Mártonffy Balázs[1]

Bevezetés a kiberdiplomáciába: alapfogalmak és elméleti viták

„A kibertér és a hozzá kapcsolódó fogalmak esetében nem kérdéses, hogy […] távol állunk az együttműködéshez szükséges mértékű egységes értelmezéstől. Ez részben a »kiber« jelzővel jellemezhető fogalmi rendszer viszonylagos újdonságából, részben az általa leírt dolgok, jelenségek, objektumok napjainkban is tapasztalható változásaiból következik."[2]

Ahogy fentebb dr. Munk Sándor, a Nemzeti Közszolgálati Egyetem egyetemi tanára is írja, a kibervilágban, és azon belül is a kiberdiplomácia világában való hatékony navigációhoz 2020 derekán még nincs kellő muníciónk. E fejezet ezen szeretne változtatni, vagy legalábbis iránymutatást adni az olvasónak, hogy az egyet nem értések és vitapontok területén el tudjon igazodni. Így e fejezet általános bevezetést nyújt a kiberdiplomácia és részben a kiberbiztonság világába.

Írásom célja, hogy bemutassam, hogyan lehet a kiberdiplomáciát koncepcionálisan értelmezni, valamint hogy hogyan alkalmazzák a fogalmat a szakpolitikákban és a tudományos szaklapokban. Megjegyzendő, hogy a kiberdiplomácia viszonylag új fogalom a nemzetközi kapcsolatok világában. Valamivel elterjedtebb ugyan a médiában, de ott sokszor túl tág fogalomként, valamint pontatlan meghatározásokkal együttesen használják. Így e fejezetben fontos tisztázni néhány kulcsfontosságú kifejezést a kiberdiplomácia megismeréséhez és megértéséhez.

Amikor a kibervilág kérdéseire és különösen a kiberdiplomáciára gondolunk, kiemelten fontos az alapfogalmak tisztázása. Általánosságban elmondható, hogy a *kiber-* előtag a számítógépes és az elektromágneses spektrumhoz kapcsolódó tevékenységekhez köthető dolgokra utal. Ezek a fogalmak magukban foglalják

[1] A szerző szeretne köszönetet mondani Urbanovics Annának, a Nemzeti Közszolgálati Egyetem hallgatójának, a kutatómunkában nyújtott segítségért.

[2] Munk Sándor: A kibertér fogalmának egyes, az egységes értelmezést biztosító kérdései. *Hadtudomány,* 28. (2018), 1. 114.

https://doi.org/10.36250/01008_01

többek között a hálózatba kapcsolt számítógépeket, az internetet, valamint az intranetet, a mobiltechnológiákat, az optikai kábeleket és a szatelliten történő kommunikációkat is. Fontos ugyanakkor kiemelni, hogy a kibertérnek van egy fizikaiinfrastruktúra-rétege is, amely alátámasztja a kiberteret. De ahogy Joseph Nye amerikai professzor is írja, a kibertér önmaga nem pusztán ez a fizikai infrastruktúra, hanem az infrastruktúra által létrehozott tér is.[3] A tér ez esetben a kibertér, a kiberdiplomácia helyszíne.

Alapfogalmak a kibervilágban

A *kiber* mint kifejezés a 21. században élőknek nem ismeretlen.[4] Így valószínűleg kötetünk olvasója is tisztában van azzal, hogy a kifejezés valamilyen módon a számítógépek kultúrájára, az információs technológiára és a virtuális valóságra utal. A kifejezést azonban gyakran összekeverik vagy szinonimaként használják az *e-,* a *virtuális* és *digitális* fogalmakkal, pedig valójában mást értünk mindegyik alatt. Érdekes felvetés továbbá, hogy miért beszélünk például virtuális, elektronikus vagy digitális bűnözés helyett a kiberbűnözésről? Valamint érdemes megvizsgálni, hogyan kapcsolódnak egymáshoz ezek a hasonló, ámde különböző kifejezések. Érdemes feltenni azt a kérdést is, hogy miért épp *kiber*diplomáciáról beszélünk, valamint hogy pontosan mi a különbség a kiberdiplomácia és a digitális diplomácia között. Összességében tehát fontos különbséget tenni a szavak között, amit lejjebb egy rövid áttekintésben meg is teszek.

A *kiber-* előtag etimológiája az ókori görög „kormányzás" szóhoz vezethető vissza, de a napjaink modern társadalmában használt fogalmat Norbert Weiner *Kibernetika* című könyvéhez tudjuk kötni.[5] A *kíber-* előtag fokozott használata, nem meglepően, követi az internet elterjedését. A 21. század elején négy fogalmat különböztetünk meg egymástól, amelyek hasonló, de mégis jól elválasztható témákra utalnak:

[3] Joseph S. Nye, Jr.: Cyber Power. *The Belfer Center for Science and Internaitonal Affairs, Harvard University*, 2010. 3.

[4] Jelenleg magyar szövegekben mind a *kiber-,* mind a *kíber-* előtag, rövid, illetve hosszú í-vel is, használatos. Itt konzekvensen a *kiber*t – rövid i-vel – használom.

[5] Weiner Norbert: *Cybernetics: Or Control and Communication in the Animal and the Machine.* Paris, Hermann & Cie & Camb. Mass. (MIT Press), második, javított kiadás, 1961.

- a *kibernetika* és a *kiber*- előtag elsősorban a biztonsági kérdésekre,
- az *e*- vagy *elektronikus* előtagok a gazdaság különböző területeire,
- a *digitális* szó leginkább a vállalati és az állami szektorra utal, illetve itt használják, míg végül
- a *virtuális* kifejezést, amely húsz évvel ezelőtt még szinte szinonimája volt a másik háromnak, mára gyakorlatilag elhagytuk a társfogalmak közül, és inkább más, *VR – virtuális valóság* alapú eszközökre és valóságokra utalva használjuk.

Mivel a *kiber*- előtagról és a *kiber* fogalmakról mint a kiberdiplomáciában leginkább elterjedtekről sok szó fog esni még a fejezetben, így itt a másik hármat mutatom be.

