

Csillik Kristóf–Hordós Alex

Zárva tartani Pandora szelencéjét: az erőszakos kiberműveletek betudásának kérdései

1. Bevezetés

Az államok, illetve a nem állami szereplők által végrehajtott kiberműveletek jelentőségét napjainkban már evidenciaként kezelhetjük. A nemzetközi kiberhadviselés első igazi „áldozata” Észtország volt 2007-ben, amikor feltehetőleg orosz érdekekből érte az ország informatikai rendszereit támadás, de például a Stuxnet vírusként elhíresült, Irán nukleáris programja ellen intézett 2010-es támadás, a WannaCry zsarolóvírus, amely a Sony ellen végrehajtott kiberkémkedés volt, vagy a NotPetya névre hallgató, Ukrajnát célzó rosszindulatú művelet¹ is mutatja a terület dinamikusan fejlődő és egyúttal egyre veszélyesebbé váló mivoltát. Nem nehéz azonosítani ezen támadó jellegű kiberműveletek vonzerejét azok elkövetői számára. Alacsony kockázat és költségek mellett lehet kiterjedt, adott esetben egész intézményrendszereket megbénító, komoly anyagi vagy akár konkrét kinetikus kárt, adott esetben pedig emberi egészséget sértő cselekményeket végrehajtani.

Erre tekintettel kiemelten fontos, hogy a nemzetközi jog hatékonyan reagáljon az új eszközök által megjelenő kihívásokra, melynek természetesen részét képezi az elkövetők azonosítása és felelősségre vonása. Mindazonáltal a kibertér nyújtotta anonimitás, a betudás technikai aspektusának ismert nehézségei és a konvencionális nemzetközi jog betudási mércéinek szigorú mivolta rend-

¹ Kiss M.: A kiberműveletek és a jus ad bellum kapcsolata, *Közjogi Szemle*, 2022/3. 100.

kívül módon megnehezíti, hogy a támadó jellegű kiberműveletek elkövetőinek cselekményeit nagy bizonyossággal betudhassuk egy államnak, és így a megfelelő jogkövetkezményeket levonhassuk.

Jelen tanulmányban a szakirodalomban és az állami gyakorlatban egyaránt megjelenő „vonakodik vagy képtelen” (*unwilling or unable*) doktrínát javasoljuk a kibertérben való betudás *lex specialis* szabályának, mely álláspontunk szerint megfelelő egyensúlyt teremt a területi állam és a célállam felelőssége között, illetve lehetőséget a megtámadott állam számára az adekvát válaszlépések megtételére.

A tanulmány hat szerkezeti egységből épül fel. A bevezetést (1. fejezet) követően a 2. fejezetben röviden vázoljuk a kibertérre vonatkozó nemzetközi jogi szabályokat, és megállapítjuk, hogy irányadó *lex specialis* hiányában a nemzetközi jog konvencionális szabályai irányadóak a kiberműveletek jogszerűségének megítélése során. Jelen tanulmányban kibertámadás alatt az Alapokmány 2. cikk (4) bekezdésébe ütköző magatartásokat értjük, ezért ismertetjük a – kibertérre is alkalmazandó – *jus contra bellum*² rezsím alapvető kereteit. A 3. fejezetben definiáljuk a „kibertámadás” fogalmát, elhatároljuk azt a kiberkémkedés és a kiberbűnözéstől és tisztázzuk, hogy csak az erőszaktilalomba ütköző magatartást tekintjük kibertámadásnak. A 4. fejezetben ismertetjük a nemzetközi jog konvencionális betudáskonceptióit és rávilágítunk arra, hogy a kibertámadások sajátosságai miatt teszük rendkívül nehézé ezen betudáskonceptiók eredményes alkalmazását. Az 5. fejezetben ismertetjük a vonakodik vagy képtelen doktrínát, és kifejtjük, miért tekintjük

² Jelen tanulmány szinonimaként értelmezi a nemzetközi jog erőszakalkalmazási rezsímjét leíró *jus ad bellum* és *jus contra bellum* fogalmakat; természetesen nem megfeledkezve arról, hogy ez a distinkció az 1945-től „hatályos” átfogó és általános erőszaktilalom térnyerése óta értelmezhető a maga teljességében. Ld. O. CORTEN: *The Law Against War: The Prohibition on the Use of Force in Contemporary International Law*, London, Hart Publishing, 2010. 2.

legitim lex specialis betudhatósági mércének a kibertérben végrehajtott cselekmények tekintetében, és hogy a – némileg hasonló – „*due diligence*” mérce miért nem elégséges a kiberműveletek betudási nehézségeinek áthidalására. Végül a VI. fejezet összefoglalja a tanulmány legfontosabb megállapításait.

2. A kiberműveletekre alkalmazandó nemzetközi jogi keretrendszer vázlata

2.1. A kiberműveletek és a nemzetközi jog viszonya

A kiberműveletek relatíve új mivolta, és az azokat lehetővé tevő infrastruktúra gyorsan változó jellege alapvető kérdéseket vet fel a nemzetközi jog kibertérre és kiberműveletekre való alkalmazhatóságával kapcsolatban. Álláspontunk szerint bármely további vizsgálódást megelőzően a kibertér és a nemzetközi jog viszonyára vonatkozó két kérdés megválaszolása szükséges: (1) *Alkalmazandó-e a nemzetközi jog a kibertérben*, valamint (2) *amennyiben igen, úgy vonatkozik-e sajátos szabályozási rezsim a kibertér használatára és a kiberműveletekre, vagy a nemzetközi jog konvencionális keretrendszere az irányadó?* E fenti két kérdésre adandó válasz értelemszerűen alapjaiban fogja meghatározni, hogy milyen jogi kontextusban értelmezendők a jelen kutatás tárgyát képező betudhatósági szabályok.

2.1.1. Alkalmazható-e a nemzetközi jog a kibertérben?

Az állami gyakorlatot tükröző UN Group of Governmental Experts jelentései,³ a G7 államok által közzétett ún. „Luccai

³ *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*,

Nyilatkozat”,⁴ a kiberműveletekre vonatkozó nemzetközi joganyag alkalmazhatósága tekintetében mérvadó alaplumnak tekintett Tallini Kézikönyv,⁵ illetve a másodlagos szakirodalom⁶ egyaránt azon az állásponton van, hogy a kibertér *egyelőre* nem képez olyan sajátos területet, amelyre vonatkozóan bármely okból ne volna alkalmazható a nemzetközi jog általános kerete. Hasonló következtetés vezethető le a Nemzetközi Bíróság (*International Court of Justice*, ICJ) Nukleáris fegyverek tanácsadó véleményéből: a testület deklarálta, hogy önmagában a fegyvernemek új és változó mivolta nem jelenti azt, hogy a nemzetközi jog korábban kikristályosodott elvei és szabályai ne volnának alkalmazhatók ezen új fegyvertípusok alkalmazásnak vonatkozásában.⁷ Ez tehát azt jelenti, hogy az Egyesült Nemzetek Alapokmányában (a továbbiakban: Alapokmány) megfogalmazott átfogó erőszaktilalom⁸ a fegyver jellegétől és újdonságától függetlenül, mintegy rugalmasan tiltja az erőszakot és az erőszakkal való fenyegetést.⁹

UNGA, Note by the Secretary-General, A/68/98, 2013. 19. bek.; *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UNGA, Note by the Secretary-General, A/70/174, 2015. 24–26. bek.

⁴ *G7 Declaration on Responsible States Behavior in Cyberspace*. 2017. (elérhető: <https://ccdcoc.org/uploads/2018/11/G7-170411-LuccaDeclaration-1.pdf>)

⁵ M. N. SCHMITT – L. VIHUL (Eds.): *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge, CUP, 2017. (a továbbiakban: Tallinn Manual 2.0)

⁶ Összegző jelleggel ld. F. DELERUE: *Cyber Operations and International Law*. Cambridge, CUP, 2020. 4–28.

⁷ *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, I.C.J. Reports 1996, p. 226. (a továbbiakban: Nukleáris fegyverek tanácsadó vélemény) 39. bek.

⁸ *Charter of the United Nations*, 26/06/1945, UNTS, Vol. 1, p. XVI. (a továbbiakban: Alapokmány) 2. cikk (4) bekezdés.

⁹ Kiss: i. m. 102.

Az első kérdésre tehát azt a(z egyébként evidensnek tetsző) választ kell adnunk, hogy *a nemzetközi jog szabályai a kibertérben is érvényesülnek.*

2.1.2. Létezik-e a kibertérre és a kiberműveletekre irányadó *lex specialis*?

Önmagában az a körülmény, hogy a nemzetközi jog normái alkalmazandóak a kibertérben még nem ad választ arra a kérdésre, hogy *mely nemzetközi jogi szabályok* jelölik ki a kibertér használatának kereteit. Másképpen fogalmazva: létezik-e olyan speciális normatömeg, amely a kibertér vonatkozásában tartalmaz sajátos előírásokat, hasonlóan a tengerek vagy a világűr jogához? E körben szintén irányadó megállapításokat tett az ICJ Nukleáris fegyverek tanácsadó véleménye, amikor elvi élel rögzítette, miszerint az adott technológia újszerűsége önmagában még nem vezet az általános szabályok félretételéhez.¹⁰ A specifikus szabályok explicit hiánya ugyanis nem jelent(het)i azt, hogy az államok az újonnan kialakult technológiák révén megkerülhetnék a nemzetközi jog generálisan alkalmazandó szabályait, amelyek így kétségtelenül alkalmazandóak a kibertérre is.¹¹

Ez természetesen nem jelenti azt, hogy a jövőben akár egyezményi, akár szokásjogi úton ne alakulhatna ki olyan *lex specialis*, amely az általánostól eltérő normákat állapít meg a kiberműveletek nemzetközi jogi viszonyrendszerében. Jelenleg viszont az egyetlen, dedikáltan a kibertérre összpontosító nemzetközi

¹⁰ Nukleáris fegyverek tanácsadó vélemény, i. m. 86. bek.

¹¹ Ez erősíti meg az állami gyakorlat, valamint a szakirodalom is. Vö. *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, UNGA, Note by the Secretary-General, A/76/135, 2021. 69–71. bek.; M. ROSCINI: *Cyber Operations and the Use of Force in International Law*, Oxford, OUP, 2014. 19.

egyezmény a kiberbűnözésről szóló budapesti egyezmény (*Convention on Cybercrime*),¹² amely valójában „csak” annyira kötelezi a szerződő feleket, hogy egyes kiberbűncselekményeket nemzeti büntetőjogukban kriminalizáljanak.

2.2. A kiberműveletek betudhatósága szempontjából legrelevánsabb nemzetközi jogi jogintézmények ismertetése

Figyelemmel arra, hogy a kibertérben nem érvényesül olyan *lex specialis*, amely az államokat terhelő nemzetközi jogból fakadó kötelezettségek tekintetében különbséget jelentene az offline térben alkalmazandó szabályokhoz képest, ezért a nemzetközi jog hagyományos normái a kibertérben is irányadóak.

A kiberműveletek betudhatósága – többek között – az államfelelősség, a *jus contra bellum*, a *jus in bello* és a nemzetközi emberi jogok körében bír kiemelt jelentőséggel.¹³ Jelen tanulmányban a kibertámadásokat az általános erőszaktilalomba ütköző kiberműveletekkel azonosítjuk, ezért csak a *jus contra bellum* körében foglalkozunk a betudhatóság kérdéskörével.

Kétségtelen, hogy amíg nem alakul ki a „kiberjogi *leges speciales*”, addig a hatályos *jus contra bellum*-normák tükrében lehet értelmezni az erőszakos kiberműveleteket is.¹⁴ Az alábbiakban

¹² *Convention on Cybercrime*, 23/11/2011, CETS, No. 185.

¹³ KAJTÁR G.: *Betudás a nemzetközi jogban. A másodlagos normák szerepe a beruházásvédelemtől a humanitárius jogig*. Budapest, ORAC, 2022. 27–29.; L. CONDORELLI – C. KRESS: *The Rules of Attribution: General Considerations*. In: James CRAWFORD – Alain PELLET – Simon OLLESON – Kate PARLETT (Eds.): *The Law of International Responsibility*. Oxford, OUP, 2010. 222.

