A TALLINNI KÉZIKÖNYV 2.0: KIEMELÉSEK ÉS MEGLÁTÁSOK

ERIC TALBOT JENSEN*

ABSZTRAKT

A rosszindulatú kibertevékenységek világszerte áthatják az egyének életét és a nemzeti kormányok nemzetbiztonsági vitáit. Ritkán telik el úgy nap, hogy valamilyen kibernetikai esemény ne kerülne be az országos hírekbe. Ezek a rosszindulatú kibertevékenységek állami és nem állami szereplőknek, például nemzetközi bűnözői csoportoknak, terrorista szervezeteknek és magánszemélyeknek egyaránt tulajdoníthatók.

Erre a széles körben elterjedt jelenségre - beleértve egy 2007-ben Észtországban történt jelentős kiberincidenst is - válaszul az észtországi Tallinnban működő Cooperative Cyber Defense Center of Excellence többéves folyamatnak adott otthont, amelynek célja, hogy neves szakértők egy csoportjának véleményét ismertesse a nemzetközi jognak a kibertevékenységekre való alkalmazásáról. Az első tallinni kézikönyv a fegyveres összeesküvésre alkalmazandó joggal foglalkozott. A második, nemrégiben kiadott Tallinni Kézikönyv (Tallinn 2.0 néven) a kiberműveletek sokkal szélesebb körével foglalkozik - a fegyveres konfliktuson belüli és kívüli kiberműveletekkel egyaránt.

Ez a cikk röviden összefoglalja a Tallinni Kézikönyv 2.0 legfontosabb pontjait, beleértve a Kézikönyvet író szakértők között a konszenzus hiányának néhány legfontosabb területét. A cikk ezután betekintést nyújt abba, hogy a kiberműveletekre vonatkozó nemzetközi jognak merre kell haladnia a jövőben.

* Jogászprofesszor, Brigham Young Egyetem Jogi Kar. Jensen professzor tagja volt a Tallinn 1.0 és a Tallinn 2.0 nemzetközi szakértői csoportnak.

I. BEVEZETÉS

A rosszindulatú kibertevékenységek életünk normális részévé váltak. Nem nemcsak a kibereseményekjelennek meg rendszeresen a hírekben,[1] hanem ezek is megragadják a filmnézők fantáziáját[2] és a televíziónézők fantáziáját, [3] és végtelen intrikát nyújtanak az irodalomban.[4] Sokan ezek közül a fizikai A forgatókönyvek olyan súlyos kibernetikai támadásokat tartalmaznak, amelyek katasztrofális következményekkel járnak, és gyakran országok közötti fegyveres konfliktushoz vezetnek.[5]

Szerencsére ilyen kiberforgatókönyv még nem fordult elő a való életben. Ehelyett a rosszindulatú kibertevékenységek túlnyomó többsége messze az államok közötti fegyveres konfliktus küszöbértéke alatt zajlik, és nem emelkedik olyan szintre, amely egy ilyen konfliktust kiváltana. A hírekben oly gyakori kibertevékenységek többsége inkább a vállalatok ellopását foglalja magában. árfolyam- hamis információk terjesztése,[7] vagy a titkok,[6]

---

1. *Lásd pl.* Juliet Eilperin & Adam Entous, *Russian Operation Hacked a Vermont Utility, Showing Risk to U.S. Electrical Grid Security, Officials Say*, WASH. POST (2016. dec. 21.), https://www.washingtonpost.com/world/national-security/russian-hackers-penetrated-us-electricity-grid through-a-utility-in-vermont/2016/12/30/8fc90cc4-ceec-11e6-b8a2-8c2a61b0436f_story.html?utm_term=.8cf73411023c.

2. BLACKHAT (Legendary Entertainment 2015); Elizabeth Weise, *Eight All-time Great Hacking Movies*, USA TODAY (2015. január 14. 12:08), https://www.usatoday.com/story/tech/2015/01/14/hacking-movies-list-cyber-blackhat/21713327/.

3. *Lásd pl.* , *CSI: Cyber*, CBS, http://www.cbs.com/shows/csi-cyber/ (utolsó látogatás 2017. június 7.) (amerikai televíziós dráma, amely kiberbűncselekmények rendőrségi nyomozásával foglalkozik); *Good or Bad, Here Are 4 New Hacker TV Shows That Debuted in 2015*, CLOUDBRIC, https://www.cloudbric.com/blog/20 15/07/good-or-bad-here-are-4-new-hacker-tv-shows-debuted-in-2015/ (utolsó látogatás 2017. június 1.).

4. *Lásd pl.* , Diane Biller, *Here Are 21 Essential Cyberpunk Books That You Absolutated Should Read*, GIZMODO (2016. január 2., 16:15) https://www.gizmodo.com.au/2016/01/the-essential-cyberpunk olvasólista/.

5. Az egyik első ilyen film a "Háborús játékok" volt, amely egy elromlott védelmi számítógép történetét meséli el, amely nukleáris háború kirobbanásával fenyeget. WAR GAMES (United Artists 1983).

6. *Lásd pl.* , James Griffiths, *Cybercrime Costs the Average U.S. Firm $15 Million a Year*, CNN TECH (2015. október 8., 3:28), http://money.cnn.com/2015/10/08/technology/cybercrime-cost business/.

7. Rebecca Greenfield, *Look What the Hacked AP Tweet About White House Bombs Did to the*

Market, THE ATLANTIC (2013. április 23.), https://www.theatlantic.com/technology/archive/2013/04/hacked-ap-tweet-white-house-bombs-stock-market/315992/.

8

kormányzati számítógépeket, hogy megpróbáljanak államtitkokat ellopni.[8] Mindazonáltal a kiberhacking jelentősége valósággá vált. több millió ember számára, akiknek személyes adatait kibernetikai eszközökkel ígérték meg.[9] Az ilyen kibereseményekgyakorisága, valamint az államokra és a nemzetközi közösség egészére jelentett kockázatok arra kényszerítették mind az államokat[10] , mind a multinacionális szervezeteket[11] , hogy felfigyeljenek rájuk és megoldásokat keressenek. E multinacionális szervezetek közé tartozik az Észak-atlanti Szerződés Szervezete (NATO), amelynek az észtországi Tallinnban működő Cooperative Cyber Defense Center of Excellence (CCD COE)[12] ( ) segített az eredeti, a kiberhadviselésre alkalmazandó nemzetközi jogról szóló tallinni kézikönyv (Tallinn Manual 1.0)[13] és az újonnan kiadott, a kiberműveletekre alkalmazandó nemzetközi jogról szóló Tallinn Manual 2.0 elkészítésében.[14] A Tallinn 1.0 tartalma a Tallinn 2.0-ban is megjelenik, bár az eredeti kiadás óta történt pontosítások miatt némileg módosított formában.

Ez a cikk röviden összefoglalja a Tallinni Kézikönyv 2.0 (a továbbiakban: a Kézikönyv) legfontosabb pontjait, beleértve a jogi szakértők között nem létező konszenzus néhány legfontosabb területének azonosítását, amelyeken a kézikönyvet író jogi szakértők nem értettek egyet.

---

8. *Lásd pl.* Ryan O'Hare, *China Proudly Debuts its New Stealth Jet it Built 'by Hacking into US Computers and Stealing Plans'*, DAILY MAIL (2016. november 1., 06:57 EDT), http://www.dailymail.co.uk/ sciencetech/article-3893126/Chinese-J-20-stealth-jet-based-military-plans-stolen-hackers-makes public-debut.html (az új kínai repülőgép állítólag nagyrészt amerikai repülőgépek lopott terveit vette alapul).

9. *Lásd* Sam Thielman, *Yahoo Hack: 1bn Accounts Compromised by Biggest Data Breach in History*, THE GUARDIAN (2016. december 15., 19:23), https://www.theguardian.com/technology/2016/dec/14/yahoo-hack-security-of-one-billion-accounts-breached.

10. *Lásd:* James R. Clapper nyilatkozata a Szenátus Fegyveres Szolgálatok Bizottsága előtt, Worldwide Threat Assessment of the US Intelligence Community 1- 4 (2016. február 9.), https://www.armed-services.senate.gov/imo/media/doc/Clapper_02-26-15.pdf; *lásd még* U.K. CABINET OFFICE, THE UK CYBER SECURITY STRATEGY 2011-2016: ANNUAL REPORT (2016), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/516331/UK_Cyber_Security_Strategy_Annual_Report_2016.pdf.

11. *Lásd* a Kormányzati Szakértői Csoport jelentése az információ és a távközlés területén a nemzetközi biztonság összefüggésében bekövetkezett fejleményekről, UN Doc. A/70/174 (2015. július 22.) [a továbbiakban: UN Doc. A/70/174]; Rep. of the Group of Governmental Experts on the Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/68/98 (2013. június 24.) [a továbbiakban: UN Doc. A/68/98].

12. NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE (CCDCOE), https://ccdcoe.org/ (utolsó látogatás 2017. június 1.).

13. TALLINN MANUAL ON INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael N. Schmitt szerk., 2012) [a továbbiakban: TALLINN MANUAL 1.0].

14. TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS (Michael N. Schmitt szerk., 2d. kiadás 2017) [a továbbiakban: TALLINN MANUAL 2.0].

a kézikönyv. A cikk megkísérel betekintést nyújtani abba is, hogy a jövőben merre kell majd haladnia a kiberműveletekre vonatkozó nemzetközi jognak.

II. A FOLYAMAT

Mindkét tallinni kézikönyvet nemzetközi jogi szakértőkből álló csoportok (a szakértők) írták:[15] a CCD COE és Michael N. Schmitt,[16] , a világ egyik kiemelkedő kibervédelmi szakértője. Az első csoportban a fegyveres összeütközések jogának (LOAC) szakértői elsősorban a nyugati félteke országaiból kerültek ki. A kritikákra reagálva a Tallinn 2.0 nemzetközi szakértői csoport mind eredetét (Thaiföldről, Japánból, Kínából és Fehéroroszországból származó tagokkal), mind pedig érdemi szakértelmét tekintve (emberi jogi, űrjogi és nemzetközi távközlési jogi szakértőkkel) szélesebb körű volt. A Vöröskereszt Nemzetközi Bizottságát (ICRC), valamint más államokat és szervezeteket is felkértek, hogy küldjenek megfigyelőket mindkét csoportba.

A projekt célja soha nem az volt, hogy törvényt alkosson, vagy olyan kézikönyvet készítsen, amely törvényerővel bír. Amint azt a bevezetés világossá teszi:

> A Tallinni Kézikönyv 2.0 végső soron csak a két nemzetközi szakértői csoport véleményét fejezi ki a jogi helyzetről.
> a kézikönyvnek a két nemzetközi szakértői csoport által 2016 júniusában történt elfogadásakor hatályos jogszabálynak az újbóli átdolgozása. Az In nem "legjobb gyakorlatok" útmutatója, nem képviseli a "jog progresszív fejlődését", és szakpolitikai és politikai szempontból semleges. Más szóval a Tallinni Kézikönyv 2.0 a *lex lata* objektív újrafogalmazásának szánja.[17]

Az eljárások némileg különböztek a kézikönyvek anyagának eredetét illetően, de mindkét esetben az anyag fiatalizálására irányuló eljárás ugyanaz volt. A szabályok, amelyek mindkét Kézikönyvben vastag, fekete betűkkel szerepelnek, konszenzust igényeltek, tehát minden egyes szabállyal kapcsolatban valamennyi szakértőnek egyet kellett értenie. A Kézikönyvben minden egyes szabály után egy meglehetősen terjedelmes megjegyzés következik.

---

15. A szerző mindkét nemzetközi szakértői csoportnak tagja volt. A nemzetközi szakértői csoport tagjairól és a TALLINN MANUAL 1.0 kiadásában részt vevő egyéb résztvevőkről lásd: TALLINN MANUAL 2.0, 14. lábjegyzet, xix-xxii. A TALLINN KÉZIKÖNYV 2.0 kiadásában részt vevőkre vonatkozóan lásd *id.* xii-xviii.

16. *Kar: Schmitt*, U.S. NAVAL WAR COLLEGE, https://usnwc.edu/Faculty-and Departments/Directory/Michael-N-Schmitt (utolsó látogatás 2017. június 1.).

17. TALLINN MANUAL 2.0, *fentebb* 14. lábjegyzet, 2-3. pont.

tary, normál betűtípussal előállítva az egyértelműség érdekében a szabályból. A kommentár tartalmazza a definíciókat, a szabályok magyarázatát, a szabály alkalmazásának részleteit, forgatókönyveket és példákat, és ami a legfontosabb, azonosítja azokat az eseteket, amikor a szakértők nem tudtak megegyezni a szabály egy adott szempontjában.

A szakértők például egyetértettek abban, hogy az előíró állampolgársági joghatóság egy állam állampolgáraira akkor is vonatkozik, ha azok a tengerentúlon tartózkodnak, de abban nem értettek egyet, hogy az adott személy adatai az állampolgár államának extraterritoriális végrehajtási joghatósága alá tartoznak-e. A szabály, amelyben valamennyi szakértő egyetértett, kimondja, hogy "Egy állam a kibertevékenységek tekintetében extraterritoriális előíró joghatóságot gyakorolhat: (a) az állampolgárai által folytatott; . . . "[18] , de egy későbbi szabályhoz fűzött kommentár szerint:

> Meg kell jegyezni, hogy néhány szakértő különbséget tett a polgárok kibertevékenységére vonatkozó előíró joghatóság és az e tevékenységek során létrehozott adatokra vonatkozó joghatóság között. Úgy vélték, hogy az államnak az adatokra vonatkozó joghatósága gyakran nem azonosítható az állampolgárai kibertevékenységei feletti joghatóságával. Abban azonban valamennyi szakértő egyetértett, hogy az adatok feletti teljes joghatósággal az az állam rendelkezik, ahol az adatok találhatók.[19]

Ez a szakasz rámutat a folyamat egy másik kulcsfontosságú részére - arra, hogy a Kézikönyv hogyan kezeli a konszenzus hiányát. Amikor a szakértők nem értettek egyet, a Kézikönyv többféleképpen is megjegyzi ezt a nézeteltérést. Ahol a csoport többségi és kisebbségi megosztottságot mutatott, a Kézikönyv ezt a tényt is megemlíti: [20] . Amikor a csoport tovább oszlott, a Kézikönyv gyakran használja a "[s]ome of the experts"[21] leírást - általában több vagy kisebbségben lévő szakértőt értve ezalatt. Időnként a Kézikönyv megjegyzi, hogy "[néhány] szakértő"[22] egy bizonyos nézetet képviselt. Ez általában azt jelenti, hogy a szakértők közül csak egy vagy néha kettő képviselte az adott nézetet. És végül

---

18. TALLINN MANUAL 2.0, 14. lábjegyzet, 60. r. 10. a) pont.

19. *Id.* at 63, ¶ 8.

20. *Lásd pl.* , *id.* at 19, ¶ 7 ("Ebben a tekintetben a szakértők megosztottak a kiberkémkedés (32. szabály) egyedi esetét illetően, amelyet egy állam végez, miközben fizikailag jelen van egy másik állam területén. A többség azon az álláspontón volt, hogy a tevékenység sérti ezt a szabályt.").

21. Például az ellenintézkedések alkalmazásával kapcsolatban a TALLINN MANUAL 2.0 előírja: "Néhány szakértő azonban ezzel ellentétes álláspontot képviselt. Megközelítésük szerint például a sértett államnak a kiber-ellenintézkedések megtétele előtt meg kellene kísérelnie a rendelkezésre álló kiber-visszavágási cselekményeket, ha azok valószínűleg arra késztetnék a felelős államot, hogy eleget tegyen kötelezettségeinek.". *Id.* at 118, ¶ 4.

22. Az emberi jogok alkalmazásával kapcsolatban például a TALLINN MANUAL 2.0 a következőket írja elő: "A szakértők közül néhányan úgy foglaltak állást, hogy mindaddig, amíg a jog gyakorlása vagy élvezete

olyan jogos nézetek voltak, amelyekről a szakértők tudták, hogy léteznek, de amelyeket egyik szakértő sem vallott. Ezekben az esetekben a Kézikönyv általában azt írja, hogy "a szakértők elismertek egy nézetet".[23]

Amint a szakértők befejezték a Tallinn 2.0 szövegét, a holland kormány több találkozót kezdeményezett az államokkal, amelyeken a kézikönyv tartalmát áttekinthették és véleményezhették, mielőtt azt véglegesítették volna. Több mint ötven állam, köztük a Biztonsági Tanács valamennyi állandó tagja élt ezekkel a találkozókkal. Ez a hozzájárulás - bár nem feltétlenül került bele a Kézikönyvbe, mivel a Kézikönyv a szakértők álláspontját tükrözi - felbecsülhetetlen értékű betekintést nyújtott abba, hogy az államok hogyan látják a nemzetközi jog végrehajtását a kiberműveletek tekintetében.

Ezenkívül a kézikönyv egyes részeit elküldték a "szakértőknek", hogy az ő véleményüket is kikérjék. Miután az összes külső vélemény beérkezett, mind az államoktól, mind a szakértőktől, azokat a szakértők elé terjesztették megfontolásra a szabálytervezetek és a kommentárok véglegesítése során.

Ez a széles körű folyamat, különösen a Tallinn 2.0 tekintetében, lehetővé tette a nézetek és a szakértelem sokkal szélesebb körének figyelembevételét és lehetséges elfogadását, mint amennyit bármely más forrásból összegyűjtöttek. Így a tallinni kézikönyvek egyedülálló és átfogó állami mentést nyújtanak a kiberműveletekre alkalmazandó nemzetközi jogról.

III. A KÉZIKÖNYV

A kézikönyv négy részre oszlik. Az I. rész az általános nemzetközi joggal és a kibertérrel foglalkozik. A II. rész a nemzetközi jog és a kibertér speciális rendszereivel foglalkozik. A III. rész a nemzetközi békével és biztonsággal, valamint a kibertevékenységekkel foglalkozik, amely főként a tallini
1.0. A IV. rész pedig a Tallinn 1.0 többi része, és a kiberjogra vonatkozik fegyveres konfliktus. Mivel a Tallinn 1.0-t már részletesen kommentálták, ez a cikk kizárólag az I. és II. részre és a III. rész egy kis részére támaszkodik.