Az *e*- az „elektronikus" szó rövidítése. Először az e-kereskedelem elterjedése révén került be a mindennapi használatba, leginkább mint az interneten alapuló kereskedelem egyik első meghatározása. A kezdeti időszakokban, például az Európai Unió (EU) lisszaboni (2000) és az Egyesült Nemzetek Szervezete (ENSZ) által szponzorált Információs Társadalom Csúcstalálkozón (World Summit on the Information Society, WSIS) közzétett nyilatkozatokban is (Genf 2003; Tunisz 2005) az *e*- volt a leggyakrabban használt előtag. Az Információs Társadalom Csúcstalálkozókon meghatározott feladatok és javaslatok olyan cselekvési irányokat adtak meg, amelyek az e-kormányzás, az e-üzlet, az e-tanulás, az e-egészségügy, az e-foglalkoztatás, az e-mezőgazdaság és az e-tudomány területein szerettek volna haladást elérni. Az *e-diplomácia* fogalmát nemzetközi szinten 2007 óta használjuk, amikor a svéd diplomácia felállította az első „virtuális" e-nagykövetségeket.[6] A kezdeti lelkesedés ellenére mára már az *e*- mint jelző egyre kisebb mértékben van jelen. Nemrégiben még az Európai Unió is elkezdett felhagyni az *e*- előtag használatával. Egyes értelmezések szerint ez azzal is magyarázható, hogy távolodni a próbál a lisszaboni menetrend kudarcától.

A digitális előtag az 1-re és a 0-ra utal. A nulla és az egyes a számítógépes kódok alapjai, azok a számjegyek, amelyek mint bináris változók az egész internetes világ alapját képezik. A múltban a digitális előtagot a digitális technika leírása mellett főként a nemzetközi fejlesztési körökben használták, leginkábbis a „digitális szakadék" ábrázolásaként. Az elmúlt néhány évben a digitalizálás nevű folyamat megkezdte az internet nyelvének meghódítását is, és beépült

[6] Molnár Dóra: *Törékeny nagyhatalmiság: a kiberbiztonság.* Budapest, Nemzeti Közszolgálati Egyetem, 2019. 38.

az Európai Unió által használt dokumentumokba és stratégiákba. Itt a konkrét, kódokkal leírt legközelebb álló fogalmakra gondolunk alapvetően.

Végezetül a *virtuális* szó leginkább az internet immateriális, nem fizikai valóságához vagy természetéhez kapcsolódik. A virtuális valóság lehet immateriális valóság (valami, amit nem lehet megérinteni), és olyan valóság is, amely nem létezik (hamis valóság). A *virtuális* szó, illetve előtag, leginkább a fent említett többértelmű jelentése miatt ritkán jelenik meg a politikai nyelvben és a nemzetközi dokumentumokban, így a kiberdiplomácia világában is elenyésző szerepet játszik.

A *kiber* fogalom a legszélesebb kategóriát képviseli az előtagok között, és a leghasznosabb a kiberdiplomácia világában való eligazodáshoz is. Tudjuk, hogy a diplomácia az államok egymással fenntartott kapcsolatainak gyakorlata, a nemzetközi jogban meghatározott alanyok külkapcsolatainak békés módon és mindenekelőtt tárgyalásos úton történő rendezése. Itt leginkább államokról és nemzetközi szervezetekről beszélünk. A kiberdiplomácia tehát, alapjaiban véve, a kibervilágban folytatott diplomáciaként is értelmezhető lenne, de ez természetesen ennél bonyolultabb.

A kiberdiplomácia meghatározása

A *kiberdiplomácia* fogalmának hatékony megismeréséhez érdemes rövid kitérőt tenni a hagyományos diplomácia világába. Mint ismeretes, a diplomáciát folytató legfőbb szereplők az államok, valamint a nemzetközi intézmények. Az államok a nemzetközi rendszer elsődleges alanyai, amelyek lakossággal és területtel, az erőszak legitim monopóliumával, valamint belső és külső legitimitással rendelkeznek. Az államok központi szerepet játszanak mind a nemzetközi kapcsolatokban, mind a tudományági megfelelőjükben, a nemzetközi kapcsolatok elméletében is. A diplomácia a nemzeti hatalom és érdek nemzetközi kapcsolatokban való érvényesítése, békés eszközökkel.

A kiberdiplomácia fogalma, valamint pontos tudományos meghatározása még mindig vitatott. Eléggé új fogalomról van szó, amely leginkább az angolszász akadémiai világban, és a világ egyik vezető kiberhatalma, az Egyesült Államok tudományos világában jelenik meg. Emellett neves egyesült királyságbeli egyetemek is foglalkoznak a kutatásával. De mindkét akadémiai világban a szakirodalom a legtöbb esetben csak érintőlegesen foglalkozik a kiberdiplo-

máciával, és leginkább a kiberbiztonság és a kiberhadviselés egyik mellékvonalaként tekint rá.

Ha viszont önálló, konkrétan a kiberdiplomáciával foglalkozó cikket keresünk, akkor a leginkább említésre méltó a *Kiberdiplomácia: a nemzetközi társadalom kialakítása a digitális korban* című tanulmány.[7] A szerzők azt állítják, hogy a kiberdiplomácia „növekvő fontossága ellenére továbbra is periferikus kérdés a nemzetközi kapcsolatok irodalmában", valamint kiemelik, hogy a kibernetikus események, köztük a kibertámadások a médiában sokkal nagyobb hangsúlyt kaptak, mint a kiberdiplomácia.

A fentiek alapján a kiberdiplomácia úgy definiálható, mint egy adott állam egyedül vagy több állammal együttesen véghez vitt olyan cselekedeteinek összessége, amelyek külpolitikai célokat és érdekeket szándékoznak érvényesíteni a kibertérben, erősen támaszkodva az információ, az információkommunikáció és a számítógépek felhasználási területeire.

