Hadtudományi Szemle
19. évfolyam (2026) 2. szám 19–33. • DOI: 10.32563/hsz.2026.2.2

Kovács Kinga Virág[1]

A kiberkémkedés értelmezési dilemmái a kiberműveletek környezetében

A kiberkémkedés definíciós készletének értelmezési nehézségei, 1. rész

Interpretive Dilemmas of Cyber Espionage in the Context of Cyber Operations

Interpretive Challenges in Defining Cyber Espionage, Part 1

Absztrakt

A kétrészes tanulmány első, jelen része a kiberkémkedés fogalmi és doktrinális elhelyezésének dilemmáit vizsgálja, rámutatva a kiberfelderítés, a kiberhírszerzés és a kiberkémkedés közötti átfedésekre és eltérésekre. Elemzi, hogy a kiberkémkedés, bár nem katonai fogalom, technikai megvalósítása és hatásai a katonai kiberműveletek környezetében jelennek meg, ami jelentős értelmezési bizonytalanságot teremt. A rész célja, hogy feltárja e fogalmi szürkezóna okait és megalapozza a kiberkémkedés további technikai és jogi vizsgálatát, amelyre a tanulmány második részében kerül sor a kiberkémkedés nemzetközi jogi besorolásának nehézségeinek bemutatásán keresztül.

Kulcsszavak: kiberkémkedés, kiberműveletek

Abstract

The first part of this two-part study examines the conceptual and doctrinal dilemmas surrounding cyber espionage, highlighting the overlaps and differences between cyber reconnaissance, cyber intelligence gathering, and cyber espionage. It analyses how cyber espionage, although not a military concept, is technically implemented and has effects in

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

the context of military cyber operations, which creates significant interpretative uncertainty. The aim of this section is to explore the reasons for this conceptual gray area and to lay the groundwork for further technical and legal examination of cyber espionage. The second part of the study analyses the difficulties of classifying cyber espionage under international law.

Keywords: cyber espionage, cyber operations

Bevezetés

Az államok és a fegyveres erők mindig is törekedtek arra, hogy információt szerezzenek egymásról, ami, főleg a modern hadviselésnek köszönhetően, nem bizonyul túl bonyolultnak. Az elektromágneses spektrum és a kibertér stratégiai jelentősége a hagyományos szárazföldi, tengeri, légi és űrbeli műveletek mellett mára megkérdőjelezhetetlenné vált. Az elektronikai hadviselés hagyományosan a rádió- és radarkibocsátások felderítésére, elemzésére és zavarására koncentrált, ugyanakkor a digitális hálózatok elterjedésével mindinkább összefonódik a kiberműveletekkel.

Ezzel párhuzamosan a kiberfelderítés és kiberhírszerzés, valamint a kiberkémkedés új kihívásokat hozott a katonai és jogi értelmezésben. Míg az elektronikai felderítés többnyire passzív tevékenységnek minősül, a kibertéri műveletek gyakran aktív behatolással, tartós jogosulatlan jelenléttel és adatexfiltrációval[2] járnak. Ez a sajátosság felveti a kérdést, hogy a kiberkémkedés önálló jelenségként vagy a kiberműveletek részeként értelmezendő, és hogy a jelenlegi nemzetközi jogi normák alkalmasak-e a kiberkémkedés kiberművelet részeként történő értelmezésében.

A kibertérben zajló információszerző tevékenységek fogalmi kerete sem egységes, részben a hírszerzésre vonatkozó nemzetközi normák hiánya, részben pedig a kiberműveletek és az elektronikai hadviselés konvergenciája miatt. A szakirodalomban és a közbeszédben gyakran egymás szinonimáiként jelenik meg a kiberkémkedés, a kiberfelderítés és a kiberhírszerzés, azonban ezek eltérő motivációjú, jogi és műveleti státuszú tevékenységeket jelölnek. A kiberkémkedés *(cyber espionage)* olyan rejtett, invazív információszerzés, amelyet államok, állami támogatású vagy nem állami szereplők gazdasági, politikai vagy ipari előnyszerzés céljából hajtanak végre, és amely a hagyományos értelemben vett civil kémkedés digitális kiterjesztéseként értelmezhető. Ezzel szemben a kiberfelderítés és a kiberhírszerzés a katonai műveletek szerves részei: előbbi a hálózatok technikai feltérképezését, utóbbi a többforrású adatfeldolgozást és döntéstámogatást jelenti. Bár a három tevékenység eszközrendszere jelentős mértékben átfedést mutat, a mögöttük meghúzódó célrendszer eltérő, és ez határozza meg katonai vagy nem katonai jellegüket.

Jelen tanulmány éppen ezért külön figyelmet fordít a kiberkémkedés vizsgálatára, arra a fogalmi és jogi szürkezónára, amelyben az információszerzés technikailag a kiberműveletek körébe illeszthető, ugyanakkor motivációja nem katonai, alapvetően civil kémkedésként értelmezhető, így nehezen sorolható be a hagyományos katonai

[2] Támadási módszer, amelynek során a támadók érzékeny adatokat gyűjtenek és továbbítanak saját szervereikre, az erre a célra alkalmas eszközök segítségével.

doktrinális keretek közé. A bevezető fogalmi elhatárolás célja a későbbi elemzés megalapozása, különösen annak vizsgálata során, hogy a kiberkémkedés mennyiben tekinthető a kiberműveletek részének, illetve hogyan értelmezhető a nemzetközi jog normatív rendszerében.

A tanulmány szempontjából ezért a kiberkémkedés *(cyber espionage)* fogalmat következetesen abban az értelemben használom, hogy államok, állami támogatású csoportok, hacker csoportok vagy gazdasági szereplők gazdasági, politikai, ipari vagy technikai adatokat szereznek megsértve a bizalmasságot, azzal a céllal, hogy azokat saját stratégiai, gazdasági vagy politikai érdekükben felhasználják. Ez a definíció tehát nem kifejezetten katonai kategória, hanem egy szélesebb információszerzési magatartás leírása, amely azonban a katonai kibertevékenységek operatív terében is megjelenik.

Jelen cikk célja, hogy feltárja a kiberkémkedés besorolásának értelmezési dilemmáit, különösen azt, hogy a jelenség a kiberműveletek rendszerében, illetve a katonai és nem katonai dimenziók határán miként helyezhető el. A tanulmány arra törekszik, hogy megmagyarázza, miért problematikus a kiberkémkedés terminológiai meghatározása, és az miként különül el vagy éppen mosódik össze a katonai értelemben vett kiberfelderítéssel.

