KISS MÁTYÁS*

KIBERMŰVELETEK A BEAVATKOZÁS TILALMA MINT NEMZETKÖZI JOGI ALAPELV TÜKRÉBEN**

https://doi.org/10.51783/ajt.2023.4.05

Az elmúlt években az ellenséges célú, államközi kiberműveletek száma exponenciálisan nőtt. Felmerül a kérdés, hogy a nemzetközi jog által kidolgozott kereteken belül az államok miként reagálnak az őket ért kiberműveletekre. Ha egy kiberművelet nem éri el az erőszak alkalmazásának szintjét, elsősorban az vizsgálandó, hogy a művelet sérti-e például a beavatkozás tilalmát. Elmondható, hogy napjainkig az államok még egyetlen esetben sem folyamodtak ahhoz, hogy erőszak alkalmazásának vagy fegyveres támadásnak minősítsenek egy kiberműveletet, ez is mutatja tehát azt, hogy nagy jelentőségű e norma vizsgálata. A beavatkozás tilalma a nemzetközi jog egyik kulcsnormája. A tilalom az ENSZ Alapokmányában megjelenő erőszaktilalmi normából és a szuverén egyenlőség elvéből vezethető le, megtalálható az Alapokmány kvázi-autentikus értelmezéseiben is. Fontos megemlíteni a Nicaragua-ügyet, amely elméleti és gyakorlati szinten is foglalkozott a kérdéssel, továbbá azt, hogy az elmúlt időszakban jelentősen megnőtt az állami nyilatkozatok, állásfoglalások száma.

A Nicaragua-ügy ítéletében körvonalazódtak azok a feltételek, amelyek vizsgálatával eldönthető, hogy az adott művelet sérti-e a beavatkozás tilalmát. A szakirodalom ezeket a feltételeket elfogadja a kiberműveletekre vonatkozóan is. Az állami nyilatkozatokból pedig kimutatható, hogy az állami gyakorlat nemzetközi jogi szakirodalommal azonos álláspontot képvisel.

Amennyiben a sértett államot ért kiberművelet nem éri el a fegyveres támadás szintjét, nem lesz lehetősége az önvédelem jogának alkalmazására. Az államok azonban ebben az esetben sem maradnak eszköztelenek. Egyfelől ellenintézkedést foganatosíthatnak, másfelől szükséghelyzetre hivatkozhatnak. A szakirodalom mellett az állami gyakorlat is egységes a kérdésben.

1. BEVEZETÉS

A kibertér olyan instabil környezetet jelent, amely gyors változásokat mutat az azt használó szereplők természetében, az alkalmazott technológiákban és az ezáltal elő-

* PhD-hallgató, PTE ÁJK, 7622 Pécs, 48-as tér 1. E-mail: *kiss.matyas@ajk.pte.hu*.

** Az Innovációs és Technológiai Minisztérium ÚNKP-22-2-I kódszámú Új Nemzeti Kiválóság Programjának a nemzeti kutatási, fejlesztési és innovációs alapból finanszírozott szakmai támogatással készült.

segített személyközi, kereskedelmi és kormányzati interakciókban.[1] Az elmúlt években drasztikusan megnőtt az ellenséges célú, államközi kiberműveletek száma. Több nemzetközi szervezet statisztikái is azt bizonyítják, hogy míg a 2010-es évek közepéig évente csupán néhány ilyen akció történt, addig a 2020-as években már százas nagyságrendben volt mérhető az ilyen műveletek száma.[2]

A nemzetközi jog egyik legfontosabb, sarokkő jellegű normája az ENSZ Alapokmányban megtalálható erőszaktilalmi norma: *„[a] Szervezet összes tagjának nemzetközi érintkezései során más Állam területi épsége, vagy politikai függetlensége ellen irányuló vagy az Egyesült Nemzetek céljaival össze nem férő bármely más módon megnyilvánuló erőszakkal való fenyegetés vagy erőszak alkalmazásától tartózkodniuk kell."*[3] Fontos megemlíteni, hogy jelenleg nincs olyan nemzetközi szerződés, amely kifejezetten a kibertér és az erőszak alkalmazásának lehetőségével foglalkozna, ezért minden további ilyen jellegű vizsgálódás középpontjában az Alapokmány által éltre hívott, generális erőszaktilalmi norma áll.[4] Részben emiatt kiemelt jelentőségűek az egyes magánkodifikációs törekvések, különösen az úgynevezett Tallinni Kézikönyv (teljes nevén: *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*[5]), amely jelenleg második kiadását éli. Megjegyzendő, hogy a harmadik kiadás is készülőben van. A szerkesztők szerint a Kézikönyv jellege változatlan marad, ugyanakkor a meglévő fejezetek felülvizsgálatán túl új részek is bekerülnek a dokumentumba, például a különböző nemzetközi szervezetek tevékenységei és nyilatkozatai.[6]

A szakirodalmi álláspontokat és az állami gyakorlatot összevetve az mondható el, hogy a kiberművelet akkor éri el az erőszak alkalmazásának szintjét, amikor annak mértéke és hatásai összehasonlíthatók lesznek egy, nem a kibertérben történő erőszak alkalmazásához.[7] Elképzelhető tehát olyan kiberművelet, amely a kinetikus térben végrehajtott katonai művelethez hasonlóan elérheti az erőszak alkalmazásának szintjét. Sőt, a kiberművelettel szemben önvédelmi cselekmény is foganatosítható – szintén a fizikai térben történő események hasonlóan – akkor, ha az eléri a fegyveres támadás szintjét, másképpen az *„[a]z állam, amely olyan kiberművelet célpontja, amely eléri a fegyveres támadás szintjét, gyakorolhatja az önvédelem jogát."*[8]

[1] Yuval Shany – Tal Mimran: „International Regulation of Cyber Operations" *Hebrew University of Jerusalom Legal Studies Research Paper Series* No. 22.2, 1., *https://dx.doi.org/10.2139/ssrn.3961263.*

[2] A Council on Foreign Relations (CFR) adatbázisa ezen a linken érhető el: *www.cfr.org/cyber-operations/.* A Center for Strategic and International Studies (CSIS) adatbázisa pedig ezen a linken érhető el: *https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.*

[3] ENSZ Alapokmány, 2. cikk (4) bek. Kihirdette: 1956. évi I. törvény az Egyesült Nemzetek Alapokmányának törvénybe iktatásáról (a továbbiakban: ENSZ Alapokmány).

[4] Francois Delerue: *Cyber Operations and International Law* (Cambridge: Cambridge University Press 2020) 283.

[5] Michael N. Schmitt*: Tallinn Manual 2.0. on the International Law Applicable to Cyber Operations* (New York: Cambridge University Press 2017) (a továbbiakban: Tallinn Manual 2.0.), *https:/doi.org/10.1017/9781316822524.*

[6] The Tallinn Manual. CCDCOE, *https://ccdcoe.org/research/tallinn-manual/.*

[7] Tallinn Manual 2.0. 69. szabály 330.

[8] Tallinn Manual 2.0. 71. szabály 339.

Mindezen szabályok ellenére fontos leszögezni, hogy jelen sorok írásáig az államok még egyetlen alkalommal sem minősítettek egy kiberműveletet sem erőszak alkalmazásnak, sem pedig fegyveres támadásnak. Továbbá a legtöbb kiberművelet olyan alacsony intenzitású, hogy nem éri el az erőszak alkalmazásának szintjét sem. Ugyanakkor az ilyen intenzitású műveletek is lehetnek nemzetközi jogi szempontból jogszerűtlenek. Abban az esetben, ha egy kiberművelet nem éri el az erőszak alkalmazásának szintjét, elsősorban az lesz vizsgálandó, sérti-e például a beavatkozás tilalmát.

A kiberműveletek kapcsán kiemelkedő fontosságú a betudhatóság témaköre is, ugyanakkor ez a kérdés meglehetősen problematikus. A betudhatósági probléma egy része az internet szerkezeti felépítéséből és a hálózatok közötti adatátviteli folyamatokból adódik, ami kiváló feltételeket kínál az anonimitás megőrzéséhez.[9] Fontos megemlíteni azt is, hogy bizonyos esetekben a más állam ellen kibertámadást végrehajtó személyek egy állam fegyveres erőihez is tartozhatnak, mivel manapság egyre több állam rendelkezik rendszeresen támadásokat végrehajtó kiberegységekkel úgy, mint Kína vagy az Egyesült Államok. Egyes államok pedig – például az Egyesült Királyság – magánszervezeteket bíztak meg kiberbiztonsági feladatoknak az állam nevében történő ellátásával.[10] Az elkövetők ugyanakkor lehetnek olyan magánszemélyek vagy vállalatok, amelyeket az államok béreltek fel, hogy kibertámadásokat hajtsanak végre.[11] Utóbbi esetben véleményem szerint a betudás még nehezebbé válik. További nehézség, hogy a Nemzetközi Bíróság eltérő kontextusban eltérő betudási normákat alkalmaz, így volt ez a Nicaragua-ügyben és a Kongó v. Uganda-ügyben is.[12]

A téma hazai szakirodalma kapcsán megjegyezném, hogy átfogó mű még nem születetett a kiberműveletek és a nemzetközi jog viszonya kapcsán. Kiemelném ugyanakkor, hogy egyes szerzők kutatásaik során érintették a témát – például Kis Kelemen Bence[13] vagy Lattmann Tamás[14] –, ezek a kutatások alapvetően a humanitárius nemzetközi jog szemszögéből vizsgálják a kibertevékenységeket.

Tanulmányomban arra a kérdésre keresem a választ, milyen kapcsolatban állhat egymással a beavatkozás tilalma mint nemzetközi jogi alapelv és az ellenséges célú kiberműveletek (II. rész), továbbá megvizsgálom azt is, hogy milyen eszközök áll-

[9] Delbert Tran: „The Law of Attribution: Rules for Attribution the Source of a Cyber-Attack" *Yale Journal of Law and Technology* 2018/1. 387.

