

**Navigálás a szürkezónában –
A kiberhírszerzés elméletben és gyakorlatban.**

JUM410

Dolgozat lezárásának dátuma: 2024. november 4.

I.	BEVEZETÉS ÉS PROBLÉMAFELVETÉS	3
II.	ALAPFOGALMAK	5
A.	Kibertér és kiberműveletek	5
1.	A számítógépes hálózat elleni támadás	6
2.	Információs műveletek	7
3.	A számítógépes hálózat kihasználására irányuló műveletek	8
B.	Hírszerzés	8
1.	Gazdasági hírszerzés	8
2.	Politikai hírszerzés	9
3.	A hírszerzés elkülönítése a kémkedéstől és a megfigyeléstől	9
4.	A leggyakoribb hírszerzési gyakorlatok	10
III.	A KIBERHÍRSZERZÉS BETUDÁSA	13
A.	A <i>de jure</i> és <i>de facto</i> állami szervek.	14
B.	Az állam irányítása vagy ellenőrzése alatt végzett műveletek.	15
C.	Az állam által saját cselekményként elismert művelet.	15
IV.	KIBERHÍRSZERZÉS ELMÉLETBEN - A KIBERHÍRSZERZÉS SZABÁLYOZÁSA	17
A.	Alkalmazandó-e a nemzetközi jog a kiberműveletekre?	17
B.	A kiberhírszerzés jogszerűsége	18
1.	A kiberhírszerzés mint <i>sui generis</i> nemzetközi jogi jogsértés	18
2.	Szuverenitás	21
3.	Belügyekbe való beavatkozás tilalma	23
4.	Diplomáciai jog	24
5.	Összegzés – A kiberhírszerzés, mint egy nemzetközi jogi szűrkezőna	27
V.	KIBERHÍRSZERZÉS A GYAKORLATBAN – JOGON TÚLI ESZKÖZÖK A KIBERHÍRSZERZÉSI MŰVELETEK ELLENI HARCBA	29
A.	A kiberinfrastruktúra fejlesztése	29
B.	Nemzetközi normák kialakítása	31
C.	Diplomácia és gazdasági szankciók	31
D.	Nemzetközi védelmi és biztonsági szövetségek	32
E.	Támadás, mint válaszreakció	33
VI.	KONKLÚZIÓ	35
VII.	FORRÁSJEGYZÉK	37

I. BEVEZETÉS ÉS PROBLÉMAFELVETÉS

A hírszerzés és a kémkedés egyidős az emberiséggel: kémekkel találkozhatunk a Bibliában, az ókori Görögországban és az ősi Kínában is.¹ Emellett a kémkedésnek óriási jelentősége volt a világháborúk során is.² A kémkedésnek azonban mindig megvoltak a korlátai és hátrányai. Az ókorban az információáramlás lassúsága, valamint a források megbízhatatlansága jelentette a legnagyobb problémát. Ezt az írásos dokumentáció megjelenése kiküszöbölte. A huszadik század kémeinek a legnagyobb nehézséget a megszerezhető információ mennyiségének korlátozottsága, valamint a felfedés veszélye jelentette.

Azonban ahogy életünk annyi más részét, a hírszerzést is a feje tetejére állította a technológia. Míg a „klasszikus időkben” egy kém legfeljebb egy-két könyvet tudott kicsempészni, addig a technológia adta lehetőségek kihasználásával a teljes könyvtár megszerezhető, ráadásul észrevétlenül. Ennyi adathoz és dokumentumhoz a régi idők kémeinek targoncára és kamionra lett volna szükségük, és szinte biztos, hogy nem tudtak volna elmenekülni anélkül, hogy felfednék őket.³ Nem véletlen, hogy a legtöbb állam a belső jogában tiltja a kiberhírszerzési műveletek végrehajtását, sőt egyes esetekben a bíróságok súlyosabb büntetéseket szabnak ki, amennyiben a kémkedést elektronikus információs eszközökkel hajtották végre.⁴ A cselekmények súlya és az államok belső joga által tükrözött hozzáállása alapján tehát azt feltételezhetnénk, hogy a kiberhírszerzés nemzetközi szinten is jogsértő. Ez azonban közel sincs így. A nemzetközi jog jelenleg nem tiltja közvetlenül a kiberhírszerzést, és a közvetett jogsértések megállapítása is kifejezetten nehéz. Mi ennek az oka? Mitől válik egy cselekmény nemzetközi szinten is jogsértővé? Milyen eszközökhöz folyamodnak az államok a kifejezett tiltás hiányában? Hogyan készülnek fel és válaszolnak az államok az ellenük végrehajtott kiberhírszerzési műveletekre? A dolgozat ezen témákat járja körbe.

A dolgozatom három nagyobb részre tagolódik. Az első részben (II.-III.) definiálom a téma megértéséhez szükséges alapfogalmakat, vagyis a kiberteret, a kiberműveleteket és a hírszerzést. Ennek keretén belül bemutatom a kiberműveletek főbb típusait, valamint a leggyakrabban bevetett hírszerzési módszereket is. Emellett az ebben az első – bevezető –

¹ Darien Pun, *Rethinking Espionage in the Modern Era* 23 Chi J Intl L 353 (2022) [‘PUN’], 353.

² Kristin A. Vara, *'Espionage: A Comparative Analysis'* 22 ILSA J Int'l & Comp L (2015) 61, 63.

³ Alexander Melnitzky, *'Defending America Against Cyber Espionage Through the Use of Active Defenses'*, 20 Cardozo J. Int'l and Comp. L. 537 (2012), 566.

⁴ *United States of America, v. Joshua Adam*, 436 F. Supp. 3d 698 (S.D.N.Y. 2020); *Chelsea Manning, Plaintiff, v. U.S. Department of Justice, et al*, 234 F. Supp. 3d 26 (D.D.C. 2017).

részben vizsgálom a kiberhírszerzési műveletek betudásának nehézségeit, valamint ismertetem a nemzetközi jogban leginkább alkalmazható betudási tesztek.

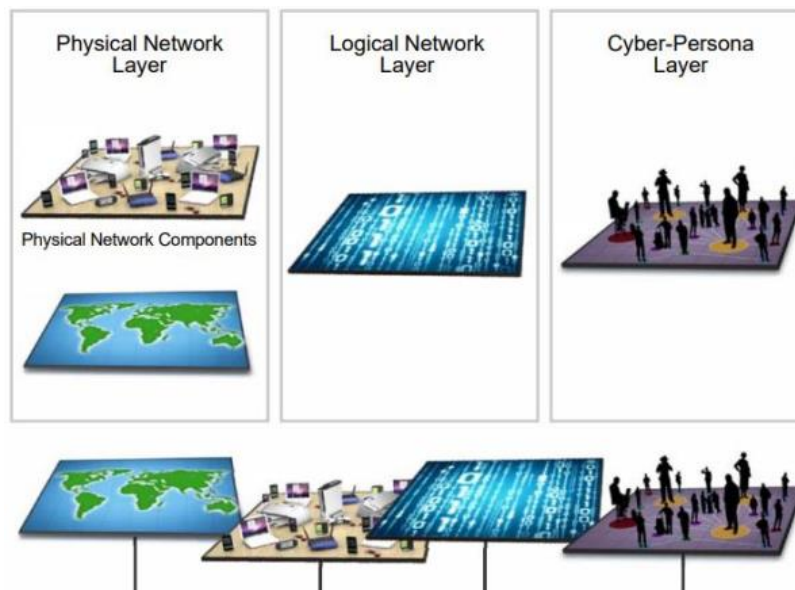
A dolgozat második részében (IV.) a kiberhírszerzési műveletek szabályozási keretrendszerét, azaz a kiberhírszerzés elméleti oldalát ismertetem. Ennek keretében elsőként tisztázom, hogy miként alkalmazandóak a nemzetközi jogi normák a kibertérben végrehajtott állami cselekményekre, majd azt vizsgálom, hogy a kiberhírszerzés milyen nemzetközi jogi normákkal lehet ellentétes.

Végül a dolgozat harmadik részében (V.) az államok hozzáállását, azaz a kiberhírszerzés gyakorlati oldalát ismertetem. Itt bemutatom, hogy az államok milyen előzetes intézkedéseket és milyen válaszlépéseket hajtanak végre a kiberhírszerzési műveletek visszaszorítása és elkerülése céljából.

II. ALAPFOGALMAK

A. Kibertér és kiberműveletek

Ahhoz, hogy beszélni tudjunk a kiberhírszerzésről, tudnunk kell pontosan, hogy mit jelez a "kiber" előtag és hogy pontosan mi az a kibertér és mik a kiberműveletek. Az Oxford Dictionary szerint a kibertér „az a képzeletbeli környezet, amelyben a számítógépes hálózatokon keresztül történő kommunikáció zajlik”;⁵ a Merriam-Webster szerint pedig „a számítógépes hálózatok és az internet online világa”.⁶ A kiberteret legjobban egy idegrendszerként lehet elképzeni, melyet több ezer a világ minden táján található számítógép, szerver, optikai kábel és egyéb eszköz alkot és tart működésben.⁷ A kibertér három külön réteg együttes működéséből, működtetéséből alakul ki. Az első (fizikai) réteget a kiberteret alkotó számítógépek, kábelek és más hardverek alkotják. A második (logikai) réteget az ezeken az eszközökön futó különböző szoftverek és kódok alkotják, melyek a kiberteret működőképesé teszik. A harmadik (szociális) réteget pedig az interneten megjelenő személyek (melyeket irányíthatnak egyaránt emberek és gépek is) alkotják, amelyek a szoftverek és hardverek együttes képességeit kihasználva „életet lehelnek” a kibertérbe.⁸ A kibertér rétegződését az 1. ábra szemlélteti.



1. ábra, forrás: NATO STANDARDIZATION OFFICE, NATO Standard AJP-3.2. Allied Joint Doctrine for Land Operations (2022) I-4.

⁵ Oxford English Dictionary, 'Cyberspace' (Letöltve: 2024.10.23.)

⁶ Merriam-Webster, 'Cyberspace' (Letöltve: 2024.10.23.)

⁷ The White House, *The National Strategy to Secure Cyberspace* (2003) 1.

⁸ David Clemente, *Cyber Security and Global Interdependence: What Is Critical?* (Chatham House 2013) 5.

A nemzetközi közösség egyelőre nem alakított ki egységes definíciót a kibertérre vonatkozóan. Azonban egyes szervezetek megpróbálták már értelmezni. A NATO például globális tartományként definiálja, „melynek alkotóelemei az egymással összekapcsolt kommunikációs, informatikai és egyéb elektronikus rendszerek, hálózatok és azok adatai, beleértve azokat is, amelyek elkülönülnek vagy függetlenek, és amelyek adatokat dolgoznak fel, tárolnak vagy továbbítanak.”⁹ Hasonlóan ehhez a fogalomhoz, a legtöbb kommentátor a kibertér definíálásakor annak globális jellegét, valamint az összekapcsolt kommunikációs infrastruktúrát emeli ki.¹⁰

A tág értelemben vett kiberműveleteknek az előbbi magyarázatból kiindulva a harmadik (fizikai) rétegben végbemenő különböző irányított folyamatokat nevezzük. A kiberműveletek hatásaikat tekintve kétfélek lehetnek: kiberműveletek, melyek hatásai csak a kibertérben érzékelhetők (például egy kibertámadás, ami megbénítja egy állam kormányának hivatalos honlapját), vagy kiberműveletek, melyek hatásai a fizikai térben manifesztálódnak (például egy kibertámadás, amely egy erőmű meghibásodását okozza).

A dolgozat szempontjából fontos elkülöníteni az államok által végrehajtott – szűkebb értelemben vett – kiberműveleteket a kiberbűnözéstől. Míg a kiberbűnözés – mely magában foglal minden bűncselekményt, amelyet elektronikus adatok és számítógépes rendszerek integritása, bizalmassága vagy hozzáférhetősége ellen irányul – többnyire az állam belső jogát érinti, és természetes és jogi személyek követhetik el, addig a kiberműveleteket államok követik el más államok ellen, és a nemzetközi jog szabályozza.¹¹ A kiberműveletek számos típusa különböztethető meg, ezek közül azonban a dolgozatban a három leggyakrabban végrehajtott műveletet említem meg.

1. A számítógépes hálózat elleni támadás

A számítógépes hálózatok ellen intézett kibertámadások (*computer network attack*) célja a célállam számítógépes eszközökön vagy számítógépes hálózaton tárolt információk, vagy

⁹ NATO Standardization Office, *NATO Standard AJP-3.2. Allied Joint Doctrine for Land Operations* (2022) 2.50.bek.

¹⁰ Nils Melzer, 'Cyberwarfare and International Law' (UNIDIR 2011) 4.; P.W. Singer and Allan Friedman, 'Cybersecurity and Cyberwar: What Everyone Needs to Know', OUP (2014) 13; U.S. Department of Defense, 'Dictionary of Military and Associated Terms', (2021) JP 3-12.

¹¹ Marco Roscini, *International Law and the Principle of Non-intervention*, OUP (2024), 377.

maguk a számítógépes eszközök vagy hálózatok megsemmisítése vagy kompromittálása.¹² Többek között ilyen támadásnak minősülnek az elosztott szolgáltatásmegtagadással járó támadások, másnéven túlterheléses támadások (*distributed denial-of-service [DDoS]*), melyek túlzott adatforgalom generálásával tesznek egy szervert elérhetetlenné. De ilyen támadások azok a rosszindulatú szoftverek is, melyek a számítógépen tárolt adatokat semmisítenek meg vagy tesznek elérhetetlenné.¹³ Számítógépes hálózatok elleni támadásnak minősült az, amikor 2015-ben¹⁴ és 2016-ban¹⁵ orosz hackercsoportok okoztak áramszünetet Ukrajna jelentős részén, de a 2010-es Irán elleni Stuxnet támadás¹⁶ vagy az 2007-es észt közintézmények honlapjai ellen intézett DDoS támadás¹⁷ is.

2. Információs műveletek

Az információs műveletek (*information operations*) vagy másnéven pszichológiai műveletek (*psychological operations*) szintén nem destruktív támadások. Céljuk az egyének gondolkodásmódjának és döntéseinek befolyásolása, mely politikai vagy katonai célok megvalósítását segíti elő.¹⁸ Ezeket a célokat különböző információk a célszemély(ek)hez való eljuttatásával éri el. Az információs műveleteket az államok többsége alkalmazza,¹⁹ hiszen a nemzetközi jogban nem vonatkozik rájuk kifejezett tilalom.²⁰ Azonban természetükből fakadóan ezek a műveletek alkalmasak lehetnek egy másik állam, vagy az állam lakossága véleményének, akaratának megváltoztatására.

¹² Remus Titiriga, 'Cyber-Attacks and International Law of Armed Conflicts; a "Jus ad Bellum" Perspective', 8(3) *Journal of International Commercial Law and Technology* 179 (2013), 179.

¹³ Adam Liff, 'Cyberwar: A New "Absolute Weapon"? The Proliferation of Cyberwarfare Capabilities and Interstate War', 35(3) *J Strateg Stud* 401 (2012), 406.

¹⁴ Council on Foreign Relations ['CFR'], 'Compromise of a Power Grid in Eastern Ukraine', <https://www.cfr.org/cyber-operations/compromise-power-grid-eastern-ukraine>, (Letöltve: 2024.10.23.)

