

Kovács Kinga Virág¹

A kiberkémkedés értelmezési dilemmái a kibernűveletek környezetében

A kiberkémkedés technikai és jogi értelmezése
a kibernűveletek rendszerében, 2. rész

Interpretive Dilemmas of Cyber Espionage in the Context of Cyber Operations

The Technical and Legal Interpretation of Cyber Espionage
within the Framework of Cyber Operations, Part 2

Absztrakt

A tanulmány a kiberkémkedés jogi és stratégiai értelmezésének dilemmáit vizsgálja szorosan kapcsolódva az első rész megállapításaihoz, amelyek a fogalmi dilemmákat tárták fel a rendelkezésre álló definíciós készlet értelmezésén keresztül. A tanulmány második része a témát a kiberkémkedés technikai és jogi sajátosságain keresztül közelíti meg, kiemelve, hogy a tevékenység jellemzően nem jár közvetlen fizikai károkkal, de a bizalmasság, a sértetlenség és a rendelkezésre állás sérelmén keresztül rendszerszintű kockázatot teremt. A tanulmány kvalitatív módszertannal elemzi a kiberkémkedés nemzetközi jogi besorolásának nehézségeit. Az elemzés rámutat, hogy a kiberkémkedés a klasszikus erőalkalmazási küszöb alatt marad, ugyanakkor a rendszerbe való jogosulatlan behatolás és a tartós jelenlét önmagában is a szuverenitás megsértését és folyamatos beavatkozást jelenthet.

Kulcsszavak: kiberkémkedés, nemzetközi jog, adatközpontú megközelítés

¹ Doktori hallgató, Nemzeti Közszolgálati Egyetem Hadtudományi Doktori Iskola, e-mail: kovacs.kinga.virag@uni-nke.hu

Abstract

The study examines the dilemmas of the legal and strategic interpretation of cyber espionage in close connection with the findings of the first part, which revealed conceptual dilemmas through the interpretation of the available set of definitions. The second part of the study approaches the topic through the technical and legal characteristics of cyber espionage, emphasising that although the activity does not typically cause direct physical damage, it creates systemic risks through breaches of confidentiality, integrity, and availability. The study uses qualitative methodology to analyse the difficulties of classifying cyber espionage under international law. The analysis points out that cyber espionage remains below the classic threshold of force, but that unauthorised intrusion into a system and sustained presence can in themselves constitute a violation of sovereignty and continuous interference.

Keywords: cyber espionage, international law, data-centric approach

Bevezetés

A tanulmány első része rámutatott arra, hogy a kiberkémkedés fogalmi elhelyezése mind a nemzetközi szakirodalomban, mind az állami doktrínák szintjén ellentmondásos. Noha technikai szempontból a kiberkémkedés a kibernműveletek egyik leggyakoribb formája, jogi és politikai értelemben továbbra sem teljesen világos, miként illeszthető be a nemzetközi normák rendszerébe. A különböző államok eltérő megközelítései azt mutatják, hogy a kiberkémkedés fogalmát nemcsak technikai, hanem normatív értelemben is újra kell értelmeznünk. A kiberkémkedés fogalmi elhelyezése a kibertéri információszerző tevékenységek között alapvetően bizonytalan, ugyanis a jelenségnek nincs egységes, katonai értelemben elfogadott definíciója, mivel elsősorban a civil kémkedést jelenti. A tanulmány első részében tisztáztuk, hogy a kiberkémkedés ugyan nem katonai fogalom, motivációi alapvetően gazdasági, politikai vagy ipari természetűek, technikai megvalósítása és műveleti hatásai azonban lényegében megegyeznek a katonai kibernműveletekével.

Ezek az átfedések indokolják, hogy a kiberkémkedést katonai kontextusban is értelmezzük, hiszen ugyanazon behatolási technikák, tartós jelenlétet lehetővé tevő módszerek és információszerző eszközök révén működik, mint a kiberfelderítés vagy más katonai műveletek. Éppen ez a kettősség mutat rá arra, hogy a kiberkémkedés definíciós készlete továbbra is problematikus, és hogy a technikai sajátosságok önmagukban nem elegendők a pontos jogi és műveleti besoroláshoz. A kiberkémkedés sajátosságából adódik, hogy a tevékenység jellemzően nem jár fizikai kárral, célja az információs előny megszerzése, nem pedig az ellenséges infrastruktúra megsemmisítése. Ez azonban nem jelenti azt, hogy a tevékenység jogi szempontból közömbös lenne. A jogosulatlan behatolás, az adatok manipulálása vagy a bizalmasság megsértése a nemzetközi jog több alapelvét is érintheti, különösen a szuverenitás, a beavatkozás tilalma és az erőalkalmazás tekintetében. A fogalmi pluralizmus következtében ugyanakkor hiányzik az egységes jogi besorolás, így a kiberkémkedés egyfajta küszöb

alatti műveletként jelenik meg, amely nem vált ki közvetlen katonai válaszlépést, de komoly következményekkel járhat.

Habár a szakirodalom elemzi a kiberműveletek erőalkalmazási küszöbét és a kiberkémkedés stratégiai jelentőségét, hiányzik egy olyan elemzési keret, amely a kiberkémkedést kifejezetten a szűrkezőzés műveletek kontextusában, a szuverenitás és az adat mint stratégiai erőforrás metszéspontjában vizsgálja. A tanulmány újdonsága abban ragadható meg, hogy egy olyan adatközpontú és hatásalapú értelmezést kínál a kiberműveletek rendszerében, amely túlmutat a kiberkémkedés jogi megítélésének jelenleg túl szűken, az erőalkalmazás kategóriájára redukálva történő vizsgálatán, valamint túl általánosan, a hírszerzési tevékenységek részeként való értelmezésén.