A. *Szuverenitás*

A kézikönyv a szuverenitásról szóló értekezéssel kezdődik, és az első szabályban leszögezi, hogy "[a] szuverenitás elve a következőkre vonatkozik:".

---

a kérdéses emberi jog valamely állam hatáskörébe vagy tényleges ellenőrzésébe tartozik, az adott állam az érintett jog tekintetében hatalommal vagy tényleges ellenőrzéssel rendelkezik az egyén felett." *Id.* 185. pont, 10. bekezdés.

23. Például a diplomáciai és konzuli helyiségek sérthetetlenségének tárgyalásakor a TALLINN MANUAL 2.0 előírja: "A szakértők elismerték azt a nézetet, amelyet egyikük sem vallott, miszerint a diplomáciai képviselet helyiségeinek sérthetetlensége abszolút." *Id.* 214,7. pont.

kibertérben."[24] Az ezt követő két szabály különbséget tesz a belső és a külső szuverenitás között,[25] és a 4. szabály kimondja, hogy "[egy] állam nem folytathat olyan kiberműveleteket, amelyek sértik egy másik állam szuverenitását".[26] A szakértő 4. szabályban megfogalmazott következtetésének alapjául szolgáló feltételezés az, hogy a szuverenitás a nemzetközi jog olyan szabálya, amelynek megsértése a nemzetközileg jogellenes cselekmény. A 4. szabály magyarázata kimondja:

> A kibernetikai kontextusban tehát a területi szuverenitás megsértésének minősül, ha egy állam szerve vagy olyan személyek, akiknek a magatartása az államnak tulajdonítható, egy másik állam területén fizikailag jelen lévő kibernetikai műveleteket hajtanak végre az adott állam vagy az ott található szervezetek vagy személyek ellen. Ha például egy állam ügynöke egy USB flash meghajtót használ arra, hogy egy másik államban található kiberinfrastruktúrába rosszindulatú programot juttasson be, akkor a szuverenitás megsértése valósul meg.[27]

Ez a "szuverenitás mint uralom" megközelítés nem általánosan elfogadott. Gary Corn ezredes, az amerikai kiberparancsnokság vezető jogi tanácsadója szerint:

> Az ezzel ellentétes nézet szerint a szuverenitás a westfáliai nemzetközi rend alapelve, amely olyan kötelező erejű normákat támaszt alá, mint az ENSZ Alapokmány 2. cikkének (4) bekezdésében foglalt erőszak alkalmazásának tilalma, vagy a nemzetközi szokásjognak a be nem avatkozás tilalmára vonatkozó szabálya, amelyet az államok szuverén egyenlőségük gyakorlásaként fogadtak el.[28]

E megközelítés szerint a szuverenitás olyan szabályokban jelenik meg, mint az erőszak alkalmazásának tilalma és a beavatkozás tilalmának szabálya, de önmagában nem képez végrehajtható szabályt.

Létezik egy harmadik, ebben a dokumentumban kifejtett nézet is a szuverenitásnak a kiberműveletekre való alkalmazásáról. E nézet szerint a szuverenitás egy elv

---

24. *Id.* a 11. r. 1. pontnál.

25. A TALLINN MANUAL 2.0 2. szabálya kimondja, hogy "Az állam a területén található kiberinfrastruktúra, személyek és kibertevékenységek tekintetében - nemzetközi jogi kötelezettségeire is figyelemmel - szuverén hatalmat élvez". *Id.* 13. r. 2. A 3. szabály kimondja, hogy "Egy állam nemzetközi kapcsolataiban szabadon folytathat kibertevékenységeket,

figyelemmel a rá nézve kötelező nemzetközi jog bármely ellentétes szabályára". *Id.* 16. pont 3. r. 3. alpont.

26. *Id.* 17. r. 4. pont.

27. *Id.* at 19, ¶ 6.

28. Gary Corn, *Tallinn Manual 2.0 -Advancing the Conversation*, JUST SECURITY (2017. február 15., 8:41), https://www.justsecurity.org/37812/tallinn-manual-2-0-advancing-conversation/#more 37812.

amely az államok területétől és gyakorlati szükségleteitől függ, és az államközi alkalmazás során kiigazításra szorul. Briefly szembeállítása azzal, hogy hogyan kezelik a szuverenitást a levegő, a szárazföld, a tenger és a világűr területi alapú rendszereiben, jól szemlélteti a lényeget.

Történelmileg a szuverenitás megelőzte a modern állam létrejöttét, és a fejedelemtől mint uralkodótól ered.[29] A modern állam kialakulásával a nemzetközi jogot az államok alakították ki, amelyek a szuverenitás doktrínáját a tények vagy az állami kölcsönhatás egyes eseteire alkalmazták. Például a szárazföldi területet tekintve a szuverenitást másképp alkalmazták a diplomatákra és a kémekre, mint más államok állampolgáraira. A kémkedés tekintetében az államok a kémkedést önmagában nem tekintették a szuverenitás megsértésének, még akkor sem, ha a kémkedés egy másik államban történik és/vagy más államban fejti ki hatását. Az államok a kémkedés módszereit a belső jog alapján rendszeresen törvényen kívül helyezik, de nem a szuverenitás megsértéseként. Hasonlóképpen, jóval a szerződések jogáról szóló bécsi egyezmény[30] kihirdetése előtt a nemzetközi szokásjog mentességet biztosított a más államok területén lévő diplomáciai létesítmények és személyek számára. Bár az államok a szuverenitás elvének alkalmazását a szárazföldi területekre vonatkozóan e két esetben eltérő módon alakították ki, ezek alátámasztják azt az állítást, hogy a szuverenitás egy olyan elv, amelyet az államok gyakorlati szükségletei alapján alkalmaznak, nem pedig a nemzetközi jog egységes szabályaként.

A szuverenitás alkalmazásának összehasonlítása a levegő, a világűr és a tenger területén szintén tanulságos.[31] Ezekben az esetekben a szuverenitás

---

29. *Lásd általában* PHILIP BOBBITT, THE SHIELD OF ACHILLES (2002) (a szuverenitás doktrínájának nyomon követése a történelem során egészen a modern alkalmazásig).

30. A szerződések jogáról szóló bécsi egyezmény, 1969. május 23., 1155 U.N.T.S. 331, 8 I.L.M. 679.

31. Az Egyesült Államok Védelmi Minisztériuma értékelése a nemzetközi jogi kérdésekről az információs tion Operations hasznos módon szembeállítja a szuverenitást a levegő, a világűr és a tenger területére vonatkoztatva:

> A nemzetközi közösség általában nem tárgyal szerződéseket a problémák kezelésére, amíg azok következményei nem kezdenek érezhetővé válni. Ez nem mindenben rossz, mivel a megoldást a ténylegesen felmerült problémákhoz lehet igazítani, nem pedig a hipotetikus lehetőségek köréhez. Az egyik következmény azonban az, hogy az így létrejövő jogot - legyen az hazai vagy nemzetközi - erősen befolyásolhatja a jogi fejleményeket előidéző események jellege, a hozzájuk kapcsolódó politikai és politikai megfontolásokkal együtt.

Jó példa erre a művi földi műholdakra vonatkozó nemzetközi jog fejlődése. Ha a nemzetek tökéletes előrelátással leültek volna, és feltették volna maguknak a kérdést: "Engedélyezzük-e, hogy azok a nemzetek közülünk, amelyek fejlett technológiához férnek hozzá, olyan műholdakat állítsanak pályára, amelyek a többiek területe felett elhaladva nagy felbontású képeket készítenek, lehallgatják a távközlésünket, rögzítik az időjárási információkat,

a nemzetközi közösség az államok gyakorlatától függően eltérően alkalmazza e területeken, ami eltérő jogi paradigmákat eredményez. A jogi következetesség hiánya ezeken a területeken különösen nehézzé teszi a kibertérre alkalmazandó szabály megfogalmazását. Az eddigi állami gyakorlat alapján úgy tűnik, hogy az államok úgy alkalmazzák a szuverenitást a kibertérrel kapcsolatban, hogy az nem zárja ki a másik állam infrastruktúráján és területén végzett kibertevékenységeket, beleértve az egyik állam által hozott olyan intézkedéseket, amelyek nem sértik a másik állam eredendően kormányzati funkcióit.

Ami egyértelműnek tűnik, az az, hogy - ahogyan azt Brian Egan, a Külügyminisztérium korábbi jogi tanácsadója megállapította - a nemzetközi közösség jelenleg "a nyilvános állami gyakorlat viszonylagos vákuumával szembesül".[32] Mike Schmitt is ezt hangoztatta a Tallinni Kézikönyv 2.0 amerikai bemutatóján. Arra a kérdésre, hogy a Kézikönyv melyik része fog a legvalószínűbben változni a következő fizetésben, azt válaszolta, hogy szerinte az lesz az, hogy az államoknak tisztázniuk kell a szuverenitással kapcsolatos álláspontjukat.[33] Ismét Brian Egan érvelése szerint "[a]z államoknak nyilvánosan ki kell fejteniük álláspontjukat arról, hogy a meglévő nemzetközi jog hogyan alkalmazandó az államok kibertérben tanúsított magatartására a lehető legnagyobb mértékben.

és közvetlenül a határainkon belüli telefonokra és számítógépekre sugározni az információkat?", akkor az űrjog nagyon korlátozó rendszere alakulhatott volna ki. Ehelyett az történt, hogy a Szovjetunió és az Egyesült Államok által felbocsátott első műholdakat teljesen jóindulatú, tudományos kutatással foglalkozó eszközöknek tekintették, és az is teljesen világos volt, hogy egyetlen nemzetnek sem áll módjában beavatkozni azokba, amikor azok a területe felett haladnak el. Ilyen körülmények között gyorsan elfogadott nemzetközi szokásjoggá vált, és hamarosan a világűrről szóló szerződésben is rögzítésre került, hogy a Föld körüli pályán keringő objektumok bármely nemzet területi igényein kívül esnek, és hogy a világűr mindenki számára hozzáférhető.

Az űrjog története éles ellentétben áll a légi jogéval. A levegőnél nehezebb légi közlekedés korai fejlődésének nagy része egybeesett az első világháborúval, amelynek során világosan megmutatkozott a repülőgépek katonai ereje a hírszerzés, a szárazföldi erők megtámadása és az ellenséges városok bombázása terén. Ennek eredményeképpen a légtérjog rendkívül korlátozott rendszere alakult ki, amelyben egy nemzet légterébe való engedély nélküli belépést a szuverenitás és a területi integritás súlyos megsértésének kellett tekinteni.

U.S. DEPARTMENT OF DEFENSE OFFICE OF GENERAL COUNSEL, AN ASSESSMENT OF INTERNATIONAL LEGAL ISSUES IN INFORMATION OPERATIONS 2 (2d ed. Nov. 1999).

32. Brian Egan, a Külügyminisztérium jogi tanácsadója, Remarks on International Law and Stability in Cyberspace at Berkeley Law 5 (2016. november 10.), https://www.justsecurity.org/wp-content/ uploads/2016/11/Brian-J.-Egan-International-Law-and-Stability-in-Cyberspace-Berkeley-Nov-201 6.pdf [a továbbiakban: Egan Remarks].

33. Michael N. Schmitt, Az Atlanti Tanács ülésén elhangzottak: Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, (2017. február 8.), http://www.atlanticcouncil.org/ blogs/new-atlanticist/tallinn-manual-2-0-defending-cyberspace (áttekintést nyújt az általános vitáról). A specific pont a szerző által a találkozón Schmittnek feltett kérdésen alapul.

nemzetközi és hazai fórumokon lehetséges."[34] Erre a kérdésre csak a szuverenitás és a kiberképességek kölcsönhatásával kapcsolatos állami álláspontok tisztázása adhat választ.

B. *Átvilágítás*

A kellő gondosság nem a nemzetközi jog anyagi jogi rendelkezése, hanem inkább az a norma, amelyet az államoknak alkalmazniuk kell annak megakadályozására, hogy területüket határokon átnyúló károkozásra használják fel.[35] A Tallinni Kézikönyv 6. szabálya szerint "az államnak kellő gondossággal kell eljárnia annak érdekében, hogy ne engedje meg, hogy területét vagy a kormányzati ellenőrzése alatt álló területet vagy kiberinfrastruktúrát olyan kiberműveletekre használják fel, amelyek más államok jogait érintik, és más államok számára súlyos hátrányos következményekkel járnak".[36] Ennek a szabálynak több fontos aspektusa van. Először is, a szabály elismeri, hogy az államoknak a kellő gondosság alkalmazására vonatkozó kötelezettsége valójában a nemzetközi jog egyik szabálya. Hogy mikor és milyen mértékben kell ezt a szabályt alkalmazni, az még vita tárgya, de az a tény, hogy a szabály létezik és az államokra vonatkozik, a szakértők nem vitatták.[37]

Az államok nem kötelesek minden határokon átnyúló kárt orvosolni, csak azt a kárt, amely súlyos káros következményekkel jár. Feltételezhető, hogy a kár bizonyos szintje nem éri el azt a küszöbértéket, amely a kellő gondosság elvét kiváltja.[38] Annak ellenére, hogy a szabályban ezt a megfogalmazást használták, a tallinni szakértők nem tudták teljes mértékben leírni, hogy mit jelentenek a "súlyos káros következmények". Sőt, arra a következtetésre jutottak, hogy a nemzetközi jog e tekintetben nem egyértelmű.[39] A szakértők azonban azzal érveltek, hogy nem volt szükség "tárgyak fizikai károsodására vagy személyek sérülésére".[40]

Ahhoz, hogy egy állam felelős legyen az országhatárokon átterjedő károk megelőzésére irányuló kellő gondosság alkalmazásáért, az államnak tudnia kell a kárról. Ez a tudás lehet vélelmezett tudás, ha az államnak az események szokásos menetében tudnia kellett volna vagy objektív módon tudnia kellett volna a kárról.[41] Ez a nézet azonban nem követeli meg az államtól, hogy megelőző intézkedéseket tegyen kiberinfrastruktúrájával, a[42] vagy akár az infrastruktúra monitorozásával.

---

34. Egan Remarks, *Supra* 33. lábjegyzet, 7. pont.
35. TALLINN MANUAL 2.0, 14. lábjegyzet, 30. r. 6. pont.
36. *Id.* r. 6.
37. *Id.* 31. pont, 4.
bekezdés. 38. *Id.*
36. pont, 22.
bekezdés.
39. *Id.* 36-37. pont, 25. n. 48. pont.
40. *Id.* 37-38, 28. pont.
41. *Id.* 41. pont, 39. bekezdés.

42. *Id.* 439. o., a 44 - 45, ¶ 7, a munkások és az egyéb résztvevők, akik részt vettek a 44 - 45, ¶ 7. o. közzétételében.

ture, hogy tájékozódhassunk a lehetséges határokon átnyúló károkról.[43] Abban a pillanatban, amikor egy állam tudomást szerez az országhatárokon átterjedő kárról, köteles "minden olyan intézkedést megtenni, amely az adott körülmények között megvalósítható a kiberműveletek megszüntetése érdekében".[44] Más szóval, az államnak meg kell tennie az "ésszerűen rendelkezésre álló és gyakorlatias" intézkedéseket,[45] bár az, hogy ezt milyen eszközökkel éri el, az állam belátása szerint történik. amelyből a kár származik.[46]

Az államok általában nem szeretik a kellő gondosság elvét, mert az bizonyos mértékű felelősséget ró rájuk. Az Egyesült Nemzetek Kormányzati Szakértői Csoportjában (UN GGE) az államok csak azt voltak hajlandóak elismerni, hogy a kellő gondosságot "kellene" gyakorolniuk, nem pedig azt, hogy "kell", ahogyan azt a szabály kimondja.[47] Ha azonban a szuverenitás korábbi elvével együtt elemezzük, még a szakértők által javasolt szabvány is nagy rést hagy, ahol a kiberkárok áldozatai kevés jogorvoslati lehetőséggel maradnak.

Tegyük fel például, hogy egy A államban lévő terrorista szervezet B államon keresztül káros kibertevékenységet folytat C államban lévő szervezetek ellen. Mind az A, mind a B államnak nincs affirmatív kötelezettsége, amíg nem tudnak a károkozásról. Mivel nincs ellenőrzési vagy megelőzési kötelezettségük, A és B állam valószínűleg csak azután szerez tudomást a károkozásról, hogy C állam elegendő kárt szenvedett ahhoz, hogy számítógépes törvényszéki vizsgálatot végezzen, és meghatározza, honnan származik a kár.

Még ha a C állam tudja is, hogy honnan származik a kár, nem tud semmilyen proaktív intézkedést - például ellenintézkedéseket - tenni, amelyekről alább lesz szó, mivel a kárt nem állami szereplő okozza. Így C állam teljes mértékben függ attól, hogy A és B állam elfogadja-e C állam állítását, A és B állam megállapítja-e, hogy az igaz, és hogy a kár a területükről származik-e (beleértve a tények megállapításához szükségesnek tartott időt és eljárást), elemzi-e, hogy mit lehetne tenni a kár elhárítása érdekében, és meghatározza, milyen megvalósítható intézkedéseket fog végrehajtani a határokon átnyúló kár megállítása érdekében.

Erre egyesek azzal érvelhetnek, hogy ez nem különbözik a kellő gondosság elvének alkalmazásától a nemzetközi jog más területein, például a nemzetközi környezetvédelmi jogban. Azonban a

---

43. *Id.*

44. *Id.* 43. r. 7.

45. *Id.* , ¶ 2.

46. *Id.* 44. pont, 6. bekezdés.

47. *Lásd* UN Doc. A/70/174, *Supra* note 11, 13(c), 28(e) b e k e z d é s ; 23. b e k e z d é s , UN Doc. A/68/98, *supra*

11. megjegyzés, 23. pont.

