Hadtudományi Szemle
19. évfolyam (2026) 1. szám 101–118. • DOI: 10.32563/hsz.2026.1.6

Kovács Kinga Virág[1]

A kiberműveletek nemzetközi jogi szabályozása

A humanitárius jog alkalmazásának megközelítései

The International Legal Regulation of Cyber Operations

Approaches to the Application of International Humanitarian Law

Absztrakt

A tanulmány a kiberműveletek nemzetközi jogi szabályozásának jelenlegi állását vizsgálja, különös tekintettel arra, hogy a nemzetközi humanitárius jog elvei miként alkalmazhatók a kibertérben. A tanulmány célja, hogy bemutassa a szabályozási megközelítések és szakértői álláspontok sokszínűségét, valamint azt, hogyan jelennek meg ezek a különbségek az állami gyakorlatban. A vizsgálat középpontjában négy állam – az Egyesült Államok, az Egyesült Királyság, Franciaország és Hollandia – álláspontja áll, amelyek eltérő jogi kultúrájuk és biztonságpolitikai hátterük révén jól szemléltetik a formális elfogadás és gyakorlati rugalmasság dinamikáját.

Kulcsszavak: kibertér, kiberműveletek, nemzetközi humanitárius jog

Abstract

The study examines the current state of international legal regulation of cyber operations, with a particular focus on how the principles of international humanitarian

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem Hadtudományi Doktori Iskola, e-mail: kovacs.kinga.virag@uni-nke.hu

law can be applied in cyberspace. The study aims to demonstrate the diversity of regulatory approaches and expert positions, and how these differences are reflected in state practice. The study focuses on the positions of four states – the United States, the United Kingdom, France and the Netherlands – which, through their different legal cultures and security policy backgrounds, illustrate the dynamics of formal acceptance and practical flexibility.

Keywords: cyberspace, cyber operations, international humanitarian law

Bevezetés

A kibertér napjainkra a nemzetközi jog egyik legvitatottabb és legösszetettebb szabályozási területévé vált. A gyors technológiai fejlődés, a digitális infrastruktúrák összekapcsoltsága és a kiberműveletek növekvő politikai, gazdasági és katonai jelentősége alapjaiban formálja át az államok közötti viszonyokat. Kiberműveletnek azokat a tevékenységeket tekintjük, amelyeket a kibertérben vagy a kibertér felhasználásával hajtanak végre, és amelyek mögött olyan állami vagy államnak tulajdonítható motiváció áll, amely jogilag releváns hatás kiváltására irányul. Ezen kibertérben végrehajtott tevékenységek növekvő jelentőségére való tekintettel a nemzetközi közösség az elmúlt két évtizedben több fórumon is kísérletet tett a kibertér szabályozási kereteinek kialakítására. Az ENSZ égisze alatt működő Group of Governmental Experts (GGE) és az Open-Ended Working Group (OEWG) olyan kulcsfontosságú mechanizmusokká váltak, amelyek az államok közötti normateremtés és jogértelmezés elsődleges terepei. Az ezt követő évek vitái azonban megmutatták, hogy az alkalmazhatóság elvi elfogadása mögött jelentős értelmezési különbségek húzódnak meg.

Bár nyíltan egyik állam sem kérdőjelezi meg a humanitárius jog alkalmazhatóságát, az értelmezési gyakorlatok eltérései jól mutatják, hogy a nemzetközi jog alkalmazása a kiberműveletek esetében még korántsem egységes. Egyes országok – mint az Egyesült Államok és az Egyesült Királyság – rugalmas, hatásalapú kereteket alkalmaznak, míg mások – mint Franciaország és Hollandia – kötöttebb, normatív értelmezést képviselnek. A tanulmány célja, hogy bemutassa a szabályozási megközelítések fő irányait, összefoglalja a szakértői álláspontokat, és feltárja, miként jelennek meg ezek az állami gyakorlatban és nyilatkozatokban. Ennek okán a tanulmány nem állásfoglalásként, hanem összehasonlító áttekintésként vizsgálja a jelenlegi szabályozási állapotokat. A tanulmány célkitűzéseinek megfelelően az elemzés két kutatási kérdés mentén igyekszik átfogó képet nyújtani:

- Milyen mértékben alkalmazható a humanitárius jog a kiberműveletek során?
- Milyen eltérések mutathatók ki az angolszász és a kontinentális jogi kultúrák kiberműveletekre vonatkozó jogértelmezésében?

A téma relevanciáját növeli, hogy a kiberműveletek egyre gyakrabban érik el azt az intenzitási küszöböt, amely már a fegyveres konfliktusok jogi kereteit is érintheti, miközben az alkalmazandó jogi normák értelmezése továbbra is vitatott. A jogértelmezési bizonytalanság közvetlen hatással van az államok magatartására és felelősségük

megállapíthatóságára is. Ezen körülmények indokolják a meglévő szabályozási megközelítések összehasonlító vizsgálatát.

A kibertér mint a szabályozni kívánt „terület"

A kibertér nehezen magyarázható meg egyetlen definícióval. Inkább munkafogalmakat használunk, amelyek egymással részben átfedő, részben eltérő meghatározások sokaságaként jelennek meg a szakirodalomban. A fogalmi nehézségeket többek között az okozza, hogy a definíciókat sokszor nem is ugyanazon a szinten tárgyaljuk, ami erősen kötődik ahhoz a hatalmas ütemű technológiai változáshoz, amely akár néhány év alatt is alapjaiban változtatja meg a területről alkotott legalapvetőbb elképzeléseinket és meghatározásainkat. Annak okán, hogy a kibertér több mint csupán a technológiai működés megértése – hiszen társadalmi, gazdasági, politikai és biztonsági tér is egyben – érdemes egy stratégiai szemléletű definíciót alkalmaznunk, amely segít abban, hogy a fogalmat ne pusztán technikai értelemben, hanem az állam működése, a nemzetbiztonság, a gazdaság és a társadalom összefüggéseiben is értelmezzük. Mivel a biztonsági és technológiai környezet is rendkívül gyorsan változik, a stratégiai megközelítés segítséget tud nyújtani abban, hogy amikor a szabályozás kérdéskörére kerül sor, ne csak a pillanatnyi állapotra reagáljunk, amely az aktuális technológiai trendeket követi le, hanem hosszú távon is érvényes kereteket hozzunk létre, ami komplex módon több szint összehangolását igényli.[2]

Ennek okán érdemes a kibertér fogalmára a 2013-as *Magyarország Nemzeti Kiberbiztonsági Stratégiájá*ban ismertetett kibertér fogalmat használni:[3]

> „A kibertér globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét jelenti. Magyarország kibertere a globális kibertér elektronikus információs rendszereinek azon része, amelyek Magyarországon találhatóak, valamint a globális kibertér elektronikus rendszerein keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok közül azok, amelyek Magyarországon történnek vagy Magyarországra irányulnak, illetve amelyekben Magyarország érintett."[4]

A kibertér szabályozói környezetének kialakítása számos nehézségbe ütközik, amelyek közül az egyik legjelentősebbnek az egységes fogalmi keretrendszer hiánya bizonyul. A szakirodalomban és a nemzetközi gyakorlatban a kibertérhez kapcsolódó alapfogalmak, mint például a kibertér, a kiberbiztonság, a kiberművelet vagy a kiberfenyegetés, eltérő értelmezésekben jelennek meg, ezzel tovább árnyalva a közös szabályozási alapok lefektetését. A fogalmak közötti bizonytalanság az elméleti megközelítésekben és a jogi gyakorlatokban is megmutatkozik, megnehezítve, vagy éppen akadályozva

[2] Kovács 2018: 16.

