Katonai Jogi és Hadijogi Szemle

A Magyar Katonai Jogi és Hadijogi Társaság Tudományos Folyóirata

11. évfolyam (2023) 3–4. szám

11. évfolyam (2023.) 3–4. szám

Főszerkesztő
Dr. habil. Hautzinger Zoltán PhD. r. ezredes

Társszerkesztők
Dr. Csiha Gábor ezredes
Dr. Farkas Ádám PhD. őrnagy
Dr. Kelemen Roland PhD.

Felelős kiadó
Magyar Katonai Jogi és Hadijogi Társaság
1055 Budapest, Markó u. 27.

A kiadó képviselője
Dr. Kádár Pál PhD. dandártábornok

Megjelenik
Elektronikusan 3 havonta
és évközi különszámokkal

Közzététel helye
www.hadijog.hu

ISSN
2064-4558

A borítót tervezte:
Dr. Czebe András (czprod.co@gmail.com)

Tartalom

Szerkesztői előszó

Tisztelt Olvasóink!

A Katonai Jogi és Hadijogi Szemle jelen száma egy olyan duplaszám, amely egyfelől a Magyar Katonai Jogi és Hadijogi Társaság tudományos pályázatának díjazott munkáit tartalmazza, másfelől pedig a modern technológiákkal kapcsolatos biztonság jogi oldalának vizsgálatát előtérbe helyező tanulmányok foglalata.

2023. több szempontból is jelentős év volt, amelyet a Társaság pályázati kiírása is tükrözött: tisztelgett a Magyar Honvédség fennállásának 175. jubileuma, valamint a rendszerváltozást követő honvédelmi törvények három évtizede előtt. A pályázatban felkínált témacsoportok közül a két díjazott pályamű az erőszakos kiberműveletek nemzetközi hadijog betudhatósága, illetve a különleges jogrendi jogkorlátozások joggyakorlat szempontjából is aktuális kérdéseit érintették, a Nemzeti Közszolgálati Egyetem, valamint az Eötvös Lóránt Tudományegyetem jelenlegi és frissen végzett hallgatóinak gondolatait megjelenítve.

Jelen lapszám tanulmányainak második köre arra reagál, hogy napjaink nemzetbiztonsági kihívásainak java részét, a társadalmi reziliencia jelentős hányadát, a geopolitikai folyamatok releváns részét a modern technológiával kapcsolatos biztonsági folyamatok és azok szabályozása jelenti. Így e lapszámban megjelenik a világűrjog, a kibertéri cselekmények betudhatósága, az információs műveletek metodikája, valamint az Európai Unió kiberbiztonsági szabályozása is. Ezeknek a témáknak mindegyike kiemelkedő jelentőséggel bír napjaink,

illetve az elkövetkező évtizedek biztonságszavatolásának a területén.

A Tisztelt Olvasónak szerkesztőségünk ez úton kíván a 2023. évi 3-4. lapszámhoz hasznos időtöltést!

A szerkesztők

TANULMÁNYOK

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 művelet[1] 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] *rezsim 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 betudáskoncepcióit és rávilágítunk arra, hogy a kibertámadások sajátosságai miért teszik rendkívül nehézzé ezen betudáskoncepciók eredményes alkalmazását. Az 5. fejezetben ismertetjük a vonakodik vagy képtelen doktrínát, és kifejtjük, miért tekintjük*

2 Jelen tanulmány szinonimaként értelmezi a nemzetközi jog erőszakalkalmazási rezsimjét 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 értelmezendőek 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 alapműnek tekintett Tallini Kézikönyv,[5] illetve a másodlagos szakirodalom[6] egyaránt azon az álláspontón 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 alkalmazhatóak ezen új fegyvertípusok alkalmazásnak vonatkozásában.[7] Ez tehát azt jelenti, hogy az Egyesült Nemzetek Alapokmányában (a továbbiakban: Alapokmány) megfogalmazott átfogó erőszaktilalom[8] 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://ccdcoe.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 éllel 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. Randelzhofer: 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. Randelzhofer: 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 cselekménnyel[20] 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 agresszió[21] (*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 – Randelzhofer: 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 Scienctiarum 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 bekövetkezett[23] 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 – Randelzhofer: 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 tágan 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 bekövetkezte 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 Honvédség[36] dokumentumai. Konszenzusos 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 megfeledkezve arról, hogy – a 2. cikk (4) bekezdés céljának megfelelően – az erőszak átfogó és teljes tilalmára tekintettel ez a „mennyiségi 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 különbségtételt 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 szervezettségi 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 terénumába 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 értelemzendő 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 kiberműveletet 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 betudáskoncepciók 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 tervezet[52] (*Articles on the Responsibility of States for Internationally Wrongful Acts*, ARSIWA) bár sosem vált nemzetközi egyezménnyé, 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 feltételrendszer[54] 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 legevidensebb módja. Ebben a rendelkezésben az állami szervre (*State organ*) történő utalást a lehető legáltalánosabban kell értelmezni, az államszervezeten 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 többízben 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 Népirtás-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 részcselekmény 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 részcselekmény, 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. cikkekhez 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: egyrészről az „és" szó jelzi, hogy a két feltétel kumulatív, vagyis az elismerésre és az elfogadásra egyaránt szükség van a betudáshoz. Másrészről 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] Harmadrészről 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 szokásjogi[74] *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 agressziónak 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 közismert, 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 – Randelzhofer: i. m. 213, 29. bek.

76 Alapokmány, i. m. 3. cikk; 4. cikk (1) bekezdés. Ugyanakkor a szakirodalom szerint az ún. *de facto* rezsimeket (pl. Tajvan) is egyaránt kötelezi a 2. cikk (4) bekezdés. Ld. Dörr – Randelzhofer: 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 előbbiekben 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'operation «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 kötelezettségszegő 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] terrorszervezetek megtűrésének és támogatásának tilalma[89]) 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 betudáskoncepciók elégtelen mivolta 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 eltúlzott,[91] a kommentátorok többsége azon az álláspontonvan, 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 nevezett[93] – 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 felléphessen, 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 kitágításával, a területi állam szuverenitásának elfogadhatatlan mértékű korlátozásáról nem is beszélve.

Álláspontunk szerint azonban két fontos jogpolitikai megfontolás is amellett 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 – Randelzhofer: 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*-rezsim 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 vizsgálandó 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 szólnunk 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. Kavaliauskas: 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"* kötelezettség[106] 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?, *Teisės 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 megszűntetését 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 ellenintézkedéskehez[110] és az önvédelem jogának gyakorlásához fűzött szükségességi-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.

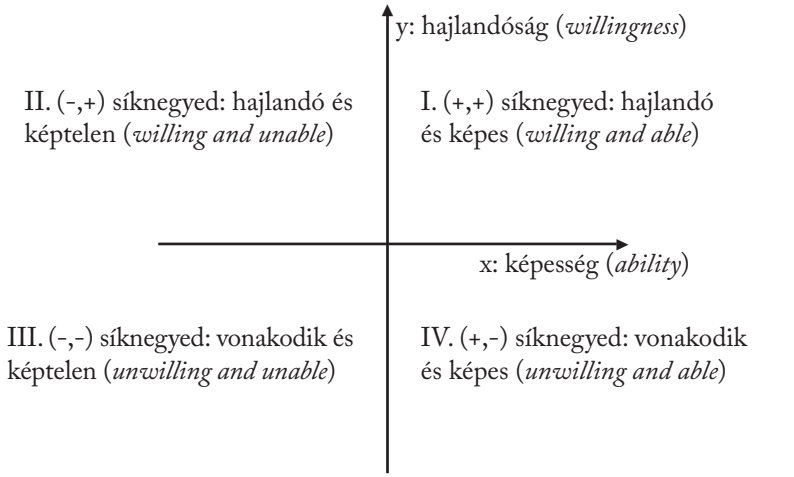
A „vonakodik vagy képtelen" teszt kapcsán két szempont vizsgálandó: (1) vonakodik avagy hajlandó-e a területi állam fellépni a területéről indított kibertámadások megakadályozása érdekében, illetve (2) technikai, gazdasági, politikai és katonai kapacitásai objektíve lehetségessé teszik-e az állam számára 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 kísérlő (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 tárgyi 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 kihatható – 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 incentívát 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 Koncepciójának 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'operation «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 Scienctiarum Budapestinensis de Rolando Eötvös nominatae*, 2015, 105–143.

Kajtár G.: Vonakodik vagy nem képes? Az önvédelem jogának újabb paradigmaváltó kísérlete. *Közjogi Szemle*, 2018/1., 1–10.

Kavaliauskas, 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. *Közjogi 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)

Lukács Bence

Dezinformációs támadások társadalmi hatásai, lehetséges ellenintézkedések azonosítása

Bevezetés

A digitális kommunikációs platformok elterjedése az információs hadviselés egy típusának, a dezinformációs támadásoknak a reneszánszát hozta, amelyek jelentős fenyegetést jelentenek az egyénekre, szervezetekre és társadalom egészére. A jelen szakirodalmi összefoglaló célja, hogy átfogó áttekintést nyújtson a dezinformációs támadásokról, feltárva a különböző támadástípusokat, az alkalmazott taktikákat és a javasolt ellenintézkedéseket. A meglévő kutatások szintetizálásával ez a dokumentum hozzájárul a dezinformáció fejlődésének megértéséhez, és betekintést nyújt káros hatásainak mérséklésébe.

Az információs korszak beköszöntével soha nem látott mértékű összekapcsolódás jött létre, de a rosszindulatú szereplők számára is új lehetőségeket teremtett az információterjesztés sebezhetőségének kihasználására. A dezinformáció, amelyet a hamis vagy félrevezető információk szándékos terjesztése jellemez, erőteljes eszközzé vált azok kezében, akik a közvélemény manipulálására, a politikai eredmények befolyásolására és az intézményekbe vetett bizalom aláásására törekszenek. Emellett a dezinformáció definíciójának kiterjesztése a történelmi, hatalmi és politikai dimenziókra is, rávilágít a hatalmi hierarchiák megerősítésére szolgáló elsődleges médiastratégiaként való használatára, hangsúlyozva a kritikai dezinformációs tanulmányok

fontosságát a dezinformáció hatásának megértésében és az ellene való küzdelemben.[1]

A dezinformáció a félretájékoztatás és az álhírek előfordulása jelentősen megnőtt az elmúlt években, amely szignifikáns hatást gyakorol a társadalmakra.[2] A dezinformáció az egyének szándékos megtévesztésére előállított hamis vagy a valóságtól eltérő környezetbe ágyazott információ, míg a félretájékoztatás hamis és/vagy félrevezető információként definiálható.[3] A dezinformáció lehet kiberművelet (hackelés) vagy nyílt tevékenység (hamis információ terjesztése).[4] Az álhíreknek több definíciója létezik, általánosságban elmondható, hogy az interneten hírformátumban megjelenő hamis történetek, melyek célja a szándékos félrevezetés és/vagy egyéb haszonszerzés tekinthetők álhíreknek.

1. Dezinformációs támadások jellemzői

1.1 Támadástípusok

A dezinformációs támadások kifejezés számos olyan szándékos manipulatív taktikát foglal magában, amelyek célja az egyének és rendszerek megtévesztése és félrevezetése.[5] A dezinformációt

1 Rachel Kuo – Alice Marwick: Critical disinformation studies: History, power, and politics, *Harvard Kennedy School Misinformation Review*, 2021. 2.4: 1–11.

2 Pythagoras N. Petratos – Alessio Faccia: Fake news, misinformation, disinformation and supply chain risks and disruptions: risk management and resilience using blockchain, *Annals of Operations Research*, 2023. 1–28.

3 Hunt Allcott – Matthew Gentzkow: Social media and fake news in the 2016 election, *Journal of economic perspectives*, 2017. 31.2: 211–236.

4 Pythagoras N. Petratos: Misinformation, disinformation, and fake news: Cyber risks to business, *Business Horizons*, 2021. 64.6: 763–774.

5 Mahmoud Abbasi, et al.: Security in the Internet of Things Application Layer: Requirements, Threats, and Solutions, *IEEE Access*, 2022. 10: 97197–97216.

többek között hibrid eszközként használják a demokratikus államok érdekei és polgáraik biztonsága elleni támadásra.[6] Jellemzője a célzott megtévesztés, amely gyakran magában foglalja az információk gyártását vagy manipulálását konkrét politikai célok elérése érdekében.[7] Emellett a dezinformációs támadásokról ismert, hogy a közösségi médiaplatformokat használják fel, ami egyre nagyobb igényt támaszt az olyan mesterséges intelligenciaeszközök iránt, amelyek képesek az ilyen támadások korai szakaszában történő azonosítására és az azokra való reagálásra.[8]

1.2 Taktikák

A támadók a dezinformációs kampányokban különböző taktikákat alkalmaznak céljaik eléréséhez. E taktikák közé tartozik a hamis vagy félrevezető információk terjesztése, a közvélemény manipulálására szolgáló számítógépes propaganda alkalmazása, valamint a társadalmon belüli viszály és polarizáció megteremtése.[9] A dezinformációs támadások magukban foglalhatják az

6 Dávid Kollár, et al.: Dezinformácie ako kľúčová bezpečnostná výzva súčasnosti v kontexte rusko-ukrajinského konfliktu, *Politické vedy*, 2022. 25.3: 87–109.

7 Michael Hameleers, et al.: Mistake or manipulation? Conceptualizing perceived mis-and disinformation among news consumers in 10 European countries, *Communication Research*, 2022. 49.7: 919–941.

8 Barry Cartwright, et al.: Detecting and responding to hostile disinformation activities on social media using machine learning and deep neural networks, *Neural Computing and Applications*, 2022. 34.18: 15141–15163.

9 Joao VS Ozawa, et al.: How Disinformation on WhatsApp Went From Campaign Weapon to Governmental Propaganda in Brazil, *Social Media+ Society*, 2023. 9.1: 20563051231160632.

álhírek terjesztését és a közösségi média használatát is a megtévesztő narratívák felerősítésére, amelyek gyakran konkrét közösségeket céloznak meg vagy politikai zavargásokat szítanak.[10] Egy a Twitter-en végzett felmérés alapján az álhírek jobban és gyorsabban terjednek, mint a valós hírek, az álhírek retweetelése (újramegosztása) akár 70%-kal valószínűbb, mint a valós híreknél.[11]

A személyre szabható internetes szolgáltatások (pl. közösségi médiák) szűrői korlátozhatják az új tartalmak megjelenését, így a fogyasztó figyelmen kívül hagyja (személyes szándékán kívűl is) az eltérő nézőpontokat, ami a saját előítéleteit növelheti.[12] Figyelembe véve, hogy az emberek az identitásukat, ideológiájukat részesítik előnyben, mint az attól eltérő véleményeket, ez a jelenség veszélyesnek tekinthető.[13] A közösségi média személyre szabott tartalmai a felhasználók meggyőződéseinek megerősítésében nagy szerepet játszanak, a szűrőbuborékok (filter-bubbles) és a visszhangkamrák (echo chambers) jelenségek révén. A szűrőbuborékok lényegében, olyan algoritmusok, amelyek a felhasználó által kedvelt tartalmakhoz hasonló tartalmakkal próbálják fenntartani a felhasználó figyelmét. A visszhangkamrák jelensége a felhasználók által kiválasztott személyek, csoportok, tartalmak követése által jön létre, tehát a kiválasztott tartalmakkal ellen-

10 Michael Hameleers: The (un) intended consequences of emphasizing the threats of mis-and disinformation, *Media and Communication*, 2023. 11.2: 5–14.

11 Soroush Vosoughi – Deb Roy – Sinan Aral: The spread of true and false news online, *Science*, 2018. 359.6380: 1146–1151.

12 Jonathan Clarke, et al.: Fake news, investor attention, and market reaction, *Information Systems Research*, 2020. 32.1: 35–52.

13 Cameron Martel – Gordon Pennycook – David G. Rand: Reliance on emotion promotes belief in fake news, *Cognitive research: principles and implications*, 2020. 5: 1–20.

tétes tartalmak megjelenése erősen korlátozott, amely elősegíti a saját vélemény folytonos megerősítését.[14]

A támadók továbbá olyan taktikákat alkalmazhatnak, mint a hamisítás és a megtévesztő kommunikációs technikák használata a célpontok megtévesztése és manipulálása érdekében.[15]

Ezek a kampányok gyakran a dezinformáció szándékos és stratégiai felhasználását jelentik politikai, társadalmi vagy ideológiai célok elérése érdekében, mind belföldön, mind nemzetközi szinten.[16] A támadók emellett kifinomult technikákat alkalmazhatnak, beleértve a számítási módszerek és a mesterséges intelligencia használatát a dezinformáció hatásának maximalizálása és a közvélemény manipulálása érdekében. E taktikák ellen különösen nagy kihívás, mivel gyakran kihasználják a közösségi média és a digitális kommunikációs platformok összekapcsolt jellegét, hogy széles közönséget érjenek el és befolyásoljanak.[17] A dezinformációs támadások taktikáinak megértése kulcsfontosságú a dezinformáció hatásának mérséklésére és a káros hatások elleni védelemre irányuló hatékony stratégiák kidolgozásához.

14 Samuel C. Rhodes: Filter bubbles, echo chambers, and fake news: how social media conditions individuals to be less critical of political misinformation, *Political Communication*, 2022. 39.1: 1–22.

15 Martin Innes – Diyana Dobreva – Helen Innes: Disinformation and digital influencing after terrorism: Spoofing, truthing and social proofing, *Contemporary Social Science*, 2021. 16.2: 241–255.

16 Martin Innes, et al.: The normalisation and domestication of digital disinformation: On the alignment and consequences of far-right and Russian state (dis) information operations and campaigns in Europe, *Journal of Cyber Policy*, 2021. 6.1: 31–49.

17 Aaron Erlich, et al.: Does analytic thinking insulate against pro-Kremlin disinformation? Evidence from Ukraine, *Political Psychology*, 2023. 44.1: 79–94.

1.3 Ellenintézkedések

A dezinformációs támadások megelőzésére és kezelésére számos stratégia és megközelítés létezik. Ilyen a tényellenőrző (fact-checking) újságírás a hamis információk terjesztése elleni kulcsfontosságú enyhítő eszköz. A tényellenőrzők releváns újságírói együttműködéseket és stratégiákat hoztak létre a dezinformáció elleni küzdelem érdekében.[18] A főbb ellenintézkedések közé tartoznak továbbá a számítási módszerek és a mesterséges intelligencia alkalmazások a közösségi médiaplatformokon megjelenő dezinformáció felderítésére és mérséklésére.[19]

A dezinformációs támadások elleni hatékony fellépéshez elengedhetetlen a különböző érdekelt felek bevonásával megvalósított sokoldalú stratégia. Mindenekelőtt a médián belüli műveltség és az oktatási kezdeményezések előmozdítása kulcsfontosságú, hogy az egyének képessé váljanak az információforrások kritikus értékelésére, az állítások tényellenőrzésére és az elfogult tartalmak kiszűrésére. Emellett a jó hírű tényellenőrző szervezetek támogatása elengedhetetlen az információk ellenőrzéséhez és a hamis állítások leleplezéséhez. Kulcsfontosságú az online platformok átláthatóságának és elszámoltathatóságának szorgalmazása, beleértve az algoritmusokra, a tartalom moderálására vonatkozó irányelvekre és a politikai hirdetésekre vonatkozó információk közzétételét. Állami oldalról továbbá a kormányok szerepet játszhatnak a hamis információkat szándékosan terjesztőkre vonatkozó jogi következményekkel járó szabályozások

18 Luisa Martínez-García – Iliana Ferrer: Fact-Checking Journalism: A Palliative Against the COVID-19 Infodemic in Ibero-America, *Journalism & Mass Communication Quarterly*, 2023. 100.2: 264–285.

19 Noémi Bontridder – Yves Poullet: The role of artificial intelligence in disinformation, *Data & Policy*, 2021. 3: e32.

meghozatalával és betartatásával. Nemzeti és nemzetközi szinten egyaránt szükség van az együttműködésre az információk, erőforrások és a dezinformáció elleni küzdelem legjobb gyakorlatainak megosztása érdekében. A közösségi médiaplatformoknak szigorú irányelveket kell érvényesíteniük, beleértve a tényellenőrzési mechanizmusokat és a tartalom moderálását, míg az algoritmikus megoldások felhasználhatók a dezinformáció terjedésének felderítésére és korlátozására. További intézkedéseket jelenthet a polgárok ösztönzése a gyanús tartalmak aktív bejelentésére, a sokszínű médiatér előmozdítása és a dezinformációs kampányok elleni válságkommunikációs tervek kidolgozása. A közvéleményt tudatosító kampányok, a digitális infrastruktúra védelmét szolgáló kiberbiztonsági intézkedések, valamint a felelős újságírói gyakorlatok – beleértve a pontos tudósításokat és az etikai normákat – előmozdítása szerves részét képezik ennek az átfogó stratégiának. Ezek az ellenintézkedések együttesen az információs ökoszisztéma megerősítését és a hamis narratívák társadalomra gyakorolt hatásának mérséklését célozzák.[20]

A nemcsak oktatási tevékenységgel való védekezés rávilágít annak fontosságára, hogy a digitális korban a dezinformáció jelentette kihívások kezelése érdekében ki kell használni a technológiai fejlődést. Az információbiztonsággal összefüggésben a hatékony sebezhetőség-ellenőrzés és a funkcióellenőrzés ellenintézkedései, például a javítás és a vírusvédelem, kritikus szerepet játszanak a támadások előrehaladásának korai szakaszban történő megállításában. Ezen túlmenően a támadások összetettségének növelése és a titkosítási algoritmusok elleni hibatámadások megelőzése érdekében olyan hibavédelmi technikák alkalmazása javasolt, mint a hamis körök és a konzisztenciaellenőrzéssel

20 Xichen Zhang – Ali A. Ghorbani: An overview of online fake news: Characterization, detection, and discussion, *Information Processing & Management*, 2020. 57.2: 102025.

ellátott redundáns számítások alkalmazása. A kriptográfia területén az állandó idejű titkosítás javasolt a távoli gyorsítótár időzítési támadások ellenintézkedéseként, ami jól mutatja a különböző kibertámadásokkal szemben ellenálló kriptográfiai technikák kifejlesztésének fontosságát. Emellett a robusztus kiberfizikai rendszerek alkalmazása és az irányítórendszerek elleni támadások meghiúsításához szükséges feltételek megfogalmazása aláhúzza a proaktív védelmi mechanizmusok jelentőségét a kritikus infrastruktúra dezinformációs alapú fenyegetésekkel szembeni védelmében.[21]

1.4 Hatások

A közösségi médián és online platformokon keresztül terjesztett dezinformáció bizonyítottan befolyásolja a közvélemény megítélését és meggyőződését, ami potenciálisan olyan valós következményekhez vezethet, mint a belföldi terrorizmus.[22] A félretájékoztatás és dezinformáció hatásainak ellensúlyozására stratégiai kommunikációs beavatkozások javasoltak, amelyek enyhítik az ilyen események által kiváltott szélesebb körű közkárokat. Továbbá a dezinformáció szándékos terjesztése bizonyítottan valós következményekkel jár az emberek hiedelmeire és viselkedésére nézve, amint azt COVID-19 járvány kitörése is bizonyította.[23] A politikai elitek által használt álhír-diskurzusoknak való kitettség csökkentheti az emberek valós információkba

21 Saeed Jamalzadeh, et al.: Weaponized disinformation spread and its impact on multi-commodity critical infrastructure networks, *Reliability Engineering & System Safety*, 2023. 109819.

22 James A. Piazza: Fake news: The effects of social media disinformation on domestic terrorism, *Dynamics of Asymmetric Conflict*, 2022. 15.1: 55–77.

23 Alyt Damstra, et al.: What does fake look like? A review of the literature on intentional deception in the news and on social media, *Journalism Studies*, 2021. 22.14: 1947–1963.

vetett bizalmát, és károsíthatja a dezinformációval szembeni ellenálló képességüket. A dezinformáció és propaganda terjesztése aláásható a nemzetközi biztonságot és a nemzeti érdekeket.[24] A propaganda eszközei a közvélemény befolyásolása, meggyőzése, olyan információkkal, amelyek objektívnek tűnnek viszont torzítanak a preferált oldal irányában.[25] Elengedhetetlen a dezinformáció elleni küzdelem és a nemzetbiztonság védelme hatékony információs politikák végrehajtásával és a dezinformáció elleni küzdelemmel szabályozási szinten. Például a kanadai kormány elismerte a külföldi dezinformáció fenyegetését, és intézkedéseket hozott annak érdekében, hogy ezt biztonsági aggályként kezelje.[26]

A digitális dezinformáció, azaz álhírek terjedése az egyik legjelentősebb fenyegetésnek számít az interneten, amely nagymértékben okoz egyéni és társadalmi károkat. Emellett a dezinformációs kampányokat a demokrácia elleni támadásokkal összefüggésben is elemezték, a kommunikáció pedig központi szerepet játszik az ilyen támadások megvalósulásában és azok következményeiben.[27]

A dezinformáció a kiberfenyegetés lencséjén keresztül elemezhető, kiemelve a kiberfenyegetésként való besorolást, amely olyan megkülönböztetett elemekkel rendelkezik, mint a fenyegető ágensek, támadási vektorok, célpontok, hatások és védelmi me-

24 Edward Deverell – Charlotte Wagnsson – Eva-Karin Olsson: Destruct, direct and suppress: Sputnik narratives on the Nordic countries, *The Journal of International Communication*, 2021. 27.1: 15–37.

25 Edson C. Tandoc Jr. – Zheng Wei Lim – Richard Ling: Defining "fake news" A typology of scholarly definitions, *Digital journalism*, 2018. 6.2: 137–153.

26 Nicole J. Jackson: The Canadian government's response to foreign disinformation: Rhetoric, stated policy intentions, and practices, *International Journal*, 2021. 76.4: 544–563.

27 Spencer McKay – Chris Tenove: Disinformation as a threat to deliberative democracy, *Political Research Quarterly*, 2021. 74.3: 703–717.

chanizmusok.[28] Elmondható, hogy a dezinformációt hivatalos és tényleges kiberfenyegetésként kellene felvenni a kiberbiztonsági szabványokba, mivel hasonló jellemzőkkel rendelkezik, mint a már létező fenyegetések.

1.5 Hibrid-hadviselés

A kibertámadásokban a dezinformáció veszélye jelentős aggodalomra ad okot a kiberbiztonság területén. A hibrid hadviselés, amely katonai és nem katonai akciókat kombinál, dezinformációt, kibertámadásokat és más nem katonai eszközöket használ fel a káosz és az instabilitás megteremtésére.[29] A fekete-tengeri régió nagyszabású kibertámadások és folyamatos dezinformációs kampányok célpontja volt, ami e tevékenységek széles körű hatását jelzi. Emellett a kibertér a kereskedelmi forgalomban kapható technológiákkal való lehetséges visszaélés a terrorista csoportok részéről, valamint az online közösségi médián keresztül zajló, ismétlődő politikai dezinformációs kampányok miatt az egyéni és a kollektív biztonság szempontjából is kritikussá vált. Az államilag támogatott „piszkos játékosok" (bad actors) egyre inkább a közösségi médiaplatformokat használják kibertámadások és dezinformációs kampányok indítására a választások idején. Továbbá bizonyíték van arra, hogy ellenséges és rosszindulatú szereplők hibrid háborús intézkedésekkel, többek között kibernetikai

28 Kevin Matthe Caramancion, et al. The missing case of disinformation from the cybersecurity risk continuum: A comparative assessment of disinformation with other cyber threats, *Data*, 2022. 7.4: 49.

29 Khorram-Amir Manesh – Krzysztof Goniewicz – Frederick M. Burkle: Social and healthcare impacts of the Russian-led hybrid war in Ukraine – a conflict with unique global consequences, *Disaster medicine and public health preparedness*, 2023. 17: e432.

behatolásokkal és dezinformációval manipulálják és kihasználják a sebezhető régiókat.[30]

Az információs hadviselés olyan stratégiai megközelítés, amelyet az információk manipulálására és befolyásolására használnak politikai, katonai vagy ideológiai célok elérése érdekében. Szorosan összefonódik az állambiztonsággal. Az államközpontú online propaganda az információs hadviselés jelentős eleme. A politikusok és az állambiztonsági erők dezinformációt és propagandát alkalmazhatnak a közvélemény formálására, erőszakra vagy az ellenzék elnyomására buzdítanak.[31] A dezinformáció elterjedése és a közösségi média platformok használata a nemzetbiztonsági rendszerek fő aggályai közé kerültek. A szélsőséges csoportok propaganda terjesztésével befolyásoljak a közvéleményt, amely hatalmas veszélyt jelent a nemzetbiztonságra.[32] A kiberbiztonság dinamikájának szintetizálása kulcsfontosságú a globális kiberbiztonsági környezet, valamint a kibertámadások és a védekezés közötti kölcsönhatások megértéséhez.[33] Emiatt a védelmi kutatások elengedhetetlenek az AI/ML modellek ellenséges támadásokkal szembeni ellenálló képességének elemzéséhez a kiberbiztonság területén.

A dezinformációnak a hibrid hadviselés eszközeként való felhasználása nem korlátozódik a katonai műveletekre, hanem

30 Flemming Splidsboel Hansen: *Russian hybrid warfare: A study of disinformation*, DIIS Report, 2017.

31 Hannah Smidt: Mitigating election violence locally: UN peacekeepers' election-education campaigns in Côte d'Ivoire, *Journal of peace research*, 2020. 57.1: 199–216.

32 Soufia Kausar – Bilal Tahir – Muhammad Amir Mehmood: ProSOUL: a framework to identify propaganda from online Urdu content, *IEEE access*, 2020. 8: 186039–186054.

33 Ren Zheng – Wenlian Lu – Shouhuai Xu: Preventive and reactive cyber defense dynamics is globally stable, *IEEE Transactions on Network Science and Engineering*, 2017. 5.2: 156–170.

kiterjed a politikai és társadalmi szférára is, pénzügyi és politikai haszonszerzés, valamint kísérleti manipuláció céljából.[34] Az ellenséges külföldi szereplők hibrid módszereket, köztük dezinformációs kampányokat használnak fel a nyugati országok ellen, felfedve felkészületlenségüket és sebezhetőségüket ezekkel a fenyegetésekkel szemben.[35] A hibrid fenyegetésekben a nemzetközi határok elmosódása és a kibertechnológia használata a dezinformációt életképes eszközzé teszi, ami hozzájárul a betudhatóság kétértelműségéhez és a rosszindulatú akciók lehetőségéhez.[36]

A dezinformációs támadások hibrid hadviselési aspektusai a taktikák széles spektrumát foglalják magukban, beleértve a kiber- és információs hadviselést, a civil intézmények célba vételét és a kétértelműség kihasználását a stratégiai célok elérése érdekében. Ezek a taktikák túlmutatnak a hagyományos katonai műveleteken, és képesek jelentősen befolyásolni a közvéleményt, a társadalmi stabilitást és a nemzetközi kapcsolatokat.

Összefoglalás

A dezinformációs támadások komoly fenyegetést jelentenek, és az álhírek terjedése káros társadalmi hatásokkal jár. A támadások közé tartoznak a hamis információk terjesztése és a közvélemény manipulálása, különösen a közösségi médiaplatformokon keresztül. Az ellenintézkedések között szerepel a tényellenőrzés, a mesterséges intelligencia alkalmazása és az oktatási kezdeményezések.

34 Marc Owen Jones: Disinformation superspreaders: the weaponisation of COVID-19 fake news in the Persian Gulf and beyond, *Global Discourse*, 2020. 10.4: 431–437.

35 Sandra Kalniete – Tomass Pildegovičs: Strengthening the EU's resilience to hybrid threats, *European View*, 2021. 20.1: 23–33.

36 B. Poornima: Cyber Threats and Nuclear Security in India, *Journal of Asian Security and International Affairs*, 2022. 9.2: 183–206.

A dezinformáció nagy mértékben befolyásolja a közvéleményt és a hibrid hadviselési stratégiák részeként jelentős nemzetbiztonsági kihívásokat vet fel. Kiemelten fontos a nemzetközi együttműködések, az átláthatóság, az oktatási kezdeményezések, és az információs ökoszisztéma megerősítése a dezinformációs kampányok hatásainak mérséklése érdekében. Mivel a dezinformációs támadások egyre összetettebbé és kifinomultabbá válnak, elengedhetetlen az interdiszciplináris kutatás és együttműködés előmozdítása a szilárd ellenintézkedések kifejlesztése érdekében. Jelen szakirodalmi áttekintés megalapozza a dezinformáció sokrétű természetének megértését, és olyan meglátásokat kínál, amelyek a jövőbeni kutatás, a szakpolitika-fejlesztés és a technológiai fejlesztések alapjául szolgálhatnak az információs manipuláció elleni folyamatos küzdelemben.

Takó Dalma

A világűr katonai célú felhasználásának nemzetközi jogi korlátai

Bevezetés

A világűr a nemzetközi közjog szabályai szerint olyan úgynevezett *res communis omnium usus* terület, mely mindenki által szabadon használható.[1] E használatnak ugyanakkor a nemzetközi jog, valamint annak részeként a nemzetközi világűrjog számos tekintetben igyekszik keretet biztosítani, rögzítve többek között azt, hogy a világűr, beleértve a Holdat és más égitesteket senki kizárólagos uralma alá nem tartozhat, a világűrben mindenféle kisajátítás vagy tulajdonszerzés tilos.[2] A világűrben végezhető tevékenységek kapcsán külön figyelmet érdemel az a kérdés, hogy e térségben vajon végezhetőek-e katonai jellegű tevékenységek, s ha igen, akkor ezekre milyen korlátok között kerülhet sor?

A fenti kérdéskör kapcsán elöljáróban megállapítható, hogy az űrtevékenységek megvalósítására képes államok már az űrkorszak

1 „A *res communis omnium usus* területek közé tartozó világűr kutatása és felhasználása az emberiség közös vállalkozásának tekintendő, mely minden állam előtt egyenlő módon nyitva áll, és minden állam javára és érdekében folytatandó." Sulyok Gábor: Világűr és önvédelem, In: Kajtár Gábor – Sonnevend Pál (szerk.): *A nemzetközi jog, az uniós jog és a nemzetközi kapcsolatok szerepe a 21. században: Tanulmányok Valki László tiszteletére*, Budapest, ELTE Eötvös Kiadó, 2021. 456. o.