A második rész célja ezért az, hogy kvalitatív módszertant alkalmazva feltárja, miként értelmezhető a kiberkémkedés a kiberműveletek nemzetközi jogi keretei között. A tanulmány a kiberkémkedés jelenségét a jogosulatlan behatolás és a CIA-triád² sérelmének összefüggésében vizsgálja, és arra a kutatási kérdésre keresi a választ, hogy milyen feltételek mellett, milyen jogi érvek mentén értelmezhető a kiberkémkedés a kiberműveletek rendszerén belül a nemzetközi jog hatálya alá tartozó cselekményként.

Módszertan és kutatási keret

A kutatás célja nem empirikus bizonyítás, hanem a kiberkémkedés jogi besorolásával kapcsolatos értelmezési keretek feltárása, különös tekintettel a szuverenitás, az erőalkalmazás és az adat mint tárgy kérdéskörére vonatkozóan. A kutatás elsődleges forrásbázisát a nemzetközi jog releváns normái és szakértői értelmezései képezik, különös tekintettel az ENSZ Alapokmányának rendelkezéseire és a *Tallinn Manual 2.0* szakértői kommentárjaira.

A vizsgálat középpontjában nem az alkalmazott eszköz technikai jellege áll, hanem a kiberműveletek tényleges vagy potenciális hatása, valamint azok következményei. Az elemzés ezért összeveti a kiberkémkedés technikai sajátosságait a nemzetközi jogban kialakult erőalkalmazási, szuverenitási és humanitárius jogi kategóriákkal.

A kvalitatív dokumentumelemzés kiindulópontját az ENSZ Alapokmány 2. cikk (4) bekezdésében rögzített erőalkalmazási tilalom képezte mint a kiberműveletek jogi minősítésének alapszabálya. Ennek normatív tartalmát elemeztem elsőként, majd megvizsgáltam, hogy ez a klasszikus nemzetközi jogi kategória miként jelenik meg a *Tallinn Manual 2.0* kiberműveletekre vonatkozó szabályrendszerében, és ott hogyan értelmezik. A cél annak feltárása volt, hogy a kiberműveletek és különösenképpen a kiberkémkedés esetében az erőalkalmazás hagyományos fogalma milyen módon értelmezhető újra.

A tanulmány korlátai közé tartozik, hogy nem empirikus vizsgálatra épül, nem elemez konkrét incidenseket esettanulmányi módszerrel, továbbá nem technikai

² A CIA-triád az információbiztonság három pillérét jelenti: a bizalmasságot (*confidentiality*), a sértetlenséget (*integrity*) és a rendelkezésre állást (*availability*). Útmutatóként szolgál a biztonsági politikák kidolgozásához azáltal, hogy a hangsúlyt az információk jogosulatlan hozzáféréssel szembeni védelmére (bizalmasság), az adatok pontosságának és megbízhatóságának biztosítására (sértetlenség), valamint az információk szükség esetén való hozzáférhetőségének garantálására (rendelkezésre állás) helyezi.

mélységű kiberbiztonsági elemzést kíván nyújtani. A cél kizárólag a jogi és stratégiai értelmezési keretek vizsgálata. Ebből következően a tanulmány nem törekszik állami gyakorlat átfogó összehasonlító elemzésére, csupán elméleti fókuszú megközelítést alkalmaz.

A kiberkémkedés technikai és jogi sajátosságai a kibernűveletek rendszerében

A kiberkémkedés az egyik leghasznosabb stratégiának bizonyul a modern kori hadviselésben, mert nem azon információkra irányul, amelyek szabadon elérhetők.³ A kiberkémkedés olyan módszerekkel megvalósított információszerezést tesz lehetővé, amely esetében már a rendszerbe történő behatolás révén, jogosulatlan módon jutunk hozzá az információkhoz. Mégis problémába ütközünk, amikor a kiberkémkedés legalitásának kérdéskörét járjuk körbe, ugyanis jelenleg nem létezik olyan jogszabályi háttér, amely a kiberkémkedésre határozná meg szabályokat. Emiatt elengedhetetlen a kiberkémkedés következményeinek vizsgálata annak érdekében, hogy választ kapjunk arra a kérdésre, kezelhetjük-e a kiberkémkedést a kibernűveletek részeként, s milyen szabályozásbeli nehézségeket azonosíthatunk ezen a téren.

A kiberkémkedés egyik sajátossága, hogy tárgyává szinte bármilyen információ válhat, amely a digitális térben előállítható, tárolható vagy továbbítható. Mivel a kibertérben nincsenek a fizikai világhoz hasonló, természetes korlátok, a megszerzhető információk köre gyakorlatilag korlátlan. A személyes adatoktól, egészségügyi nyilvántartásoktól és gazdasági titkoktól kezdve a kritikus infrastruktúrák irányítását biztosító rendszerek technikai részleteiig minden célpontként szolgálhat.⁴

A kiberkémkedés megvalósítására használt technikák túlnyomó többsége valamilyen rendszerbe való jogosulatlan behatolást feltételez. Például említhetők a *living off the land* (LOTL)⁵ támadások, amelyek a környezetben már jelen lévő, megbízható rendszereszközöket használják ki, vagy éppen a sokak által ismert *advanced persistent threat* (APT) támadások, amelyek során a támadók olyan fejlett technikákat alkalmaznak, amelyek segítségével képesek az adott rendszerhez hosszú ideig hozzáférni.⁶ Ezen támadások esetében a támadók úgy szereznek hozzáférést az adott rendszerhez és a rendszerben tárolt adatokhoz, hogy a hozzáférés-vezérlés védelmi kontrollját kijátsszák vagy teljesen megkerülik. Mivel a rendszerbe történő legitim belépés első állomása a felhasználó azonosítása és hitelesítése lenne, a kontrollok megkerülésével bejutó támadó sem azonosítani, sem hitelesíteni nem tudja magát a rendszer által elfogadott módon. Ennek következtében a rendszerben való jelenléte definíció szerint jogosulatlan.⁷

³ A szabadon hozzáférhető információk alatt az OSINT (*open source intelligence*) kategóriába tartozó nyílt forrású adatok értendők. Az OSINT a nyílt forrású hírszerzés rövidítése, amely nyilvános, jogilag elérhető forrásokból (például internetes weboldalak, közösségi média, sajtó, publikus adatbázisok stb.) származó információk gyűjtésére, elemzésére és kiértékelésére fókuszál.