¹⁵ CFR, 'A compromise causes a power outage in Kiev, Ukraine.', <https://www.cfr.org/cyber-operations/compromise-causes-power-outage-kiev-ukraine>, (Letöltve: 2024.10.23.)

¹⁶ CFR, 'Stuxnet.', <https://www.cfr.org/cyber-operations/stuxnet>, (Letöltve: 2024.10.23.)

¹⁷ CFR, 'Estonian denial of service incident.', <https://www.cfr.org/cyber-operations/estonian-denial-service-incident>, (Letöltve: 2024.10.23.)

¹⁸ Steven Collins, 'NATO and Strategic PSYOPs: Policy Pariah or Growth Industry?', 1(3) *Journal of Information Warfare* 72 (2002), 73.

¹⁹ NATO Military Committee, *MC-402.2 NATO Military Policy on Psychological Operations* (2012); U.S. Department of Defense, *Joint Publication 3.10.1* (2014).

²⁰ Peter J Smyczek, 'Regulating the Battlefield of the Future: The Legal Limitations on the Conduct of Psychological Operations (PSYOP) under Public International Law', 57 *A.F. L. Rev* 210 (2005), 213.

3. A számítógépes hálózat kihasználására irányuló műveletek

A kiberhírszerzéshez legszorosabban kapcsolódó kiberműveletek, a számítógépes hálózat kihasználására irányuló műveletek (*computer network exploitation*) nem destruktívak, mivel céljuk csupán a számítógépeken és a számítógépes hálózatokon tárolt adatokhoz való hozzáférés.²¹ Ilyen támadásnak minősült a Regin kémsoftver telepítése az Európai Unió egyes hálózataira,²² valamint a Pegasus kémsoftverrel végrehajtott megfigyelések is.²³

B. Hírszerzés

A téma megértéséhez szükségképpen szükséges ismertetni a hírszerzés definícióját is. Hírszerzésnek nevezzük „a számítógépek vagy elektronikus információs eszközök olyan használatát, melynek célja, hogy a végrehajtó állam hozzáférjen a célállamra vonatkozó érzékeny információkhoz.”²⁴ A kiberhírszerzés a kibertér bármely rétegében végrehajtható: a fizikai rétegben például elképzelhető, hogy egy pendriveon keresztül kémsoftvert juttatnak a célállam elektronikus infrastruktúrájába, amely így a logikai rétegben fejti ki a hatását. A szociális rétegben pedig a leggyakoribb hírszerzési technika az adathalászat, amely az emberi figyelmetlenséget és a szociális réteg sérülékenységét használja ki.²⁵ A kiberhírszerzésnek két fő megjelenési formája különíthető el: a gazdasági hírszerzés és a politikai hírszerzés.

1. Gazdasági hírszerzés

A gazdasági kiberhírszerzés célja a célállam iparára, technológiájára vonatkozó információk megszerzése, majd ezeknek az információknak a felhasználása a végrehajtó állam által. Ilyen műveleteket már az 1990-es évek óta hajtanak végre államok.²⁶ Ezen műveletek célpontjai lehetne egyaránt államok és jelentős, kritikus állami vállalatok is. Az ilyen műveletek fő motivációja a másik állam által képviselt fölény megsemmisítése, valamint

²¹ Steven R Chabinsky, 'Cybersecurity Strategy: A Primer for Policy Makers and Those on the Front Line', 4(27) J Nat'l Security L & Pol'y 27 (2010), 31.

²² CFR, 'Regin.', <https://www.cfr.org/cyber-operations/regin>, (Letöltve: 2024.10.23.)

²³ 'Hungarian Official: Government Bought, Used Pegasus Spyware', AP News (2021. november 4.), <https://apnews.com/article/technology-europe-hungary-malware-spyware-ccacf6da9406d38f29f0472ba44800e0>, (Letöltve: 2024.10.23.).

²⁴ David Weissbrodt, 'Cyber-Conflict, Cyber-Crime, and Cyber-Espionage', 22 Minn J Intl L 347 (2013), 370-371.

²⁵ Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, CUP (2017) ['Kézikönyv'], 32. szabály (4).

²⁶ Jeffrey L Dunoff et al, 'International Law Norms, Actors, Process: A Problem-Oriented Approach', Aspen Publishing (2020), 119-120.

(akár több milliárd dolláros²⁷) kár okozása a célállam számára. A hírszerzés összes típusa közül a gazdasági hírszerzés a leginkább szabályozott a nemzetközi közösség által. Ez a szabályozás többnyire kétoldalú állami egyezményekben valósul meg. Erre kiváló példa az Egyesült Államok és Kína között 2015-ben kötött „Cyber Agreement”, amelyben az államok vállalták, hogy nem fogják a másik állam szellemi tulajdonát megsérteni kiberműveletekkel, azaz nem hajtják végre gazdasági kiberhírszerzést.²⁸

2. Politikai hírszerzés

A hírszerzési műveletek második típusa a végrehajtó állam által a célállam ellen végrehajtott olyan hírszerzés, melynek célja a célállam államtitkainak megszerzése, és ezáltal például politikai vagy katonai előny szerzése. Államtitoknak minősülhet ebben az értelemben például a hadsereg, fegyverekre vonatkozó adatok, államok szövetségeseivel kapcsolatos információ, valamint a köztük létrejött információcsere tartalma. A politikai hírszerzés nagyobb veszéllyel jár, mint a gazdasági hírszerzés, hiszen míg az utóbbi többnyire csak vagyoni hátrányt vagy versenyhátrányt okoz, addig az előbbi a célállamra nézve sokkal nagyobb és súlyosabb következményekkel járhat.

3. A hírszerzés elkülönítése a kémkedéstől és a megfigyeléstől

A hírszerzés fogalmának definiálásakor fontos elkülöníteni azt egyrészt a háborús helyzetben elkövetett kémkedéstől, másrészt pedig az államok által végzett megfigyeléstől. Az előbbit a humanitárius jog, azaz a Genfi egyezmények, pontosabban pedig a IV. Genfi Egyezmény,²⁹ valamint az Egyezmények I. Kiegészítő Jegyzőkönyve³⁰ szabályozza. Az I. Kiegészítő Jegyzőkönyv 46(1) szakasza szerint kémnek minősül az, aki a szembenálló fél által ellenőrzött területen információszerzést folytat, amennyiben ezt hamis látszat keltésével vagy szándékosan titkolt módon (tehát például nem egyenruhában) végzi. A kémkedést – a hírszerzéssel szemben – a nemzetközi jog részletesen szabályozza, és bár a kémkedés nem

²⁷ ‘The U.S.-China Cyber Agreement: A Good First Step’, *Rand Corporation*, (2016. augusztus 8.), <https://www.rand.org/pubs/commentary/2016/08/the-us-china-cyber-agreement-a-good-first-step.html>, (Letöltve: 2024.10.23.)

²⁸ Federation of American Scientists, ‘China-U.S. Trade Issues’, *Congressional Research Service* (2022. október 6.), 47.

²⁹ A polgári lakosság háború idején való védelmére vonatkozóan Genfben, 1949. augusztus 12-én kelt Egyezmény [„IV. Genfi egyezmény”].

³⁰ Az 1949. augusztus 12-én kötött Genfi Egyezményeket Kiegészítő és a Nemzetközi Fegyveres Összeütközések Áldozatainak Védelméről Szóló Jegyzőkönyv.

tilos, a kém nem jogosult kombattáns vagy hadifogoly státuszra, amennyiben elfogják.³¹ A különbség tehát több szempontból is megragadható: míg hírszerzést államok, vagy nem állami szereplők (de az államnak betudható módon) végzik, addig a kémkedést egyének végzik, így a felelősség is rájuk hárul. Emellett míg a hírszerzést békeidőben és háborúban is végre lehet hajtani, addig a kémkedés csak háborúban követhető el.

A megfigyelést az különíti el a hírszerzéstől, hogy annak alanyai a legtöbb esetben a végrehajtó állam, ritkább esetben egy másik állam állampolgárai. Az elkövető megfigyelés esetén egy állam, amely lehallgatásokkal, telekommunikációs szolgáltatók adatainak felhasználásával, valamint közösségi médián tárolt adatok megszerzésével az állampolgárok életét követi figyelemmel.³² A leghíresebb példa erre az Edward Snowden által leleplezett tömeges megfigyelés volt az Egyesült Államokban. A Snowden által kiszivároztatott dokumentumok bebizonyították, hogy a kormányzat több millió állampolgár telefonhívását hallgatta le³³ és e-mailjeinek tartalmát gyűjtötte.³⁴ De a számos másik példa között találhatóak olyan esetek is, hogy az egy államban összes számítógépet kötelező volt egy megfigyelést lehetővé tevő szoftverrel értékesíteni.³⁵ A megfigyelések célja a hírszerzéssel szemben nem az, hogy a végrehajtó állam a célállammal szemben valamilyen előnybe kerüljön, hanem általában az állampolgárok feletti kontrollt vagy a politikai ellenfelek elnyomását szolgálja. Jelen dolgozat az itt feltüntetett fogalmak közül az államok más államok ellen végzett hírszerzését tárgyalja, ezek közül is szűken véve, a politikai hírszerzést. A dolgozatnak nem tárgya a megfigyelésnek, a kémkedésnek és a gazdasági hírszerzésnek a kibertérrel és a nemzetközi joggal való viszonya.

4. A leggyakoribb hírszerzési gyakorlatok

Ahhoz, hogy pontosan értsük, hogy a kibertérben miként valósul meg a hírszerzés, és ennek milyen következményei vannak, szükséges pár szót szólni arról, hogy mik azok a gyakorlatok, amelyeket az államok alkalmaznak. Annak ellenére, hogy az államok által elkövetett kiberhírszerzés jelentősége és veszélye óriási, az államok által alkalmazott gyakorlatok nem sokban térnek el azoktól a módszerektől, amelyeket kiberbűnözők

³¹ IV. Genfi Egyezmény, 5. Cikk.

³² U.N.Doc A/HRC/27/37.

³³ 'U.S. Court: Mass Surveillance Program Exposed by Snowden Was Illegal', *Reuters* (2020. szeptember 3.), <https://reuters.com/article/world/us-court-mass-surveillance-program-exposed-by-snowden-was-illegal-idUSKBN25T3CJ/>, (Letöltve: 2024.10.23.)

³⁴ 'Edward Snowden and the NSA Surveillance Program', 31(3) *Bill of Rights in Action* 10 (2016), 11.

³⁵ U.N.Doc A/HRC/27/37.

használnak annak érdekében, hogy információt szerezzenek emberektől. A leggyakoribb módszerek között említhető a (i) kémiszoftverek és vírusok használata, (ii) az ún. „logic bomb” módszer, az (iii) IP spoofing, (iv) az APT-támadás, (v) az ellátási lánc elleni támadások és a (vi) adathalászat.

A leginkább magától értetődő módszer a kémiszoftverek használata. A kémiszoftverek célja lehet a billentyűleütések rögzítése, képernyőképek készítése vagy a számítógépen található más információ megszerzése egy a számítógépre valamilyen módon telepített szoftver segítségével.³⁶

A „logic bomb” a kémiszoftverek egyik altípusa. Ezek jellemzője, hogy úgy tervezik meg őket, hogy egy adott időpontig vagy egy bizonyos feltétel teljesüléséig észrevétlenül maradjanak, és csak ezután válság ki a hatásaikat.³⁷

Az „IP Spoofing” egy kifinomult kiberhírszerzési módszer, mely során a támadó hamisítja a forrás IP-címét, hogy megtévessze a célrendszert, és elrejtse a valódi helyét vagy személyazonosságát, így hozzáférést szerezzen egy hálózathoz vagy adatokat lopjon.³⁸

Az APT-k olyan elhúzódó és célzott kibertámadások, amelyek során az elkövető hozzáférést szerez egy hálózathoz, és hosszabb ideig észrevétlen marad, mely alatt végig hírszerzési tevékenységet folytat.³⁹

Az ellátási lánc elleni támadás egy olyan hírszerzési módszer, amely során az elkövető az célállam által igénybe vett partnereket célozza meg, hogy ezen keresztül férjenek hozzá a célállam rendszeréhez. A támadók gyakran olyan szoftverfrissítéseket vagy hardverelemeket fertőznek meg, amelyeket a célállam használ, így észrevétlenül telepíthetnek kémiszoftvereket.⁴⁰ Egy 2010 és 2020 között végzett kutatás szerint a világ összes ellátási lánc elleni támadásának negyedét államok hajtották végre.⁴¹

Végül a legegyszerűbb, mégis a leggyakrabban alkalmazott módszer, az adathalászat, mely az állami infrastruktúra emberi tényezőjét és ennek sérülékenységét használja ki. Adathalászat során az elkövető megtévessztő e-mailek vagy weboldalak segítségével ráveszi az embereket

³⁶ ‘What Is Cyber Espionage?’ (ThreatDown) <https://www.threatdown.com/glossary/what-is-cyber-espionage/>, [‘What Is Cyber Espionage?’], (Letöltve: 2024.10.24.)

³⁷ Dana Rubenstein, ‘Nation State Cyber Espionage and its Impacts’, https://www.cse.wustl.edu/~jain/cse571-14/ftp/cyber_espionage.pdf [‘RUBENSTEIN’], (Letöltve: 2024.10.23.)

³⁸ Uo.

³⁹ *What Is Cyber Espionage?*

⁴⁰ ‘Cyber Espionage: Examples, Types & Tactics’, *Dataconomy* (2022. november 4.) <https://dataconomy.com/2022/11/04/cyber-espionage-examples-types-tactics/>, [‘Cyber Espionage: Examples, Types & Tactics’], (Letöltve: 2024.10.23.)

⁴¹ UK Parliamentary Office of Science and Technology, ‘State’s Use of Cyber Operations’, *POSTnote 684* (2023), 2.

érzékeny információk, például bejelentkezési adatok felfedésére. Az elkövetők legtöbbször megbízható személyeknek, például kollégáknak vagy kormányzati tisztviselőknek adhatják ki magukat, hogy hozzáférjenek korlátozott adatokhoz.⁴²

⁴² *Cyber Espionage: Examples, Types & Tactics.*

III. A KIBERHÍRSZERZÉS BETUDÁSA

A kiberhírszerzés viszonylatában felmerülő számos probléma közül az első a hírszerzési műveletek nemzetközi jogi betudása. A betudás folyamatának célja egy művelet elismerése, mint valamely szereplő cselekménye. Más szóval, arra keresi a választ, hogy „ki tette?”.⁴³ Nemzetközi jogban a betudás célja, hogy a végrehajtott műveletet egy valamely államhoz társítsa.⁴⁴ A betudás, és a műveletek államokhoz való társítására azért van szükség, mert a nemzetközi jogban érvényben levő államfelelősségi szabályoknak előfeltétele, hogy egy cselekmény betudható legyen egy államnak.