Az alapvető különbségek közé tartozik, hogy a határokon átnyúló környezeti károk gyakran átláthatóbban jelentkeznek, és gyakran könnyebb a felelősség megállapítása. Emellett a környezeti károk gyakran a fogadó államban is kifejthetik hatásukat a károsult államba vezető úton, ami nagyobb ösztönzést jelent a fogadó állam számára, hogy lépéseket tegyen. A környezeti károk általában egybefüggőek, és olyan szomszédokat érintenek, amelyeknek több érdekük lehet. És figyelem, kevés bizonyíték van arra, hogy az államok meghatalmazottakat használnának arra, hogy környezeti károkat okozzanak szomszédaiknak, így kevés ösztönzőt hagyva a kár tagadására vagy a jogorvoslat késleltetésére. A rosszindulatú kibertevékenységek esetében azonban egészen más a helyzet, és számos olyan állítással találkozunk, amelyek szerint az államok proxykat használnak kibertevékenységek végzésére, különösen azzal a szándékkal, hogy megtagadhassák a felelősségre vonást.[48]

Tekintettel arra, hogy a szuverenitás az egyik legnagyobb nyomás alatt álló elv, a kellő gondosság pedig a nyomásgyakorlás egyik fő eszköze, ezt a területet a következő években nagy érdeklődéssel kell követni, ahogy az állami gyakorlat fejlődik.

C. *Joghatóság*

A Kézikönyv joghatóságról szóló fejezete hat szabályt és kiterjedt kommentárt tartalmaz. A joghatóságot úgy definiálják, mint "az államok hatáskörét a személyek, tárgyak és magatartások szabályozására nemzeti joguk alapján, a nemzetközi jog által megszabott korlátokon belül".[49] A joghatóságra vonatkozó első szabály kimondja, hogy "[a] nemzetközi jogban meghatározott korlátozások mellett egy állam területi és területen kívüli joghatóságot gyakorolhat a kibertevékenységek felett".[50] Ez azt jelenti, hogy "elvben a kibertevékenységekre és az azokat végző személyekre ugyanazok a joghatósági előjogok és korlátozások vonatkoznak, mint a tevékenység bármely más formájára".[51]

A kézikönyv a joghatóság három hagyományos típusával - előíró, végrehajtó és ítélkezési joghatóság - foglalkozik, és mindegyiknek a legfontosabb szempontjait tárgyalja. Az előíró joghatóság tekintetében a Kézikönyv kifejti, hogy az államok alapvetően korlátlanok az előíró joghatóság tekintetében a szuverén területükön belül, és gyakorolhatják az előíró joghatóságot.

---

48. *Lásd* Tim Mauer, *Cyber Proxies and the Crisis in Ukraine*, *in* CYBER WAR IN PERSPECTIVE: RUSSIAN AGGRESSION AGAINST UKRAINE, NATO CCD COE 79, 81- 82 (Kenneth Geers ed., 2015) https://ccdcoe.org/sites/default/files/multimedia/pdf/CyberWarinPerspective_Maurer_09.pdf; Tim Maurer, *'Proxies' and Cyberspace*, 21 J. CONFLICT & SECURITY L. 383 (2016); Luke Penn-Hall, *The Problem with Proxies*, THE CIPHER BRIEF (2016. július 21.), https://www.thecipherbrief.com/article/tech/problem-proxies-1092.

49. TALLINN MANUAL 2.0, *Supra* note 14, 51. pont, 1. bekezdés (belső hivatkozások kihagyva).

50. *Id.* r. 8.

51. *Id.* , ¶ 2.

(azaz a kibertevékenység helye vagy annak hatásai alapján), ha az extraterritoriális joghatóság hagyományos alapjainak valamelyikén alapul.[52]

A 9. szabály[53] tárgyalja a területi joghatóságot, és megállapítja, hogy a szubjektív és objektív területi joghatóság egyaránt vonatkozik a kibertevékenységekre. A legtöbb esetben ez nem volt vitatott szabály. A csoport azonban megosztott az olyan kibertevékenységek kérdésében, amelyekhez csak minimális kapcsolat fűződik, mint például az adatok továbbítása. A csoport egy része úgy vélte, hogy egy állam joghatóságot gyakorolhat az adatátvitelre, mások viszont nem így gondolták.[54] Ezt a pontot a Kézikönyvből vett példa szemlélteti.

Tekintsünk egy olyan forgatókönyvet, amelyben az A államban kezdeményezett kiberműveletből származó adatok a B államon keresztül jutnak el a C államba, ahol tényleges hatása van. Az "A" állam gyakorolhat előíró területi joghatóságot, mint az az állam, ahol a kibertevékenység keletkezett; "C" állam szintén gyakorolhat, mint az az állam, ahol a hatások bekövetkeznek; de gyakorolhat-e joghatóságot a "B" állam? A szakértők megosztottak ebben a kérdésben.[55] A válasz meghatározásakor természetesen fontos, hogy ki határozza meg, hogy mi a minimális kapcsolat, vagy de minimis. És természetesen, bárhogyan is oldják meg ezt a kérdést, az nem akadályozza meg az államot abban, hogy a joghatóság más alapjait, például az állampolgárságot gyakorolja.[56] Továbbá, ez a meghatározás fontos következményekkel jár a kellő gondosság fentebb tárgyalt kérdésére.

A 10. szabály[57] elismeri, hogy az államok is érvényesíthetnek extraterritoriális

---

52. *Id.* 51-52. pont, 3. bekezdés.

53. TALLINN MANUAL 2.0 A 9. szabály előírja, hogy a:

> Egy állam területi joghatóságot gyakorolhat:
>
> (a) kiberinfrastruktúra és a területén kibertevékenységet folytató személyek;
> (b) a területéről származó vagy ott végzett kibertevékenységek; vagy
> (c) a területén jelentős hatást gyakorló kibertevékenységek.

Id. 55. r. 9. pont.

54. *Id.* , ¶¶ 2-3.

55. *Id.* 55-56, 4. pont.

56. *Id.* 56, 55. pont.

57. TALLINN MANUAL 2.0 A 10. szabály előírja, hogy:

> Az államok a kibertevékenységek tekintetében extraterritoriális előíró joghatóságot gyakorolhatnak:
>
> (a) a saját állampolgárai által végzett tevékenységek;
> (b) az állampolgárságával rendelkező hajók és légi járművek fedélzetén elkövetett bűncselekmények;
> (c) külföldi állampolgárok által elkövetett, és az állam alapvető érdekeinek súlyos aláásására irányuló bűncselekmények;
> (d) külföldi állampolgárok által a saját állampolgárai ellen, bizonyos korlátozásokkal; vagy
> (e) amelyek a nemzetközi jog szerint az egyetemesség elvének hatálya alá tartozó bűncselekménynek minősülnek.

Id. 60 r. 10. pont.

joghatóság az állampolgárság, a védelmi elv, a passzív személyiség és az egyetemesség révén a területükön kívüli kibertevékenységek tekintetében. Az állampolgárság szerinti joghatóság tekintetében az egyik érdekes, még megoldatlan kérdés az állam állampolgárainak kibertevékenységére vonatkozik, és arra, hogy egy állam csak a külföldön tartózkodó személyre vagy az általa létrehozott adatokra is gyakorolhat-e joghatóságot.[58] Más szóval, ha A állam állampolgára B államban adatokat hoz létre, nem világos, hogy A állam gyakorolhat-e joghatóságot az adatok és az egyén felett is.

A 11. szabály a végrehajtási joghatósággal foglalkozik.[59] Az előíró joghatósághoz hasonlóan az államok saját területükön is gyakorolhatnak végrehajtási joghatóságot, de korlátozottabban képesek a területen kívüli végrehajtási joghatóság gyakorlására; az ilyen joghatóság gyakorlása általában csak a területi állam beleegyezésével lehetséges. Ez is az egyik olyan terület, ahol a kibertevékenységek számos érdekes kérdést vetnek fel.

A 11. szabály a végrehajtási joghatóságot szűken értelmezi, és bizonyára vannak olyanok is, akik tágabb értelmezés mellett érvelnek. A Tallinni Kézikönyv álláspontja szerint a nemzetközi jog, beleértve az olyan speciális szerződéseket, mint a tengerjog, a világűr és a légi közlekedésre vonatkozó szerződések, támogathatják a végrehajtási joghatóság külföldi gyakorlását. A szakértők véleménye szerint, amennyiben ilyen joghatósági engedélyek léteznek, azok kiterjednek a kibernetikai tevékenységekre is.[60] Valójában egyes szerződések kifejezetten hivatkozhatnak bizonyos extraterritoriális végrehajtási kiváltságokra, mint például a számítógépes bűnözésről szóló egyezmény.[61]

Tekintettel a kiberadatok természetére, a tallinni csoport (a továbbiakban: csoport) elismerte, hogy előfordulhat, hogy nem egyértelmű, hogy az adatok vagy más digitális bizonyítékok melyik államban találhatók. A csoport megállapította, hogy a nemzetközi jog jelenleg nem foglalkozik egyértelműen ezzel a kérdéssel, így a csoport nem tudott semmiféle konszenzusra jutni ebben az esetben.[62] Feltételezhetően a

---

58. *Lásd id.* 63. pont, 8. bekezdés.

59. TALLINN MANUAL 2.0 A 11. szabály előírja, hogy:

> Egy állam csak a következő feltételek alapján gyakorolhat extraterritoriális joghatóságot a személyekkel, tárgyakkal és kibertevékenységekkel kapcsolatban:
>
> (a) a nemzetközi jog szerinti különleges hatáskörmegosztás; vagy
> (b) egy külföldi kormány érvényes hozzájárulása ahhoz, hogy joghatóságot gyakoroljon a területén.

Id. 66. r. 11.

60. *Id.* 67. pont, 3. bekezdés.

61. Egyezmény a számítógépes bűnözésről, Európa Tanács, E.T.S. 185, 2001. november 23. (hatályba lépett 2004. július 1-jén), https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900 001680081561.

62. TALLINN MANUAL 2.0, 14. lábjegyzet, 68. pont, 8. bekezdés.

ilyen esetben az az állam, amely úgy dönt, hogy gyakorolja végrehajtási jogkörét, ezt bizonyos kockázatnak kitéve teszi.

A szakértők azt is megjegyezték, hogy nehézségekbe ütközhet annak megítélése, hogy az interneten széles körben elérhető, de egy másik államban lévő szervereken tárolt elektronikus adatok a területi vagy a területen kívüli végrehajtási joghatóság gyakorlását jelenti-e. A csoport végül úgy döntött, hogy a területi joghatóság gyakorlásáról van szó, mivel az adatok az érintett államban hozzáférhetők. Ez akkor is igaz, ha az adatok nem nyilvánosak és jelszóval védettek, amennyiben az állam területéről érik el őket.[63] Ezzel szemben azok az adatok, amelyek az interneten keresztül hozzáférhetők, de nem az érintett államban élő egyének számára kívánják hozzáférhetővé tenni őket, a területen kívüli joghatóság gyakorlását és vagy hozzájárulást, vagy a nemzetközi jog által adott különleges engedélyt igényelnek.[64]

A Kézikönyv azt is elismeri, hogy az ítélkezési joghatóság általában egybeesik az előíró joghatósággal, de annak gyakorlását a területi állam beleegyezése korlátozhatja.[65] A külföldön tartózkodó katonák helyzetét illetően a haderők jogállásáról szóló megállapodások gyakran tartalmaznak speciális hozzájárulást a küldő államnak a haderő tagjai feletti ítélkezési joghatóság engedélyezéséhez. Más megállapodásoknak is lehetnek hasonló hatásai különleges helyzetekben.[66]

Természetesen e joghatósági típusok egyike sem kizárólagos. Az államok gyakran rendelkeznek párhuzamos joghatósággal, és ez a kibertérben is érvényesül. Figyeljük meg a kézikönyv egyik illusztrációját: "egy A állam állampolgárságával rendelkező, de B államban tartózkodó bűnöző kibernetikai műveletet hajthat végre egy C államban található webszerver ellen, hogy ellopja a D államban található személyek banki adatait".[67] Ebben az esetben minden államnak lehetősége lenne a joghatóság gyakorlására.[68] Természetesen egy ilyen forgatókönyv hangsúlyozza a nemzetközi együttműködés szükségességét.

A joghatóságról szóló fejezet a mentelmi jogról szóló szabállyal zárul[69] és a nemzetközi együttműködésről szóló szabállyal.[70] Ez a fejezet, miközben azonosítja

---

63. *Id.* 69-70. pont, 13. bekezdés.

64. *Id.*

65. *Id.* 53. pont, 10-11. bekezdés.

66. *Id.* 53-54. pont, 10-14. bekezdés.

67. *Id.* 54. pont, 15. bekezdés.

68. *Id.*

69. A TALLINN MANUAL 2.0 12. szabálya kimondja, hogy "Egy állam nem gyakorolhat végrehajtási vagy igazságszolgáltatási joghatóságot a nemzetközi jog szerint mentességet élvező

kibertevékenységet vagy kiberinfrastruktúrát folytató személyekkel szemben". *Id.* 71. r. 12. pont.

70. TALLINN MANUAL 2.0 A 13. szabály kimondja, hogy "Bár az államok általában véve nem kötelesek együttműködni a számítógépes bűncselekmények nyomozása és üldözése során, az ilyen együttműködés

Az olyan területeken, ahol nincs nemzetközi konszenzus egy kérdésben, vagy ahol a nemzetközi jog még nem egyértelmű, nem valószínű, hogy nagy vitákat fog okozni.

D. *A nemzetközi felelősség joga*

A jelenlegi kibertevékenységek jellege miatt ez egy rendkívül fontos fejezet a Kézikönyvben. Az állam felelősségének doktrínáját, amelyet főként a Nemzetközi Jogi Bizottság államfelelősségről szóló cikkei tartalmaznak, a[71] internetes szereplőkre és internetes tevékenységekre alkalmazza. A szakértők között teljes egyetértés volt abban, hogy az állam felelősségének szokásjogát kell alkalmazni a kibertevékenységekre.[72] A 14. szabály tehát kimondja, hogy "[egy] állam nemzetközi felelősséggel tartozik a kibernetikai vonatkozású cselekményért, amely az államnak tulajdonítható, és amely nemzetközi jogi kötelezettség megsértését jelenti".[73] Sem fizikai kár, sem sérülés nem szükséges ahhoz, hogy egy kibercselekmény nemzetközi jogellenes cselekménynek minősüljön,[74] és a földrajzi elhelyezkedés nem meghatározó az állami felelősség megállapításakor?[75] A kibercselekmények felróhatóságának fogalma sok vitát és megdöbbenést váltott ki.[76] A 15-17. szabály foglalkozik ezzel a kérdéssel a kiberműveletek tekintetében. A 15. szabály az állami felelősségről szóló cikkek 4. és 5. cikkét idézi, és megállapítja, hogy az állami szervek - például az Egyesült Államokban a CIA vagy az NSA - kibertevékenységei az államnak tulajdoníthatók,[77] még akkor is, ha az adott szervezet jóváhagyott hatáskörén kívül esnek, vagy *ultra vires*.[78] Ebből a célból az állam szervei közé tartoznának azok a szereplők is, amelyek a törvény szerint nem szervek, de "teljes mértékben függnek" az államtól,[79] és olyan személyek vagy szervezetek, amelyek felhatalmazással rendelkeznek.

---

az alkalmazandó szerződés vagy más nemzetközi jogi kötelezettség előírhatja." *Id.* 75. r. 13.

71. Int'l Law Comm'n, Draft Articles on Responsibility of States for Internationally Wrongful Acts, Rep. of the Int'l Law Comm'n on the Work of Its Fifty-Third Session, U.N. Doc. A/56/10 (2001) [a továbbiakban: ILC cikktervezetek a felelősségről].

72. TALLINN MANUAL 2.0, 14. lábjegyzet, 80. pont,

4. bekezdés. 73. *Id.* 84. r. 14. o.

74. *Id.* at 86, ¶ 8.

75. *Id.* 87. pont, 11.

bekezdés.

76. *Lásd* Lily Hay Newman, *Hacker Lexikon: Mi az attribúciós probléma?* , WIRED (2016. dec. 24., 7:00) https://www.wired.com/2016/12/hacker-lexicon-attribution-problem/; Dimitar Kostadi nov, The Attribution Problem in Cyber Attacks, INFOSEC INST. (2013. február 1.), http://resources.

infosecinstitute.com/attribution-problem-in-cyber-attacks/#gref; Nicholas Tsagourias, *Cyber Attacks, Self-Defence and the Problem of Attribution*, 17 J. CONFLICT & SECURITY L. 229 (2012).

77. TALLINN MANUAL 2.0, 14. lábjegyzet, 87-90. pont, 3., 8-11. bekezdés.

78. *Id.* at 89, ¶ 9.