2 Szerződés az államok tevékenységét szabályozó elvekről a világűr kutatása és felhasználása terén, beleértve a Holdat és más égitesteket (a továbbiakban: Világűrszerződés), II. cikk.

hajnalán végeztek katonai tevékenységeket a világűrben,[3] e térség már az 1967-es világűrszerződés megalkotása előtt bővelkedett katonai eszközökben.[4] Az azóta eltelt időben a világűrben végezhető tevékenységekre nézve a nemzetközi jogban számos kötelező és nem kötelező erejű dokumentum jött létre, melyek mindegyike valamilyen módon korlátokat kívánt támasztani a térség katonai célokra történő felhasználása tekintetében. Jelen tanulmány célja a világűr katonai célú felhasználását korlátozó legfontosabb nemzetközi jogi szabályok számbavétele, valamint annak ismertetése, hogy e szabályok keretében milyen tevékenységek tekinthetőek megengedettnek és melyek minősíthetőek tilosnak. Az említett kérdések feltárása kiemelt jelentőséggel bír, ugyanis a világűr jelentősége, a térség katonai, s főként védelmi célú felhasználásának szerepe egyre nő,[5] a katonai űrtevékenységek fejlesztésére egyre több állam, sőt nemzetközi szervezet is kiemelt figyelmet fordít.[6] Ennek köszönhetően kiemelt fontosságú annak ismerete, hogy az ilyen jellegű tevékenységek a világűrben milyen szabályok alapján, hogyan végezhetőek.

---

3 Stephan Hobe – Niklas Hedman: Preamble, In: Stephan Hobe – Bernhard Schmidt-Tedd – Kai-Uwe Schrogl (Eds.): *Cologne Commentary on Space Law. Outer Space Treaty*, Berlin, BWV Berliner Wissenschafts-Verlag, 2017. 159. o. „(…) már az űrkorszak hajnalán sem volt kétség a tekintetben, hogy a katonai fejlesztések és harcászati vívmányok jelentős szerepet töltenek be a világűr felé történő terjeszkedésben". Horváth Attila – Sipos Attila: A világűr katonai célú felhasználása, In: Bartóki-Gönczy Balázs – Sulyok Gábor: *Világűrjog*, Budapest, Ludovika Egyetemi Kiadó, 2022. 268. o.

4 Az első katonai műholdat 1960-ban az Egyesült Államok bocsátotta fel, amely megfigyelési céllal működött, és nagy felbontású képeket tudott készíteni. Horváth – Sipos: i. m. 280. o.

5 Bevezetés, In: Bartóki-Gönczy – Sulyok: i. m. 20. o.

6 Edl András: A világűr-politika fejlődése és irányai, In: Bartóki-Gönczy – Sulyok: i. m. 64, 72. o.; Bartóki-Gönczy Balázs: Az űrtevékenység nemzeti szintű szabályozása, In: Bartóki-Gönczy – Sulyok: i. m. 261. o.

1. A világűr katonai célú felhasználását korlátozó nemzetközi jogi szabályok

A világűr mikénti felhasználásának kérdése már az űrkorszak hajnalán, az 1960-as években felmerült, amikor az Egyesült Államok, valamint a Szovjetunió katonai célokra használható műholdakat bocsátott fel a térségbe.[7] E tevékenységek okán a nemzetközi közösség elsődleges célkitűzésévé vált a világűr használatára vonatkozó szabályok rögzítése.[8] A világűrben végezhető tevékenységek alapvető szabályait az államok öt multilaterális szerződésben foglalták össze, melyek közé az alábbi megállapodások sorolhatóak (a továbbiakban: világűrszerződések):

- Szerződés az államok tevékenységét szabályozó elvekről a világűr kutatása és felhasználása terén, beleértve a Holdat és más égitesteket – 1967 (a továbbiakban: világűrszerződés)[9]
- Egyezmény az űrhajósok mentéséről, az űrhajósok hazaküldéséről és a világűrbe felbocsátott objektumok visszaszolgáltatásáról – 1968 (a továbbiakban: mentési egyezmény)[10]
- Egyezmény az űrobjektumok által okozott károkért való nemzetközi felelősségről – 1972 (a továbbiakban: kárfelelősségi egyezmény)[11]

---

7 Az Egyesült Államok, valamint a Szovjetunió által a világűrbe felbocsátott mesterséges holdak kapcsán reális veszéllyé vált azok nukleáris robbanótöltetek célbajuttatására történő felhasználása. Gál Gyula: *Világűrjog*, Budapest, Közgazdasági és Jogi Könyvkiadó, 1964. 17–18, 190–191. o.

8 Gál: i. m. 170-171. o. A nemzetközi közösség egyetértett abban, hogy a világűr békés célú felhasználását rögzíteni kell. Stephan Hobe: Historical Background, In: Hobe – Schmidt-Tedd – Schrogl: i. m. 112. o.

9 Magyarországon kihirdette az 1967. évi 41. törvényerejű rendelet.

10 Magyarországon kihirdette az 1969. évi 22. törvényerejű rendelet.

11 Magyarországon kihirdette az 1973. évi 3. törvényerejű rendelet.

- Egyezmény a világűrbe felbocsátott objektumok nyilvántartásba vételéről – 1975 (a továbbiakban: lajstromozási egyezmény)[12]
- Egyezmény az államok tevékenységéről a Holdon és más égitesteken – 1979 (a továbbiakban: Hold-megállapodás).

Az említett szerződések mindegyike alapvető szabályként rögzíti a világűr békés célú felhasználását. A mentési egyezmény, a kárfelelősségi egyezmény, valamint a lajstromozási egyezmény e tekintetben egyaránt rögzíti, hogy a világűr békés célú kutatásának és felhasználásának elősegítése az egész emberiség közös érdeke, s a szerződések az ezzel kapcsolatos nemzetközi együttműködést igyekeznek elősegíteni.[13] A világűrszerződés, valamint a Hold-megállapodás az említettekhez képest részletesebben kitér a világűrben végezhető tevékenységekre, melynek okán e két egyezmény releváns rendelkezései külön is bemutatásra kerülnek.

A világűrszerződés preambuluma kiemeli, hogy a világűr kutatása és békés célokra történő felhasználása az egész emberiség közös érdeke, melynek okán a megállapodás a világűr kutatásának és békés célokra történő felhasználásának tudományos és jogi vonatkozásaiban széles körű nemzetközi együttműködést kíván lehetővé tenni. E célkitűzésekkel összhangban a dokumentum hivatkozik az ENSZ Közgyűlésének 1947. november 3-án elfogadott 110 (II) számú határozatára, kimondva, hogy e határozat, valamint a benne foglaltak – a béke veszélyeztetésére, békebontásra vagy agressziós cselekményre irányuló, illetve annak kiváltására vagy előmozdítására alkalmas propaganda elítélése – a világűrre is vonatkozik.[14] A preambulumban foglaltakon

12 Magyarországon kihirdette az 1978. évi 7. törvényerejű rendelet.

13 Mentési egyezmény, preambulum. Kárfelelősségi egyezmény, preambulum. Lajstromozási egyezmény, preambulum.

14 Világűrszerződés, preambulum.

felül a szerződés III. cikke is kiemeli, hogy *„A nemzetközi béke és biztonság fenntartása, valamint a nemzetközi együttműködés és megértés előmozdítása érdekében a Szerződésben részes államok a nemzetközi joggal, így az Egyesült Nemzetek Alapokmányával is összhangban folytatják tevékenységüket a világűr kutatásában és felhasználásában, beleértve a Holdat és más égitesteket."*[15] A világűrben végezhető tevékenységek kapcsán kiemelt jelentőséggel bír a szerződés IV. cikke, mely szerint: *„A Szerződésben részes államok kötelezik magukat, hogy nukleáris fegyvereket vagy bármely másfajta tömegpusztító fegyvert hordozó semmilyen objektumot nem juttatnak föld körüli pályára, ilyen fegyvereket az égitesteken nem helyeznek el, illetve a világűrben semmilyen más módon sem tartanak. A Holdat és más égitesteket a Szerződésben részes összes államok kizárólag békés célokra használhatják, Az égitesteken katonai támaszpontokat, berendezéseket és erődítéseket létesíteni, bármilyen fajta fegyverekkel kísérletezni és katonai gyakorlatokat folytatni tilos. Katonai személyeknek tudományos kutatásra vagy bármely más békés célra történő alkalmazása nincs tiltva. A Hold és más égitestek békés kutatásához szükséges bármely felszerelés vagy eszköz használata szintén megengedhető."*[16]

A világűrszerződés ismertetett rendelkezéseit a Hold-megállapodás is megerősíti,[17] valamint azokat ki is terjeszti a Naprendszer valamennyi égitestére.[18] A szerződés 2. cikke rögzíti,

15 Világűrszerződés, III. cikk.

16 Világűrszerződés, IV. cikk.

17 Sulyok Gábor: Nemzetközi jogi szabályozás, In: Bartóki-Gönczy – Sulyok: i. m. 86. o.

18 A szerződés szerint „E megállapodás Holdra vonatkozó rendelkezései a Naprendszeren belüli más égitestekre is vonatkoznak, a Földön kívül, kivéve, ha ezen égitestek bármelyikére vonatkozóan különleges jogi normák lépnek hatályba." A szerző saját fordítása a Hold-megállapodás 1. cikke alapján.

hogy *„A Holdon folytatott minden tevékenységet, beleértve annak kutatását és használatát is, a nemzetközi joggal, különösen az Egyesült Nemzetek Alapokmányával összhangban kell végezni, figyelembe véve a Közgyűlés által 1970. október 24-én elfogadott, az államok közötti baráti kapcsolatokra és együttműködésre vonatkozó nemzetközi jogi elvekről szóló nyilatkozatot, előmozdítva a nemzetközi béke és biztonság fenntartását, a nemzetközi együttműködést és kölcsönös megértést, valamint figyelembe véve az összes többi részes állam megfelelő érdekeit."*[19] A megállapodás 3. cikke értelmében *„A Holdat minden részes állam kizárólag békés célokra használhatja. A Holdon tilos az erőszak alkalmazása vagy az azzal való fenyegetés, illetve bármilyen más ellenséges cselekedet vagy ellenséges cselekedettel való fenyegetés. Ugyanígy tilos a Holdat ilyen cselekmény elkövetésére vagy ilyen fenyegetésre használni a Földdel, a Holddal, űrhajókkal, űrhajók személyzetével vagy ember alkotta űreszközökkel szemben. A részes államok nem állíthatnak a Hold körüli pályára vagy más pályára a Hold körül nukleáris fegyvereket vagy más tömegpusztító fegyvereket hordozó tárgyakat, és nem helyezhetnek el vagy használhatnak ilyen fegyvereket a Holdon vagy a Holdban. Tilos a Holdon katonai bázisok, létesítmények és erődítmények létesítése, bármilyen típusú fegyver tesztelése és katonai manőverek végrehajtása. Nem tilos a katonai személyzet tudományos kutatásra vagy más békés célokra történő alkalmazása. Nem tilos a Hold békés célú kutatásához és használatához szükséges berendezések és létesítmények használata sem."*[20]

A fentiek alapján látható, hogy a világűrben végezhető tevékenységek alapvető szabályait a világűrszerződések fektetik le. Az említetteken felül ugyanakkor más, általános nemzetközi

19 A szerző saját fordítása a Hold-megállapodás 2. cikke alapján.
20 A szerző saját fordítása a Hold-megállapodás 3. cikke alapján.

jogi szerződések is tartalmaznak releváns rendelkezéseket a világűrben végezhető tevékenységekkel összefüggésben.[21] Ebben a tekintetben mindenekelőtt tisztázni szükséges, hogy a világűrben végezhető tevékenységekre a nemzetközi jog általános szabályai is alkalmazandóak.[22] E tényre a világűrszerződés, valamint a Hold-megállapodás is kifejezetten utal, amikor rögzítik, hogy a világűrben végzett minden tevékenységet a nemzetközi joggal, különösen az Egyesült Nemzetek Alapokmányával összhangban kell végezni.[23] Ennek köszönhetően az Alapokmányban foglaltak, a nemzetközi szokásjog szabályai, valamint a nemzetközi jog feltétlen alkalmazást igénylő szabályai egyaránt kiemelt jelentőséggel bírnak a világűrben végzett tevékenységek kapcsán. Mindez többek között azt jelenti, hogy az űrtevékenységek során is tiszteletben kell tartani az erőszak alkalmazásának tilalmát,[24] vagy például az együttműködés alapelvét.

---

21 A témakörre vonatkozóan kétoldalú szerződések, valamint egy többoldalú egyezménytervezet is létrejött. Előbbire szolgálnak példaként a hadászati fegyverek korlátozásáról és számának csökkentéséről szóló kétoldalú szerződések, utóbbi kapcsán pedig az űrobjektumok elleni erőszakkal való fenyegetésnek vagy erőszak alkalmazásának megelőzéséről szóló szerződés tervezete érdemel említést, melyek ismertetésére ugyanakkor nem kerül sor. Ennek oka, hogy a „kétoldalú fegyverzetkorlátozási megállapodások már hatályukat vesztették, a szerződéstervezet kapcsán pedig régóta nem történt érdemi előrelépés". Sulyok: i. m. (2021) 457–459. o.

22 Kai-Uwe Schrogl – Julia Neumann: Article IV, In: Hobe – Schmidt-Tedd – Schrogl: i. m. 288. o.

23 Világűrszerződés, III. cikk. Hold-megállapodás, 2. cikk.

24 A tilalom ENSZ Alapokmányban, valamint nemzetközi szokásjogban foglalt tartalma ennélfogva a világűrre nézve is irányadó. Eszerint az önvédelem, valamint az ENSZ Biztonsági Tanácsa által adott felhatalmazás kivételétől eltekintve az államoknak nemzetközi érintkezéseik során az erőszakkal való fenyegetéstől, valamint az erőszak alkalmazásától tartózkodniuk kell. ENSZ Alapokmány, 2. cikk (4) bekezdés. Horváth – Sipos: i. m. 279. o.

A világűrben végzett tevékenységek szabályozásában kiemelést érdemel továbbá az 1963-as részleges atomcsend szerződés, mely a légkörben, a világűrben és a víz alatt végzett nukleáris fegyverkísérletek betiltásáról szól.[25] Az egyezmény értelmében minden részes állam vállalta, hogy *„betilt, megakadályoz és nem hajt végre nukleáris fegyverrel történő semmiféle kísérleti robbantást és semmiféle más nukleáris robbantást a joghatósága vagy ellenőrzése alá tartozó semmilyen helyen: sem a légkörben; sem annak határain túl, beleértve a világűrt; sem víz alatt, beleértve a területi vizeket és a nyílt tengert; és semmilyen más közegben, ha az ilyen robbantás az azt végrehajtó állam joghatósága vagy ellenőrzése alá tartozó területen kívül rádióaktív lecsapódást eredményez."*[26] Szintén fontos a környezetmódosító eljárások katonai vagy bármely más ellenséges szándékú alkalmazásának eltiltásáról szóló egyezmény,[27] mely a környezetmódosító eljárás fogalma alatt minden olyan eljárást ért, *„amely – a természeti folyamatokba való tudatos beavatkozás révén – megváltoztatja a Föld vagy a világűr dinamikáját, összetételét vagy szerkezetét, beleértve a Föld élővilágát, szilárd kérgét, vízkörét és légkörét."*[28] Az egyezmény értelmében minden részes államnak tartózkodnia kell az olyan környezetmódosító eljárások katonai vagy bármely más ellenséges szándékú alkalmazásától, amelyeknek bármely más részes államra széles körű, hosszan tartó súlyos

25 Horváth – Sipos: i. m. 278. o.

26 Szerződés a légkörben, a világűrben és a víz alatt végzett nukleáris fegyverkísérletek betiltásáról, I. cikk. Magyarországon kihirdette az 1963. évi 26. törvényerejű rendelet. Fontos ehelyütt megemlíteni az Átfogó Atomcsend Szerződést is, mely azonban a szükséges számú ratifikáció hiányában még nem lépett hatályba. Sulyok: i. m. (2021) 457–459. o.

27 Horváth – Sipos: i. m. 282. o.

28 Egyezmény a környezetmódosító eljárások katonai vagy bármely más ellenséges szándékú alkalmazásának eltiltásáról, 2. cikk. Magyarországon kihirdette az 1978. évi 29. törvényerejű rendelet.

hatásuk van, valamint minden részes államnak kötelezettséget kell vállalnia arra, hogy egyetlen államot, államcsoportot vagy nemzetközi szervezetet sem segít, ösztönöz vagy késztet arra, hogy ilyen tevékenységet folytasson.[29]

A világűrben végezhető tevékenységekről ugyanakkor nem csupán kötelező erejű anyagok rendelkeznek, a releváns dokumentumok sorában kiemelést érdemelnek az Egyesült Nemzetek Közgyűlésének határozatai is.[30] Ezek közül különösen fontos az államoknak a világűr felderítése és használata terén folytatott tevékenységére irányadó jogi elvekről szóló nyilatkozat (1962 (XVIII) számú határozat),[31] valamint a világűr felderítése és használata terén valamennyi állam javára és érdekében folytatott nemzetközi együttműködésről szóló nyilatkozat (51/122 számú határozat).[32] Mindkét dokumentum hangsúlyozza a világűr békés célú kutatásának és békés célú felhasználásának jelentőségét, valamint rögzíti, hogy a világűr felderítését és használatát az egész emberiség javára és az államok javára kell folytatni, ennek érdekében pedig széleskörű nemzetközi együttműködést kell kialakítani. Mindkét dokumentum rögzíti továbbá, hogy az államoknak a világűr felderítése és használata terén folytatott

29 Egyezmény a környezetmódosító eljárások katonai vagy bármely más ellenséges szándékú alkalmazásának eltiltásáról, 1. cikk.

30 Ram S. Jakhu – Steven Freeland (Eds.): *McGill Manual on International Law Applicable to Military Uses of Outer Space: Volume I – Rules,* Montreal, Centre for Research in Air and Space Law, 2022. 4. o. (a továbbiakban: McGill Manual)

31 UN GA Resolution 1962 (XVIII) of 13 December 1963. Declaration of Legal Principles Governing the Activities of States in the Exploration and Use of Outer Space.

32 UN GA Resolution 51/122 of 4 February 1997. Declaration on International Cooperation in the Exploration and Use of Outer Space for the Benefit and in the Interest of All States, Taking into Particular Account the Needs of Developing Countries.

tevékenységét a nemzetközi joggal, beleértve az Egyesült Nemzetek Alapokmányát is, összhangban kell végezni a nemzetközi béke és biztonság fenntartása, valamint a nemzetközi együttműködés és megértés előmozdítása érdekében.

A releváns ENSZ Közgyűlési határozatok között feltétlenül szükséges megemlíteni az 1348 (XVIII), valamint az 1472 (XIV) számú határozatot, melyek az ENSZ Világűrbizottságának (UNCOPUOS) felállításáról rendelkeztek, a szervezet elsődleges céljaként rögzítve a világűr békés célú felhasználásának elősegítését.[33] Szintén fontos az 1721 (XVI) számú Közgyűlési határozat, mely a világűr békés célú felhasználása terén megvalósítandó nemzetközi együttműködésről szól. E határozat szintén hangsúlyozza a világűr békés célú felhasználását, valamint annak nemzetközi joggal és az ENSZ Alapokmánnyal összhangban, az egész emberiség javára történő megvalósítását.[34] A határozatban lefektetett elveket a Közgyűlés 1802 (XVII) számú határozata is megerősítette.[35] Az említett általános határozatokon felül a Közgyűlés kifejezett lépéseket is tett a világűrben végezhető katonai tevékenységek korlátozása érdekében. A testület 1884 (XVIII) számú határozata például megerősítette, hogy a világűrben nem kerülhet sor nukleáris és tömegpusztító fegyverek elhelyezésére és használatára.[36] Az említett határozatok kapcsán fontos kiemelni, hogy azok közgyűlési határozatként nem rendelkeznek

33 UN GA Resolution 1348 (XVIII) of 13 December 1958. UN GA Resolution 1472 (XIV) of 12 December 1959.

34 UN GA Resolution 1721 A and B (XVI) of 20 December 1961. Gál: i. m. 198. o.

35 UN GA Resolution 1802 (XVII) of 14 December 1962. További határozatokban szintén megjelent a világűr békés célú felhasználásának elve, melyek között említhető például a Közgyűlés 68/74 számú határozata. UN GA Resolution 68/74 of 11 December 2013.

36 UN GA Resolution 1884 (XVIII) of 17 October 1963. Horváth – Sipos: i. m. 281. o.; Hobe – Hedman: i. m. 163. o.

kötelező erővel, azonban egyes határozatok szokásjogi jellege mellett számos szerző álláspontja szerint lehet érvelni.[37]

2. A világűrben végezhető katonai tevékenységek

Az előző fejezetben foglaltak alapján látható, hogy a világűr használatának szabályozása meglehetősen komplex, azt rengeteg eltérő jellegű és formátumú dokumentum igyekszik korlátok közé szorítani. Az ismertetett rendelkezések alapján egyértelműen megállapítható, hogy a világűr használata kapcsán kiemelt jelentőségű, alapvető szabályként érvényesül a békés célú felhasználás. Ezen elv valamennyi előző fejezetben bemutatott dokumentumban szerepel valamilyen formában, azonban annak fogalmát vagy tartalmát egyik ismertetett forrás sem írja körül egyértelműen. Éppen ezért kiemelt jelentőséggel bír annak tisztázása, hogy a békés célú felhasználás kategóriája milyen tevékenységeket foglal magában.

A békés célú felhasználás fogalmának kétféle megközelítése lehetséges.[38] Az egyik a valamennyi katonai tevékenységet kizáró nem katonai felhasználás,[39] a másik pedig a bizonyos

37 Egyes közgyűlési határozatok ugyanis széles körben kerültek, kerülnek hivatkozásra és alkalmazásra, melynek köszönhetően velük kapcsolatban a nemzetközi szokásjog mindkét feltétele – az általános, következetes gyakorlat, valamint a jogi meggyőződés – nagy valószínűséggel teljesül.

38 Sulyok: i. m. (2021) 456. o.

39 Hobe – Hedman: i. m. 159. o.; Gál: i. m. 202–204. o. Ez a megközelítés figyelhető meg az Antarktisz területe kapcsán, melyre nézve az Antarktisz egyezmény kifejezetten rögzíti, hogy a terület kizárólag tudományos és békés célokra használható, mely alatt minden katonai tevékenység kizárását kell érteni. A területen nem létesíthetőek katonai támaszpontok, nem helyezhetőek el fegyverek, nem végezhetőek hadgyakorlatok és fegyverkísérletek, katonai személyzet és felszerelés legfeljebb tudományos kutatási,

katonai tevékenységeket megengedő nem agresszív, vagy nem támadó jellegű felhasználás.[40] A két elmélet közül a világűr kapcsán mára egyértelműen utóbbi nyert általános elismerést, mely részben az előző fejezetben bemutatott dokumentumokból, részben az évtizedek óta megfigyelhető következetes és töretlen nemzetközi gyakorlatból is látható.[41] Ez utóbbi elmélet értelmében minden olyan katonai művelet, mely nem támadó jellegű, azaz nem valósít meg közvetlen fegyveres támadást, a világűr békés célú felhasználásának körébe tartozik, s ily módon megengedett.[42]

A békés célú felhasználás ilyen tartalmú értelmezése egyes álláspontok szerint már az űrkorszak hajnalán, a világűrszerződések létrehozását megelőzően egyértelművé vált, ugyanis az Egyesült Államok és a Szovjetunió már 1960-ban katonai célra alkalmazható műholdakat bocsátott fel a világűrbe, mely alapján nyilvánvaló volt, hogy mindkét állam folytatni kíván bizonyos katonai tevékenységeket a világűrben.[43] A szóban forgó álláspontot számos szakirodalmi forrás is alátámasztja, melyek szerzői egyértelműen kifejtik, hogy a békés használat nem értel-

---

vagy más békés célokra használható fel. Ily módon az Antarktisz mindenféle fegyvertől és katonai tevékenységtől mentes, teljesen demilitarizált terület. Horváth – Sipos: i. m. 279–280. o.; Schrogl – Neumann: i. m. 294. o.; Alexander Proelss: *Peaceful Purposes*, Oxford Public International Law, Oxford University Press, 2022.

40 Gál: i. m. 199. o.

41 Sulyok: i. m. (2022) 86. o.

42 Gál: i. m. 194–195. o.

43 Horváth Attila és Sipos Attila szerint „(…) mindkét akkori nagyhatalom határozottan visszautasította a fegyverkezés teljes tilalmának lehetőségét". Horváth – Sipos: i. m. 268. o. A világűr teljes demilitarizálását tehát mind az USA, mind a Szovjetunió elvetette, s a nemzetközi közösség számára is egyértelmű volt, hogy a világűr kapcsán nem kerülhet sor minden katonai tevékenység kizárására. Stephan Hobe: Article I, In: Hobe – Schmidt-Tedd – Schrogl: i. m. 174, 294. o.

mezhető úgy, hogy minden jellegű katonai tevékenység kizárt a világűrben.[44]

A fenti értelmezésnek megfelelően kerültek kialakításra a világűr felhasználását meghatározó szabályok is, melyekből egyértelműen kirajzolódik, hogy a világűr nincs teljes egészében elzárva a katonai tevékenység elől, csupán részlegesen demilitarizált területnek tekinthető.[45] Az előző fejezetben bemutatott dokumentumok alapján mindez azt jelenti, hogy nukleáris fegyverek és más tömegpusztító fegyverek sem az égitesteken, sem az azok körüli keringési pályákon, sem a világűr bármely más pontján nem helyezhetők el.[46] Az égitesteken nem hozhatóak létre továbbá katonai támaszpontok, létesítmények, valamint nem végezhetők fegyverkísérletek, hadgyakorlatok sem.[47]

Egyetlen dokumentum sem tiltja ugyanakkor hagyományos fegyverek világűrben történő elhelyezését – az égitestek kivételével, melyeken a Hold-megállapodás értelmében a hagyományos fegyverek elhelyezése is tilos –, valamint katonai személyzet és felszerelés kutatási vagy más békés célokra történő felhasználását. Az ismertetett tilalmak alá nem sorolhatóak be továbbá a műholdak elleni elektronikai támadáshoz vagy kibertámadáshoz szükséges földi telepítésű eszközök, valamint azon fegyverek sem, melyek a Földről indulva és oda visszatérve pusztán egy

44 Az említett szakirodalmi források szerint a vonatkozó nemzetközi jogi szabályozásnak nem az a célja, hogy minden katonai tevékenységet kizárjon, az pusztán az aktív, azaz támadó jellegű katonai tevékenységeket kívánja tiltani a világűrben. Horváth – Sipos: i. m. 283. o.; Gál: i. m. 200–201. o.

45 Sulyok: i. m. (2022) 86. o. A demilitarizálás Gál Gyula fogalmával élve olyan nemzetközi szerződésen alapuló korlátozás, mely alapján az adott területet katonailag nem szabad megerősíteni. Gál: i. m. 215. o.

46 Horváth – Sipos: i. m. 86. o.

47 Sulyok: i. m. (2021) 457–459. o.

rövid ideig tartózkodnak a világűrben.[48] Ezen felül Föld körüli pályán passzív katonai tevékenységet – például védekező funkciót – ellátó műholdak és űrállomások elhelyezése is megengedett.[49] Utóbbi lehetőséggel nagy számban élnek is az államok, napjainkban „a korai riasztási, megfigyelési, felderítési, távközlési, navigációs, meteorológiai és geodéziai feladatokat ellátó katonai és kettős rendeltetésű műholdak tömege kering a bolygónk körül."[50] Ezen kettős funkciót ellátó rendszerek egyaránt használhatóak polgári és katonai célokra.[51] A megfigyelési tevékenységet végző műholdak által gyűjtött adatok például egyaránt felhasználhatóak térképészeti célokra, ásványkincsek feltárásához, erdészeti

48 Sulyok: i. m. (2022) 86. o. Ahogy azt Sulyok Gábor rögzíti: „Nem terjed ki azonban a tilalmak hatálya az olyan Földről indított tömegpusztító fegyverek alkalmazására és kipróbálására, melyek a kijelölt célpont felé vezető úton csak átmenetileg lépnek ki a világűrbe, és valószínűleg azokra a tömegpusztító fegyverekre sem, melyek nem végeznek legalább egy teljes keringést a bolygónk körül. Nem terjed ki a tilalmak hatálya a nukleáris fegyverek Naprendszer égitesteit nem érintő és elhelyezésnek nem minősülő alkalmazására és kipróbálására sem." Sulyok: i. m. (2021) 456–457. o.

49 Sulyok: i. m. (2021) 457–459. o.

50 Sulyok: i. m. (2021) 457–459. o. Egyes vélemények szerint megfigyelhető, hogy a hagyományos űreszközöket egyre inkább a katonai tevékenységek irányítására használják. Yoram Dinstein: *War, Agression and Self-Defence*, Cambridge, Cambridge University Press, 2011. 24. o.

51 Ehelyütt elegendő példaként megemlíteni a GPS rendszert, mely eredetileg katonai célokra került kifejlesztésre, s csak utóbb vált polgári célokra is alkalmazandóvá. Várdai Mihail Istvanovics: A világűr militarizálásának kérdéseiről, *Honvédségi Szemle*, 2021/1. 34. o.; Tari Fruzsina: A földmegfigyelés jogi kérdései, In: Bartóki-Gönczy – Sulyok: i. m. 220, 222. o.; Horváth – Sipos: i. m. 285. o. Ugyanígy említhetőek a kommunikációs funkciót ellátó műholdak, melyek polgári és katonai üzenetek továbbítására is alkalmasak. Francis Lyall – Paul B. Larsen: *Space Law. A Treatise*, Farnham – Burlington, Ashgate, 2009. 500. o.

vagy mezőgazdasági célokra, környezetgazdálkodáshoz, valamint katonai célokra is.[52]

Mindezek alapján látható, hogy a világűr békés célú felhasználása keretében számos katonai jellegű tevékenység végzésére lehetőség van a világűrben. A gyakorlatban természetesen számos kérdés felvethető azzal kapcsolatban, hogy mely magatartások tekinthetőek jogszerűnek, s melyek ütköznek a nemzetközi jog, vagy azon belül a nemzetközi világűrjog valamely ismertetett szabályába.[53] Példaként szolgálhat erre az orosz Kozmosz–2542 műhold esete, melyről egy leváló kisebb műhold 2020. január 31-én megközelítette az USA–245 azonosítójú felderítő műholdját. Oroszország mindezt ellenőrző funkció keretében végzett tevékenységnek minősítette, mely az állam álláspontja szerint semmiféle nemzetközi szabályt nem sértett.[54] Ez a példa is jól mutatja, hogy az államok igyekeznek maximálisan kihasználni a nemzetközi jog és a világűrjog nyújtotta lehetőségeket, s előszeretettel lavíroznak a jogszerű és jogszerűtlen magatartások közötti határvonalon.[55]

Mindez annak köszönhető, hogy a világűr békés célú felhasználásának fogalma viszonylag tágan értelmezhető, hiszen

52 Hobe: i. m. (Historical Background) 125. o.

53 Példaként említhető a hírszerzési tevékenységet ellátó műholdak kérdése, melyek tevékenysége adott esetben kémkedésnek is tekinthető, melynek megítélése ugyanakkor szintén nem teljes mértékben egyértelmű a nemzetközi jogban.

54 Várdai: i. m. 46. o.

55 E tekintetben fontos megjegyezni, hogy azokban az államokban, melyek rendelkeznek a világűr katonai célú felhasználásának képességével, a világűrben végzett katonai tevékenységek szabályozása a belső jogi szabályozásban is megjelenik. Az Egyesült Államok, India, Franciaország, Oroszország és Kína belső jogában egyaránt szabályozásra került a világűr katonai felhasználásának kérdése. Horváth – Sipos: i. m. 277–278. o.; Várdai: i. m. 36, 39. o.

abba a támadó jellegű, agresszív tevékenységeken kívül csaknem bármilyen katonai tevékenység besorolható. Ráadásul teljes mértékben egyértelmű definíció hiányában „a gyakorlatban nehéz vagy egyáltalán nem lehet különbséget tenni a védelmi és a támadó, valamint a katonai és nem katonai felhasználás között."[56] Az elmúlt években jól látható tendenciaként kezd kirajzolódni, hogy az államok egyre inkább igyekeznek kiaknázni a világűrben rejlő lehetőségeket, ideértve a világűr katonai célú felhasználását. Egyes álláspontok szerint „A modern hadviselés nemcsak a fejlett technológia és a személyzet együttműködésén múlik, hanem a világűrben található eszközök és csapásmérő képességek támogatására épül."[57]

E tendenciára a nemzetközi közösség igyekszik reagálni, melynek látható eredményei közé tartoznak az ENSZ Közgyűlés azon közelmúltbeli határozatai, melyek a világűrben zajló fegyverkezés megelőzésére, korlátozására vonatkoznak. Ezek között említhetőek a Közgyűlés 71/31 és 71/32 számú határozatai, melyek a fegyverkezési verseny megelőzésének fontosságát és sürgősségét hangsúlyozzák.[58] Különösen fontos ezeken felül a Közgyűlés 75/36 számú határozata, mely a világűr által nyújtott lehetőségekben rejlő fenyegetettséget normák és úgynevezett felelős magatartásra vonatkozó elvek lefektetésével kívánja csökkenteni.[59] A határozat kiemelt jelentőséggel bír az űrrendszert fenyegető veszélyek és védelmi kockázatok beazonosítása és kezelése szempontjából.[60]

---

56 Horváth – Sipos: i. m. 285. o.

57 Horváth – Sipos: i. m. 285. o. Az űrtechnológia tehát alapvető fontosságú a katonai felhasználás szempontjából. Hobe: i. m. (Historical Background) 142. o.