⁴ Civuli et al. 2022.

⁵ Fortinet 2025b.

⁶ Fortinet 2025a.

⁷ Fortinet 2025c.

A jogosulatlan jelenlét nem csupán a támadó státuszát jelöli, de konkrét működési kockázatot is jelent, mivel lehetővé teszi olyan információk, erőforrások és műveletek elérését, amelyekhez a behatolónak nincsen jogosultsága. Továbbá a hozzáférés-vezérlés és a jogosultságkezelés kontrolljainak kijátszása révén létrejövő jogosulatlan jelenlét közvetlenül veszélyezteti a rendszerek bizalmasságát (*confidentiality*), sértetlenségét (*integrity*) és rendelkezésre állását (*availability*) – azaz a klasszikus CIA-triádot.⁸

- A *bizalmasság* sérelme esetén a jogosulatlan jelenlét lehetővé teszi érzékeny adatok olvasását és másolását, a rendszerben található összes adathoz való hozzáférést. Mivel a támadó megkerülte a hitelesítés és az azonosítás folyamatát, az információkhoz való hozzáférése nem engedélyezett folyamatokon keresztül történik.
- A *sértetlenség* megsértése esetén a támadó nemcsak olvashat, hanem módosíthat is adatokat, konfigurációkat és naplóbejegyzéseket, ennek következtében integritásvesztés történik.
- A *rendelkezésre állás* megsértése esetén pedig a szolgáltatások leállása következik be, rendeltetésszerű használatuk ellehetetlenül.

A kiberkémkedés elsősorban a bizalmasságot érinti, azonban annak okán, hogy a triád elemei összekapcsolódnak, a bizalmasságot sértő műveletek könnyen a sértetlenséget és a rendelkezésre állást is veszélyeztethetik. Mivel a kiberkémkedés elsődleges célja nem a pusztítás, hanem az információkhoz való hozzáférés minél hosszabb időn keresztül, a kiberkémkedés klasszikus értelemben nem egyenlő a kibertámadással. Azonban ha a kiberkémkedés motivációját vizsgáljuk, az tovább árnyalja ezt a megközelítést.⁹

A kiberkémkedés értelmezése kapcsán alapvető kérdésként merül fel, hogy olyan önálló, sajátos tevékenységként tekinthetünk-e rá, amelyre jelenleg nem állnak rendelkezésre explicit szabályok, vagy inkább olyan átfogóbb cselekmények – kibertámadások vagy kiberműveletek – részeként értelmezendő, amelyekre a nemzetközi jog már meghatároz bizonyos kereteket.

A *Tallinn Manual 2.0*¹⁰ 92. szabálya alapján a kibertámadás olyan támadó vagy védekező kiberművelet, amelyről észszerűen feltételezhető, hogy személyi sérülést vagy halált, illetve tárgyi kárt vagy megsemmisülést okoz.¹¹

⁸ Fortinet 2025d.

⁹ LIBICKI 2018.

¹⁰ Jelenleg az egyetlen kézzelfogható dokumentumként azt illetően, hogy a kiberműveletek esetében a nemzetközi jog miképpen érvényesülne, a *Tallinn Manual* első és második kiadása szolgál. A *Tallinn Manual 2.0* az első részt bővíti ki, és 154 *black letter* szabályt határoz meg a kiberműveletekre vonatkozóan. Noha a *Tallinn Manual 2.0* az Európai Bizottság álláspontját és szakértők személyes véleményét képviseli, továbbá hozzájárult számos állam is, jelen dokumentum jogi kötéssel nem bír, inkább ajánlasként, iránymutatásként szolgál, következtetései nem tekinthetők a nemzetközi jog kötelező erejű álláspontjának.

¹¹ SCHMITT 2017.

A kiberkémkedés értelmezése a kibernműveletek tükrében – a kiberkémkedés mint szűrkezőna

A szűrkezőna fogalma a szakirodalomban azon állami tevékenységek összességét jelöli, amelyek a nyílt fegyveres konfliktus küszöbe alatt maradnak, ugyanakkor stratégiai hatást fejtenek ki, és tudatosan kihasználják a jogi és politikai bizonytalanságokat. A szűrkezőna-műveletek jellemzően nem érik el az erőalkalmazás klasszikus küszöbét, mégis képesek tartós befolyást gyakorolni az ellenfél politikai, gazdasági vagy katonai mozgásterére. A kibernműveletek, különösképpen a kiberkémkedés, ezen logika mentén tipikusan szűrkezőnas tevékenységeknek tekinthetők, mivel nem járnak közvetlen fizikai rombolással, ugyanakkor létrehozhatnak stratégiai aszimmetriát.¹²

A kiberkémkedés jogi megítélése pont ebből kifolyólag a nemzetközi jog alapján is problémásnak minősül, és a szakértői álláspontok is megoszlanak a témát illetően. Az említett *Tallinn Manual* többek között ezen kérdéssel is foglalkozik, és több aspektusból közelíti meg a témát. A kézikönyv 32. szabálya rögzíti, hogy a békeidőbeli kiberkémkedés önmagában nem minősül nemzetközi jogba ütköző cselekménynek, mindazonáltal hangsúlyozza, hogy a végrehajtás módja könnyen sértheti a nemzetközi jog egyéb normáit. Ez történik abban az esetben, ha egy állam kibereszközei behatolnak egy másik állam területén található információs infrastruktúrába, ezzel a szuverenitás megsértését kockáztatva. A kémkedés hagyományosan a túrt kategóriába tartozik, hiszen mindenki szeretne információt szerezni a másiktól, de senki sem szeretné, ha róla szereznének információt, azonban az alkalmazott védelmi kontrollok áttörésén keresztül elért információs infrastruktúrába való behatolás már invazív jellegű.