79. *Id.* at 88, ¶ 4 (belső idézet kihagyva).

a kormányzati hatalom egyes elemeinek gyakorlására.[80]

Bár ezek a kijelentések a nemzetközi jogot nem kiberjogi helyzetekben is érintik, alkalmazásuk a kibertevékenységekre nem mentes a vitáktól. A szakértők például megjegyezték, hogy hagyományosan a kormányzati eszközök, például harckocsik vagy hadihajók használata szinte megdönthetetlen bizonyíték arra, hogy egy tevékenységet egy államnak tulajdonítanak. Ugyanez nem mondható el a kibertevékenységekről. Valójában, tekintettel a kiberinfrastruktúra elfogásának vagy meghamisításának képességére, beleértve azt is, hogy a kibertevékenységek honnan származhatnak, "pusztán az a tény, hogy egy kiberműveletet indítottak vagy más módon kormányzati kiberinfrastruktúrából származik, vagy hogy a feltört kiberinfrastruktúra ellen használt rosszindulatú szoftvereket úgy tervezték, hogy egy másik állam kormányzati kiberinfrastruktúrájának "jelentsenek vissza", általában elégtelen bizonyíték a műveletnek az adott államnak való tulajdonításához".[81]

Abban az esetben, ha az állam valamely szervét egy másik állam rendelkezésére bocsátják, és ez a szerv kizárólag a fogadó állam ellenőrzése alatt működik, és az állam céljaira és nevében cselekszik, a szerv cselekményei a fogadó államnak tulajdoníthatók.[82]

A legdiflfiktabb jogi kérdést a tulajdonítás területén azok a nem állami szereplők vetik fel, akik esetleg egy állam megbízottjaként működnek, vagy akik valamilyen módon egy állam nevében járnak el, anélkül, hogy erre egyértelmű jogi felhatalmazásuk lenne. Ezzel a kérdéssel a 17. szabály foglalkozik,[83] és az állami felelősségre vonatkozó szabályok 8. cikkét reflektálja.[84] A közelmúltbeli kibernetikai eseményekkel kapcsolatos viták nagy része arról szólt, hogy a magánszereplők cselekedeteit olyan államoknak tulajdonították, amelyekkel ezek a szereplők kapcsolatban álltak.[85] A nemzetközi joggal összhangban a nem állami szereplők által végrehajtott, de egy állam "tényleges ellenőrzése" alatt végrehajtott kiberműveletek az államnak tulajdoníthatók.[86] Az ilyen cselekmények puszta bátorítása vagy támogatása

---

80. *Id.* at 89, ¶¶ 6 -9.

81. *Id.* at 91, ¶ 13 (belső idézet kihagyva).

82. *Id.* 93. pont, 1. bekezdés.

83. TALLINN MANUAL 2.0 A 17. szabály kimondja: "A nem állami szereplő által végrehajtott kiberműveletek akkor tulajdoníthatók egy államnak, ha:

(a) az utasításai szerint, illetve az irányítása vagy ellenőrzése alatt; vagy

(b) az állam elismeri és magáévá teszi a műveleteket."

Id. 94. r. 17.

84. ILC Cikktervezet a felelősségről, 72. lábjegyzet, cikk. 8.

85. *Lásd* Dorothy Denning, *The Rise of Hacktivism*, GEO. J. INT'L AFFAIRS (2015. szeptember 8.), http://journal.georgetown.edu/the-rise-of-hacktivism/; Sarah Geary, *The Cyber-Intelligence Nexus: Russia's Use of Proxies*, CIPHER BRIEF (2017. február 24.), https://www.thecipherbrief.com/article/tech/ cyber-intelligence-nexus-russias-use-proxies-1092.

86. TALLINN MANUAL 2.0, 14. lábjegyzet, 95-96., 4-6. pont.

a nem állami szereplő cselekedetei nem elegendőek az attribúció eléréséhez.[87] Az állami szervek cselekményeivel ellentétben a nem állami szereplők *ultra vires* cselekményei ezekben a helyzetekben nem tulajdoníthatók az államnak, mivel ezek az állam "tényleges ellenőrzésén" kívül eső cselekmények lennének.[88] Végül, ha egy állam nem gyakorol tényleges ellenőrzést egy nem állami szereplő felett, de ezt követően a nem állami szereplő kibernetikai cselekményeit sajátjaként fogadja el, ezek a cselekmények szintén az államnak tulajdoníthatók.[89]

Mint általában az attribúció esetében is, sokkal könnyebb azonosítani és kimondani a szabályt, mint alkalmazni azt a tényszerű helyzetekben. Például, amint azt a szakértők megjegyezték, "egy állam túlnyomó vagy döntő részvétele a "finanszírozásban, szervezésben, kiképzésben, ellátásban és felszerelésben . . . , a katonai vagy félkatonai célpontok kiválasztásában, valamint a művelet egészének megtervezésében" elégtelennek találták a "tényleges ellenőrzés" küszöbértékének eléréséhez".[90] A kibertérben ez úgy is lefordítható, hogy az állam biztosítja a kibereszközöket, azonosítja a célpontokat és kiválasztja a kiberművelet végrehajtásának időpontját, és ez még mindig nem vonná maga után az állam felelősségét. Egyesek szerint pontosan ez a forgatókönyv érvényes Oroszország és az orosz hacktivisták esetében, akik kibertámadást intéztek Észtország ellen egy orosz háborús emlékmű elmozdítása nyomán.[91]

Idővel érdekes lesz látni, hogy az államok hogyan reagálnak a továbbiakban is a magas betudhatósági küszöbértékre. Mivel az államok továbbra is olyan kibertevékenységek áldozatai lesznek, amelyek nem tulajdoníthatók egy államnak, és a szuverenitás és a kellő gondosság szabályai nem teszik lehetővé az áldozatállamok számára, hogy hatékony fellépést követeljenek a fogadó államtól, a tulajdonítási normára nehezedő nyomás növekedni fog, mint olyan módszerre, amely lehetővé teszi az áldozatállamok számára, hogy szélesebb körben hozzáférjenek az ellenintézkedésekhez (lásd alább).

A 18. szabály a segítségnyújtás és a segítségnyújtás doktrínájával, valamint a más államok cselekményeiért való felelősséggel foglalkozik.[92] A segítségnyújtás és a segítségnyújtás tekintetében

---

87. *Id.* 97. pont, 8.
bekezdés. 88. *Id.*
98., 13. pont.
89. *Id.* 99-100, 17. pont.
90. *Id.* 97. pont, 9. bekezdés.
91. R. Ottis, *Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective*, *in* PROCEEDINGS OF THE 7TH EUROPEAN CONFERENCE ON INFORMATION WARFARE AND SECURITY,

PLYMOUTH, 2008, 163. o. (2008), https://ccdcoe.org/multimedia/analysis-2007-cyber attacks-against-estonia-information-warfare-perspective.html.

92. A TALLINN MANUAL 2.0 18. szabálya kimondja, hogy "A kiberműveletek tekintetében az állam felelős a következőkért:

(a) egy másik államnak nemzetközi jogellenes cselekmény elkövetéséhez nyújtott segítsége vagy támogatása, ha az állam a nemzetközileg jogellenes cselekmény körülményeinek ismeretében nyújt segítséget vagy támogatást, és a cselekmény nemzetközi jogellenes lenne, ha azt az állam követné el;

létfontosságú, hogy az állam tudja, hogy ténylegesen segítséget és támogatást nyújt a nemzetközileg jogellenes cselekményhez, és hogy az államnak ez a szándéka.[93] Azt is fontos megjegyezni, hogy a segítő állam csak a segítésért és a támogatásért felelős, nem pedig a tényleges jogellenes cselekményért.[94] Bár a szakértők nem foglalkoznak közvetlenül a kérdéssel, egyértelműnek tűnik, hogy a segítségnyújtás és a segítés többre van szükség annál, mint hogy az állam - még ha tudatosan is - lehetővé tegye a káros adatok átvitelét a kiberinfrastruktúráján keresztül. A logikának ellentmondana, hogy a kellő gondosság követelményét kiváltó követelmény hasonló vagy még alacsonyabb legyen, mint a segítségnyújtás és a segítés követelménye.

A kézikönyv szerint a kibertevékenységekre a jogellenességet kizáró valamennyi szokásos körülmény vonatkozik.[95] A Kézikönyv ezután meglehetősen hosszan tárgyalja az ellenintézkedéseket.[96] Mivel az ellenintézkedések nem emelkedhetnek az erő alkalmazásának szintjére, úgy tűnik, hogy a kibertevékenységek jól illeszkednek a paradigmához.[97] Fontos megjegyezni, hogy az ellenintézkedések csak az államokkal szemben alkalmazhatók, és nem zárják ki egy cselekmény jogellenességét, ha az nem állami szereplők ellen irányul, kivéve, ha azok cselekményei egy államnak tulajdoníthatók.[98] A kibernetikai ellenintézkedésnek azonban nem kell a nemzetközi jogot megsértő állam konkrét szervét céloznia, mivel maga az állam a célpont.[99] Ezen túlmenően a kiberellenes intézkedések nem korlátozódnak a "természetbeni" válaszlépésekre. Más szóval, egy állam nem kiberjellegű jogsértésre válaszul kiberellenes intézkedéssel, kiberjellegű jogsértésre pedig nem kiberjellegű ellenintézkedéssel válaszolhat.[100]

(b) az általa irányított és ellenőrzött másik állam nemzetközileg jogellenes cselekménye, ha az állam a nemzetközileg jogellenes cselekmény körülményeinek ismeretében cselekszik, és a cselekmény nemzetközileg jogellenes lenne, ha azt ő követné el; vagy

(c) egy nemzetközi jogellenes cselekményt, amelynek elkövetésére egy másik államot kényszerít". TALLINN MANUAL 2.0, *Supra* 14. lábjegyzet, 100. r. 18. o.

93. *Id.* at 101, ¶ 3.

94. *Id.* at 102, ¶ 6.

95. *Id.* at 104 -11. A TALLINN MANUAL 2.0 19. szabálya kimondja, hogy "A kiberműveletekkel kapcsolatos cselekmény jogellenessége kizárt abban az esetben, ha:

(a) hozzájárulás; b) önvédelem; c) ellenintézkedés; d) szükségesség; e) vis maior; vagy f) vészhelyzet."

Id. at 104 r. 19.

96. *Id*. 111-34.

97. *Lásd általában* Michael N. Schmitt, *"Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law*, 54 VA. J. INT'L L. 697, 718 -719 (2014).

98. TALLINN MANUAL 2.0, 14. lábjegyzet, 113. pont, 7-8.

bekezdés. 99. *Id.* 112-13. o., 6. pont.

100. *Id.* 128-129, 7. pont.

A kibernetikai ellenintézkedések számos érdekes kérdést vetnek fel. Az ellenintézkedésekkel szemben támasztott egyik követelmény, hogy ideiglenes jellegűek és a lehető legnagyobb mértékben visszafordíthatóak legyenek.[101] A szakértők ezt a követelményt tágan értelmezték, és a kibertérrel összefüggésben azzal érveltek, hogy az adatok törlése, még ha az megakadályoz is valamilyen későbbi, az ellenintézkedés utáni tevékenységet, nem zárja ki az ellenintézkedést.[102] A szakértők nem tudtak megegyezni abban, hogy két kibervédelmi ellenintézkedési lehetőség esetén kötelező-e a leginkább visszafordíthatót alkalmazni.[103]

Az ellenintézkedések egy másik eleme, amelyet a szakértők különösen figyelemre méltónak találtak, az a követelmény, hogy az ellenintézkedés meghozatala előtt értesíteni kell az érintetteket, és esetleg tárgyalásokat kell folytatni a megoldásról.[104] A szakértők megjegyezték, hogy ez a követelmény nem abszolút, és egyetértettek abban, hogy ha a célállam értesítése a kiberellenes intézkedés meghozatala előtt hatástalanná tenné az ellenintézkedést, akkor nem kell az értesítést megtenni.[105] Tekintettel a kiberműveletek jellegére, ez pragmatikus megközelítés.

A szakértők egyetértettek abban, hogy a kiberellenes intézkedések nem sérthetnek kényszerítő normát[106] és arányosnak kell lenniük a sérelemmel, amelyre reagálnak,[107] bár nem követelmény, hogy a kiberellenes intézkedésnek pontosan a nemzetközi jogot megsértő állami szervet kell céloznia.[108]

A szakértők megosztottak a kollektív ellenintézkedések kérdésében, a többség szerint nem volt jogszerű, hogy egy nem károsult állam ellenintézkedéseket tegyen egy károsult állam nevében.[109] A többség azonban megosztott abban a kérdésben, hogy a nem sérült állam segíthet-e a sérült államnak az ellenintézkedések meghozatalában.[110]

A kézikönyv fejezetének további része az ellenintézkedések harmadik felekre gyakorolt hatásával kapcsolatos szabályokat és magyarázatokat tartalmaz,[111] a

---

101. ILC Cikktervezet a felelősségről, 72. lábjegyzet, cikk. 49.

102. TALLINN MANUAL 2.0, 14. lábjegyzet, 119. pont, 8. bekezdés.

103. *Id.* , ¶ 9.

104. ILC Cikktervezet a felelősségről, 72. lábjegyzet, cikk. 52.

105. TALLINN MANUAL 2.0, 14. lábjegyzet, 120. pont, 11. bekezdés.

106. A TALLINN MANUAL 2.0 22. szabálya kimondja, hogy "Az ellenintézkedések, akár kiber jellegűek, akár nem, nem tartalmazhatnak olyan intézkedéseket, amelyek alapvető emberi jogokat érintenek, tiltott harci megtorlásnak minősülnek, vagy valamely kényszerítő normát sértenek.". Az ellenintézkedéseket foganatosító államnak teljesítenie kell a diplomáciai és konzuli sérthetetlenséggel kapcsolatos kötelezettségeit." *Id*. 122-23. r. 22.

107. A TALLINN MANUAL 2.0 23. szabálya kimondja, hogy "Az ellenintézkedéseknek, akár kibernetikai jellegűek, akár nem, arányosnak kell lenniük azzal a kárral, amelyre reagálnak". *Id.* 127. r. 23.

108. *Id.* at 129, ¶ 10.

109. *Lásd id.* 131., 5. pont.

110. *Id.* 132. pont, 7. bekezdés.

111. A TALLINN MANUAL 2.0 23. szabálya kimondja, hogy "Tilos az olyan ellenintézkedés, akár kiber jellegű, akár nem, amely egy harmadik állammal vagy más féllel szemben fennálló jogi kötelezettséget sért.". *Id*. 133. r. 23.

754[48 .
kötet

a szükségességre való hivatkozás,[112] több szabály az államok nemzetközi jogellenes cselekményekkel kapcsolatos kötelezettségeiről,[113] és egy szabály a nemzetközi szervezetek felelősségéről.[114]

Ezek a szabályok és az ellenintézkedésekkel kapcsolatos megjegyzések rávilágítanak az ellenintézkedés alkalmazása - különösen a kibertérben - és az önvédelmi célú fellépés közötti különbségre. Az ellenintézkedésekre vonatkozó, fentebb részletezett szabályok és korlátozások nagyobb mértékben korlátozzák az állam azon képességét, hogy olyan cselekményekre válaszul cselekedjen, amelyek nem jelentenek erőszak alkalmazását, mint a fegyveres támadásra válaszul tett lépések. Fontos, hogy az ellenintézkedések alkalmazására vonatkozó normák sokkal kevésbé mérlegelési jogkörrel rendelkeznek, mivel bizonyos tényleges lépéseket kell megtenni, szemben az állam azon mérlegelési jogkörébe tartozó döntésével, hogy egy cselekmény fegyveres támadásnak minősül, vagy hogy fegyveres támadás fenyeget. A kibertér tekintetében ez különösen fontos szempont, mivel az államok közötti barátságtalan kiberinterakciók nagy része nem minősül fegyveres támadásnak.

Talán éppen ez az egyensúlyhiány az, amire az államok a kiberellenes intézkedésekkel kapcsolatban vágynak. A szerző máshol már kifejtette, hogy az ellenintézkedések alkalmazásának megkönnyítése nem szándékolt káros következményekhez vezethet.[115] Mindazonáltal érdekes lesz látni, hogy a jövőben az államok a nemzetközi jogot úgy alakítják-e, hogy a kiberellenes intézkedésekre vonatkozó korlátozásokat enyhítsék, vagy enyhítsék a fegyveres támadás küszöbértékét, hogy hatékonyabb válaszintézkedéseket biztosítsanak a kibertevékenységek szélesebb körére.

E. *A kiberműveletek önmagukban nem szabályozottak*

A Kézikönyv ezen szakasza elismeri, hogy az államok egyes cselekedetei nem tartoznak a nemzetközi jog hatálya alá, de a cselekedetek egy szűk körét határozza meg, amelyek ebbe a kategóriába tartoznak. Amint azt fentebb a szuverenitással kapcsolatban említettük, a[116] szerint a nem szabályozott kibertevékenységek e kategóriája szélesebb körű. A tallinni szakértők azonban a nemzetközi jog által *önmagában* nem szabályozott kiberműveletek szigorú értelmezését vették alapul.

---

112. TALLINN MANUAL 2.0 A 23. szabály kimondja, hogy "Az állam a szükségességre való hivatkozással eljárhat olyan cselekményekre válaszul, amelyek súlyos és közvetlen veszélyt jelentenek - akár kiberjellegű, akár nem - valamely alapvető érdekre, ha ez az egyetlen eszköz annak védelmére". *Id.* 135. r. 23. o.

113. TALLINN MANUAL 2.0 A 27. szabály a megszűnésre, a biztosítékokra és garanciákra vonatkozik; a 28. és 29. szabály a jóvátételekkel foglalkozik; a 30. szabály pedig az *erga omnes* kötelezettségekkel. *Lásd id.* 142-53. o.

114. *Id.* 157. r. 157; *lásd még id.* 153-67. o.

115. *Lásd általában* Eric Talbot Jensen & Sean Watts, *A Cyber Duty of Due Diligence: Gentle*

Civilizer or Crude Destabilizer? , TEX. L. REV. (megjelenés előtt) (a szerzőkkel közösen).

116. *Lásd fentebb a* III.A. szakaszt.