Módszertan és kutatási keret

A tanulmány kvalitatív, fogalomelemzésen alapuló kutatást alkalmaz, amelynek célja a kiberkémkedés fogalmi elhelyezése és értelmezési dilemmáinak feltárása a kiberműveletek környezetében. A vizsgálat abból az alapfeltevésből indul ki, hogy a kiberkémkedésre nem létezik egységes, katonai és jogi értelemben is elfogadott definíció, ezért a jelenség értelmezése csak a rendelkezésre álló doktrinális és szakirodalmi források összevetésével vizsgálható.

A kutatás elsődleges módszere a taxatív fogalomelemzés, amely során a tanulmány vizsgálja a kiberkémkedéshez, kiberfelderítéshez és kiberhírszerzéshez kapcsolódó meghatározásokat. Az elemzés célja annak vizsgálata, hogy létezik-e koherens definíciós készlet, vagy csupán egymással részben átfedő, eltérő megközelítések azonosíthatók. Ennek keretében a fogalmak közötti azonosságokat, eltéréseket és összefüggéseket vizsgálom.

A fogalomelemzést összehasonlító elemzés egészíti ki, amelynek során a katonai doktrínákat, valamint a nemzetközi szakirodalomban megjelenő értelmezéseket vizsgáljuk. A vizsgálat nem terjed ki a magyar nemzeti doktrinális dokumentumok elemzésére, mivel azok nem képezik a tanulmány elemzési keretét, és bevonásuk a kutatás céljától eltérő lenne. Az összehasonlítás célja annak feltárása, hogy a különböző megközelítések milyen induktív következtetésekre adnak lehetőséget a kiberkémkedés széles körben elfogadható fogalmának kidolgozására.

Bár a katonai doktrínák formálisan kötelező érvényűek, gyakorlati alkalmazásuk államonként és szövetségi rendszerenként eltérő, illetve politikai és stratégiai érdekek által befolyásolt lehet. Ezen sajátosságok, bár korlátozzák a doktrínák empirikus érvényességét és gyakorlati alkalmazását, nem zárják ki fogalmi és értelmezési elemzésüket, ami jelen tanulmány fókuszában áll.

Az elektronikai hadviseléstől a kibertérig

A kiberkémkedés sajátosságainak megértéséhez nélkülözhetetlen az elektronikai hadviselés szerepének áttekintése. A kibertérben zajló kémkedés és az elektromágneses spektrumban történő felderítés között nem csupán technikai rokonság figyelhető meg, hanem műveleti kapcsolat is. Az elektromágneses spektrumból nyert információk kijelölhetik a további kibertéri felderítés irányát, míg a hálózati aktivitás megértése gyakran visszamutat a spektrális kibocsátások elemzésére. Az elektronikai hadviselés rendkívül összetett és komplex feladatokat foglal magában, amelyek sikerének kulcsa az a technikai eszközpark, amelyet folyamatosan bővíteni és fejleszteni kell, miközben figyelemmel kell kísérni a másik fél technikai fejlesztéseinek tendenciáit is.

Az elektromágneses spektrumban végzett felderítés egyik fajtája a jelfelderítés (*signal intelligence,* SIGINT), amelynek egyik része a rádiótechnikai felderítés (*electronic intelligence,* ELINT). Antennákkal, elektronikai vevőkkel és spektrumanalízissel tárják fel a rádió- és radarkibocsátásokat, azok technikai paramétereit vagy éppen operatív mintázatait. Az ELINT elsődleges célja nem a közvetlen fizikai beavatkozás, hanem a helyzetismeret, amely magába foglalja az ellenséges rendszerek azonosítását, működésük elemzését és a taktikai és stratégiai döntések alapjainak megteremtését.[3] A SIGINT-en belüli másik kategória a COMINT *(communication intelligence),* amely a kommunikációs jelek lehallgatására, elemzésére és titkosításának feltörésére összpontosít. A modern elektronikai hadviselés (*electronic warfare,* EW) három szorosan összekapcsolódó funkciót foglal magába: az elektronikai támadást (*electronic attack,* EA),[4] az elektronikai védelmet (*electronic protection,* EP) és az elektronikai támogatást (*electronic warfare support,* ES). Az ES-funkció lényegében a SIGINT/ELINT hadműveleti vetülete, amely az elektromágneses spektrumbeli észlelésre építve biztosít információkat az EA- és EP-műveletekhez.[5]

Az elektromágneses energia alkalmazásán kívül a kibertérben való műveletvégzés elengedhetetlen része a modern hadviselésnek. A katonai erők vezeték nélküli számítógépes hálózatokat használnak a műveletek koordinálására, légi és földi érzékelőkkel végzik az ellenség felderítését és helymeghatározását, rádiókat alkalmaznak a parancs- és irányítási kommunikációra, valamint elektronikai zavarással teszik nehezebbé az ellenség radarjainak és kommunikációjának működését. Mivel a harctéri kommunikációs eszközök immár szerves részét képezik a legtöbb hálózatnak, az elektromágneses spektrumon és a hálózati rétegen zajló tevékenységek funkcionálisan átfedik egymást, ezzel koherens környezetet alkotva. Ezért az elektromágneses spektrumot és a kiberteret jó ideje ugyanolyan stratégiai jelentőségűnek tekintik, mint a hagyományos szárazföldi, tengeri, légi és űrbeli műveleti területeket.[6]

Az említett kibertéri hálózatok az elektronikus rendszerekkel és az elektromágneses spektrum használatával jellemezhetők, éppen ezért a kibertéri hálózatokat

[3] Kovács 2017; Joint Chief of Staff 2012.

[4] Az EA (elektronikai támadás), EP (elektronikai védelem) és ES (elektronikai támogatás) hármas felosztása az amerikai doktrínára jellemző; más országok doktrínái az elektronikai támadást többnyire elektronikai ellentevékenység címszó alatt tárgyalják.

[5] Kovács 2017.

[6] Haig 2015.

elektronikus eszközökkel fel lehet deríteni. Technikai megvalósítását illetően ez nem is bizonyul túl bonyolultnak, azonban ennek további értelmezéséhez először is szükséges tisztáznunk a kibertér fogalmát.

