Bartkó Róbert – Sántha Ferenc

A kibertér műveletek büntetőjogi értelmezésének lehetőségei, különös tekintettel a nemzetközi bűnügyi együttműködésre

Military and Intelligence CyberSecurity Research Paper
2023/2.


UNIVERSITY OF PUBLIC SERVICE
LUDOVIKA

1.BEVEZETŐ GONDOLATOK

A számítástechnika evolúciója, az elmúlt évtizedben bekövetkezett exponenciális térhódítása jól mutatja meghatározó szerepét világunkban nemcsak a hagyományos értelemben felfogott hétköznapokban, hanem a gazdaságban, az államigazgatásban és a fegyveres erőknél is[1]. A XXI. század dinamikus változásainak hangsúlyosnak mondható dimenzióját adja a kibertér és az infokommunikáció fejlődése[2]. A technológiai vívmányok nemcsak segítik a társadalmi élet különböző területeit, az állampolgárok mindennapjait, de nagymértében mutatnak rá annak sebezhetőségére is. A hálózati összekapcsoltság térnyerése táptalaja a kibertámadásoknak[3], mely jól mutatja milyen mértékű függőségünk alakult ki jelen századunkra a kritikusnak tekinthető infrastruktúrák működésétől[4]. A modern technika segítségével számos kriminalitás az informatikai térben is megvalósítható lett, miközben az újabb és újabb elkövetési formák elleni fellépés komoly kihívás elé állítja a jogalkotókat, ebben a küzdelemben pedig a büntetőjogi és büntetőjogon kívüli eszközök igénybevétele közötti határvonalat – a szükségesség, arányosság, célszerűség elvei mentén – egyre nehezebb definiálni. Az informatika oly mértékben határozza meg mindennapjainkat, hogy kijelenthető, már nem mi vagyunk annak tulajdonában, amit létrehoztunk, hanem az ural bennünket[5]. Azaz a fejlődés előnyei egyben hátrányok, nehézségek előállását is generálják, mint ahogyan arra *Nagy Zoltán* is hivatkozik cikkében Napoleon Hill gondolatának inverz értelmezésében[6].

Ebben a környezetben érthető, hogy egyre több kutatás foglalkozik az információtechnológia fejlődésével összefüggő modernkori kihívásokkal. Vonatkozik ez természetesen nem pusztán a jogon kívüli, hanem a jog által uralt tudományterületekre, értelemszerűen azon belül a tágabb értelemben vett büntetőjogra is. Helyesen utal rá *Szathmáry Zoltán* 2022-es írásában, hogy az információs rendszerek felhasználásával elkövetett, vagy éppen az azokat támadó különféle bűncselekményekkel, a kibertérben rejlő társadalomra veszélyes aktivitásokkal, a témával kapcsolatos kriminalisztikai természetű problémákkal számos tanulmány foglalkozott már eddig is a hazai jogirodalomban, és ezek

[1] KELEMEN Roland – PATAKI Márta: A kibertámadások nemzetközi jogi értékelése. *Katonai Jogi és Hadijogi Szemle,* 2015/1. 53. o.
[2] FARKAS Ádám: A kibertér műveleti képességek kialakításának és fejlesztésének egyes szabályozási és államszervezési alapjai. *Jog-Állam-Politika,* 2/2019. 63. o.
[3] MEZEI Kitti: A modern technológiák kihívásai a büntetőjogban, különös tekintettel a kiberbűnözésre. *Állam és Jogtudomány,* 2020/4. 69.o.
[4] VIKMAN László: Szempontok a kibertér egyes aktuális fenyegetéseinek jogi értékeléséhez. *Military and Intelligence Cybersecurity Research Paper,* 2022/4. 3. o.
[5] McKenzie, WARK „Hackerkiáltvány" c. munkáját idézi: SZABÓ Alíz: Az online-térben terjedő deviancia, a cybercrime az információtechnológia tükrében. *Infokommunikáció és Jog,* 2017 Különszám, 60.
[6] NAGY Zoltán András: Kiberbűncselekmények, kiberháború, kiberterrorizmus – avagy ébresztő Magyarország! *Magyar Jog,* 2016/1. 17. o.

száma folyamatosan bővül[7]. Ez természetesen érthető és indokolt is, hiszen a kibertámadások által megvalósított bűncselekmények száma fokozatosan nő a kriminálstatisztikában, egyre „gyakoribbak a célzott és komplex támadások, különösen, amelyek a kritikus infrastruktúrákat érintik”[8]. A kiberbiztonság ezért az elmúlt időszakban a nemzetbiztonsági stratégia egyre hangsúlyosabb elemévé kezdett válni[9], hiszen az államnak is feladata – egyben érdeke is - állampolgárai védelmén túl saját biztonsági stabilitásának garantálása. A kibertámadások által okozott károk jelentősen túlmutatnak az adott „attack”-el érintett pénzügyi, vagy gazdasági terület érdekein, veszélyeztethetik a társadalom alapvető működését, ráadásul a kibertér a modernkori hadviselés egyik kiemelt eszközévé is vált[10].

A kiberbiztonság ezért kiemelt kutatási terület lett az elmúlt 10 évben hazánkban is, melynek ékes példája a Katonai Nemzetbiztonsági Szolgálat által koordinált kutatási program. A kormányzati támogatás mellett több évet átívelő és számos tudományterületet érintő interdiszciplináris projekt a mesterséges intelligencia alkalmazási irányait és a továbbfejlesztés lehetőségeit vizsgálja. Jelen tanulmány ezen kutatási program részeként alapvetően büntető anyagi jogi tárgyú kérdésre, a nemzetközi bűnügyi együttműködés területére fókuszál, ezzel mintegy hiánypótló kiegészítést szolgáltat az információtechnológiával kapcsolatos büntetőjogi tárgyú hazai szakmai cikkek sorában, azzal, hogy kizárólag az anyagi, illetve érintőlegesen az eljárási jog terrénumához kapcsolódó együttműködési formák kerülnek kiemelésre tanulmányunkban, a végrehajtási joghoz kapcsolódók, valamint a kifejezetten a felderítés eredményességét szolgálók nem. Ezen felül hangsúlyozzuk, hogy az egyes együttműködési formák részletszabályainak bemutatása sem tárgya jelen tanulmánynak. Célunk arra a kérdésre választ találni, hogy rendelkezésre állnak-e, s ha igen, milyen formában azon eszközök, melyek révén egy magyarországi sértettet – legyen az természetes vagy nem természetes személy - támadó kiberbűncselekmény elkövetőjével szemben a magyar hatóságok folytathatják le a büntetőeljárást.

Ahhoz azonban, hogy a nemzetközi bűnügyi együttműködés eszközrendszerét a kibertámadásokkal[11] szembeni küzdelem fókuszából be tudjuk mutatni, bizonyos előfeltételek fennállását feltételeznünk kell. Így – minthogy a tanulmány jellemzően anyagi jogi optikájú –

---

[7] SZATHMÁRY Zoltán: Hacking – Az információs rendszer és adat elleni bűncselekmény értelmezése. *Infokommunikáció és Jog,* 2022/2. 6.o.

[8] MEZEI Kitti: A kiberbűncselelmények hazai szabályozásának aktuális kérdései. *Magyar Jog,* 2019/5, 314. o.

[9] CSÁNYI Csaba: A Magyarországot érintő aktuális nemzetbiztonsági kihívások és az azokra adható lehetséges jogi válaszok. *Magyar Jog,* 2021/7-8., 475. o.

[10] Többek között ezen tényeknek is köszönhető, hogy az Európai Parlament 2022. novemberében két fontos területen is jelentős előrelépést tett, hiszen elfogadta a hálózati és információs rendszerek biztonságáról szóló irányelvet, valamint a digitális infrastruktúrák védelmét javító szabályrendszert. Ehhez kapcsolódik továbbá a kiberbiztonság elérése érdekében a magyar Parlament által elfogadott 2023. évi XXIII. tv. is a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről.

[11] Ehelyütt szükséges utalni arra, hogy a tanulmány a kibertámadásokkal nem tágabb értelemben foglalkozik, hiszen a bűnügyi együttműködés rendszere és eszközei bűncselekményi tényállást megvalósító támadások esetén relevánsak. Szintén nem célunk az úgynevezett „kiberműveletek”, így a kibertámadás, a kibervédelem és információszerzés hármasának elméleti bemutatása, hiszen ezen alapvetően más optikával közelítenek az információtechnológia jelentette modern kori kihívásokhoz.

felderítési kérdésekkel a felderítés során jelentkező nehézségekkel, kriminalisztikai, vagy bizonyítási kihívásokkal nem foglalkozunk, bár az tényszerűen rögzíthető, hogy az unióban a rendőri együttműködés a bűnügyi együttműködés legdinamikusabban fejlődő területe[12] lett. Kiindulópontunk, hogy az együttműködési rendszer szempontjából figyelembe vehető tényállás mind az alanyi oldal, tehát az elkövető, mind pedig a tárgyi oldal, azaz az adott kibertámadás által megvalósított bűncselekmény objektív tényállási eleminek szintjén felderített, nem állnak fenn a cselekmény büntetendőségét, vagy az elkövető büntethetőségét érintő akadályok, és – amely együttműködési formák esetében ez releváns – az ún. kettős inkrimináció feltételeinek is maradéktalanul megfelel[13].

Tanulmányunk alapvetően négy gondolati sík köré szerveződik. Egyrészt röviden foglalkozik a kiberbűncselekmény fogalmával, az ezzel kapcsolatos tudományos álláspontokkal, valamint a fogalmi alapvetés keretei között a joghatóság szempontjából lényeges főbb elvi tételekkel. Ezt követően három modell keretei között vizsgáljuk a kutatás tárgyát, illetve bontjuk ki annak eredményeit. A modellek kialakítása során a már felderített tényállás szempontjából az elkövető állampolgárságának, valamint az elkövetés helyének és az elkövető – a büntetőeljárás megindulását követően – detektált tartózkodási helyének tulajdonítottunk jelentőséget, annak érdekében, hogy jelezni tudjuk, különbség van az igénybe vehető eszközök között aszerint, hogy az elkövető magyar állampolgár-e, vagy sem, illetve, hogy a támadás magyar államterületről, vagy uniós, esetleg unión kívüli országból érkezik-e. Utóbbi kérdés nemcsak a kiberbűncselekmények tekintetében fontos kiindulási alap, de egyben elvi tétel is, ha joghatósági kérdéseket elemzünk, hiszen – ahogyan azt *Wiener A. Imre* is megfogalmazta – azzal, hogy egymás mellett léteznek büntetőhatalmat gyakorló országok, a határok bűnözési optikájú átjárhatósága magával hozza a joghatósági problémák fennállását is[14]. A három modellt, és ez által tanulmányunk fejezeteit a támadás kiindulópontja alapján állítottuk fel, alakítottuk ki, és valamennyi esetben feltételezzük, hogy a sértetti oldalon hazai természetes, vagy egyéb, nem természetes személy foglal helyet. A sértetti oldalon beemelhető újabb nemzetközi elem mentén történő elemzés álláspontunk szerint egyrészt meghaladná a tanulmány tervezett kereteit, másrészt annak célját is, hiszen elemzésünket a magyarországi hatóságok rendelkezésére álló eszközök mentén végezzük el. Szintén nem árnyaljuk terjedelmi korlátok miatt modelljeinket az elkövető személyét érintő további, az együttműködési

[12] LIGETI Katalin: Az Európai Unió büntetőpolitikája. *Állam és Jogtudomány,* 2002/1-2, 90. o.

[13] Az elv alkalmazása szempontjából is lényeges megfeleltethetőség kérdése figyelembe véve a kiberbűncselekmények széles körét olyan mély dogmatikai elemzést és értékelést igényel minden érintett tényállás esetében, amely már egy másik tudományos kutatás alapjául szolgálhat. Hozzátesszük, hogy vannak álláspontok a magyar szakirodalomban, melyek az Európai Unió szintjén jelentkező együttműködésben a kölcsönös elismerés elvének hangsúlyozása révén a kettős inkrimináció uniós szintű jelentéktelenné, másodlagossá válását vetítik előre. Lásd ezzel kapcsolatban: FARKAS Ákos: Új alkotmányos elv a magyar büntetőeljárási bizonyításban? A kölcsönös elismerés elve. In. ERDEI Árpád szerk.: *A büntető ítélet igazságtartalma.* Budapest, Magyar Közlöny Lap- és Könyvkiadó, 2010. 45-57. o.; ALFÖLDI Ágnes Dóra: A bűnügyi együttműködés általános kérdései az Európai Unióban. *Európai Jog* 2011/2. 13-17.o.