A 32. szabály a békeidőben folytatott kiberkémkedésre vonatkozik, és szinte bocsánatkérő hangnemben fogalmaz. Anélkül, hogy ténylegesen kimondaná, hogy a kiberkémkedést a nemzetközi jog megengedi, a szabály kimondja, hogy "[a]bár az államok által békeidőben folytatott kiberkémkedés önmagában nem sérti a nemzetközi jogot, a módszer, amellyel végzik, sértheti azt".[117] A szabály alkalmazásában a kiberkémkedés "minden olyan titokban vagy hamis ürüggyel elkövetett cselekmény, amely kiberképességeket használ fel információgyűjtésre vagy annak megkísérlésére".[118] A szabály csak az államok által folytatott kémkedésre vonatkozik,[119] és a szakértők elismerték, hogy nemcsak számos állam teszi a kémkedést a belső jog értelmében jogellenesnek, ha azt ellenük végzik,[120] hanem számos olyan állam is van, amely kifejezetten engedélyezte a kémkedés bizonyos formáit más államok ellen.[121]

Annak ellenére, hogy a szakértők egyetértettek abban, hogy bár *önmagában* nincs tilalom, a szakértők egyetértettek abban, hogy "a kémkedés a nemzetközi jogot sértő módon is történhet, mivel a kiberkémkedés során alkalmazott bizonyos módszerek jogellenesnek minősülnek".[122] A szakértők azonban nem tudtak konszenzusra jutni abban a kérdésben, hogy a távoli kiberkémkedés sérti-e a nemzetközi jogot. A többség úgy vélte, hogy az adatok exfiltrálása nem sérti a nemzetközi jog egyetlen szabályát sem,. Ezzel szemben néhány szakértő úgy vélte, hogy egy bizonyos ponton az exfiltráció olyan súlyos lehet, hogy az már jogellenes.[123] Hasonlóképpen a szakértők nem értettek egyet a közeli hozzáférésű műveletekkel kapcsolatban, mint például azokkal a műveletekkel, amelyek során a célállam területén egy magánszemély USB-meghajtót helyez be egy kormányzati rendszerbe, és adatokat exfiltrál. A szakértők egyike sem állította, hogy az exfiltráció a nemzetközi jog megsértését jelentené, de a többség úgy vélte, hogy az sérti a célállam szuverenitását.[124] A szakértők fennmaradó része a kémkedést a szuverenitás alóli kivételnek tekintette.[125]

A szakértők egyetértettek abban, hogy a "mézesmadzagok" - értékes adatok vagy hálózati szegmensek, amelyeket arra terveztek, hogy rosszindulatú hackereket csalogassanak be, hogy azonosítani lehessen őket és megvizsgálhassák módszereiket, de valójában ne fedjenek fel hasznos adatokat - a nemzetközi jog értelmében nem jogellenesek.[126] Fegyveres

---

117. TALLINN MANUAL 2.0, 14. lábjegyzet, 168. o. 32. o.
118. *Id.* , ¶ 2.
119. *Id.* , ¶ 3.
120. *Id.* 174., 17. pont.
121. *Id.* 169., 5. pont (belső idézet kihagyva).
122. *Id.* 170, 6. pont.
123. *Id.* 170-171, 8. pont.
124. *Id.*
125. *Id.* 171., 9. pont.
126. *Id.* 173-74, 15.
pont.

A mézeskalitkák, amelyeknél az exfiltrálásra szánt adatok olyan rosszindulatú szoftvereket tartalmaznak, amelyeket aztán az infiltrátor saját rendszerén hajtanak végre, megosztottságot okoztak a szakértők körében, a többség teljesen megengedhetőnek találta őket.[127]

A kémkedés kezelése a Tallinni Kézikönyvben szorosan kapcsolódik a szuverenitásról alkotott nézethez. Számos olyan bemutatott esetben, amikor a kémkedés "módszere" jogellenessé teheti azt, a szakértők úgy határozták meg, hogy a megsértett szabály a szuverenitás szabálya. Egyre több bizonyíték látszik arra, hogy a kibernetikai képességekkel rendelkező nemzetek kibernetikai kémkedést folytatnak.[128] A növekvő kiberkémkedés valószínűleg nyomást gyakorol majd arra a jelenlegi felfogásra, hogy a szuverenitás hogyan vonatkozik a kibertér területére, ami a jövőben talán hatással lesz a 32. szabályra.

A másik szabály ebben a szakaszban a nem szabályozott kiberműveletekről azt mondja, hogy "[a] nemzetközi jog csak korlátozott esetekben szabályozza a nem állami szereplők kiberműveleteit".[129] A kifejezetten az egyénekre alkalmazandó nemzetközi jogi rendszerek - például az emberi jogi jog és a fegyveres összeütközés joga - kivételével a szakértők úgy vélték, hogy a nemzetközi jog nem szabályozza a nem állami szereplőket.[130] Ezt az államoknak a belső jogon keresztül kell szabályozniuk.

A kémkedéshez hasonlóan ez is a nemzetközi jog olyan területe, ahol a szabály valószínűleg nyomás alá kerül. A nem állami szereplők által okozott incidensek mennyisége,[131] a kellő gondosság szabályának az államokra való korlátozó alkalmazása,[132] és a nem állami szereplőkkel szembeni ellenintézkedések alkalmazásának tilalma[133] együttesen arra kényszerítheti az államokat, hogy újragondolják a nemzetközi jog hatékonyságát a nem állami szereplőkkel szembeni végrehajtási intézkedések tekintetében.

---

127. *Id.* at 174, ¶ 16.

128. Kevin Rawlinson, *NSA Surveillance*: THE GUARDIAN (2013. október 26., 15:19 EDT), https://www.theguardian.com/world/2013/oct/ 26/nsa-surveillance-brazil-germany-un-resolution; *Russia Behind Hack on German Parliament*, DW . COM (2016. dec. 11.) http://www.dw.com/en/russia-behind-hack-on-german-parliament-paper reports/a-36729079; Jose Pagliery, *China Hacked the FDIC-and US Officials Covered it Up, Report Says*, CNN TECH (2016. július 13., 15:31), http://money.cnn.com/2016/07/13/technology/china-fdic hack/.

129. TALLINN MANUAL 2.0, 14. lábjegyzet, 174. o. 33. o.

130. *Id.* 175, 4. pont.

131. Mark Pomerlau, *Állami vs. nem állami hackerek: Hackerek: különböző taktikák, azonos fenyegetés?* , DEF. SYS. (2015. augusztus 17.), https://defensesystems.com/articles/2015/08/17/cyber-state-vs-non-state-haclers tactics.aspx.

132. *Lásd fentebb a* III.B. szakaszt.

133. *Lásd fentebb a* III.D. szakaszt.

F. *Nemzetközi emberi jogi jog*

A kézikönyvnek ez a része és az ebben a cikkben következő részek a szakértők által szakosodott rendszerekként emlegetett rendszerekre oszlanak. Ezek a rendszerek annyiban specializáltak, hogy az idők során saját, némileg önálló, a tevékenységek szűk körét szabályozó rendszerré fejlődtek. A Kézikönyv ezeket a rendszereket alkalmazza a kibertevékenységekre.

A kézikönyvben szereplő első speciális rendszer a nemzetközi emberi jogi szabályozás. A Kézikönyv e részének megalkotása során felmerült számos nehézség közvetlenül összefüggésbe hozható a nemzetközi emberi jogi jog általánosabb értelemben vett tisztázatlanságával.[134] A kiberműveletek szeszélyeivel együtt talán ez a fejezet tartalmazza a legtöbb nézeteltérést a szakértők között. Ennek megfelelően az emberi jogi jognak a kiberműveletekre való alkalmazásával kapcsolatban az egyik fontos pont az, hogy "bár egy állam tevékenysége beavatkozhat egy meghatározott nemzetközi emberi jogba, például a magánélethez való jogba, ez a tény nem ad választ arra a kérdésre, hogy megsértették-e ezt a jogot".[135] Más szóval annak megállapítása, hogy az emberi jogok egy kibertevékenységre vonatkoznak, nem jelenti azt, hogy a kibertevékenység megsértette az emberi jogokat. A lehetséges jogsértés egy különálló és kiegészítő elemzés.

A 34. szabály az alkalmazhatóság általános szabályát tartalmazza. Eszerint "[a]z emberi jogok nemzetközi joga alkalmazandó a kibernetikai tevékenységekre".[136] Az alkalmazhatóság definiálásában a szakértők egyetértettek abban, hogy "általános elvként a nemzetközi emberi jogi szokásjog a kiberjogi kontextusban egy állam területén kívül is alkalmazandó olyan helyzetekben, amikor az adott állam "hatalmat vagy tényleges ellenőrzést" gyakorol, ahogyan az offline is".[137] A szakértők azonban megosztottak voltak abban a kérdésben, hogy a "hatalom vagy tényleges ellenőrzés" megköveteli-e a "fizikai" ellenőrzést, a többség úgy vélte, hogy fizikai ellenőrzés szükséges.[138] A szakértők abban is megosztottak voltak, hogy egy olyan emberi jogi szerződést, amely nem szól a területenkívüli alkalmazásáról, úgy kell-e értelmezni, hogy az területenkívül alkalmazandó. A többség úgy vélte, hogy az egyezményt extraterritoriálisan kell alkalmazni, ha nincs olyan rendelkezés, amely korlátozza az egyezmény hatályát.

---

134. TALLINN MANUAL 2.0, 14. lábjegyzet, 179-82. pont, 1-7. bekezdés. A TALLINN MANUAL 2.0 megjegyzi, hogy "a nemzetközi szakértői csoport elismerte, hogy az egyes emberi jogi jogosultságok pontos hatályára vonatkozó állami felfogások a kiberkontextusban, valamint az emberi jogi bíróságok és más releváns emberi jogi testületek felfogása eltérő". *Id.* 182. pont, 1. bekezdés.

135. *Id.* 181., 7. pont.

136. *Id.* 182. r. 134.

137. *Id.* 184., 6. pont.

138. *Id.* at 185, ¶ 8.

hatókör.
139

A 35. szabály kimondja, hogy "Az egyének a kibernetikai tevékenységek tekintetében ugyanazokat a nemzetközi emberi jogokat élvezik, mint amilyeneket egyébként élveznek".[140] Ez magában foglalja a véleménynyilvánítás szabadságát, bár a szakértők nem tudtak megegyezni e jog pontos paramétereiben.[141] A véleménynyilvánításhoz való jog[142] és a magánélethez való jog szintén védelmet élvez.[143]

A magánélethez való joggal kapcsolatban a szakértők úgy vélték, hogy ez a jog "magában foglalja a kommunikáció titkosságát".[144] A szakértők egyetértettek abban, hogy ez védi az egyén magánjellegű kommunikációját az emberi ellenőrzéssel szemben, de megosztottak voltak abban, hogy ez a jog hogyan alkalmazható a gépek által végzett algoritmikus ellenőrzések esetében.[145] A többség azonban úgy vélte, hogy az ilyen ellenőrzés nem érinti az egyén jogát, kivéve, ha és amíg az állam valamilyen módon - beleértve az adatfeldolgozást is - nem fér hozzá a kommunikációhoz.[146] Természetesen a nyilvánosság számára hozzáférhető információk általában nem érintik a magánélethez való jogot, még akkor sem, ha azokat kibernetikai eszközökkel gyűjtik, míg a csak egy szűk csoport számára hozzáférhető információk igen. A szakértők nem voltak tisztában azzal, hogy valójában hol húzódnak a határok e két helyzet között.[147] A szakértők nem tudtak megegyezni abban, hogy a magánélethez való jog elvárása általában hogyan alkalmazható erre a jogra.[148]

A szakértők egyetértettek abban, hogy a magánélethez való jog az egyén "személyes adatait" is védi, bár a szakértők elismerték, hogy ez a fogalom a nemzetközi jogban nem jól definiált.[149] A metaadatok tekintetében a szakértők egyetértettek abban, hogy a metaadatok "személyes adatnak" minősülnek, és ezért e szabály alkalmazásában védelmet élveznek, amikor "egy személyhez kapcsolódnak, és az adott személy magánéletével kapcsolatosak".[150] Az egyéb metaadatok tekintetében a szakértők nem tudtak konszenzusra jutni.[151]

---

139. *Id.* 186., 11. pont.
140. *Id.* 187. r. 35.
141. *Id.* at 187- 88, ¶¶ 2- 4.
142. *Id.* 188-89, 5. pont.
143. *Id.* 189., 6. pont.
144. *Id.* , ¶ 7 (belső hivatkozások kihagyva).
145. *Id.* at 190, ¶ 8.
146. *Id.* , ¶ 9 n. 420.
147. *Id.* at 190 -91, ¶ 10.
148. *Id.* at 191, ¶ 11.
149. *Id.* at 191-92, ¶ 12.
150. *Id.* at 192, ¶ 13.
151. *Id.* , ¶ 14.

A szakértők megjegyezték továbbá, hogy a gazdasági, szociális és kulturális jogok szokásjogi jellege a nemzetközi jogban továbbra sem tisztázott, de egyetértettek abban, hogy amennyiben ezeket jogként ismerik el, a kiberműveletek minden bizonnyal érinthetik ezeket a jogokat.[152] Végül a szakértők megjegyezték, hogy létezik az internethez való hozzáféréshez való nemzetközi emberi jog és a "feledésbe merüléshez való jog". A szakértők egyike sem ismerte el ezeket a jelenlegi szokásjog szerinti jogként.[153]

A 36. szabály kimondja, hogy "[a]z államnak a kibertevékenységek tekintetében: (a) tiszteletben tartania az egyének nemzetközi emberi jogait; és b) védenie kell az egyének emberi jogait a harmadik felek által elkövetett visszaélésekkel szemben".[154] Az emberi jogok tiszteletben tartására vonatkozó kötelezettség általában az előző szabályban tárgyalt jogokra vonatkozik, és extraterritoriálisan alkalmazandó az applikációs jogokra.[155]

Az emberi jogok védelmére vagy tiszteletben tartásának biztosítására vonatkozó kötelezettség az államok affirmatív kötelezettsége, bár a szakértők elismerték, hogy egyes államok nem értenek egyet egy ilyen szabály létezésével, és hogy a szabály paraméterei legalábbis vitatottak.[156] A szakértők azonban egyetértettek abban, hogy létezik ilyen szabály, annak ellenére, hogy nincs egyértelmű definíciója.[157] A szakértők például nem tudtak egyetérteni abban, hogy "pontosan milyen területi körülmények között köteles egy állam egy adott személy emberi jogait megvédeni a harmadik felek beavatkozásával szemben".[158]

A szakértők egyetértettek abban, hogy ez a jog magában foglalja a megelőző intézkedések meghozatalának követelményét, például az emberi jogokra gyakorolt terrorista hatások megelőzését.[159] Visszautalva a fent tárgyalt szakértői véleményre, miszerint az internethez való jog nem létezik, a szakértők megosztottak abban a kérdésben, hogy az internethez való hozzáférés szükséges-e egy olyan emberi jog gyakorlásához, mint a szavazás.[160] A szakértők többsége azonban úgy vélte, hogy az államoknak nincs szokásjoguk arra, hogy az egyéni emberi jogok megsértése esetén jogorvoslatot nyújtsanak.[161]

A 37. szabály tárgyalja a tiszteletben tartási és védelmi kötelezettség korlátait, és kimondja, hogy "a nemzetközi emberi jogok tiszteletben tartására és védelmére vonatkozó kötelezettségek - az abszolút jogok kivételével - továbbra is a következők alá tartoznak

152. *Id.* at 194, ¶ 18.
153. *Id.* 195-96. ¶ 23.
154. *Id.* 196. r. 36.
155. *Id.* , ¶ 2.

156. *Id.* 197-98, 5. pont (belső hivatkozások kihagyva).
157. *Id.* 198, 6. pont.
158. *Id.*
159. *Id.* at 199, ¶ 9.
160. *Id.* at 199 -200, ¶ 10.
161. *Id.* at 200, ¶ 12.

bizonyos korlátozások, amelyek szükségesek a törvényes cél eléréséhez, nem diszkriminatívak, és törvény által engedélyezettek."[162] Ez a szabály elismeri, hogy az államoknak egyensúlyt kell teremteniük a kibertevékenységek tekintetében az egyéni jogok és más fontos kötelezettségek, például a közrend és a nemzetbiztonság között,[163] bár egyes jogok, például a rabszolgaság és a kínzás elleni védelem abszolút jellegűek és nem korlátozhatók.[164] A Kézikönyv ezt azzal illusztrálja, hogy "általában szükségesnek tartják az online véleménynyilvánítás szabadságának vagy a magánélethez való jognak a korlátozását a gyermekpornográfia és a gyermekek kizsákmányolásának megszüntetése, a szellemi tulajdonjogok védelme és a népirtásra való felbujtás megállítása érdekében".[165]

Az emberi jogok korlátozásának gyakorlása során a szakértők véleménye megoszlott az arányosság elvének alkalmazhatóságát illetően, a többség szerint az arányosság elvének alkalmazása mellett érveltek.[166] Valamennyi szakértő úgy vélte, hogy bármilyen korlátozásokat is alkalmaznak, azokat megkülönböztetés nélkül kell végrehajtani.[167]

A korlátozások mellett az államok bizonyos emberi jogi kötelezettségektől is eltérhetnek, amint azt a 38. szabály tárgyalja.[168] Ez a szabály teljes mértékben a szerződési jogra összpontosít, és teljes mértékben a szóban forgó szerződés konkrét rendelkezéseitől függ.

Az ebben a fejezetben a szakértők közötti nézeteltérések mértéke nemcsak az emberi jogi jog kiberjogi alkalmazását, hanem az emberi jogi jog általános elfogadottságát is érinti az államok között. A szakértők sok esetben megállapították, hogy az államok egyszerűen eltérnek - néha drámai mértékben - az emberi jogi jog alkalmazására vonatkozó nézeteikben. Ez a kiberműveleteknek az emberi jogi jogra való alkalmazásában is megmutatkozik. Ahogy az emberi jogi jog elsődleges szabályai tekintetében nagyobb egyértelműség alakul ki, kétségtelenül a kibertevékenységekre való alkalmazás is egyértelműbbé válik.

G. *Diplomáciai és konzuli jog*

A diplomáciai és konzuli jogról szóló fejezet nagymértékben támaszkodik a diplomáciai kapcsolatokról szóló 1961. évi bécsi egyezményre és az 1963. évi egyezményre.

---

162. *Id.* 201- 02 r. 37. o.

163. *Id.* 202., 1. pont (belső idézet kihagyva). 164.

Id. 202- 03, 4. pont.

165. *Id.* 203. o. (zárójelek és idézetek kihagyva).

166. *Id.* at 205, ¶ 9.

167. *Id.* at 206, ¶ 11 (belső hivatkozások kihagyva).