Magyarország 2013-as *Nemzeti Kiberbiztonsági Stratégiá*jában a következő olvasható a kibertér Magyarországi környezete vonatkozásában:[7]

> „A kibertér globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét jelenti. Magyarország kibertere a globális kibertér elektronikus információs rendszereinek azon része, amelyek Magyarországon találhatóak, valamint a globális kibertér elektronikus rendszerein keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok közül azok, amelyek Magyarországon történnek vagy Magyarországra irányulnak, illetve amelyekben Magyarország érintett."[8]

Kovács László a kibertér fogalmát a következőképpen határozza meg: „Felhasználók, eszközök, szoftverek, folyamatok, tárolt vagy átvitel alatt lévő információk, szolgáltatások és rendszerek gyűjtőfogalma, amelyek közvetlenül vagy közvetett módon számítógép-hálózathoz vannak kapcsolva."[9] A JP 3-12 amerikai katonai doktrína következőképpen ismerteti a kibertér fogalmát: „A kibertér a globális információs környezet azon része, amely az információs technológiai infrastruktúrák és a bennük tárolt vagy továbbított adatok összességét foglalja magában. Ide tartozik az internet, a távközlési hálózatok, a számítógépes rendszerek, valamint a beágyazott processzorok és vezérlők."[10]

A definíciók együttes vizsgálata rávilágít arra a fontos következtetésre, hogy a kibertér és az elektromágneses spektrum nem két független, egymástól elzárt réteg. A fenti definíciók közös vonása, hogy mindegyik az elektronikus információs rendszerekhez, hálózatokhoz és adatátviteli infrastruktúrákhoz köti a kibertér fogalmát. Ezen rendszerek működésének fizikai alapja minden esetben az elektromágneses spektrum, akár vezeték nélküli adatátvitelről, akár vezetékes infrastruktúráról van szó, az információt pedig elektromágneses jelek hordozzák. A kibertér magasabb logikai rétegei ugyan elkülöníthetők, de technikai értelemben a kibertér és az elektromágneses spektrum egymást kölcsönösen meghatározó dimenziói a modern információs környezetnek.[11]

Ennek megfelelően a doktrínák ma már a *cyber-electromagnetic activities* (CEMA), avagy a kiber-elektromágneses műveletek fogalmát is használják arra, hogy a kibertérbeli és az elektromágneses spektrumbeli támadó, védelmi és felderítő tevékenységeket egyetlen, szinkronizált műveleti keretként kezeljék.[12]

---

[7] Bár Magyarország 2025-ben új kiberbiztonsági stratégiát fogadott el, jelen tanulmány a 2013-as stratégia kibertér-definíciójára támaszkodik, mivel az a vizsgált jelenség fogalmi kereteit ugyanolyan pontossággal fedi le.

[8] 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról, II. pont.

[9] Kovács 2018: 18.

[10] Joint Chief of Staff 2018.

[11] Joint Chief of Staff 2018.

[12] U.S. Department of the Army 2014.

A kiber-elektromágneses műveletek

Az amerikai katonai doktrinális gondolkodás felismerte, hogy a kibertér és az elektromágneses spektrum együttes kezelése jelentős operatív erőfokozó hatással bír. Ennek következményeként az Egyesült Államok Hadserege kidolgozta és 2014 februárjában közzétette az FM 3-38 *Kiber-elektromágneses tevékenységek* doktrínáját, amely a CEMA-koncepciót hivatott bemutatni. A doktrína szerint a kiber-elektromágneses tevékenységek olyan összehangolt informatikai és spektrális cselekvések összessége, amelyek célja a parancsnok műveleti előnyének kialakítása és fenntartása mind a kibertérben, mind pedig az elektromágneses spektrumban, egyidejűleg pedig az ellenség analóg képességeinek felderítése, korlátozása és gyengítése is célja.[13]

A CEMA alapvetően három komponens integrált alkalmazását írja elő. A kibertérműveleteket, az elektronikai hadviselést és az elektromágneses spektrumkezelési műveleteket. A komponensek funkcióinak és képességeinek együttes használata úgy realizálódik, hogy kiegészítő és egymást erősítő hatások jöjjenek létre. Ennek eléréséhez viszont elengedhetetlen a tevékenységek koordinációja, mivel a koordinálatlan beavatkozások kölcsönös zavarásokhoz vezethetnek mind a katonai, mind a civil elektromágnesesspektrum-használók között.[14]

Operatív szempontból a CEMA-műveletek támadó és védekező elemeket egyaránt magukba foglalnak. A támadó műveletek kettős funkciót látnak el, egyrészt felderítést és céladatgyűjtést végeznek, másrészt befolyásolják, megzavarják vagy semlegesítik az ellenfél hálózati információs és kommunikációs képességeit. A támadó tevékenységek során a felderítéshez tipikusan passzív elektromágnesesspektrum-észlelés, hálózati forgalomelemzés és végpont-telemetria szolgál, míg a behatolási és hatáskeltési fázisokban *exploitok* alkalmazása, a belső mozgások lehetőségének kihasználása a jellemző. Emellett zavaró jelek, félrevezető információk és rosszindulatú szoftverek *(malware*[15]*)* használata is szerepet kaphat az ellenség információinak módosítására, törlésére vagy a rendszerek túlterhelésére. A védekező CEMA-tevékenységek célja a baráti hálózatos információs és kommunikációs rendszerek folyamatos elérhetőségének, integritásának és működőképességének biztosítása. Ez magában foglalja a hozzáférés fenntartását, a szolgáltatások rendelkezésre állásának védelmét, a titkosítási és autentikációs intézkedések alkalmazását, valamint az elektromágneses spektrum védelmének és a védelem ütemezésének menedzsmentjét. A védelem célja nem csupán a külső behatolások megakadályozása, hanem a felderítési képesség fenntartása és a kritikus folyamatok biztonságos működtetése is.