[3] Bár Magyarország 2025-ben új kiberbiztonsági stratégiát fogadott el, jelen tanulmány a 2013-as stratégia kibertérdefiníciójára támaszkodik a vizsgált jelenség fogalmi kereteinek lehatárolása érdekében.

[4] 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról, II. pont.

az egységes és koherens szabályozási struktúra kialakítását. Ennek következtében a kibertér szabályozására tett törekvések gyakran nemzetenként és szervezeti szinten is eltérő hangsúllyal jelennek meg, ami tovább nehezíti az együttműködést és a normák nemzetközi szinten történő összehangolását. Az egységes fogalmi alapok hiánya így nem pusztán terminológiai kérdés, hanem a szabályozás hatékonyságát és alkalmazhatóságát alapvetően befolyásoló tényezőként is megjelenik.

Mindezekre tekintettel kézenfekvő lépésnek bizonyult egy, legalább kiindulópontként szolgáló egységes alap megteremtése érdekében a már meglévő nemzetközi jog alkalmazhatóságának vizsgálata és elfogadása nemzetközi szinten. A kibertér nemzetközi szabályozását célzó együttműködések száma az elmúlt másfél évtizedben látványosan nőtt, ám ezek között az ENSZ égisze alatt működő fórumoknak van a legnagyobb intézményi súlya. A Groups of Governmental Experts (GGE) és az Open-Ended Working Group (OEWG) két olyan multilaterális folyamat, amely közvetlenül az ENSZ Közgyűlés mandátumával működik, és amelyek az állami magatartásra vonatkozó globális normák és jogi értelmezések kialakítását tűzték ki célul.[5]

Nemzetközi jogértelmezési keretek

Az ENSZ kibernormákról szóló megbeszélései majdnem olyan régiek, mint maga a világháló. A technológia központi szerepe a politikai-katonai kontextusban az 1990-es évek elején vált nyilvánvalóvá, amikor az Egyesült Államok domináns pozícióra tett szert a technológiai fejlődés terén, ami katonai fölényében is megnyilvánult.

Elismerve az Egyesült Államok dominanciáját az információs és kommunikációs technológia (IKT) terén, az Orosz Föderáció először 1998-ban javasolta az IKT-kérdések nemzetközi biztonsággal kapcsolatos megvitatását az ENSZ-ben. Miután többször is megpróbáltak különböző ENSZ-fórumokat használni a megbeszélések megkezdésére, úgy döntöttek, hogy a legjobb megoldás egy kormányzati szakértői csoport (GGE) létrehozása. Az Orosz Föderáció 2002-ben ENSZ-közgyűlési határozatot javasolt, amely felszólított a GGE létrehozására a kibertérben felmerülő fenyegetések és a lehetséges együttműködési intézkedések tanulmányozása céljából. A kiberkonfliktusok történetéről szóló számos különböző beszámoló szerint a 2007 előtti időszakot alacsony szintű kiberfenyegetettség-tudatosság jellemezte a felső döntéshozók, diplomaták és katonai vezetők körében. A katonai rendszerekbe történő súlyos kiberbehatolások és a kiberhírszerző műveletek a nemzetbiztonsággal kapcsolatos bizalmas akták keretein belül maradtak. 2007-ben fedezte fel a szélesebb közvélemény, hogy a kiberbiztonság stratégiai kockázat forrásává vált, amely destabilizálhat egy egész országot, és nagyszabású politikai és gazdasági káoszt okozhat. A 2007-es észtországi események figyelmeztető jelként szolgáltak, megmutatták, hogyan lehet a kibertámadásokat és a hibrid műveleteket geostratégiai kontextusban felhasználni külpolitikai célokra.

A 2013-as GGE-jelentés volt az első olyan dokumentum, amely kifejezetten kimondta, hogy a nemzetközi jog – beleértve az ENSZ Alapokmányát – alkalmazandó a kibertérben. Ezt a megállapítást a 2015-ös GGE-jelentés tovább erősítette, tizenegy,

[5] United Nations 2025.

békeidőben irányadó állami magatartási normát is megfogalmazott, a nemzetközi jogi kötelezettségek kiegészítéseként. E jelentések együttesen alapozták meg azt a ma is érvényes álláspontot, hogy a kibertérben zajló állami tevékenységekre a meglévő nemzetközi jogi normák és elvek vonatkoznak, még ha ezek gyakorlati érvényesítése továbbra is jelentős kihívásokat rejt.[6]

2019-ig az Egyesült Nemzetek Szervezetének égisze alatt működő GGE volt az egyetlen mérvadó szerv a nemzetközi közösség számára a kibertér jogi, technológiai és politikai kihívásainak a nemzetközi biztonság kontextusában kezelésére vonatkozó értékelésére és ajánlások megfogalmazására. 2017 júniusára azonban a csoportnak nem sikerült konszenzusra jutnia, és az előtte folyó munka összeomlott. Mivel az ENSZ Közgyűlés 72. ülésszakán nem történt kísérlet a folyamat újraélesztésére, úgy tűnt, mintha a kormányzati keretek mechanizmusa teljesen kimerült volna.

Ennek ellenére a kiberhatalmak és nagyhatalmi versenytársaik, mint például az Egyesült Államok és az Egyesült Királyság az egyik oldalon, valamint Oroszország és Kína a másikon, nem hagyták abba stratégiai érdekeik védelmét a kibertérben azáltal, hogy saját jogi és politikai nézeteiket népszerűsítették az ENSZ tagállamai között, miközben igyekeztek elutasítani vagy legalábbis visszafogni politikai riválisaik ellenlépéseit. Oroszország 2018-ban javaslatot tett a GGE helyettesítésére – egy Nyílt Végű Munkacsoportra (OEWG). A GGE-hez hasonlóan az OEWG is konszenzus alapján működött, de azzal ellentétben nyitott volt minden ENSZ-tagállam számára, sőt, lehetővé tette bármely érdekelt fél számára a magánszektorból, az akadémiai szférából és a civil szervezetekből, hogy részt vegyen az eljárásokban és véleményt nyilvánítson a megvitatott releváns kérdésekről.[7]

Az OEWG megosztónak bizonyult, s mivel azon országok kezdeményezték, amelyek a kibertérben kifejezetten aktívak, nem nyerték el a nyugati országok bizalmát a feltétlen együttműködés terén. Az OEWG által egyik legnagyobb különbségnek a GGE munkájához képest a kibertérben tanúsított állami magatartással kapcsolatos szerződésre irányuló törekvések bizonyulnak.[8]

Ezek a fórumok hozzájárulnak ahhoz, hogy a nemzetközi jog alapelvei a kibertérben is érvényesüljenek, és hogy a nemzetközi közösség közös normák mentén megpróbálja kezelni a kibertérben jelentkező kihívásokat. Ugyanakkor nem szabad figyelmen kívül hagyni, hogy a kibertérnek mindezek mellett katonai dimenziója is van. A politikai és jogi szintű megállapodások fontos keretet biztosítanak, de nem feltétlenül adnak választ arra, miként érvényesülnek ezek az elvek a katonai műveletek és konfliktusok során.

Ezért a téma vizsgálatát szükséges szűkíteni, és a kibertér konkrétabb szegmenseire – különösen a katonai jellegű alkalmazásokra és műveleti környezetre – fókuszálni. Ezzel lehetővé válik annak feltárása, hogy az elméletben kidolgozott normák és szabályozási elvek a gyakorlatban is működőképesek-e, illetve milyen korlátokkal szembesülünk a tényleges alkalmazásuk során.