168. TALLINN MANUAL 2.0 A 38. szabály kimondja: "Egy állam eltérhet az emberi jogi szerződésekben vállalt, kibertevékenységekre vonatkozó kötelezettségeitől, ha az adott szerződés ezt megengedi, és az adott szerződés által meghatározott feltételek mellett". *Id.* 207. r. 38. o.

A konzuli kapcsolatokról szóló bécsi egyezményt, mint a nemzetközi szokásjogot lényegében reflektívnek.[169] Az első szabály a diplomáciai és konzuli jog egyik alapelvét, a helyiségek sérthetetlenségét érinti.[170] Bár a szabállyal valamennyi szakértő egyetértett, a szabály alkalmazása megosztott véleményeket váltott ki.

A többség úgy vélte, hogy ez a védelem kizárja a telephelyen található infrastruktúrát, a[171] , valamint a nem a telephelyen található, de diplomáciai vagy konzuli célokra használt diplomáciai vagy konzuli berendezéseket érintő távoli kibertevékenységet.[172] A szakértők egyformán megosztottak abban a kérdésben, hogy a harmadik államok kötelesek-e tiszteletben tartani a helyiségek sérthetetlenségét, vagy ez a kötelezettség csak a fogadó államot terheli.[173]

A 39. cikk vizsgálata a virtuális nagykövetségek és az online diplomáciai képviseletek megvitatására késztetett. A szakértők úgy vélték, hogy a sérthetetlenség nem terjed ki ezekre a virtuális képviseletekre, kivéve, ha a fentiekben tárgyaltak szerint a helyiségekben való elhelyezés védi őket.[174] A 40. szabály előírja, hogy "[a] fogadó állam köteles minden megfelelő lépést megtenni a küldő állam diplomáciai képviseletének vagy konzuli képviseletének helyiségeiben lévő kiberinfrastruktúra behatolás vagy károsodás elleni védelme érdekében".[175] E szabály alkalmazása függ "a helyiségeket fenyegető veszély nagyságától, attól, hogy a fogadó állam milyen mértékben van tudatában a konkrét fenyegetésnek, és hogy a fogadó állam milyen mértékben képes megtenni az adott körülmények között."[176]

A 41. szabály a diplomáciai és konzuli irattárakra, dokumentumokra és hivatalos levelezésre biztosított védelmet alkalmazza ezek elektronikus változataira is.[177] A szakértők véleménye azonban megoszlott a külképviseletekhez vagy konzuli képviseletekhez intézett magánadományok tekintetében, a többség úgy vélte, hogy ezekre a szabály kiterjesztése vonatkozik.[178] A helyiségekhez hasonlóan a szakértők véleménye megoszlott a harmadik személyek kötelezettségét illetően.

---

169. *Id.* at 209, ¶ 1.

170. A TALLINN MANUAL 2.0 39. szabálya kimondja, hogy "A diplomáciai misszió vagy konzuli képviselet területén lévő kiberinfrastruktúrát a misszió vagy a konzuli képviselet sérthetetlensége védi". *Id.* 212. r. 39.

171. *Id.* at 213-14, ¶¶ 5- 6.

172. *Id.* at 215-16, ¶¶ 10 -12.

173. *Id.* at 214, ¶ 6.

174. *Id.* at 216 -17, ¶ 15.

175. *Id.* 217. r. 40.

176. *Id.* 217-18, 2. pont.

177. A TALLINN MANUAL 2.0 41. szabálya kimondja: "A diplomáciai képviselet vagy konzuli képviselet elektronikus formában lévő iratai, dokumentumai és offizikai levelezése sérthetetlenek". *Id.* 219. r. 41. o.

178. *Id.* 220, 4. pont.

államok diplomáciai vagy konzuli levéltárakra, dokumentumokra és levelezésre, a többség ismét kiterjesztette a védelmet.[179] A szakértők megosztottak abban a kérdésben is, hogy a védelem továbbra is vonatkozzon-e a misszió és a küldő állam közötti kommunikáción kívüli, például a misszió és harmadik államok közötti kommunikációra. A többség úgy vélte, hogy minden ilyen kommunikáció védelmet élvez.[180] Végezetül felmerült a kérdés a harmadik felek által nyilvánosságra hozott, általában védett közlésekkel kapcsolatban. Ebben az esetben a többség úgy vélte, hogy a védelem már nem érvényesül.[181]

A 42. szabály a kommunikáció szabadságához való joggal foglalkozik, és kimondja, hogy "a fogadó államnak engedélyeznie és védenie kell a diplomáciai képviselet vagy konzuli képviselet szabad kiberkommunikációját minden társadalmi célból".[182] A szakértők egyetértettek abban, hogy a fogadó államok "nem akadályozhatják a diplomáciai képviselet vagy konzuli képviselet olyan weboldalához való hozzáférést, amelyet arra használnak, hogy alapvető információkat közvetítsenek az országban tartózkodó állampolgáraiknak, nem szakíthatják meg vagy lassíthatják le a diplomáciai képviselet vagy konzuli képviselet internetkapcsolatát, nem blokkolhatják vagy zavarhatják a mobiltelefonjait vagy más távközlési berendezéseit".[183] Az ebben a szabályban szereplő "védelem" követelménye hasonlít a kellő gondossági szabályhoz, mivel továbbra sincs kötelezettség a megfigyelésre vagy a megelőzésre irányuló proaktív intézkedések megtételére, hanem csupán az evés orvoslására, ha a fogadó állam tudomást szerez róla.

A 43. szabály az államok helyiségeivel és személyzetével foglalkozik, és így szól:

> (a) [A diplomáciai képviselet vagy konzuli képviselet helyiségei nem használhatók olyan kibertevékenységek végzésére, amelyek összeegyeztethetetlenek a diplomáciai vagy konzuli feladatokkal, és b) a diplomáciai és konzuli képviselők nem folytathatnak olyan kibertevékenységeket, amelyek beavatkoznak a fogadó állam belügyeibe vagy összeegyeztethetetlenek a jogszabályokkal.[184]

A szakasz ezután felsorol néhány olyan kibertevékenységet, amelyek e szabály alapján kiberkörnyezetben megengedettek lennének. Fontos, hogy a szakértők arra a következtetésre jutottak, hogy a kiberkémkedés nem lenne megengedett.[185] A szakasz a diplomáciai képviselők kiváltságaira és mentességeire vonatkozó szabállyal zárul.

179. *Id.* 221-23, 7-10. pont.
180. *Id.* 224., 14-15. pont.
181. *Id.* , ¶ 14.
182. *Id.* 225. r. 25.
183. *Id.* 226., 3. pont.
184. *Id.* 227-28. r. 43.
pont.
185. *Id.*

matikus és konzuli személyzet,[186] és arra a következtetésre jut, hogy ugyanazok a kiváltságok és mentességek vonatkoznak a kibernetikai tevékenységekre is.[187]

Nyilvánvalóan számos megválaszolatlan kérdés van a kiberműveletekkel, valamint a diplomáciai és konzuli joggal kapcsolatban, különösen a kommunikációval kapcsolatban. Mivel e kommunikáció nagy része ma már kibernetikai eszközökön keresztül történik, a nemzetközi jog alkalmazása ezen a területen a jogi fejlődés fontos területe lesz.

H. *Tengeri jog*

A tengerjog hosszú múltra visszatekintő és a közelmúltban jelentős mértékben kodifikált speciális rendszer. A szakértők egyetértettek abban, hogy az Egyesült Nemzetek Tengerjogi Egyezményének nagy része[188] reflected custom ary international law, és következésképpen a szakértők nagymértékben támaszkodtak rá.[189]

A 45. szabály az alkalmazhatóság általános elvét fogalmazza meg, és kimondja, hogy "a nyílt tengeren folytatott hajózási műveletek csak békés céllal végezhetők, kivéve, ha a nemzetközi jog másként rendelkezik".[190] Példaként a szakértők arra a következtetésre jutottak, hogy "[a] kibertérrel összefüggésben különösen fontosak a nyílt tengeren való hajózás, a feletti repülés és a tenger alatti kábelek fektetésének szabadsága. Például az első két szabadság alapján mind a repülőgépek, mind a hajók jogosultak kiberműveleteket végezni a nyílt tengeren és a nyílt tengeren mindaddig, amíg nem sértik az alkalmazandó nemzetközi jogot".[191] A katonai kiberműveletek tekintetében a szakértők "nem láttak okot arra, hogy eltérjenek attól az általános elvtől, hogy a tiltott erő alkalmazásával nem járó katonai tevékenységek a nyílt tengeri szabadságok és a tenger egyéb nemzetközileg jogszerű használatának körébe tartoznak, ahogyan azt a tengerjogi egyezmény 87. cikkének (1) bekezdése meghatározza".[192] A szakértők megerősítették a "látogatási jogot" a kibertevékenységek tekintetében[193] , de megosztottak a "virtuális látogatás" megengedhetőségét illetően, ami azt jelenti, hogy

186. A TALLINN MANUAL 2.0 44. szabálya kimondja: "Amennyiben a diplomáciai képviselők és konzuli officerek mentességet élveznek a büntetőjogi, polgári jogi és közigazgatási joghatóság alól, a kibertevékenységük tekintetében is mentességet élveznek.". *Id.* 230. r. 44. pont.

187. *Id.* 231, 1-4. pont.

188. Az Egyesült Nemzetek Tengerjogi Egyezménye, 1982. december 10., 1833 U.N.T.S. 3.

189. TALLINN MANUAL 2.0, 14. lábjegyzet, 232. o., 1-2.

pont. 190. *Id.* 233. r. 45. o.

191. *Id.* 234., 3. pont (idézetek kihagyva).

192. *Id.* , ¶ 5 (idézetek kihagyva).

193. TALLINN MANUAL 2.0 A 46. szabály kimondja, hogy "A hadihajó vagy más megfelelően felhatalmazott hajó a nyílt tengeren vagy a kizárólagos gazdasági övezeten belül a flag állam beleegyezése nélkül gyakorolhatja a látogatás jogát egy hajó fedélzetére való felszálláshoz, ha alapos okkal gyanítja, hogy a hajó kibernetikai eszközöket használ fel.

a látogatás lebonyolítása kibernetikai eszközökkel.[194] A szakértők megerősítették továbbá a kellő körültekintés követelményének alkalmazását a kizárólagos gazdasági övezetben (EEZ) végrehajtott kibernetikai műveletekre,[195] bár a szakértők véleménye megoszlott az EEZ-ben végrehajtott katonai műveletek jogszerűségét illetően, mivel a többség szerint azok megengedettek.[196]

A parti tenger és az ártatlan áthaladás joga tekintetében a szakértők megállapodtak a 48. szabályban, amely kimondja, hogy "[a]zért, hogy egy hajó igényt tarthasson az ártatlan áthaladás jogára egy parti állam parti tengerén, a hajó által végzett bármilyen kibernetikai műveletnek meg kell felelnie az e jogra vonatkozó feltételeknek".[197] A szakértők segítőkészen felsoroltak néhány példát az olyan kibertevékenységekre, amelyek az áthaladást nem ártalmatlanná tennék.[198] A szakértők megvizsgálták, hogy milyen hatással lenne az ártatlan áthaladásra, ha egy A államból származó állami hajó B állam felségvizein kiberműveleteket hajtana végre C állam ellen. A szakértők többsége úgy ítélte meg, hogy ez nem lenne összeegyeztethető az ártatlan áthaladással.[199]

Annak ellenére, hogy a Kézikönyv a nemzetközi fegyveres konfliktusra vonatkozó legtöbb szabályt a Kézikönyv későbbi részeire tartja fenn, a 49. szabály kimondja, hogy "nemzetközi fegyveres konfliktus során a semleges parti állam nem tehet különbséget a harcoló felek között az adott állam felségvizein végrehajtott kiberműveletek tekintetében".[200] Az 50. szabály visszatér az általánosabb szabályokhoz, és a parti tengeren belüli végrehajtási joghatósággal foglalkozik.[201] Az előadók megosztottak a végrehajtási joghatóság kiváltásához szükséges potenciális következmények mértékét illetően. A többség úgy érvelt, hogy bármilyen jogsértés elegendő, a kisebbség viszont úgy vélte, hogy a *de minimis* hatások

---

kalózkodásra, rabszolga-kereskedelemre vagy engedély nélküli műsorszórásra készül; állampolgársággal nem rendelkezőnek tűnik; vagy a látogató hajó állampolgárságával rendelkezik." *Id.* 235. o.

194. *Id.* at 238, ¶ 10.

195. TALLINN MANUAL 2.0 A 47. szabály kimondja: "Jogai és kötelezettségei gyakorlása során egy másik állam kizárólagos gazdasági övezetében kiberműveleteket végző államnak kellően figyelembe kell vennie az adott államnak az övezetben fennálló jogait és kötelezettségeit, és a kiberműveleteket békés célokra kell végezni, kivéve, ha a nemzetközi jog másként rendelkezik.". *Id.* 239. o.

196. *Id.* at 240, ¶ 4.

197. *Id.* 241. sz. 48.
pont.

198. *Id.* at 242-43, ¶ 6-7.

199. *Id.* 243., 8. ¶

200. *Id.* 245. r. 49.

201. A TALLINN MANUAL 2.0 50. szabálya kimondja: "A parti állam a parti tengeren lévő hajók fedélzetén végrehajtási joghatóságot gyakorolhat a számítógépes műveletekkel járó bűncselekmények tekintetében, ha: a bűncselekmény következményei a parti államra is kiterjednek; a bűncselekmény olyan jellegű, hogy megzavarja a parti állam közrendjét és biztonságát vagy a parti tenger rendjét; a hajó parancsnoka vagy a flagállam kérte a parti állam hatóságainak segítségét; vagy ha szükséges a kábítószer-csempészet elleni küzdelemhez.". *Id.* 246. r. 50. o.

nem váltaná ki a jogot.[202]

A szakértők azzal érveltek, hogy a tengerjog általános rendelkezései vonatkoznak a kiberműveletekre az egybefüggő övezetben, a[203] nemzetközi tengerszorosokban, a[204] szigetvizeken, a[205] és a tenger alatti kábelekre.[206] A tenger alatti kábelek tekintetében a szakértők nem tudtak megegyezni a joghatóság alkalmazásában "a parti állam és a tenger alatti kommunikációs kábelt a parti állam kontinentális talapzatán vagy kizárólagos gazdasági övezetében fektető állam között".[207] Bár a szakértők egyetértettek abban, hogy a tenger alatti hírközlési kábelek megrongálása sérti a nemzetközi jogot, abban is egyetértettek, hogy az ilyen kábeleket adatgyűjtés és adattovábbítás céljából le lehet csapolni.[208]

A kézikönyv maga is rámutat azokra a területekre, ahol a kiberműveletek tekintetében a tengerjog még nem rendezett, például arra, hogy az államoknak meg kell találniuk egy módszert a nyílt tenger alatti tengeralattjáró kommunikációs kábelek szándékos vagy gondatlan megrongálásának büntethetőségére.[209] Tekintettel a tenger alatti kommunikációs kábeleken keresztül áthaladó hatalmas adatmennyiségre és az államok egyre növekvő hozzáférési képességére, ez szinte biztosan olyan terület, ahol az állami gyakorlat tovább fog fejlődni.

I. *Levegőjog*

A tengerjoghoz hasonlóan a szakértők megállapították, hogy a nemzetközi jogot általában az adott terület legjelentősebb szerződésének rendelkezései határozzák meg[210] - ebben az esetben a nemzetközi polgári repülésről szóló 1944. évi ICAO-egyezmény, vagy ahogyan ismertté vált, a "Chicagói Egyezmény".[211] A fejezetben használt kifejezésekre valóban az alábbiak vonatkoznak

---

202. *Id.* 247, 4. pont.

203. A TALLINN MANUAL 2.0 51. szabálya kimondja: "A parti állam szomszédos övezetében található hajók tekintetében az adott állam kibernetikai eszközöket használhat arra, hogy megakadályozza vagy kezelje a területén vagy a parti tengeren belül a fizetési, bevándorlási, egészségügyi vagy vámjogszabályai megsértését, beleértve a kibernetikai eszközökkel elkövetett jogsértéseket is.". *Id.* 248. o.

204. TALLINN MANUAL 2.0 Az 52. szabály kimondja: "A nemzetközi hajózásra használt szorosban végzett kibernetikai műveleteknek összhangban kell lenniük a tranzitátkelési joggal". *Id.* 249. o.

205. A TALLINN MANUAL 2.0 53. szabálya kimondja: "A szigetközi vizeken végzett kibernetikai műveleteknek összhangban kell lenniük az ott alkalmazandó jogi rendszerrel". *Id.* 251. o.

206. TALLINN MANUAL 2.0 Az 54. szabály kimondja: "A tenger alatti kábelekre alkalmazandó nemzetközi jog szabályai és elvei a tenger alatti hírközlési kábelekre is

vonatkoznak.". *Id.* 252. pont.

207. *Id.* at 255, ¶ 9.

208. *Id.* 257., 17.

pont.

209. *Id.* at 258, ¶ 19 (belső hivatkozások

kihagyva). 210. *Id.* 259-60. o., 4-6. pontok.