Fontos körülhatárolni a CEMA hatókörét. A doktrína kizárólag azokat az elektronikai és információs tevékenységeket sorolja a CEMA-keretbe, amelyek a hálózatba kapcsolt információs és kommunikációs rendszerekre irányulnak, vagy azok védelmére szolgálnak. Ennek következtében bizonyos lokális, nem hálózatos elektromágneses zavarások, mint például egy egyszerű rádióvezérlésű vevő improvizált zavarása nem feltétlenül minősülnek CEMA-tevékenységnek. Ez a megkülönböztetés rávilágít arra,

[13] U.S. Department of the Army 2014.
[14] Haig 2015.
[15] *Malicious software:* rosszindulatú szoftver.

hogy a CEMA operatív jelentősége elsősorban a hálózati jelleg és az információs rendszerek közötti összekapcsoltságon alapszik.[16]

A CEMA-műveletek ismertetése jelen munka szempontjából azért releváns, mert az elektronikai felderítés során nyert elektromágnesesspektrum-információk gyakran kijelölik a további kibertéri felderítés célpontjait. Egy szokatlan kibocsátás vagy rádiós anomália alapján felismerhető egy konkrét eszköz, interfész vagy csatorna, amely sebezhetőnek tűnik, ez pedig elindíthatja a célzott hálózati vizsgálatot. Innentől a felderítés iránya és célja válik meghatározóvá. Ha elsődlegesen az adatok megszerzése a cél, más lesz a jogi és stratégiai megítélés, mint akkor, ha a cél az infrastruktúra működésének zavarása. Éppen ezért a CEMA megértése természetes átvezetést ad a kizárólag kibertéri felderítés és annak következményei vizsgálatához.[17]

Hírszerzés a kibertérben – a CEMA-műveletektől a kiberkémkedésig

A CEMA integrált szemlélete rámutat, hogy az elektromágneses spektrumban és kibertérben végzett tevékenységek operatív szinten bár összetartoznak, a jogi keret értelmezése során problémába ütközünk. Míg az elektronikai felderítés (rádiófelderítés, radarfelderítés stb.) a nemzetközi gyakorlatban ismert kategória, addig a kibertéri felderítés, a kiberhírszerzés és a kiberkémkedés fogalmi meghatározásai, ezek elhatárolásai és normatív megítélései nem egyértelműek, sokszor szürkezónában maradnak. Az elektronikai felderítés általában nem minősül támadásnak, hanem hírszerzési vagy elektronikai hadviselési műveletnek tekinthető, azonban a kibertérben történő felderítés jogi és műveleti következményei lényegesen összetettebbek. Míg a hagyományos elektronikai felderítési tevékenységek passzív jellegükből adódóan elsősorban információgyűjtésnek minősülnek, a kiberfelderítés *(cyber intelligence)* gyakran magában foglal aktív behatolást és a tartós hozzáférés fenntartását, amelyek már önmagukban is jelentős műveleti hatásúak lehetnek, és amelyek átvezethetnek a jogi minősítés szintjén egy másik kategóriába. A kérdéskör további vizsgálatához szükséges a kiberfelderítés, kiberhírszerzés és kiberkémkedés fogalmi koncepciói esetében felmerülő kérdések tisztázása.

A kibertéri felderítés és a kiberhírszerzés a gyakorlatban ugyanazt a tevékenységi kört fedik le, hiszen mindkettő a kibertérben végzett információszerző műveletek összességét jelenti. Ugyanakkor nem tekinthetők szinonim fogalmaknak, mivel eltérő műveleti szinteken és célrendszerben jelennek meg. A felderítés elsősorban a taktikai adatgyűjtést, a hálózatok és rendszerek technikai feltérképezését jelenti, míg a hírszerzés az így megszerzett adatok feldolgozását, elemzését és felhasználását stratégiai döntéstámogatásra foglalja magában. Másképpen úgy is nevezhetjük, hogy a felderítés a hírszerzés része, annak adatgyűjtő fázisa, míg a hírszerzés az egész folyamatot jelenti az adatok megszerzésétől azok értelmezéséig.[18]

[16] Haig 2015.
[17] U.S. Department of the Army 2014.
[18] Vida 2013.

A kiberkémkedés *(cyber espionage)* a fenti két fogalomtól részben vagy teljesen különálló kategória, amelynek nincs egységes, katonai értelemben elfogadott definíciója. A jelenség eredetileg az ipari és politikai kémkedésből nőtt ki, és nem tartozik a katonai doktrínákban meghatározott kiberműveleti formák közé. Míg a kiberfelderítés *(cyber intelligence)* a NATO által is elismert és definiált hírszerzési tevékenység, addig a kiberkémkedés *(cyber espionage)* alapvetően civil és politikai célú információszerző magatartás, amelyet a közbeszédben és a médiában gyakran pontatlanul vagy túlzóan alkalmaznak, a katonai tevékenységekkel valójában nincs közvetlen kapcsolata. A kiberkémkedés lényege a rejtett, invazív információszerzés, amely során jogosulatlan behatolás történik informatikai rendszerekbe, és az adatokat titokban gyűjtik, módosítják vagy szivárogtatják, jellemzően úgy, hogy a tevékenység ne legyen visszakövethető az elkövető államra vagy szervezetre.

A *cyber intelligence* fogalom magába foglalja mindazt, amit a katonai terminológiában felderítésnek nevezünk, azonban ez több szinten értelmezhető. A legmagasabb szintet az *intelligence* jelenti, amely hadászati, stratégiai szinten támogatja a döntéshozatalt. Ezt követi a *surveillance,* amely hadműveleti szintű információgyűjtést takar, végül a *reconnaissance* a legalacsonyabb, harcászati szintet képviseli, és a konkrét adatgyűjtést jelenti. E három szint együtt alkotja a kibertéri hírszerzés hierarchiáját. Az *espionage* tágabb értelemben mindhárom tevékenységi szintet lefedheti, ugyanakkor a katonai értelemben vett felderítésre is igaz ugyanez: mindkettő információszerzés, csupán más kontextusban és jogi státuszban. Kiberfelderítés a kibertérben zajló információszerzés és -feldolgozás teljes folyamata, ami katonai, míg a kiberkémkedés az ipari és politikai kémkedés digitális kiterjesztése, technikailag hasonló módszereket alkalmaz, de céljában, valamint jogi és műveleti szempontból is eltér a katonai hírszerzés rendszerétől.

A kiberfelderítés és a kiberhírszerzés közötti különbség alapvetően céljaik, módszereik és eredményeik jellege alapján érthető meg a leginkább. A felderítés alapvetően taktikai tevékenység, és közvetlenül támogatja a katonai műveleteket. Ez magában foglalja az adott hálózat, rendszer vagy infrastruktúra működésével, sebezhetőségeivel és erőforrásaival kapcsolatos nyers adatok megszerzését. A felderítés eredménye általában technikai információ, például a hálózat topológiája, az azonosított eszközök, a futó szolgáltatások és a sebezhető pontok. Ez az ismeret közvetlenül felhasználható támadó vagy védekező műveletek tervezéséhez és végrehajtásához egyaránt.