A nemzetközi jog államfelelősségi rendszerét az ENSZ Nemzetközi Jogi Bizottságának [‘ILC’] Államfelelősség-tervezete [‘ARSIWA’] szabályozza, amely bár nem hivatalos jogforrás, a szokásjog jellegét több esetben is megerősítette a Nemzetközi Bíróság.⁴⁵

A kiberhírszerzési műveletek betudását több tényező is megnehezíti, melyek mindegyike a kibertérben való végrehajtásból eredeztethető. Az internet lehetővé teszi, hogy az államok akár a saját területükről végezzenek hírszerzési műveleteket, így az elkövetőnek a célállamban való jelenléte egyáltalán nem szükséges a műveletek végrehajtásához. Ez egyrészt lehetővé teszi az elkövető anonimitását (például proxy-k⁴⁶ vagy VPN használatával), másrészt sokszor maga a célállam sincs tudatában annak, hogy hírszerzési műveleteket folytatnak ellenük (ún. *Advanced Persistent Threat*). Ahhoz, hogy pontosan tudjuk, hogy ki követte el a kiberműveletet pontosan meg kell határozni az műveletet elkövető eszközt, vagy legalább annak a pontos helyét, az elkövető személyét, és az elkövető és az állam közötti viszonyt.⁴⁷ Fontos azonban megemlíteni, hogy gyakran a „technológiai betudás”, azaz annak megtalálása, hogy ki és hol követte el a műveletet még a könnyebbik lépése a betudás folyamatának. Hiszen, ha meg is találtuk, hogy ki és hol követte el a műveletet, meg kell állapítani az elkövető személy és az állam közötti viszonyt. Ezt megnehezíti, hogy az államok

⁴³ François Delerue, ‘Cyber Operations and International Law’, CUP (2022), 51.

⁴⁴ 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. [‘ARSIWA Kommentár’], 36. o., 12. bek.

⁴⁵ Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. USA), Merits, Judgment, I.C.J. Rep. (1986) 14. [‘Nicaragua ügy’], 115. bek.; 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. Rep. (2007) 43. [‘Népirtás ügy’] 393. bek., 398. bek.; United States Diplomatic and Consular Staff in Tehran (USA v. Iran), Judgment, I.C.J. Rep. (1980) 3. [‘Teheráni túsok ügye’], 74. bek.

⁴⁶ Delbert Tran, ‘The Law of Attribution: Rules for Attributing the Source of a Cyber-Attack’, Yale J L & Tech 387 (2018), 389.

⁴⁷ Csillik Kristóf - Hordós Alex, ‘Zárva tartani Pandora szelencéjét: az erőszakos kiberműveletek betudásának kérdései’, (3-4) Katonai és Hadijogi Szemle 6 (2023) [‘Csillik-Hordós’], 20-21.

nem saját nevükben, hanem gyakran nem állami szereplők háta mögé bújva követik azt el, így próbálva elkerülni a betudhatóságot.⁴⁸

Azt, hogy egy műveletet mi alapján lehet betudni egy államnak az ARSIWA II. fejezete tartalmazza. A fejezet összesen nyolc lehetséges esetet említ, melyek teljesülése esetén egy egyén által végzett művelet betudhatóvá válik egy államnak, azonban a gyakorlatban a kiberműveletekre általában a nyolc közül csak három alkalmazható. Ezek a 4., a 8. és a 11. cikkben található esetek, vagyis (i) a *de jure* és *de facto* állami szervek műveletei, (ii) az állam irányítása vagy ellenőrzése alatt végzett művelet és a (iii) az állam által saját cselekményként elismert művelet. Azért is fontos ezen cikkek vizsgálata, mert ezek teszik leginkább lehetővé a nem állami szereplők által elkövetett műveletek egy államhoz való hozzárendelését.

A. A *de jure* és *de facto* állami szervek.

Az ARSIWA 4. cikke szerint „[b]ármely állami szerv magatartása a nemzetközi jog szerint az adott állam cselekményének minősül, függetlenül attól, hogy a szerv törvényhozó, végrehajtó, bírói vagy bármilyen más funkciót tölt-e be, és függetlenül attól, hogy a központi kormány vagy az állam szerve valamely területi egységének szerve.” Szervnek minősül a cikk szerint minden olyan személy vagy szervezet, amely az állam belső joga szerint ilyen jogállással rendelkezik. Látható tehát, hogy ez a cikk azokat a cselekményeket teszi betudhatóvá, ahol nincs vagy kevés kétség van aziránt, hogy az valóban az állam cselekménye-e. Ilyenek lehetnek például az állam hivatalos titkosszolgálatai, minisztériumai vagy akár a hadsereg kiberhadtestei által elkövetett hírszerzési műveletek.⁴⁹

Az ARSIWA kommentárja alapján azonban látható, hogy szervnek minősül, és így cselekménye az államnak betudható a hivatalos definíción túl annak az entitásnak is, amely *de facto* szervként működik, de a belső jogban nincs akként definiálva.⁵⁰ Ezzel az ARSIWA azt kívánja elkerülni, hogy az államok elkerüljék a betudást csupán azáltal, hogy az elkövető entitást a belső jogukban nem definiálják szervként. A Nemzetközi Bíróság szerint egy entitás *de facto* szervnek akkor tekinthető, ha az teljes mértékben függ („*complete dependence*”) az államtól.⁵¹

⁴⁸ Uo. 22-23.

⁴⁹ The International Institute for Strategic Studies: *Cyber Capabilities and National Power: A Net Assessment*, IISS Research Papers (2021).

⁵⁰ ARSIWA Kommentár, 4. cikk (11).

⁵¹ *Népiirtás ügy*, 391-393. bek.

B. Az állam irányítása vagy ellenőrzése alatt végzett műveletek.

Az ARSIWA 8. cikke rögzíti, hogy „[e]gy személy vagy személyek csoportjának magatartása a nemzetközi jog szerint egy állam cselekményének minősül, ha a személy vagy személyek csoportja ténylegesen az adott állam utasítására cselekszik vagy az állam irányítása vagy ellenőrzése alatt áll a magatartás végrehajtása során.” Ez a cikk azokat az eseteket teszi betudhatóvá egy államnak, amikor egy állam nem állami szereplőket utasít a műveletek elvégzésére, vagy amikor a nem állami szereplők az állam irányítása vagy ellenőrzése alatt állnak. Ezekben az esetekben a nem állami szereplők az államok „segédeszközeiként” („*auxiliaries*”) viselkednek.⁵² Ahhoz, hogy egy cselekmény ezen cikk alapján betudható legyen egy államnak, a három eshetőség (utasítás, irányítás és ellenőrzés) közül legalább az egyiknek fent kell állnia.⁵³

A Nemzetközi Bíróság az ezen cikk alapján történő betudás részletszabályait és küszöbét 1984-ben, a Nicaragua ügyben fektette le. Eszerint ahhoz, hogy egy művelet betudható legyen az államnak, az állam és a nem állami szerv között effektív kontrollnak kell fennállnia. A Bíróság ezt olyan kapcsolatként definiálta, ahol a nem állami szerv által elkövetett cselekményeket az állam kontrollja nélkül nem lehetett volna megvalósítani, mivel azok végrehajtását az állam irányította vagy kényszerítette ki. A Bíróság szerint ugyanakkor egy nem állami szerv „finanszírozása, szervezése, kiképzése, felszerelése és ellátása, valamint a katonai célpontok kiválasztása és a teljes hadművelet megszervezése” együtt sem elég ahhoz, hogy az effektív kontrol bizonyított legyen.⁵⁴

C. Az állam által saját cselekményként elismert művelet.

Az ARSIWA 11. cikke szerint egy magatartás a nemzetközi jog szerint egy állam cselekményének minősül, „ha és amennyiben az állam a szóban forgó magatartást elismeri és sajátjaként elfogadja.” Ez a cikk azokat az eseteket teszi egy államnak betudhatóvá, ahol ugyan a cselekményt nem az állam követte el, és a cselekmény az előző cikkek alapján nem rendelhető hozzá az államhoz, az állam mégis vállalja érte a nemzetközi felelősséget, azáltal, hogy azt sajátjaként ismeri el. Az betudás feltétele az, hogy az elismerés világos és egyértelmű legyen.⁵⁵ A Nemzetközi Bíróság a Teheráni túsok ügyében foglalkozott az elismerés jogintézményével. Az ügyben a Bíróság kimondta, hogy azzal, hogy az iráni

⁵² ARSIWA Kommentár 8. cikk (2).

⁵³ Uo. 8. Cikk (7).

⁵⁴ Nicaragua ügy, 115. bek.

⁵⁵ ARSIWA 11. cikk (8).

külügyminiszter azt nyilatkozta, hogy Irán az diákok magatartását „támogatja és segíti” Irán elismerte az iráni diákok által elkövetett magatartást és azt sajátjaként fogadta el.⁵⁶

⁵⁶ *Teheráni túszok ügye*, 73. bek.

IV. KIBERHÍRSZERZÉS ELMÉLETBEN - A KIBERHÍRSZERZÉS SZABÁLYOZÁSA

A. Alkalmazandó-e a nemzetközi jog a kiberműveletekre?

A klasszikus nemzetközi jogi szabályok közel egyidősek a szuverén államokkal. A szabályt azonban egy korábbi kor problémáira és körülményeire tekintettel alkották meg. A 21. század és a technológiai fejlődés viszont új kihívásokat állít a nemzetközi jog elé. A kibertér mára része a nemzetközi kapcsolatoknak: az államok a kibertéren keresztül folytatnak kereskedelmet, nyújtanak szolgáltatásokat vagy működtetik az infrastruktúrájukat. Atomerőművek, komplett közlekedési rendszerek és egészségügyi szolgáltatások működnek a kibertéren keresztül. Ennek következményeképpen pedig mindennapossá váltak a kibertámadások, amelynek következtében egyre többször felmerült a kérdés, hogy ezekre a támadásokra érvényesek-e a nemzetközi jog szabályai.

A kibertámadások első megjelenése óta a nemzetközi jogi szabályok kiberműveletekre való alkalmazhatósága számos esetben megerősítésre került. A Bíróság a Nukleáris fegyverek tanácsadó véleményében leírta, hogy egy technológia újszerűsége nem akadályozza meg azt, hogy a nemzetközi jog klasszikus szabályai és elvei érvényesek legyenek rá.⁵⁷ Emellett a Tallinn Kézikönyv is kijelenti, – a NATO,⁵⁸ az ENSZ,⁵⁹ és az államok többségének véleménye alapján – hogy a létező nemzetközi jogi normák érvényesek és alkalmazandók a kiberműveletekre is. Ezt megerősítette továbbá a G20,⁶⁰ az Európai Unió,⁶¹ a Délkelet-ázsiai Nemzetek Szövetsége,⁶² és az Amerikai Államok Szervezete⁶³ is. Így már a kérdés már nem az, hogy alkalmazandóak-e a klasszikus nemzetközi szabályok a kibertérben végrehajtott műveletekre, hanem az, hogy hogyan is lehet azokat a modern kor problémáira alkalmazni.

A nemzetközi jog szerződéseai között nagyon korlátozott számban található olyan, melynek célja a kiberjog szabályozása. Ilyen szerződés például a Budapest Egyezmény a Számítástechnikai Bűnözésről⁶⁴ vagy az Afrikai Unió által megalkotott Egyezmény a

⁵⁷ *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, I.C.J. Rep. (2004) 226, 86. bek.

⁵⁸ NATO, *Warsaw Summit Communiqué*, Varsó (2016).

⁵⁹ U.N.Doc. A/68/98.

⁶⁰ *G20 Leaders' Communiqué*, Antalya (2015).

⁶¹ *EU Statement*, United Nations 1st Committee: Thematic Discussion on Other Disarmament Measures and International Security (2018).

⁶² *ASEAN-United States Leaders' Statement on Cybersecurity Cooperation*, Singapore (2018).

⁶³ O.A.S.Doc. AG/RES. 2959 (L-O/20) (2020).

⁶⁴ Az Európa Tanács Számítástechnikai Bűnözésről szóló Egyezménye (Convention on Cybercrime, Budapest, 23/11/2001, CETS No. 185.)

Kibervédelemről és a Személyes Adatok Védelméről.⁶⁵ Ezek azonban egy-egy speciális rezsím regionális szabályozását tisztázzák a kibertérben, és nem globális szinten ültetik át a nemzetközi jogot a kiberműveletekre.

A szerződések hiánya azt eredményezi, hogy a kiberműveletekre alkalmazandó nemzetközi jogot főleg a nemzetközi szokásjog, valamint az alapelvek jelentik. A „kiberszokásjog” pontos szabályai az elmúlt években egyre inkább kikristályosodtak. Ez köszönhető egyrészt annak, hogy az államok egyre nagyobb számban teszik közzé a hivatalos álláspontjaikat, másrészt pedig a kodifikációs munkák növekvő számának.

A kiberjogban alkalmazandó szokásjogot összegyűjtő munkák közül kiemelendők a NATO támogatásával készült Tallinn Kézikönyvek. A dokumentumot eredményező projekt 2009-ben indult és a Kézikönyv első verzióját 2013-ban, a második verzióját 2017-ben adták ki. A Kézikönyv második kiadását tizenkilence nemzetközi jogász szerkesztette, akik az állami gyakorlat alapos vizsgálata után százötvennégy, kommentárral ellátott szabályt állítottak fel a nemzetközi közösség számára. A Kézikönyv kiemeli, hogy nem egy hivatalos dokumentum, és nem tükrözi a NATO álláspontját, ugyanakkor azt is kijelenti, hogy a benne található szabályok a fennálló nemzetközi szokásjogot tükrözik és így kötelezőek az államok részére.⁶⁶

B. A kiberhírszerzés jogszerűsége

1. A kiberhírszerzés mint *sui generis* nemzetközi jogi jogsértés

A kibertérben alkalmazandó speciális nemzetközi jogi szabályok hiánya azt eredményezi, hogy amennyiben egy kibertérben végrehajtott művelet jogszerűségét kívánjuk megállapítani, a klasszikus nemzetközi jog szabályaiból kell kiindulnunk, valamint meg kell vizsgálnunk, a nemzetközi közösség gyakorlata nem írta-e azokat felül, és nem alakított-e ki speciális szokásjogi normákat. Ez egyaránt igaz a kibertérben végrehajtott hírszerzési műveletekre is.

A „klasszikus” hírszerzést a nemzetközi közösség jelentős többsége egyfajta szürke zónába sorolja, és nem tartja sem kifejezetten jogszerűtlennek, de nem is tartja a nemzetközi jog megsértésének.⁶⁷ Az álláspontot képviselő ez az Állandó Nemzetközi Bíróság *Lotus* ügyében hozott döntésével támasztják alá, melyben a Bíróság kimondta, hogy a nemzetközi jogban minden jogszerű, amely ellen nincs kifejezett tiltó szabály.⁶⁸ Az pedig többé-kevésbé

⁶⁵ *African Union Convention on Cyber Security and Personal Data Protection*, Equatorial Guinea, 27/06/2014.

⁶⁶ Tallinn Kézikönyv, 2. o.

⁶⁷ Nicolas Jupilat, 'From the Cuckoo's Egg to Global Surveillance: Cyber Espionage That Becomes Prohibited Intervention', 42 NCJ Int'l L 933 (2017) ['JUPILLAT'], 959.