Kiberdiplomácia kontra digitális diplomácia

A kiberdiplomáciát fontos elválasztani egy másik hasonló fogalomtól, a digitális diplomáciától. Ugyan már utaltam a digitális, az *e-,* a virtuális és a kiber fogalmak közötti különbségekre, de fontos megkülönböztetés, hogy a kiberdiplomácia nem egyezik a digitális vagy az e-diplomáciával. Bár hasonló részekből állnak össze, eltérő fogalmakat írnak le. A digitális diplomáciát és az e-diplomáciát viszont egymáshoz hasonló fogalomként használják, azonban mindkettő markánsan különbözik a kiberdiplomáciától.

Amíg a kiberdiplomácia a kibertérben alkotott külpolitikához köthető, a kibertér irányítására tett kísérleteket fedi le, addig a *digitális diplomácia konkrét diplomáciai cselekedeteket takar a kibertérben*. Előbbire példa egy, az internet szabályozásáról szóló nemzetközi egyezmény tárgyalásához a nemzeti álláspont kidolgozása és képviselete tárgyalásos úton, míg utóbbira egy Twitter-üzenet, amelyen egy ország külügyminisztériuma üdvözli például Észak-Macedónia csatlakozását a NATO-hoz. Pontosabban tehát a digitális diplomácia vagy e-diplomácia az információkommunikációs technológiai eszközök és módszerek közvetlen alkalmazása a diplomácia és a külpolitika területén. A kiberdiplo-

[7] André Barrinha – Thomas Renard: Cyber-diplomacy: The Making of an International Society in the Digital Age. *Journal of Global Affairs,* 3. (2017), 4–5. 353–364.

mácia azonban a konfliktuskezelést, a kibertér körüli megállapodásokat jelenti, és az ezzel kapcsolatos politikára utal. Ugyan a digitális és az e-diplomáciát eddig szinonimaként kezeltem, egy másik megközelítés szerint az e-diplomácia fogalmához képest a „digitális diplomácia fogalma szűkebb, alatta elsősorban a közösségi média eszközeit, a Facebookot és a Twittert értik".[8]

A kiberdiplomácia állami megközelítései

Mint általában a politikában, a kibertér rendezésére tett javaslatokban sincs konszenzus az államok és a részes szereplők között. Nincs egyetértés továbbá abban sem, hogy a kiberteret hogyan, illetve kell-e egyáltalán irányítani, illetve szabályozni. Ezek viszont olyan meghatározó kérdések, amelyek átfogják a kiberdiplomáciai kezdeményezéseket, és rendezésük nélkül nem vagy csak nagyon keveset tud a kiberdiplomáciai tér előrehaladni.

Az államok a versengés mellett már hosszú évek óta egyeztetnek a kibertérben érvényes nemzetközi jogról és viselkedési normákról, viszont alapvető különbségek vannak az álláspontok között. Az USA, az Európai Unió, illetve a NATO és tagállamai a kibertér szabad, demokratikus jogállami és biztonságos működését alapvető értéknek és érdeknek tekintik. Ehhez csatlakoznak a hasonló értékrendű és gondolkodású országok. Az úgynevezett nyugati közösség szerint a kibertér szabadságának és biztonságának szavatolása a nemzetek, kormányzatok, a tudományos és a civil szféra közös felelősségvállalásán valósulhat meg, és a többszereplős modellt tartják fontosnak. Nyugati megközelítésben a nemzetközi jognak teljes mértékben érvényesülnie kell a kibertérben, beleértve a nemzetközi humanitárius jogot és az önvédelemhez való jogot is.

A nyugati felfogással szemben Kína, Oroszország és több fejlődő ország az államok tradicionális szuverenitásának a kibertérre történő kiterjesztését támogatja, és ellenzik a közös szerepvállalást. Ezek az államok alapvetően inkább kormányközi modell alapján képzelik el az internetszabályozást. Sok helyen eltér a véleményük a nyugati csoporttól, például ezen államok szerint a kibertérre nem lehet érvényesnek tartani a hadviselésre vonatkozó nemzetközi jogot.

Persze államok nem csupán egyedül, önmagukban tudnak kiberdiplomáciát folytatni. Különböző csoportosulások, bilaterális vagy multilaterális formációk vagy szövetségi rendszerek keretében is lehet hasonló tevékenységet folytatni,

[8] Molnár (2019): i. m. 38.

attól függően, hogy melyiknek milyen hozadékát vélik a felek felfedezni. A szabályalapú többnemzeti megközelítés egyik példájaként a NATO-tagállamok elfogadták a *Tallinni kézikönyv*et, amely a kibertérben használandó irányelveket fektet le nemzetek és más, nem nemzeti szereplők számára. A *Tallinni kézikönyv* és több, más konkrét lépés miatt a NATO-ról, illetve a tagállamairól elmondható, hogy támogatják a kibertér nemzetek felett álló szabályozását. Az SCO (a Sanghaji Együttműködési Szervezet) országai viszont alapvetően eltérő megközelítést képviselnek. Ezek az országok, köztük Kína és Oroszország, a szuverenitás fontosságát hangsúlyozzák a kibertérben, és csak olyan szabályozást támogatnak, ami a nemzeti szuverenitás alatt helyezkedik el. A két megközelítés szögesen ellentmond egymásnak, emiatt a kibertérben nem pusztán kiberdiplomáciának leszünk tanúi, hanem kibertámadásoknak, és, amennyiben a helyzet eszkalálódik, akár kiberháborúnak is.

A kibervilághoz kötethő fogalmak a nemzetközi kapcsolatok szakirodalmában

A kiberhez köthető előtagok, valamint a kiberdiplomácia fogalmainak pontos meghatározása után érdemes a többi, a kiberdiplomáciához köthető fogalmat is megvizsgálni. A két leginkább elterjedt fogalom a kibertér és a kiberbiztonság. A kibertér meghatározásában sincs ugyan egyetértés, de összességében azért elmondható, hogy a „meghatározások túlnyomó többségében három értelmezéssel találkozhatunk: a kibertér egy sajátos (képzeletbeli, virtuális) környezet; a kibertér egy tartomány; a kibertér egy hálózat”.[9] Nézzük továbbá, hogy mi az a kiberbiztonság! Krasznay szerint a kiberbiztonság:

> „a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amely azért, hogy a társadalmi és gazdasági folyamatok zavartalanul működhessenek, a kibertérben lévő kockázatok elfogadható szintjét hivatott biztosítani, ezáltal pedig megcélozni a kibertér megbízható környezetté alakulását.”[10]

[9] Krasznay Csaba: *A kibertér fogalma, értelmezése és fejlődése. Információbiztonság vs. kiberbiztonság.* Budapest, NKE Kiberbiztonsági Akadémia, 2018.