[6] Tiirmaa-Klaar 2021.
[7] Efrony 2021.
[8] McDonald 2023.

A kibertér katonai dimenziója – a kibertér mint a kiberműveletek helyszíne

A kibertér sajátosságai miatt a kiberműveleteknek mint a fegyveres konfliktusokban alkalmazott hadviselési eszköznek valós és nem elhanyagolható kockázata van. A nemzetközi közösség ezért elismeri, hogy – a hadviselés más eszközeihez és módszereihez hasonlóan – a kiberműveletek is okozhatnak károkat a civil lakosságnak, valamint más védett személyeknek és objektumoknak. További veszély, hogy a kibereszközök szándékosan vagy nem szándékolt mellékhatásként rendszerszintű, széles körű következményeket válthatnak ki a kritikus polgári infrastruktúrában: érinthetik az alapvető iparágakat, a távközlést és a közlekedést, valamint a kormányzati és pénzügyi rendszereket is. A katonai kiberképességek egyre növekvő használata és az ehhez kapcsolódó humanitárius aggodalmak rávilágítottak arra, mennyire fontos közös megegyezésre jutni a fegyveres konfliktusok során a kiberműveletekre vonatkozó jogi korlátozásokról.

A kiberműveletek stratégiai jelentőségének növekedése a nemzetközi biztonsági szervezeteket is arra késztette, hogy hivatalosan is foglalkozzanak a kibertér katonai dimenziójával. E folyamat egyik legfontosabb mérföldkövét a NATO döntései jelentették, amelyek kijelölték a kiberhadviselés politikai és jogi kereteit. A 2016. július 8–9-én tartott varsói NATO-csúcstalálkozón a NATO-országok állam- és kormányfői, valamint más nemzetek, köztük Montenegró, Ukrajna, Grúzia és Oroszország képviselői a meglévő kötelezettségvállalások – például a kibervédelmi képességek megerősítése és a nemzetközi jog alkalmazhatóságának megerősítése – mellett a kibertér műveleti területként való elismeréséről döntöttek. Továbbá a NATO állam- és kormányfői a 2014. szeptember 4–5-i walesi NATO-csúcstalálkozón jóváhagyták a NATO megerősített kibervédelmi politikáját, amelyben elismerik, hogy a nemzetközi jog – beleértve a nemzetközi humanitárius jogot és az ENSZ Alapokmányát – a kibertérben is alkalmazandó. A NATO kiemeli, hogy a kibertámadások elérhetik azt a küszöböt, amely veszélyezteti a nemzeti és az euroatlanti jólétet, biztonságot és stabilitást, hatásuk pedig ugyanolyan káros lehet a modern társadalmakra, mint egy hagyományos támadás. Ebből adódóan a kibervédelem a NATO kollektív védelemre vonatkozó alapvető feladatának is része, így az Észak-atlanti Szerződés kollektív önvédelemről szóló 5. cikke olyan kibertámadás esetén is alkalmazható, amelynek hatásai összehasonlíthatók egy hagyományos fegyveres támadás hatásaival.

A Tallinn Manual alapvető megközelítéseinek kontextuális bemutatása

A NATO politikai döntéseihez hasonlóan a tudományos és jogi közösség is igyekezett választ adni a kiberműveletek szabályozásával kapcsolatos kérdésekre. Ennek egyik legjelentősebb példája a *Tallinni kézikönyv* megszületése volt, amely a kiberhadviselés nemzetközi jogi alapelveit igyekezett rendszerezni.

A kiberhadviseléssel kapcsolatos jogszabályok kristályosításának első kísérlete Michael N. Schmitt professzor nevéhez fűződik, aki a NATO Kooperatív Kibervédelmi Kiválósági Központjának meghívására nemzetközi jogi szakértőkből álló csoportot

vezetett a kiberhadviselésben alkalmazandó nemzetközi jogról szóló *Tallinni kézikönyv (Tallinn Manual)* megírásában. A 2013-ban megjelent első kiadást a 2017-es, bővített *Tallinn Manual 2.0* követte, amely már a kiberműveletekben alkalmazandó jogot is részletesen tárgyalta, 154 szabályt foglalva össze. Mindazonáltal a problémák továbbra is fennmaradtak.

A kiberhadviselésről rendelkezésre álló bőséges szakirodalom ellenére ez a jegyzet nem a meglévő humanitárius jog kiberhadviselésre való alkalmazását vizsgálja, hanem öt releváns jogi kihívás kritikai elemzésére vállalkozik. Először is, különbséget tesz a kiberhadviselés és a kiberbűnözés között, mivel a fogalmi zavar befolyásolhatja az államok jogi válaszait és ellenintézkedéseit. Másodszor, rámutat a nemzetközi jog elveinek kiberműveletekre való alkalmazása során felmerülő nehézségekre. Harmadszor, a tanulmány visszatér az öt fő jogi kérdéshez, amelyek a kiberhadviselés területén a leggyakrabban merülnek fel. A *Tallinn Manual,* bár mindenképpen irányt mutat azt illetően, hogy a humanitárius jog miként érvényesülhet a kiberműveletek vonatkozásában, semmilyen jogi kötőerővel nem bír.[9] Azonban megalkotása arra utal, hogy a nemzetközi közösség inkább a meglévő jogi normák adaptálására törekszik, mintsem hogy új, kifejezetten a kibertérre szabott szabályrendszert akarna létrehozni.

Mivel a *Tallinn Manual 2.0* nem rendelkezik kötelező jogi erővel, a szakirodalomban számos kritika érte amiatt, hogy bizonyos szabályai nem államgyakorlatokon, hanem szakértői konszenzuson alapulnak. Ebből fakadóan a kézikönyv megítélése jelentősen eltér a különböző jogrendi hagyományok között. A *Tallinn Manual* körüli szakmai viták rávilágítanak arra is, hogy a nemzetközi jog kiberműveletekre való alkalmazása nem pusztán normatív, hanem értelmezési kérdés is. Tsagourias és Farrell (2020) szerint a kibertér sajátosságai miatt az államok nem egységes módon értelmezik a meglévő jogi szabályokat, hanem azokat eltérő politikai, stratégiai és jogi megfontolások mentén alkalmazzák, ami jelentős értelmezési divergenciát okot az állami gyakorlatok szintjén.[10]

Az értelmezési kihívások egy része jogi szinten jelentkezik, hiszen a nemzetközi humanitárius jogot eredetileg fizikai hadszínterekre alkották meg. Ezért több szakértő is rávilágított arra, hogy a kiberműveletek sajátos természete miatt a meglévő jogi keretek alkalmazása komoly nehézségeket okoz, a *Tallinn Manual*ben megfogalmazottak pedig nem bizonyulnak elégségesnek, úgy, ahogy a humanitárius jog alkalmazása sem. Ezzel a megközelítéssel egy másik szemlélet azonosítható, amely azt vallja, hogy a humanitárius jog nem alkalmazható a kiberműveletek esetében, s új szabályozási keretek megalkotása lenne szükséges.