[14] WIENER A. Imre: A büntető joghatóság és gyakorlása, kivált az Európai Unióban. *Állam és Jogtudomány,* 2002/3-4. 177. o.

rendszerek szempontjából releváns ismérvekkel, mint például az elkövető kettős állampolgárságával, vagy menekült státuszával.

2. A KIBERBŰNCSELEKMÉNYEKRŐL RÖVIDEN: FOGALMI KERETEK

Minden tudományos kutatás első lépése a vizsgálat tárgyának meghatározása, így számunkra alapvető fontosságú annak a kérdésnek a megválaszolása, hogy mit értünk a kiberbűncselekmények *(cybercrimes)* fogalma alatt. A definíció napjainkban széles körben használatos, mind a nemzetközi, mind a hazai szakirodalomban, valamint számos nemzetközi jogi instrumentumban is. A kiberbűncselekmények világos meghatározása és az ebbe a körbe tartozó deliktumok megfelelő osztályozása több okból is alapvető fontosságú. Egyrészt segítséget nyújthat az államok kiberbűncselekményekkel kapcsolatos jogszabályainak harmonizálásában, mivel jelenleg jelentős különbségek vannak az európai országok között abban a tekintetben, hogy a kibertérben elkövetett illegális magatartások közül melyek minősülnek bűncselekménynek.

Másrészt amennyiben a releváns bűncselekmények nemzeti szabályozásai azonos elveken nyugodnak, és az egyes bűncselekmények elnevezését és törvényi meghatározását a lehető legnagyobb mértékben sikerül közelíteni, illetve egységesíteni, akkor a nemzetközi bűnügyi együttműködés és általában a kiberbűnözés elleni nemzetközi erőfeszítések is hatékonyabbak lehetnek.

Végül az egységes kiberbűncselekmény-fogalom, illetve a hozzá kapcsolódó statisztikai módszerek és mérőszámok egységesítése lehetővé teszi a kiberbűnözés valós terjedelmének megértését[15] és a vonatkozó bűncselekmények pontosabb mérését. Ha pedig pontosabb adatokkal rendelkezünk, akkor a kiberbűnözésre adott jogi és nem jogi válaszokat hatékonyabban lehet kidolgozni. A kiberbűncselekmények világos meghatározása és osztályozása azonban nem könnyű feladat, mivel az e fogalom alá tartozó magatartások rendkívül változatosak, és – szinte már követhetetlen módon – folyamatosan bővülnek.

Jelen tanulmányban a kiberbűncselekmények (*cybercrimes*) terminológiát használjuk, de utalunk arra, hogy mind a hazai, mind a külföldi szakirodalomban számos kifejezés létezik a jelenség leírására, amelynek egyenes következményeként „a kiberbűncselekmények definiálásának problémái magával a terminológiával kezdődnek”.[16] A terminológiák száma szinte végtelen: „kibertér-bűncselekmények” (*cyberspace crimes*); „számítógépes bűncselekmények” (*computer crimes*); „számítógéppel kapcsolatos bűncselekmények” (*computer-related crimes*); „elektronikus bűncselekmények” (*electronic crime*); „e-bűncselekmények” (*e-crimes*); „technológia-alapú bűncselekmények” (*technology-enabled crimes*); „high-tech bűncselekmények” (*high-tech crimes*), stb. A kiberbűncselekmények

[15] GRUND Borbála: A kibertér bűncselekményeiről és a kiberbűnözés hazai gyakorlatáról. *MTA Law Working Papers*, 2021/21. 2. o.
[16] PHILLIPS, Kirsty – DAVIDSON, Julia, C. – FARR, Ruby, R. – BURKHARDT, Christine – CANEPPELE, Stefano – AIKEN, Mary, P.: Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. *Forensic Sciences*, 2022/2 (2), 379. o.

fogalmával foglalkozó külföldi szakirodalmi forrásokkal valóban könyvtárakat lehetne megtölteni, jelen tanulmány első részében az egyes fogalmi és csoportosítási megközelítések rövid elemzésére, illetve az általunk is elfogadott koncepció felvázolására vállalkozunk.

2.1. A kiberbűncselekmények egyszerű definíciói

Az egyszerű definíció azt jelenti, hogy szerzője egyetlen hosszabb vagy rövidebb mondatban próbálja leírni a jelenséget. Így *Wall* szerint a kiberbűncselekmények „olyan kárt okozó magatartásokat jelentenek, amelyek valamilyen módon egy számítógéphez kapcsolódnak”.[17] *Gordon és Ford* értelmezésében minden olyan bűncselekmény e fogalom alá tartozik, amelyet számítógép, számítógépes hálózat vagy hardvereszköz felhasználásával követnek el, vagy ezek használata elősegíti a bűncselekmények elkövetését.[18] A hazai szakirodalomból *Kunos Imre* definícióját említjük, e szerint a számítógépes bűnözés azon bűncselekmények összessége, melyek esetén információtechnológiai eszközöket, rendszereket használnak a bűncselekmények elkövetésének eszközéül.[19]

Noha igazságtartalmuk általában nem vitatható, de az egyszerű, egyetlen mondatos fogalmak szükségszerűen leegyszerűsítők, hasznosíthatóságuk megkérdőjelezhető és nem képesek átfogó képet nyújtani a jelenségről. Ezért a szakirodalomban sokkal népszerűbbek a releváns bűncselekmények csoportosításával operáló definíciók.

2.2. A kiberbűncselekmények csoportosítását magukban foglaló definíciók

E fogalommeghatározások jellemzője, hogy a kiberbűncselekmények kifejezést mintegy munkafogalomként használva a hangsúlyt a csoportosításra, az egyes csoportok jellemzőinek rögzítésére, illetve a néhány releváns bűncselekmény besorolására helyezik. A szakirodalomban a kiberbűncselekmények kettős (dichotóm), illetve hármas (trichotóm) felosztása különböztethető meg.

2.2.1. A kiberbűncselekmények kettős felosztása

Mind a hazai, mind a külföldi szakirodalomban a legnépszerűbb és leginkább elfogadott dichotóm rendszer a kizárólag a kibertérben létező bűncselekmények (*cyber-dependent crimes*) és a kibertérben is elkövethető hagyományos bűncselekmények (*cyber-enabled crimes*) közötti megkülönböztetés. Az első csoportba tartozó – szűkebb értelemben vett vagy ún. valódi – kiberbűncselekmények az infokommunikációs technológia megjelenésével keletkeztek, és a digitális világon kívül nem léteznek.[20] Ide tartoznak például a hacking, a zsarolóvírus-támadások vagy az adathalászat különböző formái. A második kategória – tágabb értelemben vett kiberbűncselekmények – olyan tradicionális deliktumokat ölelnek fel, amelyek a kibertérbe

[17] WALL, David, S.: Introduction: Cybercrime and the Internet. In. Wall, David, S. (ed.) *Crime and the Internet*. Routledge: New York, NY, USA, 2001. 2. o.
[18] GORDON, Sarah – FORD, Richard: On the Definition and Classification of Cybercrime. *Journal of Computer Virology*, 2006/2 (1), 14. o.
[19] KUNOS Imre: A számítógépes bűnözés. *Belügyi Szemle*, 1999/11. 28. o.
[20] E bűncselekményeket – amelyek tárgya az információs rendszer – csak számítógépek, azok hálózatai vagy más IKT-eszközök felhasználásával lehet elkövetni.

„vándoroltak”[21], de azon kívül is elkövethetők. Ebben a körben az információs rendszer a bűncselekmény elkövetésének eszköze, illetve helyszíne, vagy megkönnyítheti a bűncselekmény elkövetését. A kibertérben is elkövethető bűncselekmények – egyebek között – a csalás, a pénzmosás, a kábítószer-kereskedelem, a zaklatás, különböző verbális bűncselekmények.[22]

2.2.2. A kiberbűncselekmények hármas felosztása

A külföldi szakirodalom leggyakrabban idézett trichotóm felosztása *Wall* nevéhez fűződik, aki az alábbi kategóriák között tesz különbséget:

a) A számítógép elleni bűncselekmények (*crimes against the machine*), vagy más néven az információs rendszer ellen elkövetett cselekmények, például a hacking, a cracking vagy a Dos-támadások),

b) A számítógép felhasználásával elkövetett bűncselekmények (*crimes using the machine*), amikor az információs rendszer a cselekmény elkövetésének eszköze, például különböző csalási cselekmények vagy a számítógépes kalózkodás),

c) A számítógépben elkövetett cselekmények (*crimes in the machine*), vagy más elnevezéssel a számítógépes tartalommal kapcsolatos cselekmények, amelyekre példa az online zaklatás vagy a gyermekpornográfia.[23]

A *Sarre, Lau, Chang* szerzőhármas pedig a techonógia szerepét és legújabb fejleményeit hangsúlyozva az alábbi csoportosítás mellett érvel:

- 1-es típusú kiberbűncselekmények, amelyek természetüknél fogva technikai jellegűek, például a hacking,
- 2-es típusú kiberbűncselekmények, amelyek emberek közötti kapcsolat létrejöttét feltételezik, például a kibertérben elkövetett zaklatás,
- 3-as típusú kiberbűncselekmények, amelyek magukban foglalják a mesterséges intelligenciák, robotok, vagy öntanuló technológiák által elkövetett cselekményeket.[24]

---

[21] BRENNER, Susan, W.: Re-thinking crime control strategies. In. Jewkes, Yvonne (ed.) *Crime Online*. Willan Publishing: Cullompton, UK, 2007. 12–28. o.

[22] A hazai szakirodalomban a fenti megkülönböztetés alapján Ambrus István szintén a kettős felosztást fogadja el, amikor különbséget tesz szorosabb és tágabb értelemben vett digitális bűncselekmények között. AMBRUS István: *Digitalizáció és büntetőjog*. Budapest, Wolters Kluwer, 2021. 290. o.

[23] WALL, David, S.: *The Transformation of Crime in the Information Age*. Polity Press, Cambridge, UK, 2007. Hasonló példa az említett hármas kategorizálásra az Európai Bizottság meghatározása, amely a következő terminológiákat használja:

a) A számítógépek és információs rendszerek vonatkozásában elkövetett bűncselekmények (például az információs rendszerek elleni támadások);

b) Hagyományos bűncselekmények (például a csalás, a különböző hamisítási cselekmények vagy a személyazonosság-lopás);

b) Tartalommal kapcsolatos bűncselekmények (pl. online gyűlöletre uszítás).

Lásd European Commission. *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*. 2013. február 7. 2013. 3-4. o.

[24] SARRE, Rick – LAU, Yiu-Chung – CHANG, Lennon, Y. C.: Responding to cybercrime: Current trends. *Police Practice and Research*, 2018/19 (6), 515–518. o.

Álláspontunk szerint a kiberbűncselekményeknek a modern technológiák szerepén alapuló hármas kategorizálása[25] előremutatóbb, mint a dichotóm felosztás, mert ez jobban tükrözi a kiberbűnözés várható jövőjét: a jövőben a legtöbb ilyen bűncselekményt valamilyen technológia fogja elősegíteni, amelyek szerepe a bűncselekmények elkövetésében szinte bizonyosan növekedni fog.

2.3. A kiberbűncselekmények rendszerezésén alapuló definíciók (a kiberbűncselekmények tachonómiája)

A kiberbűncselekmények tachonómiája a kiberbűncselekmények beazonosítását, csoportosítását és az egyes deliktumok elhelyezését jelenti egy komplex rendszeren belül, a cselekmények hasonlóságai és különbségei alapján. Olyan összetett és sok esetben bonyolult rendszert jelent, amely a kiberbűncselekmények átfogó és minél teljesebb körű meghatározására tesz kísérletet. A releváns deliktumok rendszerezésén alapuló definíciókra mind a vonatkozó nemzetközi jogi instrumentumokban, mind a külföldi szakirodalomban találunk példát.