58 UN GA Resolution 71/31 of 5 December 2016. UN GA Resolution 71/32 of 5 December 2016.

59 UN GA Resolution 75/36 of 7 December 2020.

60 Horváth – Sipos: i. m. 287–288. o.

Említést érdemel továbbá a 2022-ben napvilágot látott úgynevezett McGill Manual, mely kötelező erővel ugyan nem rendelkezik, azonban jelentős iránymutatóként szolgál a világűrben végezhető tevékenységek körének meghatározásához.[61] A dokumentum részletesen foglalkozik a világűrben végezhető katonai tevékenységek fogalmával, rögzítve, hogy e fogalom alá sorolható valamennyi katonai jellegű űrtevékenység. Ennek meghatározásához pedig a dokumentum szerint figyelembe kell venni a tevékenységben részt vevő szereplőket, a tevékenység céljait és a tevékenység hatásait.[62] E fogalom rögzítésén felül a dokumentum a világűrben végezhető katonai tevékenységekre vonatkozó alapvető elveket fekteti le, mellyel ugyanakkor pusztán megerősíti a világűrszerződésben foglaltakat.[63]

61 McGill Manual, i. m. 4. o.

62 McGill Manual, i. m. 9. o.

63 A dokumentum értelmében az államok a világűr kutatása és használata során – ideértve a katonai célú űrtevékenységeket is – nagyfokú szabadságot élveznek, amennyiben azt a nemzetközi joggal – beleértve a nemzetközi űrjogot is – összhangban végzik. E tekintetben a dokumentum kifejezetten rögzíti, hogy az államoknak tartózkodniuk kell többek között az erőszak tilalmának megsértésétől. A dokumentum ezen felül kimondja, hogy a Hold és más égitestek kizárólag békés célokra használhatók, rajtuk a katonai tevékenységek a világűrszerződés és a nemzetközi jog más alkalmazandó szabályaiban foglaltak szerint tilosak. Ennek jegyében a nukleáris és tömegpusztító fegyverek esetében teljes tilalom érvényesül, az egyéb fegyverekkel kapcsolatos űrtevékenységeket pedig a nemzetközi joggal összhangban kell végezni, beleértve az Egyesült Nemzetek Alapokmányát és a nemzetközi űrjogot is. Úgyszintén tilos a Hold és más égitestek, vagy azok természeti erőforrásainak felhasználása katonai bázisok, létesítmények és erődítmények létrehozására, bármilyen típusú fegyver tesztelésére és katonai manőverek végrehajtására a Holdon és más égitesteken. Nem tilos azonban a katonai személyzet vagy felszerelés alkalmazása tudományos kutatásra vagy más békés célokra. McGill Manual, i. m. 13, 15, 20, 22. o.

Záró gondolatok

A tanulmányban foglaltak alapján látható, hogy bár a világűr felhasználása kapcsán feltétlenül érvényesülnie kell a békés célú felhasználás elvének, azonban e követelmény nem jelenti a világűr teljes demilitarizálását, s minden katonai tevékenységtől való mentességét. A világűr térségére nem alkalmazható az Antarktisz esetében működő, valamennyi katonai tevékenységet teljes egészében kizáró modell, arra nézve csupán a támadó jellegű, agresszív katonai tevékenységek tilalma, bizonyos térségek demilitarizálása, valamint bizonyos fegyverfajták tilalma érvényesül.

A világűr katonai célú felhasználása kapcsán a nemzetközi jog, s annak részeként a nemzetközi világűrjog által felállított korlátok kiemelt jelentőséggel bírnak, ugyanakkor, ahogy az a tanulmányból látható volt, e korlátok nem jelentenek teljeskörű megoldást az államok tevékenységének keretek közé szorítására. A világűrben végzett katonai tevékenységek kapcsán ugyanis jelentős nehézségként merül fel az egyes magatartások jogszerű és jogszerűtlen jellegének, sőt sok esetben az űreszközök rendeltetésének megállapítása. A rendelkezésre álló elektrooptikai és rádiólokációs lehetőségekkel legtöbbször csak feltételezni lehet az űrobjektumok funkcióját, a katonai célú űreszközök ráadásul „általában csak a speciális manőverek végrehajtása következtében, illetve pályájuk jellemzői alapján válnak azonosíthatóvá."[64]

Az említett nehézségekhez természetesen a világűr stratégiai jelentősége, az államok védelme és biztonsága szempontjából betöltött szerepe, valamint a szóban forgó témakörök ebből fakadó érzékeny jellege is hozzájárul, mely különösen nehézzé, sőt talán lehetetlenné teszi a témakörrel kapcsolatos átfogó, részletes szabályozás kidolgozását. Az azonban egyértelműen leszögezhető,

64 Várdai: i. m. 47. o.

hogy mivel a katonai tevékenység az űrkorszak kezdete óta jelen van a világűrben,[65] s az elmúlt időszak tapasztalatai alapján jelentősége egyre csak nő,[66] kiemelt jelentőséggel bír annak vizsgálata, hogy e tevékenységnek hol húzódnak a határai, s a nemzetközi közösség mit tud tenni ezek feltárása, illetve betartása érdekében.[67] Jelen tanulmány a világűr katonai célú felhasználására vonatkozó szabályozás ismertetésével, valamint a felmerülő nehézségek feltárásával kívánja segíteni e különösen nehéz folyamatot.

65 Schrogl – Neumann: i. m. 289. o.

66 Egyes álláspontok szerint napjainkban a hadviselés elképzelhetetlen az űrkapacitások nyújtotta támogatás nélkül. Schrogl – Neumann: i. m. 289. o.

67 Egyes szerzők véleménye szerint az államoknak szorgalmazniuk kellene „a világűrben folytatott tevékenységeket illetően felmerülő vitás ügyeik békés rendezését és az egységes szabályozás megteremtését" s egy olyan nemzetközi szerződést kellene kidolgozniuk, amely „hatékony és objektív felügyeleti mechanizmus bevezetése mellett világosan meghatározza a világűrben folytatható űrtevékenységek körét". Horváth – Sipos: i. m. 289. o.

MŰHELY

Varró Tekla

Az alapjogi korlátozások kérdésköre különleges jogrend idején

„Az emberi jogok biztosítása egy demokratikus államban evidencia. Sőt, a történelmi tapasztalat az, hogy a társadalomban semmi más nem tudta biztosítani a szabadságot, a demokráciát, mint az emberi jogok."[1]

Az alapvető jogok bizonyos helyzetekben, más alapvető jogok érvényesülés érdekében korlátozhatóak. Egyes helyzetekben, például a véleménynyilvánítási szabadságát nem gyakorolhatja az állampolgár nyilvánosság előtt, ha azzal mások elpusztítására hergeli a hallgató közönséget.

Az alapjogok korlátozása az utóbbi időkig csak elvi lehetőségként jelentek meg, azonban 2020 elején megjelent Covid-19 járvány, majd a napjainkban is folyamatban lévő, szomszédos országban zajló háború magával vonzotta a különleges jogrend bevezetését, ezzel pedig az alapjogok korlátozását – mely végkimenetelét és időtartamát előre nem tudjuk.

A szerző civil szemszögből vizsgálja és bemutatja a korlátozható alapjogokat, az alapjogi gondolkodás kialakulásának és fejlődésének történelmi áttekintését, a magyar szabályozást, a szükségességi-arányossági vizsgálat lényegét, a különleges jogrendi jogalkotás alapjait, az Alaptörvény vonatkozó rendelkezéseit és a kapcsolódó alkotmánybírósági gyakorlatot. A szerző kitér a 2020-ban kialakult Covid-19 járvány okozta alapjog

1 Csink Lóránt: Alapjogok különleges jogrend idején, Védelmi-Biztonsági Szabályozási és Kormányzástani Műhelytanulmányok 2022/6, Nemzeti Közszolgálati Egyetem Védelmi-Biztonsági Szabályozási és Kormányzástani Kutatóműhely, Budapest, 2022. ISSN 2786-2283, 4. o.

korlátozásra, valamint a 2022-ben átalakult különleges jogrendi szabályozásra.

1. Bevezetés

E fejezet az alapjogok kialakulásnak rövid történetével, majd az alapjog korlátozás elméletével kívánja megalapozni a dolgozat fő témáját. Ez után az alapjogok nemzetközi korlátozásának bemutatása következik, azt követően pedig a magyarországi alapjog-korlátozás bemutatásával folytatódik. A fejezet befejezéseként a Magyarországon is alkalmazott szükségességi-arányossági teszt kerül bemutatásra.

1.1. Az alapjogok kialakulásának rövid vázlata

Az alapjogok dokumentumai közül a modern alkotmányosság alapjaként az angol törvények és nyilatkozatok (1628. évi *Petition of Right*, az 1679. évi *Habeas Corpus Act* és az 1689. évi *Bill of Rights*), az 1774-es *Declaration of Rights*, valamint az 1776-os Amerikai Függetlenségi Nyilatkozat tekinthetők. Ezek a dokumentumok alapelveket fogalmaztak meg emberi jogként, melyek a modern alapjogi katalógus alapját képezték. Franciaországban, az 1789. augusztus 26-án elfogadott, az emberi és polgári jogok tizenhét cikket tartalmazó nyilatkozata az ember természetes és elidegeníthetetlen jogairól szól. A XX. századra az alapjogok védelméről már az összes alkotmányos demokrácia rendelkezik.[2]

[2] Gárdos-Orosz Fruzsina: „Az alapjogok korlátozása", Internetes Jogtudományi Enciklopédia (Alkotmányjog rovat, rovatszerkesztő: Bodnár Eszter, Jakab András) http://ijoten.hu/szocikk/az-alapjogok-korlatozasa (2020) [1]., Letöltés: 2023.07.10.

A magyar Alaptörvény vallja, hogy az embert születésétől fogva sérthetetlen és elidegeníthetetlen alapjogok illetik meg, melyeket tiszteletben kell tartani, s melyek védelme az állam elsőrendű kötelezettsége.[3]

Az alapjog korlátozás elméletének és módszertanának kialakulása a II. világháborút követően Németországban alakultak ki a bírói gyakorlatban. A klasszikus megfogalmazás azt mondja, hogy az egyik ember szabadságjoga addig terjed, míg nem sérti más szabadságát. Az emberi jogi dokumentumokban – legyen szó nemzeti vagy nemzetközi dokumentumokról –, az európai alkotmányosság legfontosabb forrásaiban leírt jogok bár abszolútnak tűnnek, mégis minden alkotmányos „szerződés" egy korlátozási klauzulával rendelkezik.[4]

Az 1950-es évektől az alkotmányos védelem az emberi jogokat azok korlátaival egyben definiálja. A korlátozási tesztek lényege a különböző jogokban ezen kritériumok mentén valósul meg:

- abban az esetben felel meg nemzetközi jogi és alkotmányos normáknak a korlátozás, ha legitim, tehát az alkotmányos demokrácia eszméje szerint igazolható célt szolgál,
- az alkalmazott eszköznek alkalmasnak kell lenni arra, hogy az előzőekben említett célt hatékonyan szolgálja, tehát a kitűzött cél és a megvalósításhoz használt eszköz között összefüggés van,
- a jog korlátozásra elengedhetetlen a cél eléréséhez,
- a korlátozás arányos a kitűzött céllal.

A magyar jogban az a korlátozási teszt „szükségességi-arányossági teszt"-ként ismert.[5]

---

3 Magyarország Alaptörvénye, (2011. április 25.) I. cikk, Forrás: https://njt.hu/jogszabaly/2011-4301-02-00, Letöltés: 2023.07.29.

4 Gárdos-Orosz: i. m. [4].

5 Gárdos-Orosz: i. m. [5].

1.2. Az alapjogkorlátozás elmélete

Alapjogkorlátozásnál lényeges kritérium, hogy az alapvető jogokat az állam szervei magatartásukkal ne sértsék meg, melyre biztosíték az Alaptörvényben biztosított jog, miszerint az alapvető jogok védelmét az állam garantálja: *„Az alapjogok az állam lététől független jogok, melyekhez állami elismerés társul."*[6] Ez a garancia szolgál arra, hogy az alapvető jogok rendszerét nem tudja semmissé tenni az állam semmiféle eljárás során. Az alapvető jogok rendszerét az alkotmányozó hatalom még alkotmánymódosító eljárással sem tudja semmissé tenni.

Az alapvető jogok korlátozása az állam részéről sok esetben „be nem avatkozással" valósul meg, ami azt jelenti, hogy az állam a saját érdekeit képviselve nem avatkozik bele magán- és jogi személyek egymás közti viszonyába azzal, hogy bármelyik- vagy mindkét fél alapvető jogát korlátozza. Más esetekben az állam tevőleges magatartására van szükség az alapjogok érvényesüléséhez, mely az azonos élethelyzetre vonatkozó normatív rendelkezések megalkotásából, a szervezetrendszerből – amelyet ezen rendelkezések hoznak létre –, és azon hatáskörökből áll, melyek lehetővé teszik alapjogok tartalmának és terjedelmének mérlegelését.

Bizonyos közjogi és magánjogi intézményeket az állam alkotmányos szinten véd, amelynek célja, hogy ezen intézmények törvények által ne semmisülhessenek meg.

Az alapjogok védelme az állam feladata, amely nem csak a megsértésüktől történő tartózkodást, de az érvényesülésükhöz szükséges feltételek megteremtéséből is áll: a szubjektív jogok érvényesülésének összehangolása, az élethelyzetek a maguk komplexitásában történő védelme mind az állam feladata. Az egyéni magatartást szabályozó jogot az állam tudja úgy kialakítani,

6 Gárdos-Orosz: i. m. [18].

hogy az alapjogok biztosításához szükséges jogszabályok és szervezeti feltételek kialakítása oly módon történik, hogy azok a többi alapvető joggal és az állam egyéb alkotmányos feladataival is összhangban van.

Az alapvető jogok érvényesítése esetén az államnak az alkotmánybíróságok által kialakított alapvető jogokra vonatkozó korlátozási rendszernek kell megfeleltetni az alkotmányos normatartalmat. Biztosítani kell az alapvető jogok elsőségének megmaradását oly módon, hogy az állam csak akkor nyúlhat az alapjog korlátozás eszközéhez, amennyiben más alapvető jog és szabadság védelme, vagy egyéb alkotmányos érték védelme sérülne.

1.3. Emberi jogok korlátozása a nemzetközi jogban

Az emberi jogok korlátozásának három szintje van:
- alapjogok, melyek nem korlátozhatók,
- különleges jogrend idején korlátozható vagy felfüggeszthető alapjogok,
- szigorú feltételek mellett bármikor korlátozható alapjogok.

Nemzetközi egyezmények határozzák meg az alapvető emberi jogok korlátozására, módjára és mértékére vonatkozó kritériumokat: formai követelmény a törvényi szabályozás, tartalmi követelmény pedig az arányossági mérce. Formai követelmény, hogy megismerhető, világos és egyértelmű legyen a korlátozás, tartalmi követelmény pedig, hogy csak a közérdekű célok elérése érdekében, csak a szükséges mértékben és az elérni kívánt céllal arányosan történjen a korlátozás.

Az állam a nemzetközi egyezményekben, szerződésekben szereplő egyes jogokat akár állandó jelleggel is korlátozhatja törvénnyel, amennyiben ez megfelel a korlátozásra vonatkozó szabályoknak. Vannak azonban olyan jogok, amelyeket garantálni kell minden esetben, más jogokat pedig szükségállapot idején - bizonyos feltételek mellett – korlátozni lehet.

Nemzetközi bizottságokat és bíróságokat hoznak létre nemzetközi egyezmények, amelyek feladata ellenőrizni, hogy a nemzetközi kötelezettségeket az államok betartják-e, illetve korlátozási teszteket hoznak létre, melyek a korlátozási mércéket pontosítják. Az ENSZ emberi jogi alapegyezményei – a Polgári és Politikai Jogok Nemzetközi Egyezségokmánya (továbbiakban: PPJNE)[7] és a Gazdasági, Szociális és Kulturális Jogok Nemzetközi Egyezségokmánya[8] – elkülönítik az abszolút jogok és tilalmak kategóriáját, melyek a következők:

- az élethez való jog,
- a kínzás, kegyetlen embertelen, megalázó bánásmód tilalma,
- orvosi, tudományos kísérlet végzése az alanyok szabad hozzájárulása nélkül,
- a rabszolgatartás tilalma,
- a szolgaság tilalma,
- a szerződéses kötelezettség teljesítéséért való bebörtönzés tilalma,
- a visszaható hatály tilalma a büntetőjogban,
- az általános jogképesség, valamint
- a gondolat, lelkiismeret és a vallás szabadsága.

Ezen tilalmak Magyarország alkotmányában is abszolút jogoknak számítanak.

A PPJNE szóhasználata szerint szükségállapot idején az alábbi jogoktól el lehet térni:

- kényszer- vagy kötelező munka tilalma,
- a bíróság előtti eljárás egyes garanciális rendelkezései,
- a magánélet védelme,

---

7 1976. évi 8. törvényerejű rendelet az Egyesült Nemzetek Közgyűlése XXI. ülésszakán, 1966. december 16-án elfogadott Polgári és Politikai Jogok Nemzetközi Egyezségokmánya kihirdetéséről, Forrás: https://net.jogtar.hu/jogszabaly?docid=97600008.tvr. Letöltés: 2023.08.04.

8 PPJNE

- a család jogai,
- a gyermekek jogai,
- a törvény előtti egyenlőség,
- kisebbségvédelem.

Az Emberi Jogok Európai Egyezménye (továbbiakban: EJEE) 15. cikke[9] alapján háború esetén vagy a nemzet létét fenyegető más rendkívüli állapot esetén időlegesen el lehet térni az alábbiaktól:

- a kényszer vagy a kötelező munka tilalma,
- bíróság előtti eljárás egyes garanciái,
- családhoz való jog,
- adósságokért való szabadságelvonás tilalma,
- saját állampolgár kiutasításának tilalma,
- hazatérés szabadsága,
- külföldiek kollektív kiutasításnak tilalma,
- szülők iskolaválasztási joga,
- oktatáshoz való jog,
- rendszeres időközönként tartott választások tartásának kötelezettsége.[10]

Az Alaptörvény korábban hatályos 54. cikk (1) bekezdése a kilencedik módosítással megállapított 52. cikk (2) bekezdéssel egyező módon kizárja az alapvető jogok felfüggeszthetőségét vagy általános szintet meghaladó korlátozhatóságát az alábbi esetekben:

- az emberi méltóság és az élethez való jog korlátozása,
- a kínzás,
- az embertelen, megalázó bánásmód vagy büntetés alkalmazása,
- a szolgaság,

9 Emberi Jogok Európai Egyezménye, Forrás: https://www.echr.coe.int/documents/d/echr/convention_hun, Letöltés: 2023.08.04.

10 Gárdos-Orosz: i. m. [27]–[28].

- az emberkereskedelem,
- a beleegyezés nélküli emberkísérlet,
- a fajnemesítés, valamint
- a szervkereskedelem és az emberi klónozás gyakorlata.

Fenntartja:

- az ártatlanság vélelmét
- a védelem jogát a büntetőeljárás minden szakaszára,
- *a nullum crimen sine lege* elvét a nemzetközi és uniós joggal pontosított értelmében, a nemzetközi jog általános elveire is figyelemmel, és
- a kettős elítélés tilalmát.

A PPJNE 4. cikke ehhez képest a következő felsorolásban szereplő alapjogokat sorolja a nem korlátozható alapjogok körébe:

- 6. cikk: az élet védelme,
- 7. cikk: kínzás, kegyetlen, embertelen, megalázó bánásmód tilalma
- 8. cikk: 1. és 2. bekezdés: a rabszolgatartás, rabszolgaság, rabszolga-kereskedelem tilalma,
- 11. cikk: adósrabság tilalma,
- 15. cikk: nullum crimen / nulla poena sine lege.
- 16. cikk: jogképesség,
- 18. cikk: gondolat, lelkiismeret, vallás szabadsága.[11]

„A nemzet létét fenyegető és hivatalosan kihirdetett szükségállapot idején az Egyezségokmányban részes államok az adott helyzet által szigorúan megkövetelt mértékben tehetnek olyan intézkedéseket, amelyek eltérnek az Egyezségokmányban vállalt kötelezettségeiktől, feltéve, hogy az ilyen intézkedések nem állnak ellentétben egyéb nemzetközi jogi kötelezettségeikkel és nem jelentenek kizárólag faj, szín,

11 Till Szabolcs: „Különleges jogrend", Internetes Jogtudományi Enciklopédia (Alkotmányjog rovat, rovatszerkesztő: Bodnár Eszter, Jakab András) https://ijoten.hu/szocikk/kulonleges-jogrend (2019), [52]–[53]., Letöltés: 2023.12.05.

nem, nyelv, vallás vagy társadalmi származás alapján történő megkülönböztetést."[12]

Az EJEE 15. cikk 3. bekezdésében a nem korlátozható alapjogok szűkebb felsorolása található:

- 2. cikk: élethez való jog,
- 3. cikk: kínzás tilalma,
- 4. cikk: rabszolgaság és kényszermunka tilalma,
- 7. cikk: *nullum crimen / nulla poena sine lege*.

Az Alaptörvény I. cikk (3) bekezdése szerinti alapjog-korlátozás teszttől[13] való eltérés lehetősége a három felsorolásban szereplő alapjogok bármelyikére kizárt. Az Alaptörvény kilencedik módosítása szerint megállapított 52. cikk (2) bekezdése szerinti alapjogok felfüggesztése vagy nagyobb mértékű korlátozása csak a további alapjogok esetében értelmezhető.[14]

1.4. Alapjogkorlátozás Magyarországon

2012. január elsején Magyarország új alkotmánya, az Alaptörvény hatályba lépett, mely tartalmazza azon alkotmányosságot vizsgáló módszert, melyet az Alkotmánybíróság alakított ki az Alkotmányban foglaltak értelmezésére vonatkozó normaszöveg hiánya esetén. E mérce alapján az állam akkor korlátozhat alapjogot, amennyiben más alapvető jog és szabadság védelme nem érvényesül, valamint, ha egyéb alkotmányos érték védelme más módon nem érvényesíthető. Mindezek mellett szükséges, hogy a korlátozás megfeleljen az arányosság követelményeinek.

12 PPJNE

13 *„Az alapvető jogokra és kötelezettségekre vonatkozó szabályokat törvény állapítja meg. Alapvető jog más alapvető jog érvényesülése vagy valamely alkotmányos érték védelme érdekében, a feltétlenül szükséges mértékben, az elérni kívánt céllal arányosan, az alapvető jog lényeges tartalmának tiszteletben tartásával korlátozható."*

14 Till: i. m. [53]–[54].

Az Alaptörvény I. cikk (3) így fogalmaz: „*Alapvető jog más alapvető jog érvénysülése vagy valamelyik alkotmányos érték védelme érdekében, a feltétlenül szükséges mértékben, az elérni kívánt céllal arányosan, az alapvető jog lényeges tartalmának tiszteletben tartásával korlátozható.*" Korlátozás esetén a törvényhozó köteles a cél eléréshez legenyhébb eszközt választani.

Az Alaptörvény részletesen szabályozza az alapjogkorlátozás kihirdetését különleges jogrend idején, melyet az alábbiak figyelembevételével kell végrehajtania:

- kihirdetésének lehetséges okát,
- mely szerv jogosult eljárni,
- különleges jogrend határidejét,
- meghatározott garanciákat,
- felhatalmazást ad különleges intézkedések bevezetésére.

Törvény állapíthat meg az alapvető jogokra vonatkozó szabályokat. Ezek a törvények lehetnek egyszerű szótöbbséggel elfogadott törvények, melyekkel az alapjogok korlátozhatók, de az Alaptörvény előírhatja a jelen lévő képviselők kétharmadának szavazati többségét az alapjogkorlátozás bevezetéséhez.[15]

Az Alaptörvény nevesít olyan alapjogokat, amelyek abszolút jellegűek, korlátozhatatlanok, így semelyik más alapjog nem korlátozhatja. Az alaptörvény „Szabadság és felelősség" bekezdése szerint ezek a jogok:

- az élethez való jog,
- az emberi méltósághoz való jog,
- minden ember jogképes,
- a gondolati, lelkiismereti és vallási szabadsághoz való jog (ezek gyakorlása és kinyilvánítása nyilvánosság előtt már korlátozhatóak!),
- a tisztességes eljáráshoz való jog bírósági eljárásokban,

15 Gárdos-Orosz: i. m. [37]–[38].

- kínzás és embertelen bánásmód tilalma,
- ártatlanság vélelme.[16]

A tulajdonhoz való jog korlátozása abban az esetben léphet életbe, amennyiben közérdekből történik, kivételes és törvényben meghatározott esetekben és módon történik és azonnali kártalanítás vonz magával.[17]

1.5. A szükségességi-arányossági teszt

A szükségességi-arányossági teszt az alapvető jogok korlátozásának legelterjedtebb módja. A bíróságok és alkotmánybíróságok ezen vizsgálat alkalmazásával döntik el, hogy alkotmányosnak minősül-e az alapjog korlátozása más alapvető jog vagy alkotmányos érték védelmében.

Európában az elmúlt ötven évben az alapvető jogok korlátozásának legelterjedtebb módja volt, ma már globális mércének tekintendő. A teszt az Európai Unió Bírósága által is használt elem.

A szükségességi-arányossági teszt három lépésből áll, mely elemek mindegyikének teljesülnie kell ahhoz, hogy alkotmányosnak legyen tekinthető a korlátozás. Ehhez az alábbi kérdésekre mindegyikére igennel kell felelni:

- Alkotmányosnak tekinthető jogalkotói céllal jött-e létre a korlátozás?
- Az elérni kívánt cél eléréséhez szükséges-e a korlátozás?
- Az elérni kívánt céllal arányos-e a korlátozás?[18]

Az alapjogvédelem lényeges hatásköröket ad az alkotmánybíróságok és bíróságok kezébe, annak érdekében, hogy eldönthessék, hogy az alapjogkorlátozás alkotmányosnak tekinthető-e.[19]

16 Magyarország Alaptörvénye.
17 Gárdos-Orosz: i. m. [37]–[38].
18 Gárdos-Orosz: i. m. [40]–[43].
19 Gárdos-Orosz: i. m. [51].

2. A különleges jogrend új szabályai

2022. november 1-től az Alaptörvény különleges jogrendi alcíme újraszabályozásra került, s vele egy időben hatályba lépett a 2021. évi XCIII. törvény[20] (továbbiakban: Vbö.), mely a védelmi és biztonsági tevékenységeket hangolja össze, ezzel a védelmi és biztonsági igazgatás elemei egy törvény alatt összefonódnak. Az Alaptörvény 48-56. cikke részletezi az új különleges jogrendi időszakokat, az egyes időszakokra vonatkozó alapjog-korlátozási szabályozást, alkalmazási körét és az alkalmazandó rendkívüli intézkedéseket. Hazánkban a Covid-19 megjelenése óta veszélyhelyzet került kihirdetésre, majd az új veszélyhelyzeti szabályok alkalmazására is sor került az orosz-ukrán háború Magyarországra kiható következményeinek kezelése érdekében.

2.1. Alapjogok korlátozása különleges jogrend idején

Az Alaptörvény 2020. decemberében elfogadott és kihirdetett kilencedik módosítása eredetileg 2023. júliustól lépett volna hatályba, azonban a 2022. június 30-án elfogadott tizedik Alaptörvény-módosítást követően, 2022. november 1-től lépett hatályba az a szabályozás, amelyben a különleges jogrend keretrendszere jelentősen változott. Ezen tartalmi változások bemutatását és összehasonlítását az Alaptörvény kilencedik és tizedik módosításában szereplő, különösen a veszélyhelyzetre vonatkozó rendkívüli intézkedéseken keresztül kívánja véghez vinni a szerző.

A szerző fontosnak tartja tisztázni a különleges jogrend fogalmát: ezen időszak az állam életének olyan része, melynek

20 2021. évi XCIII. törvény a védelmi és biztonsági tevékenységek összehangolásáról, Forrás: https://njt.hu/jogszabaly/2021-93-00-00, Letöltés: 2023.08.05.

során az alaptörvényben meghatározott kritériumok megléte esetén kivételes hatalom, úgynevezett rendeleti kormányzás alkalmazható. Ez magába foglalja a hatályos törvények felfüggeszthetőségét, alkalmazásának korlátozhatóságát vagy ideiglenes megváltoztathatóságát, melynek során a rendeleti kormányzás, valamint az operatív intézkedések bevezethetőek és alkalmazhatóak.

„(…) a különleges jogrend egy olyan társadalmi vagy természeti jelenség kezelésére biztosított állami keretrendszer, amely az állam működésének normális állapotában nem kezelhető, és amely az embereket, az államot vagy az alkotmányos rendet veszélyezteti." [21]

A 2022. november 1-től hatályos Alaptörvény három különleges jogrendi időszakot különböztet meg, melyek a későbbiekben kerülnek bemutatásra.

Az Alaptörvény 52. cikke szerint az Alaptörvény alkalmazása nem függeszthető fel különleges jogrend idején. Az alapvető jogok gyakorlása az abszolút jellegű, korlátozhatatlan jogok kivételével, felfüggeszthetőek vagy korlátozhatóak, amennyiben más alapvető jog érvényesülése vagy valamely alkotmányos érték védelme érdekében, a feltétlenül szükséges mértékben, az elérni kívánt céllal arányosan, az alapvető jog lényeges tartalmának tiszteletben tartásával történik. A Kormány köteles minden olyan intézkedést megtenni, amely az Országgyűlés folyamatos működését szavatolja. Az Alkotmánybíróság működése nem korlátozható, a Kormány köteles minden olyan intézkedést megtenni, amely az Alkotmánybíróság működését szavatolja. A különleges jogrendben alkalmazandó részletes szabályokat sarkalatos törvény határozza meg.[22]

---

21 Csink Lóránt: „Mikor legyen a jogrend különleges?", *Iustum aequum salutare*, XIII. 2017. 4., 8. o.

22 Magyarország Alaptörvénye, 52. cikk.

2.2. A különleges jogrend szabályozása

A Kormány, az Alaptörvény 53. cikke alapján különös jogrendben rendeletet alkothat, mellyel a sarkalatos törvényben meghatározottak szerint felfüggesztheti egyes törvények alkalmazását, törvényi rendelkezésektől eltérhet és egyéb rendkívüli intézkedéseket jogosult bevezetni. A Kormány folyamatosan tájékoztatja a köztársasági elnököt, az Országgyűlés elnökét, valamint az Országgyűlés tárgykör szerinti feladat- és hatáskörrel rendelkező állandó bizottságát a különleges jogrendre vonatkozó szabályok szerint alkotott rendeleteiről. A különleges jogrendre vonatkozó szabályok szerint alkotott rendelet hatályon kívül helyezése az Országgyűlés jogkörébe tartozik, a Kormány értelemszerű korrekciós lehetőségén túl.

A hatályon kívül helyezett rendeletet a Kormány azonos tartalommal nem alkothatja újra, kivéve, ha azt a körülmények jelentős változása indokolja. „*A Kormány az így megalkotott rendeletről és a megalkotásának indokairól haladéktalanul tájékoztatja a köztársasági elnököt, az Országgyűlés elnökét és az Országgyűlés tárgykör szerinti feladat- és hatáskörrel rendelkező állandó bizottságát*."[23] A különleges jogrendet a különleges jogrend kihirdetésére jogosult szerv köteles megszüntetni, amennyiben a kihirdetés feltételei már nem állnak fenn. Míg az Alaptörvény korábbi szövegállapota a veszélyhelyzeti kormányrendeletek időbeli hatályát kötötte az Országgyűlés meghosszabbítási jogához, az új 51. cikk (2) bekezdése szerinti szabályozáson túl a rendeletek hatálya nem korlátozott, annak végső határa a veszélyhelyzethez kötődik. A különleges jogrend ezen esete az alaptörvényi főszabály szerint 30 napig maradhat hatályban, mely a veszélyhelyzet kihirdetése okot adó körülmény fennállása esetén, a Vbö. 82/A.

23 Magyarország Alaptörvénye, 53. cikk (3) bekezdés.

§-a alapján legfeljebb 180 napra – akár ismételhető módon is – meghosszabbítható, amennyiben az Országgyűlés erre felhatalmazza a Kormányt. A különleges jogrendre vonatkozó szabályok a különleges jogrend megszűnésekor hatályukat vesztik.

Az Alaptörvény 52. cikke alapján azonban vannak olyan jogok és általános szabályok, amelyek nem korlátozhatók, változatlan módon érvényesülnek. Ezek a következők: különleges jogrendben az Alaptörvény alkalmazása nem függeszthető fel, az Alkotmánybíróság működése nem korlátozható, a Kormány köteles minden intézkedést megtenni, hogy az Országgyűlés folyamatos működése biztosított legyen, az alapvető jogok gyakorlása az Alaptörvény II., III., és XXVIII. cikk (2)-(6) bekezdésében felsoroltak esetében nem függeszthető fel vagy korlátozható. Ezek a nem korlátozható alapvető jogok a következők:

- az élethez és az emberi méltósághoz való jog,
- a kínzás és az embertelen megalázó elbánás és szolgaságban tartás elleni védelem joga,
- a bírósági eljárásban védelemhez való jog,
- az ártatlanság vélelme, valamint
- a büntetőeljárás alapvető alapjogi elvei.

A különleges jogrendben alkalmazandó részletes szabályok sarkalatos törvényben kerülnek kihirdetésre.

Az Alaptörvényen kívül a következő jogszabályok adják a különleges jogrendi időszak elsődleges jogszabályi alapjait:

- a védelmi és biztonsági tevékenységek összehangolásáról szóló 2021. évi XCIII. törvény, mely kitér a különleges jogrend idején alkalmazandó szabályok átfogó megközelítésének erősítésére, valamint Magyarország és a magyar nemzet védelmére, biztonságának fenntartására, fejlesztésére létrehozott képességek összehangolt és hatékony fejlesztésére, irányítására és működtetésére,

- a honvédelemről és a Magyar Honvédségről szóló 2021. évi CXL. törvény[24], mely a katonai szolgálat és a honvédelem irányításának szintjeit tartalmazza,
- a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény[25] (továbbiakban: Kat.), mely tartalmazza a kiterjedt káresemény megelőzése érdekében, valamint annak bekövetkezése esetén, továbbá a katasztrófa károsító hatása ellen Magyarországon szükséges védekezést,
- 234/2011. (XI.10.) Kormány rendelet[26] a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény végrehajtásáról mely a központi, területi és helyi igazgatási szervek katasztrófák elleni védekezési feladatait szabályozza,
- 402/2022. (X. 24.) Kormány rendelet[27] a polgári védelmi kötelezettségről, mely a polgári védelmi szolgálat ellátására vonatkozó szabályokat tartalmazza,
- Ágazati minisztériumi rendeletek, melyek az irányításuk alá tartozó szervek különleges jogrendbeli feladatait szabályozza.

---

24 2021. évi CXL. törvény a honvédelemről és a Magyar Honvédségről, Forrás: https://njt.hu/jogszabaly/2021-140-00-00, Letöltés: 2023.08.09.

25 2011. évi CXXVIII. törvény a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról, Forrás: https://njt.hu/jogszabaly/2011-128-00-00, Letöltés: 2023.08.05.

26 234/2011. (XI.10.) Kormány rendelet a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény végrehajtásáról, Forrás: https://njt.hu/jogszabaly/2011-234-20-22, Letötés: 2023.08.05.

27 402/2022. (X. 24.) Kormány rendelet a polgári védelmi kötelezettségről, Forrás: https://njt.hu/jogszabaly/2022-402-20-22, Letöltés: 2023.08.05.

2.3 A különleges jogrend alkalmazási köre

A különleges jogrend alkalmasára az állam életének olyan időszakában kerül sor, melyben az Alaptörvényben meghatározott feltételek megléte esetén rendeleti kormányzás gyakorolható.

A 2022.05.25.-2022.07.22. között hatályos Alaptörvény hat különleges jogrendi időszakot különböztet meg, melyek a következőek:

- veszélyhelyzet,
- szükségállapot,
- rendkívüli állapot,
- terrorveszélyhelyzet,
- váratlan támadás,
- megelőző védelmi helyzet.

