás szükségképpen tükrözi az adott állam kulturális, történeti, geopolitikai és geostratégiai helyzetét és sajátosságait, ami mellett fontos azt is hangsúlyozni, hogy a nemzeti jogrendszer határozza meg az adott állam védelmi képességeinek és eljárásainak alapvető és elsődleges szabályait, méghozzá az adott állam politikai döntéshozóinak a preferenciái szerint. A nemzetállami szabályozás tehát az adott állam szakmai és nemzeti tradícióihoz és történeti tapasztalataihoz nagyban igazodó módon rendezi a védelmi funkciók, vagyis ennek részeként a kibertér műveleti erők szabályozását is, de oly módon, hogy a nemzeti keretrendszerbe a politikai mérlegelés függvényében kerülnek be a szakmai és a nemzetközi jogi elemek. Ezen sajátosságok jelentőségét tükrözi, hogy Georg Nolte — a német védelmi minisztérium megbízásából — már a kétezres évek legelején összehasonlító elemzés tárgyává tette az európai katonai jogi rendszereket,[12] és ennek részeként osztályozta az európai államok szabályozását. Ez az elemzés markáns eltéréseket mutatott ki az egyes államok szemléletében és szabályozásában, ami mind a NATO, mind az EU védelmi harmonizáció, vagy integráció tekintetében kulcsjelentőségű. E vonatkozásban azt is hangsúlyozni kell, hogy míg a védelmi szabályozást a szakmai dimenzió jelentős mértékben meghatározza, addig másik oldalról a jogi szabályozásra a tágabb értelemben vett nemzeti jogrendszer is jelentős — és sok esetben a védelem-szakmai törekvéseket megszűrő, módosító — hatást gyakorol. Fontos mindezek mellett azt is rögzíteni, hogy a nemzetállami szabályozási szintre a nemzetközi jogi dimenzió is hatással van, igaz államonként eltérő mértékben. Az új típusú biztonsági kihívások és általában a 21. század fenyegetései terén ugyanis az egyes államok nemzetközi jogi rendelkezésekhez, illetve azok értelmezéséhez való viszonyában jelentős kilengések is tapasztalhatók. Ezt épp úgy befolyásolják az adott állam nemzetközi hatalmi attribútumai, mint a szövetségi, vagy integrációs hovatartozása, illetve ezeken belül a nemzetközi politikai törekvései. Ennek megfelelően a nemzetközi

[12] E tekintetben kiemelendő, hogy a vizsgált európai államokat a kis tradicionális demokráciák, a nagy tradicionális demokráciák és a posztautokrata demokráciák közé sorolta be, ezzel is hangsúlyozva a nemzeti, ezen belül a történelmi, kulturális és geopolitikai sajátosságok fontosságát, azaz a komplexitás egy sajátos leképződését. Lásd: Nolte, 2003. A nemzeti sajátosságok fontossága persze a magyar jogi és államtudományi gondolkodásban is ismert. A mintakövetés kapcsán Concha Győző több mint száz esztendeje úgy fogalmazott: „Ha az egyik nemzet nem érezhet egészen úgy, mint a másik, egyénisége feláldozása nélkül, saját életszükségleteinek kell a kutatásra is ösztönözni, saját eszével kell gondolkodnia is; nem veheti át készen más nemzetek gondolkodása legmagasabb virágának, tudományának eredményeit, nem lehet merőben kölcsönző." (Concha, 1907, IX.)

jog és a nemzetállami szint relációjában azonosítható egyfajta harmonizációs igény a legtöbb nemzet által elfogadott szabályrendszerek tekintetében, másik oldalról azonban számos új jelenség megítélése tekintetében fragmentáltság is érződik, ami egy adott kérdés kapcsán pro és kontra jelleggel is orientálhat egy nemzetállamot. Meglátásom szerint a kibertérben végzett különféle műveletek jogi megítélésére — kötelező érvényű nemzetközi szerződés és kiforrott gyakorlat hiányában — az utóbbi jellemző. Ez azonban nem jelenti azt, hogy ne lennének a nemzetközi jognak a nemzetállami szintű szabályozást meghatározó vonatkozásai, inkább csak azt tükrözi, hogy a nemzeti szintű szabályozásban van lehetőség a részletes kimunkálásra, amihez viszonylag rugalmas nemzetközi jogi keretek ragadhatók meg.

Mindezek alapján úgy vélem, az egyes nemzetek vonatkozásában a kibertér műveleti képességek kialakítását, fejlesztését a kimunkált, az államszervezet vonatkozásában is reális, átfogó és mégis hálózatos megközelítésre épülő szakmai koncepcióknak oly módon kell meghatároznia, hogy ezek a szakmai igények idomuljanak elsődlegesen a nemzeti jogszabályi környezet kereteihez és lehetőségeihez, miközben másodlagosan a nemzetközi mintákra, megoldásokra és a formálódó nemzetközi jogi értelmezésre is kellő figyelmet fordítanak. Ezekre tekintettel az optimális megközelítés e fejlesztés tekintetében az alábbi ábrával szemléltethető, amelyben a halmazok mérete jelzi az adott dimenzió jelentőségét, vagy súlyát, de ettől függetlenül a súlyozás nem írja felül a kölcsönhatásos jelleget.