A *Tallinn Manual 2.0* 32. szabálya alapján a kiberkémkedés önmagában nem tiltott a nemzetközi jog szerint, mivel nem minősül erőszak alkalmazásának vagy fegyveres támadásnak. A kibertér sajátos jellege miatt, noha a kiberkémkedés végrehajtásának módja sértheti a nemzetközi jog normáit, az egyik legnagyobb problémát az erőalkalmazás (*use of force*) kérdéskörének kibertérbeli értelmezése okozza.

A nemzetközi jog az erő alkalmazásának kérdését az ENSZ Alapokmányában szabályozza, különösen a 2. cikk (4) bekezdése és az 51. cikk révén. A 2. cikk (4) bekezdése kimondja, hogy minden állam köteles tartózkodni az erőszak alkalmazásától más államok szuverenitása, területi integritása vagy politikai függetlensége ellen. Ez az elv az államok közötti békés együttműködés alapját képezi, és a nemzetközi jog egyik sarokköve. Az 51. cikkely ezzel szemben kivételt fogalmaz meg, amely szerint az államoknak joguk van az önvédelemre egy fegyveres támadás esetén mindaddig, amíg az ENSZ Biztonsági Tanácsa nem hoz megfelelő intézkedéseket a nemzetközi béke és biztonság fenntartása érdekében.¹³

A *Tallinn Manual 2.0* 14. fejezete értelmezi az ENSZ Alapokmány 2. cikk (4) bekezdésében lefektetett erőalkalmazási tilalmat és az önvédelemhez való jogot (51. cikk) a kibernműveletek kontextusában. A szakértők abból indulnak ki, hogy az értékelés során nem az alkalmazott eszköz, vagyis az, hogy fegyverről vagy kibereszkörről van-e szó, a meghatározó, hanem a következmények és a körülmények. Ennek értelmében, ha

¹² MAZARR 2015.

¹³ United Nations 1945.

egy kiberművelet hatásai összevethetők a hagyományos fegyveres erő alkalmazásának következményeivel, úgy az a nemzetközi jog értelmében erő alkalmazásának minősül.¹⁴

A *Tallinn Manual 2.0* 68. szabályának értelmében tilos az olyan kiberművelet, amely egy állam területi integritása vagy politikai függetlensége ellen irányul, vagy amely más egyéb módon ellentétes az ENSZ Alapokmányában megfogalmazott célokkal. A 69. szabály meghatározása szerint az erő alkalmazásának fennállását minden esetben a művelet mértéke és hatásai alapján kell megítélni. Mindazonáltal nem minden kényszerítő jellegű kiberművelet minősül erőalkalmazásnak. A pszichológiai hadviselés, a propaganda vagy akár bizonyos gazdasági jellegű nyomásgyakorlás önmagában nem sorolható ide, ugyanakkor ha egy állam például fegyveres csoportokat lát el kiberfegyverekkel, illetve olyan technológiai támogatással, amely lehetővé teszi a pusztító kiberműveletek végrehajtását, az már erőalkalmazásnak tekinthető. A 70. szabály a fenyegetés tilalmát rögzíti. Minden olyan kiberfenyegetés jogellenes, amelynek végrehajtása esetén maga a cselekmény erőalkalmazásnak minősülne.

Mivel a nemzetközi jogban nincs egyetemes, tételes definíció arra vonatkozóan, hogy mi számít a kibertérben erőalkalmazásnak, a *Tallinn Manual* szakértői értelmezési tényezőket javasolnak. Ilyen szempont többek között a súlyosság, például fizikai károk, emberéletek elvesztése vagy súlyos gazdasági károk, továbbá az azonnaliság, a művelet invazív jellege, valamint az állami részvétel bizonyíthatósága. Ezen tényezők együttes mérlegelésével dönthető el, hogy egy adott kiberművelet eléri-e az erőalkalmazás küszöbértékét.

A *Tallinn Manual 2.0* hangsúlyozza a különbséget az erőalkalmazás és a fegyveres támadás között (69. és 71. szabály). Minden fegyveres támadás egyben erőalkalmazás is, azonban nem minden erőalkalmazás minősül fegyveres támadásnak. Ez a megkülönböztetés gyakorlati szempontból döntő jelentőségű. Amennyiben egy kiberművelet eléri a fegyveres támadás szintjét, az érintett állam jogosult az ENSZ Alapokmányának 51. cikke szerinti önvédelemre, akár fegyveres eszközökkel is. Ha azonban egy művelet „csak” erőalkalmazásnak számít, de nem éri el a fegyveres támadás küszöbét, akkor a válaszlépések kizárólag ellenintézkedések, diplomáciai eszközök, illetve szankciók formájában jogszerűek, fegyveres önvédelemre viszont nincsen lehetőség. Ez a kettősség rávilágít arra, hogy a kiberműveletek sajátosságai miatt mennyire problematikus az erőalkalmazás kategóriájának átültetése a gyakorlatba.

A kiberműveletek esetében tehát elviekben lehetséges, hogy azok a nemzetközi jog értelmében elérjék az erőalkalmazás küszöbét, amennyiben hatásuk összevethető a hagyományos fegyveres cselekmények következményeivel. Ezzel szemben a kiberkémkedés sajátossága, hogy jellemzően a bizalmasság megsértésére irányul, és nem jár együtt közvetlen fizikai kárral vagy rombolással. Így a kiberkémkedés csak ritkán, speciális körülmények fennállása esetén értelmezhető az erő alkalmazásaként, legtöbbször pedig a szuverenitás megsértése, a be nem avatkozás tilalma vagy más alacsonyabb szintű normák keretében vizsgálható, amelyek nem érik el az erő alkalmazásának küszöbértékét. Ez a kettősség jelentős jogértelmezési nehézséget okoz, hiszen míg a kiberműveletek egy része nyilvánvalóan az erőalkalmazás kategóriájába sorolható, addig a kiberkémkedés tipikusan a küszöb alatti műveletek közé tartozik.

¹⁴ SCHMITT 2017.