[10] Henning Lahmann: *Unilateral Remedies to Cyber Operations* (Cambridge: Cambridge University Press 2020) 68., *https://doi.org/10.1017/9781108807050.*

[11] Marco Roscini: „World Wide Warfare – Jus Ad Bellum and the Use of Cyber Force" *Max Planck Yearbook of United Nations Law* 2010/1. 98., *https://doi.org/10.1163/18757413-90000050.*

[12] Kajtár Gábor: *Betudás a nemzetközi jogban. A másodlagos normák szerepe a beruházásvédelemtől a humanitárius jogig* (Budapest: Orac Kiadó 2022) 27.

[13] Kis Kelemen Bence: „Személyes adatok védelme fegyveres konfliktusokban" *Jogtudományi Közlöny* 2022/10. 395–402.

[14] Lattmann Tamás: „Kiber-kombattáns" – a harcos jogállás új formája a kiberhadviselésben?" in Kajtár Gábor – Sonnevend Pál (szerk.): *A nemzetközi jog, az uniós jog és a nemzetközi kapcsoaltok szerepe a 21. században: tanulmányok Valki László tiszteletére* (Budapest: ELTE Eötvös Kiadó 2021) 357–369.

nak az államok rendelkezésére, amennyiben velük szemben egy kiberművelet sérti a beavatkozás tilalmát (III. rész), megvizsgálom továbbá az állami gyakorlatot is (IV. rész), felvillantva néhány, a téma tárgyalása kapcsán releváns példát a közelmúltból (V. rész), végezetül pedig levonom a konklúziót.

2. A BEAVATKOZÁS TILALMA MINT NEMZETKÖZI JOGI ALAPELV ÉS A KIBERMŰVELETEK KAPCSOLATA

A nemzetközi jog más elveiből, úgy mint az erőszak tilalmának elvéből és a szuverén egyenlőség elvéből deriválható a non-intervenció általános elve.[15] A beavatkozás tilalmával behatóbban már Emer de Vattel svájci nemzetközi jogász is foglalkozott a 18. században a *Law of the Nations* című munkájában.[16] Az 1960-as és 1980-as években a különböző nemzetközi fórumok – különösen az ENSZ Közgyűlés – keretein belül számos alkalommal előtérbe került a beavatkozás tilalmával kapcsolatos párbeszéd; sor került továbbá különböző határozatok elfogadására is.[17] Ezek közül a két legrelevánsabb az 1965. évi az államok belügyeleibe való beavatkozás elfogadhatatlanságáról, valamint függetlenségük és szuverenitásuk védelméről szóló 2131. (XX) számú közgyűlési határozat,[18] továbbá az 1970-ben elfogadott, az államok közötti baráti kapcsolatokra és együttműködésre vonatkozó nemzetközi jog elveiről szóló nyilatkozat.[19] Ezen felül született határozat az államok belügyeibe való beavatkozásról 1976-ban[20] és 1981-ben is.[21]

1975-ben valamennyi európai állam – Albániát kivéve –, továbbá az Egyesült Államok és Kanada elfogadta az úgynevezett Helsinki Záróokmányt (*The Helsinki Final Act*), amelyet az Európai Biztonsági és Együttműködési Konferencia (mai nevén: Európai Biztonsági és Együttműködési Szervezet) hívott életre.[22] A dokumentum jelentőségét az adja, hogy kulcsfontosságú eleme volt a hidegháborús hangulat enyhítésének. Azzal a céllal jött létre, hogy erősítse az egymással ellentétes ideológiájú államok közötti kapcsolatokat. A megállapodás nem kötelező erejű, és

[15] Bruhács János: *Nemzetközi jog II. Különös Rész* (Budapest–Pécs: Dialóg Campus Kiadó 2010) 31.

[16] Emer de Vattel: *The Law of Nations* (Indianapolis: Liberty Fund 1797).

[17] Ori Pomson: „The Prohibition on Intervention Under International Law and Cyber Operations" *International Law Studies* 2022. 186.

[18] *Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty,* G.A. Res. 2131 (XX), 20 U.N. GAOR Supp. (No. 14), 11, U.N. Doc. A/6014 (1965).

[19] *Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations.* G.A. Res. 2625 (XXV), 25 U.N. GAOR Supp. (No.28), 121, U.N. Doc. A/8028. (1970).

[20] *Non-interference in the internal affairs of States,* G.A. Res. 31/91, U.N. GAOR, 31st sess., Supp. No. 39, 42, A/31/39 (1976).

[21] *Declaration on the Inadmissibility of Intervention and Interferfence in the Internal Affairs of States,* G.A. Res. 36/103, U.N. GAOR, 36th sess., Supp. No. 51, 79, A/36/51 (1981).

[22] Conference on Security and Co-operation in Europe Final Act. Helsinki 1975. (továbbiakban: Helsinki záróokmány).

nincs szerződéses státusza sem, ennek ellenére sikeresen csökkentette a feszültséget a nyugati országok és a keleti blokk államai között. A dokumentum elismerte a második világháború után kialakult európai határok sérthetetlenségét, és az aláíró nemzetek kötelezettséget vállaltak az emberi jogok tiszteletben tartására, valamint gazdasági, tudományos és humanitárius együttműködésre.[23] Mindezeken felül a beavatkozás tilalma is előkerül a Záróokmány szövegében. „[a] *részt vevő államok kölcsönös kapcsolataiktól függetlenül tartózkodnak minden közvetlen vagy közvetett, egyéni vagy kollektív beavatkozástól egy másik részt vevő állam belső joghatósága alá tartozó belső vagy külső ügyekbe. Ennek megfelelően tartózkodni fognak minden fegyveres beavatkozástól, vagy ilyen beavatkozással való fenyegetéstől egy másik részt vevő állam ellen.*"[24] Ugyanakkor elmondható, hogy a dokumentum nem hoz újdonságot a beavatkozás tilalmának rendszerében, hanem az addig elfogadott közgyűlési határozatokra épít.[25]

A Nemzetközi Bíróság a Nicaragua-ügyben részletesen vizsgálta a beavatkozás tilalmát elméleti és gyakorlati szinten egyaránt. Ennek következtében az eset mérvadó kútfőként szolgál a tilalom helyes értelmezése kapcsán.[26] A Nicaragua-ügy kapcsán a hágai testület így fogalmazott ítéletében: *[a]z általánosan elfogadott megfogalmazásokra tekintettel az elv megtiltja, hogy bármely állam vagy államcsoport közvetlenül vagy közvetve beavatkozzon más államok bel- vagy külügyeibe. A tiltott beavatkozásnak ennek megfelelően olyan ügyekre kell vonatkoznia, amelyekben az állami szuverenitás elve alapján minden állam szabadon dönthet. Ezek a politikai, gazdasági, társadalmi és kulturális rendszer megválasztása, a külpolitika kialakítása.*"[27]

Az is megállapítható az ítélet szövegéből, hogy a kényszer képezi a beavatkozás tilalmának lényegét. A kényszer különösen nyilvánvaló olyan beavatkozás esetén, amely erőszak alkalmazásával is együtt jár, akár közvetlen akár közvetett katonai akció formájában vagy a terrorista csoportoknak nyújtott támogatással.[28] A Nicaragua-ügy ítéletének szövegéből levezethető, hogy a beavatkozást egy állam valósíthatja meg egy másik állammal szemben. Magánszemély vagy valamely csoport által végrehajtott cselekmény is sértheti a beavatkozás tilalmát abban az esetben, ha tevékenységük betudható egy államnak. Továbbá az is elmondható, hogy a tiltott beavatkozás olyan ügyekre vonatkozik, amelyekben a sértett állam szabadon dönthet, ideértve a bel- és külügyeit.[29]

[23] Bővebben lásd: Michael Wood – Daniel Purisch: „Helsinki Final Act (1975)" in: *Max Planck Encyclopedia of Public International Law* [MPIL] 2011, *https://doi.org/10.1093/law:epil/9780199231690/e1051.*

[24] Helsinki záróokmány. 6.

[25] Pomson (17. lj.) 201.

[26] Pomson (17. lj.) 203.

[27] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America),* Merits, Judgement, I.C.J. Reports 1986. p. 14. para. 205 (saját fordítás).

[28] Uo.

[29] Delerue (4. lj.) 235.

Az ENSZ Alapokmánya a fent említett formában nem rendelkezik a beavatkozás tilalmáról (szemben az erőszak tilalmával). Az Alapokmányban csupán az ENSZ által a tagállamok belügyeibe történő beavatkozásról esik szó.[30]

Általánosságban a beavatkozás tilalma tehát úgy ragadható meg, mint az egyik állam kényszerítő jellegű beavatkozása egy másik állam bel- vagy külügyeibe. Csak akkor tiltott, ha az állam ügyeinek olyan területein fordul elő, amelyek kizárólag az állam saját hatáskörébe tartoznak, erőszakos vagy diktatórikus eszközökkel történnek, és az a céljuk, hogy meghatározott következményekkel járó magatartásokat kényszerítsenek egy szuverén államra.[31]

A bevezetőben már utaltam a Tallinni Kézikönyvre, amely az egyik legjelentősebb magánkodifikációs mű, amely a kibertér és a nemzetközi jog kapcsolatát taglalja. A könyv felépítése két részre osztható: a fekete betűs szabályok a szerzők egyhangú álláspontját nyilvánítják ki a *lex lata*-ról az egyes kérdésekben, ezeket pedig a kommentár követi.[32] A Kézikönyv ekképp rendelkezik a beavatkozás tilalmáról: *„Egy állam nem avatkozhat be – beleértve a kibereszközöket sem – egy másik állam belső működésébe vagy külügyeibe."*[33] A dokumentum a rendelkezéshez tartozó kommentárjában ugyanazokat a főbb megállapításokat teszi, amelyeket a Nemzetközi Bíróság a Nicaragua-ügy kapcsán kidolgozott, és amelyet a szakirodalom is megállapított. A Kézikönyvet létrehozó szakértői csoport tehát egyetértett abban, hogy a tiltott beavatkozás két elemből áll. Az első, hogy a beavatkozásnak olyan ügyre kell vonatkoznia, amelyek a sértett állam bel- vagy külügyeit érintik, másodszor pedig a cselekménynek kényszerítő jellegűnek kell lennie.[34]

3. ELLENINTÉZKEDÉSEK ÉS SZÜKSÉGHELYZET

Megállapítható, hogy az államok számára önvédelmi cselekmény foganatosítása csak és kizárólag fegyveres támadás szintjét elérő kiberműveletek esetén van lehetőségük,[35] nincs ez másképp a kiberműveletek esetében sem.[36] Az államok azonban akkor sem maradnak eszköztelenek, ha a művelet „csupán" az erőszak tilalmát,

[30] *„A jelen Alapokmány egyetlen rendelkezése sem jogosítja fel az Egyesült Nemzeteket arra, hogy olyan ügyekbe avatkozzanak, amelyek lényegileg valamely Állam belső joghatóságának körébe tartoznak, és nem kötelezi a tagokat arra sem, hogy az ilyen ügyeket a jelen Alapokmánynak megfelelő rendezési eljárás alá bocsássák".* ENSZ Alapokmány 2. cikk 7. bekezdés.