⁶⁸ S.S. 'Lotus', France v Turkey, Judgment, Judgment No. 9, PCIJ Series A, No. 10, 45. bek.

elfogadott a nemzetközi közösség által, hogy nincs semmilyen szabály, amely önmagában a hírszerzést, mint műveletet megtiltáná.⁶⁹ Ugyan a legtöbb állam a saját belső jogában bünteti a kémkedést,⁷⁰ fontos hogy ez nem jelenti automatikusan azt, hogy az ilyen cselekmények nemzetközi jogilag is jogsértők volnának. Ennek oka az, hogy az államok belső jogukban nem magukra nézve állapítanak meg korlátozásokat, így az államokat, mint a nemzetközi jog alanyait ez a tiltás nem érinti. Ezt támasztja alá az is, hogy számos állam a belső jogában kifejezett engedélyt ad a titkosszolgálatok számára kiberhírszerzési műveletek végrehajtására,⁷¹ valamint az is, hogy az államok a másik államban elfogott kémeik felelősségre vonása vagy *persona non grata*-nak minősítése ellen nem tiltakoznak.⁷²

Egyes speciális rezsimekben találhatunk kifejezett tiltó szabályokat. Például az ENSZ Tengerjogi Egyezményének⁷³ 19. cikke kifejezetten tilt bármilyen „cselekményt, amelynek célja a parti állam védelmét vagy biztonságát sértő információgyűjtés.” Emellett ritkán az államok közzétettek olyan nyilatkozatot, amelyben a hírszerzés nemzetközi jogi tilalma mellett foglalnak állást.⁷⁴ Ezek azonban inkább kivételek, és az általánosan elfogadott álláspont továbbra is az, hogy a nemzetközi jog nem szabályozza kifejezetten a hírszerzést.⁷⁵

A Nemzetközi Bíróság eddig két esetben foglalkozott érintőlegesen a hírszerzés kérdésével. Az első ügy az 1980-as Teheráni tús ügy, melyben a Bíróság a hírszerzést a diplomácia viszonylatában vizsgálta. A Bíróság kimondta bár kimondta, hogy a hírszerzési műveletek végrehajtása – a belügyekbe való beavatkozáshoz hasonlóan – a diplomáciai jogkörökkel való visszaélésnek minősülhet, nem döntött arról, hogy a hírszerzés önmagában jogsértő-e.⁷⁶

A második ügy a Kelet-Timor ügy, melyben a Bíróság 2013-ban hozott döntést. Az ügy arra vonatkozott, hogy Ausztrália lefoglalt bizonyos dokumentumokat és adatokat, amelyek Kelet-Timor tulajdonát képezték, valamint Kelet-Timor és jogi tanácsadói közötti levelezést, amely az Ausztrália és Kelet-Timor között folyamatban lévő szerződéses választottbíróági eljárással volt kapcsolatos. Ugyan az ügy nem tartalmazott határokon átnyúló elemet, mivel Ausztrália a

⁶⁹ Tallinn Kézikönyv, 32. szabály (5).

⁷⁰ Katharina Ziolkowski, 'Peacetime Cyber Espionage - New Tendencies in Public International Law', in Katharina Ziolkowski (ed.), *Peacetime Regime for State Activities in Cyberspace*. International Law, International Relations and Diplomacy, NATO CCD COE Publication (2013), 431.

⁷¹ *Uo.* (5).

⁷² Quincy Wright, 'Espionage and the Doctrine of Non-Intervention' in Roland Stanger (ed.), 'Internal Affairs, in *Essays on Espionage and International Law*' (1962), 3.

⁷³ Az Egyesült Nemzetek Tengerjogi Egyezménye (UNCLOS), 1833 UNTS 397.

⁷⁴ Joseph Soraghan, 'Reconnaissance Satellites: Legal Characterization and Possible Utilization for Peacekeeping', 13 McGill LJ 458 (1967), 470-71.

⁷⁵ Craig Forcece, 'Spies Without Borders: International Law and Intelligence Collection', 5 J Nat'l Sec L & Pol'y 195 (2011), 202.

⁷⁶ *Teheráni túsok ügye*, 85. bek.

dokumentumokat egy a saját területén lévő ügyvédi irodában foglalta le, a tényállás mégis klasszikus hírszerzésként fogható fel, mivel Ausztrália titkos vagy bizalmas információkhoz jutott hozzá a másik fél engedélye nélkül.⁷⁷ A Bíróság ebben az ügyben nem tudott érdemben dönteni, mivel Kelet-Timor visszavonta a keresetét, azonban az ideiglenes intézkedésről szóló döntésében a Bíróság megerősítette Kelet-Timor bizalmassághoz és kommunikációhoz való jogát.⁷⁸ Látható tehát, hogy a Nemzetközi Bíróság az egyik ügyben sem foglalt egyértelműen állást a hírszerzési műveletek jogszerűségéről, amely megerősíti azt az álláspontot, hogy a klasszikus hírszerzést nem szabályozza a nemzetközi jog, így pedig *sui generis* nem jogsértő a hírszerzési műveletek végrehajtása.

Változtatott-e ezen a klasszikus állásponton a technológia térnyerése a hírszerzés területén? A Tallinn Kézikönyv 32. szabálya rögzíti, hogy „a kiberhírszerzést önmagában nem szabályozza a nemzetközi jog.”⁷⁹ A Kézikönyv szerint a szokásjog nem tiltja a kiberhírszerzést. Ugyan az államok egymás ellen a kibertérben elkövetett hírszerzési műveletei vitatottak, egyelőre a kellő mennyiségű állami gyakorlat hiánya megakadályozza egy új – a kibertérben elkövetett műveletekre vonatkozó – szokásjogi tiltó szabály kialakulását.

Az államok gyakorlata valóban fogíjásnak nevezhető a területet illetően. Elvértve találhatók olyan állásfoglalások, melyek szerint az „államok szövetségesei ellen végrehajtott hírszerzési műveletei nemzetközi jogsértések”,⁸⁰ vagy hogy a kiberhírszerzés többek között a célállam szuverenitását is sérti,⁸¹ valamint egyes államok a kiberhírszerzést nemkívánatos tevékenységként definiálták⁸² ezek valójában kivételek. Az államok többsége a Tallinn Kézikönyv álláspontját erősíti meg, mely szerint a szokásjog nem tiltja a hírszerzési műveletek végrehajtását a kibertérben. Ilyen tartalmú nyilatkozatot tett többek között Új-Zéland,⁸³ Kanada,⁸⁴ az Egyesült Államok,⁸⁵ Franciaország,⁸⁶ és az Egyesült Királyság.⁸⁷

⁷⁷ JUPILLAT, 961.

⁷⁸ Questions Relating to the Seizure and Detention of Certain Documents and Data (Timor-Leste v Australia), Judgment (2014) ICJ Rep 147., 22. bek.

⁷⁹ Tallinn Kézikönyv 32. szabály (1).

⁸⁰ Julian Borger, ‘Brazilian President: US Surveillance a “Breach of International Law”’, *The Guardian* (2013. szeptember 24.), www.theguardian.com/world/2013/sep/24/brazil-president-un-speech-nsa-surveillance, (Letöltve: 2024.10.25.)

⁸¹ U.N.Doc A/67/946, 2. bek.; ‘UNASUR’s draft statement on ‘Other Disarmament Measures and International Security’ (2016).

⁸² G20, ‘Antalya Leaders’ Summit Communiqué’ (2015)

⁸³ <https://dpmc.govt.nz/sites/default/files/2020-12/The%20Application%20of%20International%20Law%20to%20State%20Activity%20in%20Cyberspace.pdf> (Letöltve: 2024.10.25.)

⁸⁴ https://www.international.gc.ca/world-monde/issues_developpement-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng, (Letöltve: 2024.10.25.)

⁸⁵ Paul C. Ney, Jr., ‘DOD General Counsel Remarks at US Cyber Command Legal Conference’, (2020).

Fontos azonban megemlíteni, hogy az államok a kiberhírszerzés illegalitását csak önmagában utasítják el. A nemzetközi közösség többsége elfogadja azt, hogy a kiberhírszerzési műveletek az elkövetés módjától függően más nemzetközi jogi szabályokat sérthetnek.⁸⁸ Az államok ezzel összefüggésben legtöbbször a szuverenitást, a belügyekbe való beavatkozást, a diplomáciai jogot és – a megfigyeléssel összefüggésben – az emberi jogokat említik meg. A következő pontokban ezeket a szabályokat vizsgálom meg a kiberhírszerzési műveletek jogszerűségével összefüggésben.

2. Szuverenitás

Az államok szuverenitása a klasszikus definíció szerint az a jog, hogy az állam „a földgolyó egy részén [...] bármely más állam kizárásával gyakorolhassa az állami funkcióit.”⁸⁹ Bár a kibertér maga egy virtuális tér, amely fizikailag nincs jelen egy állam területén sem, a kibertér alkotó eszközök mindig vagy valamely állam területén vannak.⁹⁰ Emiatt nemzetközi közösség többsége⁹¹ szerint az államoknak a kibertérnek egy adott részére kiterjed a szuverenitásuk, a kibertér egészére azonban egyik államnak sem. Ezt az ENSZ kormányközi szakértőcsoportjának (UNGGE) 2015-ös jelentése is megerősítette.⁹²

A nemzetközi jog szerint az állam szuverenitása egyértelműen sérül, amennyiben egy állam fizikailag átlép a másik állam területére, az állam engedélye vagy más igazoló ok nélkül.⁹³ Így tehát a hírszerzés olyan formája, melyben az elkövető a célállam területén tartózkodik a művelet teljesítése során sérti a célállam szuverenitását. A kiberhírszerzési műveletek azonban pont ezt az akadályt ugorják meg, hiszen mára ezeket a műveleteket az állam nem szükségszerűen a célállam területén tartózkodva követi el. És ugyan egyes álláspontok szerint, mivel az állam szuverenitása kiterjed a kiberinfrastruktúrára is, így az abba való jogtalan

⁸⁶ Ministry of Defence of France, ‘International Law Applied to Operations in Cyberspace’, (2019).

⁸⁷ <https://www.chathamhouse.org/events/all/members-event/international-law-future-frontiers> (Letöltve: 2024.10.25.)

⁸⁸ Tallinn Kézikönyv 32. szabály (6), (10).

⁸⁹ Island of Palmas (Netherlands v. United States), 2 R.I.A.A. 829, 838 (Perm. Ct. Arb. 1928).

⁹⁰ Tallinn Kézikönyv, 1. szabály (5).

⁹¹ Ezt az álláspontot tükrözi a Tallinn Kézikönyv 2.0 és az ENSZ Kormányközi Szakértőcsoportjának 2013-as és 2015-ös jelentése is, emellett Kanada, Kína, Csehország, Észtország, Finnország, Franciaország, Németország, Olaszország, Japán, Hollandia, Új-Zéland, Norvégia, Szingapúr, Svédország, Svájc és az Amerikai Egyesült államok (ld.: <https://cyberlaw.ccdcoe.org/wiki/Sovereignty> (Letöltve: 2024.10.25.)).

⁹² U.N.Doc. A/670/174 (2015).

⁹³ U.N.Doc. S/RES/138 (1960).

behatolás analóg módon sérti az állam területi szuverenitását,⁹⁴ a nemzetközi közösség többsége szerint ez nem elegendő a szuverenitás megsértéséhez.

Mikor sérül tehát a szuverenitás a kibertérben? Az alkalmazandó szokásjog szerint egy kiberhírszerzési művelet két alapon tud jogsértő lenni. Az első alap a célállam területiális integritásával van összefüggésben. Ez alapján egy kiberhírszerzési művelet sérti a célállam szuverenitását, ha (i) az fizikai kárt okoz a célállam kiberinfrastruktúrájában, vagy (ii) ha az jelentősen csökkenti a célállam kiberinfrastruktúrájának funkcionalitását.⁹⁵

Az első esetre példaként lehet hozni egy olyan kémprogramot, amely az információ megszerzése után azt törli a célállam információs rendszereiről. Ezzel a módszerrel működött például a 2012-ben bevetett Shamoon vírus is.⁹⁶ A második esetre példaként felhozható az Olympic Destroyer nevű művelet, melyet 2018-ban a dél-koreai téli olimpia alatt vetettek be. A művelet elsőként a dél-koreai kiberinfrastruktúra elleni hírszerzési műveletnek indult,⁹⁷ és csak ezen funkció teljesítését követően lépett át a második fázisba, melynek keretében a művelet olyan rendszereket célzott meg, mint a hivatalos olimpiai weboldal, a jegyértékesítési rendszerek, valamint a Wi-Fi hálózatok. A támadás miatt ezek a szolgáltatások ideiglenesen leálltak, így a kiberinfrastruktúra funkcionalitása jelentősen sérült.⁹⁸

A második alap a célállam természeténél fogva állami funkcióival („*inherently governmental functions*”) van összefüggésben. Ezzel összefüggésben egy kiberhírszerzési művelet sérti a célállam szuverenitását, ha az kisajátítja vagy beleavatkozik a célállam természeténél fogva állami funkcióiba. Fontos, hogy ebben az esetben nem szükséges, hogy a művelet kárt okozzon, vagy csökkentse a kiberinfrastruktúra funkcionalitását, mivel maga a kisajátítás vagy a beavatkozás sérti a szuverenitást.⁹⁹ Egyes államok szerint az államok által tárolt bizalmas adatok kezelése természeténél fogva állami funkciónak minősülhet, így, ha egy

⁹⁴ Russel, Buchan, 'Cyber Espionage and International Law', Hart Publishing (2019) ['BUCHAN'], 54-55.; Pål Wrange, 'Intervention in National and Private Cyberspace and International Law' Jonas Ebbesson, Marie Jacobsson, Mark Klamberg, David Langlet and Pål Wrange (eds), *International Law and Changing Perceptions of Security: Liber Amicorum Said Mahmoudi*, Brill/Nijhoff, (2014), 322.

⁹⁵ Tallinn Kézikönyv 4. Szabály (11)-(12); 'Cyber Activities and International Law: Austrian Position Paper' (2024)

⁹⁶ [https://cyberlaw.ccdcoe.org/wiki/Shamoon_\(2012\)](https://cyberlaw.ccdcoe.org/wiki/Shamoon_(2012)) (Letöltve: 2024.10.25.)

⁹⁷ 'The Olympic False Flag: How infamous OlympicDestroyer malware was designed to confuse cybersecurity community', *Kaspersky* (2018. március 9.), https://www.kaspersky.com/about/press-releases/2018_the-olympic-false-flag (Letöltve: 2024.10.25.)

⁹⁸ Jim Finkle, 'Olympic Destroyer' malware targeted Pyeongchang Games: firms', *Reuters* (2018. február 12.), <https://www.reuters.com/article/us-olympics-2018-cyber/olympic-destroyer-malware-targeted-pyeongchang-games-firms-idINKBN1FW22O> (Letöltve: 2024.10.25.)

⁹⁹ Tallinn Kézikönyv 4. Szabály (15).

állam eltulajdonítja ezeket a bizalmas adatokat, vagy azokba beleavatkozik, a célállam szuverenitása sérül.¹⁰⁰

3. Belügyekbe való beavatkozás tilalma

A más állam belügyeibe való beavatkozás tilalma a nemzetközi szokásjog szerves része és annak egyik legfontosabb szabálya. A tilalom alapján minden szuverén államnak joga van az belügyeit külső befolyások nélkül folytatni. A tilalom először 1949-ben az Nemzetközi Jogi Bizottság az államok jogairól és kötelességeiről szóló nyilatkozat tervezetében jelent meg. A tilalmat később 1965-ben a 2131 (XX), 1970-ben pedig 2625 (XXV) számú ENSZ közgyűlési határozat is megerősítette. A határozatok szerint „semelyik államnak sem áll jogában közvetlenül vagy közvetetten, bármilyen okból kifolyólag beavatkozni más állam belügyeibe.” A belügyekbe való beavatkozás tilalmának pontos tartalmát és feltételeit a Bíróság 1986-ban az ún. Nicaragua döntésében definiálta. A Bíróság szerint a tilalom sérül, amennyiben az egyik állam kényszerítő jelleggel beavatkozik egy másik állam olyan ügyeibe, amelyekkel kapcsolatban az állam a szuverén egyenlőségéből fakadóan szabadon dönthet. A Bíróság tehát a tilalom két alkotóelemét azonosította: az állam szabad döntései és a beavatkozás kényszerítő jellege.