[10] Krasznay (2018): i. m.

Itt megemlítendő, hogy a kiberbiztonság fogalmát érdemes különválasztani az információs biztonság fogalmától is, amely az informatikai rendszerek olyan állapota, amelyben a kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása biztosított.

A következő fontos, vizsgálatra érdmes fogalom a kiberháború. Mint a hagyományos diplomáciát a háborútól, úgy a kiberdiplomáciát a kiberháborútól sem lehet vegytisztán és könnyedén elválasztani, sőt a két párhuzamos fogalom között sok hasonlóságot lehet felfedezni. A kiberháború kutatásánál is kiemelten fontos kérdés természetesen az, hogy a kiberháború hagyományos értelemben vett háborúnak tekinthető-e. Mint a legtöbb tudományos vitában, ebben a viszonylag egyszerűnek tűnő kérdésben sincs egyetértés. Az egyik oldal kiáll amellett, hogy a kiberháború megfelel a hagyományos értelemben vett háború követelményeinek, míg a másik oldal szerint ez semmiképpen sem igaz, és a kiberháború fogalmát új alapokra kell helyezni.

Az első oldal ékes példájaként Stone amerikai professzor szerint a kiberháború is megfelel a tradicionális értelemben vett háború fogalmának.[11] A kibervilág egy másik tudományos szaktekintélyének számító Joseph Nye is egyetért Stone-nal. Nye szerint a kiberháború leghasznosabb meghatározása a következő: „olyan ellenséges cselekedetek a kibertérben, amelyek hatása legalábbis egyenértékű a jelentős kinetikus erőszakkal."[12]

Itt viszont el is értünk a kiberháború legfontosabb gyakorlati kérdéséhez, amely szerint a kiberteret mint virtuális világot és az azt alátámasztó infrastruktúrát érő támadásokat valamilyen módon kezelni kell. A nehézség abban rejlik, hogy ezeket egyszerre kell tudni egyben kezelni, valamint különválasztani, mivel a kibertámadások két különválasztható hatást válthatnak ki, és két külön térben tehetnek kárt: a kibertérben és a kiberteret alátámasztó fizikai infrastruktúrában.

Amikor a kibertámadások pusztán más számítógépes rendszerek kiiktatását érik el, illetve abban okoznak kárt, például amikor egy hacker leállít egy kormányzati honlapot DDoS-támadással (Distributed Denial of Service, tehát elosztott szolgáltatásmegtagadással járó támadások), akkor a helyzet egyértelmű: csak a kibertérben esik kár. Viszont egyes kibertámadásoknak konkrét kinetikus következményei is lehetnek. Ha a kibertámadás egy nukleáris reaktor vezérlőprogramját támadja meg és állítja le, akkor a nukleáris reaktorban leállás

[11] John Stone: Cyber War Will Take Place! *Journal of Strategic Studies,* 36. (2013), 1. 101.

[12] Joseph S. Nye, Jr.: How Will New Cybersecurity Norms Develop? *The Belfer Center for Science and Internaitonal Affairs, Harvard University*, 2018. március 12.

következhet be, ami akár Csernobil-szintű katasztrófához is vezethet. Ebből már egyértelműen látszik, hogy a kibertámadás kifejezés a tevékenységek széles skáláját öleli fel, kezdve az egyszerű próbáktól a webhelyek megtévesztéséig, a szolgáltatásmegtagadásig, a kémkedésig és a pusztításig.

A kiberháború és a kibertámadások így alapvetően különböznek a tradicionális támadásoktól. Hasonlóképpen a hagyományos diplomáciától is valamelyest eltér a kiberdiplomácia. Két fontos különbséget kell tenni. Az első fontos különbség, hogy a kiberdiplomácia eszközei, részei, valamint egyedi alkotóelemei nem köthetőek egyértelmű földrajzi helyhez. Ez szembemegy a hagyományos diplomácia eszközeivel, ahol a territorialitás kifejezetten fontos alapeleme az interakciónak. Egy állam egy másik államban a saját képviseletét rendkívüli és meghatalmazott nagyköveteken keresztül látja el, amelyeket az 1961. évi diplomáciai kapcsolatokról szóló bécsi egyezményként ismert nemzetközi szerződés egyértelműen szabályoz. A kiberdiplomácia világában a határvonalak nem konkrétak, és gyakran fel sem lelhetők, mivel a kibertérben gyakran a kezdeményező egyén, a cselekvést lefolytató számítógép, és a végpont akár más és más kontinensen található.

A második fontos különbség a cselekvés és a cselekvést véghez vivő egyén közötti kapcsolatban található. A hagyományos diplomáciában egyértelmű a hierarchiai rend: egy küldő ország fogadó államban akkreditált nagykövete képviseli a küldő államot, és a nagykövet cselekedetei a küldő állam jóváhagyásával, úgynevezett mandátumával bírnak. A kiberdiplomáciában és az internetes világban viszont ez sokkal komplikáltabb. Itt az attribúció, vagyis a hiteles hozzárendelés gyakori hiánya komoly problémákat vet fel. A számítógépes eseményeknek ugyan vannak világos végpontjai, ahol akár fellelhető a támadás, de kiindulási pontjuk gyakran nem egyértelmű és könnyedén elbújtatható.