A nemzetközi humanitárius jog alkalmazhatóságának megkérdőjelezése

D'Aspremont szerint ezek a nehézségek elsősorban abból erednek, hogy a nemzetközi jogászok többsége intervencionista megközelítést alkalmaz, vagyis ahelyett, hogy új normákat alkotnának, megpróbálják a meglévő jogi kereteket, például az ENSZ Alapokmányát

[9] Mann 2020.
[10] Tsagourias–Farrell 2020.

vagy a humanitárius jogot – kiterjeszteni a kibertérre. Ez a jognyújtási stratégia azonban problémás, mert a kiberműveletek jellegüknél fogva nem illeszkednek jól azokhoz a kategóriákhoz, amelyeken a humanitárius jog alapszik. A szerző szerint ez a fajta tudományos aktivizmus legitimációs válságot okoz, mert a jogászok jogalkotói szerepbe kerülnek anélkül, hogy erre felhatalmazást kaptak volna. Különösen nehéz továbbá a bizonyítás, ami a humanitárius jog alkalmazását gyakorlatilag ellehetetleníti. Az államok közötti felelősség megállapításához szükséges bizonyítékok gyakran hiányosak, manipulálhatók vagy technikailag értelmezhetetlenek, így az olyan alapelvek, mint az arányosság vagy a megkülönböztetés, nehezen vagy egyáltalán nem alkalmazhatók a kiberműveletek esetében.

A D'Aspremont által felvetett elméleti problémákat véleményem szerint a gyakorlatban tovább súlyosbítja, hogy az államok között sincs teljes egyetértés abban, hogyan kell a kiberműveleteket a nemzetközi jog rendszerébe beilleszteni. Pomson elemzése is erre hívja fel a figyelmet, aki a szokásjog és az államgyakorlat korlátait boncolgatja.

Pomson először is hangsúlyozza, hogy a kiberműveletek jogi szabályozására vonatkozó állami álláspontok földrajzilag és politikailag nem reprezentatívak. A legtöbb állásfoglalást nyugati országok tették közzé, míg számos afrikai és ázsiai állam teljesen kimaradt a diskurzusból. Ez a részleges állami részvétel aláássa annak a lehetőségét, hogy a kiberműveletekre vonatkozó egységes szokásjogi normák alakuljanak ki, hiszen a szokásjoghoz szükség van széles körű, reprezentatív és következetes államgyakorlatokra. Másodszor, a szerző szerint jelentős ellentétek vannak az államok között abban is, hogy mi minősül támadásnak a humanitárius jog alapján, ami a hadviselésre vonatkozó alapelvek alkalmazhatóságát is megnehezíti. Egyes államok kizárólag a fizikai károkozást vagy halált, serülést tekintik támadásnak, míg mások szerint már a funkcionális kiesés vagy adatvesztés is ebbe a kategóriába eshet. Ez a fogalmi széttartás gátolja a szokásjogi konvergenciát, hiszen nincs egységes értelmezés arról, hogy mely kiberműveletek sértik a humanitárius jog szabályait. Harmadszor, Pomson rámutat arra, hogy a nemzetközi szokásjog nem értelmezhető, tehát nem lehet egyszerűen kiterjesztéssel vagy analógiával a korábbi, nem kiberkörnyezetben kialakult szabályokat a kiberműveletekre alkalmazni. Ehelyett csak a tényleges államgyakorlat és a jogként való elfogadás alapján lehet megállapítani, hogy egy adott szabály alkalmazható-e. Ennek okán elmondható, hogy a nemzetközi jog egységes alkalmazása a kiberműveletek terén módszertani akadályokba is ütközik, hiszen a jogfejlődés itt nem normatív, hanem gyakorlati tapasztalatokra épül.

Állami megközelítések

A nemzetközi közösség túlnyomó része, különösen az ENSZ-ben és más nemzetközi szervezetekben aktív, főként nyugati államok, valamint a NATO-tagok támogatják a humanitárius jog kibertérben való alkalmazását, és azt magukra nézve kötelezőnek tekintik. Bár az értelmezési keretek országonként bizonyos mértékben eltérhetnek, abban széles körű egyetértés van, hogy a nemzetközi jog a kiberműveletekre is irányadó. Az elemzés négy ország – az Egyesült Államok, az Egyesült Királyság, Hollandia és Franciaország – nemzeti álláspontját mutatja be a nemzetközi humanitárius jog kiberműveletekre való alkalmazhatóságával kapcsolatban.

Franciaország és Hollandia az európai kontinentális jogi kultúrát képviselik, ezzel szemben az Egyesült Államok és az Egyesült Királyság angolszász, gyakorlatorientált megközelítése inkább a rugalmas jogalkalmazást példázza, amely során formálisan elfogadják a humanitárius jog kötelező erejét, ugyanakkor annak tartalmát és gyakorlati kiterjedését saját nemzeti érdekük és biztonságpolitikai környezetük fényében értelmezik. A kiválasztott országok nemcsak földrajzi és politikai értelemben mutatnak változatosságot, hanem jogértelmezési szinten is, ami lehetővé teszi annak bemutatását, hogy miként alakult ki a nemzetközi konszenzus a humanitárius jog alkalmazhatóságáról, és ezzel párhuzamosan hogyan maradt fenn mégis a nemzeti mozgástér az értelmezési különbségek terén. Az elemzés tehát nem az államok magatartásának normatív értékelésére, hanem a formális elfogadás és gyakorlati rugalmasság dinamikájának feltárására törekszik.

Módszertan

A tanulmány kvalitatív, összehasonlító szövegelemzésen alapul, amely a négy említett állam – az Egyesült Államok, az Egyesült Királyság, Franciaország és Hollandia – hivatalos álláspontját vizsgálja a nemzetközi humanitárius jog kiberműveletek során való alkalmazhatóságára vonatkozóan. A módszertani megközelítés célja annak feltárása, hogy a különböző jogi kultúrákhoz tartozó államok miként értelmezik a szuverenitást, a be nem avatkozás elvét, az erőalkalmazás tilalmát, az önvédelem lehetőségét, valamint az ellenintézkedéseket a kibertérben. A vizsgálat alapját kizárólag nyilvánosan hozzáférhető állami dokumentumok, kormányzati nyilatkozatok és az ENSZ-hez benyújtott hivatalos jelentések képezték, mivel ezek tekinthetők az adott ország formai jogértelmezése legmegbízhatóbb forrásainak.

A dokumentumok kiválasztását két fő szempont indokolta. Egyrészt valamennyi vizsgált állam rendelkezik olyan hivatalos, önállóan közzétett nemzeti állásfoglalással, amelyben részletesen bemutatja a kibertérre vonatkozó nemzetközijog-értelmezését. Másrészt a négy állam két különböző jogi tradíció – az angolszász és a kontinentális jogrendszer – reprezentánsa, ami lehetőséget biztosít a normatív és a gyakorlatorientált megközelítések összehasonlítására. A kiválasztott dokumentumok közé kizárólag olyan állami források kerültek, amelyek explicit módon fogalmaznak meg jogértelmezési álláspontot, különösen a szuverenitás, a be nem avatkozás, az erőalkalmazás, az önvédelem és az ellenintézkedések viszonylatában.

A szövegelemzés a CCDCOE Cyber Law Toolkit tematikus szerkezetére épülő kódolási rendszer alapján készült. A vizsgálat öt fő kategória mentén történt:

- a szuverenitás értelmezése,
- be nem avatkozás elvének alkalmazása,
- erőszak alkalmazásának tilalma,
- önvédelemhez való jog,
- ellenintézkedések.

Az angolszász és a kontinentális megközelítés közötti különbségtétel alapját a vizsgálat során a következő szempontok indokolták. A szuverenitás normatív státuszának eltérő

értelmezése, a be nem avatkozás elvének szűk vagy kiterjesztett alkalmazása, a nemzetközi jogi kötelezettségek gyakorlati érvényesítésének mértéke és rugalmassága. E három szempont mindegyike közvetlenül tükröződik a vizsgált állami dokumentumokban, és egyben összhangban áll a CCDCOE által alkalmazott tematikus felosztással is.