Ezzel szemben a kiberhírszerzés szélesebb körű folyamat, amelyet stratégiai és operatív szinten értelmeznek, és amely nem áll meg pusztán az információgyűjtésnél. A hírszerzés magába foglalja a különböző forrásokból származó adatok integrálását, feldolgozását és elemzését, függetlenül attól, hogy azok nyílt vagy titkos csatornákból származnak. A cél itt nemcsak a technikai sebezhetőségek azonosítása, hanem az ellenfél szándékainak, képességeinek és lehetséges cselekedetei átfogó képének meghatározása is, ezzel támogatva a stratégiai döntéshozatalt.

Időkeret tekintetében is figyelhetünk meg különbséget. Míg a felderítés gyakran rövid távú és előkészítő jellegű, a hírszerzés folyamatos, tartós tevékenység, amely képes azonosítani a trendeket és előre jelezni a fenyegetéseket. Módszertani szempontból a felderítés főként technikai eszközökre támaszkodik, mint például a hálózati szkennelés vagy a szolgáltatások azonosítása, míg a hírszerzés analitikai munkát,

forráskritikát és több tudományág bevonását is igényli. A felderítés eredménye nyers adat, míg a hírszerzés terméke egy értelmezett, kontextusba helyezett információ.

Szervezeti szinten a felderítés általában a katonai, operatív szintű egységek feladata, míg a hírszerzés intézményesített, állami keretek között működik, gyakran több szervezet együttműködésével. A két fogalom közötti egyértelmű megkülönböztetés fontos, mert a kiberműveletek sikere attól függ, hogy a felderítésből nyert nyers információkat megfelelően használják-e fel a hírszerzési elemzési és értékelési folyamatok során.[19]

A kiberhírszerzés felfogható az „összes forrásból származó" hírszerzésként, amelybe ugyanúgy beletartozik a nyílt forrásokból elérhető és a zárt (védett) számítógépes hálózatokban lévő információk összegyűjtése.[20]

Amikor fogalmat szeretnénk találni a kiberkémkedésre, nehézségekbe ütközünk, mivel a fentiekben leírtaknak megfelelően nem létezik egységes, mindenki által elfogadott definíció. A leginkább úgy írható körbe, mint rejtett, kibereszközökkel (jellemzően rosszindulatú szoftverekkel és célzott behatolási technikákkal) végzett információszerző tevékenység, amelynek célja az adatok megszerzése vagy módosítása, technológiák és szellemi tulajdon eltulajdonítása, a kritikus infrastruktúrák feltérképezése vagy megzavarása, illetve helyzetismeret szerzése az ellenfél szándékairól. A műveletek során gyakran a kriptográfiai védelem megkerülésére törekednek a végpontok kompromittálásával és az adatexfiltrációval.[21]

A kiberkémkedés fogalmi, valamint a végrehajtását lehetővé tevő technikák vizsgálata rámutat bizonyos definíciós korlátokra. Pusztán egy megközelítés alapján nehezen sorolható be egyértelműen a kiberműveletek közé, mindazonáltal a jelenség összetettsége messze túlmutat azon, hogy pusztán a kibertámadás fogalma alapján kategorizáljuk. A jogosulatlan behatolás, az információk megszerzése és a bizalmasság sérelme ugyan technikailag jól leírható folyamatok, ám ezek megítélése a nemzetközi jog, a katonai doktrínák és az állami stratégiák szintjén eltérő. Egyes megközelítések szerint a kiberkémkedés a kiberműveletek hírszerzési dimenziójához tartozik, míg más értelmezések szerint önálló, a politikai és katonai célrendszerek határán elhelyezkedő tevékenység. Ebből fakadóan a kiberkémkedés értelmezése nem csupán műveleti vagy technológiai kérdés, hanem nemzetközi szinten is jelentős stratégiai és jogi dilemma, amelyet a különböző országok és szövetségek doktrinális felfogásai alapvetően befolyásolnak, ezzel nehezítve az egységes definíciós készlet megteremtését.

A kiberkémkedés a szűk értelemben vett katonai doktrínák szerint nem tekinthető önálló kiberműveleti kategóriának, mégis elengedhetetlen, hogy katonai kontextusban vizsgáljuk, hiszen alapvetően a kiberkémkedés célja és motivációja határozza meg kiberműveleti besorolásának lehetőségét. Ennek oka, hogy technikai megvalósítása, célpontjai és hatásai a katonai kiberműveletekével azonos környezetben jelennek meg, így a két jelenség közötti határ gyakorlati értelemben elmosódik. A kiberkémkedés ugyan formálisan nem katonai tevékenység, közvetlenül befolyásolhatja a hadműveleti helyzetismeretet, a döntéshozatalt és a stratégiai célokat is, ezért katonai szempontú vizsgálata is indokolt. (Az eddigiek összefoglalásaként lásd az 1. táblázatot.)

[19] Deák 2023.
[20] Szeleczki 2022.
[21] Civuli et al. 2022.

1. táblázat: A kiberfelderítés, a kiberhírszerzés és a kiberkémkedés fogalmi összehasonlítása

	Kiberfelderítés	**Kiberhírszerzés**	**Kiberkémkedés**
Cél	Hálózatok és rendszerek technikai feltérképezése	Adatok feldolgozása, elemzése és döntéstámogatás	Gazdasági, politikai, ipari vagy technikai adatok megszerzése
Jelleg	Taktikai adatgyűjtés	Stratégiai és operatív szintű folyamat	Rejtett, invazív információszerzés
Műveleti szint	Harcászati	Hadműveleti és hadászati	Nem katonai, politikai és gazdasági célrendszer
Időtáv	Rövid távú, előkészítő jellegű	Folyamatos, tartós tevékenység	Tartós jogosulatlan jelenlét
Eredmény jellege	Nyers technikai információ	Értelmezett, kontextusba helyezett információ	Bizalmasság megsértése, információ eltulajdonítása
Jogi megítélés	Hírszerzési tevékenységként értelmezett	Normatív keretek között működő	Szürkezónában elhelyezkedő

Forrás: a szerző szerkesztése

A kiberkémkedés nemzetközi fogalomértelmezési dilemmái

A klasszikus kémkedéshez hasonlóan a kiberkémkedés is a mindent viszünk, de semmit sem vallunk be logikáján alapul – mindenki információt akar szerezni a másikról, de senki nem akarja, hogy róla szerezzenek információt –, ami a hallgatólagos elfogadás normáját hozza létre. Ez a kettősség magyarázza, hogy a kiberkémkedés sem nem tiltott, sem nem legitimált formában jelenik meg a nemzetközi térben.