[31] Philip Kunig: „Intervention, Prohibition of" in: *Max Planck Encyclopedia of Public International Law* [MPIL] 2008, 1. bek.

[32] Michael N. Schmitt: „Tallinn Manual 2.0 on the International Law of Cyber Operations: What It is and Isn't" *Just Security* 2017. február 9., *https://www.justsecurity.org/37559/tallinn-manual-2-0-international-law-cyber-operations/.*

[33] Tallinn Manual 2.0. 66. szabály.

[34] Tallinn Manual 2.0. 314.

[35] Kis Kelemen Bence: *Célzott likvidálás a nemzetközi jogban – különös tekintettel a felfegyverzett pilóta nélküli repülőgépek alkalmazására* (Pécs: Publikon Kiadó 2023) 95., *https://doi.org/10.51783/ajt.2023.3.06.*

[36] Tallinn Manual 2.0. 71. szabály.

netán pusztán a beavatkozás tilalmát vagy más nemzetközi jogi normát sért. Mi sem mutatja jobban ennek a kérdésnek a gyakorlati jelentőségét, mint az a tény, hogy mind ez idáig az államok egyetlen kiberműveletet sem nyilvánítottak fegyveres támadásnak (sem pedig erőszak alkalmazásának). A két legfontosabb lehetőség, amely nyitva áll számukra, az ellenintézkedés intézménye, illetve a szükséghelyzetre való hivatkozás.[37]

3.1. ELLENINTÉZKEDÉSEK

Kizárt az állam olyan cselekményének jogellenessége, amely nem felel meg egy másik állammal szemben fennálló nemzetközi kötelezettségének, ha és amennyiben a cselekmény ellenintézkedést jelent az utóbbi állammal szemben.[38] Az ellenintézkedés úgy írható le, mint egy vagy több állam által egy másik államban szemben végrehajtott békés, egyoldalú reakció, amely lényegét tekintve jogellenes, kivéve ha az azt foganatosító állam vagy államok úgy ítélik meg, hogy az állam, amellyel szemben ellenintézkedést alkalmaznak, olyan nemzetközileg jogellenes cselekményt követett el, amelyre adott válaszként mégis igazolható az ellenintézkedésként végrehajtott egyébként jogellenes magatartás.[39] A 2001. évi államfelelősségi tervezet leszögezi, hogy a sértett állam csak abból a célból foganatosíthat ellenintézkedést a felelős állammal szemben, hogy azt rábírja fennálló kötelezettségeinek teljesítésére.[40] Ebből következik, hogy ellenintézkedést csak azzal az állammal szemben lehet foganatosítani, amely megszegte valamilyen nemzetközi kötelezettségét. Fontos kritérium továbbá, hogy bár fogalmilag ellenintézkedés bármilyen jogellenes magatartásra válaszolhat, arra kell irányulnia, hogy rávegye a felelős államot a kötelezettségének betartására, és csak addig foganatosítható, amíg feltétlenül szükséges. Ebből fakadóan, az ellenintézkedések célja nem lehet a büntetés vagy megtorlás.[41]

Az ellenintézkedések sajátosságaként említhető az is, hogy nem feltétlenül kell ugyanazon kötelezettségen alapulnia, mint amelyet a korábbi jogellenes cselekmény érintett.[42] További jogi korlátként említhető ugyanakkor, hogy az ellenintézkedés nem járhat együtt erőszak alkalmazásával, nem sérthet alapvető emberi jogokat, valamint humanitárius jellegű kötelezettségeket, továbbá egyéb *jus cogens* normákat sem.[43] Eljárásjogi követelményként jelenik meg, hogy az ellenintézkedést végrehajtó államnak fel kell szólítania a felelős államot a kötelezettségeinek teljesítésére, majd értesítnie kell azt az ellenintézkedések megtételére vonatkozó minden döntésről, és tárgyalást kell felajánlania. Az ellenintézkedés alkalmazását pedig

[37] Lahmann (10. lj.) 113.; 201.

[38] *Draft articles on Responsibility of States for Internationally Wrongful Acts*, with commentaries, 12 December 2001. U.N. Doc. A/RES/56/83 (2001) (továbbiakban: ARSIWA) 22. cikk.

[39] Denis Alland: „The Definition of Countermeasures" in James Crawford (szerk.): *The Law on International Responsibility* (Oxford: Oxford University Press 2010) 1127.

[40] ARSIWA 49. cikk. (1) bek.

[41] Lahmann (10. lj.) 115.

[42] James Crawford: *State Responsibility* (Cambridge: Cambridge University Press 2013) 685.

[43] ARSIWA 50. cikk.

fel kell függeszteni, ha a jogellenes cselekmény megszűnt, vagy a vita bíróság elé kerül.[44] Ebből adódik az, hogy ellenintézkedni voltaképpen kizárólag folyamatos jellegű jogsértéssel szemben lehetséges.[45] Az államfelelősségi szabályok előírják, hogy „amennyire lehetséges" az ellenintézkedéseknek visszafordíthatónak kell lenniük.[46]

A Tallinni Kézikönyv szerkesztői szerint az állam jogosult lehet akár kiber, akár más jellegű ellenintézkedéseket hozni válaszul egy vele szemben fennálló nemzetközi kötelezettség másik állam általi megszegése esetére.[47] Fontos, hogy a kiberműveletre válaszul végrehajtott ellenintézkedésnek nem kell feltétlenül a kibertérben megtörténnie, valójában sokféle formát ölthet. A sértett állam például felfüggesztheti egy szerződés alkalmazását, vagy a gazdaság területén hozhat különböző korlátozó intézkedéseket. Ennek a fordítottja is igaz: a sértett állam a kibertéren keresztül is tehet ellenintézkedéseket függetlenül attól, hogy a jogellenes cselekmény őt nem a kibertéren keresztül érte.[48] Az ellenintézkedés célpontja nem szükségszerűen valamilyen állami szerv vagy az állam kiberinfrastruktúrája, fontos azonban, hogy rajtuk keresztül az államra irányuljon a művelet. A szakértők egyetértenek abban, hogy az ellenintézkedések – szemben a szükséghelyzettel – nem alkalmazhatók nem állami szereplőkkel szemben.[49]

Ahogy már korábban is említettem, az ellenintézkedések nem ölthetnek büntető, illetve megtorló jelleget. Például, ha „A" állam kiberműveletet hajt végre „B" állam ipari létesítményei ellen, és ezzel kárt okoz, akkor „B" állam nem hajthat végre válaszul ugyanilyen kiberműveletet. Az ilyen ellenintézkedés ugyanis visszafordíthatatlan lenne, amiből az következik, hogy a kiberművelet megtorló jelleget ölt, mintsem hogy kényszerítse a felelős államot a jogellenes tevékenység megszüntetésére. Nemcsak hogy nem lehetnek büntető jellegűek az ellenintézkedések, de nem is súlyosbíthatják a fennálló vitát. A sértett államnak figyelembe kell vennie az eszkaláció kockázatát, amikor ellenintézkedés foganatosításán gondolkodik, különösen igaz ez a kibertéren keresztül végrehajtott ellenintézkedések esetén.[50]

Az ARSIWA ugyan előírja az államok számára az értesítési kötelezettséget, tehát a sértett államnak fel kell szólítania a felelős államot kötelezettségeinek teljesítésére, és értesítenie kell az ellenintézkedés alkalmazásáról szóló döntésről, ugyanakkor a dokumentum elismeri, hogy a sértett államok „sürgős ellenintézkedéseket tehetnek, amelyek szükségesek" jogaik megőrzése érdekében.[51] A sürgős ellenintézkedésekre vonatkozó szabály lehetővé teszi, hogy az államok helyzete ne váljon hátrányosabbá azért, mert nincs lehetőségük azonnali reagálásra.[52] A sürgős ellenintézkedések kiemelése azért is fontos, mert a kiberműveletek esetében kiemelt jelentőségük lehet. Előfordulhat, hogy egy folyamatban lévő kiberművelet – például egy DDoS,

[44] ARSIWA 52. cikk (1)-(3) bek.
[45] Lahmann (10. lj.) 171.
[46] ARSIWA 49. cikk (3) bekezdés.
[47] Tallinn Manual 2.0 20. szabály 111.
[48] Delerue (4. lj.) 435. o.
[49] Tallinn Manual 2.0 113.
[50] Delerue (4. lj.) 442.
[51] ARSIWA 52. cikk (2) bek.
[52] Crawford (42. lj.) 701.

azaz terheléses támadás – esetén a sértett államnak ellenintézkedésnek minősülő, jogellenes kiberműveletet kell végrehajtania az őt ért kiberművelet hatásainak mérséklése vagy a szükséges információk megszerzése érdekében. Az ilyen, kibertéren keresztül végrehajtott ellenintézkedések sikere nagymértékben függhet a meglepetés erejétől. Az előzetes értesítés itt lehetőséget adna a felelős államnak az ellenintézkedés hatásainak elkerülésére vagy mérséklésére. Következésképp ha egy állam a kibertéren keresztül fontolgatja ellenintézkedések meghozatalát – függetlenül attól, hogy a kibertéren vagy a fizikai térben érte őt a jogsértő cselekmény – előnyös lehet a sürgős ellenintézkedéshez való folyamodás.[53]

3.2. SZÜKSÉGHELYZET

Az ellenintézkedések foganatosításán túl az államok szükséghelyzetre is hivatkozhatnak abban az esetben, ha egy ellenséges kiberművelet nem éri el a fegyveres támadás szintjét, de az mégis az állam létfontosságú érdekét súlyosan vagy küszöbön álló módon veszélyezteti. A szükséghelyzet kapcsán kiemelendő, hogy az államfelelősségi tervezet akkor teszi lehetővé a szükséghelyzetre való hivatkozást, ha a szükséghelyzetben végrehajtott magatartás az egyetlen módja annak, hogy az állam megvédje létfontosságú érdekeit a fent említett súlyos és közvetlen veszélytől, továbbá nem sérti súlyosan a kötelezettséggel érintett állam, államok vagy a nemzetközi közösség egészének érdekeit.[54] További feltételként jelenik meg, hogy az állam menynyiben hatott közre a szükséghelyzet létrejöttében, illetve maga a kötelezettség ne zárja ki a szükséghelyzetre hivatkozást.[55] Összefoglalva elmondható, hogy a hatályos nemzetközi jog csak nagyon szigorú feltételrendszer mentén teszi lehetővé az államok számára, hogy szükséghelyzetre hivatkozzanak cselekményük igazolásául.