Az első elem, az állam szabad döntései könnyen azonosíthatóak. A Bíróság a döntésében kifejti, hogy „az államok szabad döntései magában foglalják az állam politikai, gazdasági, szociális és kulturális berendezkedését, valamint a külkapcsolatait is.”¹⁰¹ Az Állandó Nemzetközi Bíróság szerint az állam szabad döntései azok, melyeket nem a nemzetközi jog szabályoz.¹⁰²

A második elem, a beavatkozás kényszerítő jellege azonban nehezebben definiálható, mindezidáig az államok sem alakítottak ki egységes álláspontot a definíciót illetően. A kiberműveletekkel összefüggésben a jogtudósok kényszerítő jelleget többféleképpen is definiálták. Eszerint kényszerítő jellegű egy olyan művelet, amelynek „ellenállni ésszerűtlen” volna a célállam részéről,¹⁰³ vagy amelynek hatására a célállam megváltoztatja az akaratát.¹⁰⁴

¹⁰⁰ Inter-American Juridical Committee, ‘Improving Transparency: International Law and State Cyber Operations - Fifth Report (2020), 29–30.; Ministry of Foreign Affairs of Costa Rica, ‘Costa Rica’s Position on the Application of International Law in Cyberspace’, (2023), 22. bek.

¹⁰¹ *Nicaragua ügy.* 205. bek.

¹⁰² *Nationality Decrees Issued in Tunis and Morocco*, Advisory Opinion, P.C.I.J. Ser. B. No. 4, (1923), 24.

¹⁰³ Harriet Moynihan, ‘The Application of International Law to State Cyberattacks: Sovereignty and Non-Intervention’, Chatham House (2019), 29.; Maziar Jamnejad, Michael Wood, ‘The Principle of Non-intervention’, 22 LJIL 345 (2009), 348.; Thibault Moulin, ‘Reviving the Principle of Non-Intervention in Cyberspace: The Path Forward’, 25(3) Journal of Conflict & Security Law 423, (2020), 445.

A Bíróság döntése alapján azonban célszerű a kényszerítő jelleget inkább egy olyan mércének tekintni, ahol az vizsgálendő, hogy a végrehajtó állam célja-e a célállam szabad döntésének megváltoztatása és hogy a művelet alkalmas-e a cél elérésére.

Ahhoz tehát, hogy egy kiberhírszerzési művelet sértse a belügyekbe való beavatkozás tilalmát, a műveletnek kényszerítő módon kell befolyásolnia a célállam döntését azokban az ügyekben, melyben a célállam a szuverén egyenlőségéből eredően szabadon dönthet. A jogtudósok többsége szerint a kiberhírszerzési műveletek nem tudnak kényszerítőek lenni, mert nem alkalmasak arra, hogy a célállam szabad döntését hatékonyan befolyásolják,¹⁰⁵ annak ellenére, hogy az azonban elképzelhető, hogy a megszerzett információt később kényszerítő módon használják fel.¹⁰⁶ Ezzel szemben, egyes jogtudósok szerint azzal, hogy egy állam sikeres kiberhírszerzési műveleteket hajt végre egy állam ellen és ezzel a célállam bizalmas információit megszerzi, aláássa a célállam önálló döntéshozatali képességét, hiszen a célállam másképp fog dönteni annak tudatában, hogy a bizalmas információit a végrehajtó állam is ismeri. Emiatt pedig ezen álláspont szerint a kiberhírszerzési műveletek a döntéshozatali képességbe való beavatkozás és annak szabad voltától való megfosztása miatt ezen műveletek igenis sértik a belügyekbe való beavatkozás tilalmát.¹⁰⁷

4. Diplomáciai jog

Ha a kiberhírszerzési műveletek jogszerűségéről esik szó, elkerülhetetlen a diplomáciai jog oldaláról is megközelíteni a kérdést, hiszen kifejezetten gyakori, hogy az államok a külképviseleteiket használják a hírszerzési műveleteik végrehajtására.¹⁰⁸ Ezt jól példázza, hogy a mai napig az egyik vezető ok a diplomaták *persona non grata*-nak való nyilvánítására

¹⁰⁴ Barrie Sander, 'Democracy Under The Influence: Paradigms of State Responsibility for Cyber Influence Operations on Elections', 18(1) Chinese JIL 1 (2019), 44-45.; Jens David Ohlin, 'Did Russian Cyber Interference in the 2016 Election Violate International Law?', 95 Tex. Law Rev. 1579 (2017), 1592.; Tallinn Kézikönyv 66. Szabály (18).

¹⁰⁵ BUCHAN, 64.

¹⁰⁶ Ido Kilovaty, 'Doxfare: Politically Motivated Leaks and the Future of the Norm on Non-Intervention in the Era of Weaponized Information' 9 Harvard National Security Journal (2017), 146.

¹⁰⁷ Patrick C. R. Terry, "'Absolute Friends': United States Espionage against Germany and Public International Law' 28 Revue Québécoise de Droit International 173 (2015), 197.

¹⁰⁸ Bridie Jabour, 'Indonesia Summons Australian Envoy Over Embassy Spying Claims', The Guardian (2013. november 1.), www.theguardian.com/world/2013/nov/01/indonesia-summons-australian-ambassador-embassy-spying-claims, (Letöltve: 2024.10.25.) 'Embassy Espionage: The NSA's Secret Spy Hub in Berlin', Spiegel, (2013. október 27.), www.spiegel.de/international/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy-a-930205.html, (Letöltve: 2024.10.25.); PUN, 368.

a hírszerzési műveletek végrehajtásának vádjá.¹⁰⁹ De a kiberhírszerzés nem csak a külképviselletekről indulhat, hiszen maguk a külképviselletek is gyakran esnek áldozatul hírszerzési műveleteknek.¹¹⁰

A diplomáciai jog nemzetközi jogi szabályait az 1961-es Bécsi Szerződés¹¹¹ rendezi. A kiberhírszerzés szempontjából a Szerződés 24., 27. és 41. cikkei relevánsak.

A Szerződés 24. cikke szerint „[a] képviselő irattárai és dokumentumai mindenkor, és bárhol is vannak elhelyezve, sérthetetlenek.” Ugyan a Szerződés nem definiálja a cikkben említett meghatározásokat, a joggyakorlat alapján a dokumentumok magában foglalják az elektronikus file-okat is.¹¹² Hasonlóan, a Tallinn Kézikönyv szerint a sérthetatlenség kiterjed „a merevlemezre, pendrive-okra és egyéb olyan adathordozókra, amelyeken elektronikus dokumentumokat tárolnak”.¹¹³ A „bárhol is vannak elhelyezve” fordulat is arra utal, hogy a kibertérbe (pl. felhőkben) tárolt adatok is sérthetetlenek.¹¹⁴ A dokumentumok sérthetatlensége azt jelenti, hogy azok nem lehetnek tárgyai lefoglalásnak, és az eltulajdonításuk (pl. hírszerzési műveletek útján) sérti a diplomáciai jogot.¹¹⁵

A Szerződés 27. cikkének (1) bekezdése szerint „[a] fogadó állam megengedi és védelemben részesíti a képviselő szabad érintkezését minden hivatalos ügyben”. Ezen kötelezettség – annak ellenére, hogy az államok rendszeresen megsértik¹¹⁶ – magában foglalja, hogy a fogadó államnak tartózkodnia kell a képviselő érintkezéseinek lehallgatásától.¹¹⁷

A Szerződés ugyanezen cikkének (2) bekezdése rögzíti, hogy „[a] képviselő hivatalos levelezése sérthetetlen. Hivatalos levelezésen kell érteni a képviselőt és annak

¹⁰⁹ Eileen Denza, 'Diplomatic Law: Commentary on the Vienna Convention on Diplomatic Relations', Oxford Academic (2016) ['DENZA'], 65.

¹¹⁰ Ewen MacAskill and Julian Borger, 'New NSA Leaks Show How US is Bugging its European Allies', *The Guardian*, (2013. június 30), www.theguardian.com/world/2013/jun/30/nsa-leaks-us-bugging-european-allies, (Letöltve: 2024.10.25.); 'China demands U.S. explain spying allegations linked to Australian missions', *Reuters* (2013. október 31), <https://www.reuters.com/article/world/china-demands-u-s-explain-spying-allegations-linked-to-australian-missions-idUSBRE99U0LU/>, (Letöltve: 2024.10.25.); 'Et Tu, UK? Anger Grows over British Spying in Berlin', *Spiegel Online* (2013. november 5.), <https://www.spiegel.de/international/europe/revelation-of-spy-nest-in-british-berlin-embassy-angers-germans-a-931868.html>, (Letöltve: 2024.10.25.); 'MI5 Tried to Bug London Embassy, says Pakistan', *Kuwait News Agency* (2003. november 6.), <https://www.kuna.net.kw/ArticleDetails.aspx?id=1404317&language=en>, (Letöltve: 2024.10.25.).

¹¹¹ 1961-es Bécsi Szerződés a diplomáciai kapcsolatokról. (Vienna Convention on Diplomatic Relations, 500 UNTS 95.)

¹¹² R (on the application of Bancoult No 3) v Secretary of State for Foreign and Commonwealth Affairs, [2018] UKSC 3, 68. bek.

¹¹³ Tallinn Kézikönyv 41. Szabály (3).

¹¹⁴ BUCHAN, 84.

¹¹⁵ Tallinn Kézikönyv 41. szabály (1).

¹¹⁶ DENZA, 184-186.

¹¹⁷ Finn Seyersted, 'Diplomatic Freedom of Communication', 14 *Scandinavian Studies in Law* 193 (1970), 219.

tevékenységével kapcsolatos minden levelezést.” A technológia fejlődése miatt mára már egyértelmű, hogy a képviselet modern szoftvereken és szolgáltatásokon keresztül folytatott levelezése is sérthetetlennek minősül.¹¹⁸ A sérthetetlenség, a 24. cikkben foglaltakhoz hasonlóan a képviselet levelezését is védi a hírszerzési műveletektől.

Míg a 24. és a 27. cikkek a képviselet ellen irányuló kiberhírszerzési műveleteket teszi jogtalanná, addig a 41. cikk a képviselet vagy a diplomaták által elkövetett műveleteket szabályozza. A Szerződés 41. cikkének (1) és (3) szerint „kötelessége [...] minden személynek, hogy tiszteletben tartsa a fogadó állam törvényeit és más jogszabályait.” Ugyancsak kötelessége, hogy „tartózkodjék a fogadó állam belügyeibe való beavatkozástól. [...] A képviselet helyiségeit nem szabad olyan módon használni, amely összeférhetetlen a képviseletnek a jelen szerződésben, vagy a nemzetközi jog általános szabályaiban vagy a küldő és a fogadó állam között hatályban levő külön megállapodásokban meghatározott feladatkörével.” Így tehát, amennyiben egy állam a saját belső jogában bünteti a kémkedést, a diplomatának tartózkodnia kell az ilyen műveletek végrehajtásától.¹¹⁹ Az első bekezdés második fordulata tiltja a beavatkozást a diplomata részéről a fogadó állam belügyeibe. Fontos tisztázni, hogy a Szerződésben használt belügyekbe való beavatkozás („*interference*”) nem azonos a szokásjog alapján jogszerűtlen belügyekbe való beavatkozással („*intervention*”), mivel az előbbi egy tágabb fogalom.¹²⁰ Emiatt sokszor az olyan műveletek, melyek a szokásjog alapján nem számítanak belügyekbe való beavatkozásnak, sérthetik a Szerződés 41. cikkét. Tipikusan ilyen műveletek a kiberhírszerzési műveletek. Mint láttuk, az többségi álláspont szerint a kiberhírszerzési műveletek nem sértik a belügyekbe való beavatkozás tilalmát a szokásjog alapján. Mindazonáltal az államok által közzétett vélemények alapján a Szerződés 41. cikkébe ütközik és így nemzetközi jogot sért, ha egy diplomata a hivatalos minőségében kiberhírszerzési műveleteket hajt végre a fogadó állam ellen.¹²¹ A 41. cikk (3) bekezdése tiltja a képviselet helyiségeivel való visszaélést azzal, hogy előírja, hogy csak meghatározott feladatkörök gyakorlásához használható. És ugyan a Szerződés 3. cikke a képviselet feladatkörébe utalja a tájékozódást, ezt a képviselet csak a „megengedett módon” teheti. Ez magában foglalja azt, hogy a képviselet által végrehajtott

¹¹⁸ BUCHAN, 86.

¹¹⁹ Uo. 89.

¹²⁰ Uo. 91.

¹²¹ Expulsions of Soviets Worldwide, 1986. Washington, D.C’, U.S. Dept. of State (1987), 4; Philip Oltermann, Julian Borger and Nicholas Watt, ‘Germany Calls in UK Ambassador over Spy Claims’, *The Guardian* (2013. november 5.), www.theguardian.com/world/2013/nov/05/germany-summons-ukambassador-spy-claims-berlin. (Letöltve: 2024.10.25.); ‘Position Paper of the Republic of Austria: Cyber Activities and International Law’ (2024), 14.

tájékoztatás nem sértheti sem a fogadó állam belső jogát, sem pedig nemzetközi jogot.¹²² A Nemzetközi Bíróság a Teheráni tús ügyben egyértelműen kijelentette, hogy a hírszerzési műveletek végrehajtása a képviselő helyiségeivel való visszaélést valósít meg.¹²³

5. Összegzés – A kiberhírszerzés, mint egy nemzetközi jogi szűrkezőna

Az előző pontok alapján elmondható, hogy a kiberhírszerzés egyáltalán nem mondható a nemzetközi jog legszabályozottabb területének. A szabályozatlanság hiánya pedig egyfajta nemzetközi jogi szűrkezőnát hoz létre, melyben az államok sosem lehetnek biztosak, hogy mi tiltott és mi szabályos. De mi ennek az oka?

A jelenlegi helyzet oka véleményem szerint a kiberhírszerzés kettősségében keresendő: amilyen veszélyesek a kiberhírszerzési műveletek, annál hasznosabbak eszköznek minősülnek egy állam nemzetbiztonsági szolgálatai számára. A műveletek hasznossága pedig pont a veszélyességében keresendő. Ami az egyik állam számára hasznos, és sikeres, az a célállam számára veszélyes és káros. Az ez által okozott kettős mérce kiválóan illusztrálja a terület szűrkezőna-jellegét és szabályozatlanságát: az államok saját hírszerzési tevékenységeiket általában szükségesnek és jogosnak tekintik, miközben más államok hasonló műveleteit jogsértőnek és elfogadhatatlannak tartják. Ez az ambivalens hozzáállás a szuverenitás és a nemzetbiztonság közötti egyensúlyozásban gyökerezik. Az államoknak érdekük fűződik a kiberhírszerzés által nyújtott előnyök kihasználásához, ugyanakkor élesen elítélik, ha azok szuverenitását sértik. Ez pedig elvezet a szabályozatlanság gyökeréhez: az államok tisztában vannak azzal, hogy egy szigorú nemzetközi szabályozás jelentősen korlátozná saját mozgásterüket, miközben más szereplők esetében nem garantálná a szabályok betartását. Így egy esetleges tiltás se nem racionális, se nem reális lehetőség a nemzetközi közösség részéről. A jelenlegi szabályozási keretek szándékosan hagynak teret a kiberhírszerzés gyakorlásának, ugyanakkor meghúznak egy határt, amely csak a legsúlyosabb műveletek esetében teszi egyértelművé a jogsértést. Így a nemzetközi közösség egyfajta skálát hozott létre, melynek az egyik végpontjában az eltűrt, semmilyen más normát nem sértő kiberhírszerzés áll, a másik végpontjában pedig a nemzetközi jog alapköveit jelentő szabályokat is sértő kiberhírszerzési műveletek állnak, melyeket a nemzetközi jog már nem tűr meg. E pragmatikus megközelítés célja az, hogy az államok mozgásterét ne korlátozza indokolatlanul, miközben lehetővé teszi, hogy a nemzetközi jogot csak a legkirívóbb esetekben alkalmazzák szankcionálásra. Ez a

¹²² BUCHAN, 91.; 'Position Paper of the Republic of Austria: Cyber Activities and International Law', 14.