Az 2023.01.01.-től hatályos Alaptörvény ezzel szemben már csak három különleges jogrendi időszakot határoz meg, melyek a következők:

- hadiállapot,
- szükségállapot,
- veszélyhelyzet.

A következő táblázatban az egyes különleges jogrendek összehasonlítása kerül bemutatásra az Alaptörvény kilencedik módosítását megelőző és követő időállapot alapján.

Különleges jogrendi időszak	Alaptörvény nyolcadik módosításáig	Alaptörvény kilencedik módosítása
Hadiállapot	-	„Az Országgyűlés a háborús helyzet kinyilvánítása vagy háborús veszély, külső fegyveres támadás, hatásában a külső fegyveres támadással egyenértékű cselekmény, valamint ezek közvetlen veszélye, vagy kollektív védelemre irányuló szövetségesi kötelezettség teljesítése esetén hadiállapotot hirdethet ki."[28] A hadiállapot kinyilvánításához, a békekötéshez, valamint a különleges jogrend kihirdetéséhez az országgyűlési képviselők kétharmadának szavazata szükséges.[29] Hadiállapot idején a Kormány gyakorolja az Országgyűlés által átruházott jogokat, valamint dönt a Magyar Honvédség külföldi vagy Magyarországi alkalmazásáról.[30]

28 Magyarország Alaptörvénye kilencedik módosításának 11. cikke szerinti megállapított 49. cikk (1) bekezdés.

29 Magyarország Alaptörvénye kilencedik módosításának 11. cikke szerinti megállapított 49. cikk (2) bekezdés.

30 Magyarország alaptörvénye kilencedik módosításának 11. cikke szerinti megállapított 49. cikk (3) bekezdés.

Szükségállapot	„A törvényes rend megdöntésére vagy a hatalom kizárólagos megszerzésére irányuló fegyveres cselekmény, továbbá az élet- és vagyonbiztonságot tömeges mértékben veszélyeztető, fegyveresen vagy felfegyverkezve elkövetett súlyos, erőszakos események esetén szükségállapotot hirdet ki."[31] Kihirdetéséhez a jelenlévő országgyűlési képviselők 2/3-ára van szükség. A Köztársasági elnök jogosult kinyilvánítani a szükségállapotot, amennyiben az Országgyűlés e döntések meghozatalában akadályoztatva van. Az akadályoztatás tényét, valamint a szükségállapot kihirdetésének indokoltságát az Országgyűlés elnöke, az Alkotmánybíróság elnöke és a miniszterelnök egybehangzóan állapítja meg.[32] Szükségállapot idején a sarkalatos törvényben meghatározott rendkívüli intézkedéseket a	„Az Országgyűlés az alkotmányos rend megdöntésére, felforgatására vagy a hatalom kizárólagos megszerzésére irányuló cselekmény, vagy az élet- és vagyonbiztonságot tömeges mértékben veszélyeztető súlyos, jogellenes cselekmény esetén szükségállapotot hirdet ki."[33] Kihirdetése az országgyűlési képviselők szavazatának 2/3-ával történik, 30 napra hirdethető ki. Az Országgyűlés képviselőinek 2/3-os szavazatával további 30 nappal meghosszabbítható, amennyiben a szükségállapotra okot adó körülmény továbbra is fennáll.[34]

31 Magyarország Alaptörvénye 2022. október 31-ig hatályos 48. cikk (1) bekezdés b) pont.

32 Magyarország Alaptörvénye 2022. október 31-ig hatályos 48. cikk (2)-(5) bekezdés.

33 Magyarország Alaptörvénye kilencedik módosításának 11. cikke szerinti megállapított 50. cikk (1) bekezdés.

34 Magyarország Alaptörvénye kilencedik. módosításának 11. cikke szerinti megállapított 50. cikk (2)-(3) bekezdés.

	köztársasági elnök rendeleti úton vezeti be. A köztársasági elnök rendeletével, a sarkalatos törvényben meghatározottak szerint, egyes törvények alkalmazását felfüggesztheti, törvényi rendelkezésektől eltérhet, valamint egyéb rendkívüli intézkedéseket vezethet be. A bevezetett rendkívüli intézkedésekről a köztársasági elnök haladéktalanul tájékoztatja az Országgyűlés elnökét. A rendeleti úton bevezetett rendkívüli intézkedések 30 napig maradnak hatályban, azonban az Országgyűlés döntésével meghosszabbítható. A köztársasági elnök rendelete a szükségállapot megszűnésével hatályát veszti.[35]	
Veszélyhelyzet	„A Kormány szomszédos országban fennálló fegyveres konfliktus, háborús helyzet vagy humanitárius katasztrófa, továbbá az élet- és vagyonbiztonságot veszélyeztető elemi csapás vagy ipari szerencsétlenség esetén, valamint ezek következményeinek az elhárítása érdekében veszélyhelyzetet hirdet ki, és sarkalatos törvényben meghatározott	„A Kormány a szomszédos országban fennálló fegyveres konfliktus, háborús helyzet vagy humanitárius katasztrófa, továbbá az élet- és vagyonbiztonságot veszélyeztető súlyos esemény – különösen elemi csapás vagy ipari szerencsétlenség – esetén, valamint ezek következményeinek az elhárítása érdekében veszélyhelyzetet hirdet ki.”[36]

35 Magyarország Alaptörvénye 2022. október 31-ig hatályos 50. cikk (2)-(6) bek.

36 Magyarország Alaptörvénye kilencedik módosításának 11. cikke szerinti megállapított 51. cikk (1) bekezdés.

	rendkívüli intézkedéseket vezethet be."[37] „A Kormány veszélyhelyzetben rendeletet alkothat, amellyel a sarkalatos törvényben meghatározottak szerint, egyes törvények alkalmazását felfüggesztheti, törvényi rendelkezésektől eltérhet, valamint egyéb rendkívüli intézkedéseket hozhat." A kormány ezen rendelete 15 napig marad hatályban, azonban az Országgyűlés felhatalmazása alapján a Kormány a rendelet hatályát meghosszabbíthatja. A veszélyhelyzet megszűntével a Kormány rendelete hatályát veszti.[38]	30 napra hirdethető ki, az Országgyűlés felhatalmazása alapján a Kormány meghosszabbíthatja a jelenlévő országgyűlési képviselők 2/3-ának szavazatával, ha a veszélyhelyzetre okot adó körülmény továbbra is fennáll.[39]
Terrorveszélyhelyzet	„Az Országgyűlés a Kormány kezdeményezésére terrortámadás jelentős és közvetlen veszélye vagy terrortámadás esetén meghatározott időre kihirdeti a terrorveszélyhelyzetet, ezzel egyidejűleg felhatalmazza a Kormányt sarkalatos törvényben meghatározott rendkívüli intézkedések bevezetésére."[40]	-

37 Magyarország Alaptörvénye tizedik módosításának 1. cikkével megállapított, 2022. október 31-ig hatályos 53. cikk (1) bekezdés.

38 Magyarország Alaptörvénye 2022. október 31-ig hatályos 53. cikk (2)-(4) bekezdés.

39 Magyarország Alaptörvénye kilencedik módosításának 11. cikke szerinti megállapított 51. cikk (2)-(4) bekezdés.

40 Magyarország Alaptörvénye 2022. október 31-ig hatályos 51/A. cikk (1) bek.

	Kihirdetéséhez és meghosszabbításához az a jelenlévő országgyűlési képviselők szavazatának 2/3-a szükséges. A Kormány által bevezetett rendkívüli intézkedések hatálya az Országgyűlés terrorveszélyhelyzet kihirdetésére vonatkozó döntéséig, de legfeljebb 15 napig tart. „A Kormány veszélyhelyzetben rendeletet alkothat, amelylyel a sarkalatos törvényben meghatározottak szerint, egyes törvények alkalmazását felfüggesztheti, törvényi rendelkezésektől eltérhet, valamint egyéb rendkívüli intézkedéseket hozhat. A Kormány rendelete a terrorveszélyhelyzet megszűnésével hatályát veszti."[41]	-
Váratlan támadás	„A Kormány külső fegyveres csoportoknak Magyarország területére történő váratlan betörése esetén a támadás elhárítására, Magyarország területének honi és szövetséges légvédelmi és repülő készültségi erőkkel való oltalmazására, a törvényes rend, az élet- és vagyonbiztonság, a közrend és a közbiztonság védelme érdekében – szükség esetén a köztársasági elnök által jóváhagyott fegyveres	-

41 Magyarország Alaptörvénye 2022. október 31-ig hatályos 51/A. cikk (2)-(6) bekezdés.

	védelmi terv szerint – a szükségállapot vagy a rendkívüli állapot kihirdetésére vonatkozó döntésig a támadással arányos és arra felkészített erőkkel azonnal intézkedni köteles."[42] „A Kormány a megtett intézkedéseiről haladéktalanul tájékoztatja az Országgyűlést és a köztársasági elnököt. A Kormány a váratlan támadás esetén rendeletet alkothat, amellyel a sarkalatos törvényben meghatározottak szerint, egyes törvények alkalmazását felfüggesztheti, törvényi rendelkezésektől eltérhet, valamint egyéb rendkívüli intézkedéseket hozhat. A Kormány rendelete a váratlan támadás megszűnésével hatályát veszti."[43]	
Megelőző védelmi helyzet	„Az Országgyűlés külső fegyveres támadás veszélye esetén vagy szövetségesi kötelezettség teljesítése érdekében meghatározott időre kihirdeti a megelőző védelmi helyzetet, ezzel egyidejűleg felhatalmazza a Kormányt sarkalatos törvényben meghatározott rendkívüli intéz-	

42 Magyarország Alaptörvénye 2022. október 31-ig hatályos 52. cikk (1) bekezdés.

43 Magyarország Alaptörvénye 2022. október 31-ig hatályos 52. cikk (2)-(4) bekezdés.

	kedések bevezetésére. A megelőző védelmi helyzet időtartama meghosszabbítható."[44] Kihirdetéséhez a jelenlévő országgyűlési képviselők 2/3-ának szavazata szükséges. A Kormány rendeletben bevezetett intézkedéseinek hatálya az Országgyűlés megelőző védelmi helyzet kihirdetésére vonatkozó döntéséig, de legfeljebb 60 napig tart.[45] „A Kormány a megelőző védelmi helyzet esetén rendeletet alkothat, amellyel a sarkalatos törvényben meghatározottak szerint, egyes törvények alkalmazását felfüggesztheti, törvényi rendelkezésektől eltérhet, valamint egyéb rendkívüli intézkedéseket hozhat. A Kormány rendelete a megelőző védelmi helyzet megszűnésével hatályát veszti."[46]	
Rendkívüli állapot	„Az Országgyűlés hadiállapot vagy idegen hatalom fegyveres támadásának közvetlen veszélye (háborús veszély) esetén kihirdeti a	-

44 Magyarország Alaptörvénye 2022. október 31-ig hatályos 51. cikk (1) bekezdés.

45 Magyarország Alaptörvénye 2022. október 31-ig hatályos 51. cikk (2)-(3) bekezdés.

46 Magyarország Alaptörvénye 2022. október 31-ig hatályos 51. cikk (4)-(5) bekezdés.

	rendkívüli állapotot, és Honvédelmi Tanácsot hoz létre."[47] Az országgyűlési képviselők szavazatának 2/3-a szükséges kihirdetéséhez. Kihirdetésére a köztársasági elnök jogosult, amennyiben az Országgyűlés e döntés meghozatalában akadályoztatva van. Az akadályoztatás tényét, valamint a rendkívüli állapot kihirdetésének indokoltságát az Országgyűlés elnöke, az Alkotmánybíróság elnöke és a miniszterelnök egybehangzóan állapítja meg.[48] „A Honvédelmi Tanács elnöke a köztársasági elnök, tagjai az Országgyűlés elnöke, az országgyűlési képviselőcsoportok vezetői, a miniszterelnök, a miniszterek és a Honvéd Vezérkar főnöke. A Honvédelmi Tanács gyakorolja az Országgyűlés által rá ruházott jogokat, a köztársasági elnök jogait, a Kormány jogait. A Honvédelmi Tanács dönt a Magyar Honvédség külföldi vagy magyarországi alkalmazásáról, békefenntartásban való	

47 Magyarország Alaptörvénye 2022. október 31-ig hatályos 48. cikk (1) bekezdés a) pont.

48 Magyarország Alaptörvénye 2022. október 31-ig hatályos 48. cikk (2)-(5) bekezdés.

	részvételéről, a külföldi fegyveres erők magyarországi vagy Magyarország területéről kiinduló alkalmazásáról, illetve magyarországi állomásoztatásáról, valamint a sarkalatos törvényben meghatározott rendkívüli intézkedések bevezetéséről. A Honvédelmi Tanács rendeletet alkothat, amelylyel a sarkalatos törvényben meghatározottak szerint, egyes törvények alkalmazását felfüggesztheti, törvényi rendelkezésektől eltérhet, valamint egyéb rendkívüli intézkedéseket hozhat. A Honvédelmi Tanács rendelete a rendkívüli állapot megszűnésével hatályát veszti, kivéve ha az Országgyűlés a rendelet hatályát meghosszabbítja."[49]	

További jelentős változás, hogy az Alaptörvény tizedik módosítása az 53. cikk (1) bekezdésében „A Kormány az élet- és vagyonbiztonságot veszélyeztető elemi csapás" szövegrész helyébe az „A Kormány szomszédos országban fennálló fegyveres konfliktus, háborús helyzet vagy humanitárius katasztrófa, továbbá az élet- és vagyonbiztonságot veszélyeztető elemi csapás" szöveget léptette.

[49] Magyarország Alaptörvénye 2022. október 31-ig hatályos módosítás 49. cikk (1)-(5) bekezdés.

2.4. A veszélyhelyzet esetén alkalmazható rendkívüli intézkedéseink főbb tartalma

Az Alaptörvény kilencedik módosításával 2020. decemberében az Országgyűlés által elfogadott és kihirdetett, a tizedik Alaptörvény-módosítás alapján 2022. november 1-től hatályos alkotmányos szabályozás szerint vizsgálja a szerző a veszélyhelyzetre vonatkozó szabályokat. A Kormány – az Országgyűlés és a köztársasági elnök haladéktalan tájékoztatása mellett – rendeleti úton történő kormányzást vezet be. A bevezetőben már említésre került, de itt is fontos kiemelni, hogy a rendeleti kormányzás 30 napig marad hatályban, azonban az Országgyűlés felhatalmazása alapján a Kormány meghosszabbíthatja azt alkalmanként 180 nappal. A Kormány rendelete hatályát veszti a veszélyhelyzet megszűnésével.

A rendkívüli intézkedések főbb tartalmát a Vbö. 80. §-a foglalja magába, mely szerint az alábbi intézkedések vezethetőek be:

§ hadiállapot, szükségállapot vagy veszélyhelyzet idején a Kormány elrendelheti egyes törvények alkalmazásának felfüggesztését, eltérhet törvényi rendelkezésektől, illetve egyéb rendkívüli intézkedéseket vezethet be az állampolgárok életének-, egészségének, személyi, vagyon- és jogbiztonságának, valamint a nemzetgazdaság stabilitásának garantálása érdekében.

§ hadiállapot, szükségállapot vagy veszélyhelyzet idején a Kormány hatáskörét a személyes szabadsággal és az életkörülményekkel összefüggésben, a gazdaság- és ellátásbiztonsággal összefüggésben, a közösségeket érintő biztonsági célú korlátozásokkal és lakossági tájékoztatásával összefüggésben, a törvényes rend, a közrend és a közbiztonság megóvásával összefüggésben, az állami és önkormányzati működéssel összefüggésben, illetve az országvédelemmel és az országmoz-

gósítással összefüggésben, a veszélyhelyzetet kiváltó esemény megelőzésével, felszámolásával, további káros hatásainak megelőzésével és elhárításával kapcsolatban szabályozási tárgykörben gyakorolhatja.

§ hadiállapot, szükségállapot vagy veszélyhelyzet idején a Kormány, a kiváltó eseményhez igazodó szükséges mértékben, az elérni kívánt céllal arányos mértékben gyakorolhatja az első pontban említett hatáskörét.

§ a Kormány a hadiállapot vagy szükségállapot kihirdetésének kezdeményezését követően egyes törvények alkalmazását felfüggesztheti, törvényi rendelkezésektől eltérhet és egyéb rendkívüli intézkedéseket hozhat a veszélyhelyzetet kiváltó eseményhez igazodó szükséges mértékben, az elérni kívánt céllal arányosan. *A Kormány ezen jogát kizárólag olyan intézkedések bevezetésével összefüggésben gyakorolhatja, melyek az azonnali reagálás érdekében, a kezelendő fenyegetéshez igazodómértékben szükségesek és arányosak*.[50] Az intézkedéseknek a kezelendő fenyegetéshez igazodó mértékűnek és arányosnak kell lennie.

§ különleges jogrendben az alapvető jogok kizárólag akkor függeszthetőek fel, amennyiben az alapvető jogok korlátozása nem elégséges az elérni kívánt célhoz és a különleges jogrendet kiváltó esemény megelőzése, felszámolása, kezelése, káros hatásainak megelőzése illetve elhárítása más módon nem garantálható.

§ amennyiben az alapvető jogok korlátozása, felfüggesztése nem indokolt, a Kormány köteles haladéktalanul megszüntetni a korlátozást vagy felfüggesztést.

§ a rendkívüli intézkedések bevezetéséről szóló rendeletet a lineáris műsorszolgáltatók hírműsoraiban, napilapokban, internetes hírmegosztó portálokon, valamint hirdetmény útján

50 Vbö. 80. §.

az aláírás napján kihirdethető. Ha a kihirdetés akadályba ütközik, a rendvédelmi szervek és a Magyar Honvédség technikai eszközeinek igénybevételével kihirdethetőek.

3. A Covid-19 járvány alatt történt alapjogkorlátozás

A Covid-19 hazánkban történő megjelenésével teljesen új időszak vette kezdetét a szinte folyamatosan kihirdetett veszélyhelyzetnek köszönhetően. Ez a fejezet részletezi a különleges jogrendi alapjogkorlátozás időtartamára vonatkozó szabályokat, az alapjogkorlátozás megközelítési lehetőségeit, az alkotmánybírósági gyakorlatot, az alapjogkorlátozás jövőbeni lehetőségeit, a különleges jogrend jogi garanciáit, a bírói attitűdöt, valamint a politikai kontrollt.

3.1. A különleges jogrendi időszakok korlátjai

A Covid-19 járványt megelőzően a szakemberek döntő részének véleménye az volt, hogy a különleges jogrendi időszak csak rövid ideig tart. A járvány vissza-visszatérő hulláma, majd az Ukrajnában dúló háború azonban huzamosan fennálló különleges jogrendi állapotot teremtettek. A társadalmat vizsgálva láthatjuk, hogy hatalmas jelentősége van annak, hogy az alapjog korlátozás hosszú vagy rövid ideig tart: a kisebb mértékű, ám hosszan tartó korlátozás esetén az emberek hajlamosak a biztonságukért többet áldozni.[51]

A különleges jogrendi korlátozás alatt az alábbi horizontális értékelési szempontok kerülnek alkalmazásra:

- az ok,
- kihirdetésre jogosult,

51 Csink: i. m. 5–6. o.

- szervezeti működés folyamatosságának hiánya esetén a helyettesítő döntéshozó,
- az eredmény,
- a békétől való eltérés szabályozhatósági felhatalmazása,
- a döntések időbeli hatálya, meghosszabbíthatósága,
- különleges jogrendi időszak korlátja,
- Alaptörvény és Alkotmánybíróság érinthetetlensége.[52]

3.2. A különleges jogrendi alapjogkorlátozás megközelítései

Három féle lehetséges megközelítést ismerünk, mely alapján az alapjogok korlátozása bevezethető. Az első lehetőség, mely szerint a különleges jogrend idején bárminemű korlátozás megengedett, mivel maga a normaszöveg is felfüggesztésről, általános mértéken túli korlátozásról szól. Másik lehetőség, hogy a már előzőekben említett általános tesztet szükséges kiindulópontnak tekinteni, mivel a súlyos alapjogi korlátozások különleges jogrend idején is alkotmányosak lehetnek. Harmadik lehetőség pedig egy, a különleges jogrend idejére kialakított teszt, melyben kötve van a rendeleti jogalkotó keze, nincs lehetőség az alapjogok felfüggesztésére, azonban a mércéje nem azonos az általános teszttel.[53]

3.3. Alapjogkorlátozásra vonatkozó alkotmánybírósági gyakorlat különleges jogrend idején

Az Alaptörvényben leírt alapjog korlátozás alkotmánybírósági értelmezését a 15/2021.(V.13.) AB határozat (továbbiakban:

52 Till: i. m. 17. o.
53 Csink: i. m. 6. o.

ABh1)[54] és a 23/2021.(VII.13.) AB határozat (továbbiakban: ABh2)[55] szemlélteti.

Az ABh1 volt az egyik legelső, alapjogkorlátozás lehetőségét elemző határozat különleges jogrend idején. Az Alkotmánybíróság egy országgyűlési képviselő indítványára vizsgálta a veszélyhelyzeti rendeletet, melyben kétszer 45 napra hosszabbították a közérdekű adat igénylésére vonatkozó határidőt.

Az ABh1-nek két kérdést kellett megválaszolni, mielőtt az érdemi vizsgálat megkezdődhetett volna:

1. Korlátozza-e az információszabadságot a norma, mely a határidővel kapcsolatos szabályt állapítja meg?
2. Az Alaptörvény 54. cikk (1) bekezdése lehetővé teszi-e, hogy az alapjog korlátozás felülvizsgálata megtörténjen?

Mindkét kérdésre igen volt a válasz. Az első kérdéssel kapcsolatban kimondta, hogy a közérdekű adat megismeréséhez való jog esetében az időszerűség a lényeges kérdés. Az idő múlásával az információk java része aktualitását veszti, így nem vagy csak kis mértékben képes a véleményformáláshoz hozzájárulni. Az Alaptörvényből nem derül ki rögzített határidő, de egyértelmű, hogy a hosszú válaszadási határidő a közérdekű adatigénylés célját ellehetetlenítené.

---

54 15/2021.(V.13.) AB határozat a veszélyhelyzet idején az egyes adatigénylési rendelkezésektől való eltérésről szóló 521/2020. (XI.25.) Korm. rendelet 1. § (3)-(5) bekezdéseire vonatkozó alkotmányos követelmény megállapításáról, Forrás: https://njt.hu/jogszabaly/2021-15-30-75, letöltés: 2023.08.04.

55 23/2021.(VII.13.) AB határozat a veszélyhelyzet idején alkalmazandó védelmi intézkedések második üteméről szóló 484/2020.(XI.10.) Korm. rendelet egyes rendelkezései alaptörvény-ellenességének megállapítására és megsemmisítésére irányuló alkotmányjogi panasz elutasításáról és alkotmányos követelmény megállapításáról, Forrás: https://net.jogtar.hu/jogszabaly?docid=a21h0023.ab, letöltés: 2023.08.04.

Az alapjog különleges jogrendi korlátozásának tartalmi vizsgálatára pedig azért volt szükség, mert az információszabadság nem szerepel az Alaptörvényben az érinthetetlen jogok között, ily módon akár úgy is értelmezhető, hogy az alapjog felfüggeszthető, tehát az alkotmányossági vizsgálat kizárt. Az Alkotmánybíróság kimondta, hogy az alkotmányozónak nem volt célja a különleges jogrendi jogalkotót felhatalmazni arra, hogy összse nem függő alapjog korlátozást vezessen be a veszélyhelyzet leküzdésére, valamint arra sem, hogy egyes alapjogokat jobban korlátozzon, mint amennyire a rendkívüli körülmény szükségessé teszi azt.

Az ABh1 tehát kimondja, hogy az Alaptörvényből nem következik, hogy az összes alapjog felfüggeszthető lenne veszélyhelyzetben, az emberi élet, a kínzás tilalma, az emberi méltósághoz való jog és a büntetőjogi garanciák kivételével. Az Alkotmánybíróság az információkorlátozást az általános alapjogi teszt alapján vizsgálta, melynek során vizsgálta, hogy a korlátozás szükséges és arányos-e, és hogy van-e legitim célja.[56]

Az ABh2 egy egyedi ügyben vizsgálta, hogy a különleges jogrend idejére elrendelt gyülekezési tilalom összhangban van-e az alaptörvényben benne foglalt gyülekezés szabadságát deklaráló cikkével. Bár a járvány terjedésének megakadályozására jött létre a korlátozás, mégsem volt semmiféle járványügyi kockázata az egyedi ügyben tartott gyülekezésnek a kezdeményező szerint. A többségi határozat szerint a gyülekezési jog gyakorlása emberek egy térben, azonos időben történő jelenlétét feltételezi, mely járványügyi kockázatot rejt. Mivel előre nem jósolható meg a gyülekezők létszáma – az esetlegesen újonnan csatlakozók miatt –, így a gyülekező személyek számával a járványügyi kockázat is növekszik. Ennek alapján egy kis létszámmal bejelentett gyülekezés is könnyen tömegrendezvénnyé válhat.

56 Csink: i. m. 7–8. o.

A Covid-19 járvány idején elrendelt *„kijárási tilalom intézménye, a lakosság utcán vagy más nyilvános helyen tartózkodásának tilalmaként került bevezetésre, nem pedig a gyülekezési jog felfüggesztéseként”*.[57]

Folyamatosan figyelemmel kell kísérni a veszélyhelyzeti jogalkotónak, hogy az alapjogok felfüggesztése valóban indokolt-e az elérni kívánt céllal, valamint vizsgálni kell, hogy a veszélyhelyzetre okot adó körülmény az alapjogkorlátozást igazolja-e, majd visszatérően dönteni kell, hogy a körülmények indokolttá teszik-e az alapjog felfüggesztést.

Bár ABh1 és ABh2 is elfogadja, hogy van mércéje az alapjog korlátozásnak, a különbség a teszt, amit alkalmaznak: ABh1 szükségességi-arányossági vizsgálatot alkalmazott, míg ABh2 a tartalom és szükségesség mellett a korlátozás időbeliségének hangsúlyozására törekedett.[58]

3.4. Bírói attitűd különleges jogrendben

Az Alkotmánybíróság működését a jogi környezet mellett közéleti szempontok is befolyásolják. Ilyenek például a bírói döntések magyarázatára létrehozott modellek. Az egyik egy stratégiai modell, mely szerint a bírót több tényező befolyásolja döntésében:

- saját preferenciái,
- belső döntéshozatali mechanizmus,
- külső, politikai környezet.

A különleges jogrend, atipikus, szokatlan jelenség, mely az államot, az alkotmányos rendet, az élet- és vagyonbiztonságot fenyegeti s melyben a különleges jogrend leküzdése politikai kormányzati felelősség, a szabályozás alkotmányosságáért pedig az Alkotmánybíróság felel. A különleges jogrendi intézkedések megsemmisítése különösen nehéz feladat, hiszen kialakulhat olyan

57 Till: i. m. [55].
58 Csink: i. m. 8. o.

kommunikáció, mely az Alkotmánybíróságot fogja okolni egy esetleges sikertelenségért vagy a nem hatékony intézkedésekért.[59]

3.5 Politikai kontroll

Különleges jogrend idején a végrehajtó hatalom megerősítése általánosan bevett szokás. Addig tekinthető demokratikusnak a hatalom megerősítése, míg a hatalom birtokosa számot tud adni, tehát feltételt tud teremteni annak, hogy ő, a hatalom birtokosa felelősségre vonható legyen.

Parlamentáris országokban a kormány a parlamentnek felel, legyen szó normál időszaki vagy különleges jogrendi kormányzásról. A parlamenti viták amennyiben nem lefolytathatóak különleges jogrend idején, úgy meg kell teremteni a lehetőséget, hogy az Országgyűlés ellenőrzési joga megmaradhasson. Mivel a kormánypárti képviselők többségben vannak a parlamentben, így meg kell teremteni egy olyan gyakorlat lehetőségét, melynek során a többség nem tudja akadályozni az ellenőrzési jogkörök gyakorlását.

A politikai kontroll két legjelentősebb fegyvere a nyilvánosság és a parlamenti ellenőrzés. Veszélyhelyzetben felértékelődik a társadalomban zajló párbeszédek fontossága, mely értelemszerűen korlátozható, de célszerű lenne a különleges jogrend megszűnése utáni nyilvános tájékoztatás a kormányzat részéről, a meghozott döntések céljáról, okáról és eredményéről.[60]

3.6 A különleges jogrend jogi garanciái

Az Alaptörvény kimondja, hogy az Alaptörvény alkalmazása különleges jogrend idején sem függeszthető fel, valamint az Alkotmánybíróság működése sem korlátozható. Ez alapján az

[59] Csink: i. m. 12. o.
[60] Csink: i. m. 13. o.

Alaptörvény az Alkotmánybíróságot garanciának szánja, mely a különleges jogrendi intézkedéseket hivatott felülvizsgálni. Különleges jogrend idején még hatványozottabban fontos az alkotmánybírósági jogvédelem, hiszen mint a rendkívüli hatáskör jogosultjának, mind az egyéneknek érdeke, hogy a rendkívüli intézkedés alkotmányosságára vonatkozó döntés megválaszolásra kerüljön.

A különleges jogrend idején hozott jogszabályokat és egyedi intézkedéseket az Alkotmánybíróság egyéb hatáskörén belül vizsgálja, melyek közül a legjellemzőbb hatáskör az alkotmányjogi panasz, a közvetlen panasz – mely a különleges jogrendi intézkedés érdekében hozott jogszabály hatályosulása folytán következik be –, és az utólagos normakontroll.

Az alkotmánybírósági döntés időbelisége kritikus pont a különleges jogrendben: az egyedi körülmények rendkívül gyors intézkedést kívánhatnak meg, gyakran változó szabályozási környezetben.

Vannak esetek, melyen során létezik határidő az indítvány elbírálására. Ilyen esetek:

- az Alaptörvény által megállapított határidő az előzetes normakontrollra (6. cikk (6), (8) bekezdés),
- az Alaptörvény módosításának felülvizsgálata (24. cikk (6) bekezdés),
- a népszavazás elrendelésével szembeni felülvizsgálat (2011. évi CLI. törvény (továbbiakban: Abtv.) 33 § (1) bekezdés[61]).[62]

3.7 A jelenben és a jövőben történő alapjogkorlátozás lehetősége különleges jogrendben

A különleges jogrend alkotmányhoz kötött hatalom, tehát csak alkotmányos keretek között valósulhat meg bármilyen nemű

61 2011. évi CLI. törvény az Alkotmánybíróságról, Forrás: https://njt.hu/jogszabaly/2011-151-00-00, letöltés: 2023.08.04.

62 Csink: i. m. 10–12. o.

intézkedés. A korlátlan vagy ellenőrizhetetlen hatalom ellentétes az Alaptörvény eszméjével, tehát a különleges jogrendi intézkedések megtétele is mérlegelhető. Ebből kifolyólag a különleges jogrend kereteit rögzíteni kell, hogy ne történhessen meg hatalommal való visszaélés. Az Alaptörvény kilencedik módosításában már látható, hogy a jogalkotó a hatalom féken tartásának érdekében a szabályozás részletezését látta megoldásnak, mely alapján az egyéni szabadságjogok akkor érvényesülnek, ha a különleges jogrendi szabályok pontosan meghatározzák a bevezethető intézkedések idejét és a bevezetést kezdeményező kilétét. Összességében a szabályozás egyszerűsödése nagyobb mozgásteret ad a különleges jogrendi hatalomnak.[63]

4. Összefoglalás

Az állam abban az esetben korlátozhat alapjogot, amennyiben más alapvető jog és szabadság védelme nem érvényesül, valamint, ha egyéb alkotmányos érték védelme más módon nem érvényesíthető. Az Alaptörvény szerint „*alapvető jog más alapvető jog érvényesülése vagy valamelyik alkotmányos érték védelme érdekében, a feltétlenül szükséges mértékben, az elérni kívánt céllal arányosan, az alapvető jog lényeges tartalmának tiszteletben tartásával korlátozható*". Az alapvető jogokra vonatkozó szabályokat egyszerű szótöbbséggel elfogadott törvények, valamint a jelenlévő képviselők kétharmadának szavazati többségével elfogadott törvények állapíthat meg. A szükségességi-arányossági teszt az alapvető jogok korlátozásának legelterjedtebb módja, melynek segítségével bíróságok és az Alkotmánybíróság dönti el, hogy alkotmányosnak minősül-e az alapjog korlátozás más alapvető jog vagy érték védelmében.

63 Csink: i. m. 9. o.

A szerző részletesen bemutatja a 2022. november 1-től hatályos Alaptörvény, valamint a vele egy időben életbe lépett Vbö. által szabályozott különleges jogrendi időszakokat, az egyes időszakokra vonatkozó alapjog korlátozásokat, valamint a veszélyhelyzet estén alkalmazandó rendkívüli intézkedéseket. Az Alaptörvény kilencedik módosítását megelőző és követő szövegváltozatának összehasonlítása a 6-ról 3-ra redukálódott különleges jogrendi időszakokat illetően, táblázatos formában történik, kiegészítve a tizedik módosítás hozta változással. A szerző véleménye szerint a Vbö. létrehozása előrelépés volt a „szétaprózódott" védelmi igazgatás alapját adó törvények, kormányrendeletek összekovácsolásában, azonban a törvény végrehajtási rendeletei nem egy időben jelentek meg magával a törvénnyel, így egyes részei egy ideig lefedetlenek, szabályozatlanok voltak. Legfontosabb változásként az Alaptörvénybe bekerült a veszélyhelyzet kihirdetésének okai közé a szomszédos országban fennálló fegyveres konfliktus, háborús veszélyhelyzet, humanitárius katasztrófa, illetve a veszélyhelyzet 30 napra történő kihirdetésének lehetősége, mely a Vbö. alapján 180 nappal hosszabbítható.