1. ábra: A kibertér műveleti erők kialakításának és fejlesztésének szabályozási szemléletét formáló dimenziók



III. A JÓ KORMÁNYZÁS ÉS A GYORSÍTOTT DÖNTÉSHOZATAL IGÉNYEINEK KAPCSOLATA A KIBERTÉR MŰVELETI KÉPESSÉGEK FEJLESZTÉSÉVEL

A 19. századtól érezhető, dinamikus technológiai, közlekedési, kommunikációs, illetve gazdasági fejlődés, valamint ezeknek a társadalomra gyakorolt hatása magával hozta az állami funkciók gyarapodását és differenciálódását, valamint a jogi szabályozás szükségszerű fejlődését és bővülését is. Ez a fejlődés egyértelműen oda vezetett, hogy egyrészről a 20. század végén és a 21. század elején okszerű igényként merült fel az állam hatékonyabbá tétele, azaz az állami folyamatok és struktúrák szisztematikus reformja és a jó kormányzás irányába való előrelépés. Másrészről azonban a valós idejű és globális kommunikáció, a valóban globális és digitalizált kapitalizmus, illetve a közlekedés fejlődése folytán a világ rendkívüli mértékben felgyorsult a korábbiakhoz képest, amihez az állami döntéshozatalnak is fel kell zárkóznia. Ez a gyorsabb döntési igény azonban a nagy fajsúlyú, vagy potenciálisan azonnali és jelentős következményekkel járó ügykörökben, mint amilyen a védelem is, fokozott kihívásként jelentkezik. Ahhoz tehát, hogy a kibertér műveleti képességek kialakításának, illetve fejlesztésének szabályozási és állami vonatkozásainak alapkérdéseiről kellő körültekintéssel gondolkodhassuk, szükséges az is, hogy a kérdést a nemzetállami szabályozás fent írt jelentőségére figyelemmel a jó kormányzás és a hatékony és gyors állami döntéshozatal megvilágításában is értelmezzük.

A *jó kormányzás* és vele a kormányzati teljesítmény mérhetősége és ez által javíthatósága az elmúlt évtizedekben elfogadott és fejlesztendő kérdésévé vált a nyugat-európai államszervezésnek és a hazai államtudományi gondolkodásnak is.[13] Akár az Államreform Bizottság 2014 és 2018 közötti működése, akár a Jó Állam Program és az ehhez kapcsolódó kutató kapacitások kialakítása a Nemzeti Közszolgálati Egyetemen, a hazai adaptáció fontos állomása. Ezek, és a kormányzás, illetve az állam tudományos elemzése terén elért holisztikus, általános eredmények mellett azonban fontos, hogy a jó kormányzás égisze alatt megjelenő törekvések és kritériumok a védelem terén is leképeződjenek. E tekintetben persze figyelemmel kell lenni a fogalom „ideologikus" kettősségére is, „annál is inkább, mert Nyugat-Európában is a »jó kormányzás« kétféle felfogásának hívei mérik össze érveiket: az állam kitüntetett szerepéről lemondó neoliberálisok (good governance) az állam megerősítésében gondolkodókkal (good government) találják szembe magukat."[14]Az előbbi az állam szerepének megerősítése helyett az államon kívüli szereplők jelentőségét hangsúlyozza és az államot elsősorban a jó kormányzás feltételeinek megteremtőjeként, de nem feladatainak megvalósítójaként fogja fel.[15]„Az államtalanítás híveivel szemben megfogalmazódó good government-koncepció viszont éppen arra

[13] A téma kapcsán lásd: Kaiser – Kis, 2014, Kaiser – Bozsó, 2016; Kaiser, 2016; Patyi 2016, 1–14.; Stumpf, 2014a; Andrews, 2008; Graham – Amos – Plumptre, 2003.
[14] Stumpf, 2014b, 68.
[15] Vö. Ua. 69–75.

támaszkodik, amiről a rivális gyakorlat lemond. A modell szerint az állam nemcsak a jó kormányzás feltételeinek megteremtésében vállal szerepet, de a jó kormányzás feladatait is magára kell vállalja."[16] Ez utóbbinak a gazdasági válság, illetve a negatív elmozdulásokon átesett biztonsági környezet is erős érveket adott, hiszen a jó, hatékony, fejlődő társadalmi és gazdasági működéshez a megfelelő szabályozó, koordináló, felügyelő képességű aktornak — az államnak — ezeken túlmenően egyértelműen és korszerűen kell szavatolni a rendezett működéshez és fejlődéshez szükséges biztonságot és stabilitást is. Ez a vonatkozás pedig már egyértelműen hozzákapcsolja a védelemhez a jó kormányzás gondolatkörét. A digitalizáció társadalom- és gazdaságformáló, illetve biztonsági jelentősége miatt tehát a kibertér műveleti képességek fejlesztése kapcsán is fontos számolni a jó kormányzás követelmény-rendszerével és gondolati sémáival.