¹²³ *Teheráni túsok ügye*, 85. bek.

„puha szabályozás” fenntartja az államok közötti viszonylagos stabilitást, miközben nem akadályozza meg, hogy az államok saját érdekeiket kiberhírszerzés útján érvényesítsék.¹²⁴

¹²⁴ A pályamunka ezen pontjának elkészülését mesterséges intelligencia használata előzte meg.

V. KIBERHÍRSZERZÉS A GYAKORLATBAN – JOGON TÚLI ESZKÖZÖK A KIBERHÍRSZERZÉSI MŰVELETEK ELLENI HARCBA

Az előző pontokból nyilvánvalóvá vált, hogy amennyiben semmilyen más feltétel nem teljesül, egy kiberhírszerzési művelet önmagában nem sért nemzetközi jogot. Azzal azonban az államok többsége egyetért, hogy az ilyen műveletek végrehajtása nem egy barátságos cselekmény.¹²⁵ Ennek megfelelően az államok különböző válaszreakciókkal igyekeznek reagálni az ellenük végrehajtott kiberhírszerzési műveletekre és ezzel elrettenteni a műveleteket végrehajtó államokat. Az elrettentés célja, hogy növelje a támadások költségeit és kockázatait, így kevésbé vonzóvá téve a kémkedést. Emellett a védelem és az információmegosztás erősítésével jelzi, hogy a támadásokat észlelik és megfelelően kezelik. Az államok egyre gyakrabban tesznek közzé hivatalos stratégiákat arról, hogy pontosan milyen válaszlépéseket fognak tenni a végrehajtó állam ellen.¹²⁶ A dolgozat ezen pontja ezeket a válaszreakciókat vizsgálja meg.

A. A kiberinfrastruktúra fejlesztése

A kiberinfrastruktúra fejlesztése a legalapvetőbb megelőző intézkedés, amely kiemelten jelentős szerepet játszik a kiberhírszerzési műveletek megelőzésében és a rendszerek ellenálló képességének növelésében.¹²⁷ Ez azért is kifejezetten fontos, mert a Microsoft szerint az alapvető kiberinfrastruktúra korszerűsítése az ellenséges kibernműveletek 98%-át képes lenne megakadályozni.¹²⁸ A kiberinfrastruktúra fejlesztése során az államok és szervezetek korszerű védelmi rendszereket – mint például tűzfalakat, behatolásészlelő rendszereket¹²⁹, titkosítási módszereket és végpontvédelmi eszközöket¹³⁰ – építenek ki, amelyek képesek időben észlelni és blokkolni a támadásokat.

¹²⁵ Geoffrey B. Demarest, 'Espionage in International Law', 24 Denv. J. Int'l L. & Pol'y 321 (1996), 347.

¹²⁶ 'National Cyber Strategy of the United States of America' (2018); <https://www.enisa.europa.eu/topics/national-cyber-security-strategies> (Letöltve: 2024.10.25.)

¹²⁷ Lester Godefrey, 'Shape or Deter? Managing Cyber-Espionage Threats to National Security Interests', 66(1) Studies in Intelligence 1 (2022), 3., A pályamunka ezen pontjának elkészülését mesterséges intelligencia használata előzte meg.

¹²⁸ Microsoft, 'Microsoft Digital Defense Report' (2021), 124.

¹²⁹ A behatolásészlelő rendszer (IDS) egy olyan kiberbiztonsági eszköz, amely figyeli a hálózat vagy rendszerek forgalmát, észleli és riasztást küld a gyanús vagy káros tevékenységekről, amelyek potenciálisan kibertámadást vagy jogosulatlan hozzáférést jelezhetnek.

¹³⁰ A végpontvédelmi eszköz egy olyan kiberbiztonsági megoldás, amely a hálózat végpontjait – például számítógépeket, laptopokat, mobil eszközöket – védi a rosszindulatú támadások, adatszivárgás és egyéb kiberfenyegetések ellen, különböző biztonsági funkciók, például vírusirtás, tűzfalak és adatszivárgás-megelőzés alkalmazásával.

A fejlesztések egy része korlátozza a támadók mozgásterét egy sikeres támadás esetén, míg például a rendszerek és szoftverek rendszeres frissítése minimalizálja a sebezhetőségek kihasználását. A fejlesztések közé tartozik az alkalmazottak képzése is, hogy felismerjék a támadási kísérleteket, például az adathalász támadásokat, mivel gyakran a legnagyobb sérülékenységet az emberi hiba okozza.

A korszerű titkosítási módszerek alkalmazása biztosítja, hogy az esetlegesen megszerzett adatok ne legyenek hasznosak a támadók számára. Emellett a proaktív fenyegetésfelderítési rendszerek, amelyek gyakran mesterséges intelligencián alapulnak, képesek azonosítani a gyanús tevékenységeket és megakadályozni a támadások kibontakozását.

A kiberinfrastruktúra fejlesztésébe gyakran beletartozik ezen kívül úgynevezett csapdák („honeypot”) beépítése az információs rendszerekbe. A csapdák látszólag értékes adatokból állnak, miközben a valóságban semmilyen hírszerzési értékkel nem rendelkeznek. A csapdákat az államok különböző célokra is fel tudják használni: egyes esetekben az államok elhárításként használják a csapdákat, hogy megfigyeljék, hogyan végzi egy másik állam a műveleteit az információs rendszeren belül. Ez értékes információkkal szolgál az adott állam viselkedési mintáiról és kiberképességeiről. Máskor az állam olyan fájlokat tárol a csapdában, amelyek önálló hírszerzési szoftverként működnek, és ezáltal információkkal szolgálnak a végrehajtó államról a fájlok megszerzését követően.¹³¹

A kiberinfrastruktúra fejlesztését, mint megelőző lépést a legjobban Észtország tevékenysége illusztrálja. Észtország 2007-ben súlyos kibertámadás-sorozatot élt át, amelyet az ország kritikus infrastruktúrái ellen követtek el. Ezek a támadások ösztönözték Észtországot, hogy növelje kiberbiztonsági kapacitásait, és azóta az ország a világ egyik vezető államává vált ezen a területen.¹³²

A kiberinfrastruktúra fejlesztésével kapcsolatban fontos továbbá megemlíteni az EU 2016/1148 irányelvét,¹³³ amely az első olyan uniós szintű szabályozás, amely kötelező kibervédelmi követelményeket ír elő a kritikus szolgáltatást nyújtó szektorra, többek között az közigazgatási szektorra is. Az irányelv célja, hogy növelje a hálózatok és információs rendszerek biztonságát az EU minden tagállamában.¹³⁴

¹³¹ Tallinn Kézikönyv 32. Szabály (15).

¹³² Josh Gold, ‘How Estonia uses Cybersecurity to Strengthen its Position in NATO’ (2019), <https://icds.ee/en/how-estonia-uses-cybersecurity-to-strengthen-its-position-in-nato/> (Letöltve: 2024.10.25.).

¹³³ A Európai Parlament és a Tanács 2022. december 14-i (EU) 2022/2555 Irányelve az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályaon kívül helyezéséről (NIS 2 irányelv).

¹³⁴ <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:4637829> (Letöltve: 2024.10.27.)

B. Nemzetközi normák kialakítása

A legcélszerűbb, azonban a legkevésbé követett megelőző intézkedés a bilaterális és multilaterális egyezmények létrehozása. Az ilyen és ehhez hasonló nemzetközi normák létrehozása segíthet a nemzetközi közösségnek abban, hogy felelősségre vonják azokat, akik nem „elfogadható” magatartást tanúsítanak, és iránymutatást adhatnak az arányos és megfelelő válaszlépésekhez.¹³⁵ Ugyan a nemzetközi jogi szabályok alkalmazandóak a kiberhírszerzési műveletekre, egyelőre nincs egy átfogó, *lex specialis* rezsim, mely csak a kiberhírszerzést szabályozná. Egyes államok – mint például az Egyesült Államok és Kína – aláírtak bilaterális egyezményeket,¹³⁶ ez a gyakorlat közel sem elterjedt, és nem is várható ezen a téren előrelépés. Ennek oka, egyrészt a klasszikus hírszerzés szabályozatlanságában rejlik, azaz abban, hogy a nemzetközi közösség a nem elektronikus eszközökkel végrehajtott hírszerzési műveleteket sem szabályozza, így nem várható, hogy máshogy tenne a kibertérben elkövetett műveletekkel összefüggésben. Másrészt pedig az államok többsége maga is végrehajt kiberhírszerzési műveleteket, így tulajdonképpen nem céljuk a terület szabályozása vagy akár kriminalizálása.

C. Diplomácia és gazdasági szankciók

A leggyakrabban alkalmazott válaszlépés az államok részéről a diplomáciai csatornák használata a kiberhírszerzési műveletek elítélésére és rosszallásuk kifejezésére. Ez magában foglalhat hivatalos tiltakozást, nyilatkozatok kiadását vagy a vádlott államok nagyköveteinek behívását.¹³⁷ Ha a kiberhírszerzési műveleteket a Bécsi Egyezmény sérelmével követték el, akkor gyakori a diplomata *persona non grata*-nak minősítése. Emellett az országok gazdasági szankciókat is gyakran ki az érintettnek vélt államok ellen. Például az Egyesült Államok és egyes európai államok a SolarWinds kiberhírszerzési műveletre¹³⁸ adott válaszként orosz

¹³⁵ UK Parliamentary Office of Science and Technology, ‘State’s Use of Cyber Operations’, *POSTnote* 684 (2023), 3.

¹³⁶ Congressional Research Service, ‘U.S.-China Cyber Agreement’ (2015) <https://china.usc.edu/congressional-research-service-us-china-cyber-agreement-oct-16-2015>, (Letöltve: 2024.10.25.); Minister of Foreign Affairs of Australia, ‘Key outcomes from inaugural High-Level Security Dialogue with China’ (2017), <https://www.foreignminister.gov.au/minister/julie-bishop/media-release/key-outcomes-inaugural-high-level-security-dialogue-china> (Letöltve: 2024.10.25.)

¹³⁷ ‘Cyber espionage and international law’, <https://www.cyber-espionage.ch/Law.html> (Letöltve: 2024.10.25.)

¹³⁸ A SolarWinds művelet egy nagyszabású kibertámadás volt 2020-ban, amely során hackerek, feltételezhetően orosz állami támogatással, egy SolarWinds nevű IT-cég szoftverének frissítését megfertőzve több ezer szervezet,

diplomatakat utasítottak ki,¹³⁹ emellett korlátozták a pénzügyi tranzakciókat, és utazási tilalmat rendeltek el a műveletben részt vevő szervezetekkel szemben. Ezen túl az Egyesült Államok megtiltotta az amerikai pénzügyi intézmények számára, hogy orosz államkötvényeket vásároljanak.¹⁴⁰

D. Nemzetközi védelmi és biztonsági szövetségek

Egy lehetséges válaszlépés a kiberhírszerzési műveletek ellen a nemzetközi védelmi és biztonsági szövetségekbe való belépés. Erre a legkiválóbb példa a NATO, amely az egyik alapvető feladatának tartja a kibertérben végrehajtott műveletek elleni védekezést.¹⁴¹ NATO célja a kibernműveletekkel kapcsolatban megelőzés, védelem, válságkezelés és biztonsági együttműködés erősítése. A NATO elismeri a kibertér operatív jelentőségét, és segíti tagállamait a nemzeti kiberbiztonság fejlesztésében, az információmegosztásban, képzésben és kollektív reagálásban.¹⁴² A NATO már 2016-ban a Varsói csúcson elismerte a kibertér, mint működési terület jelentőségét,¹⁴³ és azóta 2023-ban Vilniusban,¹⁴⁴ majd 2024-ben Washingtonban is megerősítette,¹⁴⁵ hogy figyelmet fordít a tagállamok kiberrezilienciájának fejlesztésére. Ennek keretében létrehozta a Kooperatív Kibervédelmi Kiválósági Központját (CCDCOE), mely kiemelt szerepet játszott a Tallinn Kézikönyv létrejöttében. Emellett a NATO rendszeresen tart kibervédelmi gyakorlatokat, amely során a tagállamok közösen tesztelik a koordinációs készségeiket a kibertérben.¹⁴⁶ Ezek a gyakorlatok lehetővé teszik az államok számára, hogy felkészüljenek a kiberhírszerzési műveletek kivédésére és összehangolják válaszlépéseiket, ha egy NATO-tagállamot kibertámadás érne.

Hasonló nemzetközi szövetség a Five Eyes nevű szervezet, mely a „legjobb védekezés a támadás” elvét követi. A Five Eyes egy hírszerzési együttműködés az Egyesült Államok, Kanada, Egyesült Királyság, Ausztrália és Új-Zéland között. Az 1940-es években indult

köztük amerikai kormányzati intézmények és vállalatok rendszereihez fértek hozzá, érzékeny információkat ellopva és kémkedési tevékenységet folytatva.

¹³⁹ ‘US Expels Russian Diplomats and Issues Sanctions over SolarWinds Hacking Attack’ *Deutsche Welle* (2021. április 15.), <https://www.dw.com/en/us-expels-russian-diplomats-and-issues-sanctions-over-solarwinds-hacking-attack/a-57215141>, (Letöltve: 2024.10.25.)

¹⁴⁰ ‘US Sanctions Russia over SolarWinds Cyber Attack’, *Australian Computer Society* (2021. április 16.), <https://ia.acs.org.au/article/2021/us-sanctions-russia-over-solarwinds-cyber-attack.html>, (Letöltve: 2024.10.25.)

¹⁴¹ https://www.nato.int/cps/en/natohq/topics_78170.htm (Letöltve: 2024.10.25.)

¹⁴² *Uo.*

¹⁴³ NATO, *Warsaw Summit Communique*, Varsó (2016).

¹⁴⁴ https://www.nato.int/cps/en/natohq/official_texts_217320.htm (Letöltve: 2024.10.25.)

¹⁴⁵ https://www.nato.int/cps/en/natohq/news_227647.htm (Letöltve: 2024.10.25.)