Konkrét példa az attribúciós problémra: vegyünk egy DDoS kibertámadást. A támadás végpontjai egyértelműen megállapíthatók, mivel elég megkeresni a leálló webhelyeket vagy website-okat, illetve azt, hogy ezek melyik számítógépekhez tartoznak. De a támadás eredete sokkal összetettebb kérdés. Sok esetben lehetetlen 100%-os bizonyossággal meghatározni, hogy honnan indult a támadás, mivel a forrás könnyen bújtatható. Szakértők a különbséget bemutatva úgy fogalmaznak, hogy míg a hagyományos világban például egy rakéta egyértelműen rendelkezik viszonválaszcímmel (megvizsgálható a röppályából és a technikai adatokból, hogy honnan lőtték ki), addig egy számítógépes botnet általában nem rendelkezik ilyennel. A támadó azonosításához szükséges munka hónapokat vehet igénybe, és egyáltalán nem biztos, hogy a támadó azonosítása

minden esetben lehetséges. Például a 2010. évi Stuxnet-támadás megkérdőjelezhetetlen attribúciókérdése mindmáig alapvetően bizonytalan. Bár általános egyetértés van abban, hogy az Egyesült Államok és Izrael közös művelete volt, amíg a két állam ezt el nem ismeri hivatalosan, nem lehet minden kétséget kizáróan őket okolni a támadásért.

Elmondható, hogy a kiberdiplomácia a hagyományos diplomácia világától gyökeresen eltérő térben működik. A kibertérben nincsenek földrajzi korlátozások, és számos esetben gyakorlatilag nincs hiteles attribúcióra lehetőség, pedig mind a két szempont a hagyományos diplomácia elméleti és gyakorlati sarokköveit képezi. Szinte minden tudós egyetértett ezekben a különbségekben, de hogy ezeknek mekkora szerepük van, illetve hogy milyen mértékben befolyásolják a kiberdiplomáciát és annak megvalósítását, arról nincs egyetértés.

A kiberdiplomácia célja: a hatalom, reciprocitás és normák szerepe

A kiberdiplomácia meghatározása, illetve az állami szereplők feladatköre mellett fontos értelmezési kérdés, hogy milyen célt szolgál a kiberdiplomácia. Természetesen ez a kérdés is tudományos viták tárgyát képezi, viszont abból a szempontból hasznos elméleti megközelítés, hogy segít rendezni a szakirodalmat az érdeklődő részére. A kiberdiplomáciáról szóló szakirodalmat három nagy kategóriába lehet sorolni attól függően, hogy az író és a kutató a nemzetközi kapcsolatok elméletéről melyik nagy „iskola" mentén gondolkodik.

Az első csoport a kiberdiplomáciának a hatalommal való összekapcsolódását tartja a legfontosabbnak. A második nagy csoport a reciprocitást és a kölcsönösséget helyezi előtérbe, sokszor a törvényre és a jogi szerződésekre való fókuszálással. Végezetül a harmadik nagy csoport pedig a normákhoz és a viselkedési mintákhoz fűződő kapcsolatokat tartja legfontosabbnak a kiberdiplomáciában. A nemzetközi kapcsolatok elméletében ezek a csoportok a realizmust, a liberalizmust és a konstruktivizmust követik le.

Így a nemzetközi kapcsolatokban a háború és béke kérdéseire is, a kibervilág rendezésére, illetve a kiberdiplomáciában is ezt a három fő megközelítési módot különböztetjük meg. A megközelítések a hatalomra, a reciprocitásra vagy a normákra helyezik a hangsúlyt. Kritikus kérdés lesz, hogy melyik gondolkodásmód fog az államok közötti kapcsolatokban leginkább elterjedni, és hogy sikerül-e az államoknak és a kibertérben szerepet vállaló cselekvőknek egyetértésre jutniuk.

A realista megközelítésnél a szerzők elsősorban úgy gondolkodnak, hogy a kiberdiplomácia pusztán a háború kiegészítése. A kiberdiplomáciát a szerzők szerint leginkább a katonai erőfeszítésekkel való összefüggésben lehet megérteni. Ez a csoport a kiberdiplomáciára egyszerűen úgy tekint, mint az államok nemzeti érdekeik, saját szuverenitásuk és a túlélésük megvédése érdekében tett lépések összességére.

A kiberdiplomácia realista megközelítése olyan tradicionális témákra összpontosít, mint a katonai hatalom és a gazdasági erő. Ezek olyan gondolati elemek, amelyek máshol is jelen vannak a realista irodalomban. A hatalom szerepe e szerzők szerint kiemelkedően fontos a kiberdiplomácia világában, és a hatalom felhasználásának legfontosabb formái a katonai erőforrások és eszközök. A realista írók a kiberdiplomáciát az erőszakhasználat kiegészítéseként határozzák meg. Ők kutatásaik során különös tekintettel vannak a kiberelrettentés, a kibervédelem és a kiberkényszerítés fogalmaira, a kiberdiplomáciát hasonlónak tartják a nukleáris diplomáciához.

Egy másik megközelítés, a liberalizmus és a liberális megközelítés középpontjában a reciprocitás, a kölcsönös függőség, a nemzetközi szervezetek, valamint az állami szereplők viszonossága és a jogi szerződések állnak. Ez a fajta szakirodalom a katonai erő helyett a kiberdiplomácia központi szerepét hangsúlyozza a kibertér szabályozásának és a kiberbiztonság növelésének érdekében. Itt az irodalom a liberalizmus alapvető gondolataihoz tér vissza: a kölcsönös gazdasági függőséghez, a nemzetközi szervezetek szerepéhez, valamint a demokratikus békeelmélethez.

A kiberdiplomácia megközelítéseinek harmadik és egyben utolsó nagy csoportja a nemzetközi kapcsolatok elméletének úgynevezett konstruktivista megközelítésébe sorolható. Ezek az elméleti munkák a társadalmi fogalmi konstrukciók, az identitás és a normák fontosságát hangsúlyozzák a kiberdiplomácia és a kibertér vizsgálatánál. Itt a tudományos munkák elsősorban nem magukra az internetes támadásokra vagy eseményekre összpontosítanak, hanem inkább megpróbálják kitalálni, miért fordulnak elő a támadások vagy események. A szerzők itt például arra kíváncsiak, hogy a normáknak van-e szerepük abban, hogy növekszik vagy csökken a kibertámadások gyakorisága. E megközelítés szerint a kibertérben ugyanúgy, mint a nemzetközi kapcsolatok más területein is, vannak normák, amelyek meghatározzák az egyes államok viselkedését, de a normák hatása államonként jelentősen eltér. A nem kormányzati szervezetek, a civil társadalom és az egyének ennél a megközelítésnél játsszák a legnagyobb

szerepet. Ezek az írók azt állítják, hogy a normák az állami viselkedés legfontosabb mozgatórugói.