Emiatt a kiberkémkedést nehéz a klasszikus értelemben vett kibernézetek részé-
ként értelmezni, hiszen a nemzetközi jog által felállított küszöbértékeket rendszerint
nem érik el.

Mindez rávilágít arra, hogy a jelenlegi jogértelmezések, amelyek elsősorban
az erőalkalmazás küszöbének meghatározására épülnek, nem tudják kielégítően kezelni
a kiberkémkedés lényegi problémáját. A titkos információszerző műveletek során
ugyanis már maga a rendszerbe való jogosulatlan behatolás önmagában sért olyan
alapelveket, mint a szuverenitás vagy a területi integritás, akkor is, ha a behatolás nem
jár együtt közvetlen fizikai kár okozásával, miközben a kibertérben a pusztító hozzáférés
megszerzése is önálló sérelmet jelenthet. Ez az értelmezési hiányosság eredményezi
azt, hogy a kiberkémkedés nehezen illeszthető be a meglévő jogszabályi keretekbe,
mivel túl enyhének tűnik ahhoz, hogy az erőalkalmazás alá sorolják, de túl invazív
ahhoz, hogy egyszerűen figyelmen kívül hagyják.¹⁵

Mindazonáltal a kiberkémkedés rendszerbe való jogosulatlan behatolásának
sajátossága okán nem elégséges csupán arra alapozni, hogy ez a tevékenység nem éri
el az erő alkalmazásának küszöbét. Jelentős dilemmának bizonyul ez a kibertérben,
ahol az egyik fél azon erőfeszítései, hogy információt szerezzen a másíkról, a másíkról
által egy katonai támadást megelőző kibertámadásra való felkészülésként is értel-
mezhetők. Egy kiberkémkedésre tervezett *malware* bejuttatása a rendszerbe gyakran
megegyezik egy kibertámadásra tervezettel, egy kritikus rendszerben történő felfe-
dezése pedig könnyen tekinthető a támadás közvetlen előfutárának. Ez általában arra
késztetné a célpontot, hogy válaszüreakcióval éljen, ami önmagában is súlyosbíthatja
a feszültségeket. A másíkról indítékaival kapcsolatos gyanú erős, hiszen a lehetséges
kibertámadáshoz nem kapcsolódó kiberkémkedés sem feltétlenül ártatlan. Példaként
említhető, hogy ha a feltört rendszer való időben követi nyomon a katonai egysé-
geket, azzal beláthatatlan károkat lehet okozni.¹⁶ Ebből kifolyólag szükséges más
szemszögből is megvizsgálni a kérdéskört.

Az adat mint stratégiai erőforrás a kiberkémkedés célrendszerében

Az említett példák világosan megmutatják, hogy a kiberkémkedés következményei
nem kizárólag a behatolás technikái jellemzőiből adódnak, hanem abból is, hogy
milyen információhoz jut hozzá az elkövető, és azokat miként használja fel. Az adat
önmagában stratégiai erőforrássá válik, hiszen a való idejű helyzetkép, a szakmai tudás,
a logisztikai adatok vagy a kritikusinfrastruktúra-információk birtoklása közvetlen
taktikai és stratégiai előnyt biztosíthat. Emiatt szükséges az adat mint célpont külön
elemzése stratégiai szempontból, annak érdekében, hogy jobban megértsük, az adat
miként válhat a kiberkémkedés okán egy kibernézet tárgyává.

Az adat olyan stratégiai erőforrás, amely birtoklása, feldolgozása vagy manipulálása
révén közvetlen hatalmi, gazdasági és katonai előnyt biztosít. A digitális korszakban

¹⁵ SCHMITT 2017.

¹⁶ LIBICKI 2018.

az információs fölény az államok közötti versengés egyik legfontosabb dimenziójává vált, hiszen az adat nemcsak az állami döntéshozatal alapját képezi, hanem a nemzetbiztonsági és gazdasági érdekérvényesítés eszköze is. Az adat rezilienciája és ellenőrzése az állami szuverenitás új meghatározó eleme lett, hiszen az adatáramlás feletti kontroll maga is hatalmi tényezőnek számít.¹⁷

Ezt az elképzelést tovább erősíti a *weaponised interdependence* elmélete is, amely rámutat arra, hogy a globális gazdasági és információs hálózatok szerkezete önmagában is hatalmi erőforrássá válik. Azok az államok, amelyek joghatósággal vagy tényleges kontrollal rendelkeznek a hálózati központok felett, információs előnyre tehetnek szert (*panopticon effect*), illetve korlátozhatják más szereplők hozzáférését (*chokepoint effect*). Ezen logika mentén az adat nem csupán passzív célpont, hanem olyan hálózati csomópontokon keresztül áramló erőforrás, amelynek megszerzése hatalmi aszimmetriát hozhat létre. A kiberkémkedés így értelmezhető a hálózati interdependencia tudatos kihasználásaként is, amely a pusztán információszerzésen túl eredményezheti a stratégiai befolyásszerzést is.¹⁸

A kiberkémkedés célrendszerében az adat megszerzése nem feltétlenül öncélú, hanem a stratégiai információs fölény megszerzésének egyik eszköze. A hírszerzési célponttá váló adatkészletek, mint például katonai elhelyezkedési információk, energetikai infrastruktúrák működési adatai, kutatás-fejlesztési eredmények vagy pénzügyi hálózati mintázatok, mind olyan értéket képviselnek, amely befolyásolja az állam biztonsági és gazdasági mozgásterét. Ez egyfajta erőforrás-kivonási műveletként is értelmezhető, mivel az információs javak megszerzése stratégiai kapacitást jelent, még ha a fizikai infrastruktúra sértetlen is marad. A kiberkémkedés hosszú távú következménye nem a közvetlen anyagi kár, hanem a stratégiai aszimmetria létrejötte, amely az információ birtoklásán keresztül képes alakítani az erőviszonyokat.¹⁹