A kiberműveletek jogi értékelése elsődlegesen a nemzetközi humanitárius jog keretrendszerében történik, azonban a nemzetközi jog általános szabályai közül az állami felelősség *(state responsibility)* és a kellő gondosság *(due diligence)* elvei is relevánsak. Az állami felelősség azt rögzíti, hogy egy állam a neki tulajdonítható jogsértő kiberműveletekért felelőssé tehető, a kellő gondosság kötelezettsége pedig arra kötelezi, hogy területét ne engedje harmadik felek által jogellenes kibertámadások kiindulópontjaként használni. Ez a két elv teljes körű tárgyalása azonban túlmutat a tanulmány fókuszán, mivel a kiberműveletek esetében az állami felelősség megállapítása rendkívül összetett, több egymással szorosan összefüggő aspektus együttes vizsgálatát igénylő kérdéskör. Amint Spáčil (2024) is rámutat, a jogi felelősség megállapítása nem választható el sem a technikai attribúciótól, sem pedig a politikai attribúciótól, mivel ezek együtt határozzák meg, hogy egy kiberművelet államnak tulajdonítható-e a nemzetközi jog alapján. Ez a kérdéskör önálló, részletes elemzést igényel, ezért a tanulmány ezekre csak közvetetten, a jogértelmezési divergenciák kontextusában utal.[11]

A vizsgálat módszertani korlátját az jelenti, hogy az államok jogértelmezése nem minden esetben dokumentált teljeskörűen, a nyilatkozatok pedig gyakran politikai kontextusban születnek, ami befolyásolhatja az érvelés részletességét. Az állami álláspontok elemzése elsősorban a nyilvánosan elérhető dokumentumokra támaszkodik, amelyek nem feltétlenül tükrözik az adott állam teljes jogértelmezési gyakorlatát. Valamint, a kiberjog ezen a ponton továbbra is formálódik, így a vizsgálat a jelenleg rendelkezésre álló, sokszor nem egységes állami gyakorlatokból indulhat ki. A választott összehasonlító megközelítés emellett nem képes teljes mértékben megragadni az egyes államok értelmezése mögött húzódó politikai és doktrinális különbségeket sem. Mindez nem csökkenti az elemzés érvényességét, azonban jelzi, hogy a következtetéseket a rendelkezésre álló források korlátaival együtt szükséges értelmezni. Ennek ellenére a vizsgált országok példája lehetővé teszi a két jogi kultúra közötti különbségek pontosabb azonosítását.

Angolszász megközelítések: Egyesült Államok és Egyesült Királyság

Az Egyesült Királyság 2022. május 19-én közzétett főügyészi beszéde, a „Nemzetközi jog a jövő határterületein" keretében részletezte nemzetközi jogi értelmezését a kiberműveletekről, hangsúlyozva, hogy a fegyveres konfliktusban a nemzetközi humanitárius jog szabályai ugyanúgy alkalmazandók a kibertérre is. A CCDCOE Cyber Law Toolkit Az Egyesült Királyság nemzeti álláspontja (2022) oldala ezt a beszédet tekinti a hivatalos brit álláspont magjául, és strukturáltan rendszerezi annak főbb elemeit. Az Egyesült Királyság legutóbb, 2021 júniusában megerősítette saját álláspontját

[11] Spáčil 2024.

a kibertérben való szuverenitás esetében. Nevezetesen, hogy az államok tevékenységeire vonatkozó bármilyen tilalmat, legyen az a kibertérrel vagy más ügyekkel kapcsolatos, egyértelműen meg kell határozni a nemzetközi jogban. A szuverenitás általános fogalma önmagában nem nyújt elegendő vagy egyértelmű alapot egy konkrét szuverenitási szabály vagy a be nem avatkozáson túlmutató további tilalom kiterjesztéséhez a kibertevékenységekre vonatkozóan.

Az Egyesült Királyság álláspontja szerint a be nem avatkozás elve a nemzetközi jog egyik legfontosabb alapja, amely a szuverenitás védelmét és az államok közötti békés együttélést szolgálja. Ez az elv biztosítja a viszonyítási alapot a kibertérben tanúsított állami magatartások jogszerűségének megítéléséhez, valamint a megfelelő válaszlépések meghatározásához. A 2021-ben megerősített brit álláspont szerint azonban a szuverenitás önmagában nem elegendő jogalap új, a kibertérre vonatkozó tilalmak megfogalmazására, csak az tekinthető jogsértésnek, ami világosan tiltott a nemzetközi jogban. A gyakorlatban tehát a hangsúly azon van, történt-e tényleges jogsértés – a be nem avatkozás szabálya pedig különösen fontos azokban az esetekben, amikor az államok ellenséges, de nem fegyveres küszöböt elérő kibertevékenységet folytatnak. A jogsértés megállapításához a cselekménynek kényszerítő jellegűnek kell lennie.

Az ellenintézkedések terén az Egyesült Királyság álláspontja szerint egy állam egy korábbi jogellenes cselekményre úgy is reagálhat, hogy olyasmit tesz, ami egyébként jogellenes lenne, ha ez a jogsértő magatartás megszüntetését és a jóvátétel elérését szolgálja. Az Egyesült Királyság egyértelművé tette, hogy ilyen ellenintézkedések alkalmazhatók más állam jogellenes kiberműveleteire is, és nem szükséges, hogy ugyanolyan jellegűek legyenek. A válasz nem feltétlenül kibereszköz, lehet más típusú lépés is, amennyiben az alkalmas a jogellenes kibertevékenység leállítására.[12]

Ezért az álláspont is jól illeszkedik a *formálisan elfogadom, de rugalmasan értelmezem* kategóriához, hiszen támogatja a humanitárius jog alkalmazását, de visszafogottan kezeli a szuverenitás elvét, a be nem avatkozás/kényszerítő jelleg tesztet választja békeidőmércének, és esetalapon vizsgálja az ellenintézkedéseket.

Az Egyesült Államok 2021-ben, az ENSZ Közgyűlés elé benyújtott önkéntes nemzeti hozzájárulásában (A/76/136) részletesen ismertette, miként értelmezi a nemzetközi jogot a kibertérben folytatott állami tevékenységekre vonatkozóan. A dokumentum leszögezi, hogy a meglévő nemzetközi jog, beleértve az ENSZ Alapokmányt, a nemzetközi humanitárius jogot és a szokásjogot is, teljes mértékben alkalmazandónak tartja az államok kiberműveleteire. Kiemelik, hogy a szuverenitás elve a kibertérben is érvényesül. Az államoknak tiszteletben kell tartaniuk egymás területi joghatóságát, ugyanakkor az Egyesült Államok hangsúlyozza, hogy a szuverenitás gyakorlása nem korlátlan, és összhangban kell állnia a nemzetközi jog, különösen az emberi jogok szabályaival. Az Egyesült Államok elismeri azt is, hogy bizonyos körülmények között egy másik állam területén végrehajtott, nem konszenzuson alapuló kiberművelet megsértheti a nemzetközi jogot, ugyanakkor önmagában az, hogy egy kiberművelet egy másik állam területén található rendszereket érint, nem tekinthető automatikusan jogsértőnek, különösen akkor, ha annak hatása elhanyagolható vagy technikai jellegű. Ezzel az állásponttal az Egyesült Államok a szuverenitás rugalmas, kontextusfüggő értelmezését követi.

[12] International Cyber Law 2025a.