A Covid-19 járvány hazánkban történő megjelenésével teljesen új időszak vette kezdetét, köszönhetően a folyamatosan kihirdetett veszélyhelyzetnek. A különleges jogrend bevezetésének feltétele az államot, vagy az élet-, és vagyonbiztonságot fenyegető veszély fennállása, alaptörvényi feltétele pedig az alkotmányos keretek megtartása. Ez a veszély ugyanakkor nem tekinthető abszolútnak, más alkotmányos jogokhoz és értékekhez viszonyítása szükséges, így az alkotmányossági vizsgálat során az arányosság – mint az egyik lefontosabb tényező –, nem tekinthető eleve igazoltnak. A különleges jogrendnek nem célja önmagában a szabadságjogok felfüggesztése, csupán eszközként jelenik meg. A különleges jogrend bevezetésének Alaptörvényben meghatározott céljával összhangban kell lenni a különleges

jogrendben alkotott jogszabály korlátozó intézkedés céljának. A különleges jogrend bevezetés azonban nem jár automatikusan az alapvető jogok korlátozásával. Az alapjogok korlátozására három féle lehetséges megközelítést ismerünk: első lehetőség a különleges jogrend idején megengedett bárminemű korlátozás, második lehetőség az általános teszt kiindulópontnak tekintésre, – mivel a súlyos alapjogi korlátozások különleges jogrend idején is alkotmányosak lehetnek -, valamint harmadik lehetőség egy, a különleges jogrend idejére kialakított teszt, melyben kötve van a rendeleti jogalkotó keze és nincs lehetőség az alapjogok felfüggesztésére, azonban a mércéje nem azonos az általános teszttel.

A szerző az egyik legfontosabb kérdésnek a különleges jogrend bevezetésének és vele együtt az alapjogok korlátozásának indokoltságát tartja. Till Szabolcs és Csink Lóránt szavaival egyetértve: *„Az Alkotmánybíróságnak nincs lehetősége annak vizsgálatára, hogy célszerű-e bevezetni a különleges jogrendet, vagy van-e más lehetőség az államot, alkotmányos rendet fenyegető veszély elhárítására. Még csak azt sem kell vizsgálnia, hogy a különleges jogrend bevezetése a legenyhébb eszköz-e, azaz különleges jogrend bevezetése nélkül van-e lehetőség a veszély leküzdésére. A legenyhébb eszköz ugyanis az alapjogkorlátozással szemben támasztott követelmény, a különleges jogrend bevezetése pedig önmagában nem korlátoz alapjogot."*[64] Ebből kifolyólag elmondható, hogy a különleges jogrend bevezetése nem csupán politikai döntés, hanem politikailag befolyásolt jogi döntés, melynek felülvizsgálata során az Alkotmánybíróság feladata eldönteni, hogy a bevezetés alaptörvényi feltételei fennállnak-e.

64 Csink Lóránt: A különleges jogrend bevezetésének alkotmányjogi megközelítése, Védelmi-Biztonsági Szabályozási és Kormányzástani Műhelytanulmányok, 2023/3., Nemzeti Közszolgálati Egyetem Védelmi-Biztonsági Szabályozási és Kormányzástani Kutatóműhely, Budapest, 2023. ISSN: 2786-2283, 9. o.

Különleges jogrend bevezetésénél az alaptörvényi feltételek megléte vizsgálható, azonban a politikai célszerűsége nem, ily módon az Alkotmánybíróság mozgástere igencsak lecsökken. Ezzel szemben a különleges jogrend idején bevezetett intézkedések – amennyiben alapjogokat érintenek –, célszerűségi és arányossági kérdésként vannak jelen, így felülvizsgálatuk indokolt. Az elmúlt évek különleges jogrendben eltelt időszaka, illetve az elkövetkezendő békeidő minél jobban egybecsúszik, annál inkább a különleges jogrend folyamatába épített garanciák fognak hangsúlyossá válni.[65]

Jogszabályok

Magyarország Alaptörvénye
Magyarország Alaptörvényének kilencedik módosítása (Hatályos: 2022.11.01.-)
Magyarország Alaptörvényének tizedik módosítása (Hatályos: részben 2022.05.25.- 2022.10.31.)
2021. évi XCIII. törvény a védelmi és biztonsági tevékenységek összehangolásáról
2021. évi CXL. törvény a honvédelemről és a Magyar Honvédségről
2011. évi CXXVIII. törvény a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról
2011. évi CLI. törvény az Alkotmánybíróságról
1976. évi 8. törvényerejű rendelet az Egyesült Nemzetek Közgyűlése XXI. ülésszakán, 1966. december 16-án elfogadott Polgári és Politikai Jogok Nemzetközi Egyezségokmánya kihirdetéséről.

65 Csink: i. m. (2023) 9–13. o.

1976. évi 9. törvényerejű rendelet az Egyesült Nemzetek Közgyűlése XXI: ülésszakán, 1966. december 16-án elfogadott Gazdasági, Szociális és Kulturális Jogok Nemzetközi Egyezségokmánya kihirdetéséről
234/2011. (XI. 10.) Kormány rendelet a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény végrehajtásáról
402/2022. (X. 24.) Kormány rendelet a polgári védelmi kötelezettségről
290/2011. (XII. 22.) Korm. rendelet a honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről szóló 2011. évi CXIII. törvény egyes rendelkezéseinek végrehajtásáról
15/2021. (V. 13.) AB határozat a veszélyhelyzet idején az egyes adatigénylési rendelkezésektől való eltérésről szóló 521/2020. (XI. 25.) Korm. rendelet 1. § (3)-(5) bekezdéseire vonatkozó alkotmányos követelmény megállapításáról
23/2021. (VII. 13.) AB határozat a veszélyhelyzet idején alkalmazandó védelmi intézkedések második üteméről szóló 484/2020. (XI. 10.) Korm. rendelet egyes rendelkezései alaptörvény-ellenességének megállapítására és megsemmisítésére irányuló alkotmányjogi panasz elutasításáról és alkotmányos követelmény megállapításáról
Emberi Jogok Európai Egyezménye

Irodalomjegyzék

Csink Lóránt, A különleges jogrend bevezetésének alkotmányjogi megközelítése, Védelmi-Biztonsági Szabályozási és Kormányzástani Műhelytanulmányok, 2023/3., Nemzeti Közszolgálati Egyetem Védelmi-Biztonsági Szabályozási és Kormányzástani Kutatóműhely, ISSN: 2786-2283

Csink Lóránt: Alapjogok különleges jogrend idején, Védelmi-Biztonsági Szabályozási és Kormányzástani Műhelytanulmányok 2022/6, Nemzeti Közszolgálati Egyetem Védelmi-Biztonsági Szabályozási és Kormányzástani Kutatóműhely, ISSN 2786-2283

Csink Lóránt: „Mikor legyen a jogrend különleges?", Iustum aequum salutare, XIII. 2017. 4.,

Gárdos-Orosz Fruzsina: „Az alapjogok korlátozása"

Dr. habil Lakatos László ny. okl. mk. vezérőrnagy c. egyetemi tanár, c. főiskolai tanár, ny. egyetemi docens, okl. közigazgatás-szervező, a Magyar Tudományos Akadémia Köztestületi tagja: Katasztrófavédelem szervezése 1. órai jegyzet, Budapest, 2022. november 30.

Dr. habil Lakatos László ny. okl. mk. vezérőrnagy c. egyetemi tanár, c. főiskolai tanár, ny. egyetemi docens, okl. közigazgatás-szervező, a Magyar Tudományos Akadémia Köztestületi tagja: Katasztrófavédelem szervezése 1. órai jegyzet 4. előadás, Budapest, 2022. november 30.

Dr. habil Lakatos László ny. okl. mk. vezérőrnagy c. egyetemi tanár, c. főiskolai tanár, ny. egyetemi docens, okl. közigazgatás-szervező, a Magyar Tudományos Akadémia Köztestületi tagja: Katasztrófavédelem szervezése 1. órai jegyzet 3. előadás, Budapest, 2022. november 02.

Dr. habil Lakatos László ny. okl. mk. vezérőrnagy c. egyetemi tanár, c. főiskolai tanár, ny. egyetemi docens, okl. közigazgatás-szervező, a Magyar Tudományos Akadémia Köztestületi tagja: Katasztrófavédelem szervezése 1. órai jegyzet 2. előadás, Budapest, 2022. október 06.

Till Szabolcs: „Különleges jogrend"

Krebsz Klaudia

A kibervédelmi törekvések fejlődése és az államok betudhatóságának vizsgálata

Bevezetés

Számos állam igyekszik a kibertérben védelmi mechanizmust kifejleszteni, azonban növekszik azon államok száma, amelyek a kiberteret támadásra szánják. Oroszország az elsők között említhető, de ide soroljuk még, Kínát, Iránt, Észak-Koreát, az USA-t, és az utóbbi időben Izrael, Pakisztán és India képességei is felértékelődtek A megvádolt államok többnyire nem ismerték el, hogy közük lenne a kibertámadásokhoz, és bizonyítékok hiányában, így csak feltételezhető, hogy több kibertámadásban játszottak szerepet.[1] Nagyon nehéz a támadások bizonyíthatósága, mert a kibertérben folyó műveleteknél a legnehezebb bizonyítékokra lelni, leginkább csak az elektronikus nyomok állnak rendelkezésre, de a közvetett bizonyítékokat is számba kell venni, így vizsgálható, hogy melyik országnak fűződött érdeke az akcióhoz. A támadónak azonban az a célja, hogy minden lehetséges nyomot megsemmisítsen, elfedjen, hogy az egyértelmű bizonyítás ne valósulhasson meg és a vádakat tagadni tudja. Kedvelt lépés a proxyművelet, amely annyit tesz, hogy a valódi támadó helyett más cselekszik, amelyhez az agresszor támogatást nyújthat. Ez lehet közvetett is, amikor például egy menekülési útvonalat

1 Berzsenyi Dániel: A kibertér aktuális nemzetközi biztonságpolitikai kihívásai, In: *Incidensmenedzsment. Éves továbbképzés az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy számára,* Nemzeti közszolgálati Egyetem, 2022. 10. o.

biztosít a végrehajtónak. A proxykapcsolatoknak két fajtája ismert, a belföldi és a külföldi. Az előbbi esetén egy gazdasági társaság/csoport, míg az utóbbi esetében pedig egy másik állam, vagy annak gazdasági szereplőjének/¸csoportjának támogatása valósul meg. A nagy támadások valakinek/valakiknek a számlájára írhatók, azért valamely közösség felel, hiszen egyénileg egy ekkora mértékű károkozás valószínűsíthetően nem tudna megvalósulni. Támadói csoportokat hoztak létre, amelyek közül már elég sokat azonosítottak, és a rendelkezésre álló adatok alapján elmondható, hogy ezeknek a többsége csak úgy tud működni, ha azt egy állam támogatja.[2]

1. Kibertámadások áttekintése és a rájuk adott nemzetközi reakciók

1.1. A NATO elleni korai kibertámadás

A NATO-t először az 1999-ben, Koszovóban végrehajtott bombázását követően érte kibertámadás, szerb, orosz és kínai hackerek által. Ennek oka az volt, hogy amikor jugoszláv tagállamok szakadtak el a szövetségből, az nem ment konfliktusmentesen, és a háborúskodás ezen a területen Koszovóban öltötte a legnagyobb méreteket. A cél homogén nemzetiségű ország létrehozása volt (legalábbis az elnök erre hivatkozott a Hágai Törvényszék előtt is), ezért Szerbia 1998-ban Slobodan Milosevic parancsára etnikai tisztogatásokba kezdett. Falvak ezreit égették fel, tömeggyilkosságokat követtek el, rengeteg ember az otthona elhagyására kényszerült. Ez a szerb lépés a legtöbb nemzetközi szervezetet teljesen megdöbbentette. 1999. február 6-án megkezdték

2 Kralovánszky Kristóf: A kibertér fejlődése= The Evolution of Cyberspace, *Hadmérnök,* 2019/4. 201–202. o.

a béketárgyalásokat Rambouillet-ben, de ez nem járt sikerrel, ezért a NATO 1999. március 24-én Jugoszlávia bombázása kezdett, a hadművelet az Allied Force nevet viseli.[3] Az akciót egyébként az ENSZ Biztonsági Tanácsa nem hagyta jóvá. A bombázások után került sor a szövetség honlapjának megtámadására szerbiai hackerek által. Ebből fakadóan többször is elérhetetlenné vált a weboldal. A támadás a szerb Fekete Kéz (Crna Ruka), az orosz (From Russia With Love) és kínai hackercsoportokhoz volt köthető, amely kormányzati szervereket támadta. A Szövetség ekkor ébredt rá először, hogy egy új típusú kihívással is szembe kell nézniük. Ennek nyomán 2002-ben elindult a szövetség kibervédelmi programja a prágai csúcstalálkozó keretében, és sor került a Számítógépes Incindens Reagáló Központ (NATO Computer Incident Response Capability – NCIRC) létrehozására a NATO rendszerei feltörésének elkerülése céljából. Ettől függetlenül a tagállamok hálózatai és a rendszereinek védelme az ország feladatkörébe tartozott.[4]

1.2. Kibertámadások államok ellen

1.2.1. Az Észtországot ért kibertámadás

2007-ben, Észtország ellen követtek el kibertámadást, melynek kiváltó oka a fővárosban, Tallinban egy szovjet emlékmű eltávolítása volt, amely az ott élő orosz lakosok nemtetszését váltotta

3 Takács Izabella: 78 NAP. A médiapropaganda nyelve az 1999-es évek NATO-bombázásai idején a Magyar Szó című napilap címlapjain, Pécs, 2020. 12–14. o.

4 Kelemen Roland: A kibertámadások nemzetközi jogi olvasata és a NATO általi értelmezése, különös tekintettel a válaszlehetőségekre, In: Farkas Ádám (szerk.): *Az állam katonai védelme az új típusú biztonsági kihívások tükrében*, Nemzeti Közszolgálati Egyetem, Közigazgatási Továbbképzési Intézet, 2019. 46. o.

ki.[5] Az első támadásokra a tüntetéseket követően került sor, központjukban a parlament, kormányhivatalok és a minisztériumok voltak, de támadás érte éppúgy a pénzintézeteket, telefontársaságokat és a médiacégeket is. Egy Arbor Networks nevezetű cég, amely internetes biztonságtechnikával foglalkozik, megfigyelés alatt tartotta a túlterheléses támadásokat, ez idő alatt 128 incidenst észlelt. A megvalósítani kívánt cél kétségtelenül az állam online infrastruktúrájának megbénítása volt, ezzel lehetett elérni a gazdaság és a telekommunikáció összeomlását. Számos intézményben nagy zavart okozott, a bankhálózat átmenetileg megbénult, a telefonhálózat nem működött. Oroszország a nézeteltérés elején még kereskedelmi szankciókkal riogatta Észtországot, azonban ez a virtuális offenzíva még veszélyesebbnek bizonyult a szakértők vélekedése szerint. De hogy mit is jelent számokban a kár? Az észt Hansabank, az ország legnagyobb bankja több mint egymillió dollár veszteséget szenvedett, és ez csupán egyetlen nap leforgása alatt. Ez volt május 10-én, itt érte el tetőpontját a támadás.[6] A körülmények alapján elképzelhetetlen, hogy egy ilyen szinten megszervezett, kifinomult kiberművelet ne egy államnak, hanem attól független magánszemély(ek)nek, hackercsoportoknak a tevékenysége. Az agresszió jellegéből kiindulva az agresszorok kilétének megállapítása csaknem esélytelen. Többeket orosz területen azonosítottak, de bizonyítékok hiányában nem lehetett hitelt érdemlően igazolni, hogy a támadások mögött kormányzati szerverek állnak, de az észtországi eseményeket figyelembe véve csakis Oroszországnak állt érdekében előidézni a támadásokat, természetesen ő mindezt

5 Selján Gábor – Selján Péter: Kiberbiztonsági kitekintés, *Nemzet és Biztonság*. 2021/1. 30. o.

6 Bányász Péter – Orbók Ákos. A NATO kibervédelmi politikája és kritikus infrastruktúra védelme a közösségi média tükrében, *Hadtudomány*, 2013/23. 191–192. o.

tagadta.[7] 2009-ben Konsztantyin Goloszkokov, a NÁSI, vagyis egy ifjúsági mozgalom vezetője bevallotta, hogy a cselekményeket ők okozták, és ők ezt egyáltalán nem támadásnak vélték, épp ellenkezőleg. Szerintük egy ez ellenoffenzíva volt a szerintük illegálisan eltávolított emlékmű miatt. Goloszkokov állítása alapján a támadás a saját döntésük volt és a kormánynak ehhez semmi köze, így az ismertté vált álláspont szerint a cselekmények olyan orosz hackerek műve, akik rosszallták a szovjet emlékmű likvidálását.[8]

1.2.2. A Grúziát ért kibertámadás

2008-ban Oroszország és Grúzia közötti fegyveres összeütközés során, sőt azt megelőzően is Grúziában egyes weboldalak, szerverek egy időre megszűntek működni, a kapcsolattartás akadályoztatva volt. Ennek előzménye, hogy a grúz elnök a grúz-oszét és a grúz-abház ellentétek rendezését katonai úton kívánta véghez vinni, de Oroszország ezt nem hagyta szó nélkül. Grúzia öt nap után feladta a harcot, és fegyverszünetet kért. Az orosz ellenválasz nemcsak fizikai összecsapásokban mutatkozott meg, hanem Moszkva a kiberképességeit is megcsillogtatta. A legmarkánsabb támadások Grúzia kormányzati portáljait tették működésképtelenné, valamint ezeken tartalommódosításokat hajtottak végre. Ez a defacement, másnéven honlaprongálásos támadás. Többek között az elnökből, Mihail Szakasvili-ből próbáltak gúnyt űzni azzal, hogy fotójára Hitler-bajuszt rajzoltak, ezen kívül megjelentek olyan képek is, ahol az elnököt Hitler tipikus pózaiban jelenítették meg. Ezen tevékenységekért Oroszországot vádolták, de ő tagadta, hogy a kormánynak köze lenne a cselekményekhez.

---

7 Szentgáli Gergely: A NATO kibervédelmi politikájának fejlődése, *Nemzet és Biztonság*, 2013/3–4. 78. o.

8 Bányász – Orbók: i. m. 192. o.

A kormány szóvivője azt azonban nem zárta ki, hogy ugyan állami támogatás nélkül, de előidézhették orosz polgárok is, akik így próbáltak véleményt formálni a grúz inváziójáról. Grúzia nem rendelkezik olyan fejlett kiberinfrastruktúrával, mint mondjuk Észtország, ezért az ellenük elkövetett kibertámadás kevésbé értékelhető nagymértékű károkozásnak.[9]

1.3. A kibervédelem fejlődési lépcsőfokai

A 2007-es észt, és az azt követő 2008-as grúz támadások következtében szükséges volt a kibervédelmi fejlesztések továbbgondolása, ugyanis itt mutatkozott meg legelőször, hogy milyen volumenű támadások hajthatók végre kibertéren keresztül, amelyek már egyértelműen visszahatnak a hagyományos térre is (lásd például a banki szolgáltatások leállása). 2007-ben került sor a brüsszeli védelmi minisztériumi csúcstalálkozóra, és itt fogalmazódott meg az igény egy összehangolt kibervédelmi stratégai kidolgozására. Ebből a célból fogadtak el 2008 elején Bukarestben egy új Kibervédelmi Irányelvet, amely a nemzetek eljárásának egységesítését szorgalmazta, ugyanis a NATO-nak és a „nemzeteknek is meg kell védeniük a kulcsfontosságú informatikai rendszereiket, meg kell osztaniuk a legjobb gyakorlatokat és biztosítaniuk kell a szövetséges nemzetek számára, hogy kérésre segítséget nyújthassanak a kibertámadások elhárításához."[10] A védelmi kapacitások erősítésére pár hónappal később, májusban került sor a Kooperatív Kibervédelmi Kiválósági Központ (Cooperative Cyber Defence Centre of Excellence, CCDCOE)

9 Berki Gábor: Kiberháborúk, kiberkonfliktusok, In: *Műhelymunkák,* Geopolitikai Tanács Közhasznú Alapítvány, Budapest, 2016. 266–267. o.

10 *Bucharest Summit Declaration. Issued by the Heads of State and Government participating in the meeting of the North Atlantic*, Council in Bucharest, 2008.

felállítására Tallinnben, amelynek Magyarország 2010 óta tagja.[11] Ennek a lényege, hogy a szövetség tagállamai a kibervédelmi tapasztalataik megosztásával segítsék egymás fejlődését. A szervezet projektjei között kibervédelmi gyakorlatok és konferenciák szerepelnek, ahol a jelenlévőknek lehetőségük adódik gyakorolni és megtanulni, hogy mégis milyen technikával lehet kivédeni egy igazi kibertámadást. Az Észak- atlanti Tanács még az alapítás évének őszén jogilag is nemzetközi katonai szervezetnek minősítette a Központot.[12] Emellett kialakítottak egy hatóságot (Cyber Defence Management Authority – CDMA) a kibervédelmi problémák kezelésére. Ez a Cyber Defence Management Board irányítása alatt tevékenykedik (NATO Kibervédelmi Irányító Testület), amelynek feladata a centralizált kibervédelem irányítása, a tagállamok támadásra reagálása, ezeken kívül a nemzeti kibervédelem kialakításában való segítségnyújtás. A Számítógépes Incidens Reagáló Központ alatt működik a Rapid Reaction Team (gyorsreagáló csoport), amely a nemzeteket segíti a támadásokkal szemben. Nemzeti szinten létesítésre került a Computer Emergency Response Team (CERT, Számítástechnikai Sürgősségi Reagáló Egység).[13] 2009-ben az USA felállította a kiberhadviselésért felelős parancsnokságot (USCYBERCOM). 2013-ban a Nemzeti Hírszerzési Igazgató, James Clapper a legsúlyosabb fenyegetésnek a virtuális fenyegetést jelölte meg, amely így háttérbe szorította a terrorizmust, pedig 2001. szeptember 11. óta az efféle akciók jelentették a legnagyobb veszélyt.[14]

11 Kelemen: i. m. (2019) 46–47. o.

12 Tóth Tamás: A NATO Kibervédelmi Kiválósági Központ bemutatása. *Nemzetbiztonsági Szemle*, 2018/4. 51–53. o.

13 Kelemen: i. m. (2019) 47. o.

14 Selján: i. m. 30. o.

2010-ben a lisszaboni csúcson került elfogadásra a szövetség új Stratégiai Koncepciója, amelynek sarkalatos részét adták a kibertevékenységek.[15] Leszögezte, hogy a kibertámadások egyre gyakoribbá, szervezettebbé váltak, illetve a kormányok, vállalkozások, gazdaságok és potenciálisan a közlekedési és ellátási hálózatok, valamint más kritikus infrastruktúrák számára is egyre nagyobb károkat okoznak. Elérhetik azt a küszöböt, ami már a nemzeti és euroatlanti prosperitást, biztonságot és stabilitást veszélyezteti.[16] Célként szerepelt a képességek továbbfejlesztése és a NATO-szervezetek centralizált kibervédelmének megvalósítása. 2011 júniusában Brüsszelben tartották a védelmi miniszterek találkozóját, ahol átalakították a Kibervédelmi Irányelvet, és elfogadásra került a Cselekvési Terv is, amely bevezette az újításokat a gyakorlatba. A 2012-es chicagói csúcson ismételten számottevő jelentőségű volt a kibervédelem. Ezen a találkozón megfogalmazásra került, hogy a támadások száma egyre csak nőni fog, egyre kifinomultabbakká és összetettebbekké válnak. Ugyanebben az évben Tallinnben került megrendezésre a CyCon – konferencia is, ahol elhangzott, hogy a szövetség az elosztott felelősség elvét alkalmazza a kiberbiztonságban, ehhez el kell egymástól választani a nemzeti és a NATO kiberbiztonsági követelményeit. „Minimum követelményeket kell meghatározni azon nemzeti infrastruktúrák kiberbiztonságára, amelyek NATO-műveleteket is támogatnak annak érdekében, hogy ne legyen biztonsági rés a NATO és a nemzeti infrastruktúrák védelmi szintje között."[17] 2018-ban a brüsszeli csúcstalálkozón rögzítették az Eu és NATO együttműködését a közös biztonsági fenyegetésekkel szemben, melynek középpontjában többek között a kiberbiztonság, a hibrid

15 Kelemen: i. m. (2019) 47. o.
16 Kelemen: i. m. (2019) 47. o.
17 Kelemen: i. m. (2019) 48. o.

fenyegetések állnak.[18] A 2022-es madridi csúcson megfogalmazásra került, hogy Oroszország a legnagyobb fenyegetést jelenti közvetlen katonai szempontból, ezért fontos, hogy a tagállamok védelmi képességeiket erősítsék.[19]

1.4. A kiberháborúra alkalmazandó nemzetközi jog Tallinni Kézikönyve, mint egy szakértői iránymutatás – Az első szakértői vélemény vázlatos bemutatása

2013-ban került sor A Tallinni Kézikönyv a kiberhadviselésre alkalmazandó nemzetközi jogról (Tallinn Manual on the International Law Applicable to Cyber Warfare, röviden: Tallinni Kézikönyv) című szakértői dokumentum kiadására, amely értelmezni és rendszerezni próbálja az kiberhadviselésre vonatkozó nemzetközi jog kereteit.[20] A kidolgozás igazgatója Michael N. Schmitt, koordinátora pedig Dr. Eneken Tikk. A Tallinni Kézikönyv foglalkozott elsőnek a téma átfogó vizsgálatával, habár nem kötelező erejű, csupán egy iránymutatás, javaslat, amelyet az államok átvehetnek a kibertérrel kapcsolatos nemzeti jogi értelmezésükbe.[21] A kézikönyv gyakorlatilag az Államfelelősségi Tervezetben kialakított állami betudhatóságot vetíti ki a kibertérben megvalósított cselekedetekért, bizonyos módosításokkal, kiegészítésekkel.

---

18 Európai Tanács: *NATO-csúcstalálkozó, Brüsszel, 2018. július 11–12., 2018. július 11–12,* (https://www.consilium.europa.eu/hu/meetings/international-summit/2018/07/11-12/).

19 Csiki Varga Tamás – Tálas Péter: Megerősített elrettentés és védelem – a NATO új stratégiai koncepciójának és madridi csúcstalálkozójának értékelése, *Stratégiai Védelmi Kutatóintézet Elemzések*, 2022/8. 1. o.

20 Michael N. Schmitt (Ed.): *Tallin Manual ont he international law applicable to cyber warfare*. Cambridge University Press, Cambridge, 2013.

21 Gyebrovszki Tamás: Stuxnet-mint az első alkalmazott kiberfegyver – A Tallinni Kézikönyv szabályrendszere szempontjából, *Hadmérnök*, 2014/1. 166. o.

(1) *Az államok jogi felelőssége*:
Az államot nemzetközi jogi felelősség terheli a neki felróható nemzetközi jogot sértő kiberműveletekért vagy bizonyos esetekben mulasztásokért, így például az ENSZ Alapokmányának, vagy a békeidőre szóló szabályok megsértése is ide tartozik. A kár okozása nem feltétlenül szükséges a kiberművelet nemzetközileg jogellenes minősítéséhez. Ha mégis van ilyen szabály, a kár szükségképpen kell az államfelelősség megállapításához. Az állami szerveknek még az ultra vires tevékenységei is megalapozzák az állam felelősségét, ha általuk nemzetközi jogsértés következik be, de ez akkor is így van, ha a személyek, entitások kormányzati hatalmat gyakorolnak. Nem állami szereplő magatartása is alapul szolgálhat az államfelelősség kialakulásához. Az a kiberművelet, amely olyan személyhez, csoportokhoz köthető, akik az állam utasítása, irányítása vagy ellenőrzése alatt tevékenykednek, állami cselekménynek tekintendő. Az elkövetés helye irreleváns az államfelelősség megállapításához, ha egy állam más államok számítógépeit felhasználva valósít meg kibertevékenységet, a felelősség a számítógépet felhasználó államot terheli. Szintén állami cselekménynek minősülnek azok a magatartások, amelyeket az állam sajátjaként elismer.

(2) *A kormányzati kiberinfrastrukúrából indított kiberműveletek*:
Annak ténye, hogy kiberműveletet indítottak, vagy az kormányzati infrastruktúrából származik, önmagában nem elég bizonyíték arra, hogy a művelet az államnak tulajdonítható, csupán az állam érintettségét igazolja.

(3) *Az államon keresztül indított kiberműveletek*:
Szintén nem elég bizonyíték az államhoz köthetőséghez, ha egy cselekményt egy államban található kiberinfrastruktúrán keresztül irányítottak át. Ez akkor valósul meg, ha az egyik állam kiberinfrastruktúrájában indul meg a művelet, de áthalad egy másik állam kiberinfrastruktúráján. Az utóbbi államnál nem feltételezhető, hogy részt vesz a műveletben. Azonban ha tisztában van

a tranzittal, és nem tesz észszerű intézkedéseket a megakadályozására, a felelőssége fennáll.

A szakértők úgy vélekedtek, hogy az ellenintézkedéseknek szükségesnek és arányosnak kell lenniük, továbbá csak akkor jogszerű, ha a másik állam cselekménye jogsértő, előtte azonban fel kell szólítania a jogsértő államot a jogsértés befejezésére. Ha a jogellenesség megszűnt, a sértett állam nem tarthatja fent ellenintézkedéseit, illetve nem is kezdeményezhet utóbb.[22]

1.5. Hibrid hadviselés Krímen és Ukrajnában a Geraszimov – cikk alapján

2013-ban Valerij Vasziljevics Geraszimov orosz vezérkari főnök egy új hadviselési módot, a hibrid hadviselést fogalmazta meg, amelyet egy újabb generációnak tekint. Eszerint hibrid háború a diplomáciai eszközök vegyítésével valósul meg. A direkt katonai beavatkozás helyett, vagy azzal párhuzamosan egyéb eszközök használata is megjelenik, különösen a kritikus infrastruktúra a fő célpont. Geraszimov szerint a hadviselés már nem a régi szabályok szerint folyik. Előnyben részesítik az indirekt erő bevetését (félkatonai, civil felkelők), és az információs tér adta lehetőségeket. Támogatja a tömeges bevetést, különleges erők, robotizált fegyverek (pl. drónok) használatát. Surkov/Dubovitksy, Peter Pomerantsev ezt az új hadviselést nem lineárisként írta le, majd 2014 májusában az International Herald Tribune is ezt a szókapcsolatot használta. A holland tábornok, Frank van Kappen az orosz csapásokat hibrid háborúként értékelte. 2014. július 3-án fogadta el a NATO ezt a kifejezést. A cél az ellenség befolyásolása és belső bomlasztása. A háborúban a hátországnak is nagy szerepe van. Rácz András a hibrid hadviselést 4 fázisra osztja,

22 Michael N. Schmitt (Ed.): *Tallinn manual on the international law applicable to cyber warfare,* Cambridge University Press, Cambridge, 2013. 29–36.

ezek a következők: előkészítési, politikai előkészítési, műveleti előkészítési, támadási és az elért siker stratégiai kihasználási fázisok.[23] A hadviselés megfigyelhető a Krímen és Ukrajnában is, amelyről kicsit lejjebb ejtek szót. A cikk tartalmát Geraszimov átültette a 2014-ben megjelent doktrínájában is, amely egy nem hivatalosan elfogadott dokumentum. Szintén feltűnik a tartalmában, hogy az új hadviseléshez szükséges más eszközök bevetése is a hagyományos fegyveres csapatokkal együtt. Geraszimov tanulmányában említi az Arab Tavaszt, amelynek pusztításait a valódi háborúhoz hasonlítja. Megfogalmazta, hogy a hagyományos módszereken kívüliek nagyobb hangsúlyt kaptak, azok nagyban hozzájárultak a politikai és stratégiai célok megvalósításában. Szerinte a kiberhadviselés segíti az ellenfél harci képességeinek mérséklését, és fontosnak tartja a támadások elleni védekezési képességet. Ez az anyag egyszer sem tesz említést a hibrid háborúra vagy a hadviselésre, de a doktrína kifejezés sincs nevesítve.[24] A tanulmány készítője így vélekedik a munkáról: „Geraszimov munkáját inkább egy hidegháborús nyelvezetre emlékeztető, a hadtudomány művelőinek szánt, kutatandó célokat, feladatokat, elméleti fejtegetéseket tartalmazó cikként lehet meghatározni és nem egy ún. „hibrid háborút" meghirdető katonai doktrínaként." [25] Gudrun Perrson is úgy vélekedett, hogy az Arab Tavaszhoz hasonlatos háborúk fenyegethetik Oroszországot, főleg azért, mert az orosz hadtudomány az amerikainak a közelébe sem érhet. Galeotti szerint a doktrínában foglaltakat aszopikusnak jellemezte, mert ugyan Geraszimov arról írt, hogy

23 Rácz András: Russia's Hybrid War in Ukraine Breaking the Enemy's Ability to Resist. *Finnish Institute of International Affairs Report 43,* 2015. 36–41. o.

24 Tomolya János: Az úgynevezett „Geraszimov-cikk" margójára, *Hadtudomány*, 2018/3–4. 80–81. o.

25 Tomolya: i. m. 85–86. o.

az új hadviselési mód fenyegető Oroszországra nézve, és meg kell tőle védeni az országot, valójában arra gondolt, hogy Oroszországnak kell használnia ezt a hadviselést. Tehát ugyan az írásban védekezésről van szó, de azt támadásnak kell értelmezni.[26]

A negyedik generációs hibriditást alkalmazva a Krím- félsziget annektálásának sikere érdekében 2013-tól végeztek az oroszok kibertevékenységet, ami 2015-ben több órás áramkimaradáshoz is vezetett. Ez a támadás olyan kifinomult és rendkívül összehangolt volt, hogy arra enged következtetni, az akciók mögött csak egy állam állhatott. 2014-ben pedig az oroszok Ukrajnát támadták meg, és nagy területeket foglaltak el a keleti országrészen.[27] A támadás három szakaszból állt, és minden szakaszon belül három fázis valósult meg. Makhmut Garajev tábornok álláspontja szerint a technológiai fejlődésnek hála, a hadviselés megváltozott. Az új számítógépek, elektronikus eszközökkel nagyon hamar információhoz lehet jutni, a reakcióidő pedig ezzel együtt jelentősen lecsökken. A kiberhadműveletek képesek zavart okozni az ellenség kapcsolattartásában, radarok, hadműveleti eszközök működésében. További előnyt jelent, hogy így lehetőség van áttérni egy látens, előre be nem jelentett háborúra. Vladimir Slipchenko tábornok ezt a gondolatmenetet vette át, továbbfejlesztve. Szerinte a jövő csatái „érintkezés nélküli" összecsapások lesznek, az ostrom a levegőből és a világűrből érkezik. Domináns célpontok a katonai, politikai és gazdasági érdekeltségű infrastruktúrák, melyet hagyományos fegyveres támadás nélkül kívánnak megvalósítani. A Svéd Védelmi Kutatási Ügynökség (Swedish Defence Research Agency, FOI) szakértői szerint az orosz hadművelet nagyrészt a régi volt, elnézve a katonai képességeket, dezinformációs eszközöket, azonban a katonai

26 Rácz: i. m. 15. o.
27 Selján: i. m. 35. o.

és informatikai eszközöket hatékonyan összehangolták.[28] A 2014-es walesi csúcstalálkozó eredeti céljai között a transzatlanti kapcsolatok megújítása, a szövetség bővítése és a képességek fejlesztése szerepelt,[29] azonban az ukrán helyzet felhívta a figyelmet a kollektív védelem fontosságára, és így váratlanul került napirendi tűzésre a válság megoldása.[30] A támadások irányulhatnak választások ellen is, ez történt 2015-ben, amikor Ukrajna ellen követtek el virtuális támadásokat a választások eredményének befolyásolása céljából. A tevékenységekkel Oroszországot vádolták, de az állam nem ismerte el felelősségét. A szakértők véleménye az elkövetőkről ebben a kérdésben eltérő, egyesek a Fancy Bear nevű hackercsoporthoz kötötték az akciókat.[31] A Kibervédelmi Felajánlás (Cyber Defence Pledge) elfogadására 2016-ban, a varsói védelmi miniszteri találkozón került sor. Ebben került elismerésre a tagállamok állam- és kormányfői által a biztonsági fenyegetések új arca, a kiberfenyegetések, amelytől a nemzeteket meg kell védeni. Így kötelezettségüket megerősítették, és a tagállamok vállalták, hogy a tőlük elvárható legmagasabb színvonalú védelmet nyújtják, és együttműködnek a tagországokkal.[32] A félszigeten történtek hatására ismerte el a NATO a kiberteret a szárazföld, tenger, levegő, világűr mellett újabb dimenziónak. Ezáltal, ha egy esetleges támadás olyan mértéket ölt, mint egy fizikai támadás, ellentámadás indítható, de nem csak a kibertérben. Egy ilyen eset volt, amikor az USA felkutatta

28 Rácz: i. m. 34–36., 51. o.

29 Szenes Zoltán: Új bor a régi palackban?, A walesi NATO–csúcs, *Hadtudomány*, 2014/3–4. 6. o.

30 Kelemen: i. m. (2019) 48. o.

31 Berzsenyi Dániel: A kibertér aktuális nemzetközi biztonságpolitikai kihívásai, In: *Incidensmenedzsment. Éves továbbképzés az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy számára,* Nemzeti közszolgálati Egyetem, 2022. 11–12. o.