Ez a három megközelítés a kiberdiplomácia értelmezésénél nagymértékben eltér egymástól. Ez az eltérés ugyan az államok közötti viselkedés leírására utal, ugyanakkor a napi politikában is komoly szerepet játszik, mivel a kiberdiplomácia szerepét kutatjuk a kibertérben. Ha a realista megközelítés érvényesül, akkor az államok egyfajta „kibervadnyugat"-szerű rendszerben fognak tevékenykedni, és nemzetközi kontroll nélkül, alapvetően önerőre támaszkodva igyekeznek majd nemzeti érdekeiket érvényesíteni. A liberális megközelítés már egy másik, nemzetközi jogra és hozzá kapcsolódó intézményekre épülő kiberdiplomáciai világot feltételez: az államok jól rendezett jogi szerepek között folytatnak kiberdiplomáciát, ahol nemzetközi szerződések határolják be a szerepköröket. A vitás ügyekben nem az erő, hanem a jog és valamilyen nemzetközi „kiberbíróság" lehet majd a mérvadó. A konstruktivista megközelítés szerint pedig alapvetően nem a jogi környezet vagy a nemzetközi szervezet megléte vagy hiánya fogja leginkább meghatározni az államok viselkedését és a kiberdiplomáciát, hanem hogy milyen viselkedésminták vagy normák terjednek el leginkább az államok között.

Az egyes államok megközelítései besorolhatók a három iskola valamelyikébe. Például az Egyesült Államok republikánus vezetés alatt realista, demokrata alatt pedig inkább liberális hozzáállást mutat. Más államok, például Oroszország, aki Kínával és a Sanghaji Együttműködési Szervezet többi tagjával együtt továbbra is támogatja egy ENSZ-alapú, széles körű szerződés megkötését, de csak olyan módon, hogy ne lehessen a nemzeti jogköröket csorbítani, konzekvensen realista. Mivel nincs egyetértés a világ nagyhatalmai között, várhatóan kiemelt szerep fog hárulni az egyetlen globális nemzetközi szervezetre, az ENSZ-re a kiberdiplomáciában.

A kiberdiplomácia és az ENSZ

Az Egyesült Nemzetek Szervezete nemzetközi szervezet, amelyet 1945-ben, a második világháború után alapított 51 ország a nemzetközi béke és biztonság, a nemzetek közötti baráti kapcsolat fejlesztése és a társadalmi fejlődés, valamint a jobb életszínvonal és az emberi jogok elősegítése céljából.[13] Az ENSZ-nek két fő szerve játszik kiemelt szerepet a kiberdiplomáciában. Az egyik a Bizton-

[13] Egyesült Nemzetek Szervezete: *Általános Információ az ENSZ-ről.* (2020. június 1.).

sági Tanács, a másik pedig az ENSZ főtitkára és az általa vezetett Nemzetközi Titkárság.[14]

Az ENSZ Biztonsági Tanácsában a kiberdiplomáciai kérdések egészen 1998-ig nyúlnak vissza. Ekkor Oroszország mint állandó ENSZ BT-tag a testület történetében először javaslatot nyújtott be az elektronikus és információs fegyverek betiltására. A másik fő szereplő, az ENSZ főtitkára, a tagállamoktól független tevékenységet is végez. A főtitkár létrehozott egy kormányzati szakértői csoportot (UNGGE – United Nations Group of Government Experts, az Egyesült Nemzetek Kormányzati Szakértő csoportja), ez 2004 óta ülésezik, valamint jelenleg ülésezik egy OEWG (*open ended working group,* nyílt végű munkacsoport), amely a témát sokszor mélyrehatóan tárgyalja. Mindkét csoport létezése és működése azt jelzi, hogy bár sok a rendezetlen kérdés, az ENSZ mint fórum továbbra is megmaradt a vitás pontok rendezésére tett első kísérlet helyszínének.

Rövid bevezetés Magyarország kiberdiplomáciájába

Végezetül a fejezet nem lenne teljes legalább egy kis magyar kiberdiplomáciai kitekintés nélkül. Sokszereplős a téma, de kijelenthető, hogy a jelenleg hatályos magyar kiberdiplomácia sarokkövét a 2020-as Nemzeti Biztonsági Stratégiában találjuk. Ugyan 2012-ben már készült egy Nemzeti Biztonsági Stratégia, a körülmények, a nemzetközi rendszer és a magyar külpolitika változásai megkövetelték, hogy idén új stratégiát adjon ki a kormány. 2013-ban továbbá készült egy Nemzeti Kibervédelmi Stratégia is, de mindkettőt felülírni látszik az idén tavasszal kiadott új Nemzeti Biztonsági Stratégia. A stratégia leginkább idevágó cikkelyei a 31-es, 32-es és a 48-as.

A 31. cikkely egyértelműen a kibervédelemmel foglalkozik, és a honvédelmi tárcához rendeli a felelősséget a magyar kormányzaton belül. Itt kibertámadások elhárításáról van szó, és a stratégia összeköti a hibrid, valamint a kiber- és kinetikus komponenseket egyszerre tartalmazó támadásokat.

Hibrid támadással szembeni ellenálló képességünket növeli a nemzet egysége, demokráciánk szilárdsága, a közös nyelv, a felgyorsított döntéshozatali képesség, valamint a honvédelmi és rendvédelmi erők szoros együttműködése egymással és a releváns polgári infrastruktúrával. Az új biztonsági kihívások

[14] Egyesült Nemzetek Szervezete: *Általános Információ az ENSZ-ről*. (2020. június 1.).

miatt azonban folyamatosan szükséges fejleszteni az információs és kiberhadviselés elleni védekezés rendszerét. [15]

A 32. cikkely az információs biztonságról szól, és megnevezi azt mint a kiberbiztonság egyik alapkövét.