A be nem avatkozás elve az Egyesült Államok szerint továbbra is alapvető a kibertérben is, a nemzetközi jog tiltja az olyan kényszerítő beavatkozásokat, amelyek más államok belügyeit, például politikai, gazdasági vagy kulturális döntéseit befolyásolják. Ennek értelmében egy másik ország választási rendszerébe való beavatkozás vagy az egészségügyi infrastruktúrájának kiberzavara egyértelműen sérti a be nem avatkozás tilalmát. Az Egyesült Államok azonban a szabály szűk értelmezését vallja, nem minden, más államot érintő kiberművelet minősül jogsértésnek, csak azok, amelyek ténylegesen kényszerítő hatásúak és a szuverén döntéshozatalba avatkoznak be.

Az erőalkalmazás tilalmának elve alapján az Egyesült Államok elismeri, hogy bizonyos kibertevékenységek elérhetik az erőszak alkalmazásának szintjét, ha hatásuk megfelelne egy fegyveres támadás következményeinek. Ilyen esetekben az ENSZ Alapokmányának 51. cikke értelmében az államnak joga van az önvédelemhez, függetlenül attól, hogy a támadó állami vagy nem állami szereplő. Az önvédelmi célú erőalkalmazásnak azonban szükségesnek és arányosnak kell lennie, és kizárólag a tényleges vagy közvetlen fegyveres támadás elhárítására irányulhat. Az Egyesült Államok hangsúlyozza, hogy az önvédelem formája nem kötött, a kiber- és fizikai eszközök egyaránt alkalmazhatók, attól függően, melyik alkalmasabb a fenyegetés megszüntetésére. Mielőtt egy állam az erőszak eszközéhez nyúlna, köteles mérlegelni, hogy passzív vagy alacsonyabb szintű aktív kibervédelem elegendő lenne-e a támadás elhárítására.

Az Egyesült Államok értelmezése szerint az ellenintézkedések fontos jogi eszközt jelentenek azokban az esetekben, amikor egy államot nemzetközi jogellenes kiberművelet ér, amely nem minősül fegyveres támadásnak. Ilyenkor az állam erőszakmentes ellenintézkedéseket alkalmazhat, amelyek célja a jogsértés megszüntetése és a felelős állam jogkövető magatartásának helyreállítása. Az ilyen intézkedéseknek meg kell felelniük a szükségesség és arányosság követelményeinek, és kizárólag a jogsértő állam ellen irányulhatnak. Az Egyesült Államok álláspontja szerint az ellenintézkedések nem feltétlenül kell hogy kibereszközök legyenek, lehetnek nem kiberjellegű válaszlépések is, amennyiben azok hatékonyan szolgálják a jogellenes magatartás megszüntetését. Mielőtt ilyen intézkedéseket hozna, az érintett államnak lehetőséget kell biztosítania a jogsértő félnek a cselekmény abbahagyására, kivéve, ha a helyzet sürgős fellépést követel meg.[13]

Összevetve az angolszász megközelítéseket, megfigyelhető, hogy mindkét állam a jog rugalmasságát és az operatív mozgásteret tartja elsődlegesnek, ami a biztonságpolitikai érdekek érvényesítését segíti.

Kontinentális megközelítések: Hollandia és Franciaország

Hollandia 2019-ben tette közzé a Külügyminisztérium *Letter to the Parliament on the International Legal Order in Cyberspace* című dokumentumát, amelyben részletesen kifejti álláspontját a kiberműveletek nemzetközi jogi megítéléséről. A dokumentum

[13] International Cyber Law 2025b.

kimondja, hogy a nemzetközi jog, beleértve az Egyesült Nemzetek Alapokmányát, alkalmazandó az államok információs és kommunikációs technológiák használatára is, és hogy a meglévő nemzetközi jog képezi az államok kibertérben tanúsított magatartásának keretét. Hollandia szerint azok a kiberműveletek, amelyek megsértik a nemzetközi kötelezettségeket és egy államnak tulajdoníthatók, nemzetközi jogsértésnek minősülnek.

A holland álláspont a szuverenitást a nemzetközi jog egyik alapvető szabályának tekinti, amelynek megsértését önmagában nemzetközi jogsértésnek minősíti. A kormány egyértelműen kijelenti, hogy a szuverenitás elve a nemzetközi jog szabálya, amelynek megsértése nemzetközi jogsértést jelent. Ennek megfelelően Hollandia nemcsak a közvetlen beavatkozást, hanem bármely, más állam szuverenitását sértő kiberműveletet is jogellenesnek tekint.

A holland kormány az erőalkalmazás tilalmát is kiterjeszti a kiberműveletekre, és rögzíti, hogy egy kiberművelet akkor minősül erőalkalmazásnak, ha annak mértéke és hatásai összehasonlíthatók a hagyományos katonai műveletekével, ugyanakkor a dokumentum hangsúlyozza azt is, hogy a nemzetközi humanitárius jog szabályai és elvei minden hadviselési eszközre és módszerre vonatkoznak, beleértve a kiberműveleteket is.[14]

A holland álláspont ezzel egy szigorúbban értelmezett megközelítést alkalmaz, és a kiberműveletek esetében szinte teljes egészében alkalmazhatónak tekinti a humanitárius jogot, mindenesetre kevesebb rugalmasságot enged, mint a korábban említett országok.

Franciaország álláspontja a kiberműveletek jogi kezeléséről világosan hangsúlyozza a szuverenitás elsődlegességét és annak következményeit. A tagállami normák és elvek kiterjednek az IKT-használatra és az ország területén található információs rendszerekre, és Franciaország saját területén ezeket a rendszereket szuverén joghatósága alatt gyakorolja. Ennek megfelelően bármely olyan kibertámadás, vagy a területen digitális eszközökkel előidézett hatás, amelyet állami szervek, kormányzati hatáskörrel rendelkező személyek, vagy állami utasításra, irányítás alatt eljáró szereplők idéznek elő, a szuverenitás megsértésének minősül. Ugyanakkor Franciaország nem tekint automatikusan minden távoli, technikai jellegű kiberműveletet jogsértésnek, a jogsértés fennállását a hatás és a behatás mértéke alapján, eseti alapon kell megítélni.

A be nem avatkozás elve megsértésének világos példája a választási rendszerek manipulációja vagy a kritikus egészségügyi infrastruktúra kényszerítő befolyásolása. Az ilyen kényszerítő beavatkozások tipikusan ellentétesek a nemzetközi joggal. Franciaország hangsúlyozza, hogy a szuverenitás legsúlyosabb megsértései, különösen, ha a területi integritást vagy politikai függetlenséget érintik, elérhetik az erőszakkal való fenyegetés vagy az erőszak alkalmazása tilalmának küszöbét. A küszöb átlépését nem az alkalmazott eszközökben, hanem a kiberművelet hatásaiban kell mérni, amely során lényeges tényezők lehetnek a művelet eredményei, a célszemély jellege, a behatolás mértéke, valamint a művelet eredete és felbujtó jellege. Franciaország tehát nem zárja ki, hogy fizikai hatás nélkül is fennállhat az erőszak alkalmazása, ha a következményekkel egyenértékű hatások keletkeznek.

[14] International Cyber Law 2025c.

Az önvédelem joga az ENSZ Alapokmányának 51. cikke alapján érvényesül, ha egy kibertámadás mértéke és súlyossága összehasonlítható a hagyományos fegyveres támadás következményeivel, Franciaország kész önvédelemmel reagálni. Ez kiterjedhet digitális és kinetikus eszközökre is, mindig a szükségesség és arányosság elvei szerint. Franciaország elismeri, hogy nem minden erőszak alkalmazása minősül automatikusan fegyveres támadásnak, a súlyosság, visszafordíthatóság és kumulatív hatások mérlegelése a döntő.