Így az Európa Tanács által Budapesten, 2001. november 23. napján elfogadott *Számítástechnikai Bűnözésről szóló Egyezmény* (a továbbiakban: Budapest Konvenció) és Kiegészítő Jegyzőkönyve öt kategóriába sorolva 14 különböző kiberbűncselekményt tartalmaz. Az első kategória *a számítástechnikai rendszer és számítástechnikai adat hozzáférhetősége, sértetlensége és titkossága elleni bűncselekmények*, ide tartozik a jogosulatlan belépés (2. cikk), a jogosulatlan kifürkészés (3. cikk), a számítástechnikai adat megsértése (4. cikk), a számítástechnikai rendszer megsértése (5. cikk) és az eszközökkel visszaélés (6. cikk). A második csoport *a számítógéppel kapcsolatos bűncselekmények*, amely magában foglalja a számítógéppel kapcsolatos hamisítást (7. cikk) és a számítógéppel kapcsolatos csalást (8. cikk). A harmadik *a számítástechnikai adatok tartalmával kapcsolatos bűncselekmények,* ezek az Egyezményben a gyermekpornográfiával kapcsolatos bűncselekményeket jelentik (9. cikk), a negyedik *a szerzői vagy szomszédos jogok megsértésével kapcsolatos bűncselekmények* (10. cikk). Végül – a Kiegészítő Jegyzőkönyv alapján – az ötödik csoport *a számítástechnikai rendszer útján elkövetett rasszista és xenofób jellegű bűncselekmények*, amelyek felölelik a rasszista és xenofób tartalmú anyagok számítástechnikai rendszer útján történő terjesztését, a rasszista és xenofób célzattal elkövetett fenyegetést és zaklatást, a népirtás és az emberiesség elleni bűncselekmények tagadását.

A külföldi szakirodalomban szintén számos szerző tett kísérletet a kiberbűncselekmények rendszerezésén alapuló fogalom meghatározására. A terjedelmi korlátok miatt újdonsága és

[25] A hazai szakirodalomból Grund Borbála hármas felosztását emeljük ki, e szerint kiberbűncselekmények
- az olyan bűncselekmények, amelyekben a számítógép vagy a számítógépes hálózat biztonságát fenyegeti a kriminális tevékenység, ezek az IKT létrejövetelével karöltve alakultak ki (szűk értelemben vett kiberbűnözés);
- az olyan hagyományos bűncselekmények, amelyekhez a számítógépet az elkövetés eszközeként használják fel, ezek léteztek az IKT előtt is, de új életre keltek a kibertérbe való bizonyos fokú integrálódással (számítógép segítségével megvalósuló bűnözés);
- a számítógépes tartalommal kapcsolatos bűncselekmények, amelyeknél az eszköz tartalma az elkövetés bizonyítékául szolgálhat (számítógépen tárolt adatok tartalmával kapcsolatos bűnözés). Lásd GRUND: i.m. 4. o.

eredetisége okán jelen tanulmányban csupán *Philips* és szerzőtársai koncepcióját[26] vázoljuk fel. Ebben a rendszerben – amely *A kiberbűncselekmények és kiberdevianciák új rendszere* elnevezést viseli – a szerzők igyekeztek kimerítően felsorolni az egyes kategóriákba tartozó bűncselekményeket, és figyelembe vették az infokommunikációs technológia fejlődésének legújabb fejleményeit. A megközelítés újdonsága, hogy nem csupán a kiberbűncselekményekre fókuszál, hanem azokra a kibertérben (is) elkövethető jogellenes vagy deviáns cselekményekre is, amelyek nem, vagy jelenleg még nem minősülnek bűncselekménynek.

- Az 1. számú csoportba a *számítógép elleni bűncselekmények* (*az információs rendszer és adatok elleni támadások*) tartoznak, amelynek egyik alkategóriája az egyének és a szervezetek elleni bűncselekmények: jogellenes belépés (hacking, cracking); jogellenes adatszerzés (adatkémkedés); a számítógépek közötti adatátvitel jogosulatlan lehallgatása (illegal interception); adatok jogellenes bevitele, módosítása, törlése, vagy az információs rendszerbe történő bármilyen beavatkozás (data and system interference); eszközökkel visszaélés; zsarolás, illetve zsarolóprogramok használata. A másik alkategória az államok elleni bűncselekmények, amelyek körébe tartozik a politikai beavatkozás, a kiberhadviselés és a kémkedés;

- A 2. számú csoport *a számítógép felhasználásával elkövetett bűncselekmények* (*lopás és egyéb vagyon elleni bűncselekmények*): számítógépes hamisítás; számítógépes csalás; szerzői- és más szomszédos jogok megsértése; digitális kalózkodás; spam-ekkel kapcsolatos jogsértések; személyazonosság-lopás; adathalászat; kibercsalás;

- A 3. számú csoport *a számítógépben elkövetett cselekmények* (*erőszakos cselekmények*), amelyek további alkategóriákra tagozódnak. i) *személyközi erőszak*: zaklatás; megfélemlítés; trollkodás; kényszerítés; zsarolás jellegű cselekmények, pl. az ún. romantikus csalás. ii) *szexuális erőszak*: illegális pornográf anyagokkal visszaélés; a gyermekek szexuális kihasználását, illetve bántalmazását megvalósító cselekmények; szexuális behálózás (grooming); szexuális zaklatás; intim képek felhasználásával elkövetett bántalmazás (image based abuse); szexuális tartalmú zsarolás (sextortion); szexuális tartalmak küldése (sexting); szexkereskedelem; szexturizmus. iii) *csoportok elleni erőszak*: gyűlöletbeszéd; vallási meggyőződéssel kapcsolatos bűncselekmények; idegengyűlölet; a terrorizmushoz kapcsolódó bűncselekmények; radikalizálódás. iv) *általános jellegű erőszak*: erőszakra történő felhívás/felbujtás;

- A 4. számú csoport *a számítógéppel elősegített (hagyományos) bűncselekmények*: illegális szerencsejáték és illegális online játék; pénzmosás, illetve az online pénzmosás (money muling); kábítószer-kereskedelem; bűncselekményt megvalósító kommunikáció;

- Az 5. számú csoport egyfajta "keresztül fekvő" kategória, amelybe a szervezett bűnözés körébe tartozó magatartások, a deep web piacok és más illegális virtuális piacterek, illetve kiberbűncselekmény, mint szolgáltatás (cybercrime as a service);

- Végül a 6. számú csoport szintén "keresztül fekvő" kategória, amelynek alkategóriái i) a fejlett technológia használatával elkövetett cselekmények: a mesterséges intelligencia és a gépi tanulás felhasználásával elkövetett bűncselekmények; algoritmusokon alapuló profilalkotás; deep-fake hamisítások; botok és botnetek használata. ii) hamis információk felhasználása:

[26] PHILLIPS-DAVIDSON– FARR– BURKHARDT–CANEPPELE–AIKEN: i.m. 390. o.

kibercsapatok (a közvélemény csoportos manipulálása, cyber-troops); hamis hírek terjesztése (fake-news); félretájékoztatás és dezinformáció.

Az 1. számú áttekintő táblázatban láthatjuk a *Philips és szerzőtársai* által kidolgozott rendszer felépítését és elemeit. A rendszerrel kapcsolatos kritikai megjegyzéseink az alábbiak:

Maradéktalanul egyetértünk az 1. számú csoport elnevezésével és elemeivel, a 2. számú csoport elnevezése a bűncselekmények védett jogi tárgyára figyelemmel javaslatunk szerint a "számítógép felhasználásával elkövetett vagyon jogok és a szellemi tulajdon elleni bűncselekmények". A 3. sz. csoport vonatkozásában egyrészt "a számítógép felhasználásával elkövetett személy elleni bűncselekmények" elnevezést preferáljuk, mivel az ebbe a kategóriába tartozó deliktumok esetén az információs rendszer szintén eszköze, illetve helyszíne a bűncselekménynek. Mellőznénk az "erőszak"-ra történő utalást, mivel az a magyar büntetőjogban fizikai ráhatást jelent, a csoportba tartozó bűncselekményeknek azonban ez nem tényállási eleme. A iv) alkategória elnevezése javaslatunk szerint "a verbális bűncselekmények" elnevezést viselné, amelybe a 6. sz. csoport második alkategóriájába tartozó deliktumokat is besorolnánk. A 4. sz. csoport elnevezésével és elemeivel egyetértünk, amelybe besorolnánk a szervezett bűnözés keretében elkövetett bűncselekményeket is. Az 5. sz. csoport nézetünk szerint – amely a büntető anyagi jogi szemszögéből közelít – mellőzendő, mivel a csoportba tartozó cselekmények inkább deviáns, és nem feltétlenül büntetőjogellenes cselekmények. A 6. sz. csoport létrehozása a rendszer legfontosabb újítása, amely messzemenően támogatandó.

Álláspontunk szerint kiberbűncselekmények fogalmi meghatározásai közül a legfejlettebbek a taxonómiák, vagyis azok a megoldások, amelyek rendszereznek és kategorizálnak, és a bűncselekmények legátfogóbb listáját nyújtják. Tudomásul kell venni, hogy a kiberbűncselekmények általánosan elfogadott definíciója nem létezik. Ez azonban nem jelenti azt, hogy haszontalan feladat lenne a releváns bűncselekmények olyan rendszerezése, amely figyelembe veszi a technológia fejlődését és a kiberbűnözés legújabb tendenciáit, kompatibilis a nemzetközi jogi instrumentumokkal és igyekszik naprakész lenni.

1. sz. A kiberbűncselekmények és a kiberdevianciák új rendszere (Philips és szerzőtársai, 2022)

1. Számítógép elleni bűncselekmények	*2. Számítógép felhasználásával elkövetett bűncselekmények*	*3. Számítógépben elkövetett bűncselekmények*	*4. Számítógéppel elősegített (hagyományos) bűncselekmények*	*5. "Keresztül fekvő" csoport A*	*6. "Keresztül fekvő" csoport B*
1/a. egyének és szervezetek ellen	számítógépes hamisítás	*3/a. személyközi erőszak*	illegális szerencsejáték, illegális játék	szervezett bűnözés	*6/a. fejlett technológiák*

jogellenes belépés	számítógépes csalás	zaklatás, megfélemlítés	pénzmosás, online pénzmosás	deep web piacok és illegális virtuális piacterek	mesterséges intelligencia, gépi tanulás
jogellenes adatszerzés	szerzői és más szomszédos jogok megsértése	trollkodás, kényszerítés	kábítószer-kereskedelem	kiberbűncselekmény mint szolgáltatás	algoritmusokon alapuló profilalkotás
jogosulatlan lehallgatás	digitális kalózkodás	zsarolás jellegű cselekmények	bűncselekményt megvalósító kommunikáció		deep-fake hamisítások
információs rendszerbe beavatkozás	spam-ekkel kapcsolatos jogsértések	*3/b. szexuális erőszak*			botok és botnetek
eszközökkel visszaélés	személyazonosság-lopás	illegális pornográf anyagok			*6/b. hamis információk felhasználása*
zsarolás, zsarolóprogramok	adathalászat	gyermekek szexuális kihasználása			"kibercsapatok"
1/b. állam elleni bűncselekmények	kibercsalás	szexuális behálózás, szexuális zaklatás			fake-news
politikai beavatkozás		intim képekkel visszaélés, szexuális zsarolás			dezinformáció
kiberhadviselés		szexuális tartalmak küldése			
kémkedés		szexkereskedelem, szexturizmus			

		3/c. csoportok elleni erőszak			
		gyűlöletbeszéd, vallási bűncselekmények			
		idegengyűlölet			
		terrorizmus, radikalizálódás			
		4/c. általános jellegű erőszak			
		erőszakra történő felhívás/felbujtás			

3. A JOGHATÓSÁG RELEVÁNS KÉRDÉSEI

3.1. A joghatóság fogalma, joghatósági elvek és szabályok

A 20. század közepéig a bűnözés alapvetően lokális jelenség volt, a büntető joghatóság gyakorlását szabályozó alapelvek arra az axiómára épültek, hogy a bűncselekmény egy adott földrajzi területhez kötött jelenség.[27] Ebből következett a joghatósági elvek közül a területi elv alkalmazásának dominanciája, hiszen kézenfekvő volt, hogy az az állam gyakoroljon joghatóságot, amelynek területén a bűncselekményt elkövették. Ezt követően azonban egyre gyakoribbá váltak azok a deliktumok, amelyekbe valamilyen nemzetközi elem vegyült, vagyis amelyek az elkövetés helye, az elkövető személye (állampolgársága), illetve a cselekmény jellege és körülményei folytán egyidejűleg két vagy több állam jogrendjét is sértették vagy veszélyeztették.[28] A kiberbűnözés ezt a jelenséget megsokszorozta és alapjaiban változtatta meg a bűnözés jellegét, mert azt határokat nem ismerő, nemzetközi jellegűvé tette.[29] Ezzel összefüggésben a kibertér szinte megtestesíti a deterritorializáció jelenségét, mivel lehetővé teszi a digitális adatok villámgyors átvitelét a felhasználók és eszközök között a világ minden

[27] TÓTH Dávid – GÁSPÁR Zsolt: Nemzetközi bűnügyi együttműködéssel összefüggő nehézségek a kiberbűnözés terén. *Belügyi Szemle,* 2020/2. 140.o.
[28] M. NYITRAI Péter: *Nemzetközi és európai büntetőjog*. Osiris Kiadó, Budapest, 2006. 207. o.
[29] TÓTH-GÁSPÁR: i.m. 140. o.

tájáról.[30] A deterritorializáció, vagyis a társadalmi folyamatok világméretűvé válása, az egyedi és elszigetelhető helyszínektől való eloldódás[31] igen jelentős kihívás elé állítja a jelenlegi joghatósági rendszert, amely továbbra is a területi elv elsődlegességére épül.