A szükséghelyzet annyiban mutat hasonlóságot az ellenintézkedésekkel, hogy mindkettő jogellenességet kizáró körülmény. Az ellenintézkedésekhez hasonlóan olyan válaszlépéseket foglalhatnak magukban, amelyek egyébként jogellenesek lennének, de ilyen jellegük kizárt, ugyanis az a céljuk, hogy véget vessen azoknak az ellenséges kiberműveleteknek, amelyek a választ foganatosító állam ellen irányultak. Ugyanakkor jelentős különbség a két intézmény között, hogy a szükséghelyzetre akkor is lehet hivatkozni, ha az adott kiberműveletet nem állami szereplők hajtották végre, és a művelet nem tudható be egyértelműen egy meghatározott államnak.[56]

A Tallinni Kézikönyv így fogalmaz fekete betűs szabályai között: „[e]gy állam szükséghelyzetre hivatkozással, létfontosságú érdekét érintő súlyos és közvetlen veszélyt jelentő magatartásokkal szemben – akár kiber jellegűek, akár nem – felléphet amennyiben ez az egyetlen módja a kérdéses érdek védelmének."[57]

[53] Delerue (4. lj.) 446–448.
[54] ARSIWA 25. cikk (1) bek.
[55] ARSIWA 25. cikk (2) bek.
[56] Michael N. Schmitt: „International Cyber Norms: Reflections on the Path Ahead" *https://puc.overheid.nl/mrt/doc/PUC_248171_11/*.
[57] Tallinn Manual 2.0. 26. szabály 135. (saját fordítás).

Az „létfontosságú érdek" kapcsán a pontos fogalmi meghatározás hiányával küzdünk. Abban az esetben, ha a kiberművelet emberéleteket veszélyeztet, ez a követelmény feltehetően teljesül. Általánosságban elmondható, hogy a civil lakosság biztonsága alapvető érdeknek számít.[58] Továbbá az elmúlt években konszenzus alakult ki arra vonatkozóan az államok között, hogy a kritikus infrastruktúra védelme is a létfontosságú érdek kategóriájába került. A kritikus infrastruktúra körébe sorolható az energia, a víz, a közlekedés, az egészségügyi szolgáltatások, de akár a távközlés is.[59] A Kézikönyvet készítő szerkesztői gárda szerint alapvető érdek az, amely lényeges és nagy jelentőségű az érintett állam számára. Annak meghatározása, hogy mi minősül alapvető érdeknek, mindig kontextusfüggő, illetve bizonyos mértékig államonként változhat. Egyetértettek abban is, hogy létezhetnek olyan esetek, amikor a nemzetközi közösség egészének érdeke is alapvető érdeknek minősül e szabály alkalmazása során.[60]

Azt, hogy a veszély mikor „súlyos", szintén nem definiálja az ARSIWA. Létezik olyan álláspont, amely szerint akkor beszélhetünk „súlyos" veszélyről, ha az eléri azt a súlyossági fokot, amely valószínűvé teszi érdekek megsemmisülését vagy legalábbis jelentős károsodását.[61] Így tehát ha a kiberművelet emberéleteket fenyeget, részben vagy egészben megzavarja a kritikus infrastruktúra működését, a követelmény teljesül.

Nemcsak a súlyosság, hanem a közvetlenség feltétele is kérdéses. Az ARSIWA kommentárja úgy fogalmaz, hogy a veszély fennállását objektív alapokon kell megállapítani, ha pusztán „lehetséges" annak bekövetkezése, az nem elengedő kritérium.[62] A Nemzetközi Bíróság a Bős-Nagymaros-ügyben hozott ítéletében így értékelte a kérdést: „[...] a veszélyesség fogalma messze túlmutat a »lehetőség« fogalmán, de egy hosszabb távon megjelenő veszély is »közvetlennek« tekinthető, ha bebizonyosodik, hogy ez a veszély, bármilyen távoli is legyen, nem kevésbé biztos és elkerülhetetlen."[63]

Az utolsó vizsgálandó kritérium a szükséghelyzetre való hivatkozás kapcsán az, hogy ez legyen az államnak az egyetlen lehetősége, hogy megvédje alapvető érdekeit a súlyos és közvetlen veszélytől. Kizárt tehát a szükséghelyzetre való hivatkozás, ha más jogszerű eszközök állnak rendelkezésre az állam számára, még akkor

[58] A Nemzetközi Bíróság lényegében hallgatólagosan elismerte a lakosság biztonságát alapvető érdekként, a Fal tanácsadó véleményében 2004-ben. A Bíróság így fogalmaz: „a Bíróság nem volt meggyőződve arról, hogy a fal megépítése a választott útvonal mentén az egyetlen eszköz Izrael érdekeinek megvédésére azzal a veszéllyel szemben, amire az építés indokaként hivatkozott." (saját fordítás). *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory,* Advisory Opinion. I.C.J. Reports 2004, p. 136. para. 140.

[59] Lahmann (10. lj.) 208; Tallinn Manual. 2.0. 136.

[60] Tallinn Manual 2.0. 135.

[61] Maria Agius: „The Invocation of Necessity in International Law" *Netherlands International Law Review* 2009/2. 103., *https://doi.org/10.1017/s0165070x09000953*; Tallinn Manual 2.0. 135.

[62] ARSIWA kommentár 25. bek. (15.).

[63] *Gabcikovo-Nagymaros Project (Hungary/Slovakia)*, Judgement, I.C.J. Reports 1997, p. 7. para. 54. (saját fordítás).

is, ha azok költségesebbek vagy kevésbé kényelmesek.[64] Ez a feltétel lehet az, amely miatt csak nagyon kevés esetben lehetséges – ha lehetséges egyáltalán – a kibertérben zajló események kapcsán a szükséghelyzetre hivatkozni. A kibertérben zajló műveletek gyakran egy szempillantás alatt történnek, tekintettel a kibertér sajátosságaira. Kétséges tehát, hogy egy állam mindig képes lesz-e kimerítően értékelni és tesztelni az összes technikailag elérhető védekezési eszközt, mielőtt a szükséghelyzet intézményéhez folyamodna.[65]

4. AZ ÁLLAMI GYAKORLAT

Megállapítható, hogy az elmúlt években jelentősen megnövekedett azoknak az államok a száma, amelyek állást foglaltak a kibertér és a nemzetközi jog kapcsolatáról. Az állásfoglalások jelentős hányada érintette a beavatkozás tilalmával kapcsolatos nézeteket. A következő táblázat szemlélteti a nyilatkozó államokat, továbbá nyilatkozatuk lényegét:

Nyilatkozatot tevő állam	*A nyilatkozat lényeges tartalma*
Ausztrália	„Az a kibertérben elkövetett káros magatartás, amely nem minősül erőszak alkalmazásának, továbbra is sértheti azt a kötelezettséget, hogy az állam ne avatkozzon be más állam bel- vagy külügyeibe. Tiltott a beavatkozás, ha az kényszerítő eszközökkel beavatkozik olyan ügyekbe, amelyekről más állam a szuverenitásának elve alapján szabadon dönthet."[66]
Brazília	„A beavatkozás tilalmának megsértéséhez az információs technológiai eszközök rosszindulatú felhasználásának magában kell foglalnia egy olyan kényszerelemet, amely érinti a sértett állam politikai, gazdasági, társadalmi és kulturális rendszerének szabad megválasztásához, valamint a külpolitikájának kialakításához való jogot.[67]
Kanada	„Az állami kibertevékenységek sérthetik a másik állam bel- vagy külügyeibe való beavatkozásra vonatkozó alapvető nemzetközi jogi tilalmat. Ez az eset akkor áll fenn, ha mindkét alábbi feltétel teljesül: a tevékenység célja a bel- vagy külügyekbe való beavatkozás, továbbá a tevékenység olyan hatást okoz, amelyek megfosztják vagy kényszerítik az érintett államokat olyan kérdésekben, amelyekben szabad választásuk van."[68]

[64] ARSIWA kommentár 25. bek. (15.).

[65] Lahmann (10. lj.) 219.

[66] Annex B: Australia's position on how international law applies to State conduct in cyberspace. Australian Government (továbbiakban: Ausztrália állásfoglalása), *https://www.internationalcybertech.gov.au/our-work/annexes/annex-b.*

[67] *Official compendium of voluntary national contributions ont he subject of how international law applies tot he use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266.* 13 July 2021. U.N. Doc. A/76/136* (2021) (a továbbiakban: UNGA: A/76/136) 19.