32 Kelemen: i. m. (2019) 49. o.

és megsemmisítette az Iszlám Állam hackereit, habár ez nem a NATO-hoz köthető. Az új hadszíntér megjelenésének okai között említhetjük, hogy az Egyesült Államok szerint a riválisaival szemben sokkal erősebb és intenzívebb védelemre van szükség, ehhez ő a segítségét nyújtotta. Az Egyesült Királyság közölte, hogy nem hagyja szó nélkül az ország kritikus infrastruktúrái ellen más kormány által végrehajtott támadást. Németország és Franciaország is támogatták a harcias virtuális képességek. Ezen államok részvételével a szövetségen belül egy belső kiberbiztonsági közösség jött lére, melynek a legmeghatározóbb alakja az USA volt. A kiberbiztonság megoldására összehangolt metódus nem alakult ki, az első, USA- hoz köthető ilyen módszer 2003-ból ismert, majd ezt követően a többi meghatározó állam is kialakította saját stratégiáit. Franciaország az egyetlen olyan állam a négyes közösségből, aki a legnagyobb veszélyt a nem állami szereplőkben (mint például a kiberterroristákban) látta, a többi hatalom továbbra is az államoktól tart. A szövetség az oroszok keltette problémát úgy kívánta megoldani, hogy ne vezessen a kapcsolatok megszakadásához Oroszországgal.[33] Az orosz-ukrán konfliktus hatására az Európai Uniót foglalkoztatni kezdte a dezinformációs tevékenységek blokkolása, amelyek a hibrid háborúk részét képezik, így 2015-ben létrejött az East StratCom Task Force nevezetű munkacsoport, amely arra irányult, hogy a külső szereplők általi félretájékoztatás mielőbb kitudódjon. Erre 2018-ban kidolgoztak egy cselekvési tervet is, amely úgy rendelkezik, hogy ezekkel szemben a tagállamoknak és az unió intézményeinek osztottan kell reagálniuk. Tartalmazza továbbá, hogy a kérdésben feladattal érintett szervek megerősítése szükséges, és egy riasztási rendszert is ki kell alakítani, amely majd a valós időben jelzi a problémát. A platformok felelőssége is megjelenik. Egy újabb előrelépés volt azonban a 2019-ben felállított Rapid

33 Selján: i. m. (2021) 25. o.

Alert System, amely egyszerűbb tájékoztatást és egységesebb fellépést biztosít a tagállamoknak és az uniós intézményeknek a dezinformáció kezelésére, ezáltal létrehoztak egy hálózatot a koordinálás és a tapasztalatok megosztása céljából, amelyhez a 27 tagállam kapcsolódik. A koronavírus járvány infodémiát (információs fertőzést) okozott, és az Unió felismerte, hogy meg kell egymástól különböztetni a hamis (jogellenes) és a félrevezető (káros) tartalmakat. A félrevezető tartalmaknál akkor merül fel félretájékoztatás, „ha megtévesztés, közérdeknek való károkozás vagy gazdasági károkozás szándékával tették közzé."[34] Azt, hogy melyik tartalom melyik csoportba sorolható, az adott tagállam ítéli meg.[35]

1.6. Tallinn Manual 2.0

A *Tallinni Kézikönyv 2.0 – A kiberműveletekre alkalmazandó nemzetközi jogról* című szakértői vélemény, ahogyan a nevében is szerepel, a kiberműveletekkel foglalkozik, és erre vonatkozóan betudhatósági eseteket állapít meg.[36] Gyakorlatilag a korábbi ajánlásokat fejleszti tovább és egészíti ki, kötelező erővel ezen dokumentum sem rendelkezi. Jelen fejezetben részletesen kifejtem a kézikönyvben szereplő betudhatósági eseteket, és röviden összevetem a 2001-es Államfelelősségi Tervezettel.

(1) *Nemzetközileg jogellenes kiberjogi cselekmények:*

A kézikönyv úgy rendelkezik, hogy a nemzetközi jogot sértő cselekmény, vagy mulasztás elkövetése tekintetében nemzetközi

34 Kelemen Roland: Radikalizálás, dezinformálás és tömegpszichózis modern köntösben: a hibrid konfliktus kibertérben, *Jog Állam Politika,* 2021/3. 79. o.

35 Kelemen: i. m. (2021) 79. o.

36 Michael N. Schmitt (Ed.): *Tallinn manual 2.0 on the international law applicable to cyber operations*, Cambridge University Press, 2017.

jogi felelősség terheli az államot, amennyiben a kibercselekmény az államnak tulajdonítható.[37]

Ez az Államfelelősségi Tervezetben is megtalálható, mint betudhatósági eset.[38]

(2) *Állami szervek által megalapozott államfelelősség:*
A Tallin 2.0. szerint az állam szervei, személyek vagy szervezetek kormányzati hatalom elemeinek gyakorlása során az állam által ténylegesen teljes függőségben végrehajtott kiberműveletek állami tevékenységnek számítanak. Itt figyelemmel kell lenni arra, hogy az állami tulajdonban lévő szervek nem feltétlenül minősülnek állami szerveknek. Ha egy szerv a rábízott hatásköröket túllépve nemzetközi kötelezettséget sért, az állam felelőssé tehető akkor is, ha az állam utasításait megsértve cselekszik. Ez akkor is így van, ha személyek vagy egy szervezet állami felhatalmazás alapján állami jogkörök egyes elemeit gyakorolják, és az állam nevében járnak el. Magánszemélyek esetében hivatalos, látszólag hivatalos, vagy a hatalom színe alatti cselekményei, mulasztásai államnak való felróhatóságot eredményeznek. Előfordulhat, hogy az állam nem képes egyes feladatokat ellátni, ezért ezeket magán, vagy önkéntes szervezetekre bízhatja, de ettől a felelősség ugyanúgy az államot terheli.[39]

A Tervezetben is szerepel, hogy az állami szervek, valamint az olyan személyek, szervek magatartása, amelyek közhatalmi elemet gyakorolnak, de nem állami szervek, állami tevékenységnek számítanak.[40]

(3) *Más állam átengedett szerve*:
Ha egy állam valamely szervét más állam rendelkezésére bocsátja, kormányzati funkciók gyakorlása során a fogadó államnak

37 Schmitt: i. m. (2017) 84–87.
38 *Draft articles on the responsibility of international organizations.*
39 Schmitt: i. m. (2017) 87–92.
40 *Draft articles on the responsibility of international organizations.*

lesz betudható, amennyiben az irányítást és ellenőrzést kizárólag ezen állam gyakorolja, valamint a műveleteket az állam nevében, az ő céljai megvalósítása végett végzi. Ezen szerv ultra vires tevékenysége esetében is szintén ez a helyzet áll fenn.[41]

Az Államfelelősségi Tervezet nemcsak átengedett szervekről, hanem személyekről is rendelkezik,[42] ezáltal a betudhatóság e tekintetben bővebb, mint a kézikönyvnél, ugyanis ott csak átengedett szerveket említ. Ezen kívül ez a pont is megfeleltethető a 2001-es ajánlásnak.

(4) *Nem állami szereplők tevékenysége:*
Ebben az esetben az államot akkor terheli felelősség, ha az ő utasításai szerint, irányítása vagy ellenőrzése alatt végzik vagy az állam a műveleteket elismeri és sajátjaként fogadja el.[43]

A kézikönyv itt említi az egyéni hackereket, informális csoportokat (pl. Anonymous), bűnszervezeteket, kiberterroristákat és lázadókat. Leggyakrabban a nem állami szereplő az állam segítője, és ultra vires cselekményeik általában nem tulajdoníthatók az államnak, csak ha a művelet lényeges részét jelenti annak, amely felett az állam hatalmat gyakorol.[44]

A Tervezetben szintén szerepelnek azon személyek tevékenységei, akik állami irányítás, ellenőrzés és utasítás alatt állnak.[45] Ami jelentős különbség a két dokumentum között ezen pont alapján, hogy a 2001-es külön pontban rendezi az államfelelősség azon esetkörét, amikor az állam sajátjaként ismer el egy tevékenységet, és nem korlátozza az állam sajátjaként való elismerést csak a nem állami szereplők esetére, a kézikönyv viszont erre szűkíti a kört.

41 Schmitt: i. m. (2017) 93–94.
42 *Draft articles on the responsibility of international organizations.*
43 Schmitt: i. m. (2017) 94.
44 Schmitt: i. m. (2017) 95.
45 *Draft articles on the responsibility of international organizations.*

(5) *Más államok kiberműveleteivel kapcsolatos felelősség* esetén a felelősség az államot terheli, ha

a) nemzetközi jogot sértő cselekmény elkövetésében egy másik államnak segítséget vagy támogatást nyújt, ha az állam a jogellenesség tudatában nyújt segítséget vagy támogatást, és a cselekmény nemzetközileg jogellenes lenne, ha azt az állam követné el;

b) egy másik állam az irányítása és ellenőrzése alatt elkövetett nemzetközileg jogellenes cselekménye, ha az irányítás és ellenőrzés a jogellenes cselekmény körülményeinek ismeretében történik, és a cselekmény nemzetközileg jogellenes lenne, ha azt ő követné el; vagy

c) nemzetközileg jogellenes cselekmény elkövetésére egy másik államot kényszerít.[46]

Ugyan ezt a tervezet nem egy cikk alatt tárgyalja, de mindhárom esetkör megtalálható benne.

(6) *A kiberműveletek jogellenességét kizáró körülmények*:

A Tallinni Kézikönyv hat jogellenességet kizáró körülményt ismer el, ezek a beleegyezés; az önvédelem, az ellenintézkedések, a végveszély, a vis maior vagy a szükséghelyzet.[47]

Ugyanezeket sorolja fel az Államfelelősségi Tervezet is, valamint mindkettő tartalmazza, hogy a kötelező normák (államok által elfogadott és elismert, amelytől nem lehet eltérni) megsértése nem zárja ki a cselekmény jogellenességét.[48]

Az államok részéről szükséges egy előzetes döntés azzal kapcsolatosan, hogy a tevékenység a másik államnak tulajdonítható. Egyes esetekben rövid idő áll csak rendelkezésére arra, hogy felmérje a releváns információkat a kibertérben. Ekkor az észszerűséget kell szem előtt tartani, amely minden esetben kontextusfüggő.

46 Schmitt: i. m. (2017) 100.

47 Schmitt: i. m. (2017) 104.

48 *Draft articles on the responsibility of international organizations.*

A felelősségre vonás függ a kiberművelet hatóerejétől, valamint a válaszlépés nagyságától, amelynek arányban kell állnia a kibertevékenységgel. Ha a válaszlépést alkalmazó állam téves bizonyítékokra alapozza azt, felelős a tetteiért. Ahogy a kézikönyv elődjében is szerepel, az elkövetés helye többségében nem számít a felelősségre vonásnál, hiszen államterületen kívülről is képesek az államok kiberműveletet kezdeményezni, ha egy nem állami szereplő egy másik állam utasításainak tesz eleget, ahol természetesen az utasítás helye szerinti állam tehető felelőssé, nem pedig az, ahonnan a művelet származik, ő ugyanis maximum a korrekciós műveletek elmulasztásáért felel. Így kibertevékenység folytatható saját államterületről, más állam területéről, tengerről, légtérből vagy a világűrből. Minden egyes helyzetet összefüggéseiben kell vizsgálni, és az alapján dönthető el az államnak való betudhatóság. Ennek megállapításánál a problémák ott vannak, hogy nagyon nehéz bizonyítani, ugyanis nem elegendő az, hogy egy állam kiberinfrastruktúrájából indult a művelet, még kevésbe az, hogy az állam infrastruktúrát felhasználva magánszemélyek, vagy csoportok állami megbízásból hajtották végre az ártalmas tevékenységet. Az is előfordulhat, hogy a támadók másik államra próbálják terelni a gyanút, így nehéz megbizonyosodni a valódi szereplő(k) kilétéről.[49]

2. IT Army

2022. február 24-én Oroszország megtámadta Ukrajnát, de még ezen lépés előtt is körvonalazódott az ukrán oldalon egy önkéntes kiberhadsereg létrehozására irányuló igény. Az ötletet Yegor Aushev informatikai vállalkozó vetette fel a digitális miniszternek, Mykhailo Federovnak, majd bele is kezdett a vállalkozó

49 Schmitt: i. m. (2017) 111–135.

szellemű résztvevők toborzásába. Az elképzelés egy támadó és egy védekező csoport létrehozása volt. A védekezés az infrastruktúrákra fog irányulni, az agresszor csapat pedig kiberkémkedéssel segítené Ukrajnát az oroszokkal szemben. Így jött létre ad hoc jelleggel az IT-hadsereg, anélkül, hogy bármiféle triviális tervük lett volna, végül hibrid konstrukcióvá alakult. Aushev fő célja az önkéntesek toborzásával a kritikus infrastruktúrák megvédése. A csatlakozók a védelmi minisztérium megbízásából elektronikus kémkedési műveleteket folytatnak,[50] a minisztérium az együttműködésüket azonban nem ismerte el.[51] 2022. február 26-án az ukrán miniszterelnök- helyettes felhívta az informatikai hadsereget, az orosz kormányzati, banki és vállalati weboldalak elérhetetlenné tételére.[52] Készült egy dokumentum, amely konkrét utasításokat tartalmaztak arra vonatkozóan például, hogy milyen szervert használjanak vagy hogyan rejtsék el személyazonosságukat.[53] Az IT-hadsereg két részből áll, az első egy kollektív felhíváshoz kapcsolódik, elsősorban az orosz infrastruktúra elleni összehangolt kiberműveletben való részvételre, amihez bárki csatlakozhat, aki kellő elkötelezettséget érez iránta. A másik belső rész egyre összetettebb támadásokat intéz orosz célpontok ellen. Ez alapján egy ez hierarchikus felépítésű szervezet, ahol laikusok és szakértők (civilek, katonák, hírszerzők) egyaránt közreműködnek a kibertevékenységekben. A hadsereg kormányzati weblapokat és polgári infrastruktúrákat egyaránt célba vesz, a támadások alól online gyógyszertárak, bankok, ételkiszál-

50 Ella-Magdalena Ciuperca – Victor Adrian Vevera: *Solving and managing moral dilemmas. From the cyber battle field to the future of mankind*, Internatinal Conference RCIC'22, 2020. 136.

51 Anne Sophie Delphin Amdal: *Civilian and Private Actors' Support of Ukrainian National Resistance*, Forsvarets forskningsinstitutt, 2022. 14.

52 Ellen Cornelius: *Anonymous Hacktivism: Flying the Flag of Feminist Ethics for the Ukraine IT Army,* 2022. 2.

53 Ciuperca – Vevera: i. m. 136.

lítási szolgáltatások és még a kiskereskedők sem mentesülnek. Az ukrán kormány hivatalos honlapján megjelent az internetes hadsereg elismerése.[54] A hadsereg által indított támadások nagy része a közigazgatást éri, példaként említve a kormányhivatalokat és a törvényhozó szerveket.[55] 2022. április 6.-án egy videót tettek közzé, amelyben egy orosz katona családját telefonhívásban fenyegették azzal, hogy mindent tudnak róluk, és a katona által elkövetett minden pusztításért felelőssé teszik majd őket. Federovnak két díjat ítéltek Lengyelországban az ellenállás megszervezéséért, amiről úgy nyilatkozott, hogy ez a kiberháborúban részt vett kiberközösség érdeme.[56] Az IT Army weboldalán lehetőség van a hadsereghez csatlakozni, ehhez mindösszesen két lépést kell teljesíteni. Első lépésként egy szoftvert kell telepíteni, a második lépés pedig a támadás indítása. Ezen felül ugyanezen weblapon akár célpontot is lehet javasolni.[57]

Az IT Army tekintetében bizonyosan kimondható, hogy ez hadsereg nem állami szerv, és nem is gyakorolnak állami jogköröket. A szakértők azonban a Tallinn 2.0. kommentárjában rögzítik, hogy ha az állam nem képes egyes feladatait ellátni, a feladatokat rábízhatja magán, vagy önkéntes szervezetekre, és ilyenkor ugyanúgy az állam tehető felelőssé. Erre vonatkozó kommentár viszont nincs az Államfelelősségi Tervezetben. Véleményem szerint ebbe a kategóriába a kézikönyv alapján akár be is lehetne sorolni az IT Army-t, ha valóban önkéntes szervezetről lenne szó, bár ugye itt felvetődik az a probléma, hogy a kormányzat támogatta a csoport létrehozását, és megszabta

54 Stefan Soesanto: „The IT Army of Ukraine: Structure, Tasking, and Eco-System", *CSS Cyberdefense Reports*, Zürich, 2022. 4–7.

55 William D. Done: The Information Technology Army of Ukraine and Cyber Warfare Doctrine, *Journal of Strategic Security*, 2023. 16.4: 2.

56 Soesanto: i. m. 20.

57 IT Army hivatalos weboldala. (https://itarmy.com.ua/).

a felépítését, úgyhogy az önkéntesség ebben a kontextusban némiképp vitatható. Az pedig nem jelenthető ki egyértelműen, hogy a kormányzattól származna az irányítás, utasítás vagy az ellenőrzés, de ha így lenne akkor a hackerek akciói megfeleltethetők lennének a Tallinn 2.0-ban megfogalmazott 17. szabály (a) pontjának, amely úgy szól, hogy az állam felelősségi körébe tartozik a nem állami szereplők olyan tevékenysége, amelyet állami irányítás, utasítás, vagy ellenőrzés alatt követtek el.[58] Ezt az Államfelelősségi Tervet 59. cikke is tartalmazza[59], így ha erre esetlegesen hivatkozni lehetne a Nemzetközi Bíróság előtt. A kézikönyv hiányossága, hogy nem állapít meg különböző betudhatósági szinteket. Az Atlanti Tanács Cyber Statecraft Initiative (az univerzális kihívások kezelésének központi szereplője) igazgatója, Jason Healey tíz felelősségi spektrumot állapított meg, amely azt a célt szolgálja, hogy a felelősség pontosabb meghatározását elősegítse. (1) Államilag tiltott: A kormány segít a harmadik fél támadásának megállításában. (2) Államilag tiltott, de ne megfelelő: A kormány kész lenne együttműködni, csak képtelen megállítani a támadást. (3) Állam által figyelmen kívül hagyott: A kormány tudatában van harmadik felek támadásainak, de politikai okok miatt nem intézkedik. (4) Állami bátorítás: Az ellenőrzést harmadik felek végzik, de a kormány ösztönzi őket. (5) Államilag formált: Az ellenőrzést harmadik felek végzik, de a kormány támogatást nyújt. (6) Államilag koordinált: A kormány irányítja a harmadik fél támadókat azáltal, hogy meghatároznak egy célcsoportot, vagy valamilyen részletet. (7) Állami megrendelés: Az állam harmadik felek meghatalmazottait kérik fel, hogy a nevében támadjanak. (8) Állami bűnözök által irányított: A támadást a kiberhadsereg nem ellenőrzött elemei valósítják meg. (9) Államilag végrehajtott: A támadáshoz a kormány

58 Schmitt: i. m. (2017) 94.

59 *Draft articles on the responsibility of international organizations.*

kiberhadseregét használja fel, akik közvetlen irányítás alatt vannak. (10) Államilag integrált: A kormány hadseregeibe harmadik fél támadóit integrálja.[60] Úgy vélem ebben a körben az ukrán kormányzat felelőssége a 6-os pontba mindenképpen beilleszthető, hiszen egyes részletszabályt lefektetnek az általuk kiadott dokumentumban, és ilyen tekintetben megvalósul az irányítás. A 9-es pontot fogalmazza meg lényegében a Tallinn 2.0. 17. szabálya (a) pontja is (amelyet az Államfelelősségi Tervezet is tartalmaz), de teljes bizonyossággal nem állapítható meg az irányítás, felügyelet vagy ellenőrzés, ahogy arra már fentebb hivatkoztam is. Ha nem lehet alkalmazni a betudhatósági szabályokat, de az állam, vagy a hackercsoport primer normát sért, akkor erre hivatkozva a sértett fél eljárást indíthat.

Az 1977-es Genfi Egyezmény az áldozatok védelméről szóló kiegészítő jegyzőkönyv védelmet biztosít a polgári lakosságnak, és a harci cselekményeket csak a katonai célpontok ellen engedélyezi.[61] Nos, a fentebb említett katona családjának fenyegetése egyértelműen ezzel szembe megy, ugyanis ha a család tagjai, akik civilek, kibertámadás áldozataivá válnak, akkor a kiberharccsoport súlyos jogsértést követne el, és ha esetlegesen Ukrajna betudhatósága megállapítható lenne, akkor az ő tevékenységének minősülne.

A felelős személyeket egyébként, ha más módon nem is, de négy esetkörben egyéni felelősség terheli a Nemzetközi Bíróság Büntető Statútuma szerint, ezek a következők: népirtás, háborús bűncselekmények, emberiesség elleni bűncselekmények és

60 Jason Healey: *Beyond Attribution: Seeking National Responsibility for Cyber Attacks*, The Atlantic Council of the United States, Washington DC, 2001. 2.

61 Magyarországon kihirdetett: 1989. évi 20. törvényerejű rendelet a háború áldozatainak védelmére vonatkozóan Genfben 1949. augusztus 12-én kötött Egyezmények I. és II. kiegészítő Jegyzőkönyvének kihirdetéséről.

agresszió. Ezek leginkább csak a fizikai térben alkalmazhatók, de nem kizárt, hogy egyes pontjai a kibertérben is megvalósuljanak, bár az erre vonatkozó felróhatósági vizsgálat elég szigorú. Fontos, hogy ez nem az állam felelősségét, hanem egyéni felelősséget eredményez.[62]

Konklúzió

Az államok betudhatóságára vonatkozó részletes szabályozás sokáig váratott magára, ugyanis csak a 21. század elején került sor az Államfelelősségi Tervezetben az egyes alapeseteinek átfogó kidolgozására. Előtte, a kevéssé korlátozott államközi erőszakalkalmazás korában aligha találunk erre vonatkozó törekvéseket. Azonban ahogy az erőszak egyes korlátai megfogalmazásra kerültek, és fontossá vált az állam felelősségre vonása, a betudhatóság tisztázására is szükség volt. Az Államfelelősségi Tervezet nyolc alappillért állapított meg, amely megalapozza a betudhatóságot. Bár az ENSZ Közgyűlés által elfogadott határozat nem rendelkezik kötelező erővel, ennek ellenére számtalan ügyben hivatkoztak a bíróságok az államfelelősség valamely esetére, emiatt szokásjogi szabályként felfogható.

Tekintettel arra, hogy a kibertér a hadviselés egy új dimenzióját nyitotta meg, és nagy számmal használták fel az államok támadásaik során, szükség volt a nemzetközi szabályozásban is nyomon követni az eseményeket. Már a 20. század végén is alkalmazták ezt a mechanikát, amikor a NATO honlapját tették ki támadásnak. Az elkövetőket ebben az esetben meg tudták állapítani. Az észt és a grúz támadások során ugyan Oroszországot

62 T/4490. számú törvényjavaslat az Egyesült Nemzetek Diplomáciai Konferenciája által, a Nemzetközi Büntetőbíróság Rómában, 1998. július 17-én elfogadott Statútumának kihirdetéséről.

vádolták, de ennek bizonyítása nem volt kellően megalapozott. Az egyes csúcstalálkozókon a kibervédelmi stratégiákat dolgozták ki, és azokat fejlesztették tovább, ehhez különböző szervezeteket (például Kibervédelmi Kiválósági Központ) hoztak létre. Mivel a kibertér más sajátosságokkal rendelkezik, mint a valós front, ezért az erre mérvadó betudhatósági körök kialakítása is szükségesnek bizonyult. Ezek elsősorban a 2013-mas Tallinni Kézikönyvben fogalmazódtak meg, amely a kiberháborúban alkalmazandó nemzetközi jogról rendelkezik. Az ebben foglaltakat vette át gyakorlatilag a 2017-ben kiadott Tallinn 2.0., csak sokkal részletesebben, betudhatósági kiegészítésekkel, amely a kiberműveletekkel foglalkozik, és lényegében a cselekmények államnak való tulajdonításában nem tértek el az Államfelelősségi Tervezettől, arra támaszkodtak a szakértők a munka megalkotása során. Jelenleg a Tallinn 2.0. az utolsó, amely az államok felelősségével foglalkozik. Ami újdonság, hogy a kommentárban sokkal részletesebben tárgyalja az egyes alapeseteket, amivel jobban elősegíti a betudhatóság megállapítását. Ezt főleg annál a szabálynál értem, ahol a kézikönyv tartalmazza azon önkéntes szervezetek tevékenységét, akik azért látnak el egyes feladatokat, mert az állam erre nem képes, de ettől függetlenül az állami tevékenységnek minősül. Ezt a Tervezet konkrétan nem tartalmazza, pedig ez problémát vethet fel például az ukrán internetes hadseregnél is, mert ha csak annyit fogadunk el, hogy valóban önkéntes szervezetről van szó, akkor erre vonatkozó iránymutatás a Tervezetből nem olvasható ki, ergo szigorúan véve erre nagyon nem lehetne hivatkozni. Ami pedig a kézikönyv hiányossága a korábbi munkához képest, hogy amikor az átengedett szervekről szól, a személyeket nem említi, tehát egy átengedett személy tekintetében nem rendezi a betudhatóságot, továbbá hallgat a kormányra került felkelők és az államot alapító mozgalmak tevékenységeiről. Egyik dokumentum sem szól azokról az állami szervekről, amelyek nem rendelkeznek közhatalmi jogosítvá-

nyokkal, ebből következően az ő tevékenységük nem róható fel az államnak.

Az említett dokumentumok egyike sem bír kötelező erővel, hanem különböző állásfoglalásokat, javaslatokat tartalmaz, de ahogy már utaltam rá, az kijelenthető, hogy a 2001-es ajánlásban szereplő betudhatósági csoportok szokásjogilag rögzülhettek, hiszen arra többször is hivatkoztak. A kibertérben bekövetkező műveletek esetében nem az a releváns, hogy melyik állam területéről indították, hanem melyik állam áll az akció mögött, hiszen a kibertér lehetővé teszi, hogy más államok szervereit, számítógépeit felhasználva tanúsítanak jogellenes magatartást.

Ugyan a felelősségre vonás technikai potenciálja a korábbiakhoz képest jelentősen javultak, de még így is legtöbbször bonyolult, költséges, és rengeteg időt igényel a valós tettes beazonosítása, így a betudhatóság nehezen nyer meghatározást, ugyanis a kibertérben legtöbbször nem marad nyom a támadó után, vagy éppen hamisítással más államok felelősségre vonását kívánja megvalósítani, ezért az egyértelmű bizonyítás nehézségekbe ütközik. Nem beszélve arról, hogy nem nyert megállapítást az a tény, hogy mennyi és milyen bizonyítékot követel meg a betudhatóság megállapítása.[63] Ez azért is komplikációt jelent, mert ha egy védekező állam rosszul méri fel a helyzetet, és hibás érvekre alapozva tesz ellenintézkedést, az szintén nemzetközi jogellenességet eredményez. Ha viszont túl sokat vár az ellenintézkedés megtételével azért, hogy elegendő bizonyítékot gyűjtsön a támadó államnak való tulajdonítás megalapozásáért, és a támadás megszűntével kezdi el cselekményeit, a jogellenesség a védekező állam részéről szintén beáll. Nem beszélve arról, hogy ellenintézkedés megtétele előtt fel kell hívni a jogsértő állam figyelmét a létrehozott jogellenességről, és csak ezután lehet cselekedni.

63 William Banks: Cyber Attribution and State Responsibility, *International Law Studies*, Vol. 97. (2021) No. 43, 1049.

Az ellenintézkedés a másik állam kötelezettségeinek teljesítését szolgálja.[64] A szükségesség és arányosság követelménye, valamint a határidő meggátolja, hogy ezek az ellenintézkedések represszáliába, vagy büntetésbe menjenek át.

A kibertámadások rendkívül sokszínűek lehetnek, így irányulhatnak például weblapok megrongálására, bankrendszer megbénítására, kritikus infrastruktúra támadására, vagy akár szociális intézmények rendszereinek befagyasztására. Elengedhetetlen lenne a támadó azonosítása, hogy az országok és a nemzetközi szervezetek képesek legyenek reagálni. Ennek hiánya zűrzavart és további támadásokat von maga után. Véleményem szerint fontos lenne egy egységes felelősségre vonási szabályozás kidolgozása, ugyanis a Tallinn 2.0. e tekintetben hallgat, ami ahhoz vezethet, hogy mivel az államok betudhatósága esetére nem határoz meg szankciókat, így azok továbbra is folytatják a kibertevékenységeiket mindenféle hátrány bekövetkezése nélkül. Tehát egy olyan rendszer kimunkálása lenne szükséges, amely kellő elrettentést biztosít a kibertérben megvalósuló akcióktól.

Sok szempontban nem született egyetértés, így a bizonyítási szabályokat illetően, a nyilvános felelősségre vonásban és annak következményeiben, aminek az lett az eredménye, hogy a civilek és az ő infrastruktúrájuk ellen irányított kibertámadások szabályai nem kerültek kidolgozásra arra vonatkozóan, hogy mi a helyzet akkor, ha ezeket az erőszak küszöbértéke alatt és fegyveres konfliktuson kívül követik el.[65] Így az államokat semmi nem riasztja vissza attól, hogy további kiberműveleteket hajtsanak végre, mert semmilyen következményekkel nem jár a tettük.

Összességében úgy értékelem a kiberműveletekre vonatkozó betudhatósági szabályokat, hogy maguk a jelenleg érvényes esetkörök kellően kimerítőek, ezért ha ebből nemzetközi jogszabály

64 Schmitt: i. m. (2017)
65 Banks: i. m. 1046–1047.

válna, vagy legalább szokásjogi úton elfogadásra kerülne, akkor az államoknak lehetőségük lenne erre a dokumentumra érdemben hivatkozni. Ehhez azonban egy sokkal átláthatóbb és pontosabb bizonyítási szempontrendszer kidolgozására van szükség. Végső soron az is indokolt volna, hogy a felelősség megállapítása utáni olyan szankciótár kialakítására kerüljön, amely kellő elrettentést nyújt a kibertámadások elkövetésétől, ezáltal a műveletek száma lecsökkenthető lehetne.

A nemzetközi szokásjogban, vagy elismert állami gyakorlatban jelenleg nincs meghatározva, hogy milyen szintű részvétel szükséges ahhoz, hogy az államfelelősség megállapítható legyen a kibertérben, de az idő előrehaladtával a nemzetközi konszenzus alakulhat ki erről.[66] A Cyber Statecraft Initiative által kidolgozott 10-es skála, amely a felelősség egy-egy fokát jelöli meg, jó alap lehet erre. Ez a skála a legpasszívabb felelősségtől a legaktívabb felelősségig jut el attól függően, hogy az állam hogyan viszonyul a támadáshoz.[67]

Magára az Államfelelősségi Tervezetben kimunkált betudhatósági esetkörökre nem kizárt, hogy a Nemzetközi Bíróság figyelembe veszi ítéletében. Probléma viszont, hogy nem léteznek olyan elfogadott és végrehajtható szabályok a beavatkozások államnak való betudhatósága kapcsán, amely az elejétől a végéig rendezi a kérdést. Szükséges lenne a bizonyításra vonatkozó pontos előírások megteremtése, főleg amiatt, mert egy ellenintézkedés nem megfelelő bizonyítékokra alapítása a sértett államnak is felróhatóságot eredményez. Továbbá célszerű lenne egy mindenki számára hozzáférhető nyilvántartás, amellyel esetlegesen vissza lehetne fogni a virtuális támadásokat, és segíthetik a többi államot a védekezésben. Mivel nincs megadva, hogy mi az a minimum részvétel, ami megalapozza az államfelelősséget,

66 Banks: i. m. 1067.
67 Healey: i. m. 2.

segítené a betudhatóság megállapítását az a (vagy ilyen) tízfokozatú spektrum, amit az Atlanti Tanácsban megfogalmaztak a kibertérben megvalósuló akciókra. Mindazonáltal az államok közötti kollektív megállapodás elősegíti a támadók megtalálását, és fejleszti a részes államok kibervédelmét, illetve a felróhatóság hitelességét is igazolja. Törekedni kell az ilyen szerződések létrehozására. Végső soron egy részletes szankciótár kidolgozása is indokolt volna, amely a betudhatóság fokozataira tekintettel pontosan determinálja, hogy milyen következményekkel jár az elkövetett kiberbűncselekmény, amely visszafoghatná a támadókat.