A *joghatóság* – legáltalánosabb értelemben – azt a szabályrendszert jelenti, amely a jogot működő, elérhető joggá teszi, és alkalmazásának legfontosabb előfeltétele.[32] A fogalom egyik vetülete, a *büntető joghatóság* az állam büntető jogalkotásra és jogalkalmazásra vonatkozó jogát jelenti. Szűkebb értelemben kettős jelentéstartalmat hordoz, egyrészt a nemzeti büntetőjog szabályainak alkalmazhatóságát, másrészt a büntetőügyben eljáró hatóságok hatáskörének terjedelmét értjük rajta.[33] A külföldi szakirodalmi forrásokban mellőzhetetlen részkérdés a joghatóság fogalmának háromszintű értelmezése, így a teljesség kedvéért röviden erre is utalunk. E szerint a joghatóság az állami büntetőigény jövőbeni érvényesítésének megalapozását, vagyis az állam azon jogkörét jelenti, hogy meghatározott magatartásokat szabályozzon: előírjon valamely magatartás tanúsítását, vagy – ami a büntetőjogban tipikus – tilalmazzon bizonyos cselekményeket (*jurisdiction to prescribe* vagy *legislative jurisdiction*). A joghatóság másik értelmében a végrehajtási joghatóság (*jurisdiction to enforce*), amely a már fennálló joghatóság tényleges érvényesítése, egy állam azon képessége, hogy a végrehajtói és a bírói hatalom gyakorlása révén érvényt szerezzen a jogának. Végül a joghatóság értelmezésének harmadik szintje az ítélkezési joghatóság (*jurisdiction to adjudicate*), amely egy államnak azt a hatáskörét jelenti, hogy tárgyalja a büntetőügyet, és állást foglaljon abban a kérdésben, hogy a vádlott elkövette-e a terhére rótt bűncselekményt.[34]

Noha számos nemzetközi jogi instrumentum – így a Budapesti Konvenció is – tartalmaz joghatóságra vonatkozó rendelkezéseket, a joghatóság nem csupán nemzetközi jogi kategória: a joghatóság szabályait, azok tartalmát a belső büntetőjogi rendelkezések töltik ki tartalommal. A *hatály* – mint belső büntetőjogi fogalom – az adott állam büntetőjoga alkalmazásának különböző vetületeit határozza meg (időbeli, területi, illetve személyi hatály). Erre is figyelemmel jelen tanulmányban a joghatóság fogalmát az alábbi értelemben használjuk: *A joghatóság az államnak a büntető jogszabályok alkotására és alkalmazására vonatkozó jogosultságát jelenti. A joghatóságra vonatkozó rendelkezések azt szabályozzák, hogy valamely bűncselekmény elbírálásakor mikor, hol és kikre kell alkalmazni a büntető törvényt.* A büntető joghatóságra vonatkozó rendelkezéseket a legtöbb országban – így hazánkban is – a Büntető Törvénykönyv Általános Részében találjuk, ezek értelemszerűen a kiberbűncselekmények esetében is irányadók. *A büntető joghatóságot megalapozó elv*eket a büntető jogtudomány

[30] RYNGAERT, Cedric: Extraterritorial Enforcement Jurisdiction in Cyberspace: Normative Shifts. *German Law Journal*, 2023/4 (24), 537. o.
[31] JAKAB Dénes Barna: Területiség és deterritorializáció. A terület mint a társadalomelmélet vezérfonala. *Replika*, 2009/5. 164. o.
[32] A joghatóság alapvetően nemzetközi jogi kifejezés, amely az állam jogszabály alkotására, végrehajtására, illetve az igazságszolgáltatás gyakorlására vonatkozó jogát jelenti. Lásd M. NYITRAI: i.m. 208. o.
[33] M. NYITRAI: i.m. 209. o.
[34] Lásd részletesen: BRENNER, Susan W. – KOOPS, Bert-Jaap: Approaches to Cybercrime Jurisdiction. *Journal of High Techology Law*, 2004/1 (4), 5-6. o., illetve TÓTH-GÁSPÁR: i.m. 141. o.

dolgozta ki, amelyek azonban minden esetben visszatükröződnek a Büntető Törvénykönyv joghatóságra (hatályra) vonatkozó rendelkezéseiben.

Az államok a büntető joghatóságot hagyományosan öt szempontra alapozzák: a területiségre, az állampolgárság ún. aktív és passzív aspektusára (aktív és passzív személyi elv), az állami önvédelem és az univerzalitás elvére.[35] A *területi elv* a büntető joghatóság gyakorlásának leggyakoribb alapja, amely szerint egy állam büntetőjogának hatálya kiterjed a saját területén elkövetett valamennyi bűncselekményekre, függetlenül az elkövető állampolgárságától. A Budapesti Konvenció a joghatósági szabályok közül elsőként szabályozza a területi elvet[36], és – szemben a többi joghatóságot megalapozó körülménnyel – annak belső jogban történő szabályozása és alkalmazása kötelező a részes államok számára.[37] A magyar Btk. 3. § (1) bekezdésének a) pontja[38] rögzíti a területi elvet, ennek alapján a Magyarország területén elkövetett kiberbűncselekmény esetén a magyar Btk. alkalmazandó. Itt említjük meg a *kvázi területi elv*et, amely a belföld fogalmát terjeszti ki a az adott ország lobogója alatt közlekedő hajón vagy lajstromozott repülőgépen elkövetett bűncselekmények tekintetében. A kvázi területi elv szintén szerepel a Budapesti Konvencióban[39] és azt a magyar Btk. is szabályozza.[40]

A második leggyakoribb joghatósági alap a személyi elv, illetve annak egyik aspektusa, az ún. *aktív személyi elv*, amely szerint az állam joghatósága kiterjed az állampolgára által külföldön elkövetett bűncselekményre is. A Budapesti Konvenció szerint az elv alkalmazásának további feltétele, hogy a cselekmény az elkövetés helyének joga szerint bűncselekménynek minősül és büntetendő.[41] Ezzel szemben az aktív személyi elv a magyar büntetőjogban jóval szélesebb körben jut szerephez: a magyar állampolgár által külföldön elkövetett (kiberbűncselekménynek tekintendő) cselekmény esetén a magyar törvényt alkalmazásához elegendő az, ha a cselekmény a magyar Btk. szerint minősül bűncselekménynek.[42] Itt említjük meg a Konvencióban már nem szereplő, de a magyar Btk. által szabályozott ún. *passzív személyi elv*et, amely szintén az extraterritoriális (az adott állam területén kívül elkövetett bűncselekményekre vonatkozó) joghatóságot megalapozó körülmények közé tartozik. Az elv az állam saját állampolgárát (vagy saját jogi személyét, egyéb szervezetét) védi a külföldön külföldi által elkövetett bűncselekmény esetén. Ennek alapján a magyar Btk. alkalmazandó a magyar állampolgár, a magyar jog alapján létrejött jogi személy és jogi személyiséggel nem rendelkező

[35] M. NYITRAI: i.m. 213. o.
[36] Lásd a Konvenció 22. cikk 1. a) pontját.
[37] A 22. Cikk 2. pontja szerint „Minden Szerződő Fél fenntarthatja magának azt a jogot, hogy az 1. bekezdés b)-d) pontjában foglalt joghatóságra vonatkozó szabályokat vagy azok bármely részét nem, vagy csak meghatározott esetben, illetve feltételek között alkalmazza."
[38] Btk. 3. § (1) „A magyar büntető törvényt kell alkalmazni a) a belföldön elkövetett bűncselekményre, (…)."
[39] Lásd a Konvenció 22. cikk 1. b) és c) pontját.
[40] Btk. 3. § (1) „A magyar büntető törvényt kell alkalmazni b) a Magyarország területén kívül tartózkodó magyar felségjelű úszólétesítményen vagy magyar felségjelű légi járművön elkövetett bűncselekményre, (…)."
[41] Lásd a Konvenció 22. cikk 1. d) pontját.
[42] Btk. 3. § (1) „A magyar büntető törvényt kell alkalmazni c) a magyar állampolgár által külföldön elkövetett olyan cselekményre, amely a magyar törvény szerint bűncselekmény."

egyéb jogalany sérelmére nem magyar állampolgár által külföldön elkövetett olyan cselekményre is, amely a magyar törvény szerint büntetendő.[43]

A következőkben tárgyalandó és a magyar Btk-ban is szabályozott joghatósági elvek már szintén olyan esetekben alkalmazandók, amikor a bűncselekményt *nem az állam saját állampolgára* (külföldi vagy hontalan személy) *követi el külföldön*. Megjegyzendő, hogy a Budapesti Konvenció ezeket a joghatóságot megalapozó körülményeket már nem tartalmazza, de lehetővé teszi a részes államok számára azok szabályozását és alkalmazását.[44] Elsőként említjük az *állami önvédelem elv*ét (védelmi elv), amely jellemzően azon bűncselekmények vonatkozásában érvényesül, amelyek az állam külső vagy belső biztonságát, függetlenségét vagy területi épségét sértik vagy veszélyeztetik. A magyar Btk. – két kivétellel – a kódexben szabályozott állam elleni bűncselekményeket szabályozza ebben a körben és nem szükséges a kettős inkrimináció követelménye, vagyis a Btk. alkalmazásának nem feltétele, hogy a cselekmény az elkövetés helyének joga szerint is büntetendő legyen.[45]

Az *univerzalitás elve* (a feltétlen büntetőhatalom elve) szerint „a bűn büntetlenül nem maradhat" morális töltetű célkitűzés[46] jegyében büntetni kell a bárhol bárki által elkövetett, jellemzően kiemelkedő tárgyi súlyú bűncselekményeket. Ezek jellemzően az ún. nemzetközi jogi bűncselekmények (népirtás, emberiesség elleni bűncselekmények, háborús bűncselekmények, illetve az agresszió bűntette), illetve az ún. transznacionális bűncselekmények, vagyis a nemzetközi szerződés alapján büntetendő deliktumok. A magyar Btk. szabályozza az univerzalitás elvét[47], és lényeges, hogy a kettős inkrimináció itt sem feltétel.

Végül a hazai büntetőjogban is szabályozott, ún. *képviseleti elv*en alapuló, helyettesítő büntető joghatóság[48] alapján nem csupán az előbb említett nagy tárgyi súlyú nemzetközi bűncselekmények, hanem egyéb külföldön elkövetett deliktumok esetén is lehetséges az eljárás lefolytatása és a nem saját állampolgár elkövető felelősségre vonása, alapvető feltétel viszont a kettős inkrimináció követelményének teljesülése.

---

[43] Lásd a Btk. 3. § (2) bekezdésének b) pontját.

[44] A 22. cikk 4. pontja szerint „Jelen Egyezmény nem zárja ki a Fél belső joga szerint meghatározott büntetőjogi joghatóságának gyakorlását."

[45] Btk. 3. § (2) „A magyar büntető törvényt kell alkalmazni a) a nem magyar állampolgár által külföldön elkövetett cselekményre is, ha az (…) ab) állam elleni bűncselekmény, – kivéve a szövetséges fegyveres erő ellen elkövetett kémkedést és a kémkedést az Európai Unió intézményei ellen – tekintet nélkül arra, hogy az az elkövetés helyének törvénye szerint büntetendő-e, (…)." E rendelkezés alapján egy olyan, Magyarország ellen külföldről indított kibertámadás, amelynek célja az ország hátrányára felhasználható adatok megszerzése („hírszerző tevékenység folytatása" hazánk ellen), megvalósíthatja az állam elleni bűncselekmények között szabályozott kémkedés bűntettét (Btk. 261. §), mely esetben a magyar Btk. alkalmazandó.

[46] M. NYITRAI: i.m. 228. o.