211. A Nemzetközi Polgári Repülési Szervezet egyezménye a nemzetközi polgári repülésről, 1944. december 7., 61 Stat. 1180, 15 U.N.T.S. 295.

az ICAO definíciók szerint.[212]

Az 55. szabály[213] a légtérjog általános alkalmazhatóságának szabályát mondja ki a nemzeti légtérben lévő légi járművek kiberműveleteire. A szakértők megjegyezték, hogy ez a speciális rendszer csak a légi járműre vonatkozik, az általa végzett kiberműveletekre nem. Ezekre a műveletekre más jogszabályok, például az alárendelt állam jogszabályai vonatkoznak.[214] A katonai repülőgépek tekintetében - amelyek a legnagyobb valószínűséggel részt vesznek a légi kiberműveletekben - a szakértők megjegyezték, hogy az egyezmény a szomszédos állam engedélyét írja elő a légi feletti felhajtáshoz, és megengedi a szomszédos államnak, hogy meghatározza a légi felhajtás feltételeit, amelyek között szerepelhet a kiberműveletek tilalma.[215]

A szakértők megosztottak abban a kérdésben, hogy miként kell minősíteni egy állam légterének egy másik állam kiberműveletekben részt vevő katonai repülőgépe általi megsértését. Egy kisebbség úgy vélte, hogy a beleegyezés nélküli jelenlét és a kiberműveletek végzésének kombinációja elegendő ahhoz, hogy fegyveres támadásnak minősüljön, és kiváltsa az önvédelem jogát. A többség úgy vélte, hogy a minősítés a kiberművelet jellegétől függ. A szakértők egy része azon a véleményen volt, hogy egy katonai repülőgép puszta beleegyezés nélküli jelenléte is feljogosít az erő alkalmazására a repülőgépnek az állam területéről való kiutasítása érdekében.[216]

A nemzeti légtérrel ellentétben a nemzetközi légtérben általában engedélyezettek a kiberműveletek. Az 56. szabály kimondja, hogy "[a]z állam a nemzetközi jogban foglalt korlátozásokra is figyelemmel végezhet kiberműveleteket a nemzetközi légtérben".[217] Az államok nem tarthatnak igényt a nemzetközi légtér feletti fennhatóságra. Ezen túlmenően a nemzetközi légtérben végzett kiberműveletek során az államokat csak a nemzetközi jog olyan tilalmak korlátozzák, mint a beavatkozás és az erőszak alkalmazásának tilalma, vagy az elfogadott navigációs rendszerek, mint például a nemzetközi tengerszorosok feletti repülés.[218] Ezen túlmenően, ha a navigációs rendszer hatálya alá tartozó, a normál üzemmódban történő szállítást megkövetelő repülés esetén a szakértők többsége úgy ítélte meg, hogy ez nem terjed ki az aktív kiberműveletekre, még olyan légi járművek esetében sem, amelyek célja támadó kiberműveletek végrehajtása.[219]

---

212. TALLINN MANUAL 2.0, *fentebb* 14. lábjegyzet, 260. o.

213. A TALLINN MANUAL 2.0 55. szabálya szerint "Az állam szabályozhatja a légi járművek üzemeltetését, beleértve a kiberműveleteket végző légi járműveket is, nemzeti légterében". *Id.* 261. o.

214. *Id.* at 263, ¶ 6.

215. *Id.* 264.

216. *Id.* 264-65, 12-13. pont.

217. *Id.* 265. r. 56.

218. *Id.* at 266, ¶ 4. 219.

Id. 266-67. o., 5. pont.

Végül, az államok nem végezhetnek olyan kiberműveleteket, amelyek veszélyeztethetik a nemzetközi légi közlekedés biztonságát.[220]

Amint azt korábban említettük, legalábbis a szuverenitás tekintetében a[221] állami gyakorlat a kibertérrel szemben nem tekint olyan korlátozóan, mint a légtérrel szemben. A kiberműveleteknek a levegőben lévő platformokról történő végrehajtására irányuló állami képességek növekedése potenciálisan a paradigmák összeütközését eredményezi, amikor a kevésbé korlátozó kibertéri paradigma átadja helyét a légtérre vonatkozó szigorúbb szabályoknak. Az alább tárgyalt liberálisabb űrrendszerrel szemben ez a jogi szabályozásbeli különbség a kibertechnológiai fejlesztéseket - különösen a szuverenitás elve tekintetében - a légi eszközök helyett a világűrbe terelheti.

J. *Űrjog*

Bár a légtérre és a világűrre irányadó jog közötti térbeli különbségtétel nem pontosan definiált,[222] a két rendszer közötti különbségek meglehetősen markánsak, különösen a szuverén hatalom gyakorlása tekintetében. A szakértők különbséget tettek a világűr által lehetővé tett kiberműveletek között, amelyekre a világűrre vonatkozó jog csak korlátozottan alkalmazható, és a világűr által lehetővé tett kiberműveletek között.[223] A szabályok kidolgozásakor a szakértők megjegyezték, hogy az alkalmazandó szerződéses jog kevésbé teljes és kevésbé elismert szokásjogot kodifikáló. Azokban az esetekben azonban, amikor a szakértők a különböző űrszerződések nyelvezetére támaszkodtak, ezt olyan rendelkezések alkalmazásával tették, amelyekről úgy vélték, hogy szokásjognak minősülnek.[224]

Az 58. cikk megállapítja, hogy a Holdon és más égitesteken, illetve általában az űrben a kibernetikai eszközök használatára vonatkozó jogi tilalmak eltérnek egymástól. A szabály kimondja: "a) [c]yberműveletek a Holdon és más égitesteken csak békés célokra végezhetők.
(b) A világűrben végzett kiberműveletekre az erő alkalmazására vonatkozó nemzetközi jogi korlátozások vonatkoznak."[225] A szakértők ebből a szabályból azt a következtetést vonták le, hogy a Holdon nem lehet támadó kiberképességeket elhelyezni, míg a világűrre általánosságban nem létezik hasonló tilalom.[226] Az űr tekintetében általánosságban a kiberképességek használatára vonatkozó tilalom ugyanazok a normák érvényesek

---

220. A TALLINN MANUAL 2.0 57. szabálya szerint "Egy állam nem végezhet olyan kiberműveleteket, amelyek veszélyeztetik a nemzetközi polgári repülés biztonságát". *Id.* 268. o.

221. *Lásd fentebb a* III.A. szakaszt.

222. TALLINN MANUAL 2.0, *supra* note 14, 259-60. o., 1-11. pont; *lásd még id.* 271. o., 3-4. pont. 223. *Id.* 270-71. pont, 2-3. bekezdés.

224. *Id.* at 272, ¶ 6.

225. *Id.* 273. o., 58. pont.

226. *Id.* 273-75, 1-7. pontok.

kötet

mint a földön, beleértve az ENSZ Alapokmányát is.[227]

Az 59. szabály kimondja: "a) [egy] államnak tiszteletben kell tartania a lajstromozó államok azon jogát, hogy joghatóságot és ellenőrzést gyakoroljanak a lajstromukban szereplő űreszközök felett. (b) Egy államnak a világűrrel kapcsolatos kibernetikai műveleteit a más államok békés célú űrtevékenységeibe való beavatkozás elkerülésének szükségességére kellő figyelemmel kell végeznie."[228]

E szabállyal összhangban a szakértők egyetértettek abban, hogy az államoknak joghatóságuk van műholdjaik és más űreszközök, valamint az azokon tartózkodó személyek felett, de azt is megjegyezték, hogy ez a joghatóság nem feltétlenül kizárólagos. Például, ha az egyik állam űreszközök tevékenységei érintik egy másik állam űreszközeit, akkor ezek az államok osztozhatnak az egyidejű joghatóságon.[229] A szakértők azt is megjegyezték, hogy a "kellő figyelembevétel" kifejezés ebben a szabályban ugyanazt a jelentést hordozza, mint a tengerjoggal összefüggésben.[230]

Végül, az államoknak a világűrben végzett kibertevékenységekkel kapcsolatos felelősségét illetően a 60. szabály kimondja: "a) [egy] államnak engedélyeznie és felügyelnie kell a nem kormányzati szerveinek kiber-"tevékenységeit a világűrben". (b) Az űrbeli objektumokat érintő kiberműveletekre az űrjog felelősségi és felelősségi rendszere vonatkozik."[231]

Ahogy egyre több magánszervezet kezd el tevékenykedni a világűrben, beleértve személyek űrbe juttatását is, a[232] egyre fontosabbá válik ez a szabály. A szabály követi a szerződési jogot, amikor az irányítási rendszert "nemzeti" jellegűnek minősíti.[233] Az államoknak felelősséget kell vállalniuk a nem kormányzati szervek tevékenységének ellenőrzéséért és jóváhagyásáért.

Ennek megfelelően az államok általában felelősek tetteikért az űrjogi rendszer alapján, amely magában foglalja az állami felelősségről szóló cikkek néhány alapelvét.[234] Például az indító államok felelősek a másik államnak az űrből történő indítással okozott károkért.[235] Az űreszközöknek más űreszközök által okozott károk azonban a "vétkességen" alapulnak.[236] A szakértők megállapították, hogy ezek az elvek a következőkre vonatkoznak

---

227. *Id.* at 275-77, ¶¶ 8 -11.

228. *Id.* at 277, ¶ 4.

229. *Id.* 278. o., 6. n. 229. pont.

230. *Id.* at 279, ¶ 6.

231. *Id.* 279. o. - 80 r. 60. o.

232. Calla Cofield, *SpaceX to Fly Passengers On a Private Trip Around the Moon in 2018*, SPACE.COM (2017. február 27., 18:53), http://www.space.com/35844-elon-musk-spacex announcement-today.html.

233. TALLINN MANUAL 2.0, *supra* note 14, 280. pont, 1. bekezdés (belső idézőjelek és idézőjelek kihagyva).

234. *Id.* 281., 4. n. 700. pont.

235. *Id.* 281-82., 7. pont.

236. *Id.* at 282, ¶ 8.

kiberműveletek az űrben is.

A világűrbe történő folyamatos terjeszkedés magában foglalja a kiberképességek fokozott alkalmazását. A világűrre vonatkozó jogszabályokat akkor fogalmazták meg, amikor még kevés államnak volt hozzáférése a világűrhöz, és meglehetősen megengedőek, különösen a légtérre vonatkozó szabályokhoz képest.[237] Ahogy egyre több állam - beleértve az államokon belüli magánszervezeteket is - kezd műveleteket folytatni a világűrben, beleértve a kiberműveleteket is, a megengedő rendszer átadhatja helyét egy korlátozóbb rendszernek. Jelenleg legalább egy jelentős transznacionális erőfeszítés folyik a világűrre alkalmazandó jogi rendszer alaposabb vizsgálatára[238] , és ez kétségtelenül rendkívül hasznos információkkal fog szolgálni ebben a fontos témában.

K. *Nemzetközi távközlési jog*

A Kézikönyv korábbi szakaszaitól eltérően, amelyek elsősorban a nemzetközi szokásjogra támaszkodtak az abban foglalt szabályok alátámasztására, a Kézikönyv ezen szakaszában a szakértők megjegyzik a szokásjog hiányát, és a következő szabályokat kifejezetten a Nemzetközi Távközlési Unió szerződéses rendszerére alapozzák.[239] A szakértők ezt azért érezték kényelmesnek, mert "majdnem minden állam részes fele a szerződéses rendszernek".[240]

A 61. szabály kimondja, hogy "[egy] államnak intézkedéseket kell tennie a gyors és folyamatos nemzetközi távközléshez szükséges nemzetközi távközlési infrastruktúra kiépítésének biztosítására". Ha az állam e követelménynek eleget téve a nemzetközi távközléshez kiberinfrastruktúrát hoz létre, akkor ezt az infrastruktúrát fenn kell tartania és védenie kell".[241] A szerződéses rendszer három különböző kötelezettséget állapít meg a tagállamok számára: "a gyors és zavartalan nemzetközi távközlést elősegítő infrastruktúra létrehozásának biztosítására; az infrastruktúra védelmére; és fenntartására".[242] A szakértők megjegyezték, hogy ezek a kötelezettségek a kon dukcióra, nem pedig az eredményre vonatkoznak, és ezért a megvalósíthatóságon alapulnak.[243] Így egy államnak nem kell kibernetikai eszközökkel teljesítenie a kötelezettségét, de ha úgy dönt, hogy

---

237. U.S. DEP'T OF DEFENSE, OFFICE OF GENERAL COUNSEL, AN ASSESSMENT OF INTERNATIONAL LEGAL ISSUES IN INFORMATION OPERATIONS 2 (2d ed.1999).

238. *Lásd: Manual on International Law Applicable to Military Uses of Outer Space*, MCGILL UNIVERSITY, http://www.mcgill.ca/milamos/ (utolsó látogatás 2017. június 4-én).

239. TALLINN MANUAL 2.0, 14. lábjegyzet, 284. pont, 2. bekezdés.

240. *Id.*

241. *Id.* 288. r. 61.

242. *Id.* , ¶ 2.

243. *Id.* 289-90, 3. pont.

ezt megteheti, meg kell védenie és fenn kell tartania ezt a kiberinfrastruktúrát.[244] Mivel ez a kötelezettség állami kötelezettség, a szakértők többsége úgy vélte, hogy nem jogszerű, ha egy állam a második állam beleegyezése nélkül létesít kommunikációs hálózatot egy másik államban.[245]

A szakértők megállapították, hogy az államok általában gyakorolhatják szuverén hatáskörüket a kommunikáció felfüggesztésére vagy leállítására. A 62. szabály kimondja:

> (a) [egy] állam részben vagy egészben felfüggesztheti a területén belüli nemzetközi kiberkommunikációs szolgáltatásokat. Az ilyen felfüggesztésről a többi államot haladéktalanul értesíteni kell. (b) Egy állam leállíthatja a nemzeti jogszabályaival, a közrenddel vagy a tisztességgel ellentétesnek tűnő, vagy a nemzetbiztonságra veszélyes magánkommunikáció továbbítását.[246]

A szakértők azonban megjegyzik a kommentárban, hogy "ez a jog nem sérti az érintett államot terhelő olyan nemzetközi jogi kötelezettségeket, amelyek egy adott esetben megtiltják ezt"[247] , mint például a diplomáciai kommunikáció.[248] Feltételezve, hogy a kommunikációt felfüggesztették, a szakértők megosztottak abban a kérdésben, hogy jogszerű-e, ha egy másik állam a területi állam beleegyezése nélkül helyreállítja a kommunikációt. A többség egyetértett abban, hogy az ilyen intézkedés nem lenne jogszerű a területi állam beleegyezése nélkül.[249]

A konkrét kommunikáció tekintetében a szakértők egyetértettek abban, hogy a konkrét magánjellegű kiberkommunikáció megállítása magában foglalhat "azonnali üzenetet, e-mailt vagy tweetet".[250]

A 63. szabály kimondja, hogy "[egy] állam rádióállomások használata nem zavarhatja károsan más államok védett rádiófrekvencia-használatát vezeték nélküli kiberkommunikációra vagy -szolgáltatásokra".[251] A szakértők elfogadták a káros zavarás definícióját, amely szerint az olyan zavarás, amely "veszélyezteti a rádiónavigációs szolgálat működését vagy . . . vagy súlyosan rontja, akadályozza vagy ismételten megszakítja a [Nemzetközi Távközlési Szabályzat] szerint működő rádiótávközlési szolgáltatást.

---

244. *Lásd id.*
245. *Id.* 290-91., 9-10. pont.
246. *Id.* 291. r. 62. a)-b) pont.
247. *Id.* at 291-92, ¶ 1.
248. *Id.* 294, 9. pont.
249. *Id.* 293-94. pont,
6. bekezdés.
250. *Id.* 294, 7. pont.
251. *Id.* r. 63.

munication Union] Rádiószabályzat."[252] Megállapodtak továbbá abban, hogy a szabály "kizárólag azokra az interferenciákra vonatkozik, amelyeket egy állam okoz egy másik államnak a kiberkommunikációt vagy -szolgáltatást lehetővé tevő frekvenciák használatában, bárhol is történjen az ilyen kommunikáció vagy szolgáltatás, beleértve a világűrt is".[253]

Végül a 64. szabály kivételt tesz a katonai rádióállomások alól, és kimondja, hogy "[egy] állam a nemzetközi távközlési jog alapján teljes szabadságot tart fenn a katonai rádióállomások tekintetében".[254] Bár a szabály a rádióberendezésekre korlátozódik, a szakértők egyetértettek abban, hogy az "a rádióhullámokon keresztül történő vezeték nélküli adatátvitelt lehetővé tevő eszközökre" is vonatkozik.[255] A szakértők leszögezték, hogy a mentesség csak a valóban "katonai" létesítményekre vonatkozik, más, a hadsereg által kettős katonai és polgári célú használatba vett rádióberendezésekre nem.[256]

Bár ez a rendszer szinte teljes egészében szerződésen alapul, és ezért nem tekinthető kötelező erejű nemzetközi szokásjognak, az államok közötti távközlés gyakorlata olyan normákat és gyakorlatokat fog kialakítani, amelyek kétségtelenül segíteni fogják a kibertérrel kapcsolatos szabályok kialakítását. Például egy államnak az e rendszer szerinti távközlési kommunikáció leállítására vagy felfüggesztésére vonatkozó jogának és az egyéni internet-hozzáférésre vonatkozó, kialakulóban lévő emberi jogi elvárásoknak a kölcsönhatása a jövőben is újra fogja határozni, hogy az államok milyen jogi kötelezettségeket fogadnak el a kibertérrel kapcsolatban.

L. *A viták békés rendezése*

Ez a szakasz jelzi a kézikönyv "Nemzetközi béke és biztonság és kibertevékenységek" című fejezetre való áttérésének kezdetét. E szakasz első három szabálya átvezetésként szolgál az erő alkalmazására vonatkozó szabályokhoz (*just ad bellum*) és a fegyveres összeütközésre vonatkozó szabályokhoz (*jus in bello)*. Mivel a figyelem első három szabályával a Tallinn 1.0 nem foglalkozik, itt megérdemelnek némi megjegyzést.

A 65. szabály az államok azon kötelezettségére vonatkozik, hogy vitáikat békés úton rendezzék, és az ENSZ Alapokmány 2. cikkének (3) bekezdésén és 33. cikkének (1) bekezdésén alapul[257] és

---

252. *Id.* 296., 7. n. 728. pont (belső hivatkozások kihagyva). 253. *Id.* 296-97. o., 8. pont.

254. *Id.* 298. r. 64.

255. *Id.*, 299. pont, 2. bekezdés.

256. *Id.* , ¶ 4 (belső idézet kihagyva).