Magyarország kormánya mindent megtesz hazánk kiberbiztonsága érdekében, kapacitásainkat e területen is folyamatosan fejlesztjük. Tekintettel arra, hogy a kormányzati és más kulcsfontosságú infokommunikációs rendszerek elleni támadások száma növekszik és kifinomultságuk erősödik, folyamatos erőfeszítés szükséges az infokommunikációs rendszerek védelmének erősítése érdekében. Általános jelenség továbbá a felhasználók információbiztonsági tudatosságának alacsony szintje, holott a felhasználók megfelelő információbiztonsági tudatossága a kiberincidensek megelőzésének egyik kulcseleme.[16]

Végül a 48. cikkelyben találjuk meg leginkább annak az elméleti leírásnak a vonatkozó, releváns értelmezését, amelyet a fenti vonatkozásban kifejtettem. Itt a kiberteret mint globális közjót tüntetik fel, amiért verseny folyik. Az 5G technológiáért folyó küzdelem pedig jól mutatja a kiberdiplomáciát a gyakorlatban: hogy melyik nagyvállalat telepíti ezt a technologiát egyes országokba, például az Ericsson vagy a Huawei, elköteleződést mutat az egyes országok között, és a nem egyeztetett vagy egyoldalú lépések komoly feszültségeket is kelthetnek a szövetségi rendszereken belül, mint például a NATO-ban.

A hatalmi vetélkedés mindinkább kiterjed a globális közjavakra is: fokozódó küzdelem folyik a nemzetközi vizek és az ott található erőforrások, az Északi-sarkvidék és a világűr ellenőrzéséért, valamint a kibertér dominanciájáért. Az emberiség technológiai szintjének rohamos fejlődésével (digitalizáció, ötödik generációs vezeték nélküli hálózat [5G], űrtechnológia stb.) folyamatosan új lehetőségek és kihívások jelennek meg, amelyek hatást gyakorolnak hazánk biztonságára. Az 5G jelentette technológia olyan forradalmi fejlesztéseket tehet lehetővé perspektivikusan, amelyek számottevő változásokat generálhatnak társadalmunk és gazdaságunk viszonylatában.[17]

Fontos még kiemelni, hogy a Nemzeti Biztonsági Stratégia szerint kiemelt biztonsági kockázatot képeznek a „jelentős károkat okozó kibertámadások a kormányzati informatikai rendszerek, az E-közigazgatás, a közműszolgálta-

[15] 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról (a továbbiakban: Nemzeti Biztonsági Stratégia). 31. cikk.

[16] Nemzeti Biztonsági Stratégia (2020): i. m. 32. cikk.

[17] Nemzeti Biztonsági Stratégia (2020): i. m. 48. cikk

tók, a stratégiai vállalatok, a létfontosságú infrastruktúra egyéb elemei és más, a társadalom működésében fontos szervezetek számítógépes hálózatai ellen".[18]

A stratégia mellett több szereplő foglalkozik valamilyen módon a kibertérrel és a kiberbiztonsággal Magyarországon, de a kiberdiplomáciához leginkább a Külgazdasági és Külügyminisztérium, valamint a Honvédelmi Minisztérium releváns egységei köthetők. A Külgazdasági és Külügyminisztérium kibertér-koordinátora a következő feladatokat látja el:

> „Koordinálja a kibertérrel kapcsolatos feladatok minisztériumon belüli végrehajtását, feladatkörében képviseli a minisztériumot a Nemzeti Kiberbiztonsági Koordinációs Tanácsban, és más hazai egyeztetési fórumokon, valamint kapcsolatot tart az illetékes minisztériumokkal, egyéb szervezetekkel és a kibertérrel foglalkozó nemzetközi szervezetekkel, valamint részt vesz a kibertérrel kapcsolatos magyar álláspont kidolgozásában, és gondoskodik annak összehangolt képviseletéről a bilaterális és multilaterális kapcsolatokban, tárgyalási folyamatokban és fórumokon, és végezetül pedig segíti a kiberbiztonsággal foglalkozó magyar cégek külföldi tevékenységét."[19]

A Honvédelmi Minisztérium alatt pedig a Magyar Honvédségnek „kibervédelmi központja" jött létre 2019-ben. A HM felügyelete alatt „a kibertérben jelentkező fenyegetések elhárításához naprakész, magas színvonalú oktatásra van szükség. E képzést a katonák számára a Magyar Honvédség Kiber Képzési Központja biztosítja majd."[20] Benkő Tibor honvédelmi miniszter szerint pedig

> „a kibertérben alkalmazott megtévesztő információk, zavaró tényezők, blokkoló rendszerek a hibrid hadviselés révén nemcsak a műveleti feladatok végrehajtására hathatnak ki, de békeidőben az állami működésre is. Ennek oka, hogy napjainkban már minden elektronikus formában, számítógépeken keresztül működik az orvosi ellátástól a közlekedésen át egészen az adatok nyilvántartásáig. A fenyegetések elleni védekezésre fel kell készülni, ehhez pedig megfelelő oktatási és kiképzési rendszerre van szükség."[21]

Itt fellelhető a két tárca közötti megközelítésbéli különbség. Míg a kibertér-koordinátornál a diplomáciára helyezik a hangsúlyt, a honvédelmi tárcánál már

[18] Nemzeti Biztonsági Stratégia (2020): i. m. 124. cikk.
[19] 17/2018. (VI. 11.) KKM utasítás a Külgazdasági és Külügyminisztérium Szervezeti és Működési Szabályzatáról.
[20] Átadták a Magyar Honvédség Kiber Képzési Központját. *Honvédelem.hu,* 2020. június 1.
[21] Átadták a Magyar Honvédség Kiber Képzési Központját. (2020): i. m.

egyértelműen fellelhetők a védelmi vonatkozású megközelítések, amelyek a tárcára és a honvédelmi meglátásokra egyaránt jellemzőek.