Ezen kettősség következtében a kiberkémkedés olyan értelmezési térben helyezkedik el, amely a klasszikus hírszerzési tevékenységek és a nyílt kibertámadások között húzódik meg, és amelyet a szakirodalom gyakran „szürkezónaként" ír le. A szürkezónát azok a küszöb alatti műveletek jellemzik, amelyek nem idéznek elő közvetlen romboló hatást, ugyanakkor technikai megvalósításuk és műveleti környezetük alapján egy későbbi kibertámadás előkészítéseként is értelmezhetők. A kiberkémkedés ebben az esetben a célrendszer és a kiváltott hatás függvényében változó jogi és stratégiai megítélésű tevékenységként jelenik meg.[22]

A kiberkémkedés legnagyobb dilemmája éppen ebből fakad, hiszen míg technikai értelemben a kiberműveletek eszköztárába sorolható, politikai és stratégiai szinten inkább a hírszerzési gyakorlat kiterjesztéseként értelmezhető. A hagyományos kémkedéshez képest azonban a kiberkémkedés léptéke, sebessége és célrendszere radikálisan eltérő. A kibertérben zajló műveletek nem korlátozódnak személyekre, fizikai helyekre vagy intézményekre, hanem globális hálózatokon keresztül érik el a céljaikat, gyakran anélkül, hogy az elkövető vagy a célpont tudatában lenne a műveletnek. Ezt az *advanced persistent threat* (APT) műveletekkel érik el, ami a kiberkémkedés egyik leggyakoribb

[22] Stoddart 2024.

technikája.[23] Ez alapjaiban kérdőjelezi meg, hogy a hagyományos hírszerzési normák és elrettentési mechanizmusok mennyiben alkalmazhatók ebben a környezetben.

A normatív problémák egyik legfontosabb eleme, hogy a kiberkémkedés következményei nem mindig különíthetők el a kibertámadásoktól. Egy rosszindulatú kód bejuttatása, amelyet információszerzésre terveztek, műszakilag gyakran azonos egy támadó kódéval. A célrendszer szempontjából mindkettő jogosulatlan behatolást, a bizalmasság sérelmét és a rendszer integritásának kockázatát jelenti. Libicki szerint ebből fakad a legnagyobb stratégiai paradoxon: a kiberkémkedés az észlelő fél szemszögéből sokszor felkészülésnek tűnik egy kibertámadásra, így a puszta információszerzés is feszültséget generálhat, vagy akár válaszlépést válthat ki.[24]

A nemzetközi jog hagyományos keretei nehezen kezelik ezt a szürkezónát. Mivel a kiberkémkedés nem okoz közvetlen, mérhető fizikai kárt, az ENSZ Alapokmány szerinti erőalkalmazás kategóriájába sem sorolható be. Ugyanakkor a szuverenitás sérelmét mégis megvalósíthatja, ha a behatolás az állami rendszerekbe vagy kritikus infrastruktúrákba irányul. Libicki szerint éppen ez a kettősség akadályozza a nemzetközi normák kialakulását, hiszen az államok egyszerre igyekeznek elítélni a kiberkémkedést, miközben maguk is alkalmazzák azt, így nincs közös érdek a szabályozásban. Az elméleti jogi térben a „kibertér semlegessége" és a „szuverén információs terek" közötti egyensúly megteremtése maradt a legnagyobb kihívás.[25]

A kiberkémkedés fogalmi meghatározásának és normáinak kialakulását többek között három fő tényező gátolja. Az első a technikai átláthatatlanság, ami megnehezíti a bizonyítható attribúciót,[26] így a felelősségre vonás politikailag kockázatosnak, jogilag pedig bizonytalannak tekinthető. A második a kölcsönös haszon elve, vagyis hogy minden állam profitál a kiberkémkedésből, amennyiben az információszerzés saját biztonsági érdekeit szolgálja. A harmadik a kölcsönös sérülékenység, mivel minden modern állam kiber-infrastruktúrája sebezhető, az általános tiltás bevezetése ellentétes lenne a saját hírszerzési érdekeikkel. Ez a három tényező eredményezi azt, hogy a kiberkémkedés elfogadott, de nem legitimált, bár ismert, de nem nevesített gyakorlat. Ebből fakadóan a kiberkémkedés értelmezése ma inkább stratégiai, mint jogi kérdés. Ezt az értelmezést empirikus kutatások is alátámasztják, amelyek szerint a kiberkémkedés nem elszigetelt vagy esetleges jelenség, hanem jól körülhatárolható állami szereplők között, stratégiai racionalitás mentén zajló gyakorlat. Az államok viselkedését nem a kodifikált normák, hanem a politikai célok és motivációk határozzák meg. A kölcsönös tűrés politikája egyfajta hallgatólagos egyensúlyt hozott létre, amelyben a kiberkémkedés mindaddig elfogadhatónak tekinthető, amíg nem vált ki közvetlen politikai vagy gazdasági következményt. Ez a gyakorlat azonban instabil,

[23] Az *advanced persistent threat* (APT) olyan célzott, hosszú távon fenntartott kiberműveleti tevékenységet jelöl, amelyet jellemzően állami vagy állami támogatású szereplők hajtanak végre elsősorban információszerzési céllal. A Mandiant APT1-jelentése szerint az APT-k működésére a tartós jelenlét, a célzott behatolás, a magas szintű szervezettség, valamint az adatok rejtett és folyamatos exfiltrációja jellemző, amelyek megkülönböztetik őket az opportunista vagy rövid távú kibertámadásoktól. Az APT-tevékenységek elsődleges célja nem a közvetlen romboló hatás kiváltása, hanem érzékeny politikai, gazdasági, katonai vagy technológiai információk megszerzése, ami a kiberkémkedés tipikus megnyilvánulási formájává teszi őket.

[24] Libicki 2017.

[25] Libicki 2017.