[68] International Law applicable in cyberspace. Government of Canada (a továbbiakban: Kanada állásfoglalása), 22. bek., *https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng.*

Nyilatkozatot tevő állam	*A nyilatkozat lényeges tartalma*
Észtország	„Ha egy államnak betudható kiberművelet egy másik államot bel- vagy külügyeiben olyan cselekvésre kényszerít, amelyet önként nem követne el, az tiltott beavatkozásnak minősül.[69]
Franciaország	„Egyre több állam szerzi meg a kapacitást a kibertérben történő műveletek előkészítésére és lefolytatására. Ha más állam jogának sérelmére hajtják végre, az ilyen műveletek behatolásuk mértékétől és hatásától függően sértheti a beavatkozás tilalmát vagy akár az erőszak tilalmát is. Franciaország bel- vagy külügyeibe digitális eszközökkel történő beavatkozás – vagyis olyan beavatkozás, amely az ország politikai, gazdasági, társadalmi vagy kulturális rendszerében kárt okoz vagy okozhat – a beavatkozás tilalmának megsértését jelentheti."[70]
Németország	„Németország általánosságban azon a véleményen van, hogy a kiberműveletek a nemzetközi jog szerinti tiltott beavatkozásnak minősülhetnek, ha a mértéküket és a hatásukat tekintve hasonlóak a fizikai térben alkalmazott kényszerhez."[71]
Irán	„Jogellenesnek minősül a fegyveres beavatkozás és minden egyéb beavatkozás az állam politikai, gazdasági, társadalmi és kulturális szervei ellen számítógépes vagy egyéb eszközökkel. Egyetlen állam sem kényszeríthet egy másik államot kiber- vagy egyéb eszközökkel, hogy politikai, gazdasági vagy más döntést hozzon, vagy arra ösztönözzön."[72]
Olaszország	„Olaszország úgy véli, hogy a kiberművelet a beavatkozás tilalmának megsértését eredményezi, ha egy állam kényszerítő eszközöket alkalmaz arra, hogy egy másik államot egy adott cselekvés megtételére vagy attól való tartózkodásra kényszerítsen a saját hatáskörébe tartozó ügyben."[73]
Japán	„A kiberműveletek jogellenes beavatkozásnak minősülhetnek, ha a Nicaragua-ítéletben tisztázott körülmények teljesülnek, beleértve a kényszer elemét is."[74]
Hollandia	„A digitális technológia fejlődése lehetőséget adott az államoknak arra, hogy saját határaikon kívül is befolyást gyakoroljanak, illetve beavatkozzanak más államok ügyeibe. A beavatkozás egy másik állam bel- vagy külügyeibe való beavatkozást jelenti, azzal a céllal, hogy az adott állammal szemben kényszert alkalmazzanak."[75]
Új-Zéland	„Az államnak betudható kiberművelet összeegyeztethetetlen a beavatkozás tilalmával, ha jelentős hatással van olyan ügyre, amely a célállam szuverén funkciói közé tartozik, és kényszerítő jellegű."[76]

[69] UNGA: A/76/136. 25.

[70] Droit International Appliqué Aux Opérations Dans Le Cyberspace. Ministère Des Armées (a továbbiakban: Franciaország állásfoglalása), 6., *www.justsecurity.org/wp-content/uploads/2019/09/droit-internat-appliqué-aux-opérations-cyberespace-france.pdf.*

[71] On the Application of International Law in Cyberspace. The Federal Republic (a továbbiakban: Németország állásfoglalása), 5–6., *https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf.*

[72] „General Staff of Iranian Armed Forces Warns of Tough Reaction to Any Cyber Threat" *Nournews.* 2020. augusztus 18. *nournews.ir/En/News/53144/General-Staff-of-Iranian-Armed-Forces-Warns-of-Tough-Reaction-to-Any-Cyber-Threat.*

[73] Italian Position Paper on 'International Law and Cyberspace' (a továbbiakban: Olaszország állásfoglalása) 4., *https://www.esteri.it/mae/resource/doc/2021/11/italian_position_paper_on_international_law_and_cyberspace.pdf.*

[74] Basic Position of the Government of Japan on International Law Applicable to Cyber Operations. Ministry of Foreign Affairs of Japan, 2., *https://www.mofa.go.jp/files/100200935.pdf.*

[75] Forrás: Appendix: International Law in Cyberspace (a továbbiakban: Hollandia állásfoglalása) 3., *https://ceipfiles.s3.amazonaws.com/pdf/CyberNorms/LawStatements/Appendix_+International+Law+in+Cyberspace+(Statement+by+the+Netherlands).pdf.*

[76] The Application of International Law to State Activity in Cyberspace. New Zeland Foreign Affairs and Trade, (a továbbiakban: Új-Zéland állásfoglalása) 9. bek., *https://www.dpmc.govt.nz/sites/*

Nyilatkozatot tevő állam	*A nyilatkozat lényeges tartalma*
Norvégia	„Azok a kiberműveletek, amelyek a célállamot olyan cselekvés megtételére kényszerítik, amelyet egyébként önként nem tett volna meg a belső vagy külső ügyeivel kapcsolatban, a nemzetközi jogot sértik.[77]
Románia	„A következő kritériumoknak kell teljesülniük ahhoz, hogy a kiberművelet a nemzetközi jog szerint tiltott beavatkozásnak minősüljön: ki kell terjednie azokra a kérdésekre, amelyekben az államok szabadon döntenek, a cselekménynek kényszerítő jellegűnek kell lennie, és ok-okozati összefüggésnek kell lennie a kényszerítő aktus és a célállam ügyeire gyakorolt hatás között."[78]
Szingapúr	„Szingapúr megerősíti, hogy a beavatkozás tilalma a kibertérre is vonatkozik. Az egyik állam által a másikkal szembeni tiltott beavatkozás azokra az ügyekre terjed ki, ahol a sértett állam a szuverenitás elve alapján szabadon dönthet. Szingapúr véleménye szerint a beavatkozás szükségszerűen magában foglalja a kényszer elemét is."[79]
Svédország	„A beavatkozás tilalma mint a nemzetközi jog alapelve a kibertérben is alkalmazandó. A beavatkozás tilalma általában két elemet foglal magában: a beavatkozás olyan ügyekre vonatkozik, amelyekben minden állam szabadon dönthet, és a kényszert.[80]
Svájc	„A beavatkozás tilalma a kibertérre is vonatkozik. Ez azt jelenti, hogy a kibertérben egy állam jogellenes beavatkozása egy másik állam politikai vagy gazdasági ügyeibe a szuverenitás megsértése mellett a beavatkozás tilalmát is sérti, ha a vonatkozó feltételek teljesülnek.[81]
Egyesült Királyság	„Az erőszak alkalmazásának küszöbértéke alatt az államok belügyeibe való beavatkozást tiltó nemzetközi szokásjogi szabály az államok kiberműveleteire ugyanúgy vonatkozik, mint egyéb tevékenységeikre."[82]
Egyesült Államok	„Egy másik állam alapvető funkcióiba való, kényszerítő jellegű beavatkozásra vonatkozó nemzetközi jogi tilalom az állam kibertérben tanúsított magatartására is vonatkozik.[83]

A nyilatkozó államok tehát egyetértenek abban, hogy a beavatkozás tilalma mint nemzetközi jogi alapelv a kibertérre is alkalmazandó norma. Tartalmilag pedig azokat a fogalmi elemeket ölelik fel az államok nyilatkozataikban, amelyeket a Nicaragua-ügy kapcsán a Nemzetközi Bíróság kidolgozott a tilalommal kapcsolat-

default/files/2020-12/The%20Application%20of%20International%20Law%20to%20State%20Activity%20in%20Cyberspace.pdf.

[77] UNGA: A/76/136. 68.

[78] UNGA: A/76/136. 77.

[79] UNGA: A/76/136. 83.

[80] Position Paper on the Application of International Law in Cyberspace. Government Offices of Sweden (a továbbiakban: Svédország állásfoglalása) 3., *https://www.government.se/contentassets/3c2cb6febd0e4ab0bd542f653283b140/swedens-position-paper-on-the-application-of-international-law-in-cyberspace.pdf.*

[81] Switzerland's position paper on the application of international law in Cyberpsace. Federal Department of Foreign Affairs FDFA (a továbbiakban: Svájc állásfoglalása) 3., *https://www.eda.admin.ch/dam/eda/en/documents/aussenpolitik/voelkerrecht/20210527-Schweiz-Annex-UN-GGE-Cybersecurity-2019-2021_EN.pdf.*

[82] Application of international law to state's conduct in cyberspace: UK statement. Foreign, Commonwealth and Development Office (a továbbiakban: Nagy-Britannia állásfoglalása) 8., *https://www.gov.uk/government/publications/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement.*

[83] DOD General Counsel Remarks at U.S. Cyber Command Legal Conference. U.S. Department of Defense, *https://www.defense.gov/News/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/.*

ban. Az állami gyakorlat is egységes tehát abban, hogy az államok bel- vagy külügyeibe történjen a beavatkozás a másik állam részéről, illetve kényszerítő jelleggel kell történjen. Ezen feltételek együttes fennállása esetén beszélhetünk tehát a beavatkozás tilalmának megsértéséről, a kibertérben is, amelyet így nyugodtan jellemezhetünk szokásjogi erejű normaként is.

Több állam nyilatkozatából is kitűnik, hogy azt, hogy az adott kiberművelet sérti-e a beavatkozás tilalmát – vagy adott esetben az erőszak tilalmát –, esetről esetre szükséges vizsgálni.[84]

Egyes államok állásfoglalásukban példálózó jelleggel megemlítenek eseteket, amelyek szerintük a beavatkozás tilalmát sértő kiberműveletek lehetnek.