A kiberkémkedés során megszerzett adatok értéke a felhasználás kontextusától függ. A valós idejű adat azonnali operatív előnyt biztosíthat, míg a hosszú távon feldolgozható adatkészletek, mint a kutatási adatok vagy a technológiai dokumentációk, stratégiai hatásúak. Az adat stratégiai értéke a manipulációban is megnyilvánul. A kiberkémkedés nem kizárólag információszerzést jelent, hanem a megszerzett adatok módosításán, kiszivárogtatásán keresztül befolyásolhatja az ellenfél döntéshozatali folyamatait. Az adatok ilyen jellegű fegyveresítése (*weaponisation of data*) új dimenziót ad a kiberkémkedésnek, hiszen az adatok nem csupán információs előnyt biztosítanak, hanem aktív befolyásolási és kényszerítő eszközzé is válhatnak az államok közötti konfliktusok során.²⁰

A stratégiai adatcélpontú szemlélet rámutat arra, hogy a kiberkémkedés során megszerzett információk értéke nemcsak abban rejlik, hogy mit tartalmaznak, hanem abban is, hogy milyen döntések alapjául szolgálhatnak, s miként lehet azokat felhasználni. Az adat birtoklása lehetővé teszi az ellenséges műveletek előrejelzését, a politikai folyamatok befolyásolását vagy akár a gazdasági döntések manipulálását, így a kiberkémkedés során megszerzett adatok a klasszikus hírszerzési adatokhoz

¹⁷ ROSSBACH 2024.

¹⁸ FARRELL-NEWMAN 2019.

¹⁹ DEVANNY-MARTIN-STEVENS 2021.

²⁰ SHUKLA 2025.

haszonlóan a műveleti tervezés közvetlen komponenseivé válnak. A kibertérben az adat tehát nem pusztán a célpont, hanem olyan stratégiai érték, amelynek birtoklása vagy elvesztése konkrét biztonsági következményekkel jár.

Az adat stratégiai szerepe egyben jogi kihívást is teremt, és meghatározó kérdést vet fel: miként értelmezhető az adat mint a kiberműveletek tárgya, és milyen védelem illeti meg a nemzetközi jog alapján?

Az adat mint a kiberművelet tárgya?

Az erőalkalmazás kérdéskörének nehézségei és az adat stratégiai fontosságának okán érdemes lehet a kiberkémkedés kiberműveletként történő minősítésének értelmezését eltolni az adatközpontú szemlélet felé. Ha egy művelet elsődleges célja nem egy infrastruktúra fizikai megbontása, hanem konkrét adatkészletek megszerzése, módosítása vagy megsemmisítése, akkor ez önmagában jogilag és stratégiaileg is más, releváns kimeneteket hoz. Az adatokhoz való tartós hozzáférés sok esetben nagyobb, közvetlenebb és tartósabb következményekkel járhat, mint egy rövid idejű szolgáltataskiesés, továbbá egyetlen, stratégiai jelentőségű adattömeg exfiltrációja közvetetten olyan súlyos károkat okozhat, amelyek hatásukban nem feltétlenül különböznek egy hagyományos fizikai támadástól.

A gyakorlatban ez a megközelítés két dolgot eredményez. Egyrészt a minősítés rugalmasabbá válik, és egy adatellenes művelet akkor is átlépheti az erőalkalmazás küszöbét, ha maga a művelet nem okoz közvetlen fizikai sérülést, de a kiszivárgott vagy manipulált információ következményei súlyos, az állam működését vagy a lakosság biztonságát alapvetően veszélyeztető hatásokat idéznek elő, másrészt a védelem és a jogi válasz eszköztárának bővülését is előíranyozza.

Az adatközpontú megközelítés egyik legnagyobb nehézsége jelenleg, hogy a jogszabályi környezet nem sok teret enged az adatok tárgyként való értelmezésének. A *tárgy* fogalma a nemzetközi humanitárius jogban kulcsfontosságú a polgári védelem kiterjedése és a támadási tilalmak meghatározása szempontjából. Ennek fényében meghatározó kérdés, hogy a számítógépes adatok a humanitárius jog szerinti tárgynak minősülnek-e.

A jogszabályi értelmezések alapján a tárgy anyagi jellegű entitásként jelenik meg. Az adatok ezzel szemben immateriális természetűek, hiszen hordozókhoz, folyamatokhoz és rendszerekhez kötötten fejtik ki hatásukat. Ebből következően a *tárgy* kifejezés kiterjesztése az adatokra nem igazolható. Fontos ugyanakkor, hogy e minősítés nem hagyja teljesen védelem nélkül az adatokat. Egyrészt bizonyos normák közvetlen kötelezettségeket állapítanak meg olyan funkciók zavartalanására, amelyek szükségképpen adatkezelést feltételeznek (például egészségügyi létesítmények működésének tilalmazott megzavarása), ezek alkalmazása nem attól függ, hogy az adatok tárgyak-e. Másrészt az adatok közvetett védelmet élveznek azáltal, hogy a hordozó fizikai eszközök (szerverek, adathordozók, nyomtatott anyagok) a polgári tárgyak védelmének körébe tartoznak, és támadásuk a humanitárius jog általános korlátai alá esik.