A jó kormányzás témánkra való átültetése, értelmezése érdekében talán a legjobban megragadható irányt a rossz kormányzás néhány jellemzőjének, mint ellensúlyozandó, kieszközölendő vonásoknak az áttekintése adhatja. Stumpf Istvánnak a rossz kormányzás fő indikátorairól írt gondolatai közül mindenképp kiemelhetők a következők: (1) a kormányzás tartalmi, szakmai kérdései háttérbe szorulnak a politikai és személyi vonatkozásokkal szemben, (2) a politika sajátos logikája korlátozza a szakpolitikai koncepciók érvényesülését, (3) az egydimenziós logika fokozza a problémákat, (4) a célok és a vízió hiánya összekapcsolódik az eszközök válságával, (5) a struktúrák radikális átalakítása kaotikus eredményekhez vezet.[17] Ezek azok a főbb vonatkozások, amelyeket mindenképp kerülni kell a jó kormányzás érdekében, különösen az olyan újszerű és átfogó kihívásokat hordozó fejlesztési területek kapcsán, mint amilyen a kibertér műveleti képességek fejlesztése, vagyis a tág értelemben vett információ- és kiberbiztonság.

A rossz kormányzás ezen torzulásainak elkerülésére az egyik lehetséges irány a neoweberiánus államfejlesztés gondolata, ami mind a funkciók, mind a struktúrák, mind a személyek és képességek terén a fejlesztés felé mutat. Ennek persze a fő megvalósulási mintáját a tőlünk jelentősen eltérő kulturális és geopolitikai helyzetű gazdaságfejlesztő államok adják, azonban az ott elvárt magas színvonalú, jól szervezett, koherens apparátus, a meritokratikus kiválasztás, illetve az állami és a magánszféra megfelelő együttműködése[18] — sajátosságok mellett persze, de — értelmezhető és meghonosítható a védelem terén is. A fenti okfejtésünk ugyanis, amely a szakmai, a nemzeti jogi és a nemzetközi jogi keretek összehangolása felé mutat, jól illeszthető ehhez a sémához. A Stumpf István által hangsúlyozott neoweberi jellemzők sora hívható fel itt (1) az állam szerepének újragondolásától és megerősítésétől, (2) a normativitás erősítésén és megújításán, (3) a közszolgálat eszményének helyreállításán és revitalizálásán, illetve (4) a hatékony és szolgáltatói szemléletű feladatellátáson át, egészen (5) a közszol-

[16] Ua. 75.
[17] Vö. Stumpf, 2014a, 98–100.
[18] Vö. Ua. 112–114.

gálat professzionalizációjáig.[19] E tekintetben kiemelendő a jó kormányzás azon előfeltétele, hogy „a közigazgatási döntés-előkészítés és ellenőrzés átfogó rehabilitációja, újjáépítése halaszthatatlan [...] az állam funkciói újragondolásának előfeltétele a közigazgatási szakmai tudásbázis megalkotása...”[20] Ennek átfordítása a kibertér műveleti képességek fejlesztésére azt hozza magával, hogy szükséges egy olyan multidiszciplináris szakmai-tudományos szakapparátus kialakítása, amely a stratégiai fejlesztést és kialakítást a döntés-előkészítés szintjén tudja támogatni, majd a jövőbeni korrekciókat sokrétű szakmai szempontok mentén képeslesz megalapozni. Másrészről a fentiek egy ilyen szakértő-kutató képesség kialakítása mellett szükségessé teszik

- a kibertér műveleti képességek beillesztését az állam változó feladatairól kialakítandó koncepcióba, stratégiába;
- az információ- és kiberbiztonság, valamint az ezzel összefüggő védelmi feladatokat ellátó állami funkciók szabályozásának megújítását, megerősítését, hogy a védelem egyszerre legyen korszerű, de jogállami és garanciális szemléletű;
- olyan közszolgálati életpálya- és működési modell kialakítását, amely a kibertér műveleti képességekkel összefüggő sajátos szaktudású apparátust is hivatásszerűen képes megtartani, motiválni, sőt a professzionalizáció érdekében továbbképezni; valamint
- a hatékony — de szakmai és biztonsági okokból hálózatos — képességkialakítás mellett egy olyan eljárásrend kialakítását, amely a civil társadalom számára is elfogadható, szolgáltató szegmenseiből adódóan támogatható.