¹⁴ G. NOLTE – A. RANDELZHOFFER: *Article 51*. In: Bruno SIMMA – Daniel-Erasmus KHAN – Georg NOLTE – Andreas PAULUS – Nikolai WESSENDORF (Eds.): *The Charter of the United Nations: A Commentary, Volume II*. Oxford, OUP, 2012. 1419, 43. bek.

röviden áttekintjük a *jus contra bellum* alapvető keretrendszerét, annak érdekében, hogy a tanulmány fogalmi hálója és jogi kontextusa tisztázott legyen.

Az Egyesült Nemzetek Szervezetének életre hívásával új időszámítás kezdődött az államközi erőszakalkalmazás történetében, köszönhetően az Alapokmány 2. cikk (4) bekezdésének, amely szerint „[a] Szervezet összes tagjainak nemzetközi kapcsolataikban más Állam területi épsége, vagy politikai függetlensége ellen irányuló vagy az Egyesült Nemzetek céljaival össze nem férő bármely más módon nyilvánuló erőszakkal való fenyegetéstől vagy erőszak alkalmazásától tartózkodniuk kell.”¹⁵ Ezzel az egy rendelkezéssel összefüggésben napjainkra az alábbi axiomatikus téziseket tekinthetjük a nemzetközi jog *de lege lata*-állapotának:

- Az erőszakkal való fenyegetés és az erőszak alkalmazásnak tilalma fundamentális jelentőségű elsődleges norma, amelyet több ízben neveztek az Alapokmány és a nemzetközi jog sarokkövének.¹⁶ Vitán felül áll továbbá, hogy az erőszakalkalmazás tilalma feltétlen alkalmazást igénylő, *jus cogens* norma is egyben.¹⁷

¹⁵ A hivatalos magyar fordításhoz képest a „tartózkodniok” kifejezést a modernebb „tartózkodniuk”-ra cseréltük, a „nemzetközi érintkezéseik során” helyett pedig a „nemzetközi kapcsolataikban” fordulatot alkalmaztuk, mivel meglátásunk szerint ez jobban visszaadja az Alapokmány hiteles nyelvein írt szöveg lényegét (így pl. „*in their international relations*”, „*dans leurs relations internationales*” stb.).

¹⁶ *Armed Activities on the Territory of the Congo* (Democratic Republic of the Congo v. Uganda), Merits, Judgment, I.C.J. Reports 2005. p. 168. (a továbbiakban: Fegyveres tevékenységek-ügy) 148. bek.; O. DÖRR – A. RANDELZHOFFER: Article 2(4). In: Bruno SIMMA – Daniel-Erasmus KHAN – Georg NOLTE – Andreas PAULUS – Nikolai WESSENDORF (Eds.): *The Charter of the United Nations: A Commentary, Volume I*. Oxford, OUP, 2012. 203. 1. bek.

¹⁷ *Military and Paramilitary Activities in and against Nicaragua* (Nicaragua v. United States of America), Merits, Judgment, I.C.J. Reports 1986. p. 14.

- Az előző pontban meghatározott tilalom alól mindössze két kivételt ismer a rendszer: az ENSZ Biztonsági Tanácsa (BT) által, az Alapokmány VII. fejezete szerint végrehajtott, erőszakkal járó kényszerintézkedések,¹⁸ valamint az önvédelmi jogban megnyilvánuló egyoldalú (és emiatt szűken értelmezendő) erőszakalkalmazás.¹⁹
- Az Alapokmány fogalmi rendszere három, fokozatosan súlyosodó cselekménnyel²⁰ írja le a tilalom egyes lehetséges magatartásait: a legáltalánosabb és legátfogóbb az erőszak alkalmazása (*use of force*), valamint az ezzel való fenyegetés (*threat of force*). Ennél súlyosabb az agresszió²¹ (*aggression*); ez az Alapokmány rendszerében inkább politikai, mintsem jogi jellegű fogalom, amely elsődlegesen annak köszönhető, hogy maga az agresszió a 39. cikkben jelenik meg úgy, mint egy, a BT általi olyan helyzetminősítés, amely a nemzetközi békét és biztonságot veszélyezteti. Végül az önvédelem „természetes” jogát elismerő 51. cikk rendelkezik a fegyveres támadásról (*armed attack*). A fegyveres támadás az erőszakalkalmazás kvalifikált, legsúlyosabb formája; ezt

(a továbbiakban: Nicaragua-ügy) 190. bek.; *Commentary to the Articles on the Responsibility of States for Internationally Wrongful Acts*, Yearbook of the ILC 2001. Vol. II., Pt. Two, 2007. p. 31. (a továbbiakban: ARSIWA Kommentár) 112, 4. bek.; DÖRR – RANDELZHOFFER: i. m. 203. 1. bek.

¹⁸ Alapokmány, i. m. 42. cikk.

¹⁹ Alapokmány, i. m. 51. cikk.

²⁰ A fogalmak egymáshoz való viszonyáról ld. KAJTÁR G.: Erőszak, agresszió, fegyveres támadás – *A ius contra bellum* klasszikus normáinak kialakulása, tartalma és egymáshoz való viszonya, *Acta Facultatis Politico-iuridicae Universitatis Scientiarum Budapestinensis de Rolando Eötvös nominatae*, 2015. 105–143.

²¹ A hivatalos magyar fordításban megtalálható „támadó cselekményt” annak anakronisztikus, a szakirodalom által sem használt jellegére tekintettel elvetettük.

a mennyiségi jellemzőt a támadás mértéke és hatása alapján lehet megítélni.²²

- Összhangban az Alapokmány 51. cikkével, az önvédelem jogának gyakorlása megkövetel egy mennyiségi és egy minőségi feltételt: a mennyiségi feltétel az előző pontban említett, már bekövetkezett²³ fegyveres támadás, a minőségi feltétel pedig azt követeli meg, hogy a fegyveres támadást egy állam kövesse el vagy az egy államnak betudható legyen.²⁴ Ennek az államközi „kizárólagosságnak” a következménye az is, hogy fegyveres támadás csak állam ellen követhető el.²⁵ Az önvédelmi jog gyakorlását tovább korlátozza a szükségesség és az arányosság szokásjogi követelménye.²⁶

²² Nicaragua-ügy, i. m. 191. bek., 195. bek.; T. RUYS: *'Armed Attack' and Article 51 of the UN Charter: Evolutions in Customary Law and Practice*. Cambridge, CUP, 2010. 138.; NOLTE – RANDELZHOFFER: i. m. 1401. 6. bek.

²³ Elismerjük annak az akadémiai vitának a jelentőségét, amely szerint akár az 51. cikk alapján, akár szokásjogra alapítva lehetősége lenne az államoknak megelőző önvédelmet gyakorolniuk; ezt azonban jelen keretek között nem kívánjuk vizsgálni, így pedig az Alapokmány szövegét tekintjük kiindulópontnak.

²⁴ J. KAMMERHOFER: The Resilience of the Restrictive Rules on Self-Defence. In: Marc WELLER (Ed.): *The Oxford Handbook of the Use of Force in International Law*. Oxford, OUP, 2015. 629.

²⁵ *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, Advisory Opinion, I.C.J. Reports 2004. p. 136, 139. bek.; Fegyveres tevékenységek-ügy, i. m. 146–147. bek.; J. L. KUNZ: Individual and Collective Self-Defense in Article 51 of the Charter of the United Nations. *AJIL*, 1947/4. 878.

²⁶ Nicaragua-ügy, i. m. 176. bek.; Nukleáris fegyverek tanácsadó vélemény, i. m. 41. bek.; Fegyveres tevékenységek-ügy, i. m. 147. bek.

3. A kibertámadás definíciója

A kibertámadások állami betudhatóságának érdemi vizsgálatához elengedhetetlen a „kibertámadás” fogalmának definiálása. A nemzetközi jogi relevanciával bíró kiberműveletek típusainak megkülönböztetése érdekében röviden ismertetjük a szakirodalom által elismert művelettípusokat, majd elhatároljuk egymástól a „kibertámadás”, a „kiberkémkedés” és a „kiberbűnözés” kategóriáit.

A kiberműveletek a kibertérben végzett elektronikus adatkezelés és az adatkezelő képességek működésével kapcsolatos tevékenységek, illetve tágra értelmezve az ezek védelmére és befolyásolására vagy támadására irányuló tevékenységek, folyamatok.²⁷ Ehhez képest szűkebb kategóriát jelentenek az ún. onerózus kiberműveletek, melyek a célpont számára hátrányos eredmény bekövetkezése érdekében végrehajtott kiberműveletek.

Az onerózus kiberművelet gyűjtőfogalma alá tartozó, fenti művelettípusok (kibertámadás, kiberkémkedés, kiberbűnözés) között (1) célpontjuk, (2) eszközeik, (3) motivációjuk, illetve (4) betudhatóságuk szerint tehetünk különbséget,²⁸ mely elhatárolás nem pusztán dogmatikai tisztaságot teremt, hanem a magatartás jogkövetkezményeinek meghatározása során is alapvető jelentőségű.

A kiberkémkedés az államnak betudható, alapvetően információszerzési célú onerózus kiberművelet.²⁹ A kémkedést

²⁷ 60/2013. (IX. 30.) HM utasítás a Magyar Honvédség Kibervédelmi Szakmai Koncepciójának kiadásáról (a továbbiakban: HM utasítás), 1. melléklet, 2. pont, 6. alpont.

²⁸ Az elhatárolás szempontjainak részletes elemzéséhez ld.: K. KRASZEWSKI: Classification of Cyber Operations under International Law. *Finnish Yearbook of International Law*, 2015. 145–170.

²⁹ Uo. 145.

a nemzetközi jog kategorikusan nem tiltja,³⁰ mely szabály a *lex specialis* hiányára tekintettel a kibertérben is érvényesül.³¹ A kiberbűnözés az államnak nem betudható, hátrányos eredményű kiberművelet,³² melyet az államok nemzeti büntetőjoga büntetni rendelheti, de a területi állam felelősségét nem váltja ki.³³

A kibertámadás fogalmát eltérően közelíti meg a szakirodalom,³⁴ valamint az egyes katonai doktrínák, így pl. az amerikai hadsereg,³⁵ vagy a magyar Honvédség³⁶ dokumentumai. Kon-szenzusos nemzetközi jogi „kibertámadás” fogalom mindazonáltal még nem jött létre. Mindezekre tekintettel – jelen tanulmány keretei között – a „kibertámadás” alatt olyan kiberműveletet értünk, amely az Alapokmány 2. cikk (4) bekezdésében kodifikált erőszaktilalomba ütközik. Ennek következtében nem értjük bele tehát azon onerózus kiberműveleteket, amelyek sérthetik ugyan a célállam szuverenitását, vagy amelyek a beavatkozás tilalmába ütköznek, azonban nem minősülnek erőszakalkalmazásnak.

³⁰ Uo. 165.

³¹ Uo.; Tallinn Manual 2.0, i. m. 168–169.

³² KRASZEWSKI: i. m. 168.

³³ Uo. 170.

³⁴ A kérdésről alkotott vitához lásd pl. M. N. SCHMITT: ‘Attack’ as a Term of Art in International Law: The Cyber Operations Context, In: Christian CZOSSECK – Rain OTTIS – Katharina ZIOLKOWSKI (Eds.): *4th International Conference on Cyber Conflict. Proceedings 2012*. Tallinn: NATO CCD COE, 2012. 283–293.; K. ZIOLKOWSKI: *Ius ad bellum* in Cyberspace – Some Thoughts on the “Schmitt-Criteria” for Use of Force, In: Christian CZOSSECK – Rain OTTIS – Katharina ZIOLKOWSKI (Eds.): *4th International Conference on Cyber Conflict. Proceedings 2012*. Tallinn: NATO CCD COE, 2012. 295–309.

³⁵ J. E. CARTWRIGHT: *Memorandum for Chiefs of the Military Services, Commanders of the Combatant Commands, Directors of the Joint Staff Directories on Joint Terminology for Cyberspace Operations*. Department of Defense, 2011. (elérhető: <https://info.publicintelligence.net/DoD-JointCyberTerms.pdf>)

³⁶ HM utasítás, i. m. 1, melléklet, 2. pont, 7. pont.