A *tárgy* fogalma szorosan kapcsolódik a katonai célpont meghatározásához is, amely kifejezetten tárgyakra vonatkozik, egész pontosan olyan anyagi dolgokra, amelyek

természetük, elhelyezkedésük, rendeltetésük vagy felhasználásuk révén hatékonyan hozzájárulnak a katonai műveletekhez, és amelyek megsemmisítése vagy semlegesítése egyértelmű katonai előnyt biztosít az adott körülmények között. E logika szerint az adatok mint immateriális elemek önmagukban nem tartoznak a katonai célpont kategóriájába, a hozzájuk kapcsolódó hordozók viszont igen, ha megfelelnek a fenti kritériumoknak.²¹

Jelen állás szerint a pusztán adatellenes műveletek csak akkor minősülnek támadásnak, ha előre láthatóan személyi sérülést, halált vagy fizikai tárgyak károsodását, illetve azok megsemmisülését okozzák, valamint a funkcionalitás elvesztését idézik elő a fizikai infrastruktúrában. Ezzel szemben a pusztá behatolás a rendszerbe a jelenlegi szabályok szerint nem tekinthető támadásnak.²²

Noha az adatok önmagukban nem minősülnek a nemzetközi humanitárius jog értelmében tárgynak, a fenti érvek mégis azt mutatják, hogy közvetlenül és közvetve is, de olyan védelem alatt állnak, amely releváns a kiberműveletek és a kiberkémkedés vizsgálatában. Az adatokat nem lehet egyszerűen figyelmen kívül hagyni a jogi értelmezés során, hiszen a hordozóeszközök és a működéshez nélkülözhetetlen funkciók védelme okán az adatok ténylegesen értelmezési relevanciát nyernek a következményekben. Ez rámutat többek között arra is, hogy az adatközpontú megközelítés egy olyan új értelmezési keretet biztosíthatna, amelyben rugalmasabban kezelhetővé válnának a jelenleg nehezen alkalmazható normák, és amely a kiberkémkedést a kiberműveletek részeként tenné értelmezhetővé.

A kiberkémkedést érdemes a kiberműveletek részeként vizsgálni, mivel az ilyen műveleteknek a bizalmasság célzott sérelmével jelentős hatásuk van, még akkor is, ha nem realizálódnak fizikai károkozásban. Ezt az értelmezést a jelenlegi jogi normák szűk keresztmetszete indokolja, hiszen a bizalmasság elleni kiberkémkedéshez kapcsolódó beavatkozások ma többnyire a humanitárius jog tárgyi védelmén kívül esnek, mindazonáltal az információs társadalmakban az ilyen beavatkozások következményei lehetnek a legsúlyosabbak. Ebből kifolyólag nem idegen az a szakértői elképzelés, hogy a meglévő adatvédelmi és adatbiztonsági elveket emeljék be a kiberkémkedés mint kiberművelet hatásainak értékelésébe.²³

Fontos megérteni, hogy a rendszerbe jutó és az adatokhoz hozzáférő szereplő szándéka kezdetben ismeretlen, éppen ezért a kiberkémkedés önmagában is potenciális előkészület lehet egy későbbi, fizikai hatást célzó kiberművelethez. Ez egy rugalmasabb szabályozási keretet vetít előre, amely azzal állna összhangban, hogy a humanitárius jog *tárgy* és *támadás* fogalmának feszegetése helyett a különösen érzékeny civil és katonai adatállományok ellen elkövetett kiberkémkedés tekintetében a jogi értelmezés kibővül.

Ha az adatközpontú megközelítést fogadjuk el, a kiberkémkedés érdemben kiberműveletnek minősül, mert közvetlenül a bizalmasság (és közvetetten a sértetlenség és a rendelkezésre állás) sérelmére irányul. Ez a szemlélet szükségszerűen egy rugalmasabb szabályozási keretet vetít előre, hiszen a kibetér sajátosságai miatt a meglévő jogi normák pusztá beillesztése nem elégséges. Ebből a perspektívából a kiberkémkedés

²¹ POMSON 2023.

²² MCCORMACK 2018.

²³ GEISS-LAHMANN 2021.

bizonyos körülmények között a támadás részeként is értelmezhető, míg a tanulmány első részében bemutatott hagyományos, többnyire passzív elektronikai felderítés tipikusan nem éri el ezt a küszöböt. Ez a különbség jól mutatja a kibertér sajátosságait, és indokolja egy rugalmas, hatásalapú és adatközpontú keret bevezetését, mivel a meglévő normák a kibertérben nem érvényesülnek következetesen.

Következtetések

Az eddigiek alapján világosan kirajzolódik a kiberkémkedés kiberműveletek részeként történő értelmezésének nehézsége, ezzel együtt pedig a relevanciája is. Jogi és gyakorlati értelemben a kiberkémkedés az elsődleges célja szerint jellemzően adatgyűjtésre és felderítésre irányul, és sok esetben nem okoz közvetlen fizikai károkat vagy azonnali, kényszerítő hatást, ezért formálisan nem illeszkedik a klasszikus erőalkalmazás fogalmkörébe, így problémát jelent a kiberműveletek részeként való értelmezése. Mindazonáltal az információk megszerzéséhez a rendszerbe való bejutás és a hozzáférés-vezérlés megkerülése jogosulatlan jelenlétet hoz létre, amelynek a fenntartása önmagában folyamatos beavatkozás a célpont működésébe. Még ha nem is jár azonnali fizikai kárral, ez a jelenlét rendszerszintű kockázatot teremt, mivel sérti a bizalmasságot, erodálja a sértetlenséget, és fenyegeti a rendelkezésre állást.

Az elemzés rávilágított arra, hogy a kiberkémkedés kiberműveletként történő értelmezése elsősorban a jogosulatlan rendszerhozzáférés és a tartós jelenlét fenntartásában ragadható meg, amely lehetővé teszi stratégiai jelentőségű adatkészletek megszerzését. Ha az értékelés középpontjába az adatot is behelyezzük mint önálló célpontot, a kép még árnyaltabbá válik. Egy stratégiai jelentőségű adattömeg megszerzésének következményei olyan súlyosak és tartósak lehetnek, hogy hatásukban megközelítik az erő alkalmazásának kategóriáját, így a kiberkémkedés egyes esetei a konkrét támadás részeként vagy a támadás előkészítéseként is értelmezhetők. Az adat mint stratégiai erőforrás nem csupán hírszerzési, hanem hatalmi tényezővé is vált a kibertérben, és a hozzáférés feletti kontroll immár a szuverenitás új dimenzióját jelenti. Ezzel összhangban a kiberkémkedésre irányuló műveletek nem tekinthetők pusztán technikai behatolásoknak, ezek a stratégiai információs fölény megszerzésének eszközei.