A jó kormányzás elvrendszerének terjedését és fontossá válását nagyban erősítették a valós idejű és gyorsan változó biztonsági kihívások is. Ezek mielőbbi kezelése érdekében *a kormányzati, illetve a tágabb értelemben vett közjogi döntéshozatal gyorsítása* egy olyan alapvető igény, amely az adott védelmi, illetve szakmai kérdések tekintetében a funkcióellátás teljes vertikumát érinti a tervezés és felkészítés fázisától az ügyeleti és készenléti szolgálatok, illetve szakállományok működésén keresztül egészen a felső szintű javaslattételig és döntéshozatalig. A kibertér műveleti tevékenységek körében ez a gyorsasági igény egyértelműen azonosítható, sőt megkerülhetetlen. Fontos azonban rögzíteni, hogy a védelem terén — ha nem is tekinthető problémamentesnek a rendszer, de — van már példa a normál döntéshozatali láncolattól eltérő megoldásokra mind a szervezeti keretek, mind pedig a konkrét védelmi funkciók terén. Az előbbit képviseli meglátásom szerint a nemzeti információs államtitkár intézménye,[21] a hírszerzési jellegű információk gyors becsatornázása és a kapcsolódó döntési, irányítási láncolat szakmai koordinációval való hatékonyabbá tétele érdekében.

[19] Vö. Ua. 114–118.
[20] Stumpf, 2014b, 148.
[21] A téma kapcsán lásd: Hódos, 2018, 5–16. Lásd továbbá: a Kormány tagjainak feladat- és hatásköréről szóló 94/2018. (V. 22.) Korm. rendelet 5. §-át.

Az utóbbit — azaz a konkrét védelmi funkcióhoz tapadó sajátos döntési rezsimet — pedig a légierő fegyverhasználatára és különösen az eltérített polgári légi jármű esetleges kiiktatására vonatkozó szabályozás tükrözi,[22] illetve a NATO törekvése a védelmi helyzetekkel összefüggő döntéshozatalának, működésének gyorsítására, rugalmasítására, és az ezt megalapozó tervezésre.

Kiemelendő e körben Magyarország vonatkozásában az is, hogy a 2018-as kormányalakítás folyamatában a korábban döntési jogkörrel nem rendelkező Nemzetbiztonsági Kabinet — mint a kormány védelmi és biztonsági kérdésekre szakosított politikai szerve — bekerült azon kormányszervek sorába, amelyek meghatározott kérdéskörökben a kormány döntési jogkörét gyakorolhatják. Ez a változás előremutató, hiszen a tág értelemben vett védelem stratégiai és kormányzási — koncepcionális, politikai — kérdéseit megfelelő szintre emelte a kabinet többi, döntési jogú tárgykörei mellé. Ugyanakkor fontos kiemelni, hogy a Nemzetbiztonsági Kabinet nem helyettesítheti a kormány védelmi döntéshozatalának teljes spektrumát, illetve a miniszterelnök-központú magyar kormányzati modellben értelemszerűen nem indokolt, hogy gyakorolhassa a kormányzati felelősség szempontjából kiemelt súlyú eseti döntési jogköröket, amelyekbe a konkrét védelmi műveletek feletti döntések is beletartoznak. A kabinet jellegű működés tehát elsősorban a koncepcionális, stratégiai vetületű, kormányzási-politikai döntések terén jelenthet komoly előrelépést, amihez viszont szükséges volna, hogy a nemzetbiztonság rendszerének egészét leképző szakmai támogató — munkacsoport — rendszer épüljön ki a Nemzetbiztonsági Kabinet alatt, hiszen jelenleg egy meglehetősen tagolt és rendszerszinten át nem gondolt szisztéma látható e körben.[23]

A már megvalósult szervezeti megoldások vitán felül álló módon előremutatóak, de rendszerszinten nem hozták magukkal a funkciók ellátásával kapcsolatos döntés-előkészítési és döntési mechanizmusok szisztematikus felülvizsgálatát és ott ahol ez szükséges, újszerű megoldások kialakítását. Ez pedig különösen a védelem tekintetében több szempontból is aggályos, hiszen egyrészről hazánk-

[22] A téma kapcsán lásd a honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről szóló 2011. évi CXIII. törvény 62. §-át. Lásd továbbá: Mógor, 2018, 134–139.; Papp, 2019; Sulyok, 2019, 35–60.