[26] Az attribúció az elkövető bizonyíthatóságát és megnevezését jelenti.

hiszen egyetlen félreértelmezett művelet, különösen katonai rendszerek ellen, elegendő lehet ahhoz, hogy a kiberkémkedést egy támadás előfutáraként értékeljék.[27]

Ebben a szürkezónában a nemzetközi jogi értelmezés elsősorban értelmezési keretként, nem pedig egyértelmű tiltásként jelenik meg. A *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* a kiberkémkedést önmagában nem tekinti nemzetközi jogba ütköző tevékenységnek, ugyanakkor hangsúlyozza, hogy az ilyen műveletek bizonyos körülmények között sérthetik az állami szuverenitást, illetve felvethetik a beavatkozás tilalmának és az állami felelősségnek a kérdését. A jogi megítélés így nem az információszerzés tényéhez, hanem annak módjához, intenzitásához és hatásához kötődik. Ez a megközelítés összhangban áll azzal a gyakorlattal, amely szerint a kiberkémkedés jogi megítélése a különböző esetekben politikai és stratégiai kontextusban dől el.[28] Empirikus kutatások is alátámasztják, hogy a kiberkémkedés nem elszigetelt vagy esetleges jelenség, hanem jól körülhatárolható állami szereplők között, stratégiai racionalitás mentén zajló gyakorlat.[29]

Nemzeti megközelítések a kiberkémkedés értelmezésében

A kiberkémkedés körüli normatív bizonytalanságot továbbá az is magyarázza, hogy az államok saját biztonsági érdekeik alapján értelmezik a jelenséget. A nemzetközi konszenzus hiánya így nem pusztán jogi, hanem politikai probléma is, hiszen minden állam más határvonalat húz a hírszerzés és a támadás között a kibertérben. Az alábbi példák jól mutatják, miként testesül meg ez a probléma az egyes nemzeti doktrínákban.

Az elmúlt években az Egyesült Államok a hozzá hasonló gondolkodású országokkal együtt jelezte, hogy nem tart minden kiberkémkedést elfogadható állami magatartásnak. Az USA 2010 eleje óta panaszkodik a kínai ipari kiberkémkedésre, ennek okán a 2023-as védelmi kiberstratégiájuk már nem tekinti egyértelműen csak hírszerzési tevékenységnek a kiberkémkedést. A dokumentum szerint a Kínai Népköztársaság széles körű és kiterjedt kiberkémkedési fenyegetést jelent, amely a háborúra való felkészülést szolgálja. A Pentagon értelmezése szerint a kiberkémkedés, különösen abban az esetben, ha a katonai logisztikai, ipari vagy kritikus infrastruktúrákat célozza, a kiberműveletek előkészítő szakaszának tekinthető. Ez a megközelítés elmozdulást jelent a korábbi, hírszerzéscentrikus felfogástól, amely szerint a kiberkémkedés a 2023-as amerikai doktrínában a fenyegetés és az agresszió kontinuumán helyezkedik el, ahol a határ a hírszerzés és a támadás között dinamikusan változik.[30]

Libicki (2017) szintén a kiberkémkedés normatív dilemmáinak egyik legjellemzőbb példájaként említi Kínát. Értelmezése szerint a kínai gyakorlat a klasszikus hírszerzési normák határát feszegeti azzal, hogy a kiberkémkedést gazdasági célokra is alkalmazza. Ezzel Kína túllép azon a hallgatólagos nemzetközi megállapodáson, amely a katonai hírszerzést tűrt, az ipari kémkedést viszont tiltott tevékenységként kezeli. Ugyanakkor Peking saját műveleteit az információs szuverenitás és nemzeti stabilitás védelmeként

[27] Libicki 2017.
[28] Schmitt 2017.
[29] Akoto 2024.
[30] U.S Department of Defense 2023.

értelmezi, így a nemzetközi jogi diskurzusban nem normaszegőként, hanem eltérő normarendszerben eljáró szereplőként jelenik meg. A kiberkémkedés globális szabályozását is éppen az ilyen eltérő, önmagát igazoló nemzeti értelmezések akadályozzák.[31]

Oroszország jogi megközelítése a kiberszuverenitás elvén alapul, amely a kiberkémkedést a szuverenitás sérelmeként értelmezi. Az orosz információbiztonsági doktrína (*Doctrine of Information Security,* 2016) is kimondja, hogy az állami információs rendszerekbe való jogosulatlan behatolás az állami szuverenitás és biztonság elleni cselekménynek minősül.[32] Ez a felfogás élesen eltér a tűrési megközelítéstől. Amíg Oroszország tiltani igyekszik a kiberkémkedést a szuverenitás védelmében, addig a nyugati államok a hírszerzési érdekek miatt fenntartják a *status quót.* A két felfogás közti szakadék a normatív konvergencia kialakulását tovább nehezíti.

Az Egyesült Államok, Kína és Oroszország példái egyértelműen mutatják, hogy a kiberkémkedés normatív megítélése továbbra is az állami érdekek függvénye. Az Egyesült Államok a kiberkémkedést a kibertámadások előszobájaként kezeli, míg Kína a tevékenységet az információs szuverenitás védelmeként, Oroszország pedig a szuverenitás elleni cselekményként értelmezi. Ez a három nézőpont jól szemlélteti Libicki (2017) alapvető megállapítását is, amely szerint a kiberkémkedés normarendszere nem egységesül, hanem többpólusúvá válik. A fogalom jogi és politikai jelentése így államonként eltérő lehet, a nemzetközi jog pedig nem tud olyan közös nevezőt ajánlani, amely egyszerre felelne meg a szabályozási elvárásoknak. Következésképp a kiberkémkedés a nemzetközi rend tűrt, de nem legitimált műveleti formája marad, amelyet a stratégiai érdekek, nem pedig a jogi normák szabályoznak.

Következtetések

A tanulmány első része rámutatott, hogy a kiberkémkedés fogalmi elhelyezése a kibertéri információszerző tevékenységek rendszerében továbbra is alapvetően tisztázatlan. A kiberfelderítés, a kiberhírszerzés és a kiberkémkedés közötti átfedések, valamint az a tény, hogy a kiberkémkedés technikai eszköztára gyakorlatilag azonos a katonai kiberműveletekével, azt eredményezi, hogy a jelenséget stratégiai szempontból érdemes jelen keretek között vizsgálni. Bár a kiberkémkedés nem katonai fogalom, motivációi jellemzően gazdasági, politikai vagy ipari célokhoz kötődnek, mégis olyan műveleti környezetben zajlik, ahol a katonai és nem katonai dimenziók összefonódnak. Ennek következtében a kiberkémkedés stratégiai szinten akár olyan hatást is kiválthat, mint egy katonai értelemben vett felderítési tevékenység.