[47] Btk. 3. § (2) „A magyar büntető törvényt kell alkalmazni a) a nem magyar állampolgár által külföldön elkövetett cselekményre is, ha az (…) ac) *a XIII. vagy a XIV. Fejezetben meghatározott bűncselekmény*, vagy *egyéb olyan bűncselekmény, amelynek üldözését törvényben kihirdetett nemzetközi szerződés írja elő*, (…)." A Btk. XIII. Fejezete szabályozza az emberiesség elleni bűncselekményeket, míg a XIV. Fejezet a háborús bűncselekményeket.

[48] Btk. 3. § (2) „A magyar büntető törvényt kell alkalmazni a) a nem magyar állampolgár által külföldön elkövetett cselekményre is, ha az (…) aa) a magyar törvény szerint bűncselekmény, és az elkövetés helyének törvénye szerint is büntetendő, (…)."

A magyar büntetőjogban érvényesülő joghatósági elvek és szabályok alapján megállapítható, hogy *a hazai szabályozás a területi elv elsődleges alkalmazása mellett szinte korlátlan mértékű extraterritoriális joghatóságot biztosít. Egy kiberbűncselekmény elkövetése esetén szinte minden elképzelhető szituációban alkalmazandó a magyar Btk., tekintet nélkül az elkövetés helyére és az elkövető állampolgárságára*. Egyetlen korlátot[49] látszólag a kettős inkrimináció jelent, de mivel a kiberbűncselekmények nemzetközi szerződés alapján büntetendő cselekmények („egyéb olyan bűncselekmény, amelynek üldözését törvényben kihirdetett nemzetközi szerződés írja elő"), így elvileg az univerzalitás elve alkalmazandó, és a magyar büntetőjog alkalmazásának a nem állampolgár által külföldön elkövetett kiberbűncselekmény esetén sincs akadálya. A joghatósági rendelkezések ilyen széles, szinte minden esetre kiterjedő szabályozása azonban elkerülhetetlenül joghatósági konfliktusokhoz vezet.

3.2. Joghatósági konfliktusok

A joghatósági konfliktusok két típusa ismert, a negatív és a pozitív. Az első esetben egy államnak sem áll fenn potenciális joghatósága az ügyben (ez gyakorlatilag teljesen kizárt), vagy egy állam sem kívánja az aktuálisan fennálló joghatóságát gyakorolni. Ez utóbbi szituáció elvileg, nagyon ritkán előfordulhat.[50]

Sokkal gyakoribb a pozitív joghatósági konfliktus, amikor ugyanazon ügyben egyszerre két vagy több állam is joghatóságot alapoz meg és kíván is gyakorolni. Amennyiben például egy magyar állampolgár elkövető Lengyelországban használ egy számítógépet ahhoz, hogy jogosulatlanul belépjen egy Ausztriában lévő információs rendszerbe, Magyarország az aktív személyi elv, Lengyelország a területi elv, illetve Ausztria a passzív személyi elv (avagy a területi elv) alapján potenciális joghatósággal rendelkezik.[51]

Mivel a kiberbűncselekmények sok esetben az ún. transznacionális, határokon átnyúló bűnözés körébe sorolhatók, a vonatkozó büntetőügyekben gyakran az elkövetés helyének meghatározása is nehézséget okoz, gyakori, hogy az elkövető és sértett különböző országokban tartózkodik, illetve az is előfordul, hogy a bűncselekménnyel érintett információs eszköz vagy adat harmadik országban található.[52] Ebből következően *a kiberbűncselekményekkel kapcsolatos büntetőügyekben a pozitív joghatósági konfliktus a gyakorlatban abszolút életszerű, szinte szükségszerűen bekövetkező szituáció*. A joghatósági konfliktusok feloldása

[49] A teljesség kedvéért azonban hangsúlyozni kell, hogy a nem magyar állampolgár által külföldön elkövetett bűncselekmények esetében a magyar büntető joghatóság gyakorlásának egyfajta (ön)korlátját jelenti az a rendelkezés, amely szerint a büntetőeljárás megindításához a Legfőbb Ügyész döntése szükséges.

[50] A szakirodalmi példa szerint számítógépes vírusok használatával vagy például gyűlöletbeszédet tartalmazó weboldalak közzétételével elkövetett bűncselekmények esetében előfordulhat, hogy a potenciálisan joghatósággal rendelkező országok azért nem indítanak eljárást, mert vonatkozásukban nem keletkezett olyan mértékű kár vagy más érdeksérelem, amely feltétlenül indokolná a joghatóság gyakorlását, és/vagy várakozásaik szerint más ország le kívánja folytatni a büntetőeljárást. BRENNER–KOOPS: i.m.: 41. o.

[51] Hasonló példát említ Mezei, illetve a Brenner-Koops szerzőpáros. Lásd MEZEI Kitti: *A kiberbűnözés egyes büntetőjogi szabályozási kérdései*. Doktori értekezés. Pécs, 2019. 195. o., illetve BRENNER–KOOPS: i.m.: 41. o.

[52] DORNFELD László: Az elektronikus bizonyítékszerzés aktuális kérdései. *Kriminológiai Közlemények* 77, 2017. 243. o.

alapvető érdek, hiszen ily módon elkerülhetők a párhuzamos eljárások és biztosítható a büntetőeljárás hatékony, időszerű és gazdaságos lefolytatása. A pozitív joghatósági konfliktusok feloldásának két alapvető módja a joghatósági elvek hierarchiája, illetve az érintett államok közötti konzultáció.

A *joghatósági elvek között felállított hierarchia* egyik példája az Európa Tanács joghatósági konfliktusok feloldása tárgyában 1965-ben született 420. számú Ajánlása, amely szerint büntető ügyekben annak az államnak van elsődleges joghatósága, amelynek területén a bűncselekményt elkövették. A területi elv elsődlegessége csak akkor nem érvényesül, ha a cselekmény egy állam biztonságát vagy hitelességét veszélyezteti, mert ilyen esetben a fenyegetett országé az elsődleges büntető igény. A területi elv után következik a személyi elv, végül annak az államnak a joghatósága, amelynek területén az elkövető található.[53] A joghatósági hierarchiára vonatkozó elképzelések a vonatkozó szakirodalomban is megfogalmazódtak, így a híres nemzetközi büntetőjogász, *Bassiouni* szerint szintén a területi elv primátusa kell hogy érvényesüljön, ezt az aktív és a passzív személyi elv követi, és csak ezt követően gyakorolható egyéb elv alapján a joghatóság, feltéve, ha a terhelt a joghatóságot igénylő állam területén tartózkodik.[54] A területi elv primátusa mellett valóban sok érv szól, így például a bűncselekmény felderítéséhez szükséges bizonyítékok többsége általában az elkövetés helyén található és alappal lehet bizakodni a büntetőeljárás gyors és hatékony befejezésében. Hangsúlyozni kell azonban, hogy egyrészt jelenleg nincs olyan nemzetközi szerződés, amely a joghatósági elvek között hierarchiát állapítana meg és biztosítaná a területi elv általános elsőbbségét, és a nemzetközi szokásjogból sem vonható le ilyen következtetés. Másrészt – ahogyan említettük – a kiberbűncselekmények esetében sokszor bizonytalan az elkövetési hely meghatározása. Eltérő az egyes országok szabályozása abban a tekintetben, hogy számítógépes tartalommal kapcsolatos bűncselekmények – például gyermekpornográfia – esetén mit kell az elkövetés helyének tekinteni.[55] Ez lehet az adatok, tartalmak feltöltésének, illetve letöltésének helyszíne, vagy – mint hazánkban a Kúria BH2022. 65. szám alatt közzétett döntése szerint – a weboldalt működtető szerver helye. Az elkövetési hely megállapítását tovább nehezítik azok a módszerek és programok, amelyek kifejezetten azt a célt szolgálják, hogy az elkövetők elrejtsék helyzetüket (és személyazonosságukat), így földrajzilag ne lehessen őket beazonosítani.[56]

A pozitív joghatósági konfliktusok másik módja *a joghatósággal rendelkező* és azt igénylő *államok közötti konzultáció*. A Budapesti Konvenció 22. cikk 5. pontja szerint „Ha több Fél joghatósága is kiterjed a jelen Egyezményben meghatározott feltételezett bűncselekményre, akkor az érintett Felek, amennyiben az célszerűnek mutatkozik, tárgyalást folytatnak annak érdekében, hogy eldöntsék, melyik az a Fél, aki megfelelőbben tudja lefolytatni az eljárást.”

[53] Recommendation 420 on the settlement of conflicts of jurisdiction in criminal matters adopted by the Consultative Assembly of the Council of Europe on 29 January 1965.
[54] M. NYITRAI: i.m. 243. o.
[55] BRENNER–KOOPS: i.m.: 15-16. o.
[56] Ilyen az IP-cím hamisítás (spoofing), valamint a proxy szerverek, VPN (Virtual Private Networks) vagy botnet infrastruktúra (zombigépek) használata. Lásd részletesen: MEZEI (2019): i.m. 195-196. o.

Látható, hogy a Konvenció alapján a konzultáció csupán célszerű lehetőség és nem valódi kötelezettség[57], a lakonikus rövidségű rendelkezés nem ad iránymutatást a joghatósági igények rangsorolására és hiányoznak azok a kritériumok[58] is, amelyek együttes értékelése alapján eldönthető az a kérdés, hogy melyik ország áll nyilvánvalóan a legszorosabb kapcsolatban az elkövetett bűncselekménnyel. Sőt, a Konvenció arra sem válaszol, hogy mi a teendő a konzultáció sikertelensége esetén.[59]

Álláspontunk szerint szükség lenne egy globális nemzetközi egyezményre[60], amely szabályozza a joghatósági kérdéseket és a joghatósági konfliktus esetén követendő eljárást. Az érintett államok közötti konzultáció szükséges elem, de a konzultáció lefolytatására célszerű ésszerűen rövid határidőt meghatározni. A konzultáció eredménytelensége esetén megfontolandó a joghatósági elvek közötti hierarchia felállítása, mert ellenkező esetben a kiberbűncselekmények elkövetőinek hatékony és időszerű felelősségre vonását kockáztatjuk.

Végül hangsúlyozzuk, hogy a joghatósággal rendelkező állam tisztázása csupán az első lépés az elkövető felelősségre vonása során, hiszen a joghatóság tényleges gyakorlására és az eljárás lefolytatására csak akkor kerülhet sor, ha az elkövető a joghatósággal rendelkező állam hatóságai számára rendelkezésre áll, akár oly módon is, hogy ennek az államnak az őrizetében van. Ha nem ez a helyzet, akkor az állami büntetőhatalom érvényesítéséhez igénybe kell venni a nemzetközi vagy az európai uniós bűnügyi jogsegély intézményeit.

Miután felvázoltuk a kiberbűncselekmények fogalmával kapcsolatos főbb hazai és nemzetközi álláspontokat, valamint rögzítettük a joghatóság gyakorlását megalapozó elveket és a releváns rendelkezéseket, a bevezetőben jelzett elemző modelljeinket mutatjuk be.

---

[57] A Konvenció Magyarázó Jelentése (Explanatory Report) szerint a konzultációs kötelezettség nem abszolút, hanem arra akkor kerül sor, „amennyiben az célszerűnek mutatkozik." Így például, ha az egyik állam fél tudomással bír róla, hogy hogy a konzultációra nincs szükség (mert megerősítést kapott arról, hogy a másik állam nem kíván joghatósági igénnyel élni), vagy ha az egyik állam álláspontja szerint a konzultáció hátrányosan befolyásolhatja a vizsgálatát vagy eljárását, elhalaszthatja vagy elutasíthatja a konzultációt. Lásd: Explanatory Report to the Convention on Cybercrime. https://rm.coe.int/16800cce5b (2023.07.15.)

[58] A joghatóság célszerű gyakorlását megalapozó körülmények az alábbiak lehetnek: az elkövetés helye; az elkövető állampolgársága; a terhelt és a sértett(ek) tartózkodási helye; az a hely, ahol a bűncselekmény nagyobb részében valósult meg, illetve ahol a legtöbb sértett van; az a hely, ahol a kár vagy a hátrány nagyobb része bekövetkezett; a más országok részére történő átadás vagy kiadatás lehetőségei; a terhelt érdekei, különösen a reszocializációs szempontok, stb. A kérdéskörhöz lásd NAGY Zoltán András: A joghatóság problémája a kiberbűncselekmények nyomozásában. In. Karsai Krisztina – Fantoly Zsanett – Juhász Zsuzsanna – Szomora Zsolt – Gál Andor (szerk.) *Ünnepi kötet Dr. Nagy Ferenc egyetemi tanár 70. születésnapjára.* Szeged, 2018. 761. o.