Ha a kibertámadásokban az állam felelőssége nem állapítható meg, valamilyen módon mégiscsak szükséges a bűnösök felelősségre vonása, ezért a primer normasértésekre ettől függetlenül lehet hivatkozni, illetve ha népirtás, háborús deliktum, emberiesség elleni bűncselekmény, vagy agresszió valósul meg, egyéni felelősségre vonásra is van lehetőség,[68] de közel sem biztos, hogy ezek szintjét egy virtuális művelet eléri.

68 T/4490. számú törvényjavaslat.

FÓRUM

Szladik Míra

Az Európai Unió kiberbiztonsági lépései

1. Bevezetés

A közlekedés, energetika, pénzügyi ágazatok, egészségügy egyre inkább függenek a digitális technológiától. Az utóbbi évtizedekben ez függőség még nagyobb méretűvé vált. Az Európai Unióban is számos lehetőséget nyújtotta digitalizáció árnyoldalaival is jelen lett. Ahogy az infrastruktúra, gépipar is fejlődik, úgy modernizálódnak a kibertérben elkövetett bűncselekmények is. A kibertámadások és a kiberbűncselekmények Európa szerte egyre gyakoribbakká váltak. Nem csak a gazdaság, de a társadalom is kiberfenyegetéseknek lett kitéve. Az újszerű kihívások és problémák minden ország/szervezet számára megkívánja védelmi stratégiájuknak megreformálását, illetve új alternatívák felmutatását.

Az Európai Unió az elmúlt 20 évben igyekezett a kiberbiztonsággal kapcsolatban olyan jogi környezetet alkotni, mely mindenki számára biztonságot teremt. Több fronton is dolgozik a kiberreziliencia előmozdításán, a kiberbűnözés elleni küzdelemben, illetve a kiberdiplomácia kiszélesítésében. Ezen tanulmány keretein belül bemutatom az Európai Unió fontosabb jogi lépéseit a kiberbiztonság megteremtésére.

2. Az Európai Unió kiberbiztonsági stratégiái

Az Európai Unió az elmúlt évtizedben három kiberbiztonsági stratégiát alkotott meg. Főbb elemzési pontjai a megelőzés,

reagálás, nemzetközi együttműködés, digitális biztonsági infrastruktúra, kiberbiztonsági tudatosság és az innováció.

2.1. 2013-as kiberbiztonsági stratégia

Az Európai Unió 2013-ban kezdte meg első kiberbiztonsági stratégiájának kidolgozását, ami „Az EU kiberbiztonsági stratégiája digitális évtizedre" címmel jelent meg, még ugyanabban az évben. A stratégiát az EU külügyi és biztonságpolitikai főképviselője és az Európai Bizottság dolgozta ki.[1] A 2013-as stratégia számít az első átfogó dokumentumnak, amelyet az EU a kiberbiztonság területén megalkotott. Összekapcsolta a belső biztonság kérdéseit és a külső biztonság kihívásait is. A dokumentum célul tűzte ki az egységes digitális piac létrehozását, amelyben a gazdasági növekedés kulcsát is látta, ami szorosan összefügg az emberek az internetes műveletek kapcsán tanúsított bizalmának növelésével is, ami azonban elképzelhetetlen a kibertér kockázatmentesítése nélkül.

A dokumentum öt stratégiai prioritást határoz meg a tagállamok számára. Rendelkezzenek a tagállamok rugalmas reagálási képességgel, csökkentsék a kiberbűnözés jelenségét, kibervédelmi politikát és képességeket alakítsanak ki, ipari és technológiai erőforrásokat hozzanak létre, amik szükségesek a kiberbiztonság megteremtéséhez, végül uniós szintű koherens nemzetközi kiberpolitika kialakítása.[2]

A stratégia három nagy területen tartja szükségesnek az intézkedések meghozatalát. A nemzeti szinten, ahol az állami és

---

1 Bihaly Barbara: A kibervédelem szerepe az Európai Unió közös biztonsági és védelmi politikájában, *Hadtudományi szemle,* 2021/3. 49. o.

2 Gazdag Ferenc – Remek Éva: *A biztonsági tanulmányok alapjai,* In: Hautzinger Zoltán (szerk.): *Studia Universitatis Communia,* Budapest, Dialóg Campus Kiadó, 2018. 134. o.

a magánszektor összefogása, a kapacitások hatékony fejlesztése a feladat. Az uniós szint, ahol kiemelt szerepe van az ENISA-nak a határokon átnyúló incidenskezelés fejlesztése céljából. A jogalkotás területén, amelynek ki kell terjedni arra, hogy a tagállamok egy nemzeti stratégiát alkossanak és megalakíthatók legyenek a CERT-ek.[3]

A dokumentum az kibertér kiépítésében felismerte a magánszektor szerepének fontosságát, azonban leszögezte, hogy egyre nő az igény a biztonságra, transzparenciára, valamint az elszámoltathatóságra, amelyet csak magasabb szinteken lehet eredményesen megvalósítani. Ennek tükrében fogalmazta meg általános éllel azokat az alapelveket, amelyeken a közös kiberbiztonsági stratégia nyugszik: az Európai Unió alapértékei ugyanolyan mértékben vonatkoznak a digitális világra, mint a fizikaira; a hozzáférés mindenki számára biztosított kell, hogy legyen; az érdekelt felek bevonásával történő demokratikus és hatékony irányítás; biztonság, mint közös felelősség.[4]

Szerepkörét tekintve már a dokumentum megalkotásakor is egyértelmű volt, hogy a kérdés összetettsége és az érintettek sokfélesége miatt központi felügyeleti rendszer kialakítására nem lesz lehetőség. Így a kibertámadások megelőzése és kivédésének rendszere alapvetően nemzeti szinten kell, hogy működjön, ami aztán adott esetben az uniós szintű beavatkozás által kerülhet kisegítésre. Ennek három fő pillére a NIS, a bűnüldözés és a védelem területe lesz.[5]

---

3 Kovács László: *Kiberbiztonság és -stratégia,* Budapest, Dialog Campus Kiadó, 2018. 88. o.

4 Európai Bizottság: Közös Közlemény az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának, Az Európai Unió kiberbiztonsági stratégiája, 2013.02.7., https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52013JC0001&from=EN (Letöltés: 2023.02.11.)

5 Az Európai Unió kiberbiztonsági stratégiája (2013) 20. o.

2.2. 2017-es kiberbiztonsági stratégia

Az Európai Bizottság és a tagállamok döntéshozói számára is hamar világossá vált, hogy a 2013-as kiberbiztonsági stratégia az új technikai, politikai, gazdasági változások miatt felülvizsgálatra szorul. A tagállamokban a 2013-as stratégia végrehajtása sem ment zökkenőmentesen, ez is egy ok volt, amiért a stratégia újításra szorult. 2013 óta a kiberbűnözés, fenyegetések aránya erősen megnövekedett, ami szintén egy intő jel volt, egy erősebb stratégia megalkotására.[6]

A 2017-es stratégiában nagyobb hangsúlyt kap a nemzetközi együttműködés fejlesztése, amely egy digitális egységes piac, globális stratégia, európai biztonsági stratégia, hibrid fenyegetésekkel szembeni fellépés közös kerete kialakítását könnyítené meg. Ezekkel a témákkal az Unió már korábban is foglalkozott, viszont a 2017-es stratégia elérkezettnek látta az időt, hogy ezeket a munkafolyamatokat összefogják. A 2013-as stratégiában megfogalmazott fő célok és elvek (megbízható, biztonságos és nyitott kiber-ökoszisztéma elősegítése) a 2017-es startégiában is aktuálisak, viszont nagyobb és több erőre van szükség ahhoz, hogy az egyre súlyosodó fenyegetésekkel szembe lehessen nézni.[7]

A 2017-es stratégia felhívja a figyelmet arra, hogy a kibertámadásokkal szembeni ellenállóképesség eléréséhez, illetve a stratégiai függetlenség kiépítéséhez egy olyan erős és egysége piac, nagyobb uniós technológiai fejlesztések és képzett szakemberek

6 Európai Bizottság: Közös közlemény az Európai Parlamentnek és a Tanácsnak: Ellenálló képesség, elrettentés, védelem: az Unió erőteljes kiberbiztonságának kiépítése 2017. 09. 13. 2. o.

7 Kelemen Roland: Az Európai Unió kiberbiztonsági stratégiájának evolúciója az elmúlt évtizedben. In: Bódiné Beliznai Kinga – Gosztonyi Gergely (szerk.): *Jogtörténeti Parerga III: Ünnepi tanulmányok Mezey Barna 70. születésnapja tiszteletére,* Budapest, ORAC Kiadó Kft., 2023. 182. o.

kellenek, amellyel egy átfogóbb és a szakpolitikákon átívelő megközelítést ér el.[8]

Az ENISA állandó megbízatást kapott az Bizottságtól feladatainak minél hatékonyabb ellátása érdekében. Lehetővé tette, hogy az ENISA képes legyen támogatni a tagállamokat, uniós intézményeket és vállalkozásokat olyan területeken, mint például a hálózati és információs rendszerek biztonságáról szóló irányelv, vagy a kiberbiztonsági tanúsítási keretrendszer. Az európai felkészültséget azzal is fokoznák, hogy éves összeurópai kiberbiztonsági gyakorlatokat szerveznek. Továbbá az ENISA-nak támogatnia kell az információs és kommunikációs technológiák (IKT) uniós szakpolitikáinak kidolgozását.[9]

A kiberbiztonsági piac növekedését az EU-ban számos tényező visszafogja. A termékekbe való magasabb fokú ellenálló képesség kialakítása céljából a Bizottság javaslatot nyújtott be egy uniós kiberbiztonsági tanúsítási keretrendszer létrehozásáról.

Az EU létrehozott egy olyan EU egészére érvényes tanúsítási keretrendszert, ami az információs és kommunikációs technológiai termékek, szolgáltatások és eljárások kiberbiztonsági tanúsítására vonatkozik. Az új mechanizmust az ipar például intelligens orvostechnikai eszközök tanúsítására használhatná.[10]

A rendszer szabályok, műszaki követelmények, szabványok és eljárások formájában valósul meg, ami csökkenti a piac széttagoltságát, felszámolja a szabályozási akadályokat és – amennyiben a tagállamok ténylegesen alkalmazzák őket – megkönnyíti

8 Közös közlemény az Európai Parlamentnek és a tanácsnak, Ellenálló képesség, elrettentés, védelem: az Unió erőteljes kiberbiztonságának kiépítése 3. o.

9 Közös közlemény az Európai Parlamentnek és a tanácsnak 2017.

10 Az EU közös kiberbiztonsági tanúsítási keretrendszert hoz létre és megerősíti ügynökségét – A Tanács kialakította álláspontját https://www.consilium.europa.eu/hu/press/press-releases/2018/06/08/eu-to-create-a-common-cybersecurity-certification-framework-and-beef-up-its-agency-council-agrees-its-position/ (Letöltés: 2022.10.12.)

a határokon átnyúló kereskedelmet, javítva a belső piac működésének feltételeit. A kiberbiztonsági tanúsítási rendszerek stratégiai prioritásait a Bizottság által közzétett uniós gördülő munkaprogram tartalmazza, amelyben megtalálhatók azon IKT-termékek, szolgáltatások és folyamatok, amelyek alkalmasak arra, a tanúsítási rendszer hatálya alá tartozzanak.[11]

A termékek, szolgáltatások és folyamatok jelentette kiberbiztonsági veszélyék alapján a tanúsítvány három megbízhatósági szintet – alap", „jelentős", valamint „magas" – különböztet meg. Ezek alapján határolható be, hogy rendeltetésszerű használatuk mekkora valószínűséggel, és milyen mértékű, illetve hatású veszélyt jelenthet. A gyakorlatban ez azt jelenti, hogy az a termék, amely „magas" biztosítási tanúsítványi szint szerint kerül besorolásra, az megfelelt a legmagasabb szintű biztonsági teszteknek.[12] Az ez alapján kiállított bizonyítvány elismerésre kerül az összes tagállamban, amely megkönnyíti a forgalmazását és növeli a termék, szolgáltatás, vagy folyamat megbízhatóságát.

A nemzetközi együttműködés erősítése az Európa kibertérbeli stratégiai autonómiájához való hozzájárulást szolgálja. Mivel világszerte a nemzetbiztonságra leselkedő egyik legnagyobb veszély a kibertámadás, ezért az országok érdeke egy erős szövetség és partnerség fenntartása, annak érdekében, hogy ezeket a támadásokat elhárítsák. Az Unió támogatja azt az álláspontot, miszerint a nemzetközi jog a kibertérben is érvényesüljön. A globális kiberstabilitás alapja az országok helyi és nemzeti képessége a kiberincidensek megelőzésére, azokra való reagálása. Az Unió 2013 óta vezető szerepet tölt be a nemzetközi kiberkapacitás-építésében. A 2017-es stratégia szerint továbbra is

11 Az Európai Parlament és a Tanács (EU) 2019/881 rendelete az ENISA-ról (48).

12 Az Európai Parlament és a Tanács (EU) 2019/881 rendelete az ENISA-ról (84).

a jogokon alapuló kapacitásépítési modellt fogja előmozdítani, a digitálisan a fejlődésért megközelítésnek megfelelően.[13]

Az EU a NATO-val is el fogja mélyíteni az együttműködést a kiberbiztonság, hibrid fenyegetések és a védelem terén. Továbbá támogatni fogják a kutatási és innovációs együttműködést is.

Főbb intézkedéseit tekintve: teljes körű végrehajtása a hálózati és információs rendszerek biztonságáról szóló irányelvnek, európai tanúsítási keretrendszer meghatározásáról szóló rendelet elfogadása, közös bizottsági/iparági kezdeményezés a termékek/szoftverek sebezhetőségének csökkentése érdekében, hatásvizsgálat végzése, melynek során létrehozzák az Európai Kiberbiztonsági Kutatási és Kompetenciaközpontot, tagállamok fellépése a kiberbiztonsági képzési programokba.

Összefoglalva az Unió kiberfelkészültsége központi jelentőségű az egységes digitális piac, illetve a biztonsági és védelmi unió szempontjából. A 2017-es stratégia meghatározza a kihívások nagyságrendjét és azokat az intézkedéseket, amelyeket az Európai Unió megtehet a biztonság létrehozása érdekében. Olyan célzott intézkedések javaslatait foglalja magába, melyek a tagállamok és az érintett uniós szervek együttműködésével, azok hatásköreit és feladatköreit tiszteletben tartva.

2.3. 2020-as kiberbiztonsági stratégia

2020 év végén az Európai Uniónak új kiberbiztonsági stratégiája lett Az EU kiberbiztonsági stratégiája a digitális évtizedre címmel.[14] A stratégia kiemeli, hogy a közlekedés, az energiaügy, a telekommunikáció, a pénzügy, a biztonság, az űrpolitika, a védelem és a demokratikus folyamatokat egyre inkább befolyásolja

13 Közös Közlemény az Európai Parlamentnek és a Tanácsnak 2017.

14 European Commission: The EU's Cybersecurity Strategy for the Digital Decade (2020. december 16.).

a hálózati és információs rendszerek.[15] Felvázolja, hogy az EU-nak nincs meg a kollektív helyzetismerete a kiberfenyegetésekkel kapcsolatban, ezért a kiberbiztonság javítása elengedhetetlen. Az új kiberbiztonsági stratégia meghatározza, hogyan fogja megvédeni az Európai Unió lakóit a kibertámadásoktól, illetve milyen nemzetközi együttműködéseket köt a biztonság érdekében.

A 2020-as startégiában nagy szerepet kap a globális gondolkodás és az európai cselekvés, ennek elérése érdekébe szükséges egy globális és nyílt internetet. Ezt úgy kívánja biztosítani, hogy 1. megteremti a rezilienciát, a technológiai szuverenitást, 2. az operatív kapacitásépítést a megelőzés, elrettentés és reagálás érdekében, és 3. előmozdítja a globális nyílt kiberteret.[16]

Az EU ennek a stratégia melletti elköteleződés érdekében elfogadta a Digitális Európa programot is, amelynek keretében 2021-2027-ig soha nem látott mértékű uniós digitális átállási beruházásokat tervez az új technológiai és ipari szakpolitikák, illetve a helyreállítási menetrend részeként. A Digitális Európa program célja, hogy elérhetővé tegye a vállalkozások, a polgárok és a közigazgatási intézmények számára a technológiát. Továbbá fel szeretné gyorsítani a gazdasági fellendülést és az európai társadalom és gazdaság digitális átállását is. Ez a program mindenki számára kedvező különösen a kis- és középvállalkozásoknak. Öt területet foglal magába, melyeket támogat a program: szuper-számítástechnika, mesterséges intelligencia, kiberbiztonság, fejlett digitális készségek, a digitális technológiák alkalmazása és hozzáférhetősége.[17]

15 Közös közlemény az Európai Parlamentnek és a Tanácsnak: Az EU kiberbiztonsági stratégiája a digitális évtizedre, 1. o.

16 Közös közlemény az Európai Parlamentnek és a Tanácsnak: Az EU kiberbiztonsági stratégiája a digitális évtizedre, 5. o.

17 Digital Europe: https://culture.ec.europa.eu/hu/node/1179 (Letöltés: 2023.03.28.)

A stratégia értelmében fokozni kell valamennyi érintett gazdaság és a társadalom szempontjából fontos feladatot ellátó ágazat kiberrezilienciáját.[18] A hálózati és információs rendszerek biztonságára vonatkozó szabályok alapján fokozni kell az érintett gazdaság és a társadalom szempontjából fontos feladatot ellátó ágazatok kiberrezilienciáját. Ahhoz, hogy a kifinomultabb kibertámadásokkal szemben fel lehessen lépni a Bizottság javaslatára kiépítik a biztonsági műveleti központok uniós hálózatát, amely egy kiberbiztonsági pajzsként fog funkcionálni az EU számára.[19] A hálózati és számítógépes rendszerek folyamatos nyomon követése és elemzése végett, sok nemzeti hatóság, állami szervezet számítógépes-biztonsági eseményekre reagáló csoportokat (CSIRT) és biztonsági műveleti központokat (SOC) hozott létre.[20]

Az új kiberbiztonsági stratégia értelmében a kiberbiztonság beépülne az ellátási lánc valamennyi elemébe és négy kiberbiztonsági szektoron – belső piac, bűnüldözés, diplomácia, védelem területén – átívelve még szorosabban összekapcsolná az uniós tevékenységeket.

---

18 Farkas Ádám: II.6. A kibertér állami-társadalmi-egyéni biztonsági szintjeinek metszéspontja: a reziliencia, In: Farkas Ádám – Kelemen Roland: *Nemzeti biztonság és kibertér,* Budapest, Médiatudományi Intézet, 2023. 104–110. o.; Vikman László: A közműszolgáltatások és a reziliencia egyes kérdései, különös tekintettel a kiberbiztonságra, *Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok,* 2021/14.; Kelemen Roland – Mihály Laura Dominika: A kibertér és a psziché ütközéspontjai mint a 21. századi reziliencia kulcskérdése. *Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok.* 2022/14.

19 Közös közlemény az Európai Parlamentnek és a Tanácsnak: Az EU kiberbiztonsági stratégiája a digitális évtizedre, 8. o.

20 Közös közlemény az Európai Parlamentnek és a Tanácsnak: Az EU kiberbiztonsági stratégiája a digitális évtizedre, 7. o.

3. Szabályozások átalakulása 2010 után

3.1. NIS 1. irányelv

A 2013-as Stratégia megalkotásával már lehetett látni, hogy kell egy kiegészítés, ami annak esszenciális második feleként is értelmezhető biztonsági intézkedésekről szóló irányelv lesz. 2016-ban került elfogadásra a NIS-irányelv, ami a sebezhetőség csökkentése érdekében jött létre a Kiberbiztonsági Stratégia követelményeinek megfelelően.

A dokumentum teljes címe az Európai Parlament és a Tanács (EU) 2016/1148 irányelve a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről.[21] Ahogy a címből is kiderül, a NIS-irányelv már egy konkrét jellegű jogi jellegű intézkedéseket tartalmaz, ami az Európai Unió egészére kiterjedő kiberbiztonság területén hozott szabályozás, melynek célja a kiberbiztonság mértékének növelése.

A NIS-irányelv elsősorban a nemzeti keretek kialakítását szorgalmazta, ami kiemelte, hogy a nemzeti stratégia foglalkozzon a felkészültség, reagálás, helyreállítás körében tehető intézkedések azonosításával, kockázatértékelési terv készítésével, rendszerek biztonságára vonatkozó célok és prioritások kijelölésével, a nemzeti stratégiák vonatkozásában szervezett oktatási, tájékoztató és képzési programok megjelölésével, illetve a nemzeti stratégiák végrehajtásában érintett szereplők jegyzékével.[22]

---

21 Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről, https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A32016L1148 (Letöltés: 2023.02.11.)

22 Európai Parlament és a Tanács 2016/1148 irányelve 7. cikk (1).

Az irányelv kötelezővé teszi a tagállamok számára, hogy kijelöljenek egy vagy több számítógép-biztonsági eseményekre reagáló csoportot (CSIRT), amelyek az adott szektor történéseiért felelős. Annak érdekében, hogy az egész EU területén közösségi szintű együttműködés jöhessen létre, az irányelv létrehozta az Együttműködési Csoportot, ami a hatóságok együttműködésére szolgál, illetve a CSIRT hálózatot, ami a CSIRT-ek együttműködését biztosítja.[23]

Kiépítésére került egy olyan együttműködési csoport is, amely a tagállamok, a Bizottság és az ENISA (Európai Uniós Hálózat- és Információbiztonsági Ügynökség) képviselőiből állt. Feladata az államok közötti stratégiai együttműködés, az információcsere támogatása, illetve a hálózati és információs rendszerek biztonságának megteremtése.[24]

3.2. NIS 2. irányelv

A kibertér rohamos változását mutatja, a jogalkotás területén fellépő intézkedése, ugyanis hat évvel a NIS 1. irányelv elfogadását követően 2023. január 16-án a Tanács és az Európai Parlament életbe léptette a NIS 2. irányelvet, amely az Unió egész területén egy egységes és magas szintű kiberbiztonsági környezetet kíván megteremteni. A célja az irányelvnek a NIS 1-hez hasonló, azt fejleszti tovább: javítani kíván a köz- és a magánszektor kiberrezilianciáján, illetve a kiberbiztonsági eseményekre való reagálási képesség növelésén.

A NIS 2. preambuluma is kiemeli, hogy „A hálózati és információs rendszerek a mindennapi élet központi jellemzőjévé fejlődtek a társadalom gyors digitális átalakulásával és összekapcsolódásával, beleértve a határokon átnyúló információ-

23 Európai Parlament és a Tanács 2016/1148 irányelve 11. cikk, 12. cikk.
24 Európai Parlament és a Tanács 2016/1148 irányelve 11. cikk.

megosztást is. Ez a fejlődés a kiberfenyegetettség bővüléséhez vezetett, új kihívások támasztásával, amelyek minden tagállamban kiigazított, összehangolt és innovatív reagálást igényelnek."[25]

3.2.1. Mi a különbség a NIS 2. és a NIS 1. irányelv között?

A NIS 2. irányelv tágabb hatállyal rendelkezik. Sokkal több ágazatra kiterjed a hatálya, így a korábban fókuszban lévő ágazatok mellett (energetika, közlekedés) kibővült a szolgáltatások köre is, melyet az irányelv két csoportra bont szét: a korábbi „alapvető szolgáltatásokat nyújtó" szereplők és a „digitális szolgáltatók" helyett fontos és alapvető szervezeteket határoz meg, melyeket kiemelten kritikus ágazatokhoz és egyéb kritikus ágazatokhoz sorol.[26]

Kiemelten kritikus ágazatok csoportjában átfedéseket mutat a NIS 1. irányelvvel, viszont a digitális infrastruktúra körében érintett szolgáltatások köre kiszélesedett, illetve több új elemet is beemelt az ágazati körébe (például: világűr, IKT szolgáltatások irányítása).

Az egyéb kritikus ágazatok között megjelenik a vegyszerek gyártása, digitális szolgáltatók, futárszolgáltatások stb.

Azok a szervezetek, melyek a kiemelten kritikus, vagy az egyéb kritikus ágazatokhoz tartoznak, de nem sorolhatók az alapvető szervezetek köréhez, azok fontos szervezetnek minősülnek. A tagállamok feladatköréhez sorolja a fontos és az alapvető szervezetek listájának összeállítását.[27]

A szabályok hatályára vonatkozólag is változást hozott a NIS 2. irányelv. Míg a NIS 1. irányelv alapján a tagállamok

25 Az Európai Parlament és a Tanács 2022/2555 irányelve.

26 Az Európai Parlament és a Tanács 2022/2555 irányelve 1. 2. melléklet.

27 Domokos Márton – Bertók Gábor – Huszár Daniella: *NIS 2. – az EU új kiberbiztonsági irányelve*, https://www.jogiforum.hu/hir/2023/01/03/nis2-az-eu-uj-kiberbiztonsagi-iranyelve/ (Letöltés: 2023.03.14.)

feladata, volt az, hogy melyik szervezetek felelnek meg annak a kritériumoknak, melyek alapján alapvető szolgáltatásokat nyújtó szereplőknek minősülnek. Az új irányelv megteremti a méretkorlátra vonatkozó szabályt, amely általános szabályként terjed ki a hatálya alá tartozó ágazatokban működő, illetve a hatálya alá tartozó minden közepes és nagyméretű szervezetre, amelyek szolgáltatásokat nyújtanak.[28] A NIS 2. irányelv megalkotja a jogi koherenciát más szektorspecifikus szabályokkal, mint pl. a DORA rendelet, ennek értelmében ezen szabályoknak ugyanolyan szintű védelmet kell biztosítani, mint a NIS 2. irányelvnek.[29]

A tagállamoknak, ahogyan minden uniós irányelvet, természetesen a NIS 2. irányelvet is át kell ültetniük a nemzeti jogukba. Azonban számos más kötelezettséget is előír az irányelv, többek között ki kell jelölni a tagállamoknak illetékes hatóságokat és egyedüli kapcsolattartó pontokat, nemzeti kiberbiztonsági stratégiákat és szakpolitikákat kell elfogadniuk, kiberbiztonsági válságkezelési keretek kialakítása szükséges, továbbá létre kell hozni a számítógép-biztonsági eseményekre reagáló csoportokat (CSIRT)

A tagállami átültetés alapján a nemzetközi jogban is megjelenik az érintett alapvető és fontos szervezetek számára meghatározott kötelezettség. Ilyen kötelezettség például az, hogy minden olyan eseményről, amely jelentős hatással van a szolgáltatásaik nyújtására (alapvető és fontos szervezetek),

28 EU Tanácsa: *A kiberbiztonság és -reziliencia megerősítése az EU egész területén – Ideiglenes megállapodás a Tanács és az Európai Parlament között*, https://www.consilium.europa.eu/hu/press/press-releases/2022/05/13/renforcer-la-cybersecurite-et-la-resilience-a-l-echelle-de-l-ue-accord-provisoire-du-conseil-et-du-parlement-europeen/ (Letöltés: 2023.03.14.)

29 Domokos Márton – Bertók Gábor – Huszár Daniella: *NIS 2. – az EU új kiberbiztonsági irányelve*, https://www.jogiforum.hu/hir/2023/01/03/nis2-az-eu-uj-kiberbiztonsagi-iranyelve/ (Letöltés: 2023.03.14.)

értesíteniük kell a CSIRT-jüket vagy az illetékes hatóságot.[30] A kötelezettségeket, már a NIS 1. irányelv is magába foglalta, viszont a NIS 2. szabályai jóval részletesebben kitér a kötelezettségi pontokra.

Az irányelv kiemeli a nemzetközi együttműködés nagyfokú szerepét is és ennek érdekében együttműködési csoportok létrehozását írja elő.[31] Kialakítja a nemzeti CSIRT-hálózatot, amely a tagállamok közötti gyors és hatékony együttműködést szolgálja. Létrehozták az Európai Kiberválságügyi Kapcsolattartó Szervezetek Hálózatát (EU-CyCLONe), amely a tagállamok, az Unió, ügynökségek, hivatalok közötti releváns információk rendszeres és hatékony cseréjét szolgálák.[32]

Az irányelv szabályozásai nem terjednek ki az olyan területekre, mint a védelem vagy a nemzetbiztonság, a közbiztonság, bűnüldözés és az igazságszolgáltatás. Továbbá nem terjed ki az irányelv hatálya a parlamentek és a központi bankokra sem.[33] A közigazgatási szervekre való tekintettel (mivel gyakran szerepelnek a kibertámadások célpontjai között) a NIS 2. irányelv rájuk alkalmazandó lesz.

Az EU kiberbiztonsági ügynökségének (ENISA) szerepét az irányelv növelte, magasabb szinten kell elvégeznie a meglévő feladatait. Feladatai közé tartozik az európai sérülékenység-adatbázis fenntartása, Unió kiberbiztonsági helyzetéről jelentéskészítés, DNS-szolgáltatók, a doménnév-nyilvántartási szolgáltatásokat nyújtó szervezetek, a felhőszolgáltatók, az adatközpont-szolgáltatók, a tartalomszolgáltató hálózati szolgáltatók, az irányított szolgáltatók és az irányított biztonsági szolgáltatók, valamint az

30 Az Európai Parlament és a Tanács 2022/2555 irányelve 21. cikk (1).
31 Az Európai Parlament és a Tanács 2022/2555 irányelve 14. cikk III. fejezet.
32 Az Európai Parlament és a Tanács 2022/2555 irányelve 16. cikk (1).
33 Az Európai Parlament és a Tanács 2022/2555 irányelve (8).

online piacterek, az online keresőprogramok és a közösségimédia-szolgáltatási platformok szolgáltatói nyilvántartása.[34]

A tagállamoknak a NIS 2. irányelvet, 2024. október 17-ig kell elfogadniuk és kihirdetniük. A NIS 2. irányelv elfogadása mellett sor került a pénzügyi ágazat digitális működési rezilienciájáról szóló rendelet (DORA rendelet) elfogadására. Folyamatban van a kiberreziliencia rendelet elfogadása is.

3.3. DORA rendelet

2020. szeptember 24-én az Európai Bizottság közzétette a Digital Operational Resilience Act első tervezetét (DORA rendelet). Miért volt szükség erre a rendeletre? A pénzügyi szektorban létező szervezetek egy erős kölcsönös függőségeken alapuló rendszerekben működnek, amelyek nem egységesek EU-s szinten, nehezen összeegyeztethetők az kibertérben felmerülő kockázatok kezelésére megalkotott törvényi szabályozások. Az Európai Bizottság ezért, közösségi szinten is fontosnak tartotta, hogy az informatikai kockázatokat és fenyegetéseket egységesen kezeljék. Így megszületett a DORA rendelet, amely segítségével átláthatóbb lesz a törvényi szabályozás.[35] Tehát az elsődleges cél, az IKT (információs és kommunikációs technológia) ellenállóképességének megerősítése a pénzügyi szolgáltatások terén.

A rendelet 20 pontban, tételesen felsorolja, mit kell pénzügyi szervezet alatt érteni, de a rendelet hatálya kiterjed a harmadik fél IKT-szolgáltatók körére is (adatelemzési szolgáltatásokat kínáló szolgáltatók, felhőalapú számítástechnikai

34 Az Európai Parlament és a Tanács 2022/2555 irányelve 6. cikk (34).

35 Szőllősi Zoltán: *DORA (Digital Operational Resilience Act) rendet tesz a pénzügyi kibertérben*, https://www2.deloitte.com/hu/hu/pages/kockazat/articles/dora.html (Letöltés: 2023.03.27.)

szolgáltatások.[36]) A szervezeteknek rendelkezniük kell egy ellenálló képességgel, illetve egy helyreállító képességgel az IKT-incidensek kezelése végett.

A DORA a kiberbiztonsági előírásokat öt fő területen szabályozza.[37]

— IKT kockázatkezelés;
— IKT-val kapcsolatos események kezelése, osztályozása, jelentése;
— digitális működési reziliencia tesztelése;
— harmadik féltől eredő IKT kockázat kezelése;
— információk megosztására vonatkozó megállapítások.

A rendelet mindegyik területre részletes szabályozásokat hozott meg. Az IKT kockázatkezelés kapcsán előírja az IKT-rendszerek és eszközök beállítását és karbantartását, hogy ezzel minimalizálják az IKT-kockázatok hatását. Ha felmerül IKT-kockázat, akkor ezeknek a forrását folyamatosan azonosítani kell és védelmi, illetve megelőzési intézkedéseket kell kidolgozni az elhárítás érdekében. Katasztrófa- és helyreállítási terveket kell bevezetni, amelyek biztosítják az IKT-val kapcsolatos incidensek utáni gyors helyreállítást.

A digitális működési reziliencia érdekében az IKT kockázatkezelési keretrendszer elemeinek felkészültségét időszakonként tesztelni kell. Ha gyengeségek, hiányosságok fordulnak elő a rendszerben, azokat azonosítani kell, és azonnal megszüntetni.[38]

A harmadik féltől eredő IKT kockázatok kezelése érdekében biztosítani kell a külső IKT-szolgáltatókra való támaszkodásból származó kockázatok alapos nyomon követését. A szolgáltatások kulcsfontosságú elemeit harmonizálni kell. A kritikus vagy

36 Az Európai Parlament és a Tanács 2022/2554 rendelete 63. szakasz.
37 Az Európai Parlament és a Tanács 2022/2554 rendelete 1. cikk (1) (a).
38 Az Európai Parlament és a Tanács 2022/2554 rendelete 24. cikk (1-6).

fontos funkciókat támogató IKT-szolgáltatások esetén a pénzügyi szervezeteknek kilépési stratégiát kell bevezetniük.[39]

Az információmegosztás ösztönzi az együttműködést más pénzügyi szervezetek megbízható közösségei között. Az ilyenfajta együttműködés fokozza a pénzügyi szervezetek digitális működési rugalmasságát, illetve felhívja a figyelmet az IKT-kockázatokra. Továbbá egy ösztönzés a pénzügyi szervezetek részére, hogy a kibertér fenyegetéseivel kapcsolatos információkat megosszák egymással.[40]

3.4. CER irányelv

Az Európai Bizottság 2020. december 16-án terjesztette elő a kritikus szervezetek ellenálló képességéről szóló irányelvjavaslatát (The Critical Entities Resilience Directive – CER). A tagállamoknak 2024. októberig kell beültetni az irányelvet a hazai jogba. A javaslat szakít a korábbi rendszerelem védelmére fókuszáló szemlélettel és helyére a kritikus fontosságú szervezetek működésének ellenálló képesség kialakítása kerül. Elfogadását követően az irányelv hatályánkívül helyezte a 2008-ban elfogadott, az európai kritikus infrastruktúrák azonosításáról és kijelöléséről szóló jelenlegi irányelvet. Ennek az volt az oka, hogy míg a 2008-as irányelv nem volt felkészülve azokra az új kihívásokra, amik a 2010-es években érték a világot. Például a digitális gazdaság térnyerésére, terrorveszélyre, Covid-19 világjárványra. Ezek mind rávilágítottak arra, hogy az uniós tagállamok között globális szinten is nagyfokú kölcsönös függőség áll fenn, tehát igény volt egy új, aktuális irányelv megalkotására.[41]

39 Az Európai Parlament és a Tanács 2022/2554 rendelete 28. cikk (8).

40 Az Európai Parlament és a Tanács 2022/2554 rendelete 45. cikk.

41 Az Eu Tanácsa: *Az EU rezilienciájának erősítése*, https://www.consilium.europa.eu/hu/press/press-releases/2021/12/20/strengthening-eu-resilien-

Az irányelv kilenc ágazatot sorol fel, amelyeket kritikus fontosságú szervként jelöl meg: közlekedés, energia, egészségügy, ivóvíz, szennyvíz, digitális infrastruktúra, űrágazat, banki szolgáltatások, pénzügyi piaci infrastruktúrák.[42] Az itt felsorolt ágazatoknak képesnek kell lenniük például a Covid19, terrorizmus, természeti katasztrófák megelőzésére, védelem biztosítására és az ellenálló képesség kialakítására.