Annak kapcsán, hogy mikor minősül erőszakalkalmazásnak egy kibertámadás, sem vonatkozó bírói gyakorlat, sem egyéb kötelező nemzetközi jogi jogforrás nem áll rendelkezésre, mindazonáltal a szakirodalom és a különböző *soft law* dokumentumokban konszenzus mutatkozik abban,³⁷ hogy egy kibertámadás akkor ütközik az erőszakalkalmazás tilalmába, ha annak hatását tekintve alkalmas volna az erőszaktilalom megsértésére. Ennek megfelelően csak a kinetikus támadásokkal összevethető kárt, sérülést, pusztítást okozó kiberműveletet tekintjük kibertámadásnak, nem megelégedve arról, hogy – a 2. cikk (4) bekezdés céljának megfelelően – az erőszak átfogó és teljes tilalmára tekintettel ez a „mennyei küszöb” meglehetősen alacsony.³⁸

4. Betudási kérdések a nemzetközi jogban

Ebben a fejezetben elsőként elhatároljuk egymástól az elsődleges nemzetközi jogi normákat annak érdekében, hogy a betudás dogmatikai szerepét tisztázzuk, felvázoljuk a betudás és a kibertámadások kapcsolatának alapvető kérdéseit, bemutatjuk a *jus contra bellum* rezsimben *de lege lata* alkalmazható betudási teszteket, végül rávilágítunk arra, hogy azok álláspontunk szerint miért alkalmatlanok a kibertámadások gyors és hatékony betudására.

4.1. Az elsődleges és másodlagos normák elhatárolásának relevanciája

A nemzetközi jogilag releváns cselekmények betudhatóságának vizsgálatához elengedhetetlen a nemzetközi jog szabályainak

³⁷ Tallinn Manual 2.0, i. m. 330–336.

³⁸ Részletesen ld. T. Ruys: The Meaning of “Force” and the Boundaries of the Jus Ad Bellum: Are “Minimal” Uses of Force Excluded from UN Charter Article 2(4)?, *AJIL*, 2014/2. 159–210.

elsődleges és másodlagos normákra való felosztása. A különbégtételt jellemzően Herbert L. A. Hart angol jogfilozófus *A jog fogalma* c. művéből vezetik le, ugyanakkor az elméleti elgondolás az államfelelősségi szabályok kodifikációjának a kezdeteitől fogva jelen volt.³⁹

A harti paradigmában elsődleges szabályok alatt azokat a kötelezettségeket értjük, amelyek a kezdetleges szervezetségi szinten lévő társadalmakban is megtalálhatóak, és amelyek kizárólag arra vonatkoznak, hogy az egyén mely magatartása megengedett vagy tiltott. Hart szerint az elsődleges szabályok három alapvető problémával küzdenek, nevezetesen, hogy (1) tartalmuk bizonytalan, (2) működésük statikus, valamint (3) hatékonyságuk alacsony.⁴⁰ Ezen problémák orvoslására jelennek meg a szofisztikáltabb szerveződésekben a másodlagos szabályok, melyek magukra az elsődleges szabályokra vonatkoznak. A bizonytalanságot orvosolják az „elismerési szabályok”, melyek feltárják, hogy pontosan mely szabályok alkotják ténylegesen az elsődleges kötelezettségeket, illetve milyen alaki jellemzőkkel és anyagi tartalommal kell egy normának bírnia ahhoz, hogy elsődleges szabály lehessen. A statikusságot küzdik le a „változtatási szabályok”, amelyek az elsődleges kötelezettségek létrehozásának, módosításának, illetve megszüntetésének az eljárási rendjét, valamint ezen változtatásokra hatáskörrel rendelkező alanyokat körvonalazzák. Végül a bizonytalanság eloszlatásra szolgálnak az „ítélkezési szabályok”, melyek révén az is egyértelművé válik, hogy ki jogosult megállapítani az elsődleges kötelezettség tényleges tartalmát, ezt milyen eljárási rendben teheti meg, valamint kötelezettségszegés esetén milyen szankciót alkalmazhat.⁴¹

³⁹ *Summary record of the third meeting on State Responsibility*, Yearbook of the ILC 1963, Vol. II., 1964. p. 229, 231.

⁴⁰ H. L. A. HART: *A jog fogalma*, Budapest, Osiris, 1995. 111–115.

⁴¹ Uo. 115–119.

Az erőszakalkalmazás tilalmának keretrendszere, benne az önvédelemhez való joggal az elsődleges normák részét képezi. Ezzel szemben az államfelelősségre vonatkozó nemzetközi jogi normaanyag a másodlagos normák terrénumába tartozik.⁴² Ennek az a következménye, hogy az államfelelősségi szabályok nem határozzák meg a felelősséget kiváltó elsődleges kötelezettségek tartalmát, csupán a felelősség általános feltételrendszerét, valamint az azzal járó jogkövetkezményeket rendezik.⁴³

4.2. A betudás kérdésköre a kiberműveletek terén

A „betudás” fogalma alatt azt értjük, amikor egy cselekvéshez hozzárendeljük a cselekvőt, beazonosítjuk a (nem jogi értelemben vett) felelős elkövetőt.⁴⁴ Némileg leegyszerűsítve, a betudás a „ki tette?” kérdésre adott válaszadás folyamatát hivatott leírni.⁴⁵ Rávetítve mindezt a kibertérre, a kiberműveletek betudása során megkülönböztethetünk technikai, jogi és politikai betudást.⁴⁶ Jelen tanulmányban kizárólag a jogi értelemben vett betudást vizsgálja.⁴⁷

⁴² ARSIWA Kommentár, i. m. 31. 1. bek.

⁴³ E. DAVID: Primary and Secondary Rules. In: James CRAWFORD – Alain PELLET – Simon OLLESON – Kate PARLETT (Eds.): *The Law of International Responsibility*. Oxford, OUP, 2010. 27.

⁴⁴ D. D. CLARK – S. LANDAU: Untangling Attribution. *Harvard National Security Journal*, 2011/2. 323.

⁴⁵ DELERUE: i. m. 51.

⁴⁶ N. TSAGOURIAS: Cyber Attacks, Self-Defence and the Problem of Attribution, *JCSL*, 2012/2. 233.; J. A. SCHNADER: Mal-Who? Mal-What? Mal-Where? The Future Cyber-Threat of a Non-Fiction Neuromancer: Legally Un-Attributable, Cyberspace-Bound, Decentralized Autonomous Entities, *North Carolina Journal of Law & Technology*, 2019/2. 22.

⁴⁷ A technikai betudás egyes dilemmáira összefoglaló jelleggel ld. DELERUE: i. m. 55–85.

Nemzetközi jogi értelemben vett betudás alatt azt a műveletet értjük, amelynek feladata „annak megállapítása, hogy egy természetes személy adott magatartása – függetlenül attól, hogy az tevékenységből vagy mulasztásból áll-e – a nemzetközi jog szempontjából »az állam cselekményének« (vagy bármely más, nemzetközi jogi jogalanyisággal rendelkező jogalany cselekményének) minősül-e”.⁴⁸ A betudás ilyenkor azt a logikai folyamatot írja le, amelyben egy cselekvést egy államhoz hozzákapcsolunk.⁴⁹ Erre a folyamatra elsődlegesen azért van szükség, mivel az állam mint egyfajta „jogi fikció” önmagában nem tud cselekedni, így szükségszerűen más (természetes vagy jogi) személyek cselekvésein keresztül tudja funkcióit ellátni.

A betudás kérdésköre legplasztikusabban az államfelelősségi szabályoknál érhető tetten, mindazonáltal a betudhatóság minden olyan területen releváns, ahol az állam valamilyen nemzetközi jogi joghatás kiváltására alkalmas magatartást tanúsít. Az eltérő rezsimekhez eltérő betudási mércék tartoznak,⁵⁰ emiatt pedig – a dogmatikai zűrzavar elkerülése végett – pontos elhatárolást kell tennünk. Ennek fényében a tanulmány a továbbiakban azokat a legfontosabb betudási mércéket vizsgálja meg, amelyek valamilyen formában relevanciával bírhatnak a kibertámadás – mint a *jus contra bellum* rezsimben értelmezendő cselekmény – jogi betudásában.

A kibertérben végrehajtott cselekedetek államnak való betudhatósága három meglehetősen nehezen bizonyítható körülmény konjunktív ismeretét feltételezi: (1) azon informatikai eszköz fizikai elhelyezkedésének azonosítása, amelyről a kiberműveletet megindították, (2) a kiberművelet ezen informatikai eszközről megindító személy kiléte és (3) ezen személy és az

⁴⁸ CONDORELLI – KRESS: i. m. 221.

⁴⁹ ARSIWA Kommentár, i. m. 36, 12. bek.

⁵⁰ A teljes problémakör részletes elemzéséhez ld. KAJTÁR: i. m. 2022.

állam közötti viszony.⁵¹ Az alább részletezett betudáskonceptiók a (3) feltétel megvalósítását szolgálják.

4.2.1. A (jogi értelemben vett) betudás az államfelelősségi szabályokban

Mivel az általános erőszak tilalmának megszegése nemzetközi jogot sértő cselekménynek minősül, így ez a jogsértés – az alább ismertetett feltételek fennállása esetén – államfelelősségi jogkövetkezményeket vonhat maga után. Az ENSZ Nemzetközi Jogi Bizottsága által 2001-ben elfogadott államok nemzetközi jogi felelősségéről szóló tervezet⁵² (*Articles on the Responsibility of States for Internationally Wrongful Acts*, ARSIWA) bár sosem vált nemzetközi egyezményé, tartalmának jelentős része a nemzetközi szokásjog kodifikációjának tekinthető, az aktuális, valamint korábbi ARSIWA-verziókra pedig jelentős számú nemzetközi vitarendező fórum hivatkozott,⁵³ így a szöveg normatív ereje nem megkérdőjelezhető.

Az állam nemzetközi jogi jogsértésért való felelősségének felhívásában egy hármas feltételrendszer⁵⁴ játszik központi szerepet, amelynek elsődleges, *sine qua non* feltétele a betudás, betudhatóság hiányában ugyanis nem lehet nemzetközi jogi értelem-

⁵¹ Hasonlóképp D. TRAN: The Law of Attribution: Rules for Attributing the Source of a Cyber-Attack, *YALE Journal of Law & Technology*, 2018. 387–391.

⁵² *Articles on the Responsibility of States for Internationally Wrongful Acts*, Yearbook of the ILC 2001. Vol. II., Pt. Two, 2007. p. 26. (a továbbiakban: ARSIWA).

⁵³ Kovács P.: *Nemzetközi közjog*. Budapest, Osiris, 2016. 542.; J. CRAWFORD: *State Responsibility: The General Part*. Cambridge, CUP, 2013. 43–44.

⁵⁴ Részletesen ld. J. CRAWFORD – S. OLLESON: The Character and Forms of International Responsibility. In: Malcolm D. EVANS (Ed.): *International Law*. Oxford, OUP, 2014. 452–467.

ben vett (állam)felelősségről beszélni. Ugyanakkor a „betudott” cselekmény sem eredményez automatikusan felelősséget, mivel előfordulhat, hogy az állam ténylegesen nem sértett nemzetközi jogi kötelezettséget,⁵⁵ vagy a jogsértését igazolni tudja jogellenességet kizáró okra hivatkozva.⁵⁶ Az ARSIWA II. fejezete (4–11. cikk) tartalmazza azokat a betudási teszteket, amelyek szigorúan államfelelősségi szempontból alkalmasak arra, hogy meghatározzák egy cselekmény betudhatóságát. Ezek az alábbiak:

- *de jure* és *de facto* állami szervek magatartása (4. cikk);
- kormányzati hatalom elemeinek gyakorlására feljogosított személyek vagy entitások magatartása (5. cikk);
- más állam részéről az állam rendelkezésére bocsátott szervek magatartása (6. cikk);
- *ultra vires* aktusok vagy az utasítások megtagadása (7. cikk, tekintettel a 4–6. cikkekre);
- az állam irányítása vagy ellenőrzése alatt végzett magatartás (8. cikk);
- hivatalos hatóságok hiányában vagy helyett végzett magatartás (9. cikk);
- felkelő vagy egyéb mozgalmak magatartása (10. cikk); valamint
- az állam által elismert és elfogadott magatartás (11. cikk).