[59] A konzultáció eredménytelensége esetén ugyan szóba kerülhet valamely államközi szervezet vagy (választott)bíróság igénybe vétele, de ez bizonyosan az eljárás elhúzódásához vezetne és megkérdőjelezné a később lefolytatandó büntetőeljárás időszerűségét.

[60] Itt jegyezzük meg, hogy az ENSZ keretei között folyamatban van a kiberbűnözés elleni küzdelemről szóló új egyezmény – Átfogó nemzetközi egyezmény az információs és kommunikációs technológiák bűnügyi célú felhasználása elleni küzdelemről – létrehozása (Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes.)

4. I. SZ. MODELL: A TÁMADÁS DETEKTÁLT HELYSZÍNE MAGYARORSZÁG

Dogmatikai szempontból nem merül fel joghatósági probléma, amennyiben az elkövető magyar állampolgár, és az elkövetés helye is Magyarország, hiszen ebben az esetben az aktív személyi elv, valamint a területi elv mentén a magyar államnak, így a magyar bűnüldöző szerveknek egyértelmű az eljárási jogosultságuk. Ugyanígy a területi elv segít a joghatóság megállapításában, amennyiben a magyar államterületen magyar honosságú sértett ellen, vagy a magyar állami szervet – és nem az állami önvédelem elvén belüli értelmezhető klasszikus állam elleni deliktumnak minősülő -, vagy akár önkormányzati illetve egyéb közigazgatási szervet támadó kiberbűncselekmény elkövetője nem magyar állampolgár – legyen az uniós, vagy uniós állampolgársággal nem rendelkező személy.

Az együttműködés eszközeinek akkor van szerepük, joghatósági szempontból egyben akkor kezd bonyolultabbá válni a helyzet, ha a detektált elkövető nem tartózkodik Magyarország területén a már megindult büntetőeljárás idején és mindemellett még nem is rendelkezik magyar állampolgársággal. Ha ugyanis a kiberbűncselekmény tettese, vagy részese az Európai Unió valamely tagállamában lelhető fel – vagy azért, mert oda menekült a büntetőeljárás elől, vagy azért, mert ott lakóhellyel, vagy tartózkodási hellyel bír -, a hazai jogszabályi környezet alapján vele szemben a büntetőeljárás mind az általános, mind pedig a külföldön ismert helyen tartózkodó személlyel szembeni külön eljárás szabályrendszere mentén lefolytatható. Az általános szabályok szerinti eljárás alapfeltétele a terhelt jelenléte a büntetőeljárásban – nem feltételezve, hogy a terhelt él a tárgyaláshoz való jogról történő lemondás lehetőségével -, így az azt elősegítő nemzetközi, illetve európai együttműködési formáknak van érdemi jelentősége. Így amennyiben az Európai Unió valamely tagállamában tartózkodik a terhelt, a szükséges belföldi eljárásjogi intézkedések elvégzése - belföldi, illetve európai elfogatóparancs kibocsátása – után, utóbbi eredményessége esetén van lehetőség a terheltet az *Európai Unió tagállamaival folytatott bűnügyi együttműködésről szóló* 2012. évi CLXXX. tv. (a továbbiakban: EUbütv.) 25.§-ában foglalt eljárási rendnek megfelelően átadni[61]. Ennek hiányában *A büntetőeljárásról szóló* 2017. évi XC. tv. (a továbbiakban: Be.) 754-756.§§-ai szerinti külön eljárás alkalmazásának van lehetősége.

A helyzet azonban közel sem ennyire egyszerű, ugyanis a kiberbűnözést érintő joghatósági szabályok speciális nemzetközi szabályozóban is tetten érhetők, mely szabályok számos esetben pozitív vagy éppen negatív joghatósági összeütközéseket eredményezhetnek[62]. Ahogyan a korábbi fejezetben említettük, a Budapesti Konvenció, melyet

[61] Ehelyütt fontos kiemelni, hogy a kiberbűncselekmények mindegyike megfelel annak az anyagi jogi feltételnek, amit a hivatkozott együttműködési jogszabály támaszt, mely szerint a büntetendő cselekményre az anyagi jogi szabályoknak legalább 1 év szabadságvesztés büntetés kiszabásának lehetőségét kell kilátásba helyezniük. Megjegyezzük azonban, hogy amennyiben a büntetőeljárás nyomozati szakasza a terhelt távollétében került lefolytatásra, és vele szemben vádemelésre került sor, a bírósági szakban a vádat tárgyaló bírónak csak akkor van lehetősége európai elfogatóparancs kibocsátására, így az átadás jogintézménye is csak akkor alkalmazható, ha a vádiratban végrehajtandó szabadságvesztésre tett indítványt, vagy fiatalkorú terhelt esetén legalább javítóintézeti nevelés alkalmazására .

[62] TÓTH-GÁSPÁR: i.m. 149. o.

immáron több, mint 60 – közöttük értelemszerűen európai uniós – állam is ratifikált 22. cikkének 1. pontjában a területi és kvázi területi elvnek, valamint az aktív személyi elvnek tulajdonít jelentőséget. Ennek alapján a Budapesti Konvenció értelmében a joghatóság megállapításának elvárt feltétele, hogy az adott részes állam területén, vagy általa lajstromozott hajó, vagy repülőgép fedélzetén kövessék el az adott bűncselekménynek minősülő kibertámadást, vagy annak állampolgára minősüljön a bűncselekmény elkövetőjének, feltéve, hogy az elkövetés helyének joga szerint a cselekmény büntetendő. Ennek alapján tehát abban a hipotetikus esetben, ha egy nem magyar, de a Budapesti Konvenciót ratifikált állam állampolgára Magyarországon hajt végre egy kibertámadást magyar célponttal szemben, azonban elmenekül az országból, a honossága szerinti állam – minthogy a joghatósági elvek vagylagosak az egyezményben – az aktív személyi elvre hivatkozással maga is megállapíthatja joghatóságát és lefolytathatja a büntetőeljárást, amennyiben az érintett országok tárgyalásaik során ebben állapodnak meg[63].

Természetesen ezen tárgyalások eredményét célszerűségi, eljárás-hatékonysági, bizonyítási szempontok nagymértékben befolyásolják, hiszen ezekben az esetekben tulajdonképpen a területi és a személyi elv konkurál egymással. A hazai szakirodalom pedig jól kimutatja, hogy hány fajta érdek, indok alapozhat meg joghatóságot. Ilyen lehet pl.: az a hely, ahol a bűncselekményt, vagy annak jelentős részét megvalósították, a káros eredmény bekövetkezésének helye; a terhelt tartózkodási helye, esetleg lakóhelye; a bizonyítás helye, stb.[64]Az azonban álláspontunk szerint nyilvánvalónak tűnik, hogy ha a támadásra Magyarországon kerül sor magyar honosságú sértettel szemben akkor a bizonyítási érdek és annak eredményessége a területi elv, jelen esetben a bűncselekmény elkövetésének helye irányába mozdítja el a mérleg nyelvét. Ebben az esetben pedig az Európai Unió tagállamának területéről a fentiekben már említett átadás jogintézménye biztosítja a terhelt jelenlétét a hazai büntetőeljárásban[65].

A helyzet még árnyaltabb, ha a terhelt tartózkodási helye – a kibocsátott nemzetközi elfogatóparancs alapján – egy harmadik országban, azaz nem az Európai Unió területén kerül detektálásra. Ebben az esetben az EUbütv. az együttműködés kereteinek meghatározására nem lehet alkalmas, így kiindulópontunk *A nemzetközi bűnügyi jogsegélyről szóló* 1996. évi XXXVIII.

---

[63] A Budapesti Konvenció 22. cikk 5. pontja alapján ha több állam joghatósága is kiterjed az adott egyezmény hatálya alá tartozó bűncselekményre (pozitív joghatósági összeütközés), akkor a felek egyeztetés eredményeként jogosultak célszerűségi szempontok figyelembe vételével eldönteni, hogy mely állam folytassa le az eljárást.

[64] NAGY (2018): i.m. 761. o.

[65] Megjegyezzük ugyanakkor, hogy a szintén mögöttes szabályozóként értékelhető, azonban abban az esetben, ha az ügyben érintett másik európai állam nem tagállama az Európai Uniónak a párizsi *Európai Kiadatási Egyezmény,* melyet a magyar állam az 1994. évi XVIII. tv.-el ratifikált az átadáshoz hasonló feltételek mellett szabályozza a 2. cikkben a kiadatási bűncselekmények körét. Jelen tanulmány szempontjából az Európai Kiadatási Egyezmény rendelkezését az európai államok tekintetében csak annyiban tartjuk irányadónak, amennyiben hazánk mellett a nemzetközi elemet jelentő másik állam olyan európai ország, amely nem tagja ugyan az Európai Uniónak, de ratifikálta az Európai Kiadatási Egyezményt. Az Európában a kiadatás intézményére jellemző többpólusú szabályozásra a hazai szakirodalom is felhívta már egészen korán a figyelmet. Lásd ezzel kapcsolatban: M. NYITRAI Péter: A kiadatás intézmények újragondolása Európában – az európai elfogatóparancs eszméje és alkalmazásának főbb dilemmái. *Magyar Jog,* 2003/7. 401-410. o.

tv. (a továbbiakban: Nbjtv.) lehet. Az Nbjtv. 31.§-a alapján kiadatás iránti megkeresést büntetőeljárás lefolytatása érdekében jogosult a magyar állam címezni a terhelt tartózkodási helyével érintett harmadik állam irányába[66]. Ezen jogintézmény több elemét tekintve hasonlít az uniós államok közötti bűnügyi együttműködés eszközeként ismert átadás intézményéhez, hiszen a vádemelés előtt a bűncselekmény tárgyi súlya, míg a vádemelés után a végrehajtandó szabadságvesztés-büntetés, vagy javítóintézeti nevelés intézkedése indítványozásának ténye a feltétele[67]. A joghatósági összeütközést alapvetően ebben az esetben is a Budapesti Konvenció vagylagos joghatósági feltételrendszere adja[68], ahol ebben az esetben is a területi elv (kvázi területi elv), valamint a személyi elv tud konkurálni egymással – feltételezve, hogy valamennyi érintett ország ratifikálta az egyezményt[69]. Álláspontunk szerint azonban ebben az esetben is nyilvánvaló, hogy a bizonyítás az elkövetéssel érintett államban lehet eredményesebb, így a Budapesti Konvenció szellemisége alapján ebben az esetben is indokolt a büntetőeljárás magyar szabályok alapján történő lefolytatásának favorizálása, azaz a gyakorlatban a fenti eset sem valószínű, hogy megoldhatatlan feladat elé állítaná az érintett államokat, a kiadatás működőképes jogintézmény lehet. Megjegyezzük azonban, hogy a Budapesti Konvenció lehetővé teszi az államok számára, hogy a joghatósági elvként szabályozott kvázi területi elv, valamint aktív személyi elv egyáltalán ne, vagy csak meghatározott feltételek mellett alkalmazza[70]. Ennek külön értékelése azonban jelen tanulmány keretei között nem lehetséges, hiszen annak célja általános elvek megfogalmazása. Nyilvánvaló, hogy a konkrét együttműködést igénylő esetben az érintett államok belső jogi szabályozóinak is relevanciája van.

Összegzésképpen tehát megállapítható, hogy a hazánkban, alapvetően magyar honossággal bíró sértett sérelmére elkövetett kiberbűncselekmények miatti büntetőeljárások a fenti jogintézményeknek köszönhetően az elkövető állampolgárságára tekintet nélkül is lefolytathatók hazánkban a magyar jog szabályai szerint. Azaz a nemzetközi elem esetleges

[66] Az Nbjtv. 31.§-a alapján „kiadatás iránti megkeresés büntetőeljárás lefolytatása, szabadságvesztés büntetés, illetve szabadságelvonással járó intézkedés végrehajtása érdekében terjeszthető elő a külföldi államnál".

[67] Az Nbjtv. 32.§ (1) bekezdése a nemzetközi elfogatóparancs kibocsátásának feltételéül szabja az eljárás tárgyát képező bűncselekmény kellő súlyát, mely a 11.§ (2) bekezdésére történő visszautalás okán a legalább 1 évi szabadságvesztés büntetéssel fenyegetettséghez kapcsolható, míg az Nbjtv. 32.§ (2) bekezdése alapján a vádemelést követően a szabadságelvonó szankcióra tett ügyészi indítvány megléte szintén előfeltétel.