Az ellenintézkedések tekintetében Franciaország elfogadja, hogy áldozatként jogszerűen alkalmazhat békés célú ellenintézkedéseket a jogellenes kiberműveletek megszüntetése és a jóvátétel biztosítása érdekében, ezek kizárólag a jogsértő állam ellen irányulhatnak, meg kell felelniük a nemzetközi jog követelményeinek és ideiglenes jellegűeknek kell lenniük. Tehát amint a jogsértés megszűnik, az intézkedéseket fel kell függeszteni. Kollektív ellenintézkedések alkalmazását Franciaország a saját joggyakorlatában viszont kizártnak tartja. Előzetes felszólítás általában szükséges, kivéve a sürgős eseteket, amikor is sürgős ellenintézkedések lehetősége különösen a kibertérre jellemző nyomon követési nehézségek miatt kulcsfontosságú.

Végül Franciaország felelősséget ró azokra az államokra is, amelyek nem állami szereplők tevékenységét instruálják vagy ellenőrzik, egyben támogatja a magánszektor offenzív tevékenységének szigorú szabályozását, mivel az ilyen szereplők alkalmazása rendszerszintű instabilitást okozhat. Minden válaszlépést, legyen az diplomáciai vagy katonai, Franciaország a nemzetközi jog keretein belül mérlegel, és szükség esetén jelenteni kíván a nemzetközi szervezetek felé, biztosítva, hogy az egyoldalú fellépés ideiglenes és a kollektív intézkedésekkel helyettesíthető maradjon.[15]

Az ENSZ égisze alatt működő államok számára politikailag és jogilag is vállalhatatlan lett volna, ha nem ismerik el a humanitárius jog alkalmazhatóságát a kiberműveletek esetében. Bár e konszenzus ma már alapvetésnek számít, az egyes államok különböző szempontok alapján, eltérő rugalmassággal értelmezik mind a tartalmát, mind a gyakorlati érvényesülését. Az angolszász országok – mint az Egyesült Államok és az Egyesült Királyság – a rugalmas megközelítést képviselik, míg a kontinentális európai államok – mint Franciaország és Hollandia – a kötöttebb, normatív értelmezés hívei.

Az Egyesült Államok és az Egyesült Királyság értelmezésében a szuverenitás nem önálló tiltó norma, a jogsértés csak akkor áll fenn, ha a kiberművelet kényszerítő jellegű, tehát beavatkozik az állam szuverén döntéshozatalába. Ezzel szemben Franciaország és Hollandia a szuverenitást a nemzetközi jog alapvető szabályának tekintik, amelynek bármely jellegű megsértése önmagában is jogsértést jelent. Míg az angolszász államok a be nem avatkozás elvét és az erőalkalmazás tilalmát hatásalapú módon értelmezik, addig a kontinentális országok inkább a formális megfelelésre és a humanitárius jog kiterjesztett alkalmazására törekednek.

Az ellenintézkedések és önvédelem terén is hasonló különbség mutatkozik. Az USA és az Egyesült Királyság nem tartja szükségesnek az előzetes bejelentést, ha az arányosság és szükségesség elve teljesül, és nyitva hagyják a kollektív ellenintézkedések lehetőségét is. Franciaország és Hollandia ezzel szemben szigorúbb

[15] International Cyber Law 2025d.

értelmezést követnek, az állami felelősség és a kellő körültekintés kötelező alkalmazását hangsúlyozva. Az erőalkalmazás és az önvédelem értelmezésében mindkét csoport az ENSZ Alapokmány 2. cikk (4) és 51. cikk szerinti keretet fogadja el, de míg a rugalmas értelmezést követő államok az összehasonlítható hatás alapján ítélik meg a kiberműveleteket, a normatív megközelítést alkalmazók minden fegyveres hatásúnak minősülő beavatkozást erőalkalmazásnak tekintenek.

1. táblázat: A vizsgált államok (USA, Egyesült Királyság, Franciaország, Hollandia) jogértelmezési megközelítéseinek összegzése a kiberműveletek nemzetközi jogi szabályozásában

	Angolszász jogi kultúra		**Kontinentális jogi kultúra**	
Szempont	Egyesült Államok	Egyesült Királyság	Franciaország	Hollandia
Szuverenitás	A szuverenitás nem önálló tiltó norma, csak a ténylegesen kényszerítő beavatkozás minősül jogsértésnek	Elismeri a szuverenitás elvét, de a beavatkozás csak akkor tiltott, ha kényszerítő hatású	A szuverenitás megsértését önmagában is nemzetközi jogsértésnek tekinti	A szuverenitás megsértése önálló jogsértés, még funkcionális beavatkozás esetén is
Be nem avatkozás elve	Csak a kényszerítő beavatkozás tiltott (pl. választási manipuláció, gazdasági nyomás)	Szűken értelmezett elv, csak a tényleges kényszert kifejtő beavatkozás jogsértő	Minden, politikai vagy kritikus infrastruktúrát érintő, befolyásolás jogsértésnek minősül	Minden más állam belügyeibe történő beavatkozás jogellenesnek tekintendő
Erőalkalmazás tilalma	A kiberművelet akkor minősül erőalkalmazásnak, ha hatása egy fegyveres támadás következményeivel egyenértékű	Hatásalapú megközelítés: a tényleges eredmény alapján ítélhető meg, átlépi-e a küszöböt	Fizikai hatás nélkül is fennállhat az erőalkalmazás, ha a hatás egyenértékű a fizikai támadással	A kiberműveletek funkcionális hatásai is elérhetik az erőalkalmazás szintjét
Önvédelem	Az ENSZ Alapokmány 51. cikke alapján csak fegyveres támadás szintjén, az arányosság és szükségesség elve érvényes	Az önvédelem joga elismert, akár nem kiberjellegű válaszlépéssel is	Az önvédelem joga kiterjed a súlyos kibertámadásokra; a válasz arányos és szükséges kell legyen	A humanitárius jogot az önvédelem esetén is teljeskörűen alkalmazza
Ellenintézkedések	Megengedettek erőszakmentes ellenintézkedések előzetes bejelentés nélkül is, ha arányosak	Szükséges és arányos ellenintézkedések engedélyezettek, nem feltétlenül kiberjellegűek	Csak ideiglenes, jogsértő állam ellen irányuló ellenintézkedések; előzetes értesítés jellemzően szükséges	Csak békés, arányos ellenintézkedéseket fogad el

Forrás: a szerző szerkesztése

Összességében tehát bár a humanitárius jog alkalmazhatóságát minden vizsgált állam elfogadja, az értelmezési keretek között a politikai és jogi kultúrájuknak megfelelő eltérés figyelhető meg.

Következtetések

A kiberműveletek nemzetközi jogi megítélése mára a nemzetközi jog egyik legösszetettebb kérdésévé vált. Bár a szakirodalomban továbbra is megjelennek olyan vélemények, amelyek szerint a nemzetközi jog – különösen a humanitárius jog – nem, vagy csak korlátozottan alkalmazható a kibertérre, az államok hivatalos nyilatkozataiban ez a nézet ennyire nyíltan nem jelenik meg. Az ENSZ égisze alatt működő országok számára politikailag és jogilag is vállalhatatlan lenne a humanitárius jog elutasítása, ezért az alkalmazhatóság elvi elfogadása minden állam részéről egységesen megfigyelhető. A különbségek nem az elfogadás tényében, hanem az értelmezés és a gyakorlati alkalmazás módjában mutatkoznak meg. A humanitárius jog alkalmazhatóságának kérdésköre a kiberműveletek esetében éppen ebből kifolyólag kifejezetten összetett. A vizsgált államok egyhangúlag elismerik, hogy a nemzetközi jog, ezen belül a humanitárius jog alapelvei a kibertérben is alkalmazandók, mindazonáltal az eltérések nem az elvi elfogadásban, hanem az alkalmazás gyakorlati terjedelmében és a jogértelmezés módjában jelennek meg. Míg a humanitárius jog hagyományosan fizikai hadviselési kontextusban jött létre, a kiberműveletek sajátos, nem fizikai természetük miatt új kihívásokat támasztanak már csak a fogalmak alkalmazása során is. A tanulmány ennek okán megállapítja, hogy a humanitárius jog alapelvei elviekben alkalmazhatók, de a gyakorlati megvalósulása országonként eltérő rugalmassággal történik.