[23] Ezt talán jól példázza, hogy miközben a Nemzetbiztonsági Kabinet munkáját szakmai előkészítőként hivatott támogatni a Nemzetbiztonsági Munkacsoport, aközben szintén a Nemzetbiztonsági Kabinet alá rendelve, de külön szabályozva jelenik meg a Terrorellenes Koordinációs Munkacsoport. Ezektől teljesen elkülönül a Honvédelmi Igazgatási Koordinációs Tárcaközi Munkacsoport, amely a kormány és nem a kabinet szakosított szerve, míg például a kiberbiztonság és kibervédelem, vagy a hibrid fenyegetések elleni fellépés terén nem látjuk kirajzolódni egy a Nemzetbiztonsági Kabinetet támogató munkacsoport kontúrvonalait. A téma kapcsán lásd különösen a 94/2018. (V. 22.) Korm. rendelet 158. §-át, a Kormány ügyrendjéről szóló 1144/2010. (VII. 7.) Korm. határozat 2. pont (4) bekezdését, 58. pontját, 90/D. pontját, a terrorizmus elleni küzdelem feladatainak egységes végrehajtási rendjéről szóló 1824/2015. (XI. 19.) Korm. határozatot, valamint a Honvédelmi Igazgatási Koordinációs Tárcaközi Munkacsoport létrehozásáról, valamint szervezeti és működési rendjének meghatározásáról szóló 1525/2013. (VIII. 12.) Korm. határozatot.

nak az Észak-atlanti Szerződés Szervezetében betöltött tagságából adódóan kötelezettsége a fenti NATO törekvésekhez alkalmazkodni, ami mind a végrehajtó hatalomra, mind pedig adott esetben az országgyűlésre — mint különleges jogrendet érintő fajsúlyos döntéshozóra— vonatkozó jogszabályi és működési keretek terén változásokat sürget. Másrészről a technológiafejlődése és a biztonsági környezet változása miatt gyarapodnak azok a kihívások és fenyegetések, amelyek operatív és gyors döntési/irányítási megoldásokat, illetve egy a normál kormányzati döntéshozataltól eltérő működési szisztémát igényelnek. Ez utóbbi körbe a már említett hírszerzési — illetve szükségképpen a NIÁT hatáskörébe nem sorolt elhárítási — funkciókhoz való szoros kapcsolat miatt beemelhető a hibrid konfliktusok lehetősége; hasonló módon megjeleníthető a terrorizmus elleni fellépés, amihez ma koordinatív keretek párosulnak;[24] de ide sorolható a váratlan támadás lehetősége és egyértelműen a kibertérből érkező támadások tárgyköre is.

Meglátásom szerint ezek vonatkozásában a fenti megoldások ötvözése vizsgálandó, vagyis a koordináció és a miniszterelnök döntéseit közvetlenül támogató állandó szervezeti keretek megvizsgálása mellett a konkrét és azonnali védelmi feladat ellátásának sajátos operatív irányítási és döntési rezsimjének a kialakítása akár egy e célt szolgáló nemzeti válságkezelő központ kialakításával[25] és a légierőéhez hasonló sajátos törvényi felhatalmazásokkal a többi azonnali döntést igénylő támadástípus tekintetében. Természetesen a szervezeti és aszabályozási vonatkozások össze is kapcsolhatók, azonban az biztos, hogy ez az alternatíva további tanulmányokkal részleteiben is vizsgálandó és kidolgozandó még. Fontos e körben hangsúlyt fektetni arra, hogy eltérő munkamódszerek és mérlegelési szempontok determinálják a stratégiai-politikai döntéshozatalt, azaz a kabinet és az azokat szakmailag megalapozó kormányzati munkacsoport döntéseit, és ezektől eltérő szempontok határozzák meg a konkrét és egyedi fenyegetésekre, támadásokra reagáló, illetve az azok kezelését irányító döntéseket, illetve az eseti irányítói és koordinatív aktusokat. Érdemes ezért ezeket elkülönítve, de az együttműködések révén egymást erősítve megtartani, kialakítani, illetve fejleszteni. Ennek további részletei kapcsán remélhető, hogy számos elemzés születik majd, az azonban talán vitán felül rögzíthető, hogy felgyorsult és megváltozott biztonsági környezetünk és ezen belül különösen a kibertérrel összefüggő körülményeink megkerülhetetlenné teszik a tervezés, szervezés, illetve a konkrét döntéshozatal körültekintő, rendszerszintű és jól záródó megújítását úgy a struktúrák, mint az eljárások és a szabályozás szintjén.

[24] E tekintetben lásd a Terrorellenes Koordinációs Bizottságra vonatkozó szabályozást és a további koordinatív szabályokat a 1824/2015. (XI. 19. Korm. határozatban.

[25] A téma kapcsán mérlegelhető javaslatok köréből lásd különösen: Keszely, 2017. A nemzetbiztonsági tevékenységek terén történő koordináció és koncentrált feladatellátás opciója kapcsán lásd még:Béres, 2008.