257. ENSZ Alapokmány, cikk. 2(3) bekezdése kimondja: "Minden tag köteles nemzetközi vitáit békés eszközökkel rendezni oly módon, hogy a nemzetközi béke és biztonság, valamint az igazságosság ne kerüljön veszélybe." Art. 33. cikkének (1) bekezdése kimondja: "A felek minden olyan vitában, amelynek fennállása veszélyeztetheti a nemzetközi béke és biztonság fenntartását, mindenekelőtt figyelemmel és

általánosan elfogadott nemzetközi szokásjog.[258] A szabály kimondja: "a) Az államoknak meg kell kísérelniük, hogy a nemzetközi békét és biztonságot veszélyeztető kibertevékenységeket érintő nemzetközi vitáikat békés eszközökkel rendezzék; b) Ha az államok megkísérlik a nemzetközi békét és biztonságot nem veszélyeztető kibertevékenységeket érintő nemzetközi vitáikat békés eszközökkel rendezzék.".[259]

A szakértők egyetértettek abban, hogy ez a szabály csak a nemzetközi vitákra vonatkozik, "a tisztán belső vitákra nem".[260] A szakértők azonban nem értettek egyet abban, hogy egy állam és egy nem állami szereplő közötti transznacionális vitára is alkalmazható-e, és csak egy kisebbség gondolta úgy, hogy az ilyen viták is a szabály hatálya alá tartoznak.[261] E nézeteltérés ellenére a szakértők egyetértettek abban, hogy a "béke teljes eszközei", amennyiben szükséges, nem korlátozzák a törvényes eszközökhöz való folyamodást, mint például az ellenintézkedések vagy az önvédelemben történő erőszak alkalmazása, illetve az Egyesült Nemzetek Biztonsági Tanácsa által engedélyezett bármely intézkedés.[262]

Az államoknak jóhiszeműen meg kell próbálniuk békés úton rendezni kibervitáikat,[263] de nem kell, hogy sikerrel járjanak, és nem kell, hogy kimerítsenek minden lehetséges békés eszközt ahhoz, hogy ennek a kötelezettségnek eleget tegyenek.[264] A szakértők abban is egyetértettek, hogy ez a kötelezettség még ellenségeskedés idején is fennáll, ha egy adott kibervitát illetően a békés eszközök továbbra is nyitva állnak.[265] A szakértők egyetértettek továbbá abban, hogy az államoknak akkor is békés eszközöket kell alkalmazniuk, ha olyan nemzetközi viták megoldására törekszenek, amelyek nem veszélyeztetik a nemzetközi békét és biztonságot, de az államok nem kötelesek megkísérelni a nemzetközi viták megoldását, ha nem ezt választják.[266]

Tekintettel a nemzetközi és transznacionális kiberviták növekvő számára, ez a szabály rendkívül fontos. Az államok közötti[267] és az államok és a nem állami szervezetek közötti legújabb kiberviták

---

tárgyalás, megkeresés, közvetítés, békéltetés, választottbíráskodás, bírósági rendezés, regionális ügynökségek vagy megállapodások igénybevétele, vagy más, saját választásuk szerinti békés eszköz."

258. *Lásd* TALLINN MANUAL 2.0, 14. lábjegyzet, 303. pont, 1. bekezdés.

259. *Id.* 304.

260. *Id.* 304., 2. pont.

261. *Id.* 305, 6-7. pont.

262. *Id.* 307., 11. és 13.

pont. 263. *Id.* 308., 14.

pont. 264. *Id.* 309. pont,

17-18. bekezdés.

265. *Id.* at 309-10, ¶ 20-21.

266. *Id.* at 310, ¶ 22-23.

267. *Lásd* Gina Chon, *U.S. Pursues Case Against Chinese Army Hackers*, FINANCIAL TIMES (2015. szeptember 24.), https://www.ft.com/content/a378b4c6-62b0-11e5-9846-de406ccb37f2 (a kiberlopás miatt öt kínai katonatiszt ellen emelt amerikai vádat); Jane Perez, *Xi Jingping Pledges to Work With U.S. to Stop Cybercrimes*, N.Y. TIMES (2015. szeptember 22.) https://www.nytimes.com/2015/09/23/.

szereplők[268] általában békés eszközökkel oldották meg, de a kiberintervenciók súlyosságának növekedésével ez a szabály valószínűleg próbára lesz téve. Putyin orosz elnök látszólag elutasítóan nyugtázta, hogy
a "hazafias" oroszok amerikai választásokba való beavatkozásáról,[269] dis
A következő szakaszban tárgyalt, a[270] kellő gondosság, a[271] , valamint a megtorlás és az ellenintézkedések jogorvoslati lehetőségeinek[272] kibertevékenységekre való alkalmazása során az egyértelműség fontosságát hangsúlyozza. Minél hatékonyabbnak bizonyulnak a különböző "békés eszközök" a kiberviták rendezésében, annál inkább fognak az államok ezekre támaszkodni.

M. *A beavatkozás tilalma*

A kézikönyvben a beavatkozás szokásjogi tilalma két szabályra oszlik, az első az államokra, a második pedig az Egyesült Nemzetek Szervezetére vonatkozik.

A 66. szabály a jól ismert nemzetközi jogi elvet mondja ki:[273] "Egy állam nem avatkozhat be - beleértve a kibernetikai eszközöket is - egy másik állam bel- vagy külügyeibe".[274] A szabály csak a kapcsolatokra vonatkozik

---

world/asia/xi-jinping-of-china-to-address-wary-us-business-leaders.html?_r=0 (a Kína és az Egyesült Államok közötti megállapodásról, amely szerint együtt fognak dolgozni a Kína által az Egyesült Államokban elkövetett kiberbűnözés megállítása érdekében); David Lee, *Russia and Ukraine in cyber 'stand-off'*, BBC (2014. március 5.), http://www. bbc.com/news/technology-26447200 (az Ukrajna és az állítólagos orosz állami kibererők közötti közelmúltbeli kiberhack-cseréről).

268. *Lásd* Alastair Stevenson, *It Looks Like the US Government Just Got Hacked Again - And This Time Anonymous is Claiming Responsibility*, BUS. INSIDER (2015. július 24., 7:45) http://www. businessinsider.com/anonymous-hackers-leak-4200-us-government-workers-alleged-details-to protest-ttip-and-tpp-2015-7 (az Anonymous által az Egyesült Államok Népszámlálási Hivatalának hackeléséről); Andrea Peterson, *The Sony Pictures Hack, Explained*, WASH. POST (2014. dec. 18.), https://www. washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/?utm_ term=.adaf6a618dbe; *Anonymous 'Hacks' North Korea Social Media Accounts*, BBC (2013. ápr. 4.), http://www.bbc.com/news/technology-22025724 (az Anonymous észak-koreai social me dia fiókok feltöréséről).

269. Ian Phillips & Vladimir Isachenkov, Putyin: U.S. News & World Rep. (2017. június 1.), https://www.usnews.com/news/world/articles/ 2017-06-01/putin-russian-state-has-never-been-involved-in-hacking (Putyin elnök állításait tárgyalva, miszerint Oroszország nem állami feladatként hackel, de a hazafias oroszok saját elhatározásukból dönthetnek így).

270. *Lásd fentebb a* IIIA. részt.

271. *Lásd fentebb a* IIIB. részt.

272. *Lásd fentebb a* IIID. részt.
273. *Lásd* TALLINN MANUAL 2.0, 14. lábjegyzet, 312, 314, 1. és 5. pont.
274. *Id.* 312.

államok között,[275] és csak a kényszerítő beavatkozást tiltja.[276] Bár a szakértők úgy vélték, hogy "a beavatkozás tilalmának pontos körvonalai és alkalmazása nem világosak a folyamatosan fejlődő és egyre inkább összefonódó nemzetközi kapcsolatok fényében",[277] egyetértettek a Nemzetközi Bíróság által adott definícióval, miszerint a tiltott beavatkozásnak ki kell terjednie egy állam *domaine re´serve´jére*, vagyis olyan kérdésekre, mint "a politikai, gazdasági, társadalmi és kulturális rendszer kiválasztása és a külpolitika kialakítása".[278]

A szakértők abban is egyetértettek, hogy "a *domaine re´serve´* hatálya szűkülhet, ahogy az államok a kibertérrel kapcsolatos kérdéseket a nemzetközi jog szabályozása alá vonják",[279] de arra a következtetésre jutottak, hogy "az állam *domaine re´serve´jén* belül a legegyértelműbben a politikai rendszer és a szervezet megválasztása tűnik a kérdésnek".[280] A kényszerítéssel kapcsolatban a szakértők megosztottak abban a kérdésben, hogy a kényszerítésnek "a célállam számára fenntartott kérdésben az eredmények befolyásolására vagy az azzal kapcsolatos magatartás befolyásolására kell-e irányulnia", a többség egyetértett azzal, hogy igen.[281] Abban is megosztottak, hogy a kényszerítő aktusnak közvetlenül kell-e okoznia a hatást, a többség szerint nem, "amennyiben van ok-okozati összefüggés".[282]

Hasonlóképpen, a szakértők nem értettek egyet abban, hogy az államnak ténylegesen tudnia kell-e, hogy kényszerítik, hogy a beavatkozó állam megszegje a nemzetközi jogot. A többség úgy döntött, hogy ez a tudás nem szükséges előfeltétel.[283] Másrészt a szakértők egyetértettek abban, hogy a jogsértéshez nem szükséges annak ismerete, hogy a kiberkényszer egy állam (vagy egy államnak tulajdonítható szervezet) részéről érkezik,[284] bár a kényszerítésre irányuló szándék szükséges.[285] Továbbá, a kényszerítés hatékonysága nem volt lényeges a beavatkozás fennállása szempontjából.[286] A szakértők megosztottak abban a kérdésben, hogy a célállamban tartózkodó állampolgárainak védelmét célzó kiberműveletek beavatkozásnak minősülnek-e,

275. *Id.* 313., 4. pont.
276. *Id.* 313., 3. pont.
277. *Id.* 314., 6. pont.
278. *Id.* 315., 8. pont (idézi a Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, 205 (június 27.).
279. *Id.* 316, 13. pont.
280. *Id.* 315, 10. pont.
281. *Id.* 318, 19. pont.
282. *Id.* 320, 24. pont.
283. *Id.* 320, 25. pont.
284. *Id.* 321, 26. pont.
285. *Id.* 321, 27. pont.
286. *Id.* 322., 29. pont.

a többség úgy döntött, hogy általában nem.[287] Bár a szakértők egyetértettek abban, hogy a gazdasági intézkedések, például az egyoldalú gazdasági szankciók nem minősülnének beavatkozásnak,[288] a humanitárius beavatkozást támogató kiberműveletekkel kapcsolatban megosztottak az ENSZ Biztonsági Tanácsának felhatalmazása hiányában, és a szakértők véleménye megoszlott a tekintetben, hogy szerintük maga a humanitárius beavatkozás jogszerű-e. A szakértői vélemények szerint a humanitárius beavatkozás jogszerű.[289]

A 67. cikk folytatja a beavatkozásról szóló vitát, de az ENSZ intézkedéseire összpontosít. A szabály kimondja, hogy "Az Egyesült Nemzetek nem avatkozhat be, beleértve a kibernetikai eszközöket is, olyan ügyekbe, amelyek alapvetően egy állam belső joghatósága alá tartoznak. Ez az alapelv nem érinti az ENSZ Biztonsági Tanácsa által az ENSZ Char ter VII. fejezete alapján hozott végrehajtási intézkedések meghozatalát."[290] Néhány szakértő úgy vélte, hogy ezt a szabályt általában a nemzetközi szervezetekre kellene alkalmazni, de konszenzus csak az Egyesült Nemzetek Szervezetére való alkalmazásáról sikerült konszenzust elérni.[291]

E szabály alapja az Egyesült Nemzetek Alapokmányának 2. cikkének (7) bekezdése, amely megtiltja, hogy az ENSZ beavatkozzon "olyan ügyekbe, amelyek alapvetően bármely állam belső joghatósága alá tartoznak".[292] Ennek eredményeként a szakértők egyetértettek abban, hogy ez a szabály nem korlátozza a nemzetközi békét és biztonságot érintő intézkedéseket.[293] Bár a szakértők egyetértettek abban, hogy a 2. cikk (7) bekezdésének hatálya alá tartozó ügyek köre szűkült,[294] egyetértettek abban, hogy a szabály beavatkozásra vonatkozó megfogalmazása ellenére a valóban bármely állam belső joghatósága alá tartozó ügyek esetében még az ENSZ nem kényszerítő jellegű beavatkozása is sérti ezt a szabályt.[295]

A kibernetikai beavatkozás tilalma nagyon fontossá vált a választásokba való orosz kibernetikai beavatkozással kapcsolatos közelmúltbeli állítások fényében.

287. *Id.* 323, 34. pont.
288. *Id.* 324, 35. pont.
289. *Id.* 324, 36. pont.
290. *Id.* 325.
291. *Id.* at 325, ¶ 1.

292. ENSZ Alapokmány, cikk. 2, ¶ 7.
293. *Lásd* TALLINN MANUAL 2.0, 14. lábjegyzet, 325. pont, 2. bekezdés.
294. *Id.* 326, 4. pont.
295. *Id.* 326, 5. pont.

mind az Egyesült Államokban[296] , mind Európában.[297] Bár az orosz hackertámadások egyik célpontja sem nyilvánította még az ilyen tevékenységeket a nemzetközi jog megsértésének, Obama elnök 2016 októberében a híres "vörös telefonon" keresztül némileg burkoltan megfenyegette Putyin elnököt, amikor azt mondta Putyin elnöknek, hogy "[a] nemzetközi jog, beleértve a fegyveres összeütközés jogát is, vonatkozik a kibertérben végrehajtott cselekményekre".[298]

A régóta a tiltott beavatkozás sztereotípiájaként értelmezett eseményre adott langyos nemzetközi reakció a korábban elismert normák határait feszegetheti. A Kézikönyv határozott kijelentése remélhetőleg a kibertevékenységekre alkalmazott tilalom egyik világos megfogalmazása lesz, amelyet az államok elkezdhetnek felhasználni az orosz kiberműveletek visszaszorítására.

Természetesen, amíg Putyin elnök egyszerűen "hazafias hackereknek" tulajdoníthatja a kiberbeavatkozást, majd nem vállal felelősséget azért, hogy ellenőrizze őket vagy korlátozza tevékenységüket, addig a[299] nemzetközi jognak nem sok hatása lesz a kiberbeavatkozásra. Ez ismét rávilágít a kellő gondosság elvének jövőbeli fejlődésének fontosságára, és arra a lehetőségre, hogy az államokra szigorúbb felelősséget rójon a határaikon belül vagy az ellenőrzésük alatt álló személyek kibertevékenységeiért.

A Kézikönyv további része a *jus ad bellum* és a *jus in bello* szabályait tartalmazza, és csak kismértékben módosul a Tallinni Kézikönyv 1.0-ban közzétett szabályokhoz képest.[300] Ezért itt nem kerül sor kiemelésekre.

IV. KÖVETKEZTETÉS

Fontos megjegyezni, hogy a tallinni kézikönyvekben részt vevő szakértők elkötelezettek voltak amellett, hogy a jogot úgy fogalmazzák meg, ahogyan az van, és hogy olyan kézikönyveket készítsenek, amelyek saját véleményüknek tekinthetők.

---

296. David E. Sanger & Scott Shane, *Russian Hackers Acted to Aid Trump in Election, U.S. Says*, N.Y. TIMES (2016. dec. 9.), https://www.nytimes.com/2016/12/09/us/obama-russia-election-hack. html?rref=collection%2Fnewseventcollection%2Frussian-election-hacking&action=click&content Collection=politics&region=rank&module=package&version=highlights&contentPlacement=4&pgtype=collection.

297. Oren Dorell, *Russia Engineered Election Hacks and Meddling in Europe*, USA TODAY (2017. január 9. 7:03), https://www.usatoday.com/story/news/world/2017/01/09/russia-engineered election-hacks-europe/96216556/.

298. William M. Arkin, Ken Dilanian & Cynthia McFadden, *What Obama Said to Putin on the*

Red Phone About the Election Hack, NBC NEWS (2016. december 19., 18:30), http://www.nbcnews.com/ news/us-news/what-obama-said-putin-red-phone-about-election-hack-n697116.

299. *Lásd* Phillips és Isachenkov, 270. lábjegyzet.

300. *Lásd* TALLINN MANUAL 2.0, 14. lábjegyzet, 328 -562. o.; *lásd még* TALLINN MANUAL 1.0, 14. *lábjegyzet*.

13. megjegyzés, 42-256.

és nem az államoké. A szakértők szerényebb szándékkal álltak a projekthez, mint néhányan mások, akik hozzászóltak a projekthez. Valójában, amint azt Rutger van Marrising úr, az Alföldi Királyság Külügyminisztériumának munkatársa a kézikönyv amerikai bemutatóján megjegyezte, a Tallinn 2.0-t valójában egy hosszabb és jelentősebb vita kezdetének szánták.[301]

Mindazonáltal a Tallinn 2.0 lesz a kiindulópontja a következő néhány év, de talán még hosszabb időre szóló vitáknak. Átfogó jellege, megalapozott elemzése és következtetései, valamint az állami és szakértői észrevételek beépítése mind-mind a legértékesebb hivatkozási és kiindulópontjává teszik a kiberműveletekre alkalmazandó nemzetközi jogról szóló vitáknak.

Amint azt ez a cikk megállapítja, még mindig sok területen vannak nézeteltérések és tisztázatlanságok, még a tallinni kézikönyveket író szakértők között is. Számos olyan helyzet is van, amikor az államok nem beszéltek vagy nem cselekedtek nyilvánosan a kiberműveletekkel kapcsolatban. Ez még mindig a jog növekvő területe, ahol nagy szükség van a rálátásra és a megértésre, hogy a meglévő problémákra új megközelítéseket lehessen kialakítani. Amíg azonban az államok nem tisztázzák, hogy pontosan merre tart a jog, addig a Tallinn 2.0 kiindulópontként szolgál a kiberműveletekre vonatkozó joggal kapcsolatos előrelépéshez.

301. *Lásd* Corn, 28. lábjegyzet.