Az említett tesztek közül azt a hármat mutatja be röviden a tanulmány, amely véleményünk szerint a legrelevánsabb lehet a kibertámadások betudhatóságának kérdésében. Közös ezen tesztekben, hogy elsődlegesen a hivatalos állami szervektől eltérő személyek vagy entitások magatartásának betudhatóságát teszik lehetővé, így elejét véve annak, hogy az állam kibújjon a felelősség alól azáltal, hogy nem hivatalos szerveken keresztül folytat jogellenes tevékenységet. A nem állami szereplők ezen vizsgálata

⁵⁵ ARSIWA, i. m. 2. cikk b) pont.

⁵⁶ ARSIWA, i. m. 20–25. cikk.

a kibertérben így azért releváns, mert ezen aktorok mögé könnyebben el tud rejtőzni az állam, adott esetben tehát érdekében állhat, hogy bevetésükkel elterelje a felelősséget vagy nehezítse annak megállapítását.

4.2.1.A. De facto állami szervek

Az ARSIWA 4. cikk (1) bekezdése rendezi a hivatalos (*de jure*) állami szervek betudhatóságát, ami az állammal való kapcsolat keletkeztetésének legegyszerűbb módja. Ebben a rendelkezésben az állami szervre (*State organ*) történő utalást a lehető legáltalánosabban kell értelmezni, az államszervezetben belül elfoglalt funkciótól, szinttől, illetve a hatalmi ágtól függetlenül.⁵⁷ Az elemzés fókuszára tekintettel a *de jure* szervek problematikájával – annak relatíve „egyértelműbb” betudási helyzete miatt – részletesebben nem kívánunk foglalkozni, ugyanakkor megjegyezzük, hogy számos ország rendelkezik már hivatalos katonai képességein belül különböző kiberhadtestekkel.⁵⁸

A *de jure* állami szerveken túl a 4. cikk (2) bekezdés kiemeli, hogy a „szerv” fogalma minden olyan személyt vagy entitást magába foglal, amelynek ez a státusza a belső jog szerint. Ugyanakkor a „magába foglal” fordulat révén ez a rendelkezés továbbmegy a hivatalos belső jogi státuszon, és betudhatóvá tesz minden olyan cselekményt, amely *tartalmában* olyan, mintha egy állami szerv követte volna el,⁵⁹ függetlenül a jogi formalitásoktól. Ez a megközelítés azt hivatott megelőzni, hogy egy állam

⁵⁷ ARSIWA Kommentár, i. m. 40, 6. bek.

⁵⁸ *The International Institute for Strategic Studies: Cyber Capabilities and National Power: A Net Assessment*, IISS Research Papers, 2021. (elérhető: <https://www.iiss.org/research-paper//2021/06/cyber-capabilities-national-power>)

⁵⁹ ARSIWA Kommentár, i. m. 42., 11. bek.; P. PALCHETTI: De Facto Organs of a State, *MPEPIL*, 2017. 10. bek.

a szerv belső jogi státuszának letagadása révén kerülje el a felelősséget.⁶⁰ Az ICJ gyakorlata több ízben is utalt ezekre az ún. *de facto* állami szervekre: a – jelentőségében nehezen túlbecsülhető – Nicaragua-ügyben a bíróság azt vizsgálta, hogy a sandinista hatalommal szemben felkelőharcot folytató kontrák voltak-e olyan mértékű függésben az Egyesült Államoktól, hogy cselekményeik már szinte Washington hivatalos fegyveres erőinek cselekményeivel voltak egyenértékűek. Kellő bizonyíték hiányában a hágai testület végül ezt nem találta megállapíthatónak.⁶¹

Részletesebben foglalkozott a kérdéssel az ICJ a Népir-tás-ügyben, amelyben Bosznia-Hercegovina állította azt, hogy a Bosznia-hercegovinai Szerb Köztársaság (*Republika Srpska*) hadserege, a *Vojska Republike Srpske* (VRS), valamint a „Skorpiók” nevű paramilitáris szervezet a Szerbia vezette Jugoszláv Szövetségi Köztársaság *de facto* állami szerveként járt el. E körben a bíróság úgy határozta meg a betudhatósági teszt mércéjét, mint egy olyan szigorú irányítást a személy vagy szerv felett, amely révén „teljes függőségben” (*complete dependence*)⁶² van az államtól, annak pusztán csak eszköze.⁶³ A bíróság végül itt is arra a következtetésre jutott, hogy a függetlenség minimális, de érzékelhető foka miatt nem lehetett a VRS és a Skorpiók magatartását betudni a belgrádi rezsimnek.⁶⁴

⁶⁰ CRAWFORD: i. m. 124–125.

⁶¹ Nicaragua-ügy, i. m. 109–110. bek.

⁶² Ez a kifejezés, valamint a függőség mértékére való utalás az ARSIWA-ban nem jelenik meg. Ld. M. MILANOVIĆ: State Responsibility for Genocide, *EJIL*, 2006/3. 583.

⁶³ *Application of the Convention on the Prevention and Punishment of the Crime of Genocide* (Bosnia and Herzegovina v. Serbia and Montenegro), Judgment, I.C.J. Reports 2007. p. 43. (a továbbiakban: Népirtás-ügy) 391–392. bek.

⁶⁴ Népirtás-ügy, i. m. 394–395. bek.

4.2.1.B. Irányítás vagy ellenőrzés az állam részéről

Az ARSIWA 8. cikke rendezi azt a betudhatósági esetcsoportot, amelyben egy nem állami szereplő az állam (1) utasítására, (2) irányítása vagy (3) ellenőrzése alatt cselekszik. A három feltétel diszjunktív, ugyanakkor valamelyiknek egyértelműen kapcsolódnia kell a nemzetközi jogi jogsértéshez.⁶⁵ Az általánosabb jelentéstartamú „ellenőrzés” fogalma esetről esetre, szigorúan értelmezendő: egy átfogó szervezés, pénzügyi támogatás, kiképzés és felfegyverzés sem tudja önmagában megalapozni azt a mércét, amit az ICJ a betudáshoz szükséges „hatékony ellenőrzésként” (*effective control*) címkézett a Nicaragua-ügyben.⁶⁶

A Népirtás-ügyben a bíróság megerősítette, hogy az ARSIWA 8. cikke szokásjogi erővel bír,⁶⁷ majd a Nicaragua-ügyre visszautalva elvi éllel határolta el a hatékony ellenőrzés mércéjét a teljes függőségtől: a hatékony ellenőrzés folyamán a tényleges kapcsolat intenzitása alacsonyabb, de magának az ellenőrzés meglétének minden egyes jogsértő részcsелеkmény kapcsán specifikusan és egyedileg kimutathatónak kell lennie, valamint a betudhatóság nem terjed ki azokra a cselekményekre, amelyek az ellenőrzés körén kívülre esnek.⁶⁸ Ezzel szemben a teljes függőség kivételesen alkalmazandó mércéje során az állam különösen nagyfokú ellenőrzést gyakorol a *de facto* szerv felett; ilyen esetekben azonban nem kell minden egyes részcsелеkmény, művelet kapcsán bizonyítani az ellenőrzést, ráadásul az *ultra vires* aktusok is betudhatóak lesznek.⁶⁹

⁶⁵ ARISWA Kommentár, i. m. 48, 7. bek.

⁶⁶ Nicaragua-ügy, i. m. 115. bek.; A. KEES: Responsibility of States for Private Actors, *MPEPIL*, 2011. 14–15. bek.

⁶⁷ Népirtás-ügy, i. m. 398. bek.

⁶⁸ ARISWA Kommentár, i. m. 47, 3. bek.; Népirtás-ügy, i. m. 400. bek.

⁶⁹ Népirtás-ügy, i. m. 393. bek., 400. bek.; MILANOVIĆ: i. m. 583.

4.2.1.C. Utólagos elismerés és elfogadás

Az államfelelősség egyfajta *ex post facto* megalapozásához nyújt segítséget az ARSIWA 11. cikke, amely a 4–10. cikkekhöz képest annyiban szubszidiárius,⁷⁰ hogy abban az esetben eredményez betudást, ha a többi betudási teszt alapján nem lehet megállapítani a cselekménynek az állammal való kapcsolatát. Ezen mérce szerint a nem állami szereplők cselekményei abban a mértékben lesznek betudhatóak az államnak, amennyiben azt utólag sajátjának elismeri és elfogadja (*acknowledgement and adoption*). A mérce teljesülését több szempont is keretek közé szorítja: egyrészt az „és” szó jelzi, hogy a két feltétel kumulatív, vagyis az elismerésre és az elfogadásra egyaránt szükség van a betudáshoz. Másrészt az elismerésnek és elfogadásnak világosnak és egyértelműnek kell lennie.⁷¹ Ez annyit jelent, hogy az állam által kifejezett támogatás vagy helyeslés önmagában nem elégséges a betudáshoz.⁷² Harmadrészt a szövegtervezet is kifejezi annak a tényét, hogy az állam – amennyiben más mérce szerint nem betudható neki a cselekmény, hisz ekkor nincs „választási lehetősége” – maga dönti el, hogy mennyiben és milyen mértékben („*if and to the extent*”) teszi magáévá a magánszereplői cselekményt. Az utólagos elismerés és elfogadás archetípusa a Teheráni túszok-ügy, amelyben az ICJ megállapította, hogy az amerikai nagykövetséget megostromló militarizált iráni diákok tevékenysége azáltal lett betudható Iránnak, hogy azt utólag elismerte és elfogadta. A bíróság érvelése szerint Khomeini ajatollah nyilatkozatai a nagykövetség elfoglalásáról, valamint az új iráni rezsim több hivatalos szereplőjének kifejezett és ismétlődő támogatása

⁷⁰ ARSIWA Kommentár, i. m. 53, 8. bek.

⁷¹ Uo.

⁷² CRAWFORD: i. m. 187.

„transzformálta az elfoglalás által kialakult helyzet jogi minőségét” és azokat az állam cselekményévé fordította át.⁷³

4.2.2. Betudás a *jus contra bellum* területén

A nemzetközi jog szerződéses és szokásjogi⁷⁴ *jus contra bellum*-szabályai alapján egyértelmű az a *de lege lata*-állapot, miszerint jogilag értékelhető erőszak elkövetésére csak az állam képes.⁷⁵ Ez a megállapítás egyértelműen következik abból is, ahogy az Alapokmány a 2. cikk (4) bekezdésnek személyi hatályát a „Szervezet összes tagjaiban” jelöli meg, az ENSZ tagjai pedig kizárólag államok lehetnek.⁷⁶ Erre figyelemmel a nem állami szereplők által elkövetett erőszak is csak akkor kerül(het) a *jus contra bellum* látókörébe, ha az valamilyen formában betudhatóvá válik az államnak.

Két szignifikáns betudási mérce azonosítható be a rendszeren belül, amelyeket az agresszió meghatározásáról szóló 3314. sz. ENSZ közgyűlési határozata fektetett le. A legtipikusabb agressziós cselekményeket felsoroló 3. cikk exemplifikatív listája szerint a közvetlen államcselekményen túl közvetett (indirekt) módon, de agressciónak minősül az is, (1) ha egy állam a területét rendelkezésre bocsátja egy másik államnak abból a célból, hogy ezt a másik állam arra használja, hogy egy harmadik állam

⁷³ *United States Diplomatic and Consular Staff in Tehran* (United States of America v. Iran), Judgment, I.C.J. Reports 1980. p. 3, 74. bek.

⁷⁴ Az ICJ által a Nicaragua-ügyben tett elvi jelentőségű megállapítás óta közsímet, hogy a *jus contra bellum*ra vonatkozó szerződéses és szokásjogi szabályok bár jelentős konvergenciát mutatnak, mégsem egyezik meg teljesen a tartalmuk. Ld. Nicaragua-ügy, i. m. 175–176. bek.

⁷⁵ DÖRR – RANDELZHOFFER: i. m. 213, 29. bek.