IV. ÖSSZEGZÉS

A különféle védelmi ágazatok korszerű és hatékony, a hálózatos felépítés mellett is együttműködésre képes kialakítása tekintetében egyértelműen látható, hogy a feladat aktuális és sürgető, azonban ez nem indokolhat olyan ad hoc és a szisztematikus építkezést mellőző képességkialakítási döntéseket, amelyek később egy fragmentált, vagy legalábbis nem kellően koherens rendszert eredményeznek.

A digitalizáció jelentősége, társadalmi, gazdasági és nem utolsó sorban biztonsági hatásainak korszakos fontossága abba az irányba mutat, hogy a kibertér biztonságát és védelmét garantálni hivatott nemzeti kibertér műveleti erők kialakítása nem egy aktuálisan teljesítendő és aztán elfelejthető feladat, hanem egy olyan új képességfejlesztési kihívás minden védelmi ágazatban és ez által Magyarország nemzetbiztonsági rendszerének egészében, amely egy a 21. századi biztonsághoz nélkülözhetetlen, új képesség- és funkcióösszesség létrehozásával azonosítható.

Ahhoz, hogy ezen képességek kialakítása, illetve fejlesztése hosszú távon is eredményes és a kor kívánalmainak megfelelő legyen, és ennek részeként a költségvetési forrásokat is hatékonyabban használja fel, szükséges, hogy az komplex módon, a képességek generálása és szervezeti kereteik kialakítása mellett a megfelelő szabályozás kidolgozásával és folyamatos megújításával történjen, méghozzá minden érintett védelmi ágazatra kiterjedő módon és azok együttműködésével.

A kibertér és a kibertérben megvalósuló cselekmények a polgári szférára, azaz a mindennapok szinte minden dimenziójára jelentős hatást gyakorolnak: megjelennek a rendészet, a honvédelem, a hírszerzés és elhárítás, valamint az ezek mindegyikében jelen lévő információbiztonsági szegmensekben is. Ebből adódóan az egyes védelmi funkciókon belül is ki kell alakítani az adott feladatellátás sajátosságaihoz igazodó kibertér műveleti képességeket a kiberbűnüldözéstől a kiberhírszerzésen és -elhárításon át egészen a katonai kibervédelemig.[26]

Egy ilyen összetett, széleskörű, mégis rendszerszinten záródó fejlesztés és megújítás komoly szakmai és nem utolsó sorban tudományos megalapozást igényel. A kiberbiztonság és -védelem sajátosságaiból adódó, széleskörű, sokrétű, multidiszciplináris szakmai igények és követelmények összehangolása már önmagában is jelentős feladat, hiszen a szűk értelemben vett védelmi szakkövetelmények mellett a tágabb IT szakmaiságnak, sőt a kapcsolódó összes szakterületnek és az innovációs célkitűzéseknek is megfelelően érvényesülnie kell. Ezeket a szakmai kritériumokat azonban össze kell hangolni a jog sajátosságaival, illetve kapcsolódó fejlesztési igényeivel, amin belül szükséges, hogy a nemzetközi jogi megoldások és változások feldolgozása és a nemzeti szintű komplex szabályo-

[26] Fontos azonban itt kiemelni, hogy a védelem szó ez esetben is az adott nemzet, állam, szövetség érdekeinek komplex védelmét és érvényesítését jelenti, vagyis a köznapi értelemben vett támadó cselekményekre, képességekre is kiterjed. Ezzel kapcsolatos korábbi kutatási megállapításaimat, illetve ebből adódóan a védelem sajátos szemléleti megközelítése kapcsán írtakat lásd: Farkas, i. m., 2018; Farkas, 2018d, 53–70.

zási rendszer kialakítása is megvalósuljon, beleértve ez utóbbiba a már meglévő nemzeti szintű védelmi szabályozással való összehangolást, illetve annak az egyébként is időszerű átfogó felülvizsgálatát.

Egy ilyen megalapozott és sokrétű előkészítés szükségképpen a védelmi és ezen belül a kibervédelmi funkciók sajátos igényei mellett is beépítendők az állam fejlesztésének tágabb folyamatába. A kibertér műveleti képességek kialakításánál tehát érdemes a jó kormányzás követelményeit is szem előtt tartani mind az aktív, műveleti, mind a támogató képességek és keretek kialakításánál. A képességgeneráláson túl vizsgálandó azonban a terület feletti kormányzati-politikai koordináció és irányítás szisztémája is, hiszen a szakmai koordinatív, a kormányzás szintjén megvalósuló politikai-koncepcionális, illetve a konkrét feladatellátással kapcsolatos eseti közjogi döntések fórumai nem vegyítendők. Azok ugyanis eltérő szemléletre, személyi összetételre és nem utolsó sorban közjogi hatáskörökre és célokra épülnek, vagyis eltérő, sajátos, egymást kiegészítő, de ekként nem fuzionálható államszervezeti funkciókat képviselnek. Ez utóbbiak áttekintése tehát még további elemzéseket, javaslatokat tesz szükségessé, amelyeknél szintén fontos, hogy a fenti irányvonalak érvényesülésére figyelmet szenteljenek a kutatók és a döntés-előkészítők is. Az azonban nehezen vitatható alapvetés e téren, hogy a szakmaiság, a nemzetközi jogi sajátosságok, a nemzeti jogi keretek, a jó kormányzás és a hatékony, megalapozott, gyors döntéshozatal követelményeinek összehangolása azonban nem képzelhető el széleskörű, differenciált és előremutató elemző, értékelő, kidolgozó munka nélkül.