Mind az ausztrál, mind pedig a brit dokumentum megállapítja, hogy a beavatkozás tilalmát sértik az olyan kiberműveletek, amelyek manipulálják a választási rendszert a választások eredményének megváltoztatása érdekében.[85] Hosszan értekezik a választásokba való beavatkozásról a német állásfoglalás is. Németország is elfogadja azt a véleményt, hogy a választásokat célzó kiberműveletek jogellenes beavatkozásnak minősülnek. Példaként említik azt a lehetőséget, amikor egy állam az interneten keresztül dezinformációt terjesztve okoz olyan politikai felfordulást vagy zavargásokat, amelyek akadályozzák a választások szabályszerű megtartását. Nem szükséges tehát az, hogy közvetlenül a választási rendszerekbe történjen a beavatkozás.[86] A kanadai nyilatkozat a választásokba való beavatkozásokon túl azt a példát hozza, amikor is egy kiberművelet megzavarja a sértett állam valamely gázvezetékének működését, ezáltal hátrányosabb pozícióba kényszeríti az adott államot az energiahordozókra vonatkozó szerződések tárgyalásánál.[87] Végezetül pedig az olasz és az új-zélandi dokumentumokból emelném ki azt a példát, amely szerint a beavatkozás tilalmát sértheti az a kiberművelet, amely az adott állam közegészségügyi rendszere ellen irányul, ezáltal veszélyezteti az adott állam erőfeszítéseit járvány idején.[88]

Az állami állásfoglalások, nyilatkozatok jelentős része tartalmazza az ellenintézkedésre mint az ellenséges célú kiberműveletek esetén alkalmazható jogintézményre vonatkozó álláspontokat, ezt a következő táblázat szemlélteti:

Nyilatkozatot tevő állam	*A nyilatkozat lényeges tartalma*
Ausztrália	„Ha egy állam olyan rosszindulatú kibertevékenységnek lesz az áldozata, amely a felelős államnak tulajdonítható, a sértett állam bizonyos körülmények között ellenintézkedéseket foganatosíthat, akár a kibertérben, akár más módon."[89]
Brazília	„Brazília úgy véli, hogy további egyeztetésekre van szükség a jogellenes cselekményekre adott ellenintézkedések jogszerűségéről, ideértve a kiberkontextust is."[90]

[84] Az esetről esetre történő vizsgálatot említi például a kanadai, a román, a svéd és a svájci nyilatkozat is.
[85] Lásd Ausztrália és Nagy-Britannia állásfoglalását. 9. bek.
[86] Németország állásfoglalása. 5.
[87] Kanada állásfoglalása. 22. bek.
[88] Olaszország állásfoglalása. 5; Új-Zéland állásfoglalása 10. bek.
[89] Ausztrália állásfoglalása.
[90] UNGA: A/76/136, 22.

Nyilatkozatot tevő állam	*A nyilatkozat lényeges tartalma*
Kanada	„Kanada úgy véli, hogy az államok jogosultak ellenintézkedéseket alkalmazni a jogsértő cselekményekre válaszul, ideértve a kiberteret is." „A jogsértő kiberműveletekre válaszul hozott ellenintézkedések lehetnek nem kiber jellegűek is."[91]
Észtország	„Ha egy kiberművelet nem éri el a fegyveres támadás küszöbét, de ennek ellenére a nemzetközi jog megsértését jelenti, az államok fenntartják a jogot az ellenintézkedések megtételére, az államfelelősség szabályaival összhangban."[92]
Franciaország	„Franciaország ellenintézkedésekkel (is) válaszolhat a kibertámadásokra. A nemzetközi jogot sértő kibertámadásokra válaszul Franciaország olyan ellenintézkedéseket tehet, amelyek célja egyfelől érdekeinek védelme, másfelől, hogy rábírja a felelős államot kötelezettségeinek teljesítésére."[93]
Németország	„Németország elfogadja, hogy a nemzetközi kötelezettségek megszegése esetén (legyen az kibertérrel kapcsolatos vagy a kibertéren kívüli) kiber és kibertéren kívüli ellenintézkedésekkel is lehet reagálni."[94]
Olaszország	„Olaszország úgy véli, hogy az ellenintézkedések megfelelő válaszlépések lehetnek az olyan kiberműveletekre, amelyek a fegyveres támadás küszöbértékét el nem érő jogellenes cselekménynek minősülnek."[95]
Hollandia	„Ha az állam egy másik állam által elkövetett jogellenes cselekmény áldozata, akkor bizonyos körülmények között ellenintézkedéseket tehet. Az ellenintézkedések olyan cselekmények, amelyek általában valamely kötelezettség megsértésének minősülnek, de megengedettek, mert a kötelezettség megsértésére adott válaszként funkcionál. A kibertérben például kiberművelet indítható olyan hálózatok vagy rendszerek leállítására, amelyeket egy másik állam kibertámadásra használ."[96]
Új-Zéland	„Az ellenintézkedések jogellenes cselekmények, amelyek megengedettek, ha egy másik államot bírnak rá a nemzetközi jog szerinti kötelezettségei teljesítésére. Idetartoznak olyan kibertevékenységek is, amelyeket a nemzetközi jog egyébként tiltana."[97]
Norvégia	„Ha egy állam jogellenes kiberművelet áldozata és a másik állam a nemzetközi szokásjog szerint felelősségre vonható, a sértett állam a körülményektől függően jogosult lehet ellenintézkedések megtételére."[98]
Szingapúr	„Ha az állam elleni rosszindulatú kibertevékenység nem emelkedett a fegyveres támadás szintjére, amely felhatalmazná a sértett államot az önvédelem jogának alkalmazására, a nemzetközi jog biztosítja, hogy a sértett állam ellenintézkedéshez folyamodhat."[99]
Svédország	„Ha egy államot jogellenes cselekmény ér, különféle intézkedésekkel válaszolhat. Az ilyen intézkedések magukban foglalják az ellenintézkedéseket is. […] Ez a szabály a kiberműveletekre is vonatkozik."[100]
Svájc	„Ha a fegyveres támadás küszöbét nem érték el, az államok azonnali, arányos és erőszakmentes ellenintézkedést foganatosíthatnak. […] A kiberműveletekre adott ellenintézkedéseknek nem feltétlenül kell a kibertérben megtörténniük."[101]

[91] Kanada állásfoglalása. 34–35. bek.
[92] UNGA: A/76/136, 29.
[93] Franciaország állásfoglalása. 7–8.
[94] Németország állásfoglalása. 13.
[95] Olaszország állásfoglalása. 7.
[96] Hollandia állásfoglalása. 7.
[97] Új-Zéland állásfoglalása. 21. bek.
[98] UNGA: A/76/136. 72.
[99] UNGA: A/76/136. 84.
[100] Svédország állásfoglalása. 6.
[101] Svájc állásfoglalása. 4.

Nyilatkozatot tevő állam	*A nyilatkozat lényeges tartalma*
Egyesült Királyság	„Az ellenintézkedés [...] értelmében a sértett állam a jogsértő magatartás megállítása és a jóvátétel biztosítása érdekében oly módon reagálhat egy jogellenes cselekményre, amely normál körülmények között szintén jogellenes lenne. Az Egyesült Királyság korábban egyértelművé tette, hogy az ellenintézkedések a jogellenes kiberműveletek esetében is rendelkezésre állnak."[102]
Egyesült Államok	„Az államoknak betudható jogellenes cselekménynek minősülő kibertevékenységekre válaszul hozott ellenintézkedések kiberalapú és nem a kibertéren alapuló műveletek egyaránt lehetnek."[103]

A nyilatkozatokat összevetve azt láthatjuk, hogy az államok általánosságban elfogadják az ellenintézkedés intézményét akkor, amikor az ellenséges célú kiberművelet nem éri el a fegyveres támadás szintjét. A nyilatkozó államok többsége abban is egyetért, hogy mind a kibertérben, mind a valós fizikai térben lehetséges ellenintézkedést alkalmazni, ha sértett állam pozíciójába kerülnek. Nincs vita abban sem, hogy a kiberműveletekkel szemben foganatosított ellenintézkedésekre is irányadóak az ellenintézkedésekre vonatkozó általános szabályok, amelyeket dolgozatom korábbi részében ismertettem. Egyedül a brazil nyilatkozat fogalmaz meglepően óvatosan. Amíg a többi állam nem bocsátkozik hosszas fejtegetésbe annak kapcsán, hogy az ellenintézkedés megfelelő válaszlépés lehet-e az ellenséges célú kiberműveletekre, addig a brazil állásfoglalás úgy fogalmaz: „különösen az információs technológia területén kell több tényezőt is figyelembe venni, amely arra mutat, hogy az ellenintézkedésekkel kapcsolatban óvatos megközelítést kell alkalmazni", illetve „Brazília úgy véli, hogy további egyeztetésekre van szükség" az államok között a kérdés kapcsán.[104]

Ahogy már fentebb bemutattam, az államok nemcsak ellenintézkedést alkalmazhatnak, hanem szükséghelyeztre is hivatkozhatnak abban az esetben, ha a velük szemben végrehajtott kiberművelet nem éri el a fegyveres támadás szintjét, tehát nincs lehetőség az önvédelem jogának alkalmazására. A szükséghelyzetre vonatkozó állami álláspontokat meglepően kevés nyilatkozatban találhatunk. A nyilatkozó államok kis része gondolta csupán azt, hogy a szükséghelyzet intézményével kapcsolatban is nyilatkozatot kell tennie. Ezeket az államokat és nyilatkozataik lényeges tartalmát a következő táblázat szemlélteti:

Nyilatkozatot tevő állam	*A nyilatkozat lényeges tartalma*
Franciaország	„Franciaország azt sem zárja ki, hogy végveszélyre vagy szükséghelyzetre hivatkozzon annak érdekében, hogy létfontosságú érdekeit megvédje a fegyveres támadás küszöbértéke alatti, de súlyos és közvetlen veszélyt jelentő kibertámadásokkal szemben."[105]
Németország	„Kivételesen kizárható egy államnak a nemzetközi kötelezettségeit megsértő kiberműveletének jogellenessége, ha az állam szükséghelyzetben cselekedett."[106]

[102] International Law in Future Froniers. Az Egyesült Királyság főügyészének 2022. május 19-ei beszéde, *https://www.gov.uk/government/speeches/international-law-in-future-frontiers*.
[103] UNGA: A/76/136. 142.
[104] UNGA: A/76/136. 22.
[105] Franciaország állásfoglalása. 8.
[106] Németország állásfoglalása. 14.