A vizsgált államok közül az Egyesült Államok és az Egyesült Királyság rugalmasabb, gyakorlatorientált megközelítést képviselnek, míg Franciaország és Hollandia a nemzetközi jog kötöttebb, szabályalapú értelmezését követik. A szuverenitás megsértését önmagában is jogsértésnek tekintik, a be nem avatkozás elvét szigorúan alkalmazzák, és az ellenintézkedéseket csak arányos, szükséges és békés módon tartják elfogadhatónak. Az erőalkalmazás és az önvédelem kérdésében is inkább a hagyományos, ENSZ Alapokmányon alapuló felfogást követik. Az Egyesült Államok és az Egyesült Királyság az angolszász, precedensorientált jogi kultúra képviselőiként rugalmas, hatásalapú értelmezést alkalmaznak, ezzel szemben Franciaország és Hollandia a kontinentális jogrendszert követve normatív, szabályalapú megközelítést képviselnek. Az angolszász országok a szuverenitást nem tekintik önálló tiltó normának, és csak a kényszerítő hatású beavatkozásokat tartják jogsértőnek. Ez a különbség a formális elfogadás és a gyakorlati rugalmasság közötti eltérő viszonyban ragadható meg mint a két jogi megközelítés közötti legnagyobb különbség.

Az értelmezési nehézséget tovább növelik az olyan nem nyugati országok, mint például Kína vagy Irán, amelyek a szuverenitás és a kiberműveletek jogi megítélése kapcsán ettől jelentősen eltérő, a kibertér feletti szélesebb állami kontrollt hangsúlyozó megközelítést képviselnek. Ezen megközelítések részletes vizsgálata túlmutat a jelen tanulmány fókuszán, mindazonáltal jelzi, hogy a kiberműveletek nemzetközi jogi értelmezését tovább nehezíti és új aspektusból vizsgálandóvá teszi a nyugati és

nem nyugati országok értelemzési kereteinek összehasonlítása is. A tanulmányban választott minta ezért elsősorban nem a teljes államgyakorlat reprezentációjára, hanem a jogi kultúrák közötti különbségek illusztrálására szolgál.

A vizsgált országok elemzése azt mutatja, hogy a kiberműveletek jogi keretének fejlődése nem a nemzetközi jog megtagadását jelenti, hanem annak alkalmazkodását a kibertér új kihívásaihoz. A közös alapot a nemzetközi jog és a humanitárius jog elvi elfogadása jelenti, ugyanakkor az államok nemzeti jogi kultúrája, biztonságpolitikai helyzete és stratégiai érdekei alapján különböző értelmezési hangsúlyokat alkalmaznak. A jelenlegi nemzetközi helyzetet tehát egyfajta értelmezési pluralizmus jellemzi, amelyben a szabályok alapjai közösek, de az alkalmazásuk rugalmas vagy éppen kötöttebb módon történik. Ez a sokszínűség ugyan megnehezíti az egységes nemzetközi normák kialakulását, de egyben azt is jelzi, hogy az államok – eltérő módokon ugyan, de – igyekeznek a nemzetközi jog keretein belül kezelni a kiberműveletek jelentette kihívásokat.

Felhasznált irodalom

1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról, II. pont.

CCDCOE (2025): *NATO Recognises Cyberspace as a 'Domain of Operations' at Warsaw Summit,* CCDCOE. Online: https://ccdcoe.org/incyder-articles/nato-recognises-cyberspace-as-a-domain-of-operations-at-warsaw-summit/

D'Aspremont, Jean (2016): Cyber Operations and International Law: an Interventionist Legal Thought. *Journal of Conflict and Security Law,* 21(3), 575–593. Online: https://doi.org/10.1093/jcsl/krw022

Efrony, Dan (2021): The UN Cyber Groups, GGE and OEWG – A Consensus is Optimal, But Time is of the Essence. *Just Security,* 2021. július 16. Online: https://www.justsecurity.org/77480/the-un-cyber-groups-gge-and-oewg-a-consensus-is-optimal-but-time-is-of-the-essence/

International Cyber Law: Interactive Toolkit Contributors (2025a): *National Position of the United Kingdom (2022).* Online: https://cyberlaw.ccdcoe.org/wiki/National_position_of_the_United_Kingdom_(2022)?oldid=4489

International Cyber Law: Interactive Toolkit Contributors (2025b): *National Position of the United States of America (2021).* Online: https://cyberlaw.ccdcoe.org/wiki/National_position_of_the_United_States_of_America_(2021)

International Cyber Law: Interactive Toolkit Contributors (2025c): *National Position of the Netherlands (2019).* Online: https://cyberlaw.ccdcoe.org/wiki/National_position_of_the_Netherlands_(2019)?oldid=4483

International Cyber Law: Interactive Toolkit Contributors (2025d): *National Position of France (2019).* Online: https://cyberlaw.ccdcoe.org/wiki/National_position_of_France_(2019)

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

Mann, Sharona (2020): Legal Challenges in the Realm of Cyber Warfare. *Journal of International Law and Politics Online Forum,* (Winter–Spring), 9–23. Online: https://

www.nyujilp.org/wp-content/uploads/2020/03/Mann-Note_Final-Draft_EIC-Approved.pdf

McDonald, Ellie (2023): Shaky Consensus at the OEWG on ICTs: Where Next for UN Discussions on State Behaviour in Cyberspace. *CircleID,* 2023. augusztus 16. Online: https://circleid.com/posts/20230816-shaky-consensus-at-the-oewg-on-icts-where-next-for-un-discussions-on-state-behaviour-in-cyberspace?

NATO, Wales Summit Declaration, Paragraph 72. Online: https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2014/09/05/wales-summit-declaration

Pomson, Ori (2023): Methodology of Identifying Customary International Law Applicable to Cyber Activities. *Leiden Journal of International Law,* 36(4), 1023–1047. Online: https://doi.org/10.1017/S0922156523000390

Spáčil, Jakub (2024): Attribution of Cyber Operations: Technical, Legal and Political Perspectives. *International and Comparative Law Review,* 24(2), 150–168. Online: https://journals.upol.cz/ICLR/article/view/176/143

Tiirmaa-Klaar, Heli (2021): *The Evolution of the UN Group of Governmental Experts on Cyber Issues: From a Marginal Group to a Major International Security Norm-Setting Body.* The Hague Centre for Strategic Studies & Global Commission on the Stability of Cyberspace. Online: https://hcss.nl/wp-content/uploads/2021/12/Klaar.pdf

Tsagourias, Nicholas – Farrell, Michael (2020): Cyber Attribution: Technical and Legal Approaches and Challenges. *European Journal of International Law,* 31(3), 941–967. Online: https://doi.org/10.1093/ejil/chaa057

United Nations (2025): *Developments in the Field of Information and Telecommunications in the Context of International Security.* United Nations Office for Disarmament Affairs. Online: https://disarmament.unoda.org/en/our-work/emerging-challenges/developments-field-information-and-telecommunications-context