IRODALOM

- AHRC (2013): *Backgroundpaper: Human rights in cyberspace*. Sydney, Australian Human Rights Commission.
- Andrews, Matthew (2008): *Good Government Means Different Things in Different Countries*. Harvard – John F. Kennedy School of Government, Faculty Research Working Papers, RWP08-068.
- Applegate, Scott D. (2013): The Dawn of Kinetic Cyber, in K. Podins, K. – Stinissen, J. – Maybaum, M. (eds.): *2013 5th International ConferenceonCyberConflictProceedings*. Tallinn, NATO CCD COE Publications, 163–177.
- Béres János (2008): *Napjaink muszlim terrorizmusának gyökerei és visszafordításának lehetőségei*. Budapest, Zrínyi Miklós Nemzetvédelmi Egyetem Hadtudományi Doktori Iskola, doktori értekezés.
- Blaskó Béla – Budaházi Árpád (2019): A *nemzetközi bűnügyi együttműködés joga*. Budapest, Dialóg Campus Kiadó – Wolters Kluwer.
- Chivvis, Christopher S. (2017): *Understanding Russian "Hybrid Warfare" and What Can Be Done About it.* Santa Monica, RAND Corporation.
- Concha Győző (1907): *Politika I. Alkotmánytan*. Budapest, Grill Károly Könyvkiadó vállalata.

• Csiki Tamás – Tálas Péter – Varga Gergely (2014): A NATO walesi csúcstalálkozójának napirendje és értékelése. *Nemzet és Biztonság* 4. szám, 112–128.
• Farkas Ádám (szerk.) (2018a): *Védelmi alkotmányosság az új típusú biztonsági kihívások erőterébe*. Budapest, Magyar Katonai Jogi és Hadijogi Társaság.
• Farkas Ádám (2018b): *A fegyveres védelem mint állami alrendszer és annak szabályozási sajátosságai*. Budapest, Magyar Katonai Jogi és Hadijogi Társaság.
• Farkas Ádám (2018c): *A totalitás kora? A 21. század biztonsági környezetének és kihívásainak totalitása és a totális védelem gondolatkísérlete*. Budapest, Magyar Katonai Jogi és Hadijogi Társaság.
• Farkas Ádám (2018d): Az állam védelmi kötelezettségeinek egyes kortárs aspektusai. *Jogelméleti Szemle* 4. szám, 53–70.
• Finszter Géza (018): *Rendészettan*. Budapest, Nemzeti Közszolgálati Egyetem.
• Geers, Kenneth (eds.) (2015): *Cyber War in Perspective: Russian Aggression against Ukraine*. Tallinn, NATO Cooperative Cyber Defence Centre of Excellence.
• Graham, John – Amos, Bruce – Plumptre, Tim (2003): Principles for Good Governance in the 21st Century. Ottawa, Institute on Governance – *Policy Brief* No. 15.
• Hermann, Rainer (2015): *Az iszlám állam*. Budapest, Akadémiai Kiadó.
• Hódos László (2018): Gondolatok a nemzeti hírszerző képesség koordinációjáért felelős szerv közjogi helyzetéről. *Szakmai Szemle* 4. szám, 5–16.
• Kaiser Tamás – Bozsó Gábor (2016): Az államközpontú kormányzás koncepciójának és mérhetőségének főbb aspektusai. *Államtudományi Műhelytanulmányok* 22. szám.
• Kaiser Tamás – Kis Norbert (szerk.) (2014): *A jó állam mérhetősége*. Budapest, Nemzeti Közszolgálati Egyetem.
• Kaiser Tamás (szerk.) (2016): *A jó állam nagyító alatt: speciális jelentések A-tól V-ig (az adóbürokráciától a versenyképességig)*. Budapest, Dialóg Campus Kiadó.
• Kelemen Roland – Németh Richárd (2018): A kibertér fogalmának és jellemzőinek multidiszciplináris megközelítése. In: Farkas, Ádám (szerk.): *Védelmi alkotmányosság az új típusú biztonsági kihívások erőterében.* Budapest, Magyar Katonai Jogi és Hadijogi Társaság, 147–170.
• Kelemen Roland – Pataki Márta (2015): A kibertámadások nemzetközi jogi értékelése. *Katonai Jogi és Hadijogi Szemle*, 1. szám, 53–90.
• Kelemen Roland (2018): A derogáció értelmezése a Polgári Jogok Nemzetközi Egyezségokmányának, valamint az Emberi Jogok Európai Egyezményének tükrében. *Közjogi Szemle* 4. szám, 52–58.
• Keszely László (2017): *A védelmi igazgatás szerepe a nemzeti szintű átfogó megközelítés megvalósításában*. Budapest, Nemzeti Közszolgálati Egyetem Hadtudományi Doktori Iskola, doktori értekezés.
• Klimburg, Alexander (eds.) (2012): *The national Cyber Security Framework Manual*. Tallinn, NATO Cooperative Cyber Defence Centre of Excellence.
• Lattmann Tamás (2018): Nemzetközi jogi szabályozás célzott kibertámadások esetén. In: Deák Veronika (szerk.): *Célzott kibertámadások*. Budapest, Nemzeti Közszolgálati Egyetem, 39–51.
• Mógor Tamás (2018): A légierő tevékenységének jelentősége Magyarország szuverenitásának és biztonságának fenntartásában. *Hadtudomány* 6. szám, 134–139.
• Munk Sándor (2018): A kibertér fogalmának egyes, az egységes értelmezést biztosító kérdései. *Hadtudomány* 1. szám, 113–131.