A *Tallinn Manual 2.0* releváns szabályainak elemzése alapján megállapítható, hogy a kiberkémkedés önmagában rendszerint nem minősül erőalkalmazásnak, és csak kivételes körülmények fennállása esetén érheti el a fegyveres támadás küszöbét. A nemzetközi jog jelenlegi keretrendszere elsősorban a fizikai károkozásra és a közvetlen romboló hatásokra koncentrál, ami a kibertér sajátosságai mellett értelmezési hiányosságokat is eredményez. Ugyanakkor a rendszerbe történő jogosulatlan behatolás, valamint az állami funkciók működéséhez szükséges adatokhoz való hozzáférés a szuverenitás sérelmeként vagy a be nem avatkozás tilalmának megsértéseként is relevánssá válhat. Az első rész megállapításaival összhangban mindez arra utal, hogy a kiberkémkedés a küszöb alatti műveletek kategóriájából fokozatosan a stratégiai biztonsági műveletek közé emelkedik. A fogalmi nehézségekből fakadó joghézag nem szűkíthető le pusztán jogi problémára, hanem a technológiai, stratégiai és politikai realitások vonatkozásában

kell kezelni. A kibertér hatásalapú logikája megköveteli, hogy a jövőbeli szabályozás ne a hagyományos fegyveres konfliktusok értelmezéséből, hanem az adat mint stratégiai erőforrás védelméből és a bizalmasság garanciáiból induljon ki.

A cikk fő következtetése, hogy a kibertér sajátosságai teszik lehetővé azt, hogy már a pusztá jogosulatlan hozzáférés is sérelmet okozzon, az adatok védelme pedig kulcsfontosságú azon rendszerekben, amelyekhez a támadó jogosulatlan módon szerzett hozzáférést. A jelenlegi, merev kategóriákra épülő nemzetközi normák nem érvényesülnek következetesen, így olyan rugalmas keretre van szükség, amely lehetővé teszi az arányos technikai és politikai válaszokat. Egy ilyen keret adhat hiteles választ a kiberkémkedés és a kiberműveletek közötti átmenetekre, miközben csökkenti a nem megfelelő reakciók kockázatát.

A vizsgálat több olyan területet is azonosított, amely további elemzést igényel. Nyitott kérdés marad, hogy az adat milyen feltételek mellett tekinthető a nemzetközi humanitárius jog szempontjából releváns tárgynak, illetve hogy a pusztán adatellenes műveletek mikor és milyen körülmények között minősülhetnek támadásnak. További kutatás szükséges annak feltárására is, hogy az egyes technikai trendek, mint például az APT-műveletek, a *supply chain* kompromittálás vagy az egyes rendszereszközökre építő technikák miként befolyásolják az erőalkalmazási küszöb és a szuverenitás sérelmének értelmezési kereteit.

Felhasznált irodalom

- CIVULI, Abdulla et al. (2022): Cyber Espionage Consequences as a Growing Threat. *Journal of Natural Sciences and Mathematics*, 7(13–14), 13–20.
- DEVANNY, Joe – MARTIN, Ciaran – STEVENS, Tim (2021): On the Strategic Consequences of Digital Espionage. *Journal of Cyber Policy*, 6(3), 429–450. Online: <https://doi.org/10.1080/23738871.2021.2000628>
- FARRELL, Henry – NEWMAN, L. Abraham (2019): Weaponized Interdependence: How Global Economic Networks Shape State Coercion. *International Security*, 44(1), 42–79. Online: https://doi.org/10.1162/isec_a_00351
- Fortinet [é. n. a]: *Advanced Persistent Threat: The Silent, Long-Term Cyberattack*. Online: www.fortinet.com/resources/cyberglossary/advanced-persistent-threat
- Fortinet [é. n. b]: *Living Off The Land (LOTL) Attacks And Techniques*. Online: www.fortinet.com/resources/cyberglossary/living-off-the-land-lotl
- Fortinet [é. n. c]: *What Is Access Control?* Online: www.fortinet.com/resources/cyberglossary/access-control
- Fortinet [é. n. d]: *What Is the CIA Triad?* Online: www.fortinet.com/resources/cyberglossary/cia-triad
- GEISS, Robin – LAHMANN, Henning (2021): Protection of Data in Armed Conflict. *International Law Studies*, 97, 556–572. Online: <https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=2964&context=ils>
- LIBICKI, Martin C. (2018): Drawing Inferences from Cyber Espionage. In *2018 10th International Conference on Cyber Conflict*. Tallinn: NATO CCDCOE Publications, 109–122. Online: <https://doi.org/10.23919/CYCON.2018.8405013>

- MAZARR, J. Michael (2015): *Mastering the Gray Zone: Understanding a Changing Era of Conflict*. [H. n.]: Strategic Studies Institute – U.S. Army War College. Online: <https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=1427&context=monographs>
- MCCORMACK, Tim (2018): International Humanitarian Law and the Targeting of Data. *International Law Studies*, 94, 222–240. Online: <https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1725&context=ils>
- POMSON, Ori (2023): 'Objects'? The Legal Status of Computer Data under International Humanitarian Law. *Journal of Conflict and Security Law*, 28(2), 349–387. Online: <https://doi.org/10.1093/jcsl/krad002>
- ROSSBACH, Niklas H. (2024): *Intelligence and Data Resilience. A small State Perspective on Digitalisation and National Defence Towards the 2030s*. Stockholm: Försvarshögskolan. Online: <https://doi.org/10.62061/iibr1180>
- SCHMITT, Michael N. (2017): *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press. Online: <https://doi.org/10.1017/9781316822524>
- SHUKLA, Veer Summer (2025): The Weaponization of Data: International Legal Responses to Digital Espionage and State-Sponsored Cyber Warfare. *The Yale Review of International Studies*, 2025. május 15. Online: <https://yris.yira.org/column/the-weaponization-of-data-international-legal-responses-to-digital-espionage-and-state-sponsored-cyber-warfare/>
- United Nations (1945): *Charter of the United Nations and Statute of the International Court of Justice*. San Francisco: United Nations.