¹⁴⁶ <https://www.act.nato.int/activities/cyber-coalition/> (Letöltve: 2024.10.25.)

együttműködés célja a globális hírszerzési adatok megosztása. A szövetség kiemelt figyelmet fordít a kiberbiztonságra, lehetővé téve az öt ország számára, hogy gyorsan megosszák a kiberfenyegetésekkel kapcsolatos információkat, koordinálják válaszaikat, és közös stratégiákat dolgozzanak ki a kiberhírszerzési műveletek, például az állami kémkedés elleni fellépéshez.¹⁴⁷

Végül az Európai Unión belül is számos szerv foglalkozik a tagállamokat ért kiberfenyegetések, köztük kiberhírszerzési műveletek elleni fellépéssel. Példaként említhető az Europol és az Európai Kiberbűnözés Elleni Központja,¹⁴⁸ az ENISA,¹⁴⁹ vagy a CERT-EU.¹⁵⁰

E. Támadás, mint válaszreakció

Végül a legkevésbé visszafogott válaszlépés az államok részéről maga a támadás. Az Egyesült Államok ezt „előre védekezésnek” („*defending forward*”) nevezi és integráns része a kiberstratégiájának.¹⁵¹ A támadás, mint válaszreakció lényege egyrészt ez elrettentés, vagyis erődemonstráció, másrészt pedig a kiberhírszerzési műveletek megzavarása vagy semlegesítése még azelőtt, hogy az elérné a célpontot.¹⁵² Például 2007-ben Észtország az öt ért kibertámadást követően felfüggesztett egyes szolgáltatásokat az orosz IP címmel rendelkező számítógépek számára.¹⁵³ A fejlettebb államok többsége mára rendelkezik a hadseregen belül dedikált kiberhadtesttel.¹⁵⁴ Kína már például 2003-ban,¹⁵⁵ megalapította az első ehhez hasonló hadtestet. Hasonló módon az Egyesült Államok,¹⁵⁶ Izrael,¹⁵⁷ Szíria,¹⁵⁸ és

¹⁴⁷ Josh Gold, ‘Five Eyes and Offensive Cyber Capabilities: Building a Coalition for Cyber Operations’, *NATO Cooperative Cyber Defence Centre of Excellence* (2020), 6.

¹⁴⁸ <https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3> (Letöltve: 2024.10.25.)

¹⁴⁹ <https://www.enisa.europa.eu/about-enisa> (Letöltve: 2024.10.25.)

¹⁵⁰ <https://cert.europa.eu/> (Letöltve: 2024.10.25.)

¹⁵¹ ‘2023 DoD Cyber Strategy’ (2023)

¹⁵² U.S. Cyber Command PAO, ‘CYBER 101 - Defend Forward and Persistent Engagement’ (2022).

¹⁵³ RUBENSTEIN, 7.

¹⁵⁴ The International Institute for Strategic Studies: *Cyber Capabilities and National Power: A Net Assessment*, IISS Research Papers, 2021.

¹⁵⁵ John Tkacik, ‘Trojan Dragon: China’s Cyber Threat’, The Heritage Foundation (2008).

¹⁵⁶ Mark Pomerleau, ‘Army assumes support agent role for US Cyber Command’, *Defensescoop*, (2024. június 17.), <https://defensescoop.com/2024/06/17/army-assumes-support-agent-role-cyber-command/> (Letöltve: 2024.10.25.)

¹⁵⁷ Calev Ben-David, ‘Israel to Establish Command Center for Cyber Threat Defense’, *Bloomberg*, (2011. május 18.), <https://www.bloomberg.com/news/articles/2011-05-18/israel-to-establish-command-center-for-cyber-threat-defense-1-?embedded-checkout=true> (Letöltve: 2024.10.25.)

¹⁵⁸ Helmi Noman, ‘The Emergence of Open and Organized Pro-Government Cyber Attacks in the Middle East: The Case of the Syrian Electronic Army’, *OpenNet Initiative* (2011. május 5.), <https://opennet.net/emergence->

India¹⁵⁹ is fejlesztette a kiberműveleteket végrehajtó egységeit. Az egyik legnagyobb ilyen egységgel Oroszország rendelkezik, aki már 2008-ban évente 127 millió dollárt költött a területre és a kiberhadegysége több, mint 7300 fős volt.¹⁶⁰ Európa többi országa sincs hátrányban. Az Egyesült Királyság,¹⁶¹ Franciaország,¹⁶² Németország¹⁶³ és Svájc¹⁶⁴ is versenyképes kiberegységekkel rendelkezik.

[open-and-organized-pro-government-cyber-attacks-middle-east-case-syrian-electronic-army](#), (Letöltve: 2024.10.25.)

¹⁵⁹ Harish Gupta, 'As Cyber Attacks Rise, India Sets Up Central Command to Fight Back', *DNA* (2011. május 15.), <https://www.dnaindia.com/india/report-as-cyber-attacks-rise-india-sets-up-central-command-to-fight-back-1543352>, (Letöltve: 2024.10.25.)

¹⁶⁰ Luke Pelican, 'Peacetime Cyber-Espionage: A Dangerous but Necessary Game' 20 *CommLaw Conspectus* 363 (2012), 380.

¹⁶¹ Alex Michael, 'Cyber Probing: The Politicisation Of Virtual Attack', *Defense Academy Of The United Kingdom* (2010), 20.

¹⁶² Peter Sayer, 'France Creates New National IT Security Agency', *Networkworld*, (2009. július 9.), <https://www.networkworld.com/article/784528/security-france-creates-new-national-it-security-agency.html>, (Letöltve: 2024.10.25.)

¹⁶³ Sebastian Fischer and Ole Reissmann, 'Germany Arms Itself for Cyber War', *Spiegel Online*, (2011. június 16.), <https://www.spiegel.de/international/germany/fighting-internet-threats-germany-arms-itself-for-cyber-war-a-768764.html>, (Letöltve: 2024.10.25.)

¹⁶⁴ Myriam Dunn Cavelty, *Cyberwar: Concept, Status Quo, and Limitations*, Center For Security Studies (CSS) (2010), 3.

VI. KONKLÚZIÓ

A kibertér és a kiberműveletek a mára az életünk minden területét átszövik, és maguk az államok eszközeiként is általánossá váltak; elmondható, hogy elérkeztünk a kiberkorba. A technológia, exponenciálisan fejlődik és a kiberműveletek egyre több lehetőséget rejtenek magukban. De ezzel egyre nagyobb veszélyt is jelentenek. Ahogy az ENSZ kormányközi szakértőcsoportjának jelentése is írja, a kiberműveletek kétélű fegyverek: csupán akkor veszélyesek, ha rossz kezekbe kerülnek.¹⁶⁵

A kiberhírszerzés a kiberműveleteken belül is korunk egyik legnagyobb kihívása, hiszen bár mindenki alkalmazza, a legtöbb állam még nem tudja teljesen értelmezni a technológia adta lehetőségeket és veszélyeket, és nem tudják pontosan érzékelni egy-egy kiberhírszerzési művelet súlyosságát és jelentőségét. Ez az államok szuverenitásának és biztonságának újradefiniálására készíti a nemzetközi közösséget. Miközben az államok egyre inkább szembesülnek a kiberfenyegetések hatásaival, a meglévő jogi keretek és normák nem nyújtanak egyértelmű iránymutatást ezen támadások kezelésére és a felelősség megállapítására. Jelenleg egyfajta nemzetközi szürkezőnában vagyunk.

A dolgozat ezt a szürkezőnát mutatta be. Bemutatta a kiberhírszerzési műveletek betudásának nehézségeit, és a terület szabályozatlanságát. Emellett azonban azt is bemutatta, hogy az államok a világos nemzetközi jogi normák hiányában milyen válaszlépéseket és megelőző intézkedéseket tesznek annak érdekében, hogy a kiberhírszerzési műveletek okozta fenyegetéseket csökkentsék. A dolgozatom célja az volt, hogy egy átfogó elemzést nyújtson egyrészt a nemzetközi jog jelenlegi helyzetéről, másrészt azonban az, hogy bemutassa a realitást és azt, hogy az államok a kiberhírszerzés esetén valójában nem a nemzetközi jogra, hanem más – jogon túli – eszközökre támaszkodnak.

Az államok reakciói azonban — a diplomáciai eszközöktől és szankcióktól kezdve a kibervédelmi intézkedések és nemzetközi együttműködés erősítéséig — azt mutatják, hogy a kiberhírszerzés elleni fellépés kollektív fellépést és átfogó nemzetközi jogi szabályozást igényel. Az egyértelmű és hatékony normák kialakítása nemcsak az államok közötti bizalmat erősítheti, hanem hozzájárulhat a kibertér biztonságosabbá tételéhez, ahol a nemzetközi jog és az államok együttműködése képes lépést tartani a technológia rohamos fejlődésével és az új típusú fenyegetésekkel. Ez azonban kifejezetten nehéz, hiszen egyik állam sem kívánja feláldozni a saját kiberhírszerzési műveleteinek jogszerűségét. Emiatt nem is várható a közeli

¹⁶⁵ U.N. Doc. A/68/98., A pályamunka ezen pontjának elkészülését mesterséges intelligencia használata előzte meg.

vagy távoli jövőben olyan átfogó szabályozás, amely pontot tenne a kiberhírszerzéssel kapcsolatos nemzetközi szűrkezőna végére.

VII. FORRÁSJEGYZÉK

Nemzetközi Szerződések

A polgári lakosság háború idején való védelmére vonatkozóan Genfben, 1949. augusztus 12-én kelt Egyezmény.
<i>African Union Convention on Cyber Security and Personal Data Protection</i> , Equatorial Guinea, 27/06/2014.
Az 1949. augusztus 12-én kötött Genfi Egyezményeket Kiegészítő és a Nemzetközi Fegyveres Összeütközések Áldozatainak Védelméről Szóló Jegyzőkönyv.
Az Egyesült Nemzetek Tengerjogi Egyezménye (UNCLOS), 1833 UNTS 397.
Az Európai Parlament és a Tanács 2022. december 14-i (EU) 2022/2555 Irányelve az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv).
Az Európa Tanács Számítástechnikai Bűnözésről szóló Egyezménye (Convention on Cybercrime, Budapest, 23/11/2001, CETS No. 185.)
1961-es Bécsi Szerződés a diplomáciai kapcsolatokról. (Vienna Convention on Diplomatic Relations, 500 UNTS 95.)

Nemzetközi bírósági fórumok ítéletei

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. Rep. (2007) 43.
Island of Palmas (Netherlands v. United States), 2 R.I.A.A. 829, 838 (Perm. Ct. Arb. 1928).
<i>Legality of the Threat or Use of Nuclear Weapons</i> , Advisory Opinion, I.C.J. Rep. (2004) 226.
Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. USA), Merits, Judgment. I.C.J. Rep. (1986) 14.
<i>Nationality Decrees Issued in Tunis and Morocco</i> , Advisory Opinion, P.C.I.J. Ser. B. No. 4, (1923).
Questions Relating to the Seizure and Detention of Certain Documents and Data (Timor-Leste v Australia), Judgment (2014) ICJ Rep 147.
S.S. 'Lotus', France v Turkey, Judgment, Judgment No. 9, PCIJ Series A, No. 10.
United States Diplomatic and Consular Staff in Tehran (USA v. Iran), Judgment, I.C.J. Rep. (1980) 3.

Belső jogi dokumentumok, nemzeti állásfoglalások

'2023 DoD Cyber Strategy' (2023).

Chelsea Manning, Plaintiff, v. U.S. Department of Justice, et al, 234 F. Supp. 3d 26 (D.D.C. 2017).
'Expulsions of Soviets Worldwide, 1986. Washington, D.C', U.S. Dept. of State (1987).
https://dpmc.govt.nz/sites/default/files/2020-12/The%20Application%20of%20International%20Law%20to%20State%20Activity%20in%20Cyber space.pdf (Letöltve: 2024.10.25.)
https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng , (Letöltve: 2024.10.25.)
John Tkacik, 'Trojan Dragon: China's Cyber Threat', The Heritage Foundation (2008).
Minister of Foreign Affairs of Australia, 'Key outcomes from inaugural High-Level Security Dialogue with China' (2017), https://www.foreignminister.gov.au/minister/julie-bishop/media-release/key-outcomes-inaugural-high-level-security-dialogue-china (Letöltve: 2024.10.25.).
Ministry of Defence of France, 'International Law Applied to Operations in Cyberspace', (2019).
Ministry of Foreign Affairs of Costa Rica, 'Costa Rica's Position on the Application of International Law in Cyberspace', (2023).
'National Cyber Strategy of the United States of America' (2018).
Paul C. Ney, Jr., 'DOD General Counsel Remarks at US Cyber Command Legal Conference', (2020).
'Position Paper of the Republic of Austria: Cyber Activities and International Law' (2024).
R (on the application of Bancoult No 3) v Secretary of State for Foreign and Commonwealth Affairs, [2018] UKSC 3.
The White House, <i>The National Strategy to Secure Cyberspace</i> (2003).
U.S. Cyber Command PAO, 'CYBER 101 - Defend Forward and Persistent Engagement' (2022).
U.S. Department of Defense, 'Dictionary of Military and Associated Terms', (2021).
U.S. Department of Defense, <i>Joint Publication 3.10.1</i> (2014).
UK Parliamentary Office of Science and Technology, 'State's Use of Cyber Operations', POSTnote 684 (2023).
United States of America, v. Joshua Adam, 436 F. Supp. 3d 698 (S.D.N.Y. 2020).

Értekezések és kommentárok

Eileen Denza, 'Diplomatic Law: Commentary on the Vienna Convention on Diplomatic Relations', Oxford Academic (2016).
François Delerue, 'Cyber Operations and International Law', CUP (2022), 51.
Jeffrey L Dunoff et al, 'International Law Norms, Actors, Process: A Problem-Oriented Approach' 5th edn, Aspen Publishing (2020).
Marco Roscini, <i>International Law and the Principle of Non-intervention</i> , OUP (2024).

Michael N Schmitt (ed), <i>Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations</i> CUP (2017).

Monográfiák, esszék, cikkek

Adam Liff, 'Cyberwar: A New "Absolute Weapon"? The Proliferation of Cyberwarfare Capabilities and Interstate War', 35(3) J Strateg Stud 401 (2012).
Alex Michael, 'Cyber Probing: The Politicisation Of Virtual Attack', Defense Academy Of The United Kingdom (2010).
Alexander Melnitzky, 'Defending America Against Cyber Espionage Through the Use of Active Defenses', 20 Cardozo J. Int'l and Comp. L. 537 (2012).
Barrie Sander, 'Democracy Under the Influence: Paradigms of State Responsibility for Cyber Influence Operations on Elections', 18(1) Chinese JIL 1 (2019).
Craig Forcese, 'Spies Without Borders: International Law and Intelligence Collection', 5 J Nat'l Sec L & Pol'y 195 (2011).
Csillik Kristóf - Hordós Alex, 'Zárva tartani Pandora szelencéjét: az erőszakos kiberműveletek betudásának kérdései', (3-4) Katonai és Hadijogi Szemle 6 (2023).
Darien Pun, Rethinking Espionage in the Modern Era' 23 Chi J Intl L 353 (2022).
David Clemente, <i>Cyber Security and Global Interdependence: What Is Critical?</i> (Chatham House 2013).
David Weissbrodt, 'Cyber-Conflict, Cyber-Crime, and Cyber-Espionage', 22 Minn J Intl L 347 (2013).
Delbert Tran, 'The Law of Attribution: Rules for Attributing the Source of a Cyber-Attack', Yale J L & Tech 387 (2018).
Federation of American Scientists, 'China-U.S. Trade Issues', Congressional Research Service, (2022).
Finn Seyersted, 'Diplomatic Freedom of Communication', 14 Scandinavian Studies in Law 193 (1970).
Geoffrey B. Demarest, 'Espionage in International Law', 24 Denv. J. Int'l L. & Pol'y 321 (1996).
Harriet Moynihan, 'The Application of International Law to State Cyberattacks: Sovereignty and Non-Intervention', Chatham House (2019).
Ido Kilovaty, 'Doxfare: Politically Motivated Leaks and the Future of the Norm on Non-Intervention in the Era of Weaponized Information' 9 Harvard National Security Journal (2017).
Inter-American Juridical Committee, 'Improving Transparency: International Law and State Cyber Operations - Fifth Report (2020).
Jens David Ohlin, 'Did Russian Cyber Interference in the 2016 Election Violate International Law?', 95 Tex. Law Rev. 1579 (2017).