A fogalmi bizonytalanságot tovább mélyíti, hogy a kiberkémkedés olyan definíciós térben helyezkedik el, amelyet sem a hírszerzésre vonatkozó normák, sem a kiberműveleti doktrínák nem rendeznek egyértelműen. A tevékenység formális jogi státusza éppúgy tisztázatlan, mint operatív besorolása, hiszen technikailag a kibertámadásokkal azonos megoldásokat alkalmaz, ugyanakkor elsődleges célja nem a rombolás, hanem a bizalmasság megsértése és az információhoz való tartós hozzáférés

[31] Libicki 2017.
[32] Russian Federation 2016.

biztosítása. A kiberkémkedés ezért nem sorolható egyértelműen sem a felderítéshez, sem a támadó kiberműveletekhez, ami jól tükrözi azt a fogalmi szürkezónát, amely a jelenség körül kialakult.

Mindennek következménye, hogy a kiberkémkedés mélyebb megértése megköveteli a technikai, műveleti és jogi keretek együttes vizsgálatát is. A fogalmi tisztázás ugyanis nem csupán elméleti kérdés, hanem önmagában meghatározza, miként értelmezhetők a jogosulatlan behatolás, a tartós jelenlét, a bizalmasság sérelme vagy az adat mint stratégiai erőforrás megszerzésének kérdésköre. A másik fél szemszögéből egy kiberkémkedési művelet gyakran éppúgy értelmezhető kibertámadás előfutáraként, mint önálló információszerző cselekményként, ami a műveleti besorolást és a stratégiai reakciót egyaránt bizonytalanná teszi.

Ezek a fogalmi eredmények arra mutatnak rá, hogy a kiberfelderítés, a kiberhírszerzés és a kiberkémkedés ugyanazon technikai környezetben megvalósuló, de eltérő célrendszerrel és értelmezési kerettel rendelkező tevékenységek, amelyek között nem húzható éles határ. A vizsgálat doktrinális következtetései szerint a kiberkémkedés technikai értelemben a kiberműveletek eszköztárába illeszkedik, politikai és stratégiai szinten azonban továbbra is a hírszerzési gyakorlat kiterjesztéseként értelmezhető, ami hozzájárul jogi besorolásának további bizonytalanságához.

Mindez egyúttal rámutat a nyitva maradó kérdésekre is, különösen az attribúció problematikájára, az eszkalációs kockázatok kezelésére, valamint arra, hogy a jelenlegi doktrinális és jogi keretek mennyiben képesek kezelni a katonai rendszerek ellen irányuló kiberkémkedési tevékenységeket.

A fogalmi és koncepcionális dilemmák adják meg a kiindulópontot a tanulmány második részéhez, amely már a kiberkémkedés technikai és jogi sajátosságait, valamint a nemzetközi jogi besorolás nehézségeit vizsgálja. A következő elemzés arra keresi a választ, hogy a jogosulatlan behatolás, a CIA-triád sérelme és az adat mint műveleti célpont miként értelmezhető a kiberműveletek rendszerében, és milyen feltételek mellett tekinthető a kiberkémkedés a nemzetközi jog szerint kiberműveletnek, illetve milyen mértékben minősül küszöb alatti, de stratégiai következményekkel járó beavatkozásnak.

Felhasznált irodalom

1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról.

Akoto, William (2024): Who Spies on Whom? Unravelling the Puzzle of State-Sponsored Cyber Economic Espionage. *Journal of Peace Research,* 61(1), 59–71. Online: https://doi.org/10.1177/00223433231214417

Civuli, Abdulla et al. (2022): Cyber Espionage Consequences as a Growing Threat. *Journal of Natural Sciences and Mathematics of UT,* 7, 13–20. Online: https://sites.google.com/unite.edu.mk/jnsm/vol-7-no-13-14-2022?authuser=0

Deák Veronika (2023): Hírszerzés a kibertérben. In Krasznay Csaba (szerk.): *Taktikák és stratégiák a kiberhadviselésben.* Budapest: Ludovika, 87–114. Online: https://doi.org/10.36250/01079_04

Haig, Zsolt (2015): Electronic Warfare in Cyberspace. *Security and Defence Quarterly,* 7(2), 22–35. Online: https://doi.org/10.5604/23008741.1189275
Joint Chief of Staff (2012): JP 3-13.1. *Electronic Warfare.*
Joint Chief of Staff (2018): JP 3-12. *Cyberspace Operations.*
Kovács László (2017): Az elektronikai hadviselés jelene és lehetséges jövője. *Hadmérnök,* 12(1), 213–232. Online: http://hadmernok.hu/171_17_kovacs.pdf
Kovács László (2018): *A kibertér védelme.* Budapest: Dialóg Campus. Online: www.uni-nke.hu/document/uni-nke-hu/Kov%C3%A1cs%20L%C3%A1szl%C3%B3.pdf
Libicki, Martin (2017): The Coming of Cyber Espionage Norms. *Strategic Studies Quarterly,* 11(2), 10–27. Online: https://doi.org/10.23919/CYCON.2017.8240325
Mandiant (2013): *APT1: Exposing One of China's Cyber Espionage Units.* Mandiant Intelligence Center Report. Online: https://services.google.com/fh/files/misc/mandiant-apt1-report.pdf
Russian Federation (2016): *Doctrine of Information Security of the Russian Federation.* Online: www.scrf.gov.ru/security/information/DIB_engl/
Schmitt, Michael (2017): *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press. Online: https://doi.org/10.1017/9781316822524
Stoddart, Kristan (2024): Russia's Cyber Campaigns and the Ukraine War: From the 'Gray Zone' to the 'Red Zone'. *Applied Cybersecurity & Internet Governance,* 3(1), 5–33. Online: https://doi.org/10.60097/ACIG/189358
Szeleczki Szilveszter (2022): A kiberhírszerzés értelmezése és helye a nemzetbiztonságban. *Nemzetbiztonsági Szemle,* 10(4), 17–29. Online: https://doi.org/10.32561/nsz.2022.4.2
U.S Department of Defense (2023): *Cyber Strategy of The Department of Defense, Summary.* Online: https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.pdf
U.S. Department of the Army (2014): *Field Manual 3-38: Cyber Electromagnetic Activities*. Washington, DC: Headquarters, Department of the Army. Online: https://irp.fas.org/doddir/army/fm3-38.pdf
Vida Csaba (2013): Létezik-e még a hírszerzési ciklus? (Miről szól a hírszerzés?) *Felderítő Szemle,* 12(1), 43–57. Online: https://hhk.uni-nke.hu/document/hhk-uni-nke-hu/2013-1.pdf