⁷⁶ Alapokmány, i. m. 3. cikk; 4. cikk (1) bekezdés. Ugyanakkor a szakirodalom szerint az ún. *de facto* rezsimet (pl. Tajvan) is egyaránt kötelezi a 2. cikk (4) bekezdés. Ld. DÖRR – RANDELZHOFFER: i. m. 213, 29. bek.

ellen agressziós cselekményt hajtson végre;⁷⁷ (2) ha egy állam fegyveres bandákat, csoportokat, irreguláris erőket vagy zsoldosokat küld, vagy a nevében ilyeneket küldenek egy másik állam ellen olyan fegyveres cselekmények végrehajtására, amelyek elérik a 3. cikkben felsorolt egyéb cselekmények súlyát, vagy ha egy államnak komoly része van ebben.⁷⁸

Az agresszió meghatározásáról határozat 3. cikk f) pontjában rögzített terület rendelkezésre bocsátására fogalmilag csak az állam tudatos magatartásával kerülhet sor.⁷⁹ Ebben az esetben a megengedő aktus fogja megvalósítani az indirekt agressziót, amennyiben a területre átengedett állam a harmadik állammal szemben agresszió-szintű fegyveres cselekményt hajt végre. Vagyis nem az agresszor állam cselekménye az, amit „betudunk” az átengedőnek, hanem az átengedés maga konstituálja az agressziós cselekményt, amelyet viszont csak *de jure* szerv engedélyezhet.⁸⁰ Ennek a szabálynak az erőszak tilalmáról rendelkező rezsimtől független, általános normatív megjelenése érhető tetten a – később bemutatandó – ún. „*due diligence*” kötelezettségben, amelynek értelmében az állam – amennyiben tudomása van róla – nem engedheti meg, hogy a területét olyan cselekmények végrehajtására használják, amelyek más államok jogaival ellentétesek.⁸¹

A 3. cikk g) pontja szintén indirekt agressziós helyzetet ír le. Ilyenkor az állam által vagy az állam nevében az irányítása vagy ellenőrzése alatt álló egyén vagy csoport révén küldött irreguláris

⁷⁷ *Definition of Aggression*, UNGA, A/RES/3314(XXIX), 1974. (a továbbiakban: Agresszió meghatározása) 3. cikk f) pont.

⁷⁸ Agresszió meghatározása, i. m. 3. cikk g) pont.

⁷⁹ Ez abból is következik, hogy az agresszió definíciójának fogalmi eleme az állam által történő elkövetés. Ld. Agresszió meghatározása, i. m. 1. cikk.

⁸⁰ KAJTÁR G.: *A nem állami szereplők elleni önvédelem a nemzetközi jogban*. Budapest, ELTE Eötvös, 2015. 80, 90.

⁸¹ *Corfu Channel* (United Kingdom v. Albania), Merits, Judgment, I.C.J. Reports 1949. p. 4. (a továbbiakban: Korfu-szoros-ügy) 22.

erők követnek el agressziós cselekményt. Ez a rendelkezés az ICJ olvasatában szokásjogi erővel bír,⁸² és kimondottan a cselekmény államnak való betudhatósága szempontjából való vizsgálatára alkalmas.⁸³ A küldésben való „komoly rész” (*substantial involvement*) értelmezésében egy szűkítő megközelítés tekinthető követendőnek, mivel maga az ICJ is kizárta azt, hogy az irreguláris erők rejtegetése vagy az államon belüli megtűrése elérné a 3. cikk g) pontjában meghatározott mércét,⁸⁴ továbbá a 3314. sz. határozat korábbi tervezetei tartalmazták a „szervezés”, „támogatás”, illetve „segítés” magatartásokat is, de a végleges határozatban csak a „küldés” maradt meg.⁸⁵ A szakirodalom álláspontja akként foglalható össze, hogy a „komoly rész” eléréséhez szükséges, hogy (1) az állam tudjon arról, hogy agressziós cselekmény elkövetését készítik elő, (2) ebben az előkészítésben vegyen részt, mégpedig (3) jelentős mértékben, vagyis részvétele nem lehet mellékes vagy járulékos.⁸⁶ A feltételek teljesülése esetén is indirekt agresszió valósul meg, de azt a betudás miatt úgy kell tekinteni, hogy az állam követi el.⁸⁷

Fontos, hogy az előbbieken bemutatott betudási mércék következményeként a felelősség másképp alakul, mivel a betudás lényege ehelyütt abban áll, hogy a cselekményt *államközi*

⁸² Nicaragua-ügy, i. m. 195. bek.

⁸³ Fegyveres tevékenységek-ügy, i. m. 143. bek.

⁸⁴ CORTEN: i. m. 2010. 446–447.; Ruys: i. m. (2010) 388–389, 529.

⁸⁵ S. MAHMOUDI: *Self-Defence and “Unwilling or Unable” States*. Collected Courses of the Hague Academy of International Law, Vol. 422, 2022. 295.; J. STONE: Hopes and Loopholes in the 1974 Definition of Aggression, *AJIL*, 1977/2. 237.

⁸⁶ O. CORTEN – F. DUBUISSON: L’opération «liberte immuable»: une extension abusive du concept de legitime defense, *Revue Générale de Droit International Public*, 2002/1. 56. Ellentétes véleményhez ld. E. de WET: The Invocation of the Right to Self-Defence in Response to Armed Attacks Conducted by Armed Groups: Implications for Attribution, *LJIL*, 2019/1. 103.

⁸⁷ Ruys: i. m. (2010) 138.

erőszaknak lehessen tekinteni. Pusztán az ismertetett mércék alapján az állam nem felel azokért a cselekedetekért, amelyek tekintetében az államfelelősségi mércék alapján nem betudható neki a nemzetközi jogi kötelezettségzegő cselekmény. Amiért az állam ilyen esetekben felelhet, az az a jogsértés, amit *azzal a specifikus magatartással követ el, ami egyben a betudást is kiváltja.*

Az első esetben az állam az átengedő aktusával megvalósított agresszióért felel, míg a második esetben az irreguláris erők küldése, mint az állam *saját jogsértése* tud bizonyos elsődleges kötelezettségek (pl. belügyekbe való beavatkozás tilalma,⁸⁸ terrrorszervezetek megtűrésének és támogatásának tilalma⁸⁹) megszegésének megállapításához vezetni. Amíg azonban az államfelelősségi mércék szerint ezeknek az irreguláris erőknek a cselekményei nem betudhatóak az államnak, az általuk követett magatartás miatt az állam nem tehető felelőssé.

4.3. Részösszegzés: a konvencionális betudáskonceptiók elégtelenek mi- volta a kibertérben

A kibertámadások államoknak való betudását jelentősen megnehezíti a kibertér sajátosan anonim jellege, konkrétabban fogalmazva az, hogy a kibertér lehetőséget ad arra, hogy a támadás nyomait a támadó elfedje, vagy félrevezető nyomokat helyezzen el a támadáshoz használt infrastruktúrában/platformon.⁹⁰

⁸⁸ Nicaragua-ügy, i. m. 205. bek.

⁸⁹ *Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations*, UNGA, A/RES/2625(XXV), 1970. Annex.; Fegyveres tevékenységek-ügy, i. m. 162. bek.

⁹⁰ B. PIRKER: Territorial Sovereignty and Integrity and the Challenges of Cyberspace. In: Katharina ZIOLKOWSKI (Ed.): *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy*. Tallinn, NATO CCD COE Publications, 2013. 212.

Míg egyes szerzők szerint a technikai betudás nehézségére vonatkozó tudományos konszenzus eltűzött,⁹¹ a kommentátorok többsége azon az állásponton van, hogy a technikai betudás időigényes és nem feltétlenül pontos.⁹² Önmagában a kibertámadás elkövetéséhez használt informatikai eszköz területi azonosítása azonban ugyancsak elégtelen, ugyanis az államnak való betudhatóságot – és ezáltal a jogkövetkezményeket – az eszközt működtető természetes személy és az állami közötti kapcsolat alapozhatja meg. Ez a – szakirodalomban „*human machine gap*”-nek nevezett⁹³ – problémakör további akadályát képezi a kibertámadások hatékony betudásának. Ám még az elkövető kilétének azonosítása sem elégséges, hiszen az államnak való betudhatósághoz ezen elkövető és az állam közötti kapcsolat minősítése is szükséges, figyelemmel a fent részletezett, az államfelelősség és a *jus contra bellum* körében alkalmazott betudási technikákra.

A technikai betudás nehézségei, a „*human machine gap*” és az elkövető illetve az állam közötti viszony jogi minősítése együttesen rendkívül tényintenzív, bizonyítékigényes, lassú és bizonytalan eredményű betudási kísérletekre ad csak lehetőséget. A betudás nehézkes mivolta pedig lehetetlenné teszi, hogy a megtámadott állam gyorsan és hatékonyan gyakorolja önvédelemhez való jogát vagy eredményesen alkalmazzon jogszerű ellenintézkedéseket. Álláspontunk szerint a „vonakodik vagy képtelen” doktrína betudhatósági *lex specialis* mérceként való alkalmazása kielégítő

⁹¹ TRAN: i. m. 393.

⁹² L. CHRICOP: A Due Diligence Standard of Attribution in Cyberspace, *ICLQ*, 2018/3. 646.

⁹³ R. GEISS – H. LAHMANN: Freedom and Security in Cyberspace: Shifting the Focus away from Military Responses towards Non-Forcible Countermeasures and Collective Threat-Prevention, In: Katharina ZIOLKOWSKI (Ed.): *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy*. Tallinn, NATO CCD COE Publications, 2013. 625.

megoldást ad a kibertámadások betudhatóságával kapcsolatos, fent vázolt nehézségeire.

A fent ismertetett betudási tesztek szigorú (pl. teljes függőség, hatékony ellenőrzés), bizonytalan tartalmú (pl. küldés, vagy „komoly rész” a küldésben) vagy életszerűtlen (pl. utólagos elismerés) mivolta, valamint a kibertámadások betudásának technikai akadályai már elégséges alapot szolgáltatnak egy kibertérre alkalmazandó *lex specialis* betudási mérce kidolgozására. Ehelyütt utalunk arra, hogy a klasszikus betudási mércék magas szintű bizonyítottságot megkívánó jellege önmagában még nem teszi objektíve lehetetlenné a kibertámadások betudását; ugyanakkor álláspontunk szerint a kibertámadások számának csökkentésére irányuló jogpolitikai célt jobban szolgálja egy lazább betudási mérce megfogalmazása. A visszaélések elkerülése végett ennek a mércének mindazonáltal szűk körűnek és pontosan meghatározottnak kell lennie. A következőkben erre teszünk kísérletet.

5. A „vonakodik vagy képtelen” doktrína alkalmazása a kibertámadások betudására

A kibertámadások könnyű, gyors és hatékony betudása elengedhetetlen ahhoz, hogy az állam az őt ért, az erőszak tilalmába ütköző cselekménnyel szemben fellépessen, figyelemmel a *jus contra bellum* szabályainak államközi jellegére. Amennyiben a kibertámadást egy nem állami szereplő hajtja végre, és a fenti betudási nehézségek nem teszik lehetővé a betudást, a megtámadott állam eszköztelen marad a támadás elhárítására. Ez különösen súlyos akkor, ha fegyveres támadás szintjét elérő kibertámadás merül fel, hiszen valamilyen szintű állami szerepvállalás elengedhetetlen ahhoz, hogy a megtámadott állam az Alapokmány 51.

cikke szerinti önvédelem jogát gyakorolhassa,⁹⁴ az ezt el nem érő intenzitású támadás ellen pedig ellenintézkedéssel felléphessen.⁹⁵ Ismertek olyan álláspontok, amelyek szerint az önvédelem joga nem állami szereplőkkel szemben is gyakorolható,⁹⁶ ezzel implicit módon elismerve a fegyveres támadást megvalósítani képes nem állami szereplők nemzetközi jogi jogalanyiságát. Ezen nézetrendszer logikáját követve valójában felesleges volna rugalmasabb *lex specialis* betudhatósági mércét alkalmazni a kibertámadások tekintetében, hiszen a megtámadott állam *közvetlenül* a támadást megvalósító nem állami szereplővel szemben gyakorolhatná önvédelemhez való jogát, amely könnyedén kinyithatná Pandora szelencéjét az önvédelmi jog ekkora mértékű kitérítésével, a területi állam szuverenitásának elfogadhatatlan mértékű korlátozásáról nem is beszélve.