[68] A Budapesti Konvenció joghatósági elveket szabályozó 22. cikk 1. pontja alapján a joghatóság megállapítására okot adó körülmények az alábbiak: (1) a kiberbűncselekményt az adott részes állam területén követték el; (2) vagy a fél lobogóját viselő hajó, illetve (3) a félnél lajstromozott repülőgép fedélzetén valósították meg, végül pedig (4) ha a kiberbűncselekményt valamely fél állampolgára követte el, feltéve, hogy az adott cselekmény az elkövetés helye szerinti jog alapján is büntetendő, vagy ha a bűncselekmény nem tartozik egyetlen állam joghatósága alá sem.

[69]Egyéb forgatókönyvvel ehelyütt azért nem számolunk, mert amennyiben a tartózkodási hellyel érintett állam nem tagja az Európai Uniónak, valamint az Európa Tanácsnak és nem is ratifikálta a Budapesti Konvenciót, akkor a magyar hatóságok szempontjából az Nbjtv., valamint egy esetleges, a konkrét állammal kötött nemzetközi szerződés lehet az irányadó, utóbbit viszont modell szinten sem lehetséges értékelni.

[70] A Budapesti Konvenció 22. cikk 2. pontja értelmében minden részes állam fenntartotta magának a jogot, hogy a hivatkozott joghatósági szabályokat , vagy azok bármely elemét nem, vagy csak meghatározott esetekben és feltételek mellett alkalmazza.

megléte ilyen tényállás mellett nem képezi akadályát, hogy az egyezmények, valamint a hazai anyagi jog szabályai alapján alkalmazandó joghatósági elvek[71], illetve az egyéb szabályozott együttműködési alapintézmények (kiadatás, átadás) aggálymentesen biztosítsák egyrészt a magyar állam joghatóságát, másrészt pedig a terhelt jelenlétének biztosítását a hazai büntetőeljárásban[72].

5. II. SZ. MODELL: A TÁMADÁS KIINDULÁSI PONTJA AZ EURÓPAI UNIÓ VALAMELY TAGÁLLAMA

Modell-elemzésünk második esete, amikor a kibertámadás ugyan magyar honosságú sértettet érint, azonban a támadás kiindulási pontja nem Magyarország, hanem az Európai Unió más tagállama. Ezen tényállás mellett, amennyiben az elkövető magyar állampolgár, és az elkövetés helye szerinti tagállamban tartózkodik, az aktív személyi elv mentén a magyar állam joghatósága aggálymentesen megállapítható. Ugyanakkor a Budapesti Konvenció joghatósági szabályrendszere az elkövetés helyének eltérő tagállam területre esése esetén szintén megteremti a joghatósági kollíziót, mint ahogyan arra már a fentiekben, az I. sz. modell esetében is utaltunk.

Azaz ebben az esetben alapvetően három joghatóságot érintő tényező konkurál egymással. Az egyik az elkövető magyar állampolgársága, mely az aktív személyi elvet megalapozó faktor. Másrészt a területi elv, hiszen a bűncselekményt egy másik tagállam területéről követték el, ráadásul a fenti tényállásban az elkövető még ebben a tagállamban is tartózkodik. Harmadrészt pedig értelemszerűen figyelembe lehet venni azt a tényt is, hogy magyar honosságú a sértettje a kibertámadásnak. Ebben az esetben az érintett uniós tagállam az elkövető állampolgársága okán nem tagadhatná meg sem az EUbütv. szerinti átadásban való közreműködést – a feltételek fennállása esetén – sem pedig az adott személy kiadatását a Budapesti Konvenció alapján. Azaz erős valószínűség mellett jelenthető ki, hogy ebben az esetben a magyar állampolgár elkövetővel szemben a magyar hatóságok el tudnának járni, természetesen a bizonyítást segítő jogsegély-formák alkalmazása mellett. Ezt erősíti az Európai Kiadatási Egyezmény 1. cikke is, amely kiadatási kötelezettséget szabályoz a feltételek fennállása esetén a megkeresett ország tekintetében, ha a megkereső fél már büntetőeljárást folytat az adott terhelt ellen.

[71] Ezzel összefüggésben hangsúlyozzuk, hogy maga a Budapesti Konvenció sem zárja ki expressis verbis az azt ratifikáló állam belső joga szerinti joghatósági szabályainak alkalmazását, hiszen a 22. cikk 4. pontja akként fogamaz: „jelen egyezmény nem zárja ki a fél belső joga szerint meghatározott büntetőjogi joghatóságának gyakorlását."

[72] Ha pedig az adott együttműködési forma (ti. a kiadatás) az elkövető állampolgárságára tekintettel nem lenne teljesíthető, a részes államok a Budapesti Konvencióban elkötelezték magukat abban az irányban, hogy joghatóságuk megállapítása mellett az érintett személlyel szemben a büntetőeljárást lefolytassák. Megjegyezzük azonban, hogy azon európai államok esetében, melyek az Európa Tanács keretei között megalkotásra került Európai Kiadatási Egyezményt, a dokumentum 1. cikke a kiadatási kötelezettség alapelvi rendelkezéséből indul ki.

Ugyanakkor ezek a rendelkezések tisztán a főszabálynak tekinthetők, hiszen ha az adott tagállam a területiség elve alapján maga is indított büntetőeljárást[73] és belső joga alapján nem engedélyezett a kiadatás, akkor mind a Budapesti Konvenció, mind pedig a másodlagos jogforrásként még bizonyos európai relációkban érvényesülő Európai Kiadatási Egyezmény is lehetővé teszi a főszabálytól való eltérés lehetőségét, azonban bizonyos megkötések mellett[74].

A fenti tényállás a nemzetközi elem tekintetében még árnyaltabb, amennyiben a magyar állampolgárságú elkövető nem abban a Magyarországtól eltérő tagállamban tartózkodik a büntetőeljárás megindítását követően, ahol a kibertámadást a magyar honosságú sértett sérelmére elkövette. Ebben az esetben teljesen egyértelmű, hogy az a tagállam, amely a tényálláshoz csak annyiban kapcsolódik, hogy az elkövető ott tartózkodik, önállóan büntetőeljárást kezdeményezni vele szemben nem fog, hiszen az eljárás megindításához szükséges legitim joghatósági elv az ő vonatkozásában nem biztos, hogy megállapítható. Egy ilyen helyzetben két eset lehetséges. Az egyik, hogy csak az egyik érdemi joghatósági elvvel érintett tagállamban indult meg büntetőeljárás. A másik pedig, hogy mindkettőben, tehát hazánkban is és az elkövetés helye szerinti tagállamban is. Ebben az esetben beszélhetünk párhuzamos eljárásról. Az első esetben modellezésünk szempontjából nem merül fel probléma, ha csak hazánkban indult az ügyben büntetőeljárás, mert a fentiekben már említett együttműködési formák mentén az elkövető jelenléte a büntetőeljárásban biztosítható. Ha hazánkban nem, kizárólag csak az elkövetés helye szerinti államban indult büntetőeljárás, akkor az elkövető állampolgársága okán az adott tagállam információcsere keretei között tájékoztat az eljárásról, melynek eredményeként két lehetőséges forgatókönyv jöhet számításba: (a) saját maga lefolytatja a büntetőeljárást a fentiekben jelzett szabályok alapján, majd pedig lehetőség nyílik a tagállami ítélet hazai figyelembe vételét követően az ügydöntős határozat hazai végrehajtására; vagy (b) a magyar hatóságok a büntetőeljárás megindítását követően kibocsátott elfogatóparancs alapján kezdeményezik a magyar állampolgár átadását a büntetőeljárás lefolytatása céljából[75].

---

[73] Megjegyezzük, hogy ennek lehetősége nemcsak a Budapesti Konvenció, hanem az Európai Kiadatási Egyezmény 7. cikk (1) bekezdése alapján is adott, mely alapján „a megkeresett Fél megtagadhatja a kiadni kért személy kiadatását az olyan bűncselekmény miatt, amelyet saját joga szerint egészben vagy részben saját területén vagy ezzel egy tekintet alá eső területen követtek el."

[74] Azzal, hogy ebben az esetben a joghatóságát megállapító másik országnak tájékoztatási kötelezettsége van a Budapesti Konvenció alapján a megkereső állam felé, amennyiben az azt igényli. Az egyezmény 24. cikk 6. pontja ugyanis az alábbiak szerint fogalmaz: „Ha a jelen cikk 1. bekezdésében említett bűncselekmények vonatkozásában kizárólag a kiadni kért személy állampolgársága alapján vagy azért tagadják meg a kiadatást, mert a megkeresett fél saját joghatósága alá tartozónak ítéli meg a bűncselekményt, akkor a megkeresett Fél a megkereső Fél kérelmére az eljárás lefolytatása érdekében a saját, hatáskörrel rendelkező hatóságai elé terjeszti az ügyet, és megfelelő időn belül beszámol a megkereső Félnek az ügy kimeneteléről. Az említett hatóságok a nyomozás és az eljárás folytatása, valamint a döntés meghozatal során a megkeresett Félnek a hasonló jellegű bűncselekményekre irányadó szabályai alapján járnak el."

[75] Megjegyezzük, hogy az állampolgárság, illetve az elkövetés helye, mint joghatóságot megalapozó okok a kiberbűnözéssel szembeni uniós szintű fellépés egyéb jogforrásaiban is tetten érhető, így *a gyermekek szexuális bántalmazása, szexuális kizsákmányolása és a gyermekpornográfia elleni küzdelemről, valamint a 2004/68/IB tanácsi kerethatározat felváltásáról szóló* Európai Parlament és a Tanács által elfogadott 2011/93/EU irányelvben,

Amennyiben párhuzamos eljárások vannak folyamatban, azaz egyszerre két tagállamban is folyik az elkövetővel szemben ugyanazon kiberbűncselekmény miatt büntetőeljárás, akkor az EUbütv. 106-107.§§-ai szerinti konzultációs eljárás lefolytatásának van helye, melynek megindulását megelőzően – hiszen annak eredményétől a joghatóság véglegessé válása függ – a hazai büntetőeljárást fel kell függeszteni a Be. 398.§ (2) bek. b) pontja, illetve vádemelés esetén a Be. 488.§ (1) bek. e) pontja alapján.

Amennyiben a magyar állampolgárságú elkövető nem az Európai Unió valamely tagállamában tartózkodik a büntetőeljárás megindulását követően, az Nbjtv. már felhívott kiadatási rendelkezései mentén lehet megteremteni a büntető igény érvényesítésének lehetőségét az elkövetővel szemben.

Ugyanakkor a bűncselekmény elkövetője nemcsak magyar állampolgár lehet, hanem más uniós tagállam állampolgára, vagy akár harmadik ország állampolgára is. Azaz II. sz. modellünkben ki kell térnünk arra az esetre is, ha a Magyarországon sérelmet kiváltó kiberbűncselekményt az Európai Unió más tagállamában nem magyar állampolgárságú személy követi el. Ebben az esetben a passzív személyi elven kívül egyéb tényező nem szól a büntetőeljárás magyarországi lefolytatása mellett, ráadásul a bizonyítási érdek és az elkövető állampolgársága mentén sem indokolható a hazai hatóságok joghatósága. Álláspontunk szerint ezért ilyen forgatókönyv esetén a hazai hatóságok a külföldi állam által lefolytatott büntetőeljárás számára nyújthatnak eljárási jogsegélyt, azonban sem az eljárás hazai lefolytatására, sem pedig az esetleges szankció magyarországi végrehajtására nincs ésszerű jogi, szakmai indok.

6. III. sz. modell: a támadás az Európai Unió területén kívüli, harmadik állam területén kerül elkövetésre

A harmadik, egyben utolsó modellünkben az elkövetés helye olyan állam területén található, amely nem tagállama az Európai Uniónak. Természetesen az együttműködési szabályok alkalmazása szempontjából itt is jelentősége van az elkövető állampolgárságának, az elkövető tartózkodási helyének (amennyiben eltér az elkövetés helye szerinti államtól), illetve annak, hogy az elkövetés helye szerinti állam ratifikálta-e az Európai Kiadatási Egyezményt – amennyiben például nem uniós, de európai államról van szó, valamint a Budapest Konvenciót[76]. Mivel a Budapesti Konvenció a preambulumában kijelölt célok okán *lex speciálisnak* tekinthető az Európai Kiadatási Egyezményhez képest, ezért az általunk felállított III. számú modell

az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról szóló Európai Parlament és a Tanács által elfogadott 2013/40/EU irányelvben, valamint a készpénz-helyettesítő fizetési eszközzel elkövetett csalás és *a készpénz-helyettesítő fizetési eszközök hamisítása elleni küzdelemről, valamint a 2001/413/IB tanácsi kerethatározat felváltásáról szóló* Európai Parlament és a Tanács által elfogadott 2019/713/EU irányelvben. Lásd ezzel kapcsolatban bővebben: TÓTH-GÁSPÁR: i.m. 146-147. o.