• Napoleoni, Loretta (2015): *Az iszlamista főnix*. Budapest, HVG Könyvek.
• Nolte, Georg (2003): *European military lawsystems*. Berlin, De GruyterRect.
• Papp Zoltán (2019): *A légtér-szuverenitás néhány nemzetközi jogi kérdése,* Budapest, Pázmány Péter Katolikus Egyetem Jog- és Államtudományi Doktori Iskola, doktori értekezés.
• Patyi András (2016): Good Governance and Good Public Administration. *Public Governance Andministration and Finance Law Review in the European Union and Central Eastern Europe* 1. szám, 1–14.
• Schmitt, N. Michael (eds) (2013): *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge, Cambridge University Press.
• Schmitt, N. Michael (eds) (2017): *Tallinn Manual 2.0 onthe International Law Applicable to Cyber Warfare*. Cambridge, Cambridge University Press.
• Spitzer Jenő (2019): *Önvédelem versus terrorizmus. Az erőszak tilalma és az önvédelem joga a nemzetközi jogban, különös tekintettel az Iszlám Állam elleni nemzetközi fellépés lehetőségeire*. Budapest, Magyar Katonai Jogi és Hadijogi Társaság.
• Stumpf István (szerk.) (2014): *Erős állam – alkotmányos korlátok*. Budapest, Századvég kiadó.
• Stumpf István (2014a): A „jó kormányzás" két értelme. Avagy a demokratikus kormányzás programja és feltételei. In: Stumpf István: *Erős állam, alkotmányos korlátok*. Budapest, Századvég kiadó, 67–96.
• Stumpf István (2014b): A jó kormányzás felé. In: Stumpf István: *Erős állam, alkotmányos korlátok*. Budapest, Századvég kiadó, 135–158.
• Stumpf István (2014c): Neoweberi állam és jó kormányzás. Avagy mit tennél, ha te volnál az állam? In: Stumpf István: *Erős állam, alkotmányos korlátok*. Budapest, Századvég kiadó, 97–134.
• 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 21. században*. Budapest, Gondolat kiadó, 35-60.
• Szkála Károly – Munk Sándor (2018): A kibertér fogalma, értelmezése és fejlődése. *Földrajzi Közlemények* 204. szám, 344–355.
• Tálas Péter (2016): A varsói NATO-csúcs legfontosabb döntéseiről. *Nemzet és Biztonság* 2. szám, 97–101.
• Ferm, Tiina: *Laws in the Era of Hybrid Threats*. Helsinki, The European Centre of Excellence for Countering Hybrid Threats.
• Treverton, Gregory F. – Thyedt, Andrew – Chen, Alicia R. – Lee, Kathy – McCue, Madeline (2018): *Adressing Hybrid Threats*. Stockholm, Swedish Defence University.
• Wallace, David (2018): Cyber Weapon Reviews under International Humanitarian Law: A Critical Analysis. In: *Tallinn Paper* No 11. Tallinn, NATO Cooperative Cyber Defence Centre of Excellence.
• Weiss, Michael – Hassan, Hassan (2015): *Az iszlám állam*. Budapest, HVG Könyvek,
• Ziolkowski, Katharina (2013): Peacetime Cyber Espionage – New Tendenciesin Public International Law. In: Ziolkowski, Katharina (eds.): *Peacetime Regime for State Activities in Cyberspace International Law, International Relations and Diplomacy*. Tallinn, NATO Cooperative Cyber Defence Centre of Excellence Publication, 425–464.


MATRÓZ