Joseph Soraghan, 'Reconnaissance Satellites: Legal Characterization and Possible Utilization for Peacekeeping', 13 McGill LJ 458 (1967).
Josh Gold, 'Five Eyes and Offensive Cyber Capabilities: Building a Coalition for Cyber Operations', <i>NATO Cooperative Cyber Defence Centre of Excellence</i> (2020).
Katharina Ziolkowski, 'Peacetime Cyber Espionage - New Tendencies in Public International Law', in Katharina Ziolkowski (ed.), <i>Peacetime Regime for State Activities in Cyberspace</i> . International Law, International Relations and Diplomacy, NATO CCD COE Publication (2013).
Kristin A. Vara, 'Espionage: A Comparative Analysis' 22 ILSA J Int'l & Comp L (2015) 61.
Lester Godefroy, 'Shape or Deter? Managing Cyber-Espionage Threats to National Security Interests', 66(1) <i>Studies in Intelligence</i> 1 (2022).
Luke Pelican, 'Peacetime Cyber-Espionage: A Dangerous but Necessary Game' 20 <i>CommLaw Conspectus</i> 363 (2012).
Maziar Jamnejad, Michael Wood, 'The Principle of Non-intervention', 22 LJIL 345 (2009).
Myriam Dunn Cavelty, <i>Cyberwar: Concept, Status Quo, and Limitations</i> , Center For Security Studies (CSS) (2010).
Nicolas Jupillat, 'From the Cuckoo's Egg to Global Surveillance: Cyber Espionage That Becomes Prohibited Intervention', 42 NC J Int'l L 933 (2017).
Nils Melzer, 'Cyberwarfare and International Law' (UNIDIR 2011).
P.W. Singer and Allan Friedman, 'Cybersecurity and Cyberwar: What Everyone Needs to Know', OUP (2014).
Pål Wrangé, 'Intervention in National and Private Cyberspace and International Law' Jonas Ebbesson, Marie Jacobsson, Mark Klamberg, David Langlet and Pål Wrangé (eds), <i>International Law and Changing Perceptions of Security: Liber Amicorum Said Mahmoudi</i> , Brill/Nijhoff, (2014).
Patrick C. R. Terry, "'Absolute Friends": United States Espionage against Germany and Public International Law' 28 <i>Revue Québécoise de Droit International</i> 173 (2015).
Peter J Smyczek, 'Regulating the Battlefield of the Future: The Legal Limitations on the Conduct of Psychological Operations (PSYOP) under Public International Law'. 57 A.F. L. Rev 210 (2005).
Quincy Wright, 'Espionage and the Doctrine of Non-Intervention' in Roland Stanger (ed.), 'Internal Affairs, in <i>Essays on Espionage and International Law</i> ' (1962).
Remus Titiriga, 'Cyber-Attacks and International Law of Armed Conflicts; a "Jus ad Bellum" Perspective', 8(3) <i>Journal of International Commercial Law and Technology</i> 179 (2013).
Russel, Buchan, 'Cyber Espionage and International Law', Hart Publishing (2019).
Steven Collins, 'NATO and Strategic PSYOPs: Policy Pariah or Growth Industry?', 1(3) <i>Journal of Information Warfare</i> 72 (2002).
Steven R Chabinsky, 'Cybersecurity Strategy: A Primer for Policy Makers and Those on the Front Line', 4(27) <i>J Nat'l Security L & Pol'y</i> 27 (2010).

The International Institute for Strategic Studies: Cyber Capabilities and National Power: A Net Assessment, IISS Research Papers (2021).
Thibault Moulin, ‘Reviving the Principle of Non-Intervention in Cyberspace: The Path Forward’, 25(3) Journal of Conflict & Security Law 423, (2020).

Nemzetközi szervezetek dokumentumai

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.
NATO Military Committee, <i>MC-402.2 NATO Military Policy on Psychological Operations</i> (2012).
NATO Standardization Office, <i>NATO Standard AJP-3.2. Allied Joint Doctrine for Land Operations</i> (2022).
O.A.S.Doc. AG/RES. 2959 (L-O/20) (2020).
U.N.Doc A/HRC/27/37.
U.N.Doc. A/67/946.
U.N.Doc. A/68/98.
U.N.Doc. A670/174.
U.N.Doc. S/RES/138 (1960).

Egyéb

‘ASEAN-United States Leaders’ Statement on Cybersecurity Cooperation’, Singapore (2018).
‘China demands U.S. explain spying allegations linked to Australian missions’, <i>Reuters</i> (2013. október 31.), https://www.reuters.com/article/world/china-demands-u-s-explain-spying-allegations-linked-to-australian-missions-idUSBRE99U0LU/ , (Letöltve: 2024.10.25.).
‘Cyber Espionage: Examples, Types & Tactics’ <i>Dataconomy</i> , (2022. november 4.) https://dataconomy.com/2022/11/04/cyber-espionage-examples-types-tactics/ , [‘Cyber Espionage: Examples, Types & Tactics’], (Letöltve: 2024.10.23.).
‘Edward Snowden and the NSA Surveillance Program’, 31(3) Bill of Rights in Action 10 (2016).
‘Embassy Espionage: The NSA’s Secret Spy Hub in Berlin’, <i>Spiegel</i> , (2013. október 27.), www.spiegel.de/international/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy-a-930205.html , (Letöltve: 2024.10.25.).
‘Et Tu, UK? Anger Grows over British Spying in Berlin’, <i>Spiegel Online</i> (2013. november 5.), https://www.spiegel.de/international/europe/revelation-of-spy-nest-in-british-berlin-embassy-angers-germans-a-931868.html , (Letöltve: 2024.10.25.).
‘EU Statement’, United Nations 1st Committee: Thematic Discussion on Other Disarmament Measures and International Security (2018).

‘G20 Leaders’ Communiqué’, Antalya (2015).
‘Hungarian Official: Government Bought, Used Pegasus Spyware’ <i>AP News</i> (2021. november 4.), https://apnews.com/article/technology-europe-hungary-malware-spyware-ccacf6da9406d38f29f0472ba44800e0 , (Letöltve: 2024.10.23.)
‘MI5 Tried to Bug London Embassy, says Pakistan’, <i>Kuwait News Agency</i> (2003. november 6.), https://www.kuna.net.kw/ArticleDetails.aspx?id=1404317&language=en , (Letöltve: 2024.10.25.)
‘The Olympic False Flag: How infamous OlympicDestroyer malware was designed to confuse cybersecurity community’, <i>Kaspersky</i> (2018. március 9.), https://www.kaspersky.com/about/press-releases/2018_the-olympic-false-flag , (Letöltve: 2024.10.25.)
‘The U.S.-China Cyber Agreement: A Good First Step’, <i>Rand Corporation</i> , (2016. augusztus 8.), https://www.rand.org/pubs/commentary/2016/08/the-us-china-cyber-agreement-a-good-first-step.html , (Letöltve: 2024.10.23.)
‘U.S. Court: Mass Surveillance Program Exposed by Snowden Was Illegal’, <i>Reuters</i> , (2020. szeptember 3.) https://reuters.com/article/world/us-court-mass-surveillance-program-exposed-by-snowden-was-illegal-idUSKBN25T3CJ/ , (Letöltve: 2024.10.23.)
‘UNASUR’s draft statement on ‘Other Disarmament Measures and International Security’ (2016).
‘US Expels Russian Diplomats and Issues Sanctions over SolarWinds Hacking Attack’ <i>Deutsche Welle</i> (2021. április 15.), https://www.dw.com/en/us-expels-russian-diplomats-and-issues-sanctions-over-solarwinds-hacking-attack/a-57215141 , (Letöltve: 2024.10.25.)
‘US Sanctions Russia over SolarWinds Cyber Attack’, <i>Australian Computer Society</i> (2021. április 16.), https://ia.acs.org.au/article/2021/us-sanctions-russia-over-solarwinds-cyber-attack.html , (Letöltve: 2024.10.25.)
‘What Is Cyber Espionage?’ (ThreatDown) https://www.threatdown.com/glossary/what-is-cyber-espionage/ , [‘What Is Cyber Espionage?’] (Letöltve: 2024.10.24.).
‘Cyber espionage and international law’, https://www.cyber-espionage.ch/Law.html (Letöltve: 2024.10.25.).
Bridie Jabour, ‘Indonesia Summons Australian Envoy Over Embassy Spying Claims’, <i>The Guardian</i> (2013. november 1.), www.theguardian.com/world/2013/nov/01/indonesia-summons-australian-ambassador-embassy-spying-claims , (Letöltve: 2024.10.25.).
Calev Ben-David, ‘Israel to Establish Command Center for Cyber Threat Defense’, <i>Bloomberg</i> , (2011. május 18.), https://www.bloomberg.com/news/articles/2011-05-18/israel-to-establish-command-center-for-cyber-threat-defense-1?embedded-checkout=true (Letöltve: 2024.10.25.).
Congressional Research Service, ‘U.S.-China Cyber Agreement’ (2015) https://china.usc.edu/congressional-research-service-us-china-cyber-agreement-oct-16-2015 , (Letöltve: 2024.10.25.).
Council on Foreign Relations, ‘A compromise causes a power outage in Kiev, Ukraine.’,

https://www.cfr.org/cyber-operations/compromise-causes-power-outage-kiev-ukraine , (Letöltve: 2024.10.23.)
Council on Foreign Relations, 'Compromise of a Power Grid in Eastern Ukraine', https://www.cfr.org/cyber-operations/compromise-power-grid-eastern-ukraine , (Letöltve: 2024.10.23.)
Council on Foreign Relations, 'Estonian denial of service incident.', https://www.cfr.org/cyber-operations/estonian-denial-service-incident , (Letöltve: 2024.10.23.)
Council on Foreign Relations, 'Regin.', (Letöltve: 2024.10.23.)
Council on Foreign Relations, 'Stuxnet.', https://www.cfr.org/cyber-operations/stuxnet , (Letöltve: 2024.10.23.)
Dana Rubenstein, 'Nation State Cyber Espionage and its Impacts', https://www.cse.wustl.edu/~jain/cse571-14/ftp/cyber_espionage.pdf , (Letöltve: 2024.10.23.)
Ewen MacAskill and Julian Borger, 'New NSA Leaks Show How US is Bugging its European Allies', <i>The Guardian</i> , (2013. június 30.), www.theguardian.com/world/2013/jun/30/nsa-leaks-us-bugging-european-allies , (Letöltve: 2024.10.25.)
Harish Gupta, 'As Cyber Attacks Rise, India Sets Up Central Command to Fight Back', <i>DNA</i> (2011. május 15.), https://www.dnaindia.com/india/report-as-cyber-attacks-rise-india-sets-up-central-command-to-fight-back-1543352 , (Letöltve: 2024.10.25.)
Helmi Noman, 'The Emergence of Open and Organized Pro-Government Cyber Attacks in the Middle East: The Case of the Syrian Electronic Army', <i>OpenNet Initiative</i> (2011. május 5.), https://opennet.net/emergence-open-and-organized-pro-government-cyber-attacks-middle-east-case-syrian-electronic-army , (Letöltve: 2024.10.25.)
https://cert.europa.eu/ (Letöltve: 2024.10.25.)
https://cyberlaw.ccdcoe.org/wiki/Shamoon_(2012) (Letöltve: 2024.10.25.)
https://cyberlaw.ccdcoe.org/wiki/Sovereignty (Letöltve: 2024.10.23.)
https://eur-lex.europa.eu/legal-content/EN/TEXT/HTML/?uri=LEGISSUM:4637829
https://www.act.nato.int/activities/cyber-coalition/ (Letöltve: 2024.10.25.)
https://www.chathamhouse.org/events/all/members-event/international-law-future-frontiers (Letöltve: 2024.10.25.)
https://www.enisa.europa.eu/about-enisa (Letöltve: 2024.10.25.)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies (Letöltve: 2024.10.25.)
https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 (Letöltve: 2024.10.25.)
https://www.nato.int/cps/en/natohq/news_227647.htm (Letöltve: 2024.10.25.)
https://www.nato.int/cps/en/natohq/official_texts_217320.htm (Letöltve: 2024.10.25.)
https://www.nato.int/cps/en/natohq/topics_78170.htm (Letöltve: 2024.10.25.)

Jim Finkle, 'Olympic Destroyer' malware targeted Pyeongchang Games: firms' <i>Reuters</i> (2018. február 12.), https://www.reuters.com/article/us-olympics-2018-cyber/olympic-destroyer-malware-targeted-pyeongchang-games-firms-idINKBN1FW22O , (Letöltve: 2024.10.25.)
Josh Gold, 'How Estonia uses Cybersecurity to Strengthen its Position in NATO' (2019), https://icds.ee/en/how-estonia-uses-cybersecurity-to-strengthen-its-position-in-nato/ (Letöltve: 2024.10.25.).
Julian Borger, 'Brazilian President: US Surveillance a "Breach of International Law"', <i>The Guardian</i> (2013. szeptember 24.), www.theguardian.com/world/2013/sep/24/brazil-president-un-speech-nsa-surveillance , (Letöltve: 2024.10.25.)
Mark Pomerleau, 'Army assumes support agent role for US Cyber Command', <i>Defensescoop</i> , (2024. június 17), https://defensescoop.com/2024/06/17/army-assumes-support-agent-role-cyber-command/ (Letöltve: 2024.10.25.).
Merriam-Webster, 'Cyberspace' (Letöltve: 2024.10.23.).
Microsoft, 'Microsoft Digital Defense Report' (2021).
NATO, 'Warsaw Summit Communique', Varsó (2016).
Oxford English Dictionary, 'Cyberspace' (Letöltve: 2024.10.23.)
Peter Sayer, 'France Creates New National IT Security Agency', <i>Networkworld</i> , (2009. július 9.), https://www.networkworld.com/article/784528/security-france-creates-new-national-it-security-agency.html , (Letöltve: 2024.10.25.).
Philip Oltermann, Julian Borger and Nicholas Watt, 'Germany Calls in UK Ambassador over Spy Claims', <i>The Guardian</i> (2013. november 5.), www.theguardian.com/world/2013/nov/05/germany-summons-ukambassador-spy-claims-berlin , (Letöltve: 2024.10.25.).
Sebastian Fischer and Ole Reissmann, 'Germany Arms Itself for Cyber War', <i>Spiegel Online</i> , (2011. június 16.), https://www.spiegel.de/international/germany/fighting-internet-threats-germany-arms-itself-for-cyber-war-a-768764.html , (Letöltve: 2024.10.25.)