Álláspontunk szerint azonban két fontos jogpolitikai megfontolás is amellet szól, hogy – annak érdekében, hogy az államok természetes önvédelemhez való joga megfelelően érvényesülhessen, illetve a fegyveres támadás szintjét el nem érő erőszakos cselekményekkel szemben megfelelő ellenintézkedések alkalmazására kerülhessen sor – a hagyományosan nehezen alkalmazható betudási mércékhez képest egy rugalmasabb betudási tesztet alkalmazzunk *kizárólag* a kibertámadások esetében. Egyrészt (1) a területi államnak való betudás révén a nemzetközi jog konvencionális keretei között maradhatnak az önvédelem jogát gyakorló

⁹⁴ KAJTÁR G.: Vonakodik vagy nem képes? Az önvédelem jogának újabb paradigmaváltó kísérlete, *Közjogi Szemle*, 2018/1. 2.; NOLTE – RANDELZHOFFER: i. m. 1401, 6. bek.

⁹⁵ ARSIWA, i. m. 49. cikk (1) bekezdés.

⁹⁶ Ez a nézet a 2001. szeptember 11-i terrortámadást követően terjedt el, elsősorban a nemzetközi terrorizmus elleni harc hatékonyságára, valamint a BT 1368. és 1373. sz., ködös megfogalmazású határozataira hivatkozva. A nézetek bemutatásához és átfogó kritikájához ld. Kajtár: i. m. (2015) 299–348.

államok, (hiszen így végső soron a területi állam válik a fegyveres támadás elkövetőjévé), másrészt (2) amennyiben az államközi erőszakalkalmazás szabályai között tartjuk a konfliktust, úgy a rugalmasabb betudási mérce alkalmazásával elhárulnak a technikai betudás nehézségeiből fakadó akadályok.

Ilyen rugalmas betudási mérce lehet az alább ismertetendő „vonakodik vagy képtelen” (*unwilling or unable*) mérce. A továbbiakban részletesen ismertetjük a „vonakodik vagy képtelen” doktrínát, kimutatjuk, hogy a jogrendszerben már most is jelen lévő, részben hasonló alapokon nyugvó „*due diligence*” kötelezettség annak nem megfelelő alternatívája, majd megvizsgáljuk egy puhább, illetve egy szigorúbb „vonakodik vagy képtelen” betudhatósági teszt alkalmazásának potenciális előnyeit és hátrányait.

5.1. A „vonakodik vagy képtelen” doktrína eredete és jellemzői

A „vonakodik vagy képtelen” doktrína vagy mérce a nem állami szereplőkkel szembeni önvédelmi jogot tágító elméletek egyike. A doktrína eredete a klasszikus nemzetközi jog *jus in bello*-szabályrendszerének abból a korszakából származik, amikor a fegyveres konfliktusok során kiemelt jelentősége volt a semleges államoknak. Ebben a rendszerben a semlegességgel összeegyeztethetetlen volt, ha a hadakozó felek egyikét egy harmadik, a konfliktusban nem résztvevő állam valamilyen formában megsegítette.⁹⁷ A nem állami szereplőkkel szemben való fellépést megalapozó elméletként ugyan ebben a korszakban is elvétve hivatkoztak csak az államok a doktrínára,⁹⁸ de a kibontakozó *jus contra bellum*-rezsím hamar gátat szabott a további fejlődésnek.

⁹⁷ A. S. DEEKS: “Unwilling or Unable”: Toward a Normative Framework for Extraterritorial Self-Defense, *Virginia JIL*, 2012/3. 496–503.

⁹⁸ I. BROWNLIE: International Law and the Activities of Armed Bands, *ICLQ*, 1958/4. 732–733.

A doktrína „felélesztésére” a 2001. szeptember 11-i terrortámadás után, a „*War on Terror*” és a Bush-doktrína megszületése idején került sor, az Iraki és Szíriai Iszlám Állam (ISIS) elleni küzdelmek folyamán pedig már hivatkozási alappá vált.⁹⁹ Az állami gyakorlat mellett a jogtudomány is próbálta nyomon követni a doktrína reneszánszát, különböző deklarációk, elvek, *policy paper*ök megfogalmazásával.¹⁰⁰

A doktrína lényege szerint amennyiben egy állam területéről (területi állam) nem állami szereplők az erőszak tilalmáról szóló, rezsim szempontjából értékelhető erőszakot alkalmaznak egy másik állam (célállam, megtámadott állam) ellen, akkor a nem állami szereplővel szemben a célállam közvetlenül felléphet, vagyis abban az esetben is, ha semmilyen módon nem lehet az erőszakalkalmazást a területi államnak – vagy egyéb más államnak – betudni. A doktrínát ebben a formájában elsődlegesen az önvédelmi jogon belül a szükségesség mércéjében vizsgálандó szempontnak tekintik,¹⁰¹ de megjelent már az önvédelmi jog

⁹⁹ O. CORTEN: The ‘Unwilling or Unable’ Test: Has it Been, and Could it be, Accepted?, *LJIL*, 2016/3. 777–785. Ugyanakkor a doktrínára 1981-ben már hivatkozott Izrael Jordániával szemben a Hezbollah elleni fellépésre való képtelenség, illetve vonakodás miatt. Ld. de WET: i. m. 94.

¹⁰⁰ Ezek közül a legjelentősebb az ún. *Bethlehem Principles*, ami Daniel Bethlehem, az Egyesült Királyság külügyminisztériumának volt jogi főtanácsadójához köthető. A 16 pontból álló *Principles* 11. és 12. kezeli a „vonakodik” és a „képtelen” szituációit. D. BETHLEHEM: Self-Defense Against an Imminent or Actual Armed Attack By Nonstate Actors, *AJIL*, 2012/4. 776.

¹⁰¹ Így pl. J. BRUNNÉE – S. J. TOOPE: Self-Defence against Non-State Actors: Are Powerful States Willing but Unable to Change International Law?, *ICLQ*, 2017/2. 264.; R. van STEENBERGHE: Self-Defence in Response to Attacks by Non-state Actors in the Light of Recent State Practice: A Step Forward?, *LJIL*, 2017/1. 200–202.; DEEKS: i. m. 495. Megjegyezzük, hogy ez az értelmezés akkor is hibás volna, ha egyébként a doktrína kikristályosodott tartalommal és szokásjogi erővel bírna, mivel az önvédelmi joghoz

megnyitásához vezető új jogalapként, valamint – a betudhatósági probléma áthidalása érdekében – betudási tesztként is.¹⁰²

Jelen formájában a „vonakodik vagy képtelen” doktrína legnagyobb hiányossága, hogy a neki szánt szerepet nem tudja betölteni, mivel tartalma bizonytalan,¹⁰³ *de lege lata* szokásjogi megalapozottsága pedig egyelőre nem kimutatható.¹⁰⁴ Jelen tanulmányban ezeket nem kívánjuk megcáfolni; pusztán annyit állítunk hogy a doktrína a kibertér specifikumai miatt hatékony kiegészítését adhatná a jelenlegi *jus contra bellum* által ismert betudási mércéknek. Ezt megelőzően viszont röviden szólunk kell az ezen megközelítéshez nagyban hasonlító „*due diligence*” mércéről.

5.2. A „*due diligence*” kötelezettsége ugyancsak elégtelen a kibertámadásokkal szembeni hatékony fellépéshez

Elöljáróban elmondható, hogy létezik olyan szakirodalmi álláspont, amely önmagában a „*due diligence*” mércét elégséges kontrollmechanizmusnak tartja ahhoz, hogy ne legyen indokolt a kiberműveletek kapcsán egy sajátos betudási mérce alkalmazása.¹⁰⁵ Az alábbiakban

kapcsolódó „szükségesség” nem egy jogosultságot ad az államnak, hanem éppen, hogy a *szükséges mértékre* korlátozza az egyoldalúan bevethető erőszakot. Ld. RUYS: i. m. 2010. 123–124.; CORTEN: i. m. 2016, 796.

¹⁰² KAJTÁR: i. m. (2018) 2–3.; MAHMOUDI: i. m. 353.

¹⁰³ KAJTÁR: i. m. (2018) 6.; DEEKS: i. m. 505.; BRUNNÉE – TOOPE: i. m. 280.

¹⁰⁴ CORTEN: i. m. (2016) 779.; MAHMOUDI: i. m. 378. Ellentétes véleményen van Kis Kelemen Bence, aki szerint a doktrína támogatottsága nő. KIS K. B.: *Célzott likvidálás a nemzetközi jogban, különös tekintettel a fegyveres, pilóta nélküli repülőgépek alkalmazására*, Doktori (PhD) értekezés, Pécs, Pécsi Tudományegyetem Állam- és Jogtudományi Doktori Iskola, 2021. 88–89.

¹⁰⁵ Így pl. A. KAVALIUSKAS: Can the Concept of Due Diligence Contribute to Solving the Problem of Attribution with Respect to Cyber-Attacks

röviden ismertetjük a „*due diligence*” kötelezettség leglényegesebb vonásait, majd kimutatjuk, hogy valójában miért nem képezheti hatékony alternatíváját egy rugalmasabb betudási tesztnek.

5.2.1. A „*due diligence*” mérce tartalma és lényege

A kibertérben is érvényesülő „*due diligence*” kötelezettség¹⁰⁶ alapján egy állam – amennyiben arról tudomása van, vagy arról tudomással kéne bírnia – nem engedheti meg, hogy területén nemzetközi jogi kötelezettséget sértő magatartást tanúsítsanak.¹⁰⁷ A „*due diligence*” elsődleges nemzetközi jogi kötelezettség, annak megsértése kiválthatja az állam felelősségét. A Tallinni Kézikönyv szerint a „*due diligence*” kötelezettség az államok szuverenitása tiszteletben tartásának kötelezettségéből következik, az nem foglal magába aktív megelőzési kötelezettséget, alapvetően mulasztással követhető el, valamint e mulasztás csak akkor tényállásszerű, ha annak következményeképpen a célállamot súlyos sérelem éri, tehát a „*due diligence*” kötelezettség tartalmaz valamiféle *de minimis* mentesülési lehetőséget.¹⁰⁸

5.2.2. A „*due diligence*” mércét a rugalmasabb betudhatósági teszt helyettesítőjének tekintő nézetek kritikája

A „*due diligence*” mérce álláspontunk szerint alapvetően két okból nem alkalmas arra, hogy egy rugalmasabb betudási teszt helyettesítőjeként szolgáljon. Egyrészt a „*due diligence*” a tanulmányban fent már részletesen ismertetett, harti értelemben vett elsődleges

Conducted by Non-State Actors Which Are Used as Proxies by States?, *Tézés Apžvalga Law Review*, 2022/2. 4–30.; CHRICOP: i. m. 643–668.

¹⁰⁶ Tallinn Manual 2.0, i. m. 30–43.

¹⁰⁷ Korfu-szoros-ügy, i. m. 22.

¹⁰⁸ Tallinn Manual 2.0, i. m. 36–37.

nemzetközi jogi kötelezettség. Ennek megfelelően amennyiben egy állam területéről az állam tudomásával indítanak kibertámadást, ám az bármilyen okból az államnak nem betudható, úgy a területi állam *csak* a „*due diligence*” kötelezettség megsértéséért lesz felelős, a kibertámadásért azonban nem, mely különbség súlyos következményekkel járhat. Amennyiben például az állam területéről induló kibertámadás fegyveres támadást valósít meg, ám az az államnak nem betudható, úgy a célállamot nem illeti meg az önvédelem joga. Ugyancsak probléma, hogy a kiberművelet által megsértett elsődleges nemzetközi jogi norma jellegére tekintet nélkül a területi állam továbbra is csak a „*due diligence*” kötelezettség megsértéséért lesz felelős. Amennyiben a konvencionális betudhatósági mércék alkalmazása révén az elsődleges nemzetközi jogi kötelezettséget sértő kiberművelet a területi államnak nem betudható, ám a „*due diligence*” kötelezettségét megsérti, úgy a célállam ellenintézkedései is csak a „*due diligence*” kötelezettség megsértéséhez kapcsolódhatnak. Vagyis ezen kötelezettséggel kell arányban állniuk, illetve a vonatkozó jogellenes állapot (azaz a „*due diligence*” megsértése) megszüntetésére kell, hogy irányuljanak.¹⁰⁹ Álláspontunk szerint nem elég rugalmas az a keretrendszer, amely a betudhatóság rovására a „*due diligence*” kötelezettséget tartja az államok érdekeit megfelelően kiegyensúlyozó jogvédelmi mechanizmusnak, hiszen valójában – betudás hiányában – minden elsődleges kötelezettséget megszegő cselekmény mintegy „feloldódik” a „*due diligence*” kötelezettség megsértésében. További probléma, hogy az ellenintézkedések tekintetében nincs lehetőség disztingvált válaszadásra, az ellenintézkedés nem a kiberművelet által megsértett elsődleges kötelezettséggel kell, hogy arányos legyen, illetve nem annak megszüntetését kell céloznia, azok kizárólag a „*due diligence*” kötelezettség megsértéséhez kapcsolódhatnak.