[76] A Budapesti Konvenció preambuluma értelmében az egyezmény célja kifejezetten a számítógépes bűnözéssel szembeni hatékony nemzetközi szintű fellépés elérése és ennek jegyében az Európa Tanács tagállamai között már irányadó, a nemzetközi bűnügyi együttműködésre vonatkozó hatályos egyezményeknek (így pl. az Európai Kiadatási Egyezménynek) a kiegészítése.

esetében az együttműködési rendszer vizsgálata lépcsős. Elsőként a Budapesti Konvenció alkalmazhatóságát kell vizsgálni, és ehhez képest az Európai Kiadatási Egyezmény csak másodlagos (uniós tagállamok között pedig az uniós szintű együttműködési rendszer eszközeihez viszonyítva alkalmazása gyakorlatilag nem történik meg). Ezt a vizsgálatot egészíti ki a korábbiakban már alkalmazott Nbjtv., valamint – amennyiben van – az érintett államok között speciális, egyedi együttműködési szerződés, megállapodás.

A több, fenti premisszák mentén felállítható modell közül az első eset az, ha az elkövető magyar állampolgár, és a magyar honosságú sértett sérelmére a kiberbűncselekményt egy harmadik, azonban nem uniós állam területén követi el. Ebben a modellben az elkövető egyrészt tartózkodhat a bűncselekmény hatóságok általi detektálása és a büntetőeljárás elindítását követően abban az államban, ahol elkövette a bűncselekményt, valamint más államban, akár hazánkban is. Teljesen nyilvánvaló, hogy ez utóbbi esetben dogmatikai probléma a joghatósági kérdések vonatkozásában nem merülhet fel, hiszen a hazánkban tartózkodó magyar állampolgárral szemben a magyar államnak akkor is fennáll a joghatósága, ha a bűncselekményt egy, az Európai Unióhoz nem tartozó állam területén követte el. Amennyiben viszont az elkövetés helye szerinti nem uniós államban tartózkodik az elkövető, akkor a feltételek fennállása esetén a Budapesti Konvenció 24. cikke szerinti kiadatás, vagy a konvenció alkalmazhatóságának hiányában akár az Európai Kiadatási Egyezményen alapuló kiadatási szabályok is alkalmazhatók[77]. Természetesen mindkét eset azt feltételezi, hogy az elkövetés helye szerinti állam az Európa Tanács tagjának minősül. Amennyiben ez nem áll fenn, azaz az elkövetés helye Európán kívüli állam, a magyar állampolgárságú elkövető hazai büntetőeljárási jelenlétének biztosítására az Nbjtv. kiadatásra vonatkozó rendelkezései teremtenek jogi alapot, feltéve, hogy az adott állammal speciális szabályt teremtő nemzetközi szerződés nincs hatályban[78].

Amennyiben a magyar állampolgárságú elkövető nem az elkövetés helye szerinti, de Magyarországtól eltérő országban tartózkodik, az igénybe vehető eszközök nem térnek el az előző forgatókönyvtől, hiszen ebben az esetben az adott államnak gyakorlatilag ismételten semmilyen indokolható joghatósági érve nem lehet a büntetőeljárás lefolytatására, hiszen sem az elkövetés, sem az állampolgárság nem kapcsolja hozzá az elkövetőt. Így a fentiekben már részletesen bemutatott eszközök alkalmazása ismételten attól függ, hogy uniós tagállamban, nem uniós, de európai, az Európa Tanács tagjának minősülő államban, vagy nem európai államban tartózkodik az elkövető.

---

[77] Természetesen nem kizárt, hogy az érintett állam vagy azért, mert már maga is indított büntetőeljárást, vagy azért, mert azt megindíthatónak tartja saját joghatóságának megállapítása okán – lásd az elkövetés helye – akár a Budapesti Konvenció 24. cikk 6. pontja, akár az Európai Kiadatási Egyezmény 7-8. cikkelyei alapján megtagadja a kiadatást. Ebben az esetben a büntetőeljárás lefolytatását követően a külföldi ítélet – amennyiben marasztaló ítélet születik – hazai végrehajtására nyílik lehetőség, feltéve, hogy a külföldi ítélet elismerése lehetséges az Nbjtv. rendelkezései mentén.

[78] Még ebben az esetben is előfordulhat azonban, hogy az elkövetés helye szerinti, nem európai állam maga kívánja a büntetőeljárást a magyar állampolgárságú elkövetővel szemben lefolytatni. Ebben az esetben hazai büntetőeljárás vagy el sem indul, vagy ha elindult, akkor annak felfüggesztésének van helye a vádemelés előtt a Be.394.§ (4) bek. d) pontja alapján, a vádemelés után pedig a Be. 488.§ (1) bek. i) pontja alapján.

III. számú modellünk utolsó lehetséges esetköre, ha az elkövető nem rendelkezik magyar állampolgársággal, azonban a sértett magyar honosságú. A magyar államnak ebben az esetben a kettős inkrimináció elvén alapuló passzív személyi elv mentén lenne csak elképzelhető joghatóságának megállapítása. Ugyanakkor az elkövetés helye, valamint az elkövető állampolgársága a fentiekben már bemutatott rendelkezések alapján a Budapesti Konvencióban speciális joghatósági elvek, melyeknek lehetőség szerint primátusa van az azt ratifikáló államok relációjában. Ebben a modellben tehát a Budapesti Konvenció kizárólag az Európa Tanács tagjainak vonatkozásában értelmezhető, Európán kívüli harmadik állam esetében nem. Amennyiben európai államról van szó, akkor ismételten elsődlegesen a Budapesti Konvenció szerinti kiadatásnak, amennyiben pedig – elméleti síkon - azt nem ratifikáló európai államról van szó, akkor az Európai Kiadatási Egyezmény kiadatási szabályai alkalmazásának lenne helye. Ugyanakkor – mint ahogyan arra a II. számú modellben is kitértünk – a fenti, alapvető, a joghatóságot megalapozó elvek hiányában a magyar állam legfeljebb eljárási jogsegély keretei között segítené a gyakorlatban a külföldön folyó büntetőeljárást. Ugyanerre a következtetésre juthatunk, ha a nem magyar állampolgár elkövető a kiberbűncselekményt nem európai állam területéről követte el. Hiszen ebben az esetben sincs közvetlen joghatósági kapcsolódása magyar államnak a tényálláshoz az elkövető, illetve az elkövetés helye oldaláról. A bizonyítást segítő eljárási jogsegély-típusú együttműködés ebben az esetben is valószínűbbnek mutatkozik.

7. Záró gondolatok

Tanulmányunkban a kibertérben elkövetett, bűncselekménynek minősülő magatartásokat alapvetően anyagi jogi szemüvegen keresztül vizsgáltuk. Célunk azoknak az európai, illetve nemzetközi bűnügyi együttműködési formáknak a leltározása volt, melyek segítségével a magyar hatóságok előtt folyó büntetőeljárás számára „biztosítható” az elkövető. A kutatás tárgyára, valamint a tanulmány által meghatározott terjedelmi korlátokra figyelemmel, azon esetekre helyeztük a fókuszpontot, amikor a kibertámadás célkeresztjében magyar, azaz hazai honosságú sértett áll, legyen az természetes, vagy nem természetes személy. Az egyes joghatósági kérdések vizsgálatát megelőzően azonban célunk volt a kutatás tárgyához kapcsolódó kiberbűncselekmények fogalmi kereteinek tisztázása, az ezzel kapcsolatos fontosabb hazai és külföldi szakirodalom rövid bemutatása.

Magunk részéről – tekintettel a vizsgálat tárgyának szerteágazó jellegére – a tisztán egyetlen mondatban történő definiálást nem tartjuk indokolnak és követendőnek. A kiberbűncselekmények fogalmának tipológiai szempontú megközelítése – különösen a hármas felosztás – már jóval fejlettebb, nézetünk szerint azonban a releváns bűncselekmények rendszerezésén alapuló definíciók azok, amelyek a leginkább hozzásegíthetnek bennünket a kiberbűnözés fogalmi kereteinek megértéséhez.

Modellezésünk során az egyes joghatósági kérdések vizsgálata körében alapvetően négy dokumentumot vettünk alapul, melyek mentén objektív módon az elemzés elvégezhető volt. Természetes, hogy minden eset más és más, és akkor a tényállással érintett államok közötti

kétoldalú megállapodások is árnyalhatják a képet. Ezzel azonban a modellek felállítása során nem számoltunk, hiszen lehetetlen is lett volna minden ilyen nemzetközi jogi helyzetet külön-külön is értékelni. Számunkra az uniós tagállamok között bűnügyi együttműködés alapintézményeinek, valamint a Budapesti Konvenciónak, az Európai Kiadatási Egyezménynek, valamint a nemzetközi bűnügyi jogsegély törvényünknek volt relevanciája. Ezekkel kapcsolatban tézisként rögzíthető, hogy az uniós tagállamok között bűnügyi együttműködés gördülékenysége a rendelkezésre álló és a tanulmányban is bemutatott eszközök mentén biztosítható. Álláspontunk szerint ezen jogi környezetnek van primátusa a számítógépes bűncselekmények miatti büntetőeljárásokban is, amennyiben a tényállásba uniós elem keveredne. Ehhez képest nézetünk szerint a Budapesti Konvenció – mely saját preambulumában megfogalmazott elvei alapján is egyfajta kiegészítését biztosítja a már meglévő együttműködési keretrendszernek – valamint még inkább az Európai Kiadatási Egyezmény másodlagosnak tekinthető. Minthogy mindkét egyezmény az Európa Tanács keretei között került elfogadásra, értelemszerűen olyan európai államok viszonylatában bírnak jelentőséggel, amelyek nem tagjai az Európai Uniónak. A tanulmányban is hivatkozott Nbjtv. pedig elsődlegesen akkor bírhat relevanciával, ha az érintett – Magyarországon kívüli – másik állam, vagy olyan európai állam lenne, amely nem tagja az Európa Tanácsnak (ez tulajdonképpen hipotetikus kérdés, hiszen az európai államok közül Fehéroroszország, valamint a Vatikán nem tagja az Európa Tanácsnak), vagy pedig Európán kívüli állam. Összességében azonban elmondható, hogy a rendelkezésre álló együttműködési eszközök hatékony fellépést biztosítanak az európai és a nemzetközi térben is a határokon átívelő kiberbűncselekmények elkövetőivel szembeni fellépés során.


UNIVERSITY OF PUBLIC SERVICE
LUDOVIKA

Military and Intelligence CyberSecurity Research Paper 2023/2.

Szerző(k) / Author(s):
Dr. Bartkó Róbert PhD – Dr. Sántha Ferenc PhD

Kézirat lezárásának ideje / Manuscript closing time:
2023.08.15.

Szerkesztők / Editors:
Dr. Farkas Ádám PhD
Dr. Magyar Sánor PhD

Kiadó / Publisher:
Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar
Nemzetbiztonsági Intézet Katonai Nemzetbiztonsági Tanszék
University of Public Service (Hungary), Faculty of Military Sciences and Officer Training, National Security Institute Department of Military National Security

Kiadó képviselője / Representative of the publisher:
Dr. Magyar Sándor PhD

Elérhetőségek /Contacts:
https://nbi.uni-nke.hu/oktatasi-egysegek/katonai-nemzetbiztonsagi-tanszek/katonai-nemzetbiztonsagi-kiberter-muveleti-szakcsoport/researchpaper

farkas.adam@uni-nke.hu | magyar.sandor@uni-nke.hu

1011 Budapest, Hungária krt. 9-11. /9-11. Hungária Blvd., Budapest, H1011

ISSN:
2786-3778

A borító https://www.stockvault.net/photo/270507/cyber-security-web-security-network-security címen elérhető ingyenes háttérkép felhasználásával 2021. február 25-én készült.

The cover was created on 25. February 2021, using a free wallpaper available at https://www.stockvault.net/photo/270507/cyber-security-web-security-network-security.