Nyilatkozatot tevő állam	*A nyilatkozat lényeges tartalma*
Hollandia	„A szükséghelyzet olyan jogellenességet kizáró körülmény, amely bizonyos szigorú feltételek mellett igazolja az egyébként jogellenes cselekményt, például egy másik állam ellen irányuló, támadó jellegű kiberműveletet."[107]
Norvégia	„Szükséghelyzet esetén az állam úgy is reagálhat egy kiberműveletre, hogy az elviekben egy nemzetközi jogi kötelezettség megsértését jelenti, de a nemzetközi jog szerint mégsem kell felelősséget vállalnia a tetteiért."[108]
Svédország	„Bizonyos szigorú feltételek mentén az állam olyan intézkedéseket alkalmazhat, amelyek egyébként sértenének egy nemzetközi jogi kötelezettséget annak érdekében, hogy megvédjék alapvető érdekeiket egy súlyos és közvetlen veszélytől. Ez a kibertér kontextusában is érvényes, ugyanakkor csak kivételesen állnak rendelkezésre valamely kötelezettség elmulasztása esetén."[109]
Svájc	„Az államfelelősségre vonatkozó szabályok az ellenintézkedések mellett egyéb különleges körülményeket is biztosítanak, amelyek kizárják egy olyan magatartás jogellenességét, amely egyébként nem lenne összhangban az állam nemzetközi jogi kötelezettségeivel. Például egy állam mentesülhet egy kötelezettsége betartása alól, ha így tudja megvédeni lényeges érdekeit a súlyos és közvetlen veszélytől. Ezek a szabályok a kiberműveletekkel összefüggésben is alkalmazhatók."[110]

A nyilatkozatokat megvizsgálva azt láthatjuk, hogy az állami gyakorlatban is előkerül az „alapvető érdekek", valamint a „súlyos és közvetlen veszély" kifejezések használata. Egységesek az állásfoglalások abban a tekintetben is, hogy hangsúlyozzák a szükséghelyzetre való hivatkozás kivételes jellegét.

A nyilatkozatokat tekintve egyedül a német és a holland nyilatkozat az, amely nemcsak pár sorban deklarálja az elvi lehetőségét a szükséghelyzetre való hivatkozásnak, hanem a gyakorlati alkalmazhatóságát is fejtegeti. A német nyilatkozat szerint az „alapvető érdekek" mint fogalom azon keresztül határozható meg, hogy a rosszindulatú kiberművelet ténylegesen vagy potenciálisan milyen típusú infrastruktúrát céloz meg, valamint hogy az infrastruktúra az állam szempontjából milyen jelentőséggel rendelkezik. Példaként említi a nyilatkozat, hogy az állampolgárok védelme a súlyos fizikai sérülésekkel szemben minden állam „alapvető érdeke". Annak meghatározása pedig, hogy a veszély „súlyos-e", eseti értékelés szükséges. Minél fontosabb az „alapvető érdek", annál alacsonyabb a „súlyosság kritériuma." Németország szerint nem szükséges a testi sérülés bekövetkezése, elegendő a jelentős mértékű funkcionális károsodás is.[111]

A holland nyilatkozat példálózó jelleggel sorolja fel, mi minősülhet alapvető érdeknek: idetartozik a villamosenergia-hálózat, a vízellátás és a bankrendszer működése is. A veszély súlyosságára vonatkozóan pedig a holland nyilatkozat is az eseti alapon történő vizsgálatot részesíti előnyben.[112]

[107] Hollandia állásfoglalása. 7.
[108] UNGA: A/76/136. 73.
[109] Svédország állásfoglalása. 6.
[110] Svájc állásfoglalása. 7.
[111] Németország állásfoglalása. 11–12.
[112] Hollandia állásfoglalása. 8.

5. A KÖZELMÚLT ESEMÉNYEI

A 2007-es év mérföldkőnek tekinthető a kibertér történetében. Ekkor hajtották végre az első olyan kibertámadást, amely jelentős állami háttérrel rendelkezett, és egy másik állam ellen irányult. A műveleteket orosz IP címekről hajtották végre, a sértett állam pedig Észtország volt. A támadás főként az észt sajtótermékeket, bankszektort, illetve az ország kormányzati szféráját érintette. Ugyanakkor a támadásnak nem volt halálos áldozata, nem keletkezett helyrehozhatatlan vagy súlyos infrastrukturális károsodás. A lakosság annyit érzékelt az eseményekből, hogy egyes banki szolgáltatások nem voltak elérhetők, illetve az elektronikus levelezésekhez nehezebben lehetett hozzáférni.[113] Mindezekre tekintettel megállapítható, hogy ha a kiberművelet nem éri el az erőszak alkalmazásának szintjét, sokkal inkább az képezheti vizsgálat tárgyát, hogy a beavatkozás tilalma mint nemzetközi jogi alapelv sérült-e.

A kiberművelet hátterében az észt kormánynak az a döntése állhatott, miszerint a Vörös Hadseregnek emléket állító szoborcsoportot Tallinn központjából egy kevésbé központi helyszínre kell költöztetni.[114] Véleményem szerint annak a döntésnek a joga, hogy a szoborcsoport a város melyik részén kapjon helyet, az adott állam kormányáé vagy éppen a város vezetéséé, ily módon az állam belügyeibe tartozik, a műveletek célja pedig egyfajta „megtorlás" lett volna válaszul az átköltöztetésre. Úgy gondolom, hogy amennyiben megerősítést nyerne, hogy a támadás hátterében Oroszország áll, megállapítható lenne a beavatkozás tilalmának megsértése.

2014 novemberében a magát Béke Őrzőinek nevező csoport hajtott végre támadást a Sony Pictures ellen. A nagyszabású akció keretében a hackerek számos, a vállaltra nézve rendkívül érzékeny információt gyűjtöttek össze, továbbá azt követelték, hogy a Sony mondja le az „Interjú" című film bemutatóját, ami az észak-koreai vezető, Kim Dzsong Un meggyilkolását is ábrázolta volna. Az FBI a nyomozás során megállapította, hogy Észak-Korea áll a támadás hátterében, egészen pontosan annak hírhedt Bureau 121 kódnevű hackercsapata.[115] Jeh Johnson, az akkori belbiztonsági miniszter úgy nyilatkozott az esetet követően, hogy *„[a] Sony Pictures Entertainment elleni kibertámadás nem csupán egy vállalat és alkalmazottai elleni támadás volt. Ez a véleménynyilvánítási szabadságunk és az életmódunk elleni támadás is volt egyben."*[116]

Felmerül a kérdés, hogy a Sonyt ért támadás megsértheti-e a beavatkozás tilalmát. Az első vizsgálandó kritérium az, hogy a támadás betudható-e egy államnak, valamint az, hogy egy másik állam ellen kell irányulnia. Bár teljeskörűen sosem sikerült bebizonyítani, hogy Észak-Korea áll az események mögött, az FBI jelentésére ala-

[113] Damien McGuinness: „How a cyber attack transformed Estonia" *BBC* 2017. április 27.

[114] Uo.

[115] Oliver Laughland – Dominic Rushe: „Sony cyber attack linked to North Korean government hackers, FBI says" *The Guardian* 2014. december 19.

[116] Statement By Secretary Johnson on Cyber Attack on Sony Pictures Entertainment. Homeland Security, *https://www.dhs.gov/news/2014/12/19/statement-secretary-johnson-cyber-attack-sony-pictures-entertainment.*

pozva, tételezzük fel, hogy a támadás betudható az ázsiai országnak. Ugyanakkor a belső levelezések nyilvánosságra hozatala, a film megjelentetésének késleltetése, illetve a Sony vállalat gazdasági nehézségei csupán a vállalatra vonatkozó problémák. Még ha a támadást be is tudhatjuk Észak-Koreának, a sértett ebben az esetben nem egy állam volt – jelen esetben nem az Egyesült Államok –, hanem egy magánvállalat, ily módon ez a művelet nem jelenti a beavatkozás tilalmának megsértését. Továbbá a műveletnek sem közvetlen, sem közvetett módon nem volt kényszerítő hatása az Egyesült Államokra mint államra.[117]

Az állami gyakorlat vizsgálata során szembetűnő, hogy több állam is kiemeli a választási manipulációt, mint lehetséges példát a beavatkozás tilalmának megsértésére a kibertérben. A következőkben két esetet szeretnék megvizsgálni, ahol egy választást a kibertéren keresztül próbáltak megzavarni.

A 2016-os amerikai elnökválasztást több olyan incidens is érintette, amely a kibertéren keresztül valósult meg.[118] Először is a Demokrata Párt rendszerének feltörése borzolta a kedélyeket. A támadók hozzáfértek a párt adatbázisához, továbbá gyakorlatilag valamennyi prominens tag levelezéséhez és üzenetváltásaihoz. Az amerikai fél szerint a támadást Oroszország követte el, ugyanakkor az oroszok tagadták, hogy közük lenne az incidenshez.[119] Később az is kiderült, hogy nem csak a demokratákat rendszerét érte támadás a választással összefüggésben. Harminckilenc államban magát a szavazórendszert is támadás érte, Illinois államban pedig a hackerek megpróbálták törölni, illetve meghamisítani a szavazók adatait.[120]

Az eseményekkel kapcsolatban felmerül a kérdés, hogy mi volt pontosan a műveletek célja. Az egyik feltevés az, hogy a támadásokat azért követték el, hogy elősegítsék Donald Trump megválasztását, mivel Vlagyimir Putyin őt preferálta Hillary Clintonnal szemben.[121] Ha a beavatkozás tilalma mentén vizsgáljuk meg a történteket, azt láthatjuk, hogy a választási folyamatba történő beavatkozás mindenképp az állam belügyeibe való beavatkozást jelenti. Egyes szerzők úgy gondolják, hogy általánosságban a választási rendszerek feltörése csupán a szuverenitás megsértését jelenti, az a beavatkozás tilalmát nem sérti. Ezt arra alapozzák, hogy a fájlok feltörése csupán egy előkészületi tevékenység, a beavatkozás tilalma csak akkor sérül, ha a fájlokat nyilvánosságra is hozzák.[122] Jelen esetben a nyilvánosságra hozatal meg-

[117] Delerue (4. lj.) 240.