¹⁰⁹ ARSIWA, i. m. 49. cikk (1) bekezdés.

Másrészt a „*due diligence*” kötelezettséghez kapcsolt *de minimis* kivétel okán a célállam adott esetben arra kényszerülne, hogy az elsődleges nemzetközi jogi kötelezettséget sértő, ám a területi államnak nem betudható kibertámadást megtorlatlanul hagyja, amennyiben annak következményei egy bizonyos szintet nem érnek el. Álláspontunk szerint azonban a rugalmasabb betudhatósági mérce adekvátabb módon szabályozná a célállam lehetőségeit, hiszen így az erőszak szintjét elérő bármely kiberművelettel szemben felléphetne, mely fellépési lehetőség azonban nem vezetne eszkalációhoz, figyelemmel az ellenintézkedéskehez¹¹⁰ és az önvédelem jogának gyakorlásához fűzött szükséges-ségi-arányossági megszorítására.

5.3. A „vonakodik vagy képtelen” teszt, mint specifikus kiber betudhatósági mérce

A kibertámadásokkal szembeni hatékony fellépés lehetőségét tehát sem a klasszikus betudási mércék alkalmazása, sem a „*due diligence*” kötelezettség nem garantálja. Ezzel szemben a „vonakodik vagy képtelen” doktrína betudhatósági tesztként történő alkalmazása minden fent vázolt problémára megoldást nyújt, azzal a megkötéssel, hogy magának a tesztnek is több értelmezése lehetséges.

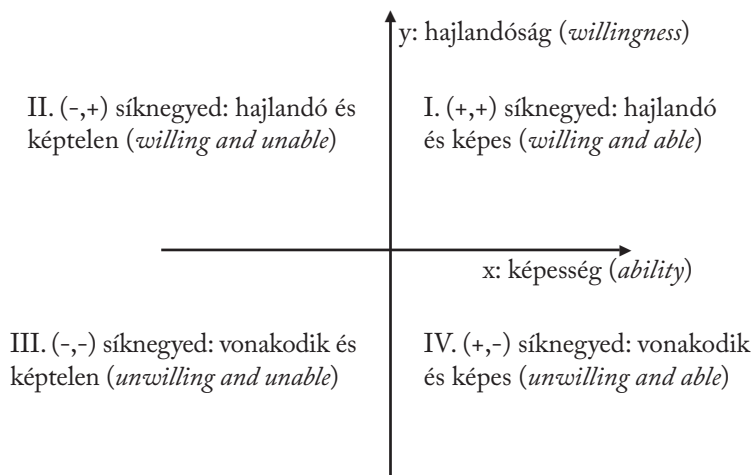
A „vonakodik vagy képtelen” teszt kapcsán két szempont vizsgálendő: (1) vonakodik avagy hajlandó-e a területi állam fellépni a területéről indított kibertámadások megakadályozása érdekében, illetve (2) technikai, gazdasági, politikai és katonai kapacitásai objektíve lehetségessé teszik-e az állam számára a felismert fenyegetés vagy támadás elhárítását. Az ezen változók által meghatározott viszonyulási lehetőségeket az 1. ábra szemlélteti.

A nem állami szereplő által végrehajtott kibertámadásról tudomással bíró, ám azt elhárítani meg sem kísérő (tehát vonakodó)

¹¹⁰ ARSIWA, i. m. 49–51. cikk.

államnak való betudhatóság evidensnek tetszik, a vonatkozó magatartás részben az utólagos elismerés klasszikus betudási mércéjével is rokonítható (bár annál enyhébb feltételekkel bír), hiszen a nemzetközi jogot sértő magatartások tudott és vállalt megtűrése bizonyos értelemben annak helyeslését fejezi ki. Ennek megfelelően az 1. ábra III. és IV. síknegyedében megjelenő esetekben *a kibertámadás egyértelműen betudható volna a területi államnak*.

Természetesen amennyiben a területi állam képes és hajlandó is fellépni a nem állami szereplő által elkövetett kibertámadással szemben (I. síknegyed), úgy a kibertámadás maga sem valósul meg, vagy – amennyiben megvalósul, úgy – a területi állam az elkövetőket még azelőtt felelősségre vonja, hogy a célállam önvédelemhez való jogát gyakorolhatná vagy ellenintézkedéseket foganatosíthatna, ennek megfelelően *ebben az esetben a kibertámadás a területi államnak nem volna betudható*.



1. ábra: a területi állam lehetséges viszonyulásai a területéről induló kibertámadásokhoz

Az értelmezési nehézséget – és kapcsolódó joggyakorlat híján kizárólag jogpolitikai megfontolások alapján eldönthető dilemmát – a II. síknegyedben megjelenő helyzet jelenti, amikor is a területi állam tudomással bír a területéről indított kibertámadásról, annak megakadályozására hajlandóságot mutat, azonban híján van azoknak a technikai, gazdasági, katonai eszközöknek, amelyekkel a támadást ténylegesen elháríthatná. Az alább felvázolt „képtelen” alteszt megengedőbb és szigorúbb értelmezési lehetőségének jogkövetkezményeit bemutatva világunk rá a két lehetséges megközelítés előnyeire és hátrányaira.

5.3.1. A „képtelen” alteszt lazításának előnyei és hátrányai

A „képtelen” alteszt lazább értelmezése szerint a területi államokat egyfajta eredménykötelem (*obligation of result*) terheli a kibertámadások megállítása kapcsán, amennyiben ugyanis egy állam területéről nem állami szereplők kibertámadást indítanak, úgy alappal vethető fel, hogy – már pusztán a támadás elindítása okán – a területi állam vagy nem volt képes, vagy nem is kívánta megakadályozni a támadást.

Ez a lazább, de következményei szerint szigorúbb betudhatósági teszt alkalmazása lehetővé teszi, hogy a célállam gyors, hatékony és a kibertámadás által elszenvedett jogsértéssel arányos válaszlépéseket tegyen. A kibertámadások betudhatóságának fent ismertetett nehézségei kevésbé érvényesülnek, ugyanakkor a támadást és a válaszlépéseket az államközi konfliktusok körébe emeli, ami segíthet a nemzetközi jog konvencionális keretei között tartani az eseményeket. Ugyancsak a nemzetközi jog konvencionális kereteinek erősítését jelenti az objektív felelősségi rendszer, hiszen a lazább „képtelen” alteszt alkalmazása esetén a területi állam magatartását nem tudja kimenteni azáltal, hogy megfelelő – ám végül eredménytelen – lépéseket tett a kibertámadás elhárítására.

A lazábbra szabott „képtelen” alteszt nem elhallgatható hátránya azonban, hogy már rövidtávon is megronthatja a területi állam és a célállam közötti viszonyt, illetve csökkentheti a felek közötti együttműködési hajlandóságot, figyelemmel arra, hogy a területi állam a jogsértést nem tudja kimenteni, így óhatatlanul szembe kerülnek egymással az érintett felek.

A „vonakodik vagy képtelen” doktrína alkalmazásával szemben gyakran megfogalmazott kritikát, miszerint az a konfliktusok eszkalációjához vezet, ebben a körben nem tudjuk elfogadni. A lazább teszt által betudott jogsértés jogkövetkezményeként alkalmazott ellenintézkedés és önvédelem gyakorlása ugyanis csak akkor volna jogszerű, ha mindkét magatartás a maga szűkre szabott feltételrendszerei között valósulna meg. Ezért önmagában az a tény, hogy a jogsértés az államnak betudható, nem vezet feltétlenül az egyoldalú erőszak alkalmazása kiterjesztéséhez. Pandora szelencéje tehát a könnyebb betudás ellenére zárva marad.

5.3.2. A „képtelen” alteszt szigorításának előnyei és hátrányai

A „képtelen” alteszt szigorúbb értelmezése szerint önmagában a kibertámadás területi állam területéről történő megindítása még nem feltétlenül eredményezi a támadás betudását is, ugyanis ezen megszorító értelmezés alapján a támadások csak akkor válnának a területi állam cselekedeteivé, ha a területi állam elhúzódóan, konzisztens módon sem képes azok megállítására, illetve nem teszi meg a hatalmában álló lépéseket azok megfékezésére. Ebben a tekintetben ez az értelmezés polgári jogi analógiával – szemben a lazábbra szabott értelmezési lehetőséggel – egyfajta gondossági kötelmet (*obligation of conduct*) telepít a területi államra, amely azáltal kerülheti el a területéről indított kibertámadás betudását, hogy a rendelkezésére álló eszközökkel küzd azok ellen, még akkor is, ha ezen küzdelem végül nem vezet eredményre.

A megközelítés hátránya, hogy betudás hiányában a célállam jogszerűen nem élhet ellenintézkedéssel, sőt, extrém esetben még az önvédelem joga sem nyílik meg, hiába éri el egyébként a nem állami szereplő által elkövetett kibertámadás a fegyveres támadás intenzitását. Előnye ugyanakkor, hogy az államok közötti békés együttműködést facilitáló politikai környezetet teremthet azáltal, hogy a jogsértés betudását – és ezért az érintettek közötti politikai szembenállást – nem teszi automatikussá, hanem éppen ellenkezőleg, kooperációra ösztönzi őket.

5.3.3. A „vonakodik vagy képtelen” teszt *de lege ferenda*-javaslata

A „képtelen” alteszt fenti lazább és szigorúbb értelmezési lehetőségei közül álláspontunk szerint a *lazább értelmezési lehetőség elfogadása tűnik indokoltnak*, a lazább betudási mércével járó előnyök ugyanis lényegesen meghaladják az annak alkalmazásával járó hátrányokat. A lazább alteszt gyors, hatékony, a nemzetközi jog konvencionális keretei közé illeszkedő, ám mégis korlátok közé szorított válaszlépések megtételét teszi lehetővé a célállam számára, megszüntetve ezzel a betudhatóság hiányában kényszerűen válaszlépések nélkül hagyandó, nem állami szereplők által elkövetett kibertámadások anomáliáját.

Minderre tekintettel az alábbi, a kibertámadások betudására alkalmazandó *lex specialis* normaként az alábbi tesztet javasoljuk: „Az állam területéről indított bármely kibertámadást úgy kell tekinteni, mintha azt maga a területi állam indította volna. Kibertámadás az erőszak alkalmazásának tilalmába ütköző kiberművelet.”

A fenti betudási teszt illeszkedik az erőszak tilalma tárgygi hatályához, amely – mint látható volt – a kiberműveletekre is irányadó. Ez a lassan alakuló nemzetközi jogi normatömeg változhat ugyan, ám épp ezen rugalmas fogalmazásmód miatt az erőszak tilalmába ütköző kibertámadások továbbra is betudhatóak

lesznek a területi államnak.¹¹¹ A megfogalmazott teszt így nem módosít az erőszak tilalma hatályán, annak – a kibertérre is kiható – autonóm fejlődését érintetlenül hagyja. A „vonakodik vagy képtelen” doktrína betudhatósági mérceként való alkalmazása a nemzetközi jog jelen állapotában nem gyakori, ugyanakkor az állami gyakorlatban pontszerűen már jelen van,¹¹² a jogtudomány pedig az utóbbi időkben kiemelt figyelmet fordított a téma kutatására.¹¹³ Minderre tekintettel a megfogalmazott *lex specialis* mérce gyakorlati relevanciával is bír. Végezetül továbbra is hangsúlyozzuk, hogy ez a mérce elsődlegesen a területi államokra irányuló incentivát kíván tükrözni, mivel ők vannak a legjobb pozícióban arra, hogy a területekről kiinduló onerózus kiberműveleteknek gátat szabjanak.