A tagállamok számára is előír kötelezettségeket az irányelv. Négyévente kockázatértékelést kell végezniük és azonosítaniuk kell az alapvető szolgáltatásokat nyújtó, kritikus fontosságú szervezeteket, olyan releváns kockázat értékelése érdekében, melyek zavart okozhatnak.[43]

Az irányelv azonosítja a különös európai jelentőségű kritikus szervezeteket is. Akkor minősülhet egy szervezet kiemelt európai jelentőségű, kritikus fontosságú szervezetnek, ha a tagállamok közül hat vagy több állam számára nyújt alapvető szolgáltatásokat. A tagállamok ebben az esetben felkereshetik a Bizottságot, hogy az tanácsadó missziókat az érintett szervezetek kötelezettségeinek teljesítése érdekében bevezetett intézkedések értékelése céljából.[44]

Létrehoz az irányelv egy kritikus szervezetek rezilienciájával foglalkozó csoportot is, aminek a célja az, hogy segítse a tagállamok közötti együttműködést és az információcserét ezen irányelvvel kapcsolatban.[45]

---

ce-council-adopts-negotiating-mandate-on-the-resilience-of-critical-entities/

42 Az Európai Parlament és a Tanács (EU) 2022/2557 irányelve a kritikus szervezetek rezilianciájáról (5).

43 Az Európai Parlament és a Tanács (EU) 2022/2557 irányelve a kritikus szervezetek rezilianciájáról III. fejezet 12. cikk (1).

44 Az Európai Parlament és a Tanács (EU) 2022/2557 irányelve a kritikus szervezetek rezilianciájáról 18. cikk (1).

45 Az Európai Parlament és a Tanács (EU) 2022/2557 irányelve a kritikus szervezetek rezilianciájáról 19. cikk.

A CER és a NIS 2. irányelv kapcsán a tagállamok hangsúlyozzák, hogy a két irányelvet össze kell hangolni egymással. Tehát a kritikus fontosságú szervezetek rezilienciájáról szóló irányelv hatálya alá tartozó ágazatok a NIS 2. irányelv hatálya alá is tartozzon.[46]

4. Intézmények

4.1. Európai Uniós Hálózat- és Információbiztonsági Ügynökség

A hírközlő hálózatok és az információs rendszerek is a társadalmi fejlődés alapvető elemeivé váltak. Mindenhol jelen vannak: vízellátás, villamos energia stb. Alapvető prioritás ezeknek a rendszereknek a biztonságos működése, ugyanis egy esetleges baleset, támadás során ezeknek az infrastrukturális rendszereknek a meghibásodása óriási problémákat tudnak okozni a polgárok számára. Szükségessé vált egy olyan európai szintű szakértői központ létrehozása, amely iránymutatást és tanácsot ad, segítséget nyújt. Ezen igények kielégítése céljából az Európai Parlament és a Tanács a 460/2004/EK rendeletével létrehozta az Európai Hálózat- és Információbiztonsági Ügynökséget (továbbiakban: ENISA).[47]

Alapfeladatai között megjelenik a tagállamoknak való tanácsadás a tudatosság növelése érdekében, ugyanis a hálózati és információs rendszerek iránti bizalom biztosítása miatt szükséges

46 Az Eu Tanácsa: *Az EU rezilienciájának erősítése*, https://www.consilium.europa.eu/hu/press/press-releases/2021/12/20/strengthening-eu-resilience-council-adopts-negotiating-mandate-on-the-resilience-of-critical-entities (Letöltés: 2023.04.03.)

47 Az Európai Parlament és a Tanács 460/2004/EK rendelete az Európai Hálózat- és Információbiztonsági Ügynökség létrehozásáról (11).

az egyének, vállalkozások, közigazgatási szervek megfelelő tájékozottsága. Nemcsak a tagállamoknak nyújthat tanácsokat, hanem az Európai Parlament, a Bizottság, az európai szervek is részesülhetnek a segítségében. Tevékenységeivel elő kell segítenie a belső piac zavartalan működését, azzal, hogy kifejleszti a hálózat- és információbiztonság kulturáját. Szorgalmazza az együttműködést a Bizottság és a tagállamok között is, hogy megelőzzék a hálózat- és információbiztonsággal kapcsolatos problémákat, illetve azokra hatékonyan reagáljanak. Előmozdítja a kockázatértékelési tevékenységet (veszély meghatározása, a veszély jellemzése, a veszélyeztetettség mértékének felmérése és a kockázat jellemzése) és a megelőzés-kezelési megoldásokkal kapcsolatos kutatásokat a köz- és a magánszektorban működő szervezeteken belül. [48]

Az ENISA feladatkörének és céljainak teljesítése során nem sértheti a tagállamok hálózat- és információbiztonsággal kapcsolatos hatásköreit, illetve a közbiztonsággal, avédelemmel, a nemzetbiztonsággal kapcsolatos tevékenységeket sem.[49]

Az ENISA-t szervezetileg három rész alkotja: az igazgatóság, az ügyvezető igazgató, az érdekeltek állandó csoportja. Az igazgatóság a tagállamok egy-egy képviselőjéből, a Bizottság által kinevezett három képviselőből, a Tanács által kinevezett három képviselőből áll. Az igazgatóság fogadja el az ENISA belső működési szabályzatát, amit nyilvánosságra kell hozni. Az ügyvezető igazgató az ENISA vezetője, aki a feladatok ellátásában független. Az igazgatóság nevezi ki a Bizottság javaslata alapján, maximum öt évre. Az érdekeltek állandó csoportja az információ- és hírközléstechnológiai iparágat, a fogyasztói csoportokat és a hálózat- és információbiztonsággal foglalkozó tudományos szakértőket képviseli. A csoport tanácsokkal

48 Az Európai Parlament és a Tanács 460/2004/EK rendelete 3. cikk.
49 Az Európai Parlament és a Tanács 460/2004/EK rendelete 1. cikk (3).

láthatja el az ügyvezető igazgatót a meghatározott feladatainak ellátásához.[50]

Az ENISA létrehozása óta rengetek technológia változás, társadalmi-gazdasági folyamatok, piaci fejlemények történtek, melyek szükségessé tették a 2004-es rendelet átreformálását. AZ Európai Parlament és a Tanács 526/2013/EU rendeletének a célja, hogy megerősítsék az ENISA-t annak érdekében, hogy még nagyobb sikerrel járulhasson hozzá az uniós intézmények és a tagállamok olyan erőfeszítéseihez, amelyekkel európai kapacitást szándékoznak létrehozni a hálózat- és információbiztoság területén jelentkező kihívások kezelésre.[51] A 2013-as rendelet kiemeli, hogy a digitális gazdaság méretére való tekintettel, meg kell növelni az Ügynökség számára elkülönített pénzügyi és emberi erőforrásokat. Továbbra is tanácsokkal kell ellátnia a Bizottságot, a tagállamokat, a hivatalokat, az uniós intézményeket.

Az uniós hálózat- és információbiztonság magas szintjének biztosítása érdekében a számítógép-biztonsági és incidenskezelő csoportok (CSIRT) és a hálózatbiztonsági vészhelyzetekkel elhárító csoportok (CERT) közötti együttműködést ösztönöznie kell.[52]

Az ENISA-ról hozott két rendelet nem tudta hatékonyan felvenni a kibertámadásokkal való harcot, mert a megbízatása korlátozta. Felül kell vizsgálni az ENISA megbízatását a megváltozott kiberbiztonsági helyzetben, annak érdekében, hogy hatékonyabban tudjon hozzájárulni a kiberbiztonsági kihívásokra uniós szinten. Az Európai Parlament és a Tanács 2019/881 rendeletében egy még erősebb intézkedécsomagot fogadtak el

50 Az Európai Parlament és a Tanács 460/2004/EK rendelete 6–8. cikk.

51 Az Európai Parlament és a Tanács 526/2013/EU rendelete az Európai Uniós Hálózat és Információbiztonsági Ügynökségről (ENISA) és a 460/2004/EK rendelet hatályon kívül helyezéséről (11).

52 Az Európai Parlament és a Tanács 526/2013/EU (31).

az ENISA-ról. A 2019-es rendelet értelmében minden eddigi ENISA-ról hozott rendeletben meghatározott feladatát továbbra is el kell látnia. Az ENISA-nak segítenie kell az (EU) 2016/1148 irányelvben foglaltak megvalósítását. (NIS 1. irányelv).[53]

A reform keretében az ENISA a korábbi mandátumához képest állandó megbízást kapott, amely egyébként kiterjedt a szintén újításként megteremtett tanúsítási rendszerek kidolgozásában való közreműködésre is.[54]

Az ENISA-nak együtt kell működni a a különböző nemzetközi szervezetekkel, az OECD-vel, az EBESZ-szel és a NATO-val. Az együttműködés kiterjedhet közös kiberbiztonsági gyakorlatokra, illetve biztonsági eseményekre való reagálás közös koordinációjára is. Továbbá támogatnia kell a CSIRT-ek és a CERT-EU operatív együttműködését.[55]

Feladatkörét tekintve három területre lehet szétosztani. Elsősorban gyakorlati tanácsokkal és megoldásokkal szolgál, amely támogatja a tagállamokat a nemzeti kiberbiztonsági stratégiák kidolgozásában. Másrészt tanulmányokat és jelentéseket készít. Végül pedig közreműködik a hálózat- és információbiztonságra vonatkozó uniós szakpolitikák és jogszabályok megszövegezésében.[56]

Tevékenységét éves munkaprogramok határozzák meg. Az ENISA szoros együttműködésben áll az Európai Rendőrségi Hivatallal (EUROPOL) és a Számítástechnikai Bűnözés Elleni Európai Központtal is.[57]

---

53 Az Európai Parlament és a Tanács (EU) 2019/881 rendelete az ENISA-ról és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívüli helyezéséről (16).

54 COM (2017) 477.

55 Az Európai Parlament és a Tanács (EU) 2019/881 rendelete.

56 Az Európai Parlament és a Tanács 2019/881 rendelete, https:// eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32019R0881&from=EN (Letöltés: 2022.10.12.)

57 Az Európai Parlament és a Tanács 526/2013/EU rendelete (28).

A 2019-es rendelet átalakította az ENISA struktúráját. Az igazgatótanács, a felügyelőtestület, az ügyvezető igazgató, az ENISA tanácsadó csoportja és a nemzeti kapcsolattartó tisztviselők hálózata alkotja a szervezetét. Az igazgatótanács tagállamonként egy, a Bizottság által kijelölt két tagból áll. Feladatuk az ENISA működésének irányát meghatározni, elfogadni a költségvetést, felügyelni a működést. Az egyik újítás a 2013-as rendelethez képest a szervezeti felépítésben a felügyelőtestület bevezetése. A felügyelőtestület segíti az igazgatótanács munkáját, illetve elkészíti az igazgatótanács által elfogadandó határozatokat. A felügyelőtestület öt tagból áll. Az ügyvezető igazgató vezeti az ENISA-t. A másik új elem az ENISA tanácsadó csoportja. A csoport releváns érdekelt felekből (pl. IKT-ágazatot, nyilvánosan elérhető elektronikus hírközlési szolgáltatások nyújtóit, kiberbiztonság területén tevékenykedő tudományos szakembereket), képviselő elismert szakértőkből, illetékes hatóságokból, európai szabványügyi szervekből, bűnüldözői hatóságokból és adatvédelmi felügyeleti hatóságokból áll. Ahogy a nevéből is látszik feladata a tanácsadás az ENISA feladatainak ellátásával kapcsolatban. A harmadik új szervezeti elem a nemzeti kapcsolattartó tisztviselők hálózata, mely a tagállamok képviselőiből áll. Feladatuk, hogy megkönnyítsék az ENISA és a tagállamok közötti információcserét.[58]

4.2. Europol Számítástechnikai Bűnözés Elleni Központ (EC3)

Az Europol 1999. július 1-jén kezdte meg a működését, miután a tagállamok ratifikálták az Europol-egyezményt. 2010 januárjában az Europol új jogi kerettel és kiterjesztett feladatkörrel rendelkező, teljes jogú uniós ügynökséggé vált. (Európai Rendőr-

58 Az Európai Parlament és a Tanács (EU) 2019/881 rendelete az ENISA-ról 13–23. cikk.

ségi Hivatal (Europol) létrehozásáról szóló 2009. április 6-i, 2009/371/IB számú tanácsi határozat alkotta meg.)[59] Hivatalos ügynökséggé válása után az integráltabb együttműködés kialakítása volt a fő feladata.

Az Europol az Európai Unió bűnüldöző hatósága, melynek fő feladat az EU biztonságosabbá tétele. Feladatkörébe tartozik az EU-tagállamok hatóságainak támogatása, a kölcsönös információmegosztás a nemzeti rendőrségekkel és a bűnügyi adatok szakszerű elemzése. A nagy kiterjedésű bűnszervezetek és terrorista hálózatok fenyegetése miatt erősebb szabályozásokra volt szükség, ezért 2016 májusában hatályon kívül helyezték a 2009/371/IB tanácsi határozatot és új lépéseket kellett bevezetnie az Europolnak.[60]

2012 márciusában nyújtotta be az Európai Bizottság a javaslatát a számítástechnikai bűnözés elleni küzdelem európai központjának létrehozására (továbbiakban EC3), amely a Stockholmi Program egyik fontos eleme.[61] Az EC3-at Hágában az Európai Rendőrségi Hivatalon belül hozták létre, működését 2013. január 11-én kezdte. Céljaiban kitűzte, hogy egy kapcsolattartó pontként működjön a számítástechnikai bűnözés elleni küzdelemben, részt vegyen az unión belüli rendészeti koordinációban, operatív támogatással segítse a tagállami rendészeti szerveket a konkrét nyomozások során.

---

59 Tájékoztató az EUROPOL rendszerről, https://www.naih.hu/europol/tajekoztato-europol-rendszerrol (Letöltés: 2023.04.02.)

60 Az Európai Parlament és a Tanács (EU) 2016/794 rendelete a Bűnüldözési Együttműködés Európai Uniós Ügynökségéről (Europol), valamint a 2009/371/IB, a 2009/934/IB, a 2009/935/IB, a 2009/936/IB és a 2009/968/IB tanácsi határozat felváltásáról és hatályon kívül helyezéséről.

61 Az Európai Tanács tájékoztatása. A Stockholmi Program 2010. https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=LEGISSUM%3Ajl0034 (Letöltés: 2023.04.03.)

A számítástechnikai bűnözés három fő területére is kitér: 1. a szervezett bűnözői csoportok által elkövetett számítástechnikai bűncselekmények 2. olyan számítástechnikai bűncselekmények, amelyek súlyos kárt okoznak az áldozataiknak pl. gyermekek szexuális kizsákmányolása 3. olyan számítástechnikai bűncselekmények, melyek az Unión belüli kritikus infrastruktúrákat és információs rendszereket érintik.[62]

Az EC3-nak öt feladatkörét említeném: 1. Adatokat gyűjt a számítógépes bűnözésről: ezeket az adatokat feldolgozzák a tagállami nyomozó hatóságok részére. 2. Támogatja a közös nyomozócsoportok létrehozását a tagállamok számára, ezzel is koordinálva a tagállamok közötti együttműködést a számítógépes bűncselekmények nyomozásában. Az Eurojusttal és az Interpollal is szoros együttműködésben áll. 3. Elemzi a kibertérből érkező fenyegetéseket és ezekből igyekszik előrejelezni a számítógépes bűnözés alakulását. 4. CERT-ekkel kapcsolattartás a minél hatékonyabb fellépések érdekében 5. Szorosan együttműködik a tagállamok nyomozó hatóságaival és igazságügyi szervezeteivel.[63]

5. Közös biztonság és védelempolitika

Az Európai Unió közös biztonság és védelempolitikája (Common Security an Defence Policy, CSDP) elengedhetetlen szerepet tölt be a nemzetközösség együttes kül- és biztonságpolitikájában. A 2009-es lisszaboni szerződés vezette be a CSDP fogalmát és

62 Bizottság közleménye a Tanácsnak és az Európai Parlamentnek: Küzdelem digitális korunk bűnözésével: Számítástechnikai Bűnözés Elleni Európai Központ létrehozása 2012. 03. 28.

63 Gyaraki Réka: A nemzetközi intézmények szerepe a kiberbiztonságban, In: Török Bernát (szerk.) *Információ-és kiberbiztonság*, Budapest, 2020. 192–193. o.

létrehozta a kölcsönös védelmi záradékot (Treaty on European Union Article 42).[64]

A 2013. évi kiberbiztonsági stratégia (melyet a korábbi fejezetben kifejtettem). A stratégia releváns a közös biztonság és védelempolitika tekintetében is, ugyanis a belső biztonság kérdéseit a külső biztonság kihívásaival egyeztette össze, tehát az Európai Unió biztonságvédelmének két szintjét kapcsolta össze. [65]

2014-ben az Európai Tanács elfogadta az első kibervédelmi politikai keretrendszert. A keretrendszer kibervédelmi és nemzetközi kiberpolitikai célokat tűzött ki az EU tagállamai számára, mint például: a tagállamok CSDP-vel kapcsolatos kibervédelmi képességeinek fejlesztése, CSDP kommunikáció hálózatainak védelme, oktatási, továbbképzési lehetőségek fokozása, erősíteni a nemzetközi partnerekkel való együttműködést.[66]

Mivel a 2013. évi kiberbiztonsági stratégia nem hozta meg a kívánt eredményeket, ezért arra ösztönözte az Európai Uniót, hogy újabb erőfeszítéseket tegyen a védelem érdekében. 2017-ben el is fogadták az új kiberbiztonsági stratégiát. A CSDP szempontjából ez a stratégia a kiberbiztonsági elrettentés kiépítésére összpontosít a tagállamok védelmi képességeinek felhasználásával.

2017. évi stratégia alapján az EU közös kiberbiztonsági tanúsítási keretrendszerét (Cyber Defence Policy Framework) 2018-ban frissítették. Ezt a kiberképességek fejlesztése és a CSDP támogatása miatt kezdeményezték.

---

64 Kölcsönös védelmi záradék, https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=LEGISSUM:mutual_defence (Letöltés: 2023.03.12.)

65 Wessel A. Ramses: Towards EU Cybersecurity Law. Regulating a New Policy Field. In: Nicholas Tsagourias – Russell Buchan (Eds.): *Research Handbook on International Law and Cyberspace*, H. n., Edward Elgar Publishing, 2015. 403–426.

66 Council Of the European Union: EU Cyber Defence Policy Framework (2014. november 18.).

Fontos leszögezni, hogy a CSDP kibervédelmének katonai koncepciója a tagállamok képességein és együttműködésén alapszik. A biztonság és védelem területén a tagállamok nemzeti érdekeket támasztanak.[67]

2020-ban jelent meg az EU új kiberbiztonsági stratégiája (EU kiberbiztonsági stratégiája a digitális étvizedre)[68]. Az új stratégia szerint a tagállamoknak növelniük kell a kiberfenyegetések megelőzésére és azokra való reagálás képességét. A kiberbiztonsági stratégiával összhangban a CDSP számára a következő stratégiai pontok váltak meghatározóvá: Az EU-nak tovább kell folytatnia a vonatkozó CSDP-struktúrák csatlakozását a NATO szövetségi missziói hálózatához, a CSDP katonai missziói és műveletei számára az EU katonai elképzelésének és stratégiájának kidolgozása a kibertérben, a polgári CSDP-paktum keretében a polgári CSDP-missziók hozzájárulhatnak az EU szélesebb körű munkájához a kiberbiztonsági kihívások leküzdésében.[69]

6. Kiberdiplomácia

6.1. Kiberdiplomácia meghatározása

A kiberdiplomáciának – ahogyan az a kibertér fogalmának esetére is igaz – nincsen pontos tudományos meghatározása. A kiberdiplomácia a kibertérben folytatott diplomáciaként definiálható,

67 O. Moskalenko – V. Streltsov: Shaping a 'hybrid' CFSP to face 'hybrid' security challenges. *European Foreign Affairs Review,* 22. 2017/4. 513–532. o.

68 European Commission: The EU's Cybersecurity Strategy for the Digital Decade.

69 Bihaly Barbara: A kibervédelem szerepe az Európai Unió közös biztonsági és védelmi politikájában, *Hadtudományi Szemle*, 2021/3. 52. o.

vagyis a diplomáciai erőforrások felhasználása, illetve a diplomáciai funkciók ellátása a kibertérben a kibertérrel kapcsolatos nemzeti érdekek biztosítása érdekében.[70] A kibertér számos olyan jellemzőt halmozott fel, amelyek az érdekelt felek közötti diplomáciai kötelezettségvállalást jelentik. Először is, ez egy globális terület, amely összeköti a világ országait/nemzeteit és polgárait, ahol különböző módokon kölcsönhatások és súrlódások keletkeznek közöttük. Egy ilyen nagy globális közös javaknak a mindenki számára való hozzáférés biztosítása és a konfliktusok elkerülése érdekében szükség van minimális szabályokra és előírásokra, amelyeket csak a diplomáciai tárgyalások eredményeként lehet létrehozni.[71]

6.2. Kiberdiplomácia megjelenése az Európai Unióban

2015-ben látott napvilágot az a dokumentum, amely először használta a kiberdiplomácia kifejezést az Európai Unióban. Ezen dokumentum célnak tűzte ki, hogy megvédi az emberi jogokat és biztosítja, hogy az internettel ne lehessen visszaélni , de továbbra is a szabad véleménynyilvánítás fóruma maradjon. Továbbá az uniós diplomácia és a jogi eszközök segítségével igyekszik megakadályozni a kiberbiztonsági fenyegetéseket és hozzájárul a nemzetközi kapcsolatok stabilitásának növekedéséhez.[72]

Az Európai Unión belüli szakpolitikák mélyülése megkövetelte, hogy a diplomáciai eszköztárat megerősítsék. A nagyobb védelem érdekében az Európai Unió Tanácsa 2017-ben

70 André Barrinha – Thomas Renard: Cyber-diplomacy: the making of an international society in the digital age, Global Affairs, 2017. 3:4–5, 353–364.

71 S. J. Buck: *The global commons: An introduction*, Washington DC, Island Press, 1998. 6. o.

72 Az Európai Unió Tanácsa, 2015. A Tanács következtetései a kiberdiplomáciáról.

megegyezett abban, hogy az Unió politikai, biztonsági és gazdasági érdekeinek széleskörű védelme érdekében kialakít egy közös uniós diplomáciai keretrendszert az állami és nem állami szereplők által végrehajtott rosszindulatú és szándékos kibertevékenységek ellen. Ez a megállapodás létrehozta a kiberdiplomáciai eszköztárat (EU Cyberdiplomacy Toolbox)[73] A Tanács azt szerette volna megvalósítani a Toolboxxal, hogy a közös uniós diplomáciai intézkedések keretében előmozdítsák a veszélyek csökkentését. Továbbá döntöttek arról is, hogy a kibertámadások körében alkalmazni fogják a közös kül-és biztonságpolitika területéhez tartozó intézkedéseket is, vagyis akár az esetleges szankciós intézkedéseket is. A szankcióknak a nemzetközi joggal összefüggésben arányosnak kell lenniük a kibertevékenység által okozott hatásokkal.[74]

A Politikai és Biztonsági Bizottság 2017 októberében végrehajtási iránymutatásokat fogadott el a kiberdiplomáciai eszköztárra vonatkozóan. Öt kategóriát sorol fel a dokumentum:

– megelőző intézkedések;
– együttműködési intézkedések;
– stabilitást szolgáló intézkedések;
– korlátozó intézkedések;
– lehetséges uniós támogatás a tagállamok jogszerű válaszaihoz.[75]

Az Európai Unió tagállamait fenyegető kibertámadásokkal szemben 2019-ben kiadták a KKBP-határozatot[76] és egy új

73 13007/17 – Implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities.

74 Council of the European Union (2017a): Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities – approval of the final text, Brussels, 9 October 2017.

75 Agnes Kasper – Anna-Maria Osula – Anna Molnár: *EU cybersecurity and cyber diplomacy*, 2021. 8. o.

76 Tanács (KKBP) 2019/797. határozata.

tanácsi rendeletet.[77] Ezen dokumentumok a rossz szándékú és a szándékos kibertevékenységekkel szembeni közös uniós korlátozó intézkedések alkalmazhatóságának kérdéséről döntött és a kibertámadásokra válaszul adott szankciók alkalmazását teszik lehetővé. Ezzel a jogi aktussal tehát az Európai Uniónak lehetősége lett szankciókat kivetni (például utazási tilalom, bizonyos eszközök befagyasztása).[78] 2020. júliusában valósult meg először gyakorlatban a szankciók alkalmazása 6 személy és 3 szervezet ellen, akikről kiderült, hogy az uniós tagállamok elleni különböző kibertámadásokért felelősek.[79]

7. Összegzés

A 2000-es évek elején a digitalizáció és az IKT-eszközökkel kapcsolatos kérdésköröket az Európai Unió jogalkotói és döntéshozói csupán gazdasági oldalról közelítették meg. A 2013-as kiberbiztonsági stratégia mondható egy fontos állomásnak az EU kiberbiztonsági intézkedéseinek körében, ugyanis innentől kezdve álltak neki biztonságiasítani a kiberteret.

A Cyberdiplomacy Toolboxban foglalt korlátozó intézkedések aktiválása egy mérföldkővé vált az EU kibertérben folytatott rosszindulatú tevékenységekre való reagálás közös megközelítésének kialakításában. A szankciórendszer hasznos lehet a tagállamok közötti együttműködés fellendítésére is, ugyanis az ilyenfajta korlátozó intézkedések meghozatalára az Európai Unió Tanácsára van szükség. Az egyes államok ellenállóképes-

77 Tanács (EU) 2019/796 rendelete.

78 Kelemen Roland: III.2. Az Európai Unió szerepe a kibertér biztonsági aspektusaiban, In: Farkas Ádám – Kelemen Roland: *Nemzeti biztonság és kibertér,* Budapest, Médiatudományi Intézet, 2023. 134., 137–138. o.

79 Regulation EU 2020/1124 of 30 July 2020.

ségének javításában és ezzel előmozdítva a releváns uniós jogszabályoknak (például NIS-irányelv) való megfelelést is szolgálja. Természetesen nem teljesen kikövetkeztethető, hogy a szankciók 100%-ig beválnak és a jövőbeli kiberfenyegetéseket sikerül elrettenteni, de az EU mindenesetre megadta az eszközt, hogy sikeresebben lehessen kezelni ezeket a helyzeteket. A tanulmányban említett dokumentumok elemezve világossá válik az Európai Unió törekvése, egy olyan Európa létrehozása, amely ellenáll és megvédi az egyéneket, államokat a kibertérben előforduló támadások, fenyegetésekkel szemben. Olyan stratégiákat alakít ki, amely gyors reagálási képességet és erősebb védelmet alakít ki. A rendelkezések mind olyan intézkedéseket kívánnak létrehozni, amelyek összehangolják a tagállamokat, így tovább erősítve az Unió kiberbiztonságát. Az EU kiberbiztonsági szabályozásai biztonságosabb online környezetet biztosítanak mindenkinek, az internetes adatvédelem és a személyes adatok védelme érdekében. Az EU által hozott kiberbiztonsági szabályozások összességében azt mutatják, hogy az EU kiemelten fontosnak tartja a kiberbiztonság javítását és a kiberbiztonsági fenyegetések elleni küzdelmet, valamint a digitális gazdaság és társadalom védelmét. Az EU arra törekszik, hogy a kiberbiztonsági szabályozások folyamatosan fejlődjenek, és a jövőbeli kiberbiztonsági kihívásokra is hatékony válaszokat adjanak.

Szerzőink

Dr. Csillik Kristóf PhD hallgató, ELTE ÁJK, ügyvédjelölt, Bassola Ügyvédi Iroda

Hordós Alex egyetemi hallgató, ELTE ÁJK, a Bibó István Szakkollégium tagja

Lukács Bence közgazdász (BSC), mesterszakos egyetemi hallgató, Széchenyi István Egyetem Kautz Gyula Gazdaságtudományi Kar

Dr. Takó Dalma tanársegéd, Széchenyi István Egyetem Deák Ferenc Állam- és Jogtudományi Kar, az MKJHT tagja

Varró Tekla egyetemi hallgató, katasztrófavédelem mesterképzési szak Nemzeti Közszolgálati Egyetem Katasztrófavédelmi Intézet

Krebsz Klaudia egyetemi hallgató, Széchenyi István Egyetem Deák Ferenc Állam- és Jogtudományi Kar

Szladik Míra nemzetközi kapcsolatok szakértő (BSc), mesterszakos hallgató Széchenyi István Egyetem Deák Ferenc Állam- és Jogtudományi Kar

Szerzői útmutató

A Katonai Jogi és Hadijogi Szemle magyar nyelven beküldött, az e folyóiratot kiadó Magyar Katonai Jogi és Hadijogi Társaság által művelt tudományos vagy szakmai területhez kapcsolódó – az alábbi formai követelményekhez illeszkedő – kéziratokat (tanulmányokat, recenziókat) fogad be.

Általános feltételek

A kéziratok terjedelme tudományos közlemény esetében legalább 20.000 karakter (fél ív) lehet, és nem haladhatja meg a 80.000 karaktert (2 ív). Könyvismertetés vagy tudományos értékű hozzászólás nem haladhatja meg a 20.000 karaktert.

A kézirat megküldésekor a szerző kilétét úgy kell feltüntetni, ahogyan azt a szerző a folyóiratban megjelentetni szeretné.

A fő szöveget, a címet, a fejezetcímek és az alcímek times new roman betűtípussal és 12-es betűmérettel kérjük formázni. A fő szöveg esetében kérjük a szimpla sorközt és a sorkizárt beállítást alkalmazni. A címet, a fejezetcímet, alfejezet címet követően kérjük kizárólag egy sorköz (enter leütése) szerepeljen. Kerülni kell a behúzásokat, tabulátorokat, térközöket és egyéb formázásokat.

Kiemelések a szövegben és lábjegyzetben kizárólag dőlt betűvel lehetségeseket, kérjük kerülni a ritkítás, az aláhúzás, a vastag betű stb. használatát.

A táblázatokat és ábrákat megfelelően formázva, a forrást hivatkozva, képaláírással ellátva kell feltüntetni. Táblázatok esetében kérjük, hogy a maximális méret egy B5-ös oldalt ne haladja meg.

A szöveg tagolása decimális számozással jelölt fejezetcímekkel (például 1.), illetve alcímekkel lehetséges (például: 1.1.1.). Kérjük az automatikus számozás mellőzését. Maximális háromszintű tagolást (például: 3.4.1.) kérünk alkalmazni.

Felsorolások esetében elsődlegesen decimális jelölést alkalmazzunk, ahol kérjük szintén a maximális három szint betartását.

Hivatkozások

A hivatkozásokat lábjegyzetben kérjük feltüntetni, több hivatkozás esetében pontosvessző használatával. A lábjegyzetbe a fő szövegben idézett vagy ott felhasznált forrásokat kell hivatkozni. Kérjük kerülni a végjegyzetet vagy a szövegben történő hivatkozást. A lábjegyzetben egy műre történő első hivatkozás esetében az összes bibliográfiai adatot fel kell tüntetni. A későbbi hivatkozások esetén elég az i. m. használata (pl. Mezey: i. m. 23. o.). Ha ugyanazon szerzőtől több művet is idézünk akkor az i. m. után zárójelben tüntessük fel a művek kiadási évét [pl. Mezey: i. m. (2003) 23. o.]. Ugyanazon szerzőtől, azonos évben megjelent műveinek ismételt idézése esetén abc jelölést kérjük alkalmazni a hivatkozás sorrendjében [pl. Mezey: i. m. (2003a) 23. o.]. Lábjegyzet esetében fontos hangsúlyozni, hogy az minden esetben mondatnak minősül, így mindig nagybetűvel kezdődik és ponttal zárul. Sem a szövegben, sem a lábjegyzetben nem kell feltüntetni az idézett mű szerzőjének titulusát (vagyis a dr. rövidítést sem).

Hivatkozások módszerei

a) könyvek

Ferdinandy Gejza: *A magyar alkotmány történelmi fejlődése*, Budapest, Franklin-Társulat magyar irod. intézet és nyomda, 1906. 45. o.

b) gyűjteményes művek

Hans Kelsen: Ki legyen az alkotmány őre?, In: Takács Péter (szerk.): *Államtan – Írások a XX. századi általános államtudomány köréből*, Budapest, Szent István Társulat, 2003. 289–332. o.

c) folyóiratcikkek

Patyi András: Hatáskör és eljárás a magyar közigazgatási bíráskodás történeti modelljében, *Magyar Közigazgatás*, 2001/11. 655–667. o.

d) elektronikus források

Paál Vince (szerk.): *Magyar sajtójogi szabályok annotált gyűjteménye 1848-1989* (http://mtmi.hu/).

e) jogszabályok

A független magyar felelős ministerium alakításáról szóló 1848. évi III. törvénycikk.

f) országgyűlési napló és irományok

Pulszky Ágost a közigazgatási bíróságról szóló törvényjavaslatot megvitató bizottság képviselőházi előadója ismertette a bizottság álláspontját a képviselőház előtt, *Képviselőházi napló*, 1892. XXXIII. kötet, 1896. május 11. – június 30., 624. ülésnap.
Lukács László miniszterelnök indokolása a háború esetére szóló kivételes intézkedésekről szóló törvényjavaslathoz, *Képviselőházi irományok*, 1910. XXII. kötet, 633. számú iromány.

Szerkesztőség a formai kritériumoktól eltérő kéziratokat visszaküldi a szerzőnek javítás céljából.