[118] Petrovics Roberto: „Az Egyesült Államok 2016. évi elnökválasztása és az orosz befolyás az erőszak tilalmának tükrében" *Scriptura* 2019/1. 1.

[119] Ellen Nakashima: „Russian government hackers penetrated DNC, stole opposition research on Trump" *The Washington Post* 2016. június 14. *www.washingtonpost.com/world/national-security/russian-government-hackers-penetrated-dnc-stole-opposition-research-on-trump/2016/06/14/cf006cb4-316e-11e6-8ff7-7b6c1998b7a0_story.html.*

[120] Michael Riley – Jordan Robertson: „Russian Hacks on U.S. Voting System Wider Than Previously Known" *Bloomberg* 2017. június 13. *www.bloomberg.com/news/articles/2017-06-13/russian-breach-of-39-states-threatens-future-u-s-elections.*

[121] Andew Roth: „Putin says Trump is 'absolute leader' in U.S. presidental race" T*he Washington Post* 2015. december 17., *https://www.washingtonpost.com/world/putin-no-major-gaps-with-washington-over-efforts-to-end-syria-conflict/2015/12/17/a178255e-a431-11e5-8318-bd8caed8c588_story.html.*

[122] Delerue (4. lj.) 250.

történt, az orosz titkosszolgálat ügynökei álnéven megosztották a WikiLeaks nevű szervezettel, amely több mint húszezer e-mail tartalmát tette közzé.[123]

Széles körben elfogadott, hogy a támadás hátterében a Kreml állt, ugyanakkor Oroszország tagadta, hogy köze lenne a műveletekhez.[124] Minden feltételt összevetve, ha elfogadjuk, hogy a támadás mögött valóban Oroszország áll, akkor az amerikai elnökválasztással kapcsolatos kiberműveletek sérthetik a beavatkozás tilalmát. A fentebb bemutatott állami gyakorlat is egységes abban, hogy a választási rendszerekbe történő beavatkozás a beavatkozás tilalmának a megsértését jelenti.

Fél évvel később Franciaországban játszódtak le hasonló események. Ezúttal Emmanuel Macron és pártja, az „*En Marche!*" volt összehangolt kiberműveletek célpontja. A párt közleménye szerint a támadók különféle dokumentumokat, e-maileket, szerződéseket és könyvelésre vonatkozó adatokat szereztek meg. A választás előtti napokban pedig egy „*EMLEAKS*" nevű felhasználó a *Pastebin* fájlmegosztó portálon tette közzé a megszerzett adatokat, a dokumentumok pedig *MacronLeaks* néven kezdtek terjedni a közösségi hálózatokon.[125] Nagy valószínűséggel ez az eset is teljesíti a beavatkozás tilalmának megsértésével kapcsolatos valamennyi feltételt. A választási rendszerekbe való beavatkozás mindenképp az állam belső ügyeibe való beavatkozást jelenti, megvalósul továbbá a kényszerítés is. Az egyetlen kérdéses fogalmi elem az, hogy a támadás betudható-e valamely államnak. A szakirodalom és a különböző jelentések egyértelműen az orosz felet jelölik meg a műveletek felelőseként, hozzá kell tenni azonban, hogy a francia állam sosem nevezte meg az oroszokat mint a támadás lehetséges elkövetőjét. Amennyiben azonban elfogadjuk, hogy a támadások hátterében egy állam (ebben az esetben éppen Oroszoroszág) áll, a beavatkozás tilalmának megsértéséről beszélhetünk.[126]

6. KONKLÚZIÓ

A fentiek alapján megállapító, hogy mind a szakirodalom, mind az állami gyakorlat egységes abban, hogy létezhetnek olyan kiberműveletek, amelyek elérhetik a fegyveres támadás szintjét. Hozzá kell tenni ugyanakkor azt, hogy jelenleg egyetlen olyan ellenséges célú kiberműveletről sem tudunk, amelyet valamely állam ekként értékelt volna. Ha a kiberművelet nem éri el ezt a súlyossági szintet, nem jelenti azt, hogy nemzetközi jogi értelemben mindig jogszerű lesz. Ilyenkor elsősorban az vizsgálandó, hogy a művelet sérti-e a nemzetközi jog valamely szabályát, úgy, mint az erőszak vagy a beavatkozás tilalmát.

[123] Abigail Abrams: „Here's What We Know So Far About Russia's 2016 Meddling" *Time* 2019. április 18., *https://time.com/5565991/russia-influence-2016-election/*.

[124] Geoff Cutmore – Arjun Kharpal: „Putin says claims that Russia interfered in US elections are lies" *CNBC* 2017. március 30., *https://www.cnbc.com/2017/03/30/putin-russia-trump-us-elections-lies.html*.

[125] Kim Willsher – Jon Henley: „Emmanuel Macron's campaign hacked on eve of French election" *The Guardian* 2017. május 6., *https://www.theguardian.com/world/2017/may/06/emmanuel-macron-targeted-by-hackers-on-eve-of-french-election*.

[126] Delerue (4. lj.) 254.

A szakirodalom egyetért abban, hogy a beavatkozás tilalmának megsértéséről akkor beszélhetünk, ha egy állam beavatkozik egy másik állam bel- vagy külügyeibe, mégpedig olyan területen, amelyek kizárólag az állam felelősségi körébe tartozik, és a céljuk, hogy meghatározott magatartásokat kényszerítsenek egy szuverén államra. E feltételek kidolgozása pedig a Nemzetközi Bíróság által a Nicaragua-ügy kapcsán történt meg.

Amennyiben a beavatkozás tilalma – vagy más nemzetközi jogi alapelv – sérül, a sértett államok számára lehetőség nyílik arra, hogy ellenintézkedést foganatosítsanak, vagy szükséghelyzetre hivatkozzanak. Mindkettő jogellenességet kizáró körülmény, közös továbbá bennük, hogy a rájuk való hivatkozás nem jogosítja fel a sértett államot arra, hogy *jus cogens*-nek minősülő nemzetközi jogi normát sértsen. Az ellenintézkedések kapcsán kiemelendő, hogy lehetőség szerint visszafordíthatónak kell lenniük, valamint fontos az arányosság követelményének betartása. A szükséghelyeztre pedig akkor lehet hivatkozni, ha „létfontosságú érdekek" kerülnek „súlyos és közvetlen" veszélybe, e fogalmak tartalma azonban a mai napig nem teljesen tisztázott.

Az elmúlt években jelentősen megnőtt a kibertér és a nemzetközi jog kapcsolatában nyilatkozatot tevő államok száma. Ezek az állami állásfoglalások, nyilatkozatok rendre foglalkoztak a beavatkozás tilalmának kérdésével is. A nyilatkozó államok egyetértenek abban, hogy a beavatkozás tilalma, mint nemzetközi jogi alapelv a kibertérben is alkalmazandó. Tartalmilag pedig azonos fogalmi elemeket tekintenek lényegesnek, mint a Nemzetközi Bíróság a Nicaragua-ügy kapcsán, az állami gyakorlat tehát párhuzamos a szakirodalommal a lényeges kérdések tekintetében, így kétséget kizáróan szokásjogi beágyazottságú szabályokról beszélhetünk. Egyes nyilatkozatok kiemelik ugyanakkor, hogy mindig esetről esetre szükséges vizsgálni azt, hogy sérül-e a beavatkozás tilalma, illetőleg egyes államok különböző példákat is említenek, amelyek szerintük a tilalom megsértésének minősülnek. Ezek közül pedig a választási rendszerekbe való beavatkozások élveznek megkülönböztetett figyelmet, különösen annak fényében, hogy megfigyelhető egy trend a választási rendszerek digitalizációja irányába is.[127]

Végezetül pedig szeretném kiemelni, hogy bár számos környező állam kiadta a hivatalos állásfoglalását, nyilatkozatát, Magyarország egyelőre adós maradt ezzel. Egy 2020-as, a Nemzeti Biztonsági Stratégiával kapcsolatos kormányhatározat ugyan megjegyzi: *„Magyarország a fizikai biztonságot veszélyeztető vagy jelentős anyagi károk okozására képes kiberképességeket fegyvernek, alkalmazásukat fegyveres agressziónak tekinti, amelyre a fizikai térben történő válaszadás is lehetséges. A kiberműveletek sokszor nehezen bizonyítható attribúciójára, az elkövető azonosítására, megnevezésére való tekintettel a válaszlépések különösen körültekintő, eseti elbírálást igényelnek az érintett kormányzati szervek bevonásával."*[128]

[127] Horváth Dominik: „Az országgyűlési választások digitalizációjának lehetősége Magyarországon" in Békési Gábor – Kiss Mátyás – Várallai Luca (szerk.): *A technológia és a jog korrelációja* (Pécs: Pécsi Tudományegyetem Állam- és Jogtudományi Kar Óriás Nándor Szakkollégium 2022) 69–71.

[128] *A Kormány 1163/2020 (IV.21.) Korm. határozata Magyarország Nemzeti Biztonsági Stratégiájáról* [101]. bek.

Ebből az következik, hogy megszületetett a magyar álláspont abban a nemzetközi jogi kérdésben, hogy tekinthető-e „fegyveres agressziónak" egy esetleges kibertámadás, és azzal szemben gyakorolható-e az önvédelem joga. A Stratégia e bekezdése szerint igen, amely Magyarország álláspontjának tekinthető.[129]Ez a dokumentum ugyanakkor csupán érintőlegesen rendelkezik a kérdésről, sem tartalmilag, sem terjedelmileg nem hasonlítható össze a fentebb tárgyalt állásfoglalásokkal. A kormányhatározat célja nem is a kibertér és a nemzetközi jog kapcsolatának értékelése volt, hanem az ország Nemzeti Biztonsági Stratégiájának az elfogadása.

[129] LATTMANN Tamás: „Egy szakmai észrevétel a nemzetbiztonsági törvény ma elfogadott módosításához" *Lattmann Tamás blogja* 2020. május 20., *https://lattmanntamas.hu/2020/05/20/egy-szakmai-eszrevetel-a-nemzetbiztonsagi-torveny-ma-elfogadott-modositasahoz/*.