Felhasznált irodalom

1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról. Online: https://net.jogtar.hu/jogszabaly?docid=A20H1163.KOR&txtreferer=00000001.txt

4/2019 (III. 13.) KKM utasítás a Külgazdasági és Külügyminisztérium Szervezeti és Működési Szabályzatáról. Online: https://2015-2019.kormany.hu/download/a/64/91000/A%20Külgazdasági%20és%20Külügyminisztérium%20SZMSZ-e.pdf#!DocumentBrowse

Átadták a Magyar Honvédség Kiber Képzési Központját. *Honvédelem.hu,* 2019. június 13. Online: https://honvedelem.hu/media/aktualis-videok/atadtak-a-magyar-honvedseg-kiber-kepzesi-kozpontjat.html

Barrinha, André – Thomas Renard: Cyber-diplomacy: The Making of an International Society in the Digital Age. *Journal of Global Affairs,* 3. (2017), 4–5. 353–364.

Egyesült Nemzetek Szervezete: *Általános információ az ENSZ-ről* (2020. június 1.). Online: www.unis.unvienna.org/unis/hu/topics/un-general.html

Krasznay Csaba: *A kibertér fogalma, értelmezése és fejlődése. Információbiztonság vs. kiberbiztonság.* Budapest, NKE Kiberbiztonsági Akadémia, 2018.

Molnár Dóra: *Törékeny nagyhatalmiság: a kiberbiztonság.* Budapest, Nemzeti Közszolgálati Egyetem, 2019.

Munk Sándor: A kibertér fogalmának egyes, az egységes értelmezést biztosító kérdései. *Hadtudomány,* 28. (2018), 1. 113–131.

Nemzeti Biztonsági Stratégia 2020. 1. melléklet az 1163/2020. (IV. 21.) Korm. határozathoz.

Nye, Joseph S. Jr: Cyber Power. *The Belfer Center for Science and International Affairs, Harvard University*, 2010. Online: www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf.

Nye, Joseph S. Jr.: How Will New Cybersecurity Norms Develop? *The Belfer Center for Science and Internaitonal Affairs, Harvard University,* 2018. március 12. Online: www.belfercenter.org/publication/how-will-new-cybersecurity-norms-develop.

Stone, John: Cyber War Will Take Place! *Journal of Strategic Studies,* 36. (2013), 1. 101–108.

Weiner, Norbert: *Cybernetics: Or Control and Communication in the Animal and the Machine.* Paris, Hermann & Cie & Camb. Mass. (MIT Press), második, javított verzió, 1961.

Ajánlott irodalom

Barnard-Wills, David – Debi Ashenden: Securing Virtual Space: Cyber War, Cyber Terror, and Risk. *Space and Culture,* 15. (2012), 2. 110–123.

Betts, Richard K.: The Soft Underbelly of American Primacy: Tactical Advantages of Terror. *Political Science Quarterly,* 117. (2002), 1. 19–36.

Buchan, Russel: Cyber attacks: Unlawful Uses of Force or Prohibited Interventions? *Journal of Conflict and Security Law,* 17. (2012), 2. 211–227.

Clark, Richard A. – Robert K. Knake: *Cyber War: The Next Threat to National Security and What to Do About It*. New York, HarperCollins, 2010.

De Bruijn, Hans – Marijn Janssen: Building Cyber Security Awareness: The Need for Evidence-based Framing Strategies. *Government Information Quarterly,* 34. (2017), 1. 1–7.

Denning, Dorothy E.: Framework and Principles for Active Cyber Defense. *Computers and Security,* 40. (2013). 108–113.

Department of State of the United States: *Office of the Coordinator for Cyber Issues* (2020. április 1). Online: www.state.gov/about-us-office-of-the-coordinator-for-cyber-issues/

Dinstein, Yoram: The Principle of Distinction and Cyber War in International Armed Conflicts. *Journal of Conflict and Security Law,* 17. (2012), 2. 261–277.

Elliott, David: Deterring strategic Cyber attack. *IEEE Security and Privacy,* 9. (2011), 5. 36–40.

Farwell, James P. – Rafael Rohozinski: Stuxnet and the Future of Cyber War. *Survival,* 53. (2011), 1. 23–40.

Geers, Kenneth: The Challenge of Cyber Attack Deterrence. *Computer Law and Security Review,* 26. (2010), 3. 298–303.

Junio, Timothy J.: How Probable is Cyber War? Bringing IR Theory Back In to the Cyber Conflict Debate. *Journal of Strategic Studies,* 36. (2013), 1. 125–133.

Lawson, Sean: Putting the „War" in Cyberwar: Metaphor, Analogy, and Cyber Security Discourse in the United States. *First Monday,* 17. (2012), 7.

Liff, Adam P.: Cyber War: A New „Absolute Weapon"? The Proliferation of Cyberwarfare Capabilities and Interstate War. *Journal of Strategic Studies,* 35. (2012), 3. 401–428.

Lindsay, Jon R.: The Impact of China on Cyber Security: Fiction and Friction. *International Security,* 39. (2015), 3. 7–47.

Lindsay, Jon R.: Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence against Cyberattack. *Journal of Cybersecurity,* 1. (2015), 1. 53–67.

Lynn, William J. III.: Defending a New Domain: The Pentagon's Cyberstrategy. *Foreign Affairs,* 89. (2010), 5. 97–108.

McGraw, Gary: Cyber War is Inevitable (Unless We Build Security In). *Journal of Strategic Studies,* 36. (2013), 1. 109–119.

Magyarország Nemzeti Biztonsági Stratégiája „Biztonságos Magyarország egy változékony világban". *Magyar Közlöny,* 2020. április 21.

Nye, Joseph S. Jr.: Nuclear Lessons for Cyber Security?. *Strategic Studies Quarterly,* 5. (2011), 4. 18–38.

Nye, Joseph S. Jr.: *The Future of Power.* New York, Public Affairs, 2011.

Nye, Joseph S. Jr.: Deterrence and Dissuasion in Cyber space. *International Security,* 41. (2016), 3. 44–71.

Power, Marcus: Digitized Virtuosity: Video War Games and Post-9/11 Cyber-Deterrence. *Security Dialogue,* 38. (2007), 2. 271–288.

Valeriano, Brandon – Ryan C. Maness: *Cyber War versus Cyber Realities: Cyber Conflict in the International System.* Oxford, Oxford University Press, 2015.