6. Összefoglalás

Jelen tanulmány a *jus contra bellum* keretei között vizsgálta a kibertámadások betudhatóságát. Elsőként felvázoltuk a kibertérre alkalmazandó nemzetközi jogi keretrendszert, megállapítottuk, hogy a nemzetközi jog konvencionális szabályai alkalmazandóak rá *lex specialis* nélkül, definiáltuk a „kibertámadás” fogalmát, melyet az erőszaktilalomba ütköző eredményt megvalósító kiberművelettel azonosítottunk. Felvázoltuk a *jus contra bellum* körében legrelevánsabb betudási teszteket, majd ismertettük, hogy a technikai azonosíthatóság által támasztott nehézségek okán

¹¹¹ Ez a megállapítás természetesen mindaddig lehet érvényes csak, amíg nem alakul ki az erőszak tilalmáról szóló rezsimen belül egy *lex specialis* kibertámadás fogalom.

¹¹² KIS K. B.: i. m. 88.; BRUNNÉE – TOOPE: i. m. 282.

¹¹³ Mi sem támasztja alá ezt jobban, hogy a tanulmány által hivatkozott releváns források mindegyike az elmúlt bő egy évtizeden belül született.

miért tartjuk alkalmatlannak ezeket a kibertámadások hatékony betudására. Bemutattuk a „*due diligence*” kötelezettséget, mint egy rugalmasabb betudási mérce potenciális alternatíváját, majd cáfoltuk annak alkalmasságát. Végül javaslatot tettünk egy lehetséges, a kibertámadások betudására vonatkozó *lex specialis* szabályra, melyet a „vonakodik vagy képtelen” doktrínában jelöltünk meg, amely a klasszikus betudási tesztek nehézkes alkalmazhatóságával szemben egyszerűen és evidens módon teszi betudhatóvá a kibertámadásokat a területi államnak, mely betudás azonban nem jár a konfliktusok eszkalációjával, tekintettel az ellenintézkedések és az önvédelemhez való jog gyakorlása során egyaránt érvényesülő szükségesség és arányosság követelményével.

Irodalomjegyzék

Nemzetközi egyezmények

Charter of the United Nations, 26/06/1945, UNTS, Vol. 1, p. XVI.
Convention on Cybercrime, 23/11/2011, CETS, No. 185.

ENSZ-dokumentumok

Articles on the Responsibility of States for Internationally Wrongful Acts, Yearbook of the ILC 2001, Vol. II., Pt. Two, 2007, p. 26.
Commentary to the Articles on the Responsibility of States for Internationally Wrongful Acts, Yearbook of the ILC 2001, Vol. II., Pt. Two, 2007, p. 31.

Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations, UNGA, A/RES/2625(XXV), 1970.

Definition of Aggression, UNGA, A/RES/3314(XXIX), 1974.

Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UNGA, Note by the Secretary-General, A/68/98, 2013.

Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UNGA, Note by the Secretary-General, A/70/174, 2015.

Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, UNGA, Note by the Secretary-General, A/76/135, 2021.

Summary record of the third meeting on State Responsibility, Yearbook of the ILC 1963, Vol. II., 1964, p. 229.

Bírósági ítéletek

Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), Judgment, I.C.J. Reports 2007, p. 43.

Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda), Merits, Judgment, I.C.J. Reports 2005, p. 168.

Corfu Channel (United Kingdom v. Albania), Merits, Judgment, I.C.J. Reports 1949, p. 4.

Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, I.C.J. Reports 2004, p. 136.

Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, I.C.J. Reports 1996, p. 226.

Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgment, I.C.J. Reports 1986, p. 14.

United States Diplomatic and Consular Staff in Tehran (United States of America v. Iran), Judgment, I.C.J. Reports 1980, p. 3.

Nemzeti jogi jogforrások

60/2013. (IX. 30.) HM utasítás a Magyar Honvédség Kibervédelmi Szakmai Konceptiójának kiadásáról.

Monográfiák

Corten, O.: *The Law Against War: The Prohibition on the Use of Force in Contemporary International Law*, London, Hart Publishing, 2010.

Crawford, J.: *State Responsibility: The General Part*. Cambridge: CUP, 2013.

Delerue, F.: *Cyber Operations and International Law*. Cambridge: CUP, 2020.

Hart, H. L. A.: *A jog fogalma*. Budapest: Osiris, 1995.

Kajtár G.: *A nem állami szereplők elleni önvédelem a nemzetközi jogban*. Budapest: ELTE Eötvös, 2015.

Kajtár G.: *Betudás a nemzetközi jogban. A másodlagos normák szerepe a beruházásvédelemtől a humanitárius jogig*. Budapest: ORAC, 2022.

Kis K. B.: *Célzott likvidálás a nemzetközi jogban, különös tekintettel a fegyveres, pilóta nélküli repülőgépek alkalmazására*. Doktori (PhD) értekezés, Pécs: Pécsi Tudományegyetem Állam- és Jogtudományi Doktori Iskola, 2021.

Kovács P.: *Nemzetközi közjog*. Budapest: Osiris, 2016.

Mahmoudi, S.: *Self-Defence and “Unwilling or Unable” States*. Collected Courses of the Hague Academy of International Law, Vol. 422, 2022.

Roscini, M.: *Cyber Operations and the Use of Force in International Law*. Oxford: OUP, 2014.

Ruys, T.: *'Armed Attack' and Article 51 of the UN Charter: Evolutions in Customary Law and Practice*. Cambridge: CUP, 2010.

Szerkesztett kötetek

Condorelli, L. – Kreß, C.: The Rules of Attribution: General Considerations. In James Crawford – Alain Pellet – Simon Olleson – Kate Parlett (eds.): *The Law of International Responsibility*. Oxford: OUP, 2010.

Crawford, J. – Olleson, S.: The Character and Forms of International Responsibility. In Malcolm D. Evans (ed.): *International Law*. Oxford: OUP, 2014.

David, E.: Primary and Secondary Rules. In James Crawford – Alain Pellet – Simon Olleson – Kate Parlett (eds.): *The Law of International Responsibility*. Oxford: OUP, 2010.

Dörr, O. – Randelzhofer, A.: Article 2(4). In Bruno Simma – Daniel-Erasmus Khan – Georg Nolte – Andreas Paulus – Nikolai Wessendorf (eds.): *The Charter of the United Nations: A Commentary, Volume I*. Oxford: OUP, 2012.

Geiß, R. – Lahmann, H.: Freedom and Security in Cyberspace: Shifting the Focus away from Military Responses towards Non-Forcible Countermeasures and Collective Threat-Prevention. In Katharina Ziolkowski (ed.): *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy*. Tallinn: NATO CCD COE Publications, 2013.

Kammerhofer, J.: The Resilience of the Restrictive Rules on Self-Defence. In Marc Weller (ed.): *The Oxford Handbook of the Use of Force in International Law*. Oxford: OUP, 2015.

Nolte, G. – Randelzhofer, A.: Article 51. In: Bruno Simma – Daniel-Erasmus Khan – Georg Nolte – Andreas Paulus – Nikolai Wessendorf (eds.): *The Charter of the United Nations: A Commentary, Volume II*. Oxford: OUP, 2012.

- Pirker, B.: Territorial Sovereignty and Integrity and the Challenges of Cyberspace. In Katharina Ziolkowski (ed.): *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy*. Tallinn: NATO CCD COE Publications, 2013.
- Schmitt, M. N.: ‘Attack’ as a Term of Art in International Law: The Cyber Operations Context. In Christian Czosseck – Rain Ottis – Katharina Ziolkowski (eds.): *4th International Conference on Cyber Conflict. Proceedings 2012*. Tallinn: NATO CCD COE, 2012.
- Schmitt, M. N. – Vihul, L. (eds.): *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: CUP, 2017.
- Ziolkowski, K.: *Ius ad bellum* in Cyberspace – Some Thoughts on the “Schmitt-Criteria” for Use of Force. In Christian Czosseck – Rain Ottis – Katharina Ziolkowski (eds.): *4th International Conference on Cyber Conflict. Proceedings 2012*. Tallinn: NATO CCD COE, 2012, 295–309.

Tanulmányok

- Bethlehem, D.: Self-Defense Against an Imminent or Actual Armed Attack by Nonstate Actors. *AJIL*, 2012/4., 770–777.
- Brownlie, I.: International Law and the Activities of Armed Bands. *ICLQ*, 1958/4., 712–735.
- Brunnée, J. – Toope, S. J.: Self-Defence against Non-State Actors: Are Powerful States Willing but Unable to Change International Law?. *ICLQ*, 2017/2., 263–286.
- Chricop, L.: A Due Diligence Standard of Attribution in Cyberspace. *ICLQ*, 2018/3., 643–668.
- Clark, D. D. – Landau, S.: Untangling Attribution. *Harvard National Security Journal*, 2011/2., 323–352.

- Corten, O.: The 'Unwilling or Unable' Test: Has it Been, and Could it be, Accepted?. *LJIL*, 2016/3., 777–799.
- Corten, O. – Dubuisson, F.: L'opération «liberte immuable»: une extension abusive du concept de legitime defense. *Revue Générale de Droit International Public*, 2002/1., 51–77.
- de Wet, E.: The Invocation of the Right to Self-Defence in Response to Armed Attacks Conducted by Armed Groups: Implications for Attribution. *LJIL*, 2019/1., 91–110.
- Deeks, A. S.: "Unwilling or Unable": Toward a Normative Framework for Extraterritorial Self-Defense. *Virginia JIL*, 2012/3., 483–550.
- Kajtár G.: Erőszak, agresszió, fegyveres támadás - A *ius contra bellum* klasszikus normáinak kialakulása, tartalma és egymáshoz való viszonya. *Acta Facultatis Politico-iuridicae Universitatis Scientiarum Budapestinensis de Rolando Eötvös nominatae*, 2015, 105–143.
- Kajtár G.: Vonakodik vagy nem képes? Az önvédelem jogának újabb paradigmaváltó kísérlete. *Közzogi Szemle*, 2018/1., 1–10.
- Kavaliuskas, A.: Can the Concept of Due Diligence Contribute to Solving the Problem of Attribution with Respect to Cyber-Attacks Conducted by Non-State Actors Which Are Used as Proxies by States?. *Teisės Apžvalga Law Review*, 2022/2., 4–30.
- Kees, A.: Responsibility of States for Private Actors. *MPEPIL*, 2011.
- Kiss M.: A kiberműveletek és a jus ad bellum kapcsolata. *Közzogi Szemle*, 2022/3., 100–107.
- Kraszewski, K.: Classification of Cyber Operations under International Law. *Finnish Yearbook of International Law*, 2015, 141–174.
- Kunz, J. L.: Individual and Collective Self-Defense in Article 51 of the Charter of the United Nations. *AJIL*, 1947/4., 872–879.
- Milanović, M.: State Responsibility for Genocide. *EJIL*, 2006/3., 553–604.

- Palchetti, P.: De Facto Organs of a State. *MPEPIL*, 2017.
- Ruys, T.: The Meaning of “Force” and the Boundaries of the Jus Ad Bellum: Are “Minimal” Uses of Force Excluded from UN Charter Article 2(4)? *AJIL*, 2014/2., 159–210.
- Schnader, J. A.: Mal-Who? Mal-What? Mal-Where? The Future Cyber-Threat of a Non-Fiction Neuromancer: Legally Un-Attributable, Cyberspace-Bound, Decentralized Autonomous Entities. *North Carolina Journal of Law & Technology*, 2019/2., 1–40.
- van Steenberghe, R.: Self-Defence in Response to Attacks by Non-state Actors in the Light of Recent State Practice: A Step Forward?. *LJIL*, 2017/1., 183–208.
- Tran, D.: The Law of Attribution: Rules for Attributing the Source of a Cyber-Attack. *YALE Journal of Law & Technology*, 2018, 376–441.
- Tsagourias, N.: Cyber Attacks, Self-Defence and the Problem of Attribution. *JCSL*, 2012/2., 229–244.

Internetes források

- Cartwright, J. E.: *Memorandum for Chiefs of the Military Services, Commanders of the Combatant Commands, Directors of the Joint Staff Directories on Joint Terminology for Cyberspace Operations*. Department of Defense, 2011. (elérhető: <https://info.publicintelligence.net/DoD-JointCyberTerms.pdf>)
- G7 Declaration on Responsible States Behavior in Cyberspace. 2017. (elérhető: <https://ccdcoe.org/uploads/2018/11/G7-170411-LuccaDeclaration-1.pdf>)
- The International Institute for Strategic Studies: *Cyber Capabilities and National Power: A Net Assessment*. IISS Research Papers, 2021. (elérhető: <https://www.iiss.org/research-paper//2021/06/cyber-